УДК 004.052.42
DOI: 10.18372/2073-4751.76.18244

Русанова О.В., к.т.н.,
orcid.org/0000-0003-0145-3012,
Дайко І.В.

МЕТОД КРИПТОГРАФІЧНО СТРОГО ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА БАЗІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЙ

Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

igordaiko1604@gmail.com

Вступ

Швидкий розвиток технологій стимулює якісні зміни характеру взаємодії користувачів та систем віддаленого надання їм інформаційних, обчислювальних та програмних ресурсів. Ці зміни обумовлені насамперед швидкою інтеграцією технологій віддаленої інформаційної взаємодії у всі сфери людської діяльності. В останні роки прийняті у багатьох країнах світу через пандемію *COVID*-19 віддалені режими роботи дали потужний імпульс подальшому розвитку цього процесу. З іншого боку, значний вплив справляє зростаюча комерціалізація віддаленого надання інформаційних послуг, а також швидке збільшення кількості користувачів і інтенсивності їх взаємодії з віддаленими системами.

Зазначені зміни характеру віддаленої взаємодії користувачів та систем потребують адекватного вдосконалення засобів забезпечення інформаційної безпеки та контролю за правами доступу до даних. Вузловою компонентою цих засобів є ідентифікація віддалених абонентів. Зазначені вище тенденції сучасного розвитку віддаленої взаємодії з одного боку диктують нагальну необхідність підвищення рівня захищеності, а з іншого – потребують прискорення виконання ідентифікації. Вирішення цих суперечливих вимог, що диктуються сучасним характером віддаленої взаємодії, вимагає пошуку нових підходів до організації швидкої та надійної ідентифікації віддалених користувачів. Теоретично найбільший рівень захисту від незаконного доступу забезпечують технології криптографічно строгої автентифікації, які відповідають концепції “нульового розголошення” [1].

Таким чином, наукова задача підвищення ефективності криптографічно строгої автентифікації шляхом прискорення її реалізації та підвищення здатності протистояти атакам на процеси віддаленої взаємодії є актуальною для сучасного етапу розвитку інформаційних технологій.

Аналіз тенденцій в забезпеченні безпеки віддаленої взаємодії та огляд методів ідентифікації

Динамічний процес розширення форм і застосувань віддаленої взаємодії в різних сферах людської діяльності призводить до ускладнення задач забезпечення інформаційної безпеки і, відповідно, до збільшення числа моделей аналізу захисту даних [2]. Традиційно ці моделі розділяють на симетричні та несиметричні [3]. Традиційна модель взаємодія великої кількості віддалених абонентів з системою, яка надає їм певні ресурси відноситься до класу несиметричних. Мета зловмисника, з позицій цієї моделі, полягає в отриманні незаконного доступу до ресурсів системи. На практиці для досягнення мети використовуються дві стратегії : незаконне отримання паролю легального абонента та витіснення останнього з сеансу взаємодії після його ідентифікації системою(класична *middle attack*) [4]. Для отримання паролю легального абонента може використовуватися пасивне прослуховування обміну даними в процесі ідентифікації, хакерська або вірусна атака на систему для

одержання ідентифікаційних даних з наступним реконструюванням паролів.

Динамічна комерціалізація надання віддалених послуг стимулює необхідність захисту від спроб імітації їх надання системою [4].

Проведений аналіз загроз в рамках розглянутої моделі визначає такі вимоги до процедур ідентифікації віддалених абонентів:

- для протидії отримання паролів легальних абонентів їх перехопленням в каналі, паролі повинні змінюватися в кожному із сеансів взаємодії з системою;
- для протидії спробам реконструкції паролю легальних абонентів за даними, що зберігаються в системі, а також для виключення можливості імітацією системою сеансу взаємодії з віддаленим абонентом, наявна в системі ідентифікаційна інформація має надавати можливість лише перевірки коректності паролю але не достатньою для створення коректного паролю абонента самою системою;
- для протидії спробам перехоплення сеансу віддаленої взаємодії абонента після його ідентифікацією системою, потрібно проводити періодичні сеанси вторинної ідентифікації;
- для забезпечення можливості роботи систем в реальному часі з великою кількістю віддалених абоненті, а також для ефективного застосування циклів вторинної ідентифікації процедури ідентифікації мають виконуватися швидко.

