УДК 519.711.3:343.98

Н.А. Кошева, Н.І. Мазниченко

Національний університет «Юридична академія України імені Ярослава Мудрого», Харків

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ: АНАЛІЗ І ПРОГНОЗУВАННЯ ПІДХОДІВ

Стаття присвячена огляду та аналізу сучасних підходів, які використовуються сьогодні для ідентифікації користувачів комп'ютерних систем. Це особливо важливо в зв'язку з актуальністю проблеми захисту комп'ютерної інформації та обмеженню доступу до інформаційних та технічних 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 користувачів ЕОМ.*

Вступ

У зв'язку з загальним розповсюдженням комп'ютерних технологій все гострішою встає проблема захисту інформації в комп'ютерних інформаційних системах. Тому дуже актуальними бачаться теоретичні розробки в області захисту комп'ютерної інформації та практичне їх застосування безпосередньо в певних конкретних комп'ютерних системах. Питання захисту інформації в комп'ютерних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до комп'ютерних даних, що захищаються. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1].

Управління доступом – ефективний метод захисту інформації, регулюючий використовування ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки [2]. 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.

Як бачимо, ідентифікація користувачів є невід'ємним та важливим елементом і основою ефективності будь-якої системи управління доступом до інформаційних ресурсів комп'ютерних систем.

Аналіз літератури. Управління та розмежування доступу до комп'ютерних систем і до їх ресурсів є одним з важливих аспектів інформаційної безпеки, що може бути реалізовано за рахунок ідентифікації користувачів. Останнім часом все більша увага науковців в галузі інформаційної безпеки приділяється способам ідентифікації особи користувача. Доказом цього можна вважати значне збільшення досліджень та публікацій, які присвячені цій проблемі. Але слід зауважити, що значна більшість наукових статей присвячується докладному розгляданню лише одного з можливих способів ідентифікації користувачів. Наприклад, парольна ідентифікація на сьогоднішній день є найбільш дослідженим способом ідентифікації, тому більша частина публікацій присвячується саме даному способу [3, 4]. Біометричній ідентифікації також приділяється значна увага, про свідчіть велика кількість публікацій в науковій літературі [5, 6, 7, 8], але найчастіше розглядаються лише окремі біометричні ознаки, що використовуються для визначення особи користувача. Стосовно апаратної ідентифікації серед розглянутих джерел можна знайти лише запропоновані практичні рішення без докладного аналізу та порівняльної характеристики [9]. Що ж стосується комплексного підходу до ідентифікації користувачів, то в сучасній науковій літературі майже не представлено досліджень та практичних рішень систем, в яких використовується декілька ознак для ідентифікації одночасно [10, 11, 12].

Мета статті. Кожен сучасний користувач повинен добре орієнтуватись у сучасних підходах до реалізації задачі ідентифікації. Основною метою статті є спроба проаналізувати існуючі сучасні підходи до задачі ідентифікації користувачів комп'ютерних систем, виявлення позитивних рис та недоліків кожного з них. На основі зроблених досліджень сформулюва-

ти висновки щодо доцільності використання кожного зі способів ідентифікації та порад і рекомендацій користувачам для їх застосування для організації власних систем захисту комп'ютерної інформації за рахунок ідентифікації користувачів.

Основна частина

Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційної системи [13].

Під несанкціонованим доступом до інформації розумітимемо доступ до інформації, що порушує встановлені правила розмежування доступу і здійснюваний з використанням штатних засобів обчислювальної техніки або автоматизованих систем. НСД може носити випадковий або навмисний характер.

Задачею систем ідентифікації і аутентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи.

Ідентифікація дозволяє суб'єкту (користувачу, процесу, діючому від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). Ідентифікація – це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка достовірності". Аутентифікація – це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу.

Ці процедури (ідентифікація та аутентифікація) нерозривно зв'язані між собою, оскільки спосіб перевірки визначає, яким чином і що користувач повинен пред'явити системі, щоб отримати доступ.

Сьогодні існує декілька способів ідентифікації користувачів [14].

