ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

https://doi.org/10.31649/1997-9266-2018-140-5-41-52

УДК 681.327.12

В. В. Ковтун[1]

КОНЦЕПЦІЯ ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ МОВЦЯ У ПРОЦЕС АВТЕНТИФІКАЦІЇ ДЛЯ ДОСТУПУ ДО КРИТИЧНОЇ СИСТЕМИ

[1]Вінницький національний технічний університет

Запропонована відповідна актуальному стандарту безпеки інформаційних систем ISO/IEC 27001:2013, обчислювальна ефективна та зручна для користувача концепція надійної автентифікації для мультисерверної інформаційної системи критичного застосування, до складу якої входить, зокрема, множина користувачів, множина серверів та виділений сервер-реєстраційний центр для обліку об'єктів системи без ведення верифікаційних таблиць. Інформаційний обмін між об'єктами системи організовано з використанням захищених сесій на основі ключів з механізмом узгодження на основі односторонніх хеш-функцій та криптографії еліптичних кривих, яка на сьогодні забезпечує найкраще співвідношення надійності шифрування по відношенню до довжини ключа серед існуючих криптосистем. Роботу з користувачами персоніфіковано за допомогою індивідуальних карт доступу, які захищено на основі положень криптографічної теорії еліптичних кривих. На картах доступу, окрім ідентифікаційної інформації та паролю, зберігається біометрична інформація про особливості голосу користувача у вигляді вектора-еталона індивідуальних ознак. Додаток для автентифікації, який встановлюється на обчислювальному засобі користувача, ініціюється двоступінчастою процедурою розпізнавання користувача (за умови наявності ідентифікаційної карти) – за індивідуальними особливостями його голосу та за введеним паролем, що разом зі зручністю забезпечує надійність процесу автентифікації. Запропоновану у статті базову концепцію впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи протестовано та обґрунтовано її відповідність стандарту ISO/IEC 27001:2013. Втім, досвід практичної експлуатації системи автентифікації для доступу до ресурсів інформаційної системи критичного застосування виявив у базовій концепції низку вразливостей, з метою позбавлення яких створено удосконалену концепцію, яка містить відповідні механізми захисту і також повністю задовольняє вимогам стандарту ISO/IEC 27001:2013. Оцінено обчислювальну ефективність запропонованих концепцій шляхом підрахунку кількості найбільш обчислювально складних операцій — масштабованого множення T_m та обчислення хеш-функції T_h під час проведення автентифікації об'єктів у складі інформаційної системи критичного застосування (користувача, сервера, реєстраційного центру та всіх цих об'єктів разом). Підсумкова обчислювальна складність базової концепції склала $4T_m + 15T_h$, а удосконаленої — $6T_m + 17T_h$, що в абсолютних показниках є середнім результатом порівняно з аналогами, але застосування криптографії еліптичних кривих робить операції хешування приблизно у 6 разів швидшою від застосованої у аналогах криптографії з відкритим ключем.

Ключові слова: автоматизована система розпізнавання мовців критичного застосування, автентифікація, криптосистема.

Вступ

Швидкий розвиток мережевих технологій загалом та технологій розподілених обчислень зокрема спричинив зміни в архітектурі інформаційних систем критичного застосування (ІКС) у напрямку переходу від односерверної до мультисерверної їхньої організації. Мультисерверним ІКС властива значно більша обчислювальна потужність та комунікаційні можливості, стійкість до перевантаження, підтримка сучасних протоколів віддаленого резервування інформації тощо [1].

Втім, архітектурна еволюція ІКС у напрямку мультисерверної архітектури привела до зростання складності задачі забезпечення їхньої інформаційної безпеки, зокрема, у вирішенні завдання надійної автентифікації. Так у випадку односерверних ІКС основна задача інформаційної безпеки полягає у забезпеченні надійної взаємної автентифікації користувачів і системи, представленої сервером, а у мультисерверних ІКС ця задача набуває комплексності у зв'язку з необхідністю взаємної автентифікації апаратних елементів мільтисерверної структури. Ця обставина привела до неможливості або недоцільності адаптації створених для односерверних ІКС концепцій процесу автентифікації [2]—[4] для використання у мультисерверних ІКС. Адже навіть у першому наближенні у разі застосування цих концепцій автентифікації користувачеві необхідно було б пройти незалежні процедури реєстрації на кожному із серверів у складі ІКС і, відповідно, здійснювати незалежні процедури взаємної автентифікації з ними для здійснення інформаційного обміну. Питання ж внутрішньої безпеки міжсерверної взаємодії у таких концепціях взагалі не розглядається.

Отже, для задоволення вимог безпеки мультисерверних ІКС відповідно до актуальних стандартів безпеки інформаційних систем та забезпечення обчислювальної ефективності процесу автентифікації у багатосерверному середовищі, в останні роки запропоновано багато концепцій організації процесу автентифікації. Зокрема, відомі концепції з використанням верифікаційних таблиць [5], з апаратним захистом на основі карт доступу [6], на основі індивідуальних біометричних характеристик людини [7], з використанням нейронних мереж з динамічним ідентифікатором [8], з використанням цифрового підпису або хеш-функцій [7], [9]. Проте цим системам властива або вразливість до певних видів атак, або низька обчислювальна ефективність, або суттєвий дискомфорт для користувача під час здійснення процедури автентифікації. Наявність цих недоліків зумовлює актуальність задачі покращення концепції забезпечення надійної автентифікації для доступу до ІКС.

Постановка задачі дослідження

Враховуючі виявлені недоліки існуючих концепцій процесу автентифікації, *метою статті* є створення відповідної концепції для мультисерверної ІКС з множиною об'єктів-учасників, яка включає множину користувачів, множину серверів та виділений сервер-реєстраційний центр для обліку об'єктів системи без ведення верифікаційних таблиць. Інформаційний обмін між об'єктами системи пропонується організувати у вигляді захищених сесій на основі ключів з механізмом узгодження на основі односторонніх хеш-функцій та криптографії еліптичних кривих [10], яка на сьогодні забезпечує найкраще співвідношення надійності шифрування по відношенню до довжини ключа серед існуючих криптосистем. Роботу з користувачами пропонується персоніфікувати, застосувавши захищені на основі положень криптографічної теорії еліптичних кривих індивідуальні карти доступу на яких, окрім ідентифікаційної інформації та паролю, зберігатиметься індивідуальна біометрична інформація про особливості голосу. Додаток для автентифікації, який встановлюватиметься на обчислювальному засобі користувача, ініціюватиметься двоступінчастою процедурою розпізнавання користувача (за умови наявності ідентифікаційної карти) — за індивідуальними особливостями його голосу та за введеним паролем, що поряд зі зручністю забезпечуватиме надійність процесу автентифікації. Також у статті необхідно виконати аналіз стійкості запропонованої концепції для автентифікації до видів атак згідно зі стандартом [11] та оцінити її обчислювальну ефективність.

Базова концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи

Для включення у склад ІКС сервер S_j має пройти процедуру реєстрації у реєстраційному центрі (Registration Center, *RC*), яка включає таку послідовність дій:

1. $S_j \to RC : SID_j$. Сервер S_j, використовуючи захищене з'єднання, передає у центр *RC* свій унікальний ідентифікатор SID_j;

2. $RC \to S_j : h\left(SID_j \| y\right)$. У центрі *RC* обчислюється секретний ключ $R_j = h\left(SID_j \| y\right)$ для сервера S_j, де y — частина секретного ключа *RC* для реєстрації сервера, $h(\ )$ — одностороння хеш-функція [10], а $\|$ — операція конкатенації. Центр *RC* надсилає секретний ключ R_j захищеним каналом зв'язку серверу S_j для зберігання.

Аналогічно користувач U_i також спочатку має пройти процедуру реєстрації на сервері *RC*, яка включає таку послідовність дій:

1. $U \to RC: \{ID, B, h(PW \| B)\}$. Користувач U_i використовує встановлений на власному обчислювальному засобі додаток для автентифікації (Application for Authentication, *AA*) для утворення еталону свого голосу B_i, вибору та введення унікального ідентифікатора ID_i та паролю PW_i. *AA* обчислює значення $h(PW_i \| B_i)$ та, використовуючи захищене з'єднання, передає у центр *RC* повідомлення $\{ID_i, B_i, h(PW_i \| B_i)\}$;

2. $RC \to U: \{IC(Z, B, h(\ ), d(\ ), \tau)\}$. У центрі *RC* обчислюються секретні ключі $R_i = h(ID_i \| x)$ та $Z_i = R_i \oplus h(PW_i \| B_i)$ для користувача U_i, де x — частина секретного ключа *RC* для реєстрації користувача, $d(\ )$ — симетрична параметрична функція [10], τ_i — поріг надійності для процесу розпізнавання особи *i*-го користувача за індивідуальними особливостями його голосу, який визначається центром *RC* на основі аналізу наданого *i*-м користувачем узагальненого еталону голосу B_i за методом [12], $\oplus$ — операція суми по модулю 2 (XOR). Далі масив інформації $\{Z_i, B_i, h(\ ), d(, \tau_i)\}$ записується на індивідуальну карту користувача (Individual Card, *IC*), яку передають користувачеві з гарантуванням безпеки цієї операції.

Отриманню доступу користувача U_i до ресурсів серверу S_j, який є складовою ІКС, має передувати процедура взаємної автентифікації, у якій прийматимуть участь користувач U_i, сервер S_j та центр *RC*. Ця процедура складатиметься з такої послідовності дій:

1. $U \to S_j: \{ID, X, C_1\}$. Якщо користувач U_i бажає синхронізувати ключ сесії з сервером S_j, він має ініціювати індивідуальну карту *IC*, відкрити додаток *AA* та сформувати, використовуючи його можливості, фонограму із записом власного голосу B_i' для подальшого аналізу. Далі додаток *AA* порівнює індивідуальні ознаки голосу, виділені з B_i', зі збереженими на *IC*, і якщо $d(B_i, B_i') \geq \tau_i$, то процес автентифікації вважається невдалим і описані вище дії потрібно повторювати. Якщо ж $d(B_i, B_i') < \tau_i$, то процедура розпізнавання користувача за індивідуальними ознаками його голосу вважається успішно пройденою і додаток *AA* надає користувачеві U_i можливість ввести свій код ID_i і пароль PW_i, а згодом випадковим чином генерує ціле число $\alpha \in [1, q-1]$, розраховує значення $R_i = Z_i \oplus h(PW_i \| B_i)$, $X = \alpha \times P$ і $C_1 = h(h(ID_i \| x) \| \alpha \times P) = h(R_i \| X)$ та надсилає повідомлення M_1 з параметрами $\{ID_i, X, C_1\}$ серверу S_j. У вищенаведених виразах P є вихідною точкою з адитичної множини точок $E(F_p)$ над скінченим полем F_p, де $E(F_p) = \{(x, y): x, y \in F_p$ задовольняє $y^2 = x^3 + ax + b\} \cup \{O\}$), E — несуперсингулярна еліптична крива над скінченним полем F_p — $E: y^2 = (x^3 + ax + b) \bmod p$, p — велике (1024-2048 біт) просте число, $\alpha, \beta \in [1, p-1]$ — випадково обрані цілі числа, які задовольняють нерівності $(4a^3 + 27b) \bmod p \neq 0$. Ці положення відповідають теорії еліптичної криптографії і детальніше описані у [13];

2. $S_j \to RC: \{ID, X, C_1, SID_j, Y, C_2\}$. Отримавши описане у п.1 повідомлення M_1, сервер S_j генерує випадкове ціле число $\beta \in [1, q-1]$, розраховує значення $Y = \beta \times P$ і параметр $C_2 = h(h(SID_j \| y) \| \beta P) = h(R_j \| Y)$ та надсилає повідомлення M_2 з параметрами $\{ID_i, X, C_1, SID_j, Y, C_2\}$ центру *RC*;

3. $RC \to S_j: \{C_3, C_4\}$. На основі даних із повідомлення M_2 центр *RC* розраховує значення $C_1' = h(h(ID_i \| x) \| \alpha P) = h(h(ID_i \| x) \| X)$ та $C_2' = h(h(SID_j \| y) \| \beta P) = h(h(SID_j \| y) \| Y)$ і перевіряє, чи

виконуються обидві рівності $C_1 = C_1'$ та $C_2 = C_2'$. Якщо ні, то центр *RC* ініціює переривання сесії, а якщо виконуються, то обчислює параметри $V = h\left(h\left(SID_j \| y\right) \| Y \| X\right)$, $W = h\left(h\left(ID_i \| x\right) \| SID_j \| X \| Y\right)$ та коефіцієнти $C_3 = V \oplus W$ і $C_4 = h\left(V \| W\right)$ на їх основі, які включаються у повідомлення $M_3 = \left\{C_3, C_4\right\}$, що надсилається серверу S_j. Параметр W є одноразовим секретним ключем для сесії між користувачем U_i та сервером S_j;