В найбільшій мірі наведені вимоги задовольняються в рамках теоретичної концепції криптографічно строгої ідентифікації, яка отримала назву "нульового розголошення" (*Zero-Knowledge Identification*) [3]. Суть цієї ідентифікації полягає в тому, що користувач володіє криптографічним механізмом генерації "коректних" сеансових паролів для встановлення контакту з системою. Остання має криптографічний механізм перевірки коректності отриманого від користувача паролю, який виключає можливість генерації таких паролів самою системою.

Вважаючи на практичну важливість криптографічно строгої ідентифікації для захисту віддалених форм інформаційної взаємодії, до теперішнього часу запропоновано доволі багато методів ідентифікації, що реалізують концепцію "нульового розголошення" [5].

Їх можна розділити на два класи. До першого з них відносяться методи, в яких кожен з множини коректних сеансових паролів не залежить від іншого. Відповідно, другий клас утворюють методи, в яких коректні сеансові паролі певним чином залежать один від одного. Зокрема, практично в усіх відомих методах криптографічно строгої ідентифікації цього класу коректні паролі попарно залежні і утворюють "ланцюжок" сеансових паролів. Це означає, що вони мають використовуватися користувачем послідовно. Саме тому, такий підхід до реалізації концепції "нульового розголошення" отримав назву ідентифікації на основі неперервності контакту, тобто фактично задіяні при цьому криптографічні механізми реалізують доведення в поточному сеансі того, що саме цей користувач здійснював попередній сеанс з системою.

До першої групи відносяться історично найбільш ранні методи криптографічно строгої ідентифікації такі як *FFSIS* [7], схеми Шнорра [8] та Гіллоу-Квіскватера [9].

В математичному сенсі ці методи базуються на властивостях важкорозв'язуваних задач теорії чисел таких як факторізація та дискретне логарифммування. Як відомо, не існує аналітичних методів розв'язання таких задач і, відповідно, єдиним шляхом віднаходиження рішень полягає в переборі. При великий значеннях розрядностей чисел на яких розв'язуються ці задачі реалізація перебору стає практично недоцільною. В сучасних системах криптографічного захисту, що базуються на таких задачах розрядність становить 2048 і вище. Це забезпечує практичну неможливість формування сеансового паролю за інформацією, що зберігається в системі. З іншого боку, задача дискретного логарифмування має не скінченну множину

можливих розв'язків і це зумовлює можливість використання в схемах ідентифікації цього типу необмежену кількість сеансових паролів.

Очевидний недолік методів ідентифікації, в основі яких лежать задачі теорії чисел, полягає в тому, що їх реалізація вимагає багато часу, що зумовлено високою обчислювальною складністю мультиплікативних операцій модулярної арифметики над числами, розрядність яких в десятки разів більше розрядності сучасних процесорів.

Для прискорення криптографічно строгої ідентифікації запропонована значна кількість підходів, які різняться між собою вибором важкорозв'язуваних задач, що використовуються для реалізації концепції "нульового розголошення". Зокрема, активно розвиваються [10] схеми криптографічно строгої ідентифікації на основі складних задач теорії решіток. Загальний недолік всіх цих схем полягає в значній обчислювальній складності перевірки коректності сеансового паролю , пов'язаною з великою розмірністю задач.

Кардинально прискорити криптографічно строгу ідентифікацію можна за рахунок використання незворотних перетворень булевої алгебри. Прикладом такого підходу можу слугувати робота [11], в якій пропонується використовувати для ідентифікації хеш-перетворення з програмованими колізіями, які відіграють роль сеансових паролей. Ця схема має високу швидкодію, але потребує значних обчислювальних ресурсів для побудови користувачем відповідного хеш-перетворення.

Схеми криптографічно строгої ідентифікації другого класу використовують "ланцюжки" пов'язаних незворотними перетвореннями сеансових паролів. Такі перетворення значно простіші, оскільки щодо них не висувається вимога неоднозначності. Це дозволяє на порядки прискорити обчислювальну реалізацію таких перетворень. Відповідно, задля досягнення високої швидкодії використовуються нелінійних булеві перетворення. Історично перша схема [12] криптографічно строгої ідентифікації на основі "ланцюжка" сеансових паролів, використовувала в стандартизовані хеш-перетворення. Згодом були запропоновані схеми криптографічно строгої автентифікації подібного типу на базі стандартизованих щифроблоків [13].

Стійка тенденція до зростання кількості користувачів, що обслуговуються системами вимагає подальшого підвищення швидкодії ідентифікації.

Відповідно, існує об'єктивна потреба в розробці нових, більш швидкодіючих методів ідентифікації, що реалізують концепцію нульового розголошення і надають можливості ефективного захисту від спроб перехоплення взаємодії між системою і користувачем.

Мета досліджень

Мета досліджень полягає в підвищенні ефективності захисту від стороннього втручання віддаленої інформаційної взаємодії абонентів та системи за рахунок прискорення обчислювальної реалізації криптографічно строгої ідентифікації, а також за рахунок підвищення рівня захищеності від перехоплень сеансу з витіснення з нього користувача.

Організація ідентифікації на базі псевдовипадкових двійкових послідовностей

Для досягнення поставленої мети пропонується метод криптографічно строгої ідентифікації віддалених абонентів, яка реалізує концепцію "ланцюжка" сеансових паролів з використанням генераторів псевдо випадкових двійкових послідовностей (ГПВДП). Реалізація теоретичної концепції "нульового розголошення" при цьому базується на властивостях незворотності криптографічних ГПВДП, які широко використовуються для потокового шифрування даних в реальному часі [14].

Головна перевага використання ГПВДП в якості незворотних перетворень для реалізації криптографічної концепції "нульового розголошення" при ідентифікації віддалених користувачів полягає в суттєво більшій швидкодії в порівнянні з хеш-перетвореннями та шифроблоками.

На рис.1 показана узагальнена модель ГПВДП у вигляді абстрактного автомату. Ця модель включає пам'ять поточного стану Q ГПВДП об'ємом m біт, функцію Ф зміни стану ГПВДП, а також і функцію Ψ формування вихідного біту s в залежності від коду Q поточного стану. В криптографічних ГПВДП існує можливість можливістю гнучкого налаштування функції Ф зміни поточного стану ГПВДП та функції s=Ψ(Q) формування вихідного біту в залежності від стану генератора. Також існує можливість зовнішньої установки коду Q поточного стану генератора.

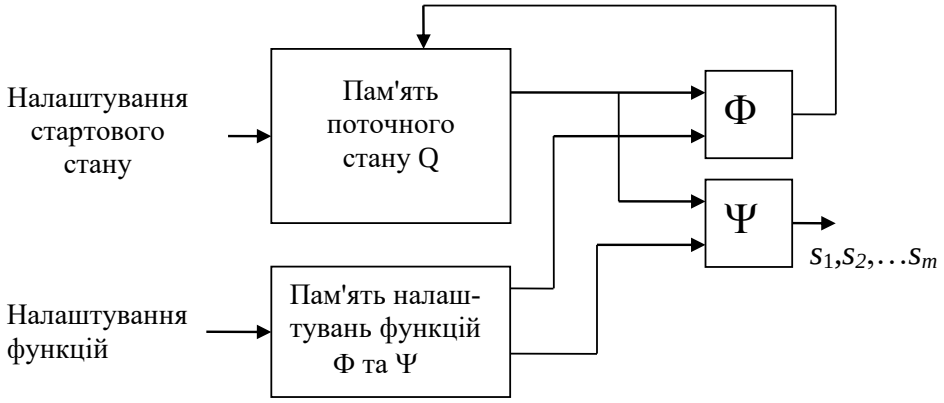

Рис. 1. Модель ГПВДП у вигляді абстрактного автомату з налаштуванням функцій зміни стану та формування вихідної послідовності бітів

Функція Q_{i+1} = Ф(Q_i) зміни поточного i-того стану ГПВДП має забезпечувати максимальний період повторення двійкової послідовності, близький до 2^m. В реальних ГПВДП пам'ять поточного стану та функція Ф його зміни найчастіше реалізуються у вигляді одного або декількох *LFSR* (*Linear Feedback Shift Register*) [3], що доволі просто забезпечує період повторення коду стану 2^m-1 за умови, що функція зворотного зв'язку відповідає простому поліному на кінцевих полях Галуа. Якщо пам'ять ГПВДП виконана у вигляді одного або системи *LFSR*, то налаштування функції Ф зміни поточного стану ГПВДП полягає в зміні коефіцієнтів лінійної функції зворотного зв'язку *LFSR*. Відповідно, кількість можливих налаштувань визначається числом простих поліномів на полі Галуа [1].

