УДК 004.042

І. В. Калініна, О. І. Лісовиченко©

СИСТЕМИ АВТОРИЗАЦІЇ З ВИКОРИСТАННЯМ РІЗНИХ МЕТОДІВ АУТЕНТИФІКАЦІЇ

Анотація: У роботі розглянуто сучасні методи аутентифікації на базі визначених показників. Проведено порівняльний аналіз переваг і недоліків методів аутентифікації користувачів для підвищення безпеки доступу і простоти користування до систем авторизації.

Ключові слова: системи авторизації; методи аутентифікації; безпека доступу до систем авторизації біометрична ідентифікація; паролі; PIN-коди; карти; токери; комбіновані методи.

Вступ

Кожний користувач сучасних технологій декілька разів на день стикається з системами авторизації.

Авторизація – керування рівнями та засобами доступу до певного захищеного ресурсу, як в фізичному розумінні, так і в галузі цифрових технологій та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних.

Посвідчення, паспорти, бейджі, підписи, паролі, PIN-коди необхідні нам для авторизації при вході в будинок, перетині кордону, отриманні грошей в банку чи, автоматично, в банкоматі тощо.

Важливе значення для систем авторизації є забезпечення безпеки доступу.

Щоб авторизуватись в систему необхідно пройти перевірку відповідності імені входу і пароля – аутентифікацію.

Існує декілька методів аутентифікації (рис. 1), які різняться своєю складністю, надійністю, вартістю та іншими показниками. Кожний з цих методів має свої позитивні та негативні сторони, аналізу яких присвячена ця робота.

Постановка задачі

Провести аналіз методів аутентифікації на базі визначених показників для підвищення безпеки доступу і простоти користування до систем авторизації.