У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних комп'ютерних системах, інші – в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно вирішувати, який спосіб ідентифікації реалізовувати у власних інформаційних комп'ютерних системах.

Існує три найпоширеніших види ідентифікації:

1). Парольна ідентифікація. Ще не дуже давно парольна ідентифікація була ледве не єдиним способом визначення особистості користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її 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 особистість 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.

2). Апаратна (або електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. Природно, мова йде не про звичні для більшості людей ключі, а про спеціальні електронні [9]. 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, в них реалізовано чимало різних захисних механізмів. Ну а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Ну а тепер давайте поговоримо про недоліки апаратної ідентифікації. Мабуть, найбільш серйозною небезпекою у випадку використання апаратної ідентифікації 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, 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 однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом де-

які типи ключів можуть зношуватися, крім того, вони можуть бути загублені й т.д. Тобто апаратна ідентифікація вимагає деяких експлуатаційних витрат.

3). Біометрична ідентифікація. Біометрія – це ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини. А тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак [5].

Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Головним достоїнством біометричних технологій є найвища надійність. 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 зізнатися, що сучасні пристрої значно стійкіші по відношенню до подібної фальсифікації.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входить 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.

Поки що було розглянуто три види (або підходи) однофакторної ідентифікації користувачів інформаційних 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 про неї нагадати і розповісти.

Комплексна (або багатофакторна) ідентифікація. В системах комплексної ідентифікації для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів [11]. Причому комбінуватися ці параметри можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбора його пароля зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

Розглянемо кожен з перерахованих підходів більш докладно.

Парольні системи захисту

Головна перевага парольної ідентифікації – простота і звичність [15]. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності 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. Але поки символьний пароль – найпоширеніший спосіб ідентифікації і аутентифікації користувачів і ще довго їм залишатиметься.

Наступні заходи дозволять значно підвищити надійність парольного захисту [3]:

– накладання технічних обмежень: встановлення мінімальної довжини пароля, використання в паролі різних груп символів (пароль повинен містити букви, цифри, знаки пунктуації і т.п.);

– управління терміном дії паролів, їх періодична зміна;

– обмеження доступу до файлу паролів;

– обмеження кількості невдалих спроб входу в систему;

– використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні паролі, що запам'ятовуються).

Для детальнішого розгляду принципів побудови парольних систем сформулюємо декілька основних визначень.

Ідентифікатор користувача – деяка унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача.

Пароль користувача – деяка секретна кількість інформації, відома тільки користувачу і парольній системі, яке може запам'ятати користувачем і пред'явлене для проходження процедури аутентифікації. Одноразовий пароль дає можливість користувачу однократно пройти аутентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

Обліковий запис користувача – сукупність його ідентифікатора і його пароля.

База даних користувачів парольної системи містить облікові записи всіх користувачів даної парольної системи.

Під парольною системою розумітимемо програмно-апаратний комплекс, що реалізовує системи

ідентифікації і аутентифікації користувачів автоматизованих систем (АС) на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Основними компонентами парольної системи є:

– інтерфейс користувача;

– інтерфейс адміністратора;

– модуль сполучення з іншими підсистемами безпеки;

– база даних облікових записів.

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 з перших об'єктів атаки при вторгненні зловмисника в захищену систему. Нижче перераховані типи загроз безпеки парольних систем.

1). Розголошування параметрів облікового запису через:

– підбір в інтерактивному режимі;

– підглядання;

– навмисну передачу пароля його власником іншій особі;

– захват бази даних парольної системи;

– перехоплення переданої по мережі інформації про пароль;

– зберігання пароля в доступному місці.

2). Втручання у функціонування компонентів парольної системи через:

– впровадження програмних закладок;

– виявлення і використовування помилок, допущених на стадії розробки;

– виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського фактору, 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 в доступному місці;

– ввести пароль так, що його зможуть побачити сторонні;

– передати пароль іншій особі навмисно або під впливом помилки.

