УДК 519.711.3:343.98

Кульчицький О. С.;
Грицюк В. В.;
Зотова І. Г.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в інформаційно-телекомунікаційних системах

Резюме. У статті проведено аналіз сучасних підходів, які на сьогодні використовуються для ідентифікації користувачів в інформаційно-телекомунікаційних системах.

Ключові слова: захист інформаційно-телекомунікаційних систем, ідентифікація користувачів персональних електронно-обчислювальна машина (ПЕОМ).

Постановка проблеми. З розповсюдженням комп'ютерних технологій все гостріше постає проблема захисту інформації в інформаційно-телекомунікаційних системах. Тому, на сьогодні актуальними є теоретичні концептуальні проекти в області захисту інформації та їх практичне застосування безпосередньо в конкретних інформаційно-телекомунікаційних системах (далі ІТС). Створення єдиної, керованої системи безпеки є однією з умов для існування сучасної ІТС.

Управління доступом - один із методів захисту інформації, який регулює та санкціонує доступ до інформаційних ресурсів системи, для якої розробляється комплексна система захисту інформації (далі КСЗІ). Методи і системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в ІТС:

- ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;
- упізнання і встановлення достовірності користувача за присвоєним логіном та паролем, що вводяться (на цьому принципі працює більшість моделей інформаційної безпеки);
- надання певних ролей та повноважень, кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей ІТС;
- протоколювання всіх дій користувачів на ПЕОМ, інформаційна безпека яких захищає інформаційні ресурси від несанкціонованого доступу і відстежує всі транзакції користувачів у системі.

Управління та розмежування доступу до комп'ютерних систем і до їх ресурсів є одним з важливих аспектів інформаційної безпеки. Це може бути реалізовано за рахунок ідентифікації користувачів.

Аналіз останніх досліджень і публікацій. Останнім часом все більше зростає увага науковців у галузі інформаційної безпеки до способів ідентифікації особи користувача. Як доказ цьому - значне збільшення досліджень та публікацій, які присвячені цій проблемі. Але слід зауважити, що значна більшість наукових статей присвячена докладному аналізу найбільш поширеному зі способів ідентифікації користувачів - парольній ідентифікація [2, 3]. Біометричній ідентифікації також приділяється значна увага, про що свідчать публікації [4, 5]. Але найчастіше розглядаються лише окремі біометричні ознаки, що використовуються для визначення особи користувача. Що стосується комплексного підходу до ідентифікації користувачів, то в сучасній науковій літературі майже не представлено досліджень та практичних рішень з одночасним використанням декількох ознак для ідентифікації [7-10].

Метою статті є формулювання обґрунтованих рекомендацій щодо доцільності використання існуючих способів ідентифікації і методів аутентифікації при створенні КСЗІ в інформаційно-телекомунікаційних системах, на основі аналізу позитивних рис та недоліків кожного з них.

Виклад основного матеріалу. Під несанкціонованим доступом розуміється доступ до інформації, що порушує встановлені правила розмежування і здійснюється з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

Задачею систем ідентифікації і аутентифікації є визначення і верифікація

набору повноважень суб'єкта при доступі до інформаційної системи.

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). На сьогодні існує декілька способів ідентифікації користувачів [5], у кожного з яких свої переваги і недоліки.

Аутентифікація - це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу. Методи аутентифікації можна розділити на 4 великі групи [9], які наведені у табл. 1.

Таблиця 1

№	Методи аутентифікації	Характеристика методу
1	Методи, засновані на знанні секретної інформації	Класичним прикладом таких методів є парольний захист, коли в якості засобу аутентифікації користувачу пропонується ввести пароль – деяку послідовність символів. Такі методи аутентифікації є найпоширенішими
2	Методи, засновані на використанні унікального предмета	В якості такого предмета можуть бути використані: смарт-карта, токен, електронний ключ тощо.
3	Методи, засновані на використанні біомет-ричних характеристик людини	На практиці частіше використовуються одна або деякі з наступних біометричних характеристик: відбитки пальців (найбільш розповсюджено); малюнок сітківки або райдужної оболонки ока; термографія долоні; геометрія і термограма обличчя; почерк (підпис); голос
4	Методи, засновані на інформації, асоційованій з користувачем	Прикладом такої інформації можуть бути координати користувача, визначені за допомогою GPS. Цей підхід навряд чи може бути використаний як єдиний механізм аутентифікації, проте цілком допустимо його використання як додаткового елементу захисту

Поширена практика сумісного використання декількох з перерахованих вище механізмів – у таких випадках кажуть про багатофакторну аутентифікацію.

Розглянемо перераховані підходи докладніше.

Парольні системи захисту. Головна перевага парольної ідентифікації - простота і звичність [2]. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу (НСД).

Заходи, які дають змогу значно підвищити надійність парольного захисту [3]:

- накладання технічних обмежень: встановлення мінімальної довжини пароля, використання у паролях різних груп символів (букв, цифр, знаків пунктуації тощо);
- управління терміном дії паролів, їх періодична зміна;
- обмеження доступу до файла паролів;
- обмеження кількості невдалих спроб входу в систему;
- використання програмних генераторів паролів.

Парольна система є "переднім краєм оборони" всієї системи безпеки. Деякі її елементи (зокрема ті, що реалізують інтерфейс користувача) можуть бути розташовані в місцях, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним із перших об'єктів атаки при вторгненні зловмисника в захищену систему.

Перерахуємо типи загроз безпеки парольних систем:

- розголошування параметрів облікового запису через: підбір в інтерактивному режимі; навмисну передачу пароля його власником іншій особі; перехоплення переданої по мережі інформації про пароль;
- втручання у функціонування компонентів парольної системи через: впровадження програмних закладок; виявлення і використовування помилок, допущених на стадії розроблення; виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю, так званого, людського фактора, що виявляється в тому, що користувач може вибрати пароль, який легко запам'ятати і також легко підібрати; записати пароль, який складно запам'ятати, і покласти запис у доступному місці; передати пароль іншій особі навмисно або під впливом.

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів у базі даних облікових записів. Можливі наступні варіанти зберігання паролів: у відкритому вигляді; у вигляді згорток (хешування); зашифрованими за деяким ключем.

Найбільш цікавими є другий і третій способи, які мають ряд особливостей.

Хешування (використання незворотної хеш-функції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору

паролів по словнику у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати неспівпадання значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність згорток у випадку, якщо два користувачі вибирають однакові паролі.

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів. Перерахуємо деякі можливі варіанти: ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження; ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску; ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску.

Найбезпечніше зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при їх комбінації.

Враховуючи, що користувачі нерідко вибирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого по мережі значення згортки пароля представляють серйозну загрозу безпеці парольної системи. [10].

У захищеній системі передачу можна застосовувати тільки у поєднанні із засобами захисту мережевого трафіку.

Ідентифікація з використанням унікального предмета. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм (eToken), який зазвичай невеликих розмірів (його можна носити із собою), зручний та недорогий.

Основне призначення:

- двофакторна аутентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);
- безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків тощо в незалежній пам'яті ключа;
- апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування електронного цифрового підпису - ЕЦП).

Можливі переваги застосування:

- сувора аутентифікація користувачів при доступі до серверів, баз даних, розділів веб-сайтів;
- безпечне зберігання секретної інформації: паролів, ключів шифрування, закритих ключів цифрових сертифікатів;
- захист електронної пошти (цифровий підпис і шифрування, доступ);
- системи електронної торгівлі;
- захист комп'ютерів;
- захист мереж та каналів передачі даних за рахунок побудови - віртуальні приватні мережі;

Переваги eToken:

- аутентифікація користувачів за рахунок використання криптографічних методів;
- безпечне зберігання ключів шифрування і ЕЦП;
- мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері);
- безпечне використання - скористатися ключем eToken може тільки його власник;
- реалізація як західних, так і вітчизняних стандартів на шифрування ;
- зручність роботи - ключ виконаний у вигляді брелока зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів;
- використання одного ключа для вирішення безлічі завдань - входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП.

Біометрична ідентифікація. Біометрична ідентифікація - це спосіб ідентифікації особи за окремими специфічними біометричними ознаками [6]. Сучасний рівень розвитку комп'ютерних технологій дав змогу використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про доступ до ресурсів. Біометричні механізми ідентифікації наведені у табл. 2.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці серед них небагато. Основних методів три - розпізнавання за відбитком пальця, за зображенням особи (двомірному або тривимірному), за райдужною оболонкою та за сітківкою ока.

Важко не погодитися, що біометричні технології надійніші та зручніші за засоби захисту, які широко застосовувалися до сьогодні [5].

Комплексна (або багатофакторна) ідентифікація. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку. Нині існують комбіновані системи наступних типів:

- системи на базі безконтактних смарт-карт і USB-ключів;
- системи на базі гібридних смарт-карт;
- біоелектронні системи.

Таблиця 2

Вид ознаки	Характеристика механізмів ідентифікації
Статичні ознаки - ознаки, які практично не змінюються з часом, починаючи з народження людини (фізіологічні характеристики)	*Ідентифікація за відбитком пальця* побудована таким чином: за допомогою сканера одержують зображення відбитку, потім це зображення за складним алгоритмом перетворюється на спеціальний цифровий код, який далі порівнюється з еталонними кодами, що зберігаються в базі даних
	Ідентифікація за розташуванням вен на долоні. Прилад, який зчитує інформацію в цьому випадку, є інфрачервона камера. У результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці людини. Не потребує контакту людини з пристроєм для сканування. Має високі показники надійності і достовірності
	Ідентифікація за сітківкою ока. В цьому випадку сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. За допомогою програмного забезпечення із зображення виділяється малюнок потрібної райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів
	Ідентифікація за райдужною оболонкою ока. Малюнок райдужної оболонки ока - унікальний для кожної людини. За допомогою програмного забезпечення із зображення виділяється малюнок потрібної райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів
	Ідентифікація за формою кисті руки ґрунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код
	Ідентифікація за формою обличчя. Двовимірне розпізнавання обличчя на сьогодні - один із самих неефективних методів біометрії, тому має обмежене коло застосування або використовується тільки в сукупності з іншими методами
Динамічні ознаки - поведінкові характеристики, які побудовані на особливостях підсвідомих рухів у процесі відтворення будь-якої дії	*Ідентифікація за голосом* – враховуються унікальні частотні характеристики голосу людини
	Ідентифікація за почерком - досліджується почерк людини. Перевіряються такі динамічні характеристики: графічні параметри, сила натиску на поверхню, швидкість написання. На основі цих характеристиках і будується цифровий код
	Ідентифікація за клавіатурним почерком - метод аналогічний ідентифікації за почерком. Замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується по динаміці набору певного слова або фрази

Безконтактні смарт-карти і USB-ключі. У корпус брелока USB-ключа вбудовується антена і мікросхема для створення безконтактного інтерфейсу. Це дасть змогу організувати управління доступом у приміщення і до комп'ютера, використовуючи один ідентифікатор. Ця схема використовування ідентифікатора може виключити ситуацію, коли співробітник, покидаючи робоче місце, залишає USB-ключ у роз'ємі комп'ютера, що дасть змогу працювати під його ідентифікатором.

Гібридні смарт-карти. Один чип підтримує контактний інтерфейс, інший - безконтактний. Як і гібридні USB-ключі, гібридні смарт-карти розв'язують дві задачі: доступ у приміщення і доступ до комп'ютера. Додатково на карту можна нанести логотип компанії, фотографію співробітника або магнітну смугу, що робить можливим повністю замінити звичайні перепустки і перейти до єдиної "електронної перепустки".

Біоелектронні системи. Як правило, для захисту комп'ютерних систем від несанкціонованого доступу застосовується комбінація з двох систем - біометричної і контактної на базі смарт-карт або USB-ключів.

Досягти підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна за рахунок об'єднання використання біометричних характеристик разом із класичними способами ідентифікації користувачів (наприклад, парольний захист, РПЧ-код, використання різноманітних карт) [9].

Висновки. На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів ІТС, можна впевнено сказати, що парольний захист на сьогодні є одним із найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах розподілених систем. Проте без використовування інших механізмів захисту парольний захист не є надійним, оскільки не може забезпечити потрібного захисту. Слід зауважити, що останнім часом все більше набувають популярності дорогі системи

ідентифікації, які використовують біометричні характеристики людини при розв'язанні задачі доступу до ІТС. Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, власник ІТС повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/аутентифікації. Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем.

Подальші дослідження. Актуальною бачиться проблема розроблення і дослідження комплексних систем, що використовують для прийняття рішення доступу до інформаційних систем декілька біометричних характеристик користувача (наприклад, використовувати разом особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором "миша" або відбитків декількох пальців) [7].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Воронова В. А. Системы контроля и управлений доступом /В. А. Воронова, В. А. Тихонов. - М.: "Горячая линия – Телеком", 2010 - 272 с.
2. Даклин Пол. Простые советы по более разумному выбору и использованию паролей / Пол Даклин. [Електронний ресурс]. — http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml – название с экрана.
3. Безмалый В. Парольная защита: прошлое, настоящее, будущее / В. Безмалый // IT сообщество України жовтень 2014 [Електронний ресурс]. - https://www.it-community.in.ua/2014/10/parolnaya-zashhita-proshloe-nastoyashhee-budushhee.html/
4. Голубев Г.А. Современное состояние и перспективы развития биометрических технологий / Г.А. Голубев,Б.А. Габриелян // Нейрокомпьютеры: разработка, применение. - 2004. -№10.- С. 39-46.
5. Десятчиков А. А. Синхронная биометрическая многофакторная идентификация / А. А. Десятчиков, А. Б. Муринин, Ю. П. Тресков, В. Я. Чучупал // Труды ИСА РАН. Динамика неоднородных систем. - М.: УРСС. -2005. - Вып. 9 (1). - С. 188-194.
6. Коновалов Д. Н. Технология защиты информации на основе идентификации голоса / Д. Н. Коновалов, А. Г. Бояров // [Електронний ресурс]. -Режим доступу к ресурсу: http://www.fact.ru/archive/07/voice.shtml
7. Завгородний В. И. Комплексная защита информации в компьютерных системах: учебное пособие / В. И. Завгородний. - М.: Логос; ПБОЮЛН.А. Егоров, 2001. - 264 с.
8. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А. Ю. Щеглов. - СПб.: Наука и техника, 2004. - 384 с.
9. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. - К: Изд-во Юниор, 2003. - 504 с.
10. Конахович Г. Ф. Захист інформації в мережах передачі даних: підручник /Г. Ф. Конахович, О. Т. Корченко, О. К. Юдін. - К: Видавництво ТОВ НЕП "ШТЕРСЕР-ВІС", 2009. - 714 с.

Стаття надійшла до редакції 28.10.2016

Кульчицкий А. С.;
Грицюк В. В.;
Зотова И. Г.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Анализ существующих подходов при идентификации пользователей в информационно-телекоммуникационных системах

Резюме. В статье проводится анализ современных подходов, которые используются для идентификации пользователей в информационно-телекоммуникационных системах.

Ключевые слова: защита информационно-телекоммуникационных систем, идентификация пользователей персональных электронно-вычислительных машин (ПЕОМ).

O. Kulchitskiy;
V. Hrytsiuk;
I. Zotova

Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovsky, Kyiv

Analysis of existing approaches to authenticate users in telecommunications systems

Resume. The article analyzes the current approaches used in the present for identification for users in information and telecommunication systems.

Keywords: protection of information and telecommunication systems, identification of users of personal electronic computer (PC).