4. $S_j \to U : \left\{Y, C_5\right\}$. Сервер S_j обчислює параметри $V' = h\left(R_j \| Y \| X\right)$, $W' = V' \oplus C_3$ і $C_4' = h\left(V' \| W'\right)$ та перевіряє, чи виконується рівність $C_4 = C_4'$. Якщо рівність не виконується, то сервер S_j перериває сесію, а якщо виконується, то сервер S_j обчислює ключ сесії $SK_j = \beta \times X = \alpha\beta \times P$ і значення параметра $C_5 = h\left(ID_i \| SID_j \| W' \| SK_j\right)$, яке, на додачу до значення *Y*, надсилає повідомленням $M_4 = \left\{Y, C_5\right\}$ користувачеві U_i;

5. $U_i \to S_j : \left\{C_6\right\}$. Додаток *AA*, отримавши повідомлення M_4, обчислює значення $W'' = h\left(R_i \| SID_j \| X \| Y\right)$, $SK_i = \alpha \times Y = \alpha\beta \times P$ і параметр $C_5' = h\left(ID_i \| SID_j \| W'' \| SK_i\right)$ на їх основі, та аналізує, чи виконується рівність $C_5 = C_5'$. Якщо рівність не виконується, то додаток *AA* ініціює переривання сесії, а якщо виконується, то розраховує значення $C_6 = h\left(W'' \| SK_i \| Y\right)$ і надсилає його серверу S_j у складі повідомлення $M_5 = \left\{C_6\right\}$.

6. Сервер S_j розраховує значення $C_6' = h\left(W' \| SK_j \| Y\right)$ та аналізує, чи виконується рівність $C_6 = C_6'$. Якщо рівність не виконується, то сервер S_j ініціює переривання сесії, а якщо виконується, то процес автентифікації користувача U_i для доступу до серверу S_j, який є складовою ІКС, вважається успішно завершеним. Протягом сесії користувач U_i і сервер S_j використовують секретний ключ $SK = \alpha\beta P$.

Якщо користувач U_i бажає змінити пароль чи оновити еталон голосу, який використовується в процесі розпізнавання його особи, йому слід виконати таку послідовність дій:

1. $U \to IC : \left\{B^*\right\}$. Користувач U_i ініціює свою індивідуальну карту *IC*, запускає додаток *AA* та утворює користуючись його можливостями фонограму власного голосу B_i^* для подальшого аналізу;

2. $d\left(B, B^*\right) < \tau \xrightarrow{+} IC : \left\{B^* \to B\right\}$. Додаток *AA* здійснює порівняння наданої фонограми B_i^* з еталоном голосу користувача B_i і якщо нерівність $d\left(B_i, B_i^*\right) < \tau_i$ виконується, то користувачеві U_i надається можливість замінити B_i на B_i^* зі збереженням змін на індивідуальній карті *IC*. Якщо вищезгадана нерівність не виконується, то процес оновлення інформації на карті *IC* припиняється;

3. $U \to IC\left\{PW^*\right\}$. Якщо п. 2 цієї послідовності дій завершився коректно, то додаток *AA* пропонує користувачеві U_i оновити свій пароль, для чого пропонується ввести поточний пароль PW_i та бажаний новий пароль PW_i^*;

4. $PW \overset{?}{=} PW \xrightarrow{+} IC : \left\{PW^*, Z^*\right\} \to \left\{PW, Z\right\}$. Якщо, відповідно до п. 3 цієї послідовності дій, користувач U_i невірно ввів свій поточний пароль PW_i, то додаток *AA* припиняє процес оновлення особових даних. Якщо ж поточний пароль PW_i введено правильно, то додаток *AA* обчислює значення $Z_i^* = Z_i \oplus h\left(PW_i \| B_i\right) \oplus h\left(PW_i^* \| B_i^*\right)$ та замінює значення Z_i та PW_i на картці *IC* користувача U_i новими значеннями Z_i^* та PW_i^*, відповідно.

Аналіз безпеки базової концепції впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи

Згідно з актуальним стандартом безпеки інформаційних систем ISO/IEC 27001:2013 [11] надійна система автентифікації повинна захищати від таких типів атак: атаки із вгадуванням паролю, атаки з відтворенням запису паролю, атаки з використанням викрадених засобів верифікації, атаки з використанням викрадених ідентифікаційних карт, атаки на основі авторизованих аккаунтів користувачів (інсайдерів), спуфінг-атаки, атаки з підбором паролю, атаки зі спробою підробки ключа сесії, атаки на основі частини відомих ключів сесій, атаки на основі ключів сесій довготривалого використання, атаки на основі одноразових паролів, атаки в процесі оновлення паролю, атаки із перевантаженням апаратних засобів.

