УДК 007.5

А. О. Азарова
Ю. О. Мисько
Д. С. Сембрат

РОЗРОБКА ПРОГРАМНИХ МОДУЛІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ВІДБИТКАМИ ПАЛЬЦІВ ЧЕРЕЗ СМАРТФОН З ПОДАЛЬШОЮ АВТОРИЗАЦІЄЮ

Вінницький національний технічний університет

Анотація. В статті розглянуто сучасні методи біометричної ідентифікації користувачів комп'ютерних систем, призначені для забезпечення захисту конфіденційної інформації. Встановлено недоліки та переваги кожного методу, наведено показники якості ідентифікації та обґрунтовано перспективні напрями досліджень. Для захисту інформаційних комп'ютерних систем від небажаного доступу з боку неавторизованих користувачів у роботі запропоновано систему контролю та управління доступом, в якій його розмежування досягається шляхом ідентифікації користувача за відбитками пальців через смартфон.

Ключові слова: ідентифікація користувача, парольна ідентифікація, апаратна ідентифікація, біометрична ідентифікація, багатофакторна ідентифікація, відбитки пальців.

Development of software user identification modules for fingerprints through a smartphone with subsequent authorization

Abstract. The article considers modern methods of biometric identification of users of computer systems intended to provide protection of confidential information. The disadvantages and advantages of each method are set, identification of quality indicators is presented and perspective directions of research are substantiated. In order to protect computer information systems from unwanted access from unauthorized users, an access control and access control system is proposed in which its differentiation is achieved by identifying the user with fingerprints through a smartphone.

Keywords: user identification, password identification, hardware identification, biometric identification, multi-factor identification, fingerprints.

Вступ

Із появою та розвитком нових інформаційних технологій виникла проблема інформаційної безпеки, пов'язана із потребою безпечного збереження і конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Вирішенню цих проблем приділяється все більша увага, удосконалюються існуючі методи захисту інформаційних систем, постійно розробляються нові методи, які дозволяють збільшувати надійність і стійкість систем, призначених для вирішення такого роду задач.

Задача інформаційної безпеки набуває ще більшої значущості у зв'язку зі зростанням злочинності в сфері використання комп'ютерної інформації.

Доступ користувачів до різних класів інформації повинен визначатися ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача. Останнім часом все більше набувають популярності системи на основі біометричних методів розмежування та контролю доступу. Сформувався специфічний ринок біометричних пристроїв і відповідних програмних продуктів, оскільки вони дозволять вирішувати важливі завдання в області інформаційної безпеки.

Необхідність ідентифікації особистості людини зумовлена активною інформатизацією сучасного суспільства та збільшенням потоків конфіденційної інформації. Аналіз сучасних систем контролю доступу свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

Матеріал і методи дослідження

Порівняно з технологіями розпізнавання за сітківкою і райдужною оболонкою ока, сканування відбитків пальців є дешевшим і зручнішим; порівняно з технологіями розпізнавання за рукописним і клавіатурним почерком, технології ідентифікації за відбитками пальців на кілька порядків кращі за статистичними показниками помилок першого і другого роду; порівняно з технологіями розпізнавання за «геометрією» обличчя — відбитки пальців не змінюються, отже це не погіршує статистичну надійність методу, крім того геометричний метод потребує дуже дорогого обладнання, а також зміна міміки обличчя і перешкоди на ньому погіршують статистичну надійність методу.

Отже, дослідження у напрямку захисту інформації шляхом ідентифікації відбитків пальців через смартфон є актуальним.

Дослідження, проведене в роботі, здійснювалося в межах секційного наукового напрямку кафедри МБІС — «Системи забезпечення захисту інформації в комунікаційних процесах».

Об’єкт дослідження — процес захисту інформації шляхом обмеження доступу в комп’ютерних системах.

Предмет дослідження — метод ідентифікації користувача через смартфон із подальшою авторизацією.

Метою дослідження є покращення ефективності захисту конфіденційних даних від несанкціонованих дій шляхом розмежування доступу за допомогою ідентифікації користувачів за відбитками пальців.