На додаток до вище сказаного необхідно наголосити на існуванні "парадоксу людського фактору". Полягає він в тому, що користувач нерідко прагне виступати скоріш супротивником парольної системи, як, втім, і будь-якої системи безпеки, функціонування якої впливає на його робочі умови, ніж союзником системи захисту, тим самим послаблюючи її.

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів в базі даних облікових записів. Можливі наступні варіанти зберігання паролів:

– у відкритому виді;

– у вигляді згорток (хешування);

– зашифрованими за деяким ключем.

Найбільший інтерес представляють 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 неспівпадіння значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність згорток в тому випадку, якщо два користувача вибирають однакові паролі. Для цього при розрахунку кожної згортки зазвичай використовують деяку кількість "випадкової" інформації, наприклад, видаваною генератором псевдовипадкових чисел.

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.

У другому випадку необхідно забезпечити неможливість автоматичного перезапуску системи, навіть якщо вона виявляє носій з ключем. Для цього можна зажадати від адміністратора підтверджувати продовження процедури завантаження, наприклад, натисненням клавіші на клавіатурі.

Найбільш безпечне зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при комбінації другого і третього способів.

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.

В більшості випадків аутентифікація відбувається в розподілених системах і пов'язана з передачею по мережі інформації про параметри облікових записів користувачів. Якщо інформація, що передається по мережі в процесі аутентифікації, не захи-

щена належним чином, виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи [16]. Відомо, що багато комп'ютерних систем дозволяють перемикати мережевий адаптер в режим прослуховування адресованого іншим одержувачам мережевого трафіку в мережі, заснованій на передачі пакетів даних.

Нагадаємо основні види захисту мережевого трафіку:

– фізичний захист мережі;

– кінцеве шифрування;

– шифрування пакетів.

Поширені наступні способи передачі по мережі паролів:

– у відкритому вигляді;

– зашифрованими;

– у вигляді згорток;

– без безпосередньої передачі інформації про пароль ("з нульовим розголошуванням").

Перший спосіб застосовується і сьогодні в багатьох популярних додатках (наприклад, TELNET, FTP). У захищеній системі його можна застосовувати тільки у поєднанні із засобами захисту мережевого трафіку. При передачі паролів в зашифрованому вигляді або у вигляді згорток по мережі з відкритим фізичним доступом можлива реалізація наступних погроз безпеці парольної системи:

– перехоплення і повторне використання інформації;

– перехоплення і відновлення паролів;

– модифікація інформації, що передається, з метою введення в оману перевіряючої сторони;

– імітація зловмисником дій перевіряючої сторони для введення в оману користувача.

Схеми аутентифікації "з нульовим знанням" або "з нульовим розголошуванням" вперше з'явилися в середині 80-х – на початку 90-х років. Їх основна ідея полягає в тому, щоб забезпечити можливість одному з пари суб'єктів довести істинність деякого твердження другому, при цьому не повідомляючи йому ніякої інформації про зміст самого твердження. Наприклад, перший суб'єкт (що "доводить") може переконати другого ("перевіряючого"), що знає певний пароль, насправді не передаючи тому жодної інформації про сам пароль. Ця ідея і відбита в терміні "доказ з нульовим розголошуванням". Стосовно парольного захисту це означає, що якщо на місці перевіряючого суб'єкта виявляється зловмисник, він не отримує ніякої інформації про доказуване твердження і, зокрема, про пароль. Загальна схема процедури аутентифікації з нульовим розголошуванням складається з послідовності інформаційних обмінів (ітерацій) між двома учасниками процедури, по завершенню якої перевіряючий із заданою ймовірністю робить правильний висновок про істинність твердження, що перевіряється. Із збільшенням числа ітерацій зростає ймовірність правильного розпізнавання істинності (або помилковості) твердження.