Вищезапропонована базова концепція безпечного доступу до ресурсів критичної системи захищена від атак із вгадуванням паролю у всіх режимах роботи (он-, офф-лайн, та в процесі обміну повідомленнями між елементами системи). Працюючи в режимі он-лайн центр *RC* однозначно автентифікує користувача *U* після виконання третього етапу послідовності дій для автентифікації користувача. Офф-лайн атака з вгадуванням паролю також не спрацює, оскільки на додачу до паролю *PW* для автентифікації користувача *U* використовується порівняння фонограми голосу особи з еталоном голосу *B*, і лише зі збігом значень цих параметрів в межах порогу τ обчислюється ключ користувача *R* на основі параметра *Z*. Використання односторонніх хеш-функцій та випадкових значень в процесі інформаційного обміну у вигляді повідомлень M_1—M_6 захищає систему від втрати секретних ключів *RC* та *x* при перехоплені цих повідомлень. У запропонованій базовій концепції передбачено захист від атак з відтворенням запису паролю, оскільки весь інформаційний обмін у системі персоніфікується за рахунок ключів *x* та *y* і ключів сесій *SK*, які передаються у хешованих повідомленнях M_4 та M_5 і розшифровуються лише з відомими випадковими числами α і β. Атаки з використанням викрадених засобів верифікації, атаки з використанням викрадених ідентифікаційних карт та інсайдерські атаки не уражують систему, оскільки на серверах *S* та у реєстраційному центрі *RC*, згідно із запропонованою концепцією автентифікації, не зберігається необхідна для верифікації користувача інформація (*PW*, *B*) у явному вигляді. Втім, навіть маючи індивідуальну карту користувача *IC* та знаючи його пароль *PW*, зловмиснику доведеться проходити процедуру голосового розпізнавання. Аналогічно у системі реалізовано захист від спуфінг-атак зі спробами зловмисника видати себе за сервер *S*, центр *RC* або користувача *U*, адже значення $h(ID_i \| x)$, $h(SID_j \| y)$ і *W*, відповідно, забезпечують взаємну ідентифікацію цих складових системи. Захист від атак з підбором паролю забезпечується надійністю вибраного методу хешування на основі еліптичних кривих та постійній взаємній перевірці компонентами системи автентичності одне одного на основі інформації із повідомлень M_1—M_6. Захист від атак зі спробою підробки ключа сесії забезпечуються унікальністю ключів кожної із сесій, повторюваність яких виключається способом їх формування на основі параметра *W* з використанням випадкових чисел α і β, а застосування процедури хешування унеможливлює присутність повторюваних послідовностей у ключах сесій вибраної довжини. Захист системи від атаки на основі ключів сесій довготривалого використання базується на проблемі дискретного логарифмування еліптичних кривих (Elliptic Curve Discrete Logarithm Problem, ECDLP) [12], [14] яка полягає у складності задачі обчислення секретного ключа α на основі відомої точки публічного ключа $Q = \alpha P$ та проблемі протоколу Діфі–Хелмана на еліптичних кривих (Elliptic Curve Diffie–Hellman Problem, ECDHP) [12], [13] яка полягає у складності пошуку $\alpha\beta P$ для відомих точок αP та βP. Тобто, навіть отримавши ключі довготривалого використання *x* та *y*, пароль користувача *PW* і параметри еталону його голосу *B*, зловмисник не розрахує ключ сесій $SK = \alpha\beta P$ без відомих значень α і β. Так само, навіть взнавши αP і βP зловмисник не обчислить ключ сесій *SK*. Одноразові паролі у запропонованій концепції безпечного доступу не передбачені. Стійкість системи до атак у процесі оновлення паролю забезпечується надійністю процесу розпізнавання користувача за індивідуальними параметрами його голосу *B* та необхідністю розрахунку параметра *Z* зі знанням попередньої індивідуальної інформації. Атаки з перевантаженням апаратних засобів не можуть вразити запропоновану систему через те, що процедура автентифікації не може значно завантажити канали зв'язку системи, а кількість користувачів, які можуть спробувати одночасно отримати доступ до системи можна однозначно обмежити кількістю обчислювальних пристроїв зі встановленими додатками для автентифікації.

Таким чином, запропонована базова концепція безпечного доступу до ресурсів критичної системи з використанням інформації про індивідуальні особливості голосу користувача відповідає всім вимогам до такого класу систем, викладеним у актуальному стандарті ISO/IEC 27001:2013.

Удосконалена концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи

Досвід практичної експлуатації системи автентифікації для доступу до ресурсів ІКС виявив у вищенаведеній базовій концепції низку вразливостей, описаних нижче.

Не зважаючи на те, що згідно з базовою концепцією користувач U при реєстрації не надсилає свої індивідуальні дані у центр *RC* у відкритому вигляді, зловмисник все ж може їх отримати, виконавши такі дії: маючи доступ до ресурсів центру *RC* та не захищеного хешуванням значення B_i зловмисник може змінювати пароль PW_i' і обчислювати значення $h' = h\left(PW_i' \| B_i\right)$ допоки воно не зрівняється з надісланим користувачем значенням $h\left(PW_i \| B_i\right)$, що означатиме, що $PW_i' = PW_i$.

Схожою за сутністю є і друга вразливість, пов'язана з несанкціонованим доступом до карти *IC* та додатку *AA*. Припустимо зловмиснику вдалося екстрагувати секретну інформацію $\left\{Z_i, B_i, h(\ ), d(\ ), \tau_i\right\}$ з карти *IC* користувача U_i та перехопити повідомлення $M_1 = \left\{ID_i, X, C_1\right\}$, яке додаток *AA* надсилатиме від імені користувача U_i на сервер S_j. В цьому разі зловмисник може підбирати значення паролю PW_i^* допоки рівність $C_1 = C_1^* = h\left(Z_i \oplus h\left(PW_i^* \| B_i\right) \| X\right)$ не виконається, тобто PW_i^* не збіжиться з PW_i.

І, нарешті, третя вразливість проявляється у разі доступу зловмисника до додатку *AA* та сервера S_j. Нехай зловмисник U_A хоче, щоби сервер S_j автентифікував його як користувача U_i. Для цього U_A на загальних підставах проходить процедуру реєстрації за базовою послідовністю дій і отримує свої секретні дані $Z_A = R_A \oplus h\left(PW_A \| B_A\right) = h\left(ID_A \| x\right) \oplus h\left(PW_A \| B_A\right)$, на основі яких він, знаючи згенероване на його обчислювальному засобі α, обчислює значення $R_A = Z_A \oplus h\left(PW_A \| B_A\right)$, $X = \alpha P$, $C_1 = h\left(R_A \| X\right)$, які надсилає на сервер S_j у вигляді повідомлення $M_1 = \left\{ID_i, X, C_1\right\}$. Отримавши повідомлення M_1, сервер S_j генерує випадкове ціле β та, обчисливши $Y = \beta P$ і $C_2 = h\left(R_j \| Y\right)$, надсилає повідомлення $M_2 = \left\{ID_i, X, C_1, SID_j, Y, C_2\right\}$ у центр *RC*, яке зловмисник U_A перехоплює і заміняє повідомленням $M_2' = \left\{ID_A, X, C_1, SID_j, Y, C_2\right\}$. На основі отриманого повідомлення M_2' центр *RC* перевіряє чи виконуються рівності $C_1 = h\left(h\left(ID_A \| x\right) \| X\right)$ $C_2 = h\left(h\left(SID_j \| y\right) \| Y\right)$, і якщо так, то надсилає серверу S_j повідомлення $M_3 = \left\{C_3, C_4\right\}$. Отримавши повідомлення M_3, сервер S_j перевіряє чи виконується рівність $C_4 = h\left(h\left(R_j \| Y \| X\right) \| h\left(R_j \| Y \| X\right) \oplus C_3\right)$, і якщо так, то обчисливши ключ сесії $SK_j = \beta X = \alpha\beta P$ і $C_5 = h\left(ID_i \| SID_j \| W \| SK_j\right)$, надсилає повідомлення $M_4 = \left\{Y, C_5\right\}$ зловмисникові U_A. Отримавши M_4, зловмисник U_A досягає рівності $C_5 = h\left(ID_i \| SID_j \| h\left(R_i \| SID_j \| X \| Y\right) \| \alpha\beta P\right)$ після чого, обчисливши $C_6 = h\left(h\left(R_i \| SID_j \| X \| Y\right) \| SK_i \| Y\right)$, надсилає його повідомленням $M_5 = \left\{C_6\right\}$ серверу S_j, який, перевіривши виконання рівності $C_6 = h\left(h\left(R_j \| Y \| X\right) \oplus C_3 \| SK_j \| Y\right)$, автентифікує зловмисника U_A як користувача U_i.

