РОЗРОБКА СПЕЦІАЛЬНОГО АЛГОРИТМУ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

М.І. ОГУРЦОВ,
Інститут кібернетики імені В.М. Глушкова НАН України, Київ, Україна
neizvestny@gmail.com

Анотація. *Актуальність захисту інформації з обмеженим доступом (ІзОД) зростає впродовж останніх десятиріч і продовжуватиме зростати. Для підвищення рівня захисту ІзОД виконано розробку спеціального алгоритму багатофакторної автентифікації користувачів із застосуванням технології комунікації ближнього поля – Near Field Communication. На її основі пропонується створити канал передачі секретних автентифікаційних даних для роботи алгоритмів захисту ІзОД.*
Ключові слова: *захист інформації, автентифікація, комунікація ближнього поля, інформація з обмеженим доступом.*

Постановка проблеми. Актуальність захисту інформації з обмеженим доступом (ІзОД) зростає впродовж останніх десятиріч і продовжуватиме зростати в майбутньому, оскільки постійно зростає вартість ІзОД (як державної, так і приватної) та обсяги втрат, що можуть бути викликані її розголошенням, спотворенням або знищенням [1].

Аналіз останніх публікацій. На сьогоднішній день захист ІзОД забезпечується криптографічними засобами для шифрування та забезпечення контролю доступу [1-5], стеганографічними – для приховування факту передачі інформації [6-7]. Але засоби багатофакторної автентифікації користувача при спробі отримання ним доступу до ІзОД залишаються недостатньо [8].

Метою роботи стала розробка спеціального алгоритму багатофакторної автентифікації користувачів та захисту інформації при доступі до неї із застосуванням технології комунікації ближнього поля – Near Field Communication для підвищення рівня захисту ІзОД.

Архітектуру системи ЗІ (СЗІ) на основі багатофакторної автентифікації користувачів пропонується реалізовувати із застосуванням технології комунікації ближнього поля – Near Field Communication (NFC) [9]. На її основі пропонується створити канал передачі секретних автентифікаційних даних для роботи алгоритмів ЗІ від НсД.

Розглянемо, як можна підвищити рівень захисту ІзОД на основі використання NFC. Для цього пропонується застосувати метод неперервного контролю користувачів, для якого кожен користувач повинен мати NFC пристрій для автентифікації. Відповідно до **розробленого алгоритму неперервного контролю користувачів**, NFC-пристрої, що кожен користувач має з собою, будуть постійно використовуватись для відстеження наявності та місцезнаходження користувачів, визначаючи при цьому його рівень повноважень (рисунок 1).

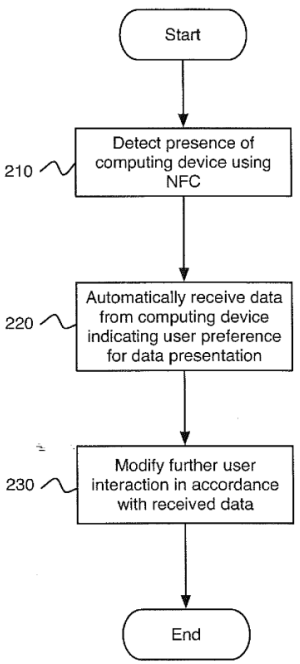

Рисунок 1 – Схема алгоритму неперервного контролю користувачів

Порядок роботи алгоритму:

1. При початку роботи з ІзОД (першому запиті користувача) він вводить пароль.

2. Під час перевірки пароля NFC-зчитувачем автоматично перевіряється наявність в зоні зчитування NFC-автентифікатора, що відповідає даному паролю.

3. Якщо пароль вірний, але NFC-автентифікатор відсутній – в доступі відмовлено.

4. При подальшій роботі з ІзОД NFC-автентифікатор регулярно (не рідше ніж раз на декілька секунд) сканується на наявність.