Ще одним способом підвищення стійкості парольних систем, пов'язаної з передачею паролів по мережі, є застосування одноразових (one - time) паролів. Загальний підхід до застосування одноразових паролів заснований на послідовному використанні хеш-функції для розрахунку чергового одноразового пароля на основі попереднього. На початку користувач одержує впорядкований список одноразових паролів, останній з яких також зберігається в системі аутентифікації. При кожній реєстрації користувач вводить черговий пароль, а система розраховує його згортку і порівнює з еталоном, що зберігається у системі. У разі співпадіння користувач успішно проходить аутентифікацію, а введений ним пароль зберігається для використання як еталон при наступній реєстрації. Захист від мережевого перехоплення в такій схемі заснований на властивості необоротності хеш-функції. Найбільш відомі практичні реалізації схем з одноразовими паролями – це програмний пакет S/KEY. і розроблена на його основі система OPIE.

Апаратна (або електронна) ідентифікація

Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. До складу електронних систем ідентифікації і аутентифікації входять:

1). Переносні токени:

– асинхронні – користувач вводить рядок в пристрій, отримує відповідь і вводить її в комп'ютер;

– PIN/асинхронні – асинхронний метод доповнюється введенням PIN-кода в пристрій;

– синхронні – наприклад, токен синхронізований за часом з сервером і генерує для даного користувача в дану хвилину пароль, який вже і вводиться в систему;

– PIN/синхронні.

2). Різноманітні карти – це пристрої, схожі на переносні аутентифікатори, але складніші по своєму складу.

Карти бувають:

– пасивні (карти з пам'яттю);

– активні (інтелектуальні карти).

Останні включають CPU, мініатюрну операційну систему, годинник, програми на ROM (read-only memory – пам'ять тільки для читання), буферну пам'ять (RAM) для криптографічних розрахунків, незалежну пам'ять або EEPROM (Electrically Erasable Programmable Read-Only Memory) для зберігання цифрових ключів. За допомогою смарт-карти проводиться розрахунок одноразових паролів і здійснюється взаємодія з пристроєм через картридер. Після введення PIN-кода картридер сам запрошує смарт-карту, і подальший процес протікає без участі людини, завдяки чому можна використовува-

ти достатньо довгі ключі.

Карт досить багато, і працюють вони по різних принципах. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксіміті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти – аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д.

Що таке USB-ключ, розглянемо на прикладі eToken від компанії Aladdin Software.

eToken – персональний засіб аутентифікації і зберігання даних, що апаратно підтримує роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП). eToken може бути виконаний у вигляді USB-ключа або стандартної смарт-карти. eToken підтримує роботу і інтегрується зі всіма основними системами і додатками, що використовують технології смарт-карт або PKI (Public Key Infrastructure).

Основне призначення:

– двохфакторна аутентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);

– безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків і інше в незалежній пам'яті ключа;

– апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування ЕЦП).

eToken як засіб аутентифікації підтримується більшістю сучасних операційних систем, бізнес-додатків і продуктів по інформаційній безпеці.

Можливості застосування:

– сувора аутентифікація користувачів при доступі до серверів, баз даних, розділів Web-сайтів;

– безпечне зберігання секретної інформації: паролів, ключів шифрування, закритих ключів цифрових сертифікатів;

– захист електронної пошти (цифровий підпис і шифрування, доступ);

– системи електронної торгівлі, «клієнт-банк», «домашній банк»;

– захист комп'ютерів;

– захист мереж та каналів передачі даних за рахунок побудови VPN (virtual private network – віртуальні приватні мережі);

– клієнт-банк, home-банк.

eToken забезпечує:

– аутентифікацію користувачів за рахунок використання криптографічних методів;

– безпечне зберігання ключів шифрування і ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж і інформаційних ресурсів;

– мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері) за рахунок того, що ключі шифрування і ЕЦП генеруються ключем eToken апаратно і не можуть бути перехоплені;

– безпечне використання – скористатися ключем eToken може тільки його власник, що знає PIN-код ключа;

– реалізацію як західних та російських, так і вітчизняних стандартів на шифрування і ЕЦП;

– зручність роботи – ключ виконаний у вигляді брелока зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів, якими зараз оснащено 100% комп'ютерів, не вимагає спеціальних зчитувачів, блоків живлення, проводів і т.п.;

– використання одного ключа для вирішення безлічі різних завдань – входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП, безпечного доступу до захищених розділів Web-сайтів, інформаційних порталів і тому подібне.