Звичайно, у процесі реальної експлуатації запропонованої системи автентифікації імовірність появи вищеописаних вразливостей вкрай низька, але, враховуючи важливість критичних систем, ними не можна нехтувати, тому створимо удосконалену концепцію впровадження автоматизова-

ної системи розпізнавання мовця у процес автентифікації для доступу до критичної системи.

Аналіз процедури реєстрації сервера S_j у центрі *RC*, яку описано у базовій концепції, показав, що запропонована послідовності дій не містить вразливостей, отже, залишається без змін. А от безпеку процедури реєстрації користувача U_i, як виявилося, необхідно підсилити. Удосконалимо цю процедуру, представивши її такою послідовністю дій:

1. $U \to RC:\{ID, B, h(PW \| B \| b)\}$. Користувач U_i використовує додаток *AA* для утворення еталону свого голосу B_i, вибору та введення унікального ідентифікатора ID_i та паролю PW_i. Після чого додаток *AA* генерує випадкове ціле число b_i, обчислює значення $h(PW_i \| B_i \| b_i)$ та, використовуючи захищене з'єднання, передає у центр *RC* повідомлення $\{ID_i, B_i, h(PW_i \| B_i \| b_i)\}$;

2. $RC \to U:\{IC(Z, B, h(\ ), d(\ ), \tau)\}$. У центрі *RC* обчислюються секретні ключі $R_i = h(ID_i \| x) \times P$ та $Z_i = R_i \oplus h(PW_i \| B_i \| b_i)$ і масив інформації $\{Z_i, B_i, h(\ ), d(, \tau_i)\}$ записується на карту *IC*, яку передають користувачеві U_i з гарантією безпеки цієї операції;

3. $AA \to U:\{IC(b)\}$. Додаток *AA* завершує процес реєстрації користувача U_i дозаписавши на карту *IC* значення $\{b_i\}$.

Зазнає удосконалення і процедура взаємної автентифікації користувача U_i і сервера S_j у процесі отримання користувачем U_i доступу до ресурсів серверу S_j за участю центра *RC*:

1. $U \to S_j:\{ID, X, C_1\}$. Користувач U_i ініціює свою карту *IC* і додаток *AA* та формує, використовуючи його можливості, фонограму із записом власного голосу B_i' для подальшого аналізу. Далі *AA* порівнює індивідуальні ознаки, виділені з B_i', зі збереженими на *IC*, і якщо $d(B_i, B_i') \ge \tau_i$, то процес автентифікації вважається невдалим і вищеописану дію потрібно повторювати. Якщо ж $d(B_i, B_i') < \tau_i$, то додаток *AA* надає користувачеві можливість ввести свій код ID_i і пароль PW_i, а згодом випадковим чином генерує ціле число $\alpha \in [1, q-1]$, розраховує значення $R_i = Z_i \oplus h(PW_i \| B_i \| b_i)$, $X = \alpha \times P$, $X' = \alpha \times R_i$ $C_1 = h(h(ID_i \| x) \| \alpha \times P \| \alpha \times R_i) = h(R_i \| X \| X')$ та надсилає повідомлення M_1 з параметрами $\{ID_i, X, C_1\}$ серверу S_j;

2. $S_j \to RC:\{ID, X, C_1, SID_j, Y, C_2\}$. Отримавши описане у п.1 повідомлення M_1, сервер S_j генерує випадкове ціле число $\beta \in [1, q-1]$, розраховує значення $Y = \beta \times P$ і $C_2 = h(ID_i \| X \| C_1 \| R_j \| Y)$ та надсилає повідомлення M_2 з параметрами $\{ID_i, X, C_1, SID_j, Y, C_2\}$ центру *RC*;

3. $RC \to S_j:\{C_3, C_4\}$. На основі даних із повідомлення M_2 центр *RC* розраховує значення $C_1' = h(ID_i \| X \| h(ID_i \| x) \times X)$ та $C_2' = h(ID_i \| X \| C_1 \| h(SID_j \| y) \| Y)$ і перевіряє, чи виконуються обидві рівності $C_1 = C_1'$ та $C_2 = C_2'$. Якщо ні, то центр *RC* ініціює переривання сесії, а якщо виконуються, то обчислює параметри $V = h(h(SID_j \| y) \| Y \| X)$, $W = h(h(ID_i \| x) \times X \| SID_j \| X \| Y)$ та коефіцієнти $C_3 = V \oplus W$ і $C_4 = h(V \| W \| ID_i)$ на їх основі, які включаються у повідомлення $M_3 = \{C_3, C_4\}$, що надсилається серверу S_j;

4. $S_j \to U:\{Y, C_5\}$. Сервер S_j обчислює параметри $V' = h(R_j \| Y \| X)$, $W' = V' \oplus C_3$ і $C_4' = h(V' \| W' \| ID_i)$ та перевіряє, чи виконується рівність $C_4 = C_4'$. Якщо рівність не виконується, то сервер S_j перериває сесію, а якщо виконується, то сервер S_j обчислює ключ сесії

$SK_j = \beta \times X = \alpha\beta \times P$ і значення параметра $C_5 = h\left(ID_i \| SID_j \| W' \| SK_j\right)$, та надсилає повідомлення $M_4 = \{Y, C_5\}$ додатку *AA*;

5. $U_i \to S_j : \{C_6\}$. Додаток *AA*, отримавши повідомлення M_4, обчислює значення $W'' = h\left(SID_j \| X \| Y \| X'\right)$, $SK_i = \alpha \times Y = \alpha\beta \times P$ і параметр $C_5' = h\left(ID_i \| SID_j \| W'' \| SK_i\right)$, аналізує, чи виконується рівність $C_5 = C_5'$. Якщо рівність не виконується, то додаток *AA* ініціює переривання сесії, а якщо виконується, то розраховується значення $C_6 = h\left(W'' \| SK_i \| Y\right)$ і надсилається серверу S_j у складі повідомлення $M_5 = \{C_6\}$.