Наукова новизна результатів дослідження полягає у вдосконаленні методу автентифікації користувачів шляхом використання маскувальних елементів біометричних даних за відбитками пальців, який, на відміну від існуючих підходів, розширює функціональні можливості засобів автентифікації, що уможливлює підвищення ефективності системи захисту.

Практичне значення результатів дослідження полягає у розробленні програмного модулю ідентифікації користувача через смартфон із подальшою авторизацією. Усі запропоновані в роботі шляхи до вирішення поставлених задач розроблено автором самостійно.

Результати дослідження

Ідентифікація — процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Ідентифікація дозволяє суб'єкту (користувачу, процесу, чинним від імені визначеного користувача, чи іншого апаратно-програмного компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона пересвідчується, що суб'єкт дійсно той, за кого він себе видає.

Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу до будь-якої інформаційної системи.

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 кілька способів ідентифікації користувачів (рис. 1).

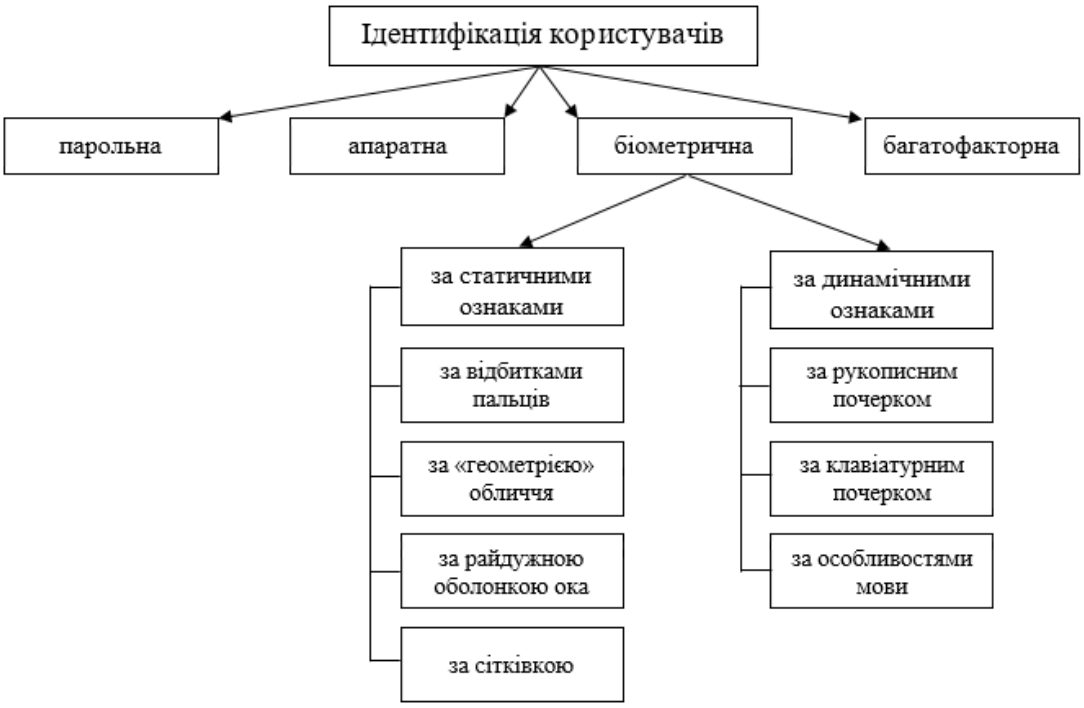

Рисунок 1 — Схематичне зображення способів ідентифікації користувачів

У даний час існують три основні підходи до ідентифікації користувачів інформаційних систем:

1) користувачу відоме щось, що він може повідомити системі і що дозволяє однозначно його ідентифікувати (наприклад, пароль, PIN-код, ключ і т.п.);

2) користувач може виконати деяку унікальну процедуру (наприклад, використати всілякі карти, магнітні брелоки і т.п.);

3) вимірювання і використовування унікальних характеристик користувача (біометричних).