Булева функція s=Ψ(Q) формування поточного вихідного сигналу s в залежності від коду Q стану в криптографічних генераторах забезпечує практичну неможливість відновлення цього коду аналітичним чином по вибірці значень згенерованої двійкової послідовності $s_1,s_2,\ldots s_m$. Для цього функція Ψ має мати певні криптографічні властивості [14] і, зокрема високу нелінійність. За цих умов не існує аналітичного способу розв'язання системи булевих рівнянь, які пов'язують код Q_i з бітами послідовності $s_i,s_{i+1},\ldots,s_{i+m}$, що генеруються ГПВДП починаючи зі стану Q_i:

$$\begin{cases} \Psi(Q_i) = s_i \\ \Psi(Q_{i+1}) = \Psi(\Phi(Q_i)) = s_{i+1} \\ \Psi(Q_{i+2}) = \Psi(\Phi(\Phi(Q_i))) = s_{i+2} \\ \quad\vdots \\ \Psi(Q_{i+m}) = \Psi(\Phi(\Phi(\cdots\Phi(Q_{i)}))) = s_{i+m} \end{cases} . \quad (1)$$

Це означає, що не існує іншого способу розв'язання системи булевих рівнянь (1), тобто відновлення m–бітового коду Q_i по заданій послідовності $s_i,s_{i+1},\ldots,s_{i+m}$, крім перебору [1]. При значеннях m для реальних криптографічних ГПВДП (m>124) здійснення перебору об'ємом 2^m потребує обчислювальних ресурсів, які виходять за межі технічних можливостей і практичної доцільності. Іншими словами, якщо повністю відомий алгоритм функціонування ГПВДП, включаючи функції Ф та Ψ, то по заданому фрагменту послідовності $s_i,s_{i+1},\ldots,s_{i+m}$ практично неможливо

відновити код Q_i стану генератора, починаючи з якого вказаний фрагмент було сформовано.

Розроблений метод включає в себе процедуру авторизації абонента в системі, процедуру його ідентифікації на початку сеансу взаємодії та процедуру вторинної ідентифікації, яка виконується періодично на протязі сеансу і має на меті взаємне підтвердження наявності інформаційного контакту.

Запропонована процедура авторизації абонента в системі включає в себе виконання наступної послідовності дій:

1. Абонент визначає максимальну кількість n сеансів обміну даними з системою до наступного циклу авторизації. Лічильник i номеру сеансу ідентифікації встановлюється в n: $i=n$. Довільно генерується код стану Q_n.

2. Абонентом довільним чином формуються код U_Φ налаштування функції Ф та код U_Ψ налаштування функції Ψ ГПВДП. Здійснюється налаштування генератора кодами U_Φ та код U_Ψ.

3. Абонентом випадковим чином формується значення $h_i > 3 \cdot m$. В якості стартового коду ГПВДП встановлюється код Q_i. Генерується h_i бітів двійкової послідовності. Останні m із згенерованих бітів утворюють код Q_{i-1}. Пара кодів $<Q_i,h_i>$ утворюють i–тий сеансовий пароль P_i і зберігаються користувачем в захищеній пам'яті.

4. Лічильник i номеру сеансу зменшується на одиницю: $i=i-1$.Якщо $i > 0$, здійснюється повернення на повторне виконання п.3.

5. Абонент встановлює код Y рівним Q_0 : $Y=Q_0$. Коди Y,U_Φ та U_Ψ шифруються відкритим ключем системи і надсилаються системі.

6. Система приймає від абонента зашифровані коди Y,U_Φ та U_Ψ, дешифрує їх своїм секретним ключем і зберігає в області пам'яті абонента, причому прийнятий код Y зберігається в системі в якості коду доступу D : $D=Y$.

Схематичне зображення прикладу формування кодів Q_n,Q_{n-1},Q_{n-2} для трьох останніх сеансових паролів показане на рис.2.