6. Сервер S_j розраховує значення $C_6' = h\left(W' \| SK_j \| Y\right)$ та аналізує, чи виконується рівність $C_6 = C_6'$. Якщо рівність не виконується, то сервер S_j ініціює переривання сесії, а якщо виконується, то процес автентифікації користувача U_i і сервера S_j вважається успішно завершеним і між ними встановлюється сесія для обміну інформацією з ключем сесії $SK = \alpha\beta P$.

Незначних змін для позбавлення виявленої вразливості зазнала процедура оновлення еталону голосу B_i чи паролю PW_i користувача U_i:

1. $U \to IC : \left\{B^*\right\}$. Користувач U_i ініціює свою карту *IC*, запускає додаток *AA* та утворює, користуючись його можливостями, фонограму власного голосу B_i^* для подальшого аналізу;

2. $d\left(B, B^*\right) < \tau \xrightarrow{+} IC : \left\{B^* \to B\right\}$. Додаток *AA* здійснює порівняння наданої фонограми B_i^* з еталоном голосу користувача B_i і якщо нерівність $d\left(B_i, B_i^*\right) < \tau_i$ виконується, то користувачеві U_i надається можливість замінити B_i на B_i^* зі збереженням змін на індивідуальній карті *IC*. Якщо вищезгадана нерівність не виконується, то процес оновлення інформації на картці *IC* припиняється;

3. $U \to IC\left\{PW^*\right\}$. Якщо п. 2 цієї послідовності дій завершився коректно, то додаток *AA* пропонує користувачеві U_i оновити свій пароль, для чого пропонується ввести поточний пароль PW_i та бажаний новий пароль PW_i^*.

4. $PW \overset{?}{=} PW \xrightarrow{+} IC : \left\{PW^*, Z^*\right\} \to \{PW, Z\}$. Якщо, відповідно до п. 3 цієї послідовності дій, користувач U_i неправильно ввів свій поточний пароль PW_i, то додаток *AA* припиняє процес оновлення особових даних. Якщо ж поточний пароль PW_i введено правильно, то додаток *AA* обчислює значення $Z_i^* = Z_i \oplus h\left(PW_i \| B_i \| b_i\right) \oplus h\left(PW_i^* \| B_i^* \| b_i\right)$ та замінює значення Z_i та PW_i на картці *IC* користувача U_i новими значеннями Z_i^* та PW_i^*, відповідно.

Аналіз безпеки та обчислювальної ефективності концепцій впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи

Введення додаткового випадкового цілого числа b_i, яке використовується у процесі автентифікації додатком *AA* і сервером S_j, але у явному вигляді невідоме центру *RC*, дозволяє вважати, що удосконалену концепцію убезпечено від першої з виявлених вразливостей базової концепції. Взагалі для того, щоби зловмисник видав себе за користувача U_i перед сервером S_j йому необхідно буде згенерувати правильне повідомлення $M_1 = \{ID_i, X, C_1\} = \left\{ID_i, \alpha \times P, h\left(ID_i \| \alpha \times P \| X'\right)\right\} =$ $= \left\{ID_i, \alpha \times P, h\left(ID_i \| \alpha \times P \| \alpha \times h\left(ID_i \| x\right) \times P\right)\right\}$, яке включає значення $h\left(ID_i \| x\right) \times P$, підробити яке без доступу до сервера S_j і центру *RC* неможливо. Складнішою для системи автентифікації буде

ситуація, в якій зловмисник отримав доступ до карти *IC* і дешифрував інформацію $\{Z_i, B_i, h(\ ), d(\ ), \tau_i\}$, яка на ній записана. У такому разі зловмисник зможе обчислити значення X, але обчислити правильне значення $X' = \alpha \times R_i = \alpha \times Z_i \oplus h\left(PW_i \| B_i \| b_i\right)$ для розрахунку параметра C_1, не маючи паролю PW_i, він не зможе. Якщо зловмисник захоче видати себе за сервер S_j перед користувачем U_i, йому необхідно підробити повідомлення $M_4 = \{Y, C_5\}$, маючи інформацію з повідомлення $M_1 = \{ID_i, X, C_1\}$, для чого необхідно обчислити значення $h\left(ID_i \| x\right) \times X$, що можливо лише за відомого секретного ключа x, який зберігається лише у центрі *RC*. Якщо зловмисник спробує перехопити повідомлення M_1, надіслане користувачем U_i з метою видати себе за нього перед сервером S_j, то він не зможе правильно обчислити ключ $SK_i = \alpha\beta \times P$, адже не знатиме значення випадкового цілого α, і відповідно, не зможе надіслати серверу S_j правильного повідомлення $M_5 = \{C_6\}$. Взагалі інформаційний обмін у процесі аутентифікації за удосконаленою концепцією повністю регламентований множиною повідомлень $M = \{M_1, M_2, \ldots, M_5\}$ із вбудованими автентифікаційними кодами $C = \{C_1, C_2, \ldots, C_6\}$ і для вдалого втручання у цей процес зловмисникові фактично слід мати доступ до карти *IC*, додатку *AA* (секретний код R_i), сервера S_j (секретний код R_j) і центру *RC* (секретні коди x та y). Але навіть якщо зловмисник знає всі ці параметри і здатний підробляти інформаційні повідомлення системи, то під час обчислення ключа сесії $SK_j = \alpha\beta \times P$ він стикнеться з ECDLP-проблемою. Таким чином, удосконалена концепції впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи має всі переваги базової концепції і захищена від виявлених експлуатаційних вразливостей стійкістю математичного апарату еліптичної криптографії та індивідуальністю голосу людини.

Оцінювання обчислювальної ефективності запропонованих концепцій впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи виконаємо, підрахувавши кількість операцій масштабованого множення T_m та обчислення хеш-функції T_h при проведенні автентифікації об'єктів системи безпеки (користувача U_i, сервера S_j, центру *RC* та всіх цих об'єктів разом). Ці операції є обчислювально найзатратнішими, і часом на виконання решти операцій при автентифікації порівняно з ними можна знехтувати. Результати оцінювання показано на рис. 1, де *БК* та *УК* — абревіатури базової та удосконаленої концепцій, відповідно.