Безконтактні смарт-карти розділяються на ідентифікатори Proximity і смарт-карти, що базуються на міжнародних стандартах ISO/IEC 15693 і ISO/IEC 14443. У основі більшості пристроїв на базі безконтактних смарт-карт лежить технологія радіочастотної ідентифікації.

Основними компонентами безконтактних пристроїв є чип і антена. Ідентифікатори можуть бути як активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64 розрядні серійні номери.

Системи ідентифікації на базі Proximity криптографічно не захищені, за винятком спеціальних рекомендованих систем.

USB-ключі працюють з USB-портом комп'ютера. Виготовляються у вигляді брелоків. Кожний ключ має 32/64 розрядний серійний номер.

USB-ключі, представлені на ринку:

- eToken R2, eToken Pro – компанія Aladdin Knowledge Systems;

– iKey10xx, iKey20xx,iKey 3000 – компанія Rainbow Technologies;

– ePass 1000 ePass 2000 – фірма Feitian Technologies;

– ruToken – розробка компанії «Актив» і фірми «АНКАД»;

– uaToken – компанія ТОВ «Технотрейд».

USB-ключі – це спадкоємці смарт-карт, через це структури USB-ключів і смарт-карт ідентичні.

Біометрична ідентифікація

Біометрична ідентифікація – це спосіб ідентифікації особи по окремих специфічних біометричних

ознаках, властивих конкретній людині [6]. 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.

Серед біометричних механізмів ідентифікації 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.

Серед статичних методів в задачах ідентифікації користувача комп'ютерних систем використовуються наступні:

1. Ідентифікація по відбитку пальця. В основу цього методу встановлена унікальність малюнка папілярних узорів на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитку, потім це зображення по складному алгоритму перетворюється на спеціальний цифровий код. Далі цей код порівнюється з еталонними кодами, які зберігаються в базі даних.

2. Ідентифікація по розташуванню вен на долоні. Прилад, який прочитує інформацію в цьому випадку, є інфрачервона камера. В 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.

3. Ідентифікація по сітківці ока. В даному випадку сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. Зрозуміло, що цей малюнок спостерігається тільки за певних умов: при скануванні людина дивиться на видалене світлове джерело і спеціальна камера сканує її очне дно, що в свою чергу може викликати неприємні відчуття у людини. Вважається одним з самих надійних біометричних методів.

4. Ідентифікація по райдужній оболонці ока. Малюнок райдужної оболонки ока – унікальний для кожної людини. В цьому методі важлива не тільки спеціальна камера, але і надійне програмне забезпечення. Адже саме за допомогою програмного забезпечення із зображення виділяється малюнок потрібної нам райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів.

5. Ідентифікація за формою кисті руки. Цей метод грунтується 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.

6. Ідентифікація за формою обличчя. На практиці використовується як двовимірне так і тривимірне зображення. Причому двовимірне розпізнавання обличчя на сьогоднішній день –один з самих неефективних методів біометрії, тому має обмежене коло застосування або використовується тільки в сукупності з іншими методами. Розпізнавання за тривимірним зображенням обличчя чимось схоже на метод ідентифікації за формою кисті руки. Тут так само будується тривимірний образ обличчя. Спеціальне програмне забезпечення виділяє з цього образу контури очей, губ і інших частин лиця. Далі проводяться точні вимірювання між заданими контурами. Саме за цими даними будується цифровий код.

Серед динамічних методів, які використовуються для ідентифікації особи користувача, можна назвати наступні:

1. Ідентифікація по голосу. В даний час існує безліч програм по розпізнаванню голосу. В методі ідентифікації по голосу важливі частотні характеристики голосу людини. Саме по частотних характеристиках і будується цифрова модель.

2. Ідентифікація по почерку. При ідентифікації за даним методом звичайно досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. На основі цих характеристиках і будується цифровий код.

3. Ідентифікація по клавіатурному почерку. Даний метод аналогічний ідентифікації по почерку, але замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується по динаміці набору певного слова або фрази.

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

На сьогоднішній день всі біометричні технології є імовірнісними і нерідко дана обставина служить основою для критики біометрії.

Важко не погодитися, що біометричні технології надійніші і зручніші за ті засоби захисту, які широко застосовувалися до теперішнього часу [5]. Але, незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня.

Комплексна (або багатофакторна) ідентифікація

Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку.

На сьогодні існують комбіновані системи наступних типів:

– системи на базі безконтактних смарт-карт і USB-ключів;

– системи на базі гібридних смарт-карт;

– біоелектронні системи.

1). Безконтактні смарт-карти і USB-ключі

У корпус брелока USB-ключа вбудовується антена і мікросхема для створення безконтактного інтерфейсу. Це дозволить організувати управління доступом в приміщення і до комп'ютера, використовуючи один ідентифікатор. Дана схема використовування ідентифікатора може виключити ситуацію, коли співробітник, покидаючи робоче місце, залишає USB-ключ в роз'ємі комп'ютера, що дозволить працювати під його ідентифікатором. У разі ж, коли не можна вийти з приміщення, не використовуючи безконтактний ідентифікатор, даної ситуації вдасться уникнути.

На сьогодні найбільш поширено два ідентифікатори подібного типу:

– RfiKey – компанія Rainbow Technologies;

– eToken PRO RM – компанія Aladdin Software Security R.D.

eToken RM – USB-ключі і смарт-карти eToken PRO, доповнені пасивними RFID-мітками.

RFID-технологія (Radio Frequency Identification, радіочастотна ідентифікація) є найпопулярнішою на сьогодні технологією безконтактної ідентифікації. Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом так званих RFID-міток, несучих ідентифікаційну і іншу інформацію.

З сімейства USB-ключів eToken RFID-міткою може бути доповнений тільки eToken PRO/32K.

2). Гібридні смарт-карти

Гібридні смарт-карти містять різнорідні чипи. Один чип підтримує контактний інтерфейс, інший – безконтактний. Як і у разі гібридних USB-ключів, гібридні смарт-карти вирішують дві задачі: доступ в приміщення і доступ до комп'ютера. Додатково на карту можна нанести логотип компанії, фотографію співробітника або магнітну смугу, що робить можливим повністю замінити звичайні пропуски і перейти до єдиного "електронного пропуску".

Смарт-карти подібного типу розробляють багато компаній: HID Corporation, Axalto, GemPlus, Indala, Aladdin Knowledge Systems і ін.

У Росії компанією Aladdin Software Security R.D. розроблена технологія виробництва гібридних смарт-карт eToken Pro/SC RM. В них мікросхеми з контактним інтерфейсом eToken Pro вбудовуються в безконтактні смарт-карти. Смарт-карти eToken PRO можуть бути доповнені пасивними RFID-мітками виробництва HID/ISOProx II, EM-Marine (частота 125 кГц), Cotag (частота 122/66 кГц), Ангстрем/КИБИ-002 (частота 13,56 Мгц), Mifare і інших компаній. Вибір варіанту комбінування визначає замовник.

3). 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.

Найчастіше як біометричні системи застосовуються системи розпізнавання відбитків пальців. При збігу відбитку з шаблоном дозволяється доступ. До недоліків такого способу ідентифікації можна віднести можливість використовування муляжу відбитку.

Досягти підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна за рахунок об'єднання використання біометричних характеристик разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PIN-код, використання різноманітних карт і т.д.) [11].

Актуальною бачиться проблема розробки 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 використання відбитків декількох пальців і т.д.) [12, 17]. Деякі виробники вже розпочали інтеграцію двох методів розпізнавання облич, включаючи дво- і тривимірні зображення.

Висновки

На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів інформаційних систем, можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту. Досить розповсюдженими в якості ідентифікаторів є також різноманітні електронні ключі (токени, карти і т.і.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних систем.

Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей 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 парольної аутентифікації.