Запропонована процедура ідентифікації абоненту на i–тому сеансі реалізується наступною послідовністю дій:

1. Абонент читає з пам'яті i-тий сеансовий пароль P_i, який складається з пари кодів: $<Q_i,h_i>$. Пароль надсилається системі. Абонент встановлює в якості стартового для ГПВДП код Q_i, налаштовує генератор кодами U_Φ та U_Ψ. Генерує, з використанням налаштованого таким чином ГПВДП, послідовність h_i+d бітів. Останні d зі згенерованої послідовності бітів абонент зберігає в якості коду W.

2. Система приймає від абонента сеансовий пароль P_i, що складається з пари кодів Q_i та h_i. З пам'яті читає налаштування U_Φ та U_Ψ , що співвідносяться з конкретним абонентом, а також його поточний код D доступу. Здійснюється налаштування ГПВДП на боці системи: функції Ф та Ψ налаштовуються згідно з кодами U_Ψ і U_Ψ відповідно, а в якості стартового встановлюється код Q_i.

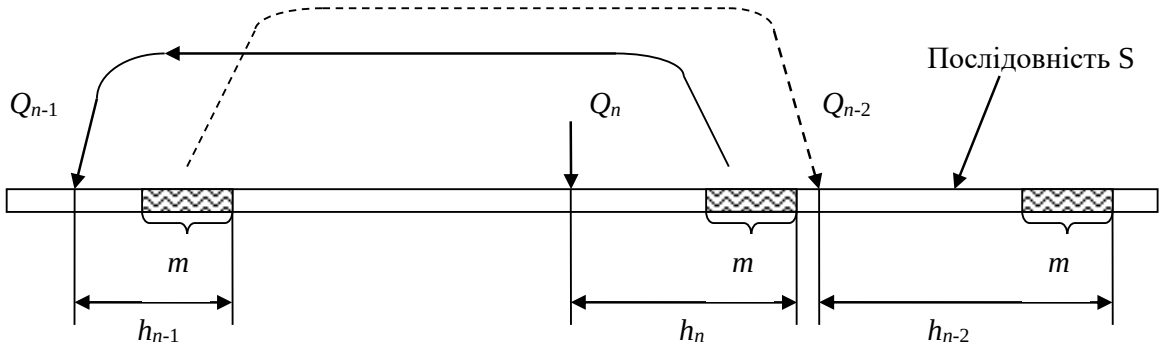

Рис. 2. Схематичне представлення прикладу формування за запропонованою процедурою послідовності компонент Qn,Qn-1,Qn-2 трьох останніх сеансових паролів

3. Система генерує послідовність з $h_i + d$ бітів з використанням налаштованого описаним чином ГПВДП. Останні d зі згенерованої послідовності бітів система зберігає в якості коду F, а попередні m бітів утворюють код Y.

4. Система порівнює згенерований код Y з кодом доступу D. Якщо ці коди співпадають, тобто $Y=D$, то абонент вважається ідентифікованим і йому надається доступ до ресурсів системи. При цьому система замінює код доступу D на прийнятий код Q_i: $D=Q_i$, система надсилає абоненту код F.

5. Абонент приймає від системи код F і порівнює його з кодом W: якщо вони співпадають, тобто $F=W$, користувач отримує підтвердження про успішну ідентифікацію.

6. Абонент обирає випадковим чином m–бітовий код G, встановлює його в якості стартового коду ГПВДП після чого генерує m-бітову послідовність, яка утворює код E. Цей код надсилається системі і розпочинається сеанс інформаційної взаємодії з системою. Код G зберігається в пам'яті.

7. Система отримує від абонента код E і зберігає його в пам'яті як код Z доступу для першого із вторинних циклів ідентифікації. Розпочинає сеанс інформаційної взаємодії з ідентифікованим абонентом.

Розроблена процедура реалізує ідентифікацію системою абонента у відповідності з теоретичною концепцією "нульового розголошення": в кожному з сеансів інформаційної взаємодії використовується інший сеансний пароль, система за наявним в її розпорядженні кодом доступу D не здатна сама отримати пароль, який дозволяє генерувати код D. Цілком очевидно, що задача формування такого паролю системою в математичному сенсі еквівалента задачі розв'язання системи нелінійних булевих рівнянь (1) з їх невідомою кількістю. Як було показано вище, ця задача може бути розв'язана тільки шляхом перебору, об'єм якого, в середньому оцінюється як 2^{m-1} і при реальних значеннях m>124 потребує обчислювальних ресурсів, об'єм яких виключає практичну доцільність підбору паролю.