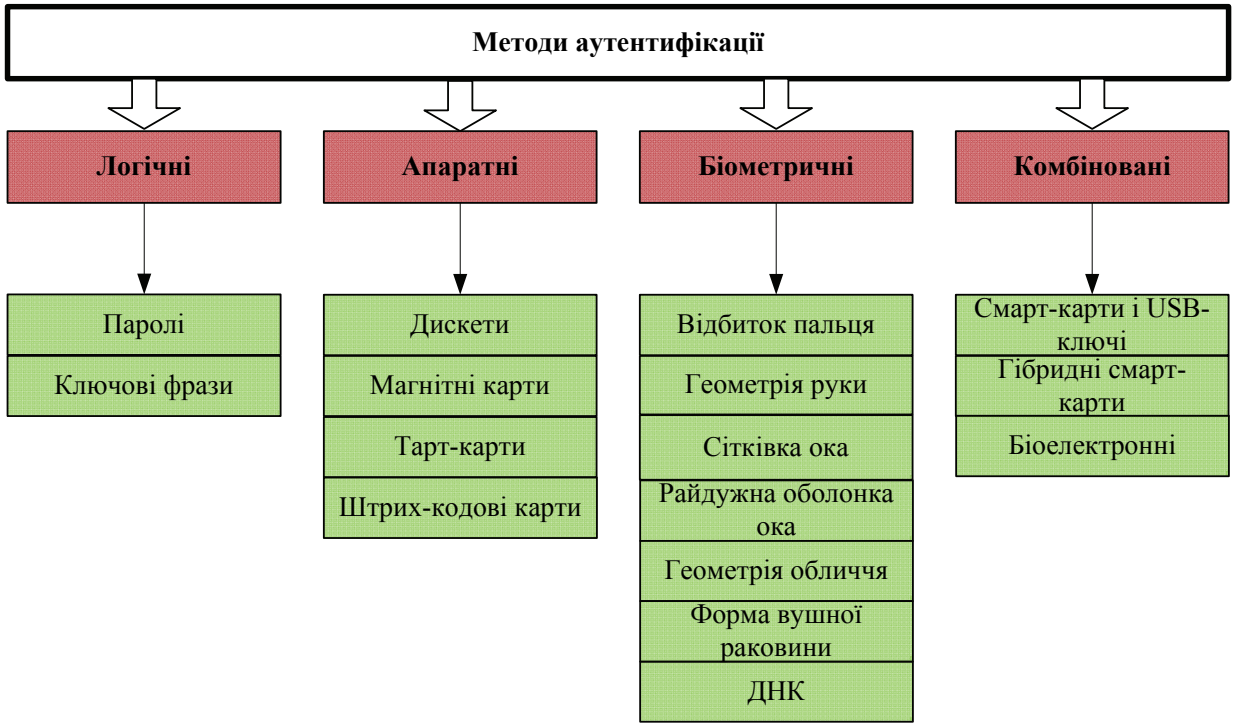

Рис. 1. Методи аутентифікації

Аналіз методів

Система аутентифікації є одним з ключових елементів інфраструктури захисту безпеки доступу до будь-якої системи авторизації.

Для аналізу методів аутентифікації основними показниками будуть:

1) Стійкість до перебору.

2) Захищеність від підглядання.

3) Захищеність у разі викрадання матеріальних носіїв, на яких зберігається аутентифікатор.

4) Простота запам’ятовування аутентифікатора.

5) Простота процедури аутентифікації.

6) Завадозахищеність системи аутентифікації (рівень похибок першого та другого роду).

7) Стійкість до дій зовнішніх факторів: температура, освітлення, механічне пошкодження.

Як вже зазначалося, методи аутентифікації діляться на наступні групи: логічні, апаратні, біометричні і комбіновані. Спробуємо проаналізувати їх за вище наведеними показники.

Логічні методи аутентифікації

Яким би складним не був пароль, існує дві можливості його зламу (не враховуючи варіанти підглядування та викрадення з матеріальних

носіїв): шляхом автоматичного підбору всіх можливих комбінацій знаків і використання програмної закладки («троянський кінь», «руткіт»), яка викрадає пароль із спеціальної області операційної системи.

Для боротьби із системами автоматичного підбору необхідно збільшувати кількість можливих комбінацій знаків, що призведе до збільшення необхідного часу для виконання операцій перебору всіх можливих варіантів. За цей час інформація застаріє і буде неактуальною або буде змінений пароль, і всю процедуру необхідно буде розпочати знову.

Мірою стійкості паролів традиційно є ентропія міра невизначеності, вимірювана звичайно в бітах. Ентропія в N біт відповідає невизначеності вибору з 2^8 паролів. У разі використання випадковихпаролів (наприклад, випадкових чисел, що згенеровані за допомогою генератора) ентропія обчислюється досить просто: вона залежить від кількості можливих паролів для заданих параметрів. Так, для випадкового пароля завдовжки N символів, складеного з алфавіту, що містить M букв, ентропія буде рівна:

$$E = log_2 M^8.$$

Виникнення помилок першого та другого родів при використанні парольної системи аутентифікації можливе лише у випадках порушення правильної роботи системи аутентифікації і призводить, в першому випадку, до обмеження користувача в правах доступу до певних ресурсів (на доступ до яких він має право), а у другому до надання суб'єкту прав доступу до певних ресурсів (на що він прав не має).

Іншим недоліком системи парольної аутентифікації є те, що пароль, насправді, дозволяє аутентифікувати не конкретний суб'єкт, а лише зафіксувати відповідність аутентифікатора суб'єкта його ідентифікатору, тобто пароль може беззастережно використовувати будь-який суб'єкт, незважаючи на те, яким чином він його отримав.

Апаратні методи аутентифікації

Цей метод аутентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі (токени).

Токени, як правило, захищаються PIN-кодом і максимально

спрощують процедуру введення та зміни аутентифікатора.