З усього розмаїття БТ для рішення задач інформаційної безпеки найбільш оптимальним є використання систем побудованих на скануванні та розпізнанні відбитків пальців. Порівняльні переваги даного виду біометричної аутентифікації є наступними:

- у порівнянні з технологіями розпізнавання за сітківкою і райдужною оболонкою ока — сканування відбитків пальців є дешевшим і зручнішим, тому що для входу в різні програмні системи і виконання в них критичних операцій, що вимагають строгої ідентифікації користувача, простіше кілька разів прикласти палець до сканера, ніж декілька разів правильно приставляти око до камери;

- у порівнянні з технологіями розпізнавання за формою та розташуванням вен на лицьовій стороні долоні — сканери відбитків пальців на порядок менш громіздкі і процес безпосереднього зчитування ідентифікуючих ознак також зручніший;

- у порівнянні з технологіями розпізнання за формою і термограмою обличчя — усі що перераховано вище, тобто незручність використання в повсякденних діях і громіздкість устаткування;

- у порівнянні з технологіями розпізнання по рукописному і клавіатурному почерку — у технології ідентифікації за відбитками пальців на кілька порядків кращі статистичні показники помилок першого і другого роду, це ж відноситься і до систем розпізнавання за голосом.

Сканер відбитків пальців — це тип біометричної технології безпеки, яка використовує комбінацію апаратних і програмних методів для розпізнавання за відбитками пальців. Він ідентифікує та перевіряє справжність відбитків пальців людини, щоб дозволити або заборонити

доступ до смартфону, додаткам і іншим місцям, які потребують захисту від небажаного втручання. Чому саме сканер відбитків? Все просто: плати для сканування відбитків досить дешеві та прості як у виготовленні, так і у використанні. Доторкнувся до сканера і твій смартфон миттєво розблокований і готовий до роботи.

Ідентифікація за відбитками пальців — на сьогодні найпоширеніша БТ. За даними International Biometric Group, частка систем розпізнавання за відбитками пальців складає 48% від усіх використовуваних у світі БС.

Як і у всіх біометричних методах, процес ідентифікації особи за відбитком пальця поділяється на два ключових етапи: реєстрацію і розпізнавання (ідентифікацію/аутентифікацію).

При реєстрації можна виділити три фази: введення зображення малюнка ПЛ; виділення індивідуальних елементарних деталей малюнка і формування (обчислення) образу малюнка (шаблона, ідентифікаційної формули); збереження зразка.

В даний час у пристроях ідентифікації на базі методу розпізнавання за відбитком пальця використовується програмне забезпечення, що дозволяє проводити аналіз лише елементарних деталей малюнка ПЛ, а не розташування пор на шкірі пальців. У специфікаціях IAFIS вказується також роздільна здатність для кожного пікселя зображення, яка повинна складати вісім біт на піксель, що дозволяє одержати 256 градацій яскравості.

В даний час на ринку існує кілька типів сканерів. Всі вони працюють за одним і тим же принципом: сканер зчитує відбиток власника смартфона і при спробі розблокувати його, порівнює «малюнок» з тим, який запрограмований заздалегідь в пристрої. Якщо відбиток пальця збігається, пристрій буде розблоковано. В іншому випадку з'явиться повідомлення про помилку.

Сканери не аналізують весь малюнок відбитка пальця. Перевіряються лише деякі з характерних рис або візерунків. Це, наприклад, розгалуження, роздвоєння або обривання відбитків пальців. Вони перетворять картинку в Templ (шаблон), і за алгоритмом порівнюють відстань між кривими і лініями. Це дозволяє зробити процес перевірки набагато коротшим, ніж якщо б вам потрібно було проаналізувати весь відбиток пальця.

Дані зберігаються в спеціальній області, що перешкоджає вилучення відбитків з бази.

Сканер відбитку пальців в Android-пристроях — річ вже не нова. Але функціональність сканерів на той час обмежувалася тільки можливістю розблокування смартфона. І оскільки раніше Android офіційно не підтримував роботу зі сканерами, виробникам доводилося писати свої «милиці». Але після того, як Google представили Android 6.0 Marshmallow, одним з важливих нововведень якого як раз стала якраз нативна підтримка сканерів відбитка і Fingerprint API, розробники нарешті отримали можливість скористатися наявними можливостями сканера в своїх додатках.