Для захисту від атак перехопленням сеансу після ідентифікації абонента, в рамках розробленого методу крім описаних вище процедур передбачена процедура "підтвердження присутності" або вторинна ідентифікація. Її суть полягає в тому, що періодично на протязі сеансу інформаційної взаємодії система перевіряє: чи дійсно вона має контракт з ідентифікованим на початку сеансу абонентом. Кількість z циклів виконання цієї процедури залежить від тривалості сеансу інформаційної взаємодії.

При реалізації процедури вторинної ідентифікації (підтвердження присудності), розробленим методом передбачено виконання такої послідовності дій:

1. Система в проміжку часу між циклами ідентифікації підраховує об'єм V (в байтах) інформації, що передані абоненту. Останній за цей же часовий проміжок підраховує об'єм V' прийнятих від системи даних.

2. Система після певного проміжку часу видає запит абоненту на проведення вторинної ідентифікації.

3. Якщо абонента не задовольняє інформаційна взаємодія з системою протягом поточного часу, то він надсилає системі m-бітовий нульовий код L і здійснюється перехід на п.8.

4. Абонент читає з пам'яті код G і обчислює код L підтвердження контакту як суму за модулем 2 цього коду G та об'єму V' прийнятої від системи інформації: $L=G\oplus V'$. Обчислений таким чином пароль L абонент надсилає системі. Після цього абонент випадковим чином обирає нове значення m-розрядного коду G, встановлює його в якості стартового коду ГПВДП і генерує m-бітову послідовність, яка утворює код E. Код G абонент зберігає в пам'яті, а код E надсилає системі в якості коду доступу для наступного циклу ідентифиікації.

5. Система, отримавши від абонента пароль L, обчислює стартовий код G

генератора як суму за модулем два переданого об'єму V даних та прийнятого коду L: $G = L \oplus V$. Обчислений таким чином код G встановлюється в якості стартового коду ГПВДП, після чого генерується m-бітова послідовність, яка утворює код N. Цей код порівнюється зі збереженим в пам'яті системи кодом Z: якщо вони рівні між собою, тобто $N=Z$, то система впевнюється у тому, що з нею взаємодіє легальний абонент, який отримав переданий йому об’єм даних. Якщо коди N і Z різні, тобто $N \neq Z$, система переривае сеанс взаємодії.

6. Система отримує від абонента код доступу E для наступної вторинної ідентифікації в зберігає його в пам'яті, як нове значення коду Z.

Таким чином, вторинна ідентифікація абонента, що здійснюється періодично для перевірки наявності його контакту з системою являє собою спрощену версію запропонованої вище процедури ідентифікації на початку сеансу. При цьому спрощення здійснене задля прискорення виконання вторинної ідентифікації, яке не повинно помітним чином впливати на швидкість інформаційної взаємодії між абонентом та системою.

Фактично в кожному попередньому циклі ідентифікації абонент випадковим чином формує m-бітовий стартовий код G генератора для наступного циклу і генерує код доступу E, який надсилає системі в якості коду доступу. Маючи код доступу $Z=E$ для наступного сеансу, система не здатна, в силу властивостей незворотності ГПВДП, сама відновити стартовий код G для наступного циклу вторинної ідентифікації. Тобто, описана процедура реалізує криптографічно строгу ідентифікацію у відповідності з концепцією “нульового розголошення”. В запропонованій процедурі пароль L, що змінюється в кожному із циклів вторинної ідентифікації утворюється логічним додаванням стартового коду G генератора та об'єму V' інформації що передана системою в часовому проміжку між суміжними циклами ідентифікації. Це дозволяє здійснити контроль об’єму інформаційного трафіку від системи до користувача. Фактично, в розробленій процедурі, контроль наявності контакту реалізується двома складовими: оцінкою адекватності інформаційного контексту самим користувачем та об’ємом даних, надісланим йому.