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 літератури

1. Галатенко В.А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. академика РАН В.Б. Бетелина, 4-е изд. – М.: Интернет-Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.

2. Воронова В.А. Системы контроля и управления доступом / В.А. Воронова, В.А. Тихонов. – М.: «Горячая линия – Телеком», 2010. – 272 с.

3. Даклин Пол. Простые советы по более разумному выбору и использованию паролей / Пол Даклин. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml.

4. Безмалый В. Парольная защита: прошлое, настоящее, будущее / В. Безмалый // Журнал «КомпьютерПресс». – 2008. – №9. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.compress.ru/article.aspx?Id=20509&iid=901.

5. Голубев Г.А. Современное состояние и перспективы развития биометрических технологий / Г.А. Голубев, Б.А. Габриелян // Нейрокомпьютеры: разработка, применение. – 2004. – № 10. – С. 39-46.

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

7. Коновалов Д.Н. Технология защиты информации на основе идентификации голоса / Д.Н. Коновалов, А.Г. Бояров // [Електронний ресурс]. –Режим доступу до ресурсу: http://www.fact.ru/archive/07/voice.shtml.

8. Шарипов Р.Р. Идентификация и аутентификация пользователей по клавиатурному почерку / Р.Р. Шарипов // Электронное приборостроение: Научно практический сборник. – Казань: ЗАО «Новое знание», 2005. – Вып. 3(44).

9. Джхунян В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с.

10. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие / В.И. Завгородний. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.

11. Шрамко В.Н. Комбинированные системы идентификации и аутентификации / В.Н. Шрамко // PCWeek/RE. – 2004. – №45.

12. Десятчиков А.А. Синхронная биометрическая многофакторная идентификация / А.А. Десятчиков, А.Б. Мурынин, Ю.П. Тресков, В.Я. Чучупал // Труды ИСА РАН. Динамика неоднородных систем. – М.: УРСС. – 2005. – Вып. 9 (1). – С. 188-194.

13. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.

14. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Изд-во Юниор, 2003. – 504 с.

15. Романец Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

16. Конахович Г.Ф. Захист інформації в мережах передачі даних: підручник / Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.

17. Десятчиков А.А. Об объединении дистанционных биометрических методов распознавания человека / А.А. Десятчиков, В.В. Лобанцов, И.А. Матвеев, А.Б. Мурынин // Современный экстремизм в Российской Федерации: особенности проявления и средства противодействия: Материалы всероссийской научно-практической конференции в Академии Управления МВД России. – М.: Академия управления МВД РФ, 2006. – С. 374-379.

Надійшла до редколегії 30.05.2013

Рецензент: д-р фіз.-мат. наук, проф. М.Г. Любарський, Національний університет «Юридична академія України імені Ярослава Мудрого», Харків.

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННО- КОМПЬЮТЕРНЫХ СИСТЕМ: АНАЛИЗ И ПРОГНОЗИРОВАНИЕ ПОДХОДОВ

Н.А. Кошевая, Н.И. Мазниченко

Статья посвящена обзору и анализу современных подходов, которые используются сегодня для идентификации пользователей компьютерных систем. Это в особенности важно в связи с актуальностью проблемы защиты компьютерной информации и ограничению доступа к информационным и техническим ресурсам компьютера. Результаты выполненных исследований и сформулированные выводы могут быть полезные при создании собственных систем защиты компьютерной информации отдельными пользователями.

***Ключевые слова:** защита компьютерной информации, идентификация пользователей ЭВМ.*

AUTHENTICATION OF USERS OF THE INFORMATIVE COMPUTER SYSTEMS: ANALYSIS AND PROGNOSTICATION OF APPROACHES

N.A. Koshevaya, N.I. Maznichenko

The article is devoted to the review and analysis of modern approaches which are used today for authentication of users of the computer systems. This is important especially in communication with actuality of problem of defence of computer information and access restriction to the informative and technical resources of cjmputer. The results of the implemented researches and done conclusions can be useful at creation of the own systems of protection of computer information by separate users.

***Keywords:** protection of computer information, computer user identification.*