Прихід сканерів відбитків пальців на пристроях Android надає додаткам альтернативу традиційним методом аутентифікації користувача. Використання відбитків пальців для аутентифікації користувача дозволяє додатку включити захист, який менш нав'язливий, ніж ім'я користувача і пароль.

Обговорення отриманих результатів

Для використання програмного продукту було розроблено інструкцію користувача.

Розглянемо як відбувається налаштування вбудованого у смартфон сканеру відбитків пальців на прикладі Xiaomi Redmi Note 4x.

1) Зайшовши в меню «Налаштування» необхідно зі списку «Система та пристрій» вибрати вкладку «Екран блокування та пароль».

2) Далі натискаємо на вкладку «Керувати відбитками пальців».

3) У новому відкритому меню звертаємо увагу на самий нижній пункт у вікні — «Додати відбиток пальця» (система також пропонує задати пароль на той випадок, якщо поставлений відбиток на сканері не спрацює або пристрій частково вийде з ладу).

Але варто зазначити, що даний смартфон зберігає лише до 5 відбитків пальців. Якщо виникла необхідність додати інший відбиток, то потрібно звільнити для нього місце, видаливши один із вже існуючих.

4) На екрані смартфону з'являється повідомлення із подальшими вказівками для користувача.

5) Багатократно прикладаємо будь-який палець (один і той самий) до поверхні сканеру вашого смартфону. Про успішність кожного етапу сканування вам повідомить анімація з заповненням кружка та легка вібрація пристрою. Ці дії потрібно повторювати до тих пір, поки не заповняться усі пусті лінії в кружку.

6) Якщо все зроблено правильно — ви отримуєте сповіщення про успішне налаштування. Після чого, ваш пристрій готовий до подальшої роботи.

Рисунок 2 — Схематичне зображення налаштування відбитків пальців у смартфоні

7) Наступним кроком буде встановлення додатку для ідентифікації користувачів за відбитками пальців на смартфон.

8) Головне вікно перевіряє чи користувач авторизований. Якщо ні — відкриває вікно для першого входу в додаток, у якому потрібно ввести логін та пароль свого облікового запису, а також IP-адресу серверу до якого підключено комп'ютер.

9) Далі, якщо користувача було авторизовано, відкривається діалог зчитування пальця. При 5 невірних спробах, відбувається вихід із профілю, стираються усі дані і потрібно буде повторити крок 8.

10) Якщо авторизація пройшла успішно, а відбиток пальця розпізнано, користувачеві надається доступ до вікна, у якому за допомогою відбитку пальця відбувається його ідентифікація та подальша авторизація.

11) Якщо необхідно вийти з облікового запису, достатньо лише натиснути відповідний значок.

