Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____

(повна назва)

Кафедра _____Безпеки інформаційних технологій____

(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти _____другий(магістерський)_____

Методи двофакторної автентифікації користувачів в мобільних пристроях

Виконав:

студент __6___ курсу, групи БДІРм-20-1

Білан Леся Олексіївна_____

(прізвище, ініціали)

Спеціальність ___125 Кібербезпека _____

(код і повна назва спеціальності)

Освітня програма «Безпека державних інформаційних ресурсів»

(повна назва освітньої програми)

Керівник _доц. Сєвєрінов О.В._____

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З.__

(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління _____

Кафедра_____Безпеки інформаційних технологій _____

Рівень вищої освіти_____другий(магістерський)_____

Спеціальність_____125 Кібербезпека _____
(код і повна назва)

Освітня програма_____«Безпека державних інформаційних ресурсів»___
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові_Білан Лесі Олексіївні_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Методи двофакторної автентифікації користувачів в мобільних пристроях_____
_____
затверджена наказом по університету від __8__ листопада__2021 р. 1684_Ст_____
2. Термін подання студентом роботи до екзаменаційної комісії ____ _____ 20__ р.
3. Вихідні дані до роботи Методи двофакторної автентифікації

4. Перелік питань, що потрібно опрацювати в роботі
   - Автентифікація
   - Методи автентифікації в мобільних пристроях
   - Двофакторна автентифікація

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
_презентаційний матеріал у вигляді слайдів_____
_____

6. КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів теми кваліфікаційної роботи	Строки виконання етапів роботи	Примітка
1	Вибір здобувачем теми кваліфікаційної роботи	01.09.2021	Виконано
2	Затвердження плану і завдання кваліфікаційної роботи	08.09.2021	Виконано
3	Оформлення пояснювальної записки кваліфікаційної роботи	08.09.2021 – 05.12.2021	Виконано
4	Здача роботи керівнику	05.12.2021	Виконано
5	Підпис кваліфікаційної роботи у керівника	10.12.2021	Виконано
6	Перевірка та підпис кваліфікаційної роботи у нормоконтролера	14.12.2021	Виконано
7	Проходження перевірки на оригінальність кваліфікаційної роботи	14.12.2021	Виконано
8	Допуск завідувачем кафедри до захисту	15.12.2021	Виконано
9	Захист кваліфікаційної роботи	16.12.2021	Виконано

Дата видачі завдання 01 вересня 2021 р.

Студент _____
(підпис)

Керівник роботи _____ ___доц. Сєвєрінов О.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 72 с., 8 табл., 18 джерел.

АВТЕНТИФІКАЦІЯ, ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ, ПАРОЛЬНА АВТЕНТИФІКАЦІЯ

Об’єкт дослідження − автентифікація користувачів в мобільних пристроях.

Предмет дослідження – забезпечення двофакторної автентифікації в мобільних пристроях.

Мета роботи – забезпечення автентифікації користуваців за рахунок використання адаптивного багатофакторного методу автентифікації.

Методи досліджень базуються на використанні криптографії, криптоаналізу, методів організації та проведення наукових досліджень, апробованих рекомендацій та стандартів, що знайшли визнання та застосування на міжнародному та регіональному рівнях.

Кваліфікаційна робота присвячена дослідженню та аналізу методів автентифікації користувачів, та дослідженню використання технології двофакторної автентифікації.

ABSTRACT

Qualification work: 72 pages, 8 tables, 18 sources.

AUTHENTICATION, TWO-FACTOR AUTHENTICATION, BIOMETRIC AUTHENTICATION, PASSWORD AUTHENTICATION

The object of research is the study of two-factor authentication methods.

The subject of research is the two-factor authentication service in mobile devices.

The aim of the work is to investigate the existing methods of two-factor authentication, methods of authentication using these methods and identify their advantages and disadvantages.

Research methods are based on the use of cryptography, cryptanalysis, methods of organizing and conducting research, proven recommendations and standards that have found recognition and application at the international and regional levels.

Qualification work is devoted to the study and analysis of methods of user authentication, and research on the use of two-factor authentication technology.

ЗМІСТ

ВСТУП

Автентифікація - це процедура, яка дозволяє здійснити перевірку справжності зазначених користувачем даних. Після успішного проходження автентифікації користувачеві надається доступ до закритої інформації на інтернет-ресурсі.

Сучасні системи автентифікації базуються на пред’явленні користувачем статичної пари ідентифікатор/пароль. Однак такі пари можуть бути скомпрометовані через халатність користувачів або можливості підбору паролів зловмисником.