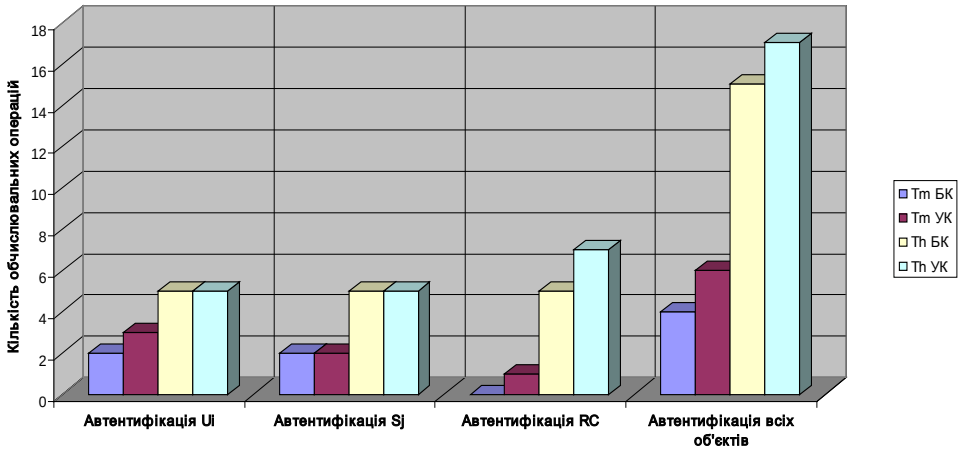

Рис. 1. Оцінювання обчислювальної ефективності: *БК* — базової і *УК* — удосконаленої концепцій впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи

Як випливає з рис. 1, удосконалена концепція в цілому є обчислювально затратнішою (на 10-15 %) порівняно з базовою концепцію. Але зважаючи на те, що удосконалена концепція позбавлена виявлених у процесі експлуатації базової концепції вразливостей та орієнтація запропонованих концепцій для автентифікації об'єктів, що входять до складу ІКС, саме використання удосконаленої концепції є рекомендованим.

Висновки

Розвиток інформаційних систем критичного застосування у напрямку впровадження мультисерверної архітектури спричинив ускладнення при забезпеченні їх інформаційної безпеки, зокрема, у вирішенні завдання надійної автентифікації складових елементів цих систем. Існуючим концепціям забезпечення надійності процесу автентифікації у інформаційних системах критичного застосування властиві недоліки, основні з яких — невідповідність актуальному стандарту безпеки інформаційних систем ISO/IEC 27001:2013, обчислювальна неефективність та низький комфорт процесу автентифікації.

Запропонована позбавлена цих недоліків концепція надійної автентифікації для мультисерверної інформаційної системи критичного застосування, до складу якої входить, зокрема, множина користувачів, множина серверів та виділений сервер-реєстраційний центр для обліку об'єктів системи без ведення верифікаційних таблиць. Інформаційний обмін між об'єктами системи організовано у вигляді захищених сесій на основі ключів з механізмом узгодження на основі односторонніх хеш-функцій та криптографії еліптичних кривих, яка на сьогодні забезпечує найкраще співвідношення надійності шифрування по відношенню до довжини ключа серед існуючих криптосистем. Роботу з користувачами персоніфіковано за допомогою індивідуальних карт доступу, які захищено на основі положень криптографічної теорії еліптичних кривих. На картах доступу, окрім ідентифікаційної інформації та паролю, зберігається індивідуальна біометрична інформація про особливості голосу користувача. Додаток для автентифікації, який встановлюється на обчислювальному засобі користувача, ініціюється двоступінчастою процедурою розпізнавання користувача (за умови наявності ідентифікаційної карти) — за індивідуальними особливостями його голосу та за введеним паролем, що разом зі зручністю, забезпечує надійність процесу автентифікації.

Запропоновану базову концепцію впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи протестовано та обґрунтовано її відповідність стандарту ISO/IEC 27001:2013, включаючи наявність механізмів захисту від таких типів атак: атаки із вгадуванням паролю, атаки з відтворенням запису паролю, атаки з використанням викрадених засобів верифікації, атаки з використанням викрадених ідентифікаційних карт, атаки на основі авторизованих аккаунтів користувачів (інсайдерів), спуфінг-атаки, атаки з підбором паролю, атаки зі спробою підробки ключа сесії, атаки на основі частини відомих ключів сесій, атаки на основі ключів сесій довготривалого використання, атаки на основі одноразових паролів, атаки в процесі оновлення паролю, атаки з перевантаженням апаратних засобів. Втім, досвід практичної експлуатації системи автентифікації для доступу до ресурсів інформаційної системи критичного застосування виявив у базовій концепції низку вразливостей, з метою позбавлення яких створено удосконалену концепцію впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи, яка містить відповідні механізми захисту і також повністю задовольняє вимогам стандарту ISO/IEC 27001:2013.

У статті оцінено обчислювальну ефективність запропонованих концепцій шляхом підрахунку кількості обчислювально найскладніших операцій — масштабованого множення T_m та обчислення хеш-функції T_h під час проведення автентифікації об'єктів у складі інформаційної системи критичного застосування (користувача, сервера, реєстраційного центру та всіх цих об'єктів разом). Підсумкова обчислювальна складність базової концепції склала $4T_m + 15T_h$, а удосконаленої — $6T_m + 17T_h$, що є середнім результатом порівняно з аналогами, але застосування криптографії еліптичних кривих робить операції хешування приблизно у 6 разів швидшою від застосованої у аналогах криптографії з відкритим ключем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Will Larson, "Overview of Single vs. Multi Server Architecture." [Electronic resource], Access mode: https://lethain.com/overview-of-single-vs-multi-server-architecture/.

[2] L. Catuogno, and C. Galdi, "On user authentication by means of video events recognition," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 6, pp. 909-918, 2014.

[3] D. He, Y. Zhang, and J. Chen, "Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks," *Wireless Personal Communications*, vol. 74, no. 2, pp. 229-243, 2014.

[4] P. Guo, J. Wang, B. Li, and S. Lee, "A variable threshold-value authentication architecture for wireless mesh networks," *Journal of Internet Technology*, no. 15, pp. 929-936, 2014. https://doi.org/10.6138/JIT.2014.15.6.05 .

[5] L. Lamport "Password authentication with insecure communication." [Electronic resource], Access mode:

https://lamport.azurewebsites.net/pubs/password.pdf .

[6] C. C. Chang, and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards,” *Proc of third international conference on cyberworlds (CW’04)*. IEEE Computer Society, Los Alamitos, pp. 417-422, 2004. https://doi.org/10.1109/CW.2004.17.

[7] E. J. Yoon, and K. Y. Yoo, “Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235-255, 2013.

[8] L. H. Li, I. C. Lin, and M. S. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks,” *IEEE Transactions on Neural Networks*, vol. 12, iss. 6, pp. 1498-1504, 2001.

[9] Y. P. Liao, and S. S. Wang, “A secure dynamic id based remote user authentication scheme for multi-server environment,” *Computer Standards & Interfaces*, vol. 31, pp. 24–29, 2009.