В випадку якщо зловмисник здійснює активну атаку на віддалену взаємодію системи з легальним абонентом шляхом повного або часткового його витіснення, об’єм V даних переданих користувачеві не співпадає з об’ємом V' прийнятих ним даних. Відповідно, згідно запропонованої процедури, контакт буде перервано. Іншими словами, ціль зловмисника – отримати певні ресурси з боку системи ціною визначених затрат на здійснення активної атаки каналу не досягається. Для того, щоб підробити пароль легального абонента при вторинній ідентифікації, зловмисник має знати об’єм V даних переданих системою, що, в принципі можливо, а також стартовий код G ГПВДП, при якому генерується двійкова послідовність, яка утворює відомий код E. Якщо зловмисник має доступ до інформації, яка використовується системою для ідентифікації, тобто він знає налаштувань U_Φ та U_Ψ генератора для конкретного легального абонента, то відновлення коду G зводиться до розв’язання системи рівнянь (1), що при реальних значеннях m потребує ресурсів, об’єм яких виходить за межі практичної доцільності.

Час виконання циклу вторинної ідентифікації визначається часом генерації двійкової послідовності довжиною m бітів.

Основна перевага запропонованого методу з реалізацією концепції “ланцюжка” сеансових паролів з використанням криптографічних властивостей ГПВДП полягає в тому, що він забезпечує більш високий рівень захисту віддаленої взаємодії за рахунок використання циклів вторинної ідентифікації, що виконуються під час сеансу і дозволяють виявити перехоплення зловмисником взаємодії з системою шляхом витісненням з неї легального користувача.

Існуючі схеми криптографічно строгої ідентифікації не дозволяють

реалізувати вторинну ідентифікацію безпосередньо під час сеансу. Фактично для контролю контакту між абонентом та системою потрібно здійснювати новий цикл ідентифікації, що потребує значних часових затрат.

Вказана перевага досягнута за рахунок інтеграції в рамках одного технологічного рішення, а саме використання ГПВДП, криптографічно строгої ідентифікації учасників взаємодії на початку сеансу, криптографічно строгої процедури підтвердження контакту під час сеансу і можливості швидкісного шифрування потоків даних, якими обмінюються абонент та система.

Орієнтація на використання швидкодіючих ГПВДП дозволяє зменшити час ідентифікації в порівнянні з відомими схемами криптографічно строгої ідентифікації на основі "ланцюжка" сеансових паролів, які використовують стандартизовані хеш-перетворення або шифроблоки. Проведені експериментальні дослідження показали, що використання ГПВДП в рамках запропонованого методу дозволяє прискорити виконання обчислювальних процедур криптографічно строгої ідентифікації в 5-6 раз у порівнянні з схемами такої ідентифікації на основі шифроблоків *AES* [13].

Висновки

В результаті проведених досліджень, направлених на підвищення ефективності захисту від стороннього втручання віддаленої інформаційної взаємодії системи та абонентів запропоновано метод криптографічно строгої їх ідентифікації на основі незворотного "ланцюжка" сеансових паролів.

Базова відмінність запропонованого методу від відомих методів цього типу полягає в використанні для реалізації незворотних перетворень криптографічних генераторів псевдовипадкових двійкових послідовностей. Це дозволило в рамках єдиного технологічного рішення організувати первинну ідентифікацію учасників взаємодії перед початком сеансу та цикли вторинної прискореної ідентифікації, що здійснюються безпосередньо під час сеансу взаємодії. За рахунок цього реалізована протидія перехопленню зловмисником сеансу взаємодії системи з абонентом шляхом його відсторонення. Крім того, використання криптографічних генераторів псевдовипадкових двійкових послідовностей дозволяє здійснювати швидкісне потокове шифрування даних, якими обмінюються учасники взаємодії. Все це дозволяє суттєво підвищити рівень захищеності стороннього втручання віддаленої інформаційної взаємодії системи та абонентів і прискорити процедуру криптографічно строгої ідентифікації в порівнянні з відомими методами реалізації незворотного "ланцюжка" сеансових паролів на базі хеш-перетворень.

Література

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed.John Wiley, 1996. 758 p.

