УДК 004.415.056:658.115

А. О. Азарова
В. О. Гудзь
В. О. Блонський

УДОСКОНАЛЕННЯ МЕТОДУ ТРИФАКТОРНОЇ АУТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вінницький національний технічний університет

Анотація

Розглянуто теоретичні засади захисту інформації на основі сучасних методів багатофакторної ідентифікації, виявлено їх переваги та недоліки. На основі виконаного аналізу розроблено пристрій трифакторної ідентифікації та автентифікації користувачів із можливістю розмежування контролю доступу до інформаційного середовища, що містить конфіденційні відомості, для захисту від несанкціонованого доступу. Доведено економічну доцільність розробленого пристрою. Обґрунтовано доцільність використання пристрою як у системах безпеки, так і в індивідуальному порядку.

Ключові слова: трифакторна ідентифікація, захист інформації, несанкціонований доступ.

Abstract

Theoretical principles of information protection based on modern methods of multifactor identification are considered, their advantages and disadvantages are revealed. Based on the analysis, a device of three-factor identification and authentication of users with the ability to differentiate access control to the information environment containing confidential information to protect against unauthorized access. The economic expediency of the developed device is proved. The expediency of using the device both in security systems and individually is substantiated.

Keywords: three-factor identification, biometric scanner, information security, unauthorized access.

Сучасні інформаційні технології, що забезпечують дотримання властивостей інформації охоплюють методи збирання, оброблення, передавання, перетворення, зберігання і розподілу інформації, існували протягом тривалого часу на паперовій та мовній основі, та не могли повністю задовольняти вимогам захищеності інформації [1].

Існуючі методи захисту інформації охоплюють усі можливі джерела інформаційних загроз, такі як збирання, модифікація, витік та знищення конфіденційної інформації [2]. Сучасні технології захисту інформації реалізуються за допомогою трьох підходів до захисту конфіденційних даних:

- апаратний – генератори кодів, біометричні пристрої та пристрої «прозорого» шифрування;
- програмний – антивірусне програмне забезпечення, криптографічні засоби, засоби ідентифікації санкціонованих користувачів, засоби аудиту;
- організаційний – розроблення нормативно-правової документації, яка регламентує процеси створення, оброблення, зберігання, передавання та отримання, захисту конфіденційної інформації, а також заснування відділу інформаційної безпеки підприємства, що несе відповідальність за інформаційну безпеку організації в цілому [3].

Організаційні заходи захисту інформації необхідні для забезпечення дотримання правил розмежування доступу, що також описані у посадових інструкціях працівників установи, застосування інших заходів і засобів захисту. Оскільки організаційний захист не виключає витік інформації в цілому, необхідно застосовувати апаратні та програмні засоби захисту.

Організаційні заходи захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розроблення та функціонування інформаційної системи.

Апаратні та програмні засоби та заходи захисту засновані на використанні електронних пристроїв і спеціального програмного забезпечення, що входить до складу автоматизованої системи і виконує функції захисту інформації самостійно або в комплексі з іншими засобами захисту інформації (рис 1).

Використання програмно-апаратних засобів захисту інформації зумовлює високий рівень захищеності даних від несанкціонованого доступу [4].

Рисунок 1 – Методи і засоби захисту конфіденційної інформації

Одним із найкращих методів захисту є використання пристроїв ідентифікації користувачів у системі безпеки. Існують три підходи до виявлення санкціонованого користувача – особи, що отримала визначені права доступу для роботи із конфіденційною інформацією:

– реєстрація того, що має користувач – представлення користувачем ідентифікатора, що визначає його особу. Ним може виступати деякий предмет, що реєструє особу у системі захисту інформації, а також розділяє права доступу до інформації;

– реєстрація того, що знає користувач – наявність у користувача унікального паролю, пін-коду доступу або спеціальної фрази, за якою користувач автентифікується.

– реєстрація того, що невід'ємне у користувача – відбитки пальців, долоні, зчитування сітківки ока, тембр голосу, геометрія обличчя, тобто фізіологічна особливість людини.

Усі три підходи до запобігання несанкціонованого доступу до інформаційних ресурсів уособлює багатофакторна автентифікація – розширена автентифікація, метод контролю доступу до інформаційного середовища, в якому користувачеві для отримання доступу до даних необхідно пред'явити більше одного «доказу механізму аутентифікації» [5].

Багатофакторна аутентифікація не стандартизована. Існують різні форми її реалізації. Отже, проблема полягає в її здатності до взаємодії. Існує багато процесів і аспектів, які необхідно враховувати під час вибору, розроблення, тестування, впровадження та підтримки цілісної системи управління ідентифікацією безпеки, включаючи всі релевантні механізми аутентифікації і супутніх технологій [6].

Багатофакторна аутентифікація має ряд недоліків, які перешкоджають її поширенню. Зокрема, людині, яка не розбирається в цій області, складно стежити за розвитком апаратних токенів. Багато користувачів не можуть самостійно встановити сертифіковане програмне забезпечення, оскільки не володіють відповідними технічними навиками. Загалом, багатофакторні рішення вимагають додаткових витрат на встановлення та оплату експлуатаційних витрат [7]. Багатоапаратні комплекси, засновані на токенах, запатентовані, і деякі розробники стягують з користувачів щорічну плату. З точки зору логістики, розмістити апаратні токени важко, оскільки вони можуть бути ушкоджені або втрачені. Випуск токенів в таких галузях, як банківська сфера або підприємництво повинен бути відрегульованим. Крім витрат на установку багатофакторної аутентифікації значну суму також становить оплата технічного обслуговування [8].

Сучасні засоби трифакторної аутентифікації користувачів в залежності від використовуваного методу захисту інформації мають практично однакові компоненти, які виконують функції зчитування, оброблення та зберігання даних із подальшим їх використанням, тобто порівняння пред'явленого ідентифікатора та еталону [9].

Автори пропонують удосконалення методу аутентифікації, що базується на комбінуванні біометричного сканування відбитків пальців, QR-ідентифікатора та парольної ідентифікації.

Першим етапом роботи пристрою є визначення належності користувача до системи безпеки. Також на першому етапі відбувається розмежування прав доступу до інформаційного середовища.

Цей етап відносить користувача до одного із трьох рівнів, наприклад, рівень 3 – «Бухгалтер», рівень 2 – «Заступник по замовленням», рівень 1 – «Головний фінансовий аналітик». Кожен рівень має інформацію різного ступеня важливості, потрапляння якої до третіх осіб нанесе шкоду підприємству чи установі різними ступенями важкості. Звідси виникає необхідність розмежування прав доступу, яка реалізується поєднанням методів аутентифікації, а саме: для рівня 3 – зчитування QR-коду, рівня 2 – зчитування QR-ідентифікатора та підтвердження особи зчитуванням відбитку пальця, для рівня 1 – зчитування ідентифікатора користувача, підтвердження біометричними ознаками особи, а також запит унікального паролю для доступу до рівня системи.

У випадку підтвердження усіх етапів користувачеві надається доступ до інформаційного середовища. Якщо користувач на першому етапі не підтверджує належності до інформаційної бази даних, пристрій надає другу спробу для зчитування ідентифікатора. На другому та третьому етапах також надається повторна аутентифікація користувача для зменшення ймовірності помилок другого роду в системі, прикладом якої може бути ненадання доступу санкціонованому користувачеві.

У випадку, коли засіб захисту виявляє несанкціонованого користувача, записується час, дата та кількість невдалих спроб на добу в електронний журнал системи захисту, що дає змогу аналітиками безпеки установи або підприємства зчитувати відомості про загальну ситуацію у системі безпеки інформаційного середовища, а також сповіщує про несанкціонований доступ до системи охорони.

Таке удосконалення дозволяє зменшити витрати на впровадження та обслуговування пристрою у системі безпеки, використовувати та налаштовувати пристрій без спеціально навчаної особи, передчасно виявляти несанкціонований доступ до інформаційного середовища, а також в умовах аварійних та виняткових ситуацій надавати доступ санкціонованим користувачам [10-14].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Погрищук Б., Паночишин Ю. Інформаційні технології та комп'ютерна техніка. К. : Видавництво Знання, 2012. 463 с.
2. Богуш В. М., Юдин О. К. Інформаційна безпека держави. К. : «МК-Прес», 2005. 432 с.
3. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Вінниця : ВНТУ, 2017. 120 с.
4. Іванченко С. О., Гавриленко О. В., Липський О. А., Шевцов А. С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. К. : ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
5. Зайцев А. П., Шелупанов А. А, Мещеряков Р. В., Скрыль С. В., Голубятников И. В. Технические средства и методы защити информации. М. : «Машиностроение». 2009. 508 с
6. Свідоцтво про реєстрацію авторського права на твір №79707. Розробка контролеру кодового доступу до сейфа на мікроконтролері Arduino / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80960. Дата реєстрації 14.06.2018 р.
7. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.
8. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма «Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації» / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
9. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма «Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
10. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма «Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією» / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
11. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма «Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах» / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
12. Azarova A., Azarova L., Rosol N., Bystritskiy O. Models and methods of electronic digital signature. Theoretical and scientific f oundations of engineering: collective monograph / International Science Group. Boston : Primedia eLaunch, 2020. P. 24 – 33.

Азарова Анжеліка Олексіївна, кандидат технічних наук, професор, заступник декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва.

Блонський Владислав Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-15б, vlados,blonskiy@gmail.com.

Гудзь Віталій Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-15б, vitalik1211@ukr.net.

Anzhelika Azarova, Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Vladyslav Blonskyi, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vlados.blonskiy@gmail.com.

Vitalii Hudz, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vitalik1211@ukr.net.