[10] А. А. Болотов, С. Б. Гашков, А. Б. Фролов, и А. А. Часовских, *Элементарное введение в эллиптическую криптографию*. Москва: КомКнига, 2006, 260 с.

[11] ISO/IEC 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements.” [Electronic resource], Access mode: https://trofisecurity.com/assets/img/iso27001-2013.pdf .

[12] М. М. Биков, та В. В. Ковтун, «Оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосув ання,» *Вісник Вінницького політехнічного інституту*, № 2, с. 70-76, 2017.

[13] О. Н. Жданов, и В. В. Золотарев, *Методы и средства криптографической защиты информации*. Красноярск: СибГАУ, 2007, 217 с.

[14] О. Н. Жданов, и Т. А. Чалкин, *Применение эллиптических кривых в криптографии*. Красноярск: СибГАУ, 2011, 65 с.

Рекомендована кафедрою комп’ютерних систем управління ВНТУ

Стаття надійшла в редакцію 19.09.2018

Ковтун В’ячеслав Васильович — канд. техн наук, доцент, доцент кафедри комп’ютерних систем управління, e-mail: kovtun_v_v@vntu.edu.ua .

Вінницький національний технічний університет, Вінниця

V. V. Kovtun[1]

The Concept of Introduction of the Automated Speaker Recognition System in the Authentication Process for Access to the Critical System

[1]Vinnytsia National Technical University

In the article, ISO/IEC 27001: 2013, an effective and user-friendly concept of reliable authentication for accessing a multi-server information critical system, which includes, in particular, a set of users, a set of servers and a dedicated server —a registration center for a system objects registration without the maintenance of verification tables, is proposed. Information exchange between the objects of the system is organized using secure sessions based on an secret keys with a matching mechanism based on one-way hash functions and cryptography of elliptic curves, which now provides the best correlation between encryption reliability and a size of a secret key among existing cryptosystems. Work with users is personalized using individual access cards, which are protected based on the provisions of the cryptographic theory of elliptical curves. Access cards, in addition to identification information and password, store biometric information about the features of the user's voice in the form of a information features vector. The application for authentication, which is installed on the user's computing device, is initiated by a two-step user recognition procedure (with an identification card) — according to the individual features of his voice and the entered password, which together with convenience ensures the reliability of the authentication process. The basic concept of introduction of the automated speaker recognition system in the authentication process for access to the critical system was proposed in the article, and according to the results of the tests it was concluded that it conforms to the requirements of the ISO/IEC 27001: 2013 standard. However, experience in the practical use of the authentication system for accessing information critical system found a number of vulnerabilities in the basic concept, for the purpose of eliminating them, an improved concept was created that also fully meets the requirements of ISO/IEC 27001: 2013. The article evaluates the computational efficiency of the proposed concepts on the basis of calculating the number of the most computationally complex operations — scalable multiplication T_m and calculating the hash function T_h for authentication of objects as part of the information critical system (user, server, registration center and all these objects together). The final computational complexity of the basic concept was $4T_m + 15T_h$, and of the advanced one — $6T_m + 17T_h$, which in absolute terms is an average result in comparison with analogues. However, the use of cryptography of elliptical curves makes hashing operations about 6 times faster than hashing with the use of a public key, as in analogues.

Keywords: automated speaker recognition system for critical use, authentication, cryptosystem.

Kovtun Viatcheslav V. — Cand. Sc. (Eng.), Assistant Professor, Assistant Professor of the Chair of Computer Control Systems, e-mail: kovtun_v_v@vntu.edu.ua

В. В. Ковтун[1]

Концепция внедрения автоматизированной системы распознавания диктора в процесс аутентификации доступа к критической системе

[1]Винницкий национальный технический университет

Предложена соответствующая актуальному стандарту безопасности информационных систем ISO/IEC 27001: 2013, вычислительная эффективная и удобная для пользователя концепция надежной аутентификации для доступа к мультисерверной информационной критической системе, в состав которой входит, в частности, множество пользователей, множество серверов и выделенный сервер-регистрационный центр для учета объектов системы без ведения верификационных таблиц. Информационный обмен между объектами системы организован с использованием защищенных сессий на основе ключей с механизмом согласования на основе односторонних хэш-функций и криптографии эллиптических кривых, которая на сегодня обеспечивает наилучшее соотношение между надежностью шифрования и длинной ключа среди существующих криптосистем. Работа с пользователями персонифицирована с помощью индивидуальных карт доступа, защищенных на основе положений криптографической теории эллиптических кривых. На картах доступа, кроме идентификационной информации и пароля, хранится биометрическая информация об особенностях голоса пользователя в виде вектора-эталона информационных признаков. Приложение для аутентификации, которое устанавливается на вычислительном устройстве пользователя, инициируется двухступенчатой процедурой распознавания пользователя (при наличии идентификационной карты) — по индивидуальным особенностям его голоса и по введенному паролю, что наряду с удобством обеспечивает надежность процесса аутентификации. Предложенная в статье базовая концепция внедрения автоматизированной системы распознавания диктора в процесс аутентификации для доступа к критической системе протестирована и по результатам тестов сделан вывод о ее соответствии требованиям стандарта ISO/IEC 27001: 2013. Впрочем, опыт практической эксплуатации системы аутентификации для доступа к ресурсам информационной критической системы обнаружил в базовой концепции ряд уязвимостей, с целью устранения которых была создана усовершенствованная концепция, которая содержит соответствующие механизмы защиты и тоже полностью удовлетворяет требованиям стандарта ISO/IEC 27001: 2013. Проведена оценка вычислительной эффективности предложенных концепций на основе подсчета количества наиболее вычислительно сложных операций — масштабируемого умножения T_m и вычисления хэш-функции T_h при проведении аутентификации объектов в составе информационной критической системы (пользователя, сервера, регистрационного центра и всех этих объектов вместе). Итоговая вычислительная сложность базовой концепции составила $4T_m + 15T_h$, а усовершенствованной — $6T_m + 17T_h$, что в абсолютных показателях является средним результатом по сравнению с аналогами. Впрочем, применение криптографии эллиптических кривых делает операции хэширования примерно в 6 раз более скоростными, чем хэширование с применением с открытого ключа, как в аналогах.

Ключевые слова: автоматизированная система распознавания диктора критического применения, аутентификация, криптосистема.

Ковтун Вячеслав Васильевич — канд. техн. наук, доцент, доцент кафедры компьютерных систем управления, e-mail: kovtun_v_v@vntu.edu.ua