

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ ТРИФАКТОРНОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В СИСТЕМАХ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Проаналізовано існуючі типи, засоби та заходи захисту інформації від несанкціонованого доступу, виявлено їх недоліки та переваги. За результатами проведеного дослідження було запропоновано пристрій, який здійснює захист інформації від несанкціонованого доступу користувачів, створений на основі трифакторної автентифікації користувача, а саме: зчитування безконтактної картки доступу RFID, запиту унікального пароля, а також зчитування унікальних відбитків пальців користувача, що дозволяє покращити систему захисту та передчасно виявляти спробу несанкціонованого отримання інформації.

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

Abstract

Different types and measures of protection of information from unauthorized access are analyzed, their disadvantages and advantages are revealed. According to the results of the research, a device was proposed that protects information from unauthorized access of users, created on the basis of three-factor authentication of the user, namely: reading a contactless RFID access card, requesting a unique password, as well as reading unique fingerprints for improving the security system. and early detection of unauthorized attempts to obtain information.

Keywords: three-factor authentication, information security, unauthorized access.

Сучасні технології захисту інформації дедалі більше потребують вдосконалення методів, засобів та заходів захисту конфіденційної інформації із збільшенням її цінності, тому все більше стає необхідність її збереження як від несанкціонованого доступу та використання, так і від її модифікації [1].

Проаналізовано великий об'єм методів та засобів захисту інформації, що створені на основі різних типів автентифікації користувачів як за біологічними особливостями, такими як відбитки пальців чи геометрії руки, так і від використання унікального ключа, в ролі якого може виступати пароль користувача або індивідуальний ключ доступу до інформаційної системи [2-4].

Попри все, сучасні засоби захисту мають і невирішені проблеми з точки зору захисту інформації, а саме: існують обмеження можливостей зчитування фізіологічних особливостей користувача, висока імовірність помилкового спрацювання, що викликана неякісним устаткуванням, відсутні можливості вдосконалення та модифікації пристроїв у системі захисту, недоступність компонентів обладнання для своєчасного обслуговування пристроїв та їх малий час автономності, відсутність контролю пристроїв у системі безпеки, недоступність дистанційного керування пристроями захисту, велика дороговизна пристроїв та їх окремих компонентів а також великі габарити конструкції засобів захисту [5].

Отже, розроблення пристрою захисту інформації на основі трифакторної автентифікації користувачів є досить актуальним, адже вирішення вищезазначених проблем призведе до отримання необхідного рівня захисту інформації в цілому [6,7].

Можливість циркулювання інформації у будь-якому вигляді та на будь-якому підприємстві приватного типу або державної форми власності обумовлює необхідність дотримання правил та інструкцій обробки та зберігання інформації від несанкціонованого доступу. Належний рівень захисту досягається при використанні в сукупності організаційних, правових та технічних заходів та засобів захисту інформації. Адже використання окремих типів захисту не можуть цілком вирішити проблему викрадення або модифікації конфіденційних даних.

Цілком зрозуміло, що програмно-апаратні технічні пристрої значно підвищують ступінь захисту та мінімізують відсоток несанкціонованого доступу до інформації, що дозволяє безперервно працювати усім підприємствам та організаціям, спрямовуючи свої ресурси на клієнтів, а не на захист від зловмисників [8, 9]. Таким чином у даній роботі запропоновано використання технічного пристрою

захисту інформації від несанкціонованого доступу, а саме забезпечення належних умов збереження інформації в приміщеннях та спеціально виділених для цієї мети конструкціях. Принцип роботи пристрою полягає у використанні трифакторної аутентифікації користувачів у системі безпеки шляхом зчитування біометричних ознак людини, а саме відбитків пальців, введення унікального ключа, в ролі якого може бути пін-код або пароль, а також зчитування картки-ідентифікатора користувача типу RFID. Також надається можливість перемикати режими доступу до однофакторної аутентифікації користувача. Пристрій буде надавати доступ користувачу тільки у тому випадку, коли усі введенні ідентифікатори будуть співпадати із зареєстрованими зразками. В іншому випадку пристрій надасть сигнал у систему безпеки про спробу несанкціонованого доступу при другому некоректному введенні ідентифікатора.

Із вищеописаного можна дійти висновку, що для забезпечення належного рівня захисту інформації необхідно використовувати разом із організаційними та правовими заходами спеціальні програмно-апаратні засоби захисту, що в свою чергу мають охоплювати усі можливі методи аутентифікації користувачів у системі безпеки, що викликає доцільність розроблення запропонованого пристрою, а також вивчення можливості його модифікації для урахування усіх можливих ризиків несанкціонованого доступу.

Отже, автори пропонують розроблення програмно-апаратного засобу захисту інформації, що може використовуватись як приватними підприємствами так і державними установами, на основі трифакторної аутентифікації користувачів у системі безпеки. Запропонований технічний пристрій уможливує його використання без спеціальних знань в технічній галузі інформаційної безпеки, можливість зміни ступеня захисту шляхом перемикання режимів роботи від одно- до трифакторної аутентифікації, що пришвидшує процес аутентифікації користувачів, дистанційне керування технічним пристроєм у системі, зворотній зв'язок пристрою із системою безпеки при введенні некоректного ідентифікатора, довготривалий час автономної роботи пристрою.

На відміну від сучасних засобів запропонований пристрій дозволяє реалізувати захист даних із використанням менших коштів у декілька разів, створити та виконувати налаштування пристрою власноруч без спеціалізованого обладнання та знань у галузі радіоелектроніки із використанням доступних комплектуючих, швидко встановлювати його у будь-якій організації чи установі.

Запропонований технічний пристрій було протестовано на працездатність в установах Вінницької області.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. С. Остапов. Технології захисту інформації / Остапов. С. – К.: Видавництво Родовід, 2014. – 428 с.
2. Євсєєв С. П., Король О. Г. Технології захисту інформації. Навчальний посібник /О.Г. Король, С. П. Євсєєв – К. : Видавництво «ХНЕУ», 2013. – 476 с.
3. В. Б. Чередниченко, К. Е. Чередниченко. Біометричні методи у системах захисту інформації [Текст] / Чередниченко К. Е., Чередниченко В. Б. – Суми : СДУ, 20120. – С. 145-148.
4. Бугаєнко Х. А., Горбенко І. Д. Аналіз трьох біометричних методів автентифікації особи / Х.А. Бугаєнко, І. Д. Горбенко // Прикладна радіоелектроніка. – № 2. – К. : "Друкарня Мадрид". – 2012. – С. 262-266.
5. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. С., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
6. Азарова А. О. Математичні моделі оцінювання стратегічного потенціалу підприємства та прийняття рішень щодо його підвищення [Текст] / А. О. Азарова, О. В. Антоноук. — Вінниця : ВНТУ, 2012. – 168 с.
7. Азарова А. О. Розробка методики визначення економічної безпеки підприємства [Текст] / А. О. Азарова, О. В. Гаврилова // Збірник наукових праць «Економіка: проблеми теорії та практики». – Дніпропетровськ : ДНУ, 2004. – Вип.191, т. III. – С. 719–727.
8. Азарова А. О. Розроблення механізму покращення інноваційної діяльності підприємства сучасними інформаційними технологіями [Текст] / А. О. Азарова // Колективна монографія: «Управління інноваційною, інвестиційною та економічною діяльністю інтегрованих об'єднань та підприємств» – 2016. – № 1. – С. 124–133.
9. Азарова А. О. Автоматизовані засоби покращення управління організаційним капіталом [Текст] / А. О. Азарова // Вісник Хмельницького національного університету. Економічні науки. Том 1. – №4. – 2015. – С. 85–88.

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-19м, vlados.blonskiy@gmail.com.

Гудзь Віталій Олександрович, Вінницький національний технічний університет, м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-19м, 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 Blonskiy, 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.