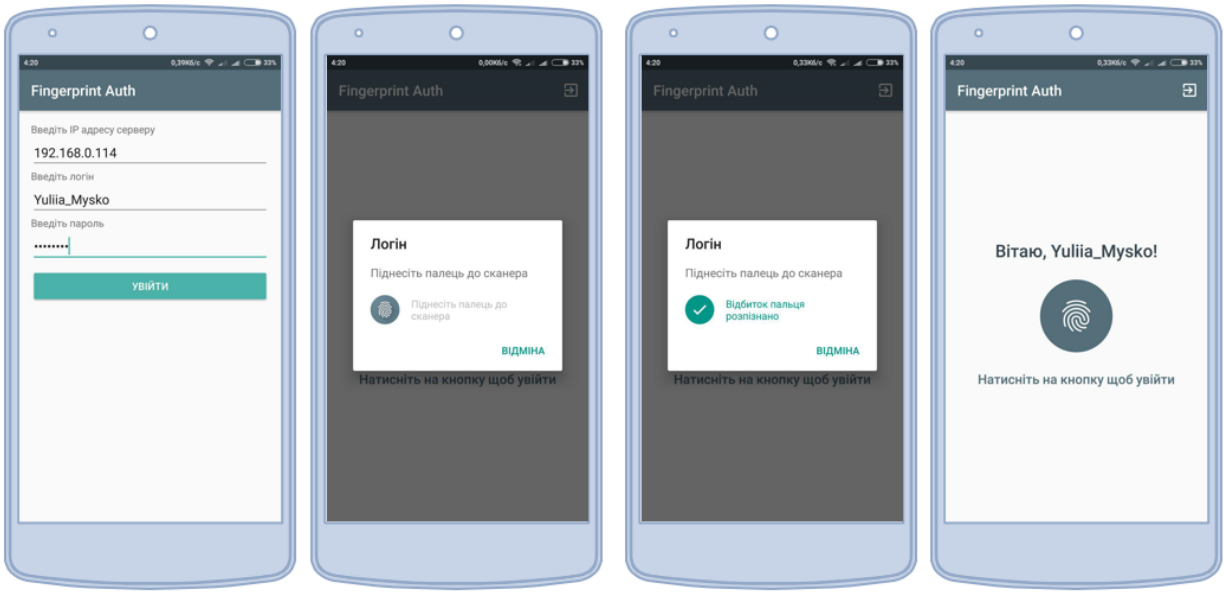

Рисунок 3 — Вигляд програмного модулю

Висновки

Переваги біометричних систем ідентифікації користувачів — незаперечні. Швидкість обробки даних, постійність авторизаційної інформації в поєднанні з доступною ціною, все це беззаперечно повинно схилити підприємців до впровадження біометричних систем ідентифікації. Використання біометричних засобів спрощує процедуру ідентифікації особи, а також підвищує надійність систем безпеки. Для підтвердження особи при використанні мобільного телефону, планшета або ноутбука найбільш підходящою ІТ є біометрія за відбитками пальців. Проаналізувавши переваги та недоліки методу ідентифікації та алгоритм захисту інформації в комп'ютерних мережах на основі біометричних даних з використанням відбитків пальців акцентовано, що захист комп'ютерних мереж необхідно виконувати на основі системного підходу, забезпечуючи необхідний рівень захищеності на всіх рівнях. У результаті дослідження було обґрунтовано біометричний метод за відбитками пальців як оптимальний підхід для захисту інформації в комп'ютерних мережах через смартфон. Отже, було розроблено програмний модуль ідентифікації користувача за відбитками пальців через смартфон та інструкцію користувача до нього.

Список використаної літератури

1. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы развития биометрических технологий // Нейрокомпьютеры. Разработка. Применение. № 10, 2004, – С. 39 – 46. 3. Беленков В. Д. Электронные системы идентификации подписей // Защита информации. Конфидент. 1997, № 6, – С.39 – 42.

2. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений – Пенза: Издательство Пензенского государственного университета, 2000, С. 188.

3. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека [Текст] / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.

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

Мисько Юлія Олегівна, ст. гр. УБ-14б, факультету Менеджменту та інформаційної безпеки Вінницького національного технічного університету, м. Вінниця, e-mail: yuliia.mysko@gmail.com.

Сембрат Дем'ян Сергійович, ст. гр. 2АВ-14б, факультету Комп'ютерних систем та автоматики Вінницького національного технічного університету, м. Вінниця, e-mail: sdsvin@gmail.com.

Науковий керівник: ***Азарова Анжеліка Олексіївна —*** кандидат технічних наук, професор кафедри МБІС, заступник декана ФМІБ з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету.

Mysko Yuliia, UB-14b group, Management and information security faculty of Vinnytsia National Technical University, Vinnytsia, email: yuliia.mysko@gmail.com;

Sembrat Demian, 2AV-14b group, Computer systems and automation faculty of Vinnytsia national technical university, Vinnytsia, mail: sdsvin@gmail.com.

Supervisor: **Azarova Anzhelika O.** - PhD, Professor of the Department of MBIS, Deputy Dean of the Faculty of Management and Information Security on Scientific Work and International Cooperation of Vinnytsia National Technical University.