5. У випадку, якщо при скануванні NFC-автентифікатор не виявлений, доступ до ІзОД блокується і крок 1 має бути повторений.

6. Якщо користувач переміщується (виходив на перерву, переходить на інше робоче місце і т.д.) – крок 1 має бути повторений.

В результаті реалізації цього алгоритму користувачі будуть вводити пароль лише приходячи на роботу, та повертаючись з перерви, а далі їм досить буде мати NFC-автентифікатор при собі, щоб отримувати доступ до ІзОД в рамках своїх повноважень. При цьому крадіжка NFC-автентифікатора нічого не дасть, оскільки для отримання доступу до ІзОД потрібно додатково вводити пароль, що відомий лише легітимному користувачеві. При цьому СЗІ в режимі реального часу відстежує присутність, місцезнаходження та дії кожного користувача, перевіряючи за необхідності його права доступу в автоматичному режимі.

Побудова СЗІ на основі запропонованого алгоритму дозволить захиститись від найбільш небезпечних загроз, спростить розгортання, модифікацію та масштабування СЗІ та підвищить надійність захисту ІзОД. Застосування NFC-пристрою дозволить забезпечити ефективну та прозору для користувачів багатофакторну автентифікацію.

Розроблений алгоритм багатофакторної автентифікації користувачів, що базуються на технології NFC, при застосуванні дозволить легке та гнучке розгортання, масштабування та оновлення СЗІ. Відповідно до алгоритму пропонується, щоб місцезнаходження та дії користувачів постійно відстежувались СЗІ в автоматичному режимі. В якості засобу автентифікації пропонується застосовувати NFC-пристрій, що дозволить реалізувати цей метод та забезпечить багатофакторну аутентифікацію.

Разом з тим вимагають подальших досліджень наступні питання:

• які конкретно програмно-апаратні засоби слід застосовувати для побудови СЗІ кожного конкретного об’єкту;

• економічне обґрунтування доцільності застосування NFC-автентифікатора.

Література.

1. Коц Д. В. Сучасний стан розвитку системи захисту інформації з обмеженим доступом в Україні // Порівняльно-аналітичне право. – 2020. – №. 1. – С. 343-346.
2. Прокопович Л. В., Лопаков О. С., Солодкий Д. М. Шляхи підвищення захисту персональних даних користувачів соціальних мереж // The Scientific Heritage. – 2021. – №. 65-1. – С. 32-37.
3. Миколайко О. О. Кібербезпека критичних інформаційно-телекомунікаційних систем. – 2021.
4. Maksym Ogurtsov Three-Keys Cryptographic Algorythm for UAV Network Communication // Інформаційні технології та комп’ютерне моделювання; матеріали статей Міжнародної науково-практичної конференції, м. Івано-Франківськ, 5-10 липня 2021 року. – Івано-Франківськ: п. Голіней О.М., 2021. – с. 118-119.
5. Огурцов М.І. Засоби підвищення рівня захисту даних, що циркулюють між БПЛА та оператором // Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту – ISDMCI’2020: матеріали міжнар. наук. конф. (25-29 травня 2020 р., с. Залізний Порт). – Херсон: Видавництво ФОП Вишемирський В. С., 2020. 170 с. – с. 126-127.
6. Kuznetsov A. A., Kononchenko G. V. Стеганографічні методи в векторній графіці // Radiotekhnika. – 2021. – №. 205. – С. 32-41.
7. Корольов В.Ю., Ходзінський О.М. JPEG стеганографія на базі теоретико-чисельних перетворень // Вісник Хмельницького національного університету. – №1(209). – 2014. – С.61-69.
8. Reese K. et al. A usability study of five two-factor authentication methods // Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019). – 2019. – С. 357-370.
9. Tiruvilwamalai Venkatraman Raman Personalized access using near field communication. Google Inc. US20120311019 / EP 2530664 A1 http://www.google.com/patents/EP2530664A1