2. Mu Han, Yin Zhikun, Chen Pengzhou, Zhang Xing, Ma Shidian. Zero-knowledge identity authentication for internet of vehicles: Improvement and application. *PLoS ONE*. 2020. V. 15. No. 9. P. 217–247.

3. Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001. 780 p.

4. Conti M., Dragoni N., Lesyk V. A Survey of Man in the Middle Attacks. *IEEE Communications Surveys and Tutorials*. 2016. Vol. 18. No. 3. P. 2027–2051.

5. Kittichokenai K., Care G. Secret Key-based Identification and Authentication with a Privacy Constraint. *IEEE Trans. Inf. Theory*. 2016. V. 62. No. 11. P. 6189–6203.

6. Захариудакис Лефтерис. Метод быстрой аутентификации удаленных пользователей на основе концепции "нулевых знаний". *Наукові записки Українського науково-дослідного інституту зв'язку*. 2017. № 1(45). С.109–117.

7. Feige U., Fiat A., Shamir A. Zero knowledge proofs of identity. *Journal of Cryptology*. 1988. V. 1. No. 2. P. 77–94.

8. Schnorr C.P. Method for Identification Subscribers and for Generating and

Verificating Electronic Signatures in data Exchange System. US Patent #4995,083.19. 1991.

9. Guillou L.C., Quisquater J.J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memore. *Proceeding of Advances of Cryptology – Eurocrypt-88* / Davos, Switzerland, 1988. P. 123–128.

10. Rafaël Del Pino. Efficient lattice-based zero-knowledge proofs and applications. Cryptography and Security. Université Paris sciences et lettres, 2018. 110 p.

11. Stavroulakis P., Markovskyi O., Bardis N., Doucas N. Efficient Zero Knowledge identification based on one way Boolean transformations. *IEEE Globecom Workshops* / Houston, USA, 2011. P. 275–280.

12. Lamport L. Password Authentication with Insecure Communication. *Communications of the ACM*. 1981. V. 24. No. 11. P. 770–772.

13. Bardis N., Doucas N., Markovskyi O. Zero-Knowledge Identification Method Based on Block Ciphers. *Proceeding of 2017 International Conference on Control, Artificial Intelligence, Robotic & Optimization (ICCAIRO)* / Prague, Czech Republic, 2017. P. 307–311.

14. Soo Yun Hwang, Gi Yoon Parkm Dae Ho Kim, Kyong Son Jhang. Efficient Implementation of a Pseudorandom Sequence Generator for High-Speed Data Communications. *ETRI Journal*. 2010. V. 32. No. 2. P. 222–229.

Русанова О.В., Дайко І.В.

МЕТОД КРИПТОГРАФІЧНО СТРОГОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА БАЗІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У статті пропонується метод криптографічно строгої ідентифікації віддалених користувачів, який ґрунтується на властивостях незворотності криптографічних генераторів псевдовипадкових послідовностей. Це дозволило інтегрувати в рамках єдиного технологічного рішення криптографічно строгу ідентифікацію користувача перед сеансом, постійну взаємну автентифікацію під час сеансу, а також забезпечити можливість потокового шифрування обміну даними між користувачем та системою. Показано, що використання запропонованого методу дозволяє зменшити час ідентифікації та підвищити захищеність до атак на віддалену взаємодію між системою і користувачем шляхом його відтискання.

***Ключові слова**: ідентифікація на основі нульового розголошення, криптографічно строга автентифікація, псевдовипадкові двійкові послідовності, атаки проникненням посередника, захист віддаленої взаємодії.*

Rusanova O.V., Daiko I.V.

METHOD FOR CRYPTOGRAPHICALLY STRICT IDENTIFICATION OF REMOTE ABONENTS BASED ON PSEUDORANDOM SEQUENCES GENERATORS

The article proposes a method for cryptographically strong remote abonents identification, which is based on the irreversibility properties of cryptographic generators of pseudo-random sequences. This made it possible to integrate, within a single technological solution, a cryptographically strong user identification before a session, permanent mutual authentication during a session, and also provide the possibility of streaming encryption of data exchange between the user and the system. It is shown that the use of the proposed method allows to reduce the identification time and increase the security against middle attacks.

***Keywords**: Zero-Knowledge Identification, cryptographically strong identification, pseudo-random bit sequences, middle attacks, protection of remote interaction.*