Перевагою систем аутентифікації на основі токенів є відсутність необхідності запам’ятовування аутентифікатора (окрім, можливо, нескладного PIN-коду). Це дозволяє використовувати достатньо довгі ключі, а за необхідності, надає можливість реалізувати процедуру зміни ключа при кожному вході в систему, мережу тощо. Також виключається можливість підглядання інформації, яка використовується для аутентифікації.

При зазначених перевагах ця система аутентифікації має певні недоліки:

– токен можна загубити або його можуть вкрасти (від негативних наслідків в цьому випадку захищає PIN-код та алгоритми блокування або стирання інформації після фіксованого числа невірних спроб введення PIN-коду);

– окремі токени не захищені від копіювання аутентифікатора безпосередньо з носія інформації з використанням спеціальних засобів, або ж шляхом механічного зламування токена;

– з використанням спеціальної апаратури можливий підбір (перебір) можливих значень аутентифікатора безпосередньо на терміналі системи аутентифікації;

– використання токенів у більшості випадків вимагає наявності додаткового обладнання на терміналах аутентифікації для системи авторизації.

Виникнення помилок першого та другого роду при використанні токенів можливе лише у випадках порушення правильної роботи системи аутентифікації.

Надійність роботи токенів залежить від особливостей їх реалізації: наявність спеціальних вологозахисних, пилозахисних, ударостійких оболонок значно подовжує термін роботи токенів.

Контактні токени, особливо смарт-карти та токени з USB-інтерфейсом, менш довговічні.

Біометричні методи аутентифікації

Біометричні системи в наш час являють собою друге покоління систем безпеки, оскільки саме біометрія використовує вимірювання індивідуальних параметрів людини для її ідентифікації.

Сама процедура біометричної аутентифікації відносно проста (наприклад, прикласти палець чи руку, підставити під камеру, або

пристрій для сканування обличчя або око) і не потребує будь-якого фізичного або психологічного напруження; немає потреби щось запам'ятовувати, періодично змінювати, або приховувати, чи постійно щось із собою носити.

З урахуванням того, що в біометричних системах інформація, яка використовується для аутентифікації, незмінна, виникає можливість підміни біометричних параметрів (наприклад, виготовлення та використання силіконового пальця для дактилоскопічної системи). Але ця процедура теж має певну вартість, яка може співвідноситись із вартістю самої системи аутентифікації, і тому має сенс лише у випадку, коли вартість інформації, що захищається, суттєво вища вартості спуфінга. Зі спуфінгом можливо боротися із застосуванням спеціальних технологій, наприклад, технології «живого пальця».

Збереження біометричних параметрів суб'єкта порівняно з паролями та магнітними картами досить велика, але системи біометричноїаутентифікації не захищені від випадків суттєвої зміни біометричних параметрів – пошкодження пальців, рук і інших частин тіла, які використовуються при аутентифікації.

Важливий недолік біометричних систем аутентифікації – неможливість одночасного зменшення рівня помилок першого та другого роду. Якість вирішення цієї проблеми пропорційна вартості систем.

Комбінована (або багатофакторна) аутентифкація

На сьогодні існують комбіновані системи наступних типів:

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

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, зали- шає 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.

– *системи на базі гібридних смарт-карт;*

Гібридні смарт-карти містять різнорідні чипи. Один чип підтримує контактний інтерфейс, інший – безконтактний. Як і у разі гібридних

 ISSN 1560-8956

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".

– *біоелектронні системи.*

Для 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 безпеки авторизації систем можна за рахунок об'єднання використання біометричних характеристик разом з класичними способами ідентифікації користувачів – відбиток пальця + смарт-карта; відбиток пальця + USB-ключі. В основі комбінованих методів аутентифікації є метод відбитку пальця, так як найбільш вивчений метод розпізнавання, простий та зручний для сканування, найнижча ціна серед біометричних систем ідентифікації.

Порівняльну характеристику методів аутентифікації для систем авторизації можна представити таблицею 1.