У сучасних інформаційних системах зберігається дуже багато інформації. Частина її є загальнодоступною, і з нею може ознайомитися будь-хто. Однак, крім загальнодоступної інформації в базах даних, може зберігатися службова, комерційна або державна таємниця, персональні дані або просто особиста інформація користувача. Для цієї інформації необхідно виконання якості конфіденційності. Але якщо закрита інформація (інформація обмеженого доступу) є, отже, вона має бути доступна лише тим суб'єктам (користувачам), кому вона довірена. Права доступу суб'єктів до об'єктів (інформації) регламентуються сукупністю правил, що називаються правилами розмежування доступу.

Існує велика кількість способів автентифікації, серед яких найпоширенішим досі залишається парольний захист. Однак через її серйозні недоліки останнім часом все більшої актуальності набуває так звана посилена автентифікація - процедура перевірки, при якій використовуються надійніші методи.

Посилена автентифікація впроваджується нині повсюдно. Такий захист застосовується, наприклад, у поштових сервісах, сервісах електронних платежів, соціальних мережах, на порталах державних послуг для захисту

облікових записів користувачів, а також в операційних системах для розмежування доступу до інформації, що зберігається на комп'ютері.

Об’єкт дослідження − автентифікація користувачів в мобільних пристроях.

Предмет дослідження – забезпечення двофакторної автентифікації в мобільних пристроях.

Мета роботи – забезпечення автентифікації користуваців за рахунок використання адаптивного багатофакторного методу автентифікації.

Кваліфікаційна робота присвячена дослідженню та аналізу методів автентифікації користувачів, та дослідженню використання технології двофакторної автентифікації.

1 ОСНОВНІ ЗАВДАННЯ АВТЕНТИФІКАЦІЇ

Автентифікація - це процедура, яка дозволяє здійснити перевірку справжності зазначених користувачем даних. Після успішного проходження автентифікації користувачеві надається доступ до закритої інформації на інтернет-ресурсі.

Для проходження автентифікації користувачеві пропонується ввести комбінацію певних даних, наприклад, логін і пароль використовуваної облікового запису. Необхідна інформація вноситься відвідувачем в спеціальну HTML-форму. Після натискання на кнопку підтвердження введення програма автентифікації надсилає відповідні дані на сервер для порівняння з наявними в базі записами. Якщо зберігається на сайті комбінація збігається з введеної інформацією, здійснюється переадресація користувача до закритої частини сайту. При розбіжності вписаних даних відвідувачеві пропонується виконати авторизацію заново [2].

Процедура автентифікації проводиться з метою надання користувачеві певних прав, яких немає у неавторизованих гостей. Після успішного виконання входу користувач може отримати доступ до особистого кабінету, в якому отримає можливість змінювати дані облікового запису та виробляти додаткові настройки і операції. Наприклад, після проходження автентифікації в соціальних мережах користувач отримує право вести переписку і виробляти публікації від свого імені.

1.1 Принцип роботи автентифікації

Під час автентифікації облікові дані, що надаються користувачем, порівнюються з даними у файлі в базі даних авторизованих користувачів або в локальній операційній системі або через сервер автентифікації. Якщо облікові дані збігаються, а авторизований об'єкт має право використовувати цей ресурс, процес завершується і користувачеві надається доступ. Повернення дозволів і папок визначають як середовище, яке бачить користувач, так і спосіб взаємодії з ним, включаючи години доступу та інші права, такі як обсяг місця для зберігання ресурсів.

Традиційно автентифікація здійснювалася за допомогою систем або ресурсів, до яких здійснювався доступ; наприклад, сервер автентифікує користувачів, використовуючи власну систему паролів, реалізовану локально, використовуючи ідентифікатори для входу (імена користувачів) і паролі. Знання облікових даних для входу в систему вважається гарантованим, що користувач є автентичним. Кожен користувач спочатку реєструється (або реєструється іншим, наприклад, системним адміністратором), використовуючи призначений або самозваний пароль. При кожному наступному використанні користувач повинен знати і використовувати попередньо оголошений пароль.

Проте протоколи додатків мережі, HTTP і HTTPS, не мають статусу, а це означає, що сувора автентифікація потребує повторної автентифікації кінцевих користувачів кожного разу, коли вони отримують доступ до ресурсу за допомогою HTTPS. Замість того, щоб навантажувати кінцевих користувачів цим процесом для кожної взаємодії через Інтернет, захищені системи часто покладаються на автