УДК 004.056.53

Мазниченко Наталя Іванівна

Ст. викладач кафедри криміналістики

Національний юридичний університет імені Ярослава Мудрого

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ СИСТЕМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Анотація. *Стаття присвячена огляду та аналізу сучасних підходів, які використовуються сьогодні для ідентифікації та аутентифікації користувачів комп'ютерних систем. Важливість дослідження обумовлена актуальністю проблеми захисту комп'ютерної інформації та обмеження доступу до інформаційних ресурсів комп'ютера. Результати виконаних досліджень і зроблені висновки можуть бути корисні при створенні власних систем захисту комп'ютерної інформації окремими користувачами.*

Ключові слова: *захист комп'ютерної інформації, ідентифікація, аутентифікація*

Abstract. *The article is devoted a review and analysis of modern approaches which are used today for information and authentication of users of the computer*

systems. Research importance is conditioned actuality of problem of defence of computer information and access restriction to the informative resources of computer. Results of the executed researches and done conclusions can be useful at creation of the own systems of defence of computer information separate users.

***Keywords**: defence of computer information, identification, authentication*

Постановка проблеми. Зростання застосування сучасних інформаційних технологій в різних сферах діяльності людини робить можливим поширення різних зловживань, пов'язаних з використанням обчислювальної техніки. Величезна кількість інформації обмеженого доступу зберігається і обробляється в інформаційних комп'ютерних системах, що формує потребу в забезпеченні їх інформаційної захищеності. Саме тому останнім часом виріс інтерес до питань захисту комп'ютерної інформації з обмеженим доступом.

При забезпеченні інформаційної безпеки комп'ютерних систем необхідно враховувати, що обмін інформацією є щонайпершою умовою життєдіяльності кожної організації. Для протидії злочинам в інформаційній сфері або хоч би зменшення збитку необхідно грамотно вибирати заходи і засоби забезпечення захисту комп'ютерної інформації від умисного руйнування, крадіжки, псування, несанкціонованого доступу, несанкціонованого читання і копіювання. Важливою проблемою забезпечення безпеки інформаційних ресурсів комп'ютерних систем є завдання обмеження кола осіб, що мають доступ до конкретної інформації і захисту її від несанкціонованого доступу.

У інформаційній сфері історично сформувалися два напрями захисту від несанкціонованого доступу. У системах фізичного захисту вони називаються системами управління доступом (СУД), а в комп'ютерній сфері – системами ідентифікації і аутентифікації. [1, с. 172]

Ідентифікацію і аутентифікацію можна вважати основою програмно-технічних засобів безпеки тому, що решта сервісів розраховують на обслуговування іменованих суб'єктів. Ідентифікація і аутентифікація – це

перша лінія захисту, «прохідна» інформаційного простору комп'ютерної системи. [2, с. 127] Саме від коректності рішення цих двох завдань залежить, чи можна дозволити доступ до ресурсів комп'ютерної системи конкретному користувачеві. Засоби ідентифікації (розпізнавання користувача по пред'явленому ідентифікатору) та аутентифікації (встановлення достовірності ідентифікованого користувача) належать до категорії класичних механізмів управління доступом користувачів і інформаційної безпеки комп'ютерних систем та мереж.

Система захисту виконує ідентифікацію та аутентифікацію на основі певної унікальної інформації, яка характеризує конкретного користувача системи [3].

Сьогодні використовуються наступні підходи до задач ідентифікації та аутентифікації користувачів [4, с. 216]:

1) парольний – використовує унікальне знання (наприклад, логін-пароль);

2) апаратний (або електронний) – використовує унікальний предмет (проксіміті-карти, смарт-карти, магнітні карти, токени і т.д.);

3) біометричний – використовує унікальні характеристики людини (відбитки пальців, сітківка ока, голос, почерк і т.д.).

У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші - в інших. Але строго однозначного рішення немає, тому користувачам приходиться самостійно обирати, який спосіб ідентифікації реалізовувати у власних інформаційних комп'ютерних системах. Такий вибір повинен бути обґрунтованим, а для цього потрібно ретельно проаналізувати можливості кожного з перерахованих підходів.

Виклад основного матеріалу. Управління доступом – ефективний метод захисту інформації, регулюючий використання ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки. Методи і системи захисту інформації, що спираються на управління доступом, включають

наступні функції захисту інформації в інформаційних системах:

– ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;

– впізнання і встановлення достовірності користувача за обліковими даними, що вводяться (на даному принципі працює більшість моделей інформаційної безпеки);

– допуск до певних умов роботи згідно регламенту, наказаному кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей інформаційних систем;

– протоколювання звертань користувачів до ресурсів, інформаційна безпека яких захищає ресурси від несанкціонованого доступу і відстежує некоректну поведінку користувачів системи.

З вищенаведеного можна впевнено стверджувати, що система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу до будь-якої інформаційної комп'ютерної системи.

Розглянемо кожен з перерахованих підходів більш докладно.

Парольна ідентифікація/аутентифікація.

На сьогоднішній день парольна ідентифікація/аутентифікація є найпоширенішим способом визначення особи користувача [5, с. 14]. І в цьому немає абсолютно нічого дивного. Цей спосіб найбільш простий як у реалізації, так й у використанні. Суть парольної ідентифікації/аутентифікації зводиться до наступного. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (звичайно використаються пари логин-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особу та ідентифікує її.

Головна перевага парольної ідентифікації – це простота реалізації й

використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною.

Тепер перейдемо до недоліків. На жаль, їх багато. І самий, мабуть, головний – величезна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. До них відносяться занадто короткі паролі, загальновідомі сполучення символів і т.д. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів. Оскільки володіння вірним паролем майже завжди гарантує зловмиснику владу над інформаційною системою, атаки на парольні системи є найбільш поширеними формами дій інформаційних порушників. Для досягнення цієї мети зловмисники часто звертаються до спеціальних програм, що спрямовані на «злам» парольної системи.

При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкість парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу.

Наступні заходи дозволять значно підвищити надійність парольного захисту [6]:

– накладення технічних обмежень (пароль повинен бути не дуже коротким, він повинен містити букви, цифри, знаки пунктуації і т.п.);

– управління терміном дії паролів, їх періодична зміна;

– обмеження доступу до файлу паролів;

– обмеження числа невдалих спроб входу в систему (це утруднить застосування «методу грубої сили»);

– використання програмних генераторів паролів (така програма,

ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні паролі, що достатньо легко запам'ятовуються).

Апаратна (або електронна) ідентифікація/аутентифікація.

Цей принцип ідентифікації та аутентифікації ґрунтується на визначенні особи користувача по якомусь предмету, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера.

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, у них реалізовано чимало різних захисних механізмів. Ну а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації/аутентифікації користувача, але й виконувати деякі інші корисні функції.

Ну а тепер давайте поговоримо про недоліки апаратної ідентифікації/аутентифікації. Мабуть, найбільш серйозною небезпекою у випадку використання даного методу є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології – ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте, для введення в експлуатацію системи такої ідентифікації/аутентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами або картами. Крім того, згодом деякі типи ключів можуть зношуватися, крім того, вони можуть бути загублені й т.д. Тобто апаратна ідентифікація/аутентифікація вимагає деяких експлуатаційних витрат.

Біометрична ідентифікація/аутентифікація.

Біометрична ідентифікація/аутентифікація – це спосіб визначення особи по окремих специфічних біометричних ознаках, властивих конкретній людині [7, с. 8]. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про можливість доступу до ресурсів комп’ютерних систем. Даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак.

Серед біометричних механізмів ідентифікації/аутентифікації можна виділити такі:

1) по статичних ознаках – те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);

2) по динамічних ознаках – поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

В задачах ідентифікації користувача комп’ютерних систем використовуються наступні статичні ознаки (характеристики): відбиток пальця, сітківка ока, райдужна оболонка ока, форма грона руки, форма обличчя (двохвимірне та трьохвимірне) та інші.

Серед динамічних ознак в задачах ідентифікації/аутентифікації користувачів використовуються наступні: голос, почерк, клавіатурний почерк, особливості роботи з маніпулятором «миша».

Всі біометричні системи ідентифікації/аутентифікації працюють за однаковим принципом: фізичний або поведінковий зразок за допомогою спеціального пристрою (сканера, спеціальної камери) запам'ятовується системою (процес запису), потім по складному алгоритму перетворюється на цифровий код. Далі цей код порівнюється з еталонними кодами зареєстрованих користувачів, які зберігаються в базі даних комп’ютерної системи. За результатами порівняння біометрична система робить висновок про можливість

доступу до інформаційних ресурсів, що захищаються.

Головним достоїнством біометричних технологій є найвища точність [8, с.3]. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або може бути використана фотографія пальця зареєстрованого користувача. Втім, треба зазначити, що сучасні пристрої значно стійкіші по відношенню до подібної фальсифікації.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються. Крім того, не дуже давно з'явилися миші й клавіатури з вбудованими дактилоскопічними сканерами.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці, серед них небагато. В основному використовують наступні – розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному), по райдужній оболонці ока, по сітківці ока, по голосу.

Поки що було розглянуто три види (або підходи) однофакторної ідентифікації/аутентифікації користувачів комп’ютерних систем. Тобто в розглянутих системах для визначення особи користувача використовувався тільки один фактор. Однак подібні процеси сьогодні не можна назвати надійними. Останнім часом набуває поширення комплексна або багатофакторна ідентифікація, яку не можна виділити в окремий вид, але потрібно обов’язково її розглянути і проаналізувати.

Комплексна (або багатофакторна) ідентифікація/аутентифікація.

В таких системах для визначення особи користувача комп’ютерної інформаційної системи застосовується відразу кілька параметрів. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак

і тим самим підвищує безпеку [9, с.42]. Причому комбінуватися ці параметри можуть у довільному порядку і можуть належати як системам одного класу так і різним. Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист (або PIN-код) і токен. Основною перевагою такої ідентифікації/аутентифікації є додаткова стійкість до «злому». Адже втрата апаратного ключа не спричиняє за собою компрометації пароля, оскільки окрім ключа для доступу до комп'ютерної системи потрібний ще і PIN-код до ключа. При організації системи строгої ідентифікації/аутентифікації слід використати, як мінімум, двохфакторну схему.

У деяких системах для максимальної надійності процедури ідентифікації/аутентифікації застосовуються одночасно паролі, токени і біометричні характеристики людини.

Досягти підвищення надійності та точності автоматизованих систем ідентифікації/аутентифікації користувачів можна за рахунок об'єднання використання біометричних характеристик (наприклад, відбиток пальця) разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PIN-код, використання різноманітних карт і т.д.).

Також підвищити надійність систем ідентифікації/аутентифікації користувачів, на мій погляд, можна поєднанням захисту за допомогою пароля (як найпоширенішого на сьогоднішній день) і за допомогою аналізу клавіатурного почерку користувача (особливість та манера введення парольної фрази). Основною перевагою комбінації даних методів є відсутність необхідності використання додаткового устаткування.

Актуальною бачиться задача розробки і дослідження комплексних систем, що використовують для прийняття рішення доступу до комп'ютерних систем декілька біометричних характеристик користувача (наприклад, використовувати разом особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором «миша» або використання відбитків декількох пальців і т.д.). Деякі виробники вже розпочали інтеграцію двох

методів розпізнавання облич, включаючи дво- і тривимірні зображення.

Сильні і слабкі сторони багатофакторної ідентифікації, загалом, відомі. До її переваг можна віднести здатність підвищення захищеності інформаційних ресурсів комп'ютерних систем за рахунок використання декількох рівнів захисту. Певною слабкістю можна вважати необхідність використання додаткових програмно-апаратних комплексів, засобів зберігання і зчитування даних. Слід відзначити, що методам захисту, заснованим на механізмах багатофакторної аутентифікації, сьогодні довіряє багато зарубіжних компаній.

Висновки. Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання загроз для інформаційних ресурсів комп'ютерних систем все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до захищеності комп'ютерних систем.

Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/аутентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бакланов В. В. Введение в информационную безопасность. Направления информационной защиты: Учеб. пособие // Екатеринбург: Изд-во Урал. ун-та, 2007. 236 с.

2. Основы компьютерной безопасности: курс лекций. Учебное пособие (издание третье). Галатенко В.А. Под редакцией академика РАН В.Б Бетелина. – М.: ИНТУИТРУ «Интернет-университет Информационных технологий», 2006. – 208 с.

3. Сарбуков А.Е. Аутентификация в компьютерных системах / А.Е. Сарбуков, А.А. Грушо // Системы безопасности. – 2003. – № 5(53). – С. 118–122. [Електронний ресурс] Режим доступу: http://cctv-pro.com.ua/article/3780/a-sarbukov-a--grusho--autentifikaciya-v-kompyuternyh-sistemah-/

4. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. С 215-223.

5. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс: учебное пособие. – Ростов-на-Дону: Феникс, 2008. – 173 с.

6. Даклин Пол. Простые советы по более разумному выбору и использованию паролей / Сетевая газета InfoSecurity.ru. [Електронний ресурс]. Режим доступу: http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml

7. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.

8. Савинов А.Н. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах: Автореф. дис. … канд. техн. наук: 05.13.19. – СПб: СПб НИУ ИТМО, 2013. – 19 с.

9. Безмалый В.Ф. Парольная защита: прошлое, настоящее, будущее // Науково- технічний журнал «Захист інформації». – 2006. – №3. С. 38-45.