Таблиця 1

Порівняльна характеристика методів аутентифікації

Методи / Критерій	Логічні	Ідентифікаційні	Біометричні	Комбіновані
Стійкість до перебору	□	□	+	+
Захищеність від підглядання	□	+	+	+
Захищеність у разі викрадання матеріальних носіїв	□	□	+	+
Простота запам'ятовування аутентифікатора	+	+	+	+
Простота процедури аутентифікації	+	+	+	+
Завадозахищеність системи аутентифікації	□	+	□	+
Стійкість до дій зовнішніх факторів	+	□	+□	+

Зробивши порівняльний аналіз на базі визначених критеріїв можна дійти висновку, що парольний захист на сьогодні є одним із найпоширеніших способів безпеки доступу до інформації 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 може забезпечити серйозного захисту. Досить розповсюдженими в якості аутентифікації використовуються також різноманітні електронні ключі (токени, карти і т.і.). Але слід зауважити, що останнім часом все більшого поширення набувають системи аутентифікації, які використовують біометричні характеристики людини і які мають безліч переваг – зручність, простота використання, мінімальні затрати часу на проведення операції авторизації, але присутній важливий недолік – завадозахищеність системи аутентифікації, тобто виникнення одночасно помилок першого і другого роду, а також спуфінг-загроз. Тому, щоб уникнути цих недоліків і збільшити захист доступу до систем авторизації необхідно використовувати комбіновані методи аутентифікації.

Щодо вибору системи аутентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, і вартості програмно-апаратного забезпечення аутентифікації, яке обираєте; оцінити зручність у використанні (контактні, безконтактні), а також визначити потрібний рівень захищеності.

Висновки

Розглянуто сучасні методи аутентифікації, зроблено порівняльний аналіз методів аутентифікації (переваги та недоліки) на базі визначених показників.

Таким чином, на основі проведеного аналізу технології логічної, апаратної, біометричної та комбінованої аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш затребуваним буде саме вживання систем комплексної (одночасне використання двох і більше методів) аутентифікації для систем авторизації. Підвищення безпеки доступу систем авторизації досягається використанням біоелектронних систем, що дозволить одночасно зменшити помилок першого і другого роду та спуфінг-загроз.

Для простоти користування до систем авторизації є метод відбитку пальця: відбиток пальця + смарт-карта; відбиток пальця + USB-ключі,

так як метод відбитку пальця найбільш вивчений метод розпізнавання, простий та зручний для сканування, найнижча ціна серед біометричних систем ідентифікації.

Список використаних джерел

1. Застосування біометричних систем для ідентифікації особи / Х. А. Лисенко, О. С. Мельник // Юридичні науки 2004. Вип. 60/62. – С. 88-91. - ISSN 1728

2. Чайковський Я. І. Платіжні системи: нав. посібник / Я. І. Чайковський. – Тернопіль: Карт-бланш, 2006. – 62 с.

3. Ідентифікація користувачів інформаційно-комп’ютерних систем: аналізі прогнозування підходів: інфокомунікаційні системи: наук.-техн. зб. / Н. А. Кошева, Н . І. Мазниченко – 2013. Вип. 6(113). – С. 215-223.

4. Малков А. Классификация механизмов аутентификации пользователей и их обзор / А. Малков // Информационная безопасность. – Режим доступу: https://habrahabr.ru/post/177551/

5. Попиріна О. Методи аутентифікації / О. Попиріна // Ідентифікація та аутентифікація – Режим доступу : https://sites.google.com/ /site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie

6. О цифровой идентификации личности : сб. науч. трудов. НАКУ / Д. В. Ландэ, В. Н. Фурашев – 2007. – Вип. 34. – С. 127-135.

7. Кличенко Я. Ідентифікація на основі біометричних даних / Я. Кличенко // Економічні науки. Режим доступу : http://nauka.kushnir.mk.ua/?p=16437