УДК 004.056.53

О. В. Бондаренко
В. В. Карпінець

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ В СИСТЕМАХ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

Вінницький національний технічний університет

Анотація

В даній роботі досліджено системи контролю і управління доступом. Впровадження сучасних систем контролю і управління доступом в організаціях дозволяє підтримувати високий рівень безпеки та надійності. Однак, деякі з цих систем, що працюють на основі розпізнавання людини по зображенню обличчя, мають суттєвий недолік. За результатами проведеного дослідження було запропоновано використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу.

Ключові слова: система контролю і управління доступом, СКУД, ідентифікація, інформаційна безпека, біометричний контроль доступу, двофакторна аутентифікація, графічний пароль.

Abstract

This paper explores access control and control systems. The implementation of modern systems of access control and management in organizations allows to maintain a high level of security and reliability. However, some of these systems that operate on the basis of human face recognition have a significant disadvantage. According to the results of the study, it was proposed to use a comprehensive identification system that combines several approaches to solving access problems.

Keywords: access control systems, ACS, identification, information security, biometric access control, two-factor authentication, graphic password.

Вступ

Одним із найважливіших завдань інформаційної безпеки для будь-якої організації є управління та керування доступом до інформаційних систем та ресурсів. Адже, правильно побудована та впроваджена система керування та управління доступом (СКУД) може значно знизити ризики несанкціонованих дій, можливості витоку інформації, ризики отримання користувачами неправомірного доступу та прав до інформаційних ресурсів, тощо [1].

Отже, основним завданням систем управління доступом до інформаційних ресурсів є запобігання несанкціонованому доступу до конфіденційної інформації або дії з інформацією, що порушують встановлені правила доступу до інформаційних систем.

Установка системи контролю та управління доступом є однією з найбільш важливих і необхідних систем в структурі будь-якого підприємства.

Результати дослідження

Система контролю і управління доступом до інформаційних систем та ресурсів повинна надавати користувачам лише необхідний доступ, а процес управління доступом повинен бути керованим та контрольованим.

Сучасні технічні засоби СКУД дозволяють вирішувати низку важливих проблем, таких як:

- протидія промисловому шпигунству;
- протидія крадіжкам;
- захист конфіденційної інформації;
- моніторинг дій користувачів та співробітників організації;
- керування та розмежування доступом [1].

Додаткові завдання СКУД - це ідентифікація осіб. Система контролю і управління доступом складається з цілого ряду компонентів, починаючи з тих, які ідентифікують співробітника, і закінчуючи тими, що приймають рішення про надання доступу.

За рівнем ідентифікації доступу СКУД поділяються на:

- однорівневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки);
- багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних) [2].

В системі контролю доступу для ідентифікації об'єктів використовуються наступне:

- ключі, карти;
- бейджи або жетони;
- за відбитками пальців;
- розпізнавання за райдужною оболонкою ока;
- розпізнавання осіб;
- квитки зі штрих-кодом або QR-кодом;
- паролі, коди.

Для ідентифікації у складі СКУД застосовують атрибутні та біометричні ідентифікатори. Біометричний контроль доступу являє собою автоматизований метод, за допомогою якого проходить ідентифікація людини. В біометричних ідентифікаторах використовують статичні та динамічні методи. Будь-яка біометрична технологія проводиться поетапно: сканування об’єкта, витяг окремої інформації, формування шаблону, порівняння поточного зразка із збереженим в базі даних шаблоном [3].

Серед біометричних систем розпізнавання людини за образом обличчя виділяється тим, що, по-перше, не вимагає особливого дорогого обладнання, достатньою умовою використання є наявність персонального комп’ютера та звичайної камери. По-друге, немає фізичного контакту між людиною і пристроями. Розпізнавання обличчя в будь-якій біометричній системі виконується в кілька етапів: виявлення обличчя, оцінка якості, побудова шаблону, зіставлення і прийняття рішення [3].

Основна відмінність біометричного способу ідентифікації від інших полягає в тому, що ідентифікація має принципово ймовірнісний характер. Рішення про допуск приймаються на основі ймовірнісного характеру отриманої інформації. Помилки в прийнятті рішень неминучі, а рівень цих помилок являється критерієм якості системи.

Отже, у більшості випадків для забезпечення безпечного доступу одного фактору аутентифікації недостатньо. Було досліджено, що будь-які способи ідентифікації та аутентифікації мають свої недоліки [2]. Тому побудувати захищену на 100% систему неможливо. Однак, використовуючи переваги факторів аутентифікації в комплексі, можна звести ризики до мінімуму.

СКУД має один істотний недолік - можливість підміни зловмисником зображення реального людини його портретом, тобто спроба видати портрет за реальну людину, що призводить до проникнення зловмисника на об'єкт інформаційної діяльності [4]. Підвищити ефективність СКУД в цьому випадку можна за допомогою багатофакторної ідентифікації. Наприклад, двофакторна ідентифікація припускає використання кодової клавіатури і Prox-карти. Принципово завдання захисту від несанкціонованого доступу така ідентифікація не вирішує, проте ускладнює роботу порушників, адже їм в даному випадку, необхідно вкрасти або зімітувати карту і дізнатися код (пароль) доступу [5].

Для підвищення надійності та точності роботи системи ідентифікації та аутентифікації користувачів запропоновано об’єднати біометричні характеристики із класичним способом аутентифікації, а саме, із графічним паролем. Використання графічних паролів є більш зручними та більш практичними для користувачів, за допомогою яких підвищується рівень безпеки та доступу до інформаційних систем [6].

Висновки

Отже, використання даного методу багатофакторної аутентифікації унеможливлює отримання доступу неавторизованим користувачем до інформаційних систем або об’єктів та забезпечує безпеку введеної ключової інформації. Якщо в спробі аутентифікації хоча б один з

компонентів відсутній або вказаний невірно, то ідентифікація користувача не встановлюється з достатнім ступенем впевненості та доступу до об’єкту (наприклад, до будівлі або даних), захищеному багатофакторною аутентифікацією, залишається заблокованим.

СКУД визнані одним з найбільш ефективних методів вирішення завдань комплексної безпеки для об'єктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем. - 2005.
2. Юдін О. Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74–79.
3. Задорожный В. Н. Обзор биометрических технологий / В. Н. Задорожный // Защита информации. Конфидент. – 2003. – № 5. – С. 26-29.
4. Воронова В. А. Системы контроля и управления доступом / В. А. Воронова, В. А. Тихонов. – М.: «Горячая линия – Телеком». -2010. – 272 с.
5. Конявская С. Контроль доступа – [Електронний ресурс] / С. Конявская //Информационная безопасность – Режим доступу : http://lib.itsec.ru/articles2/sys_ogr_dost/kontrol-dostupa
6. S. Wiedenbeck, J. Waters, J. C. Birgit, and A. Brodsky, “Authentication using graphical passwords: Basic results.” 2016 – Режим доступу : http://www.jimwaters.info/pubs/Graphical-Password-Basic-Results-2005.pdf
7. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Аза-рова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Бондаренко Олександр Володимирович **–** студент групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м.Вінниця, email: fm.ub15b.bondarenko@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Bondarenko Oleksandr V. – student of UB-19m group, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: fm.ub15b.bondarenko@gmail.com

Supervisor: ***Vasyl V Karpinets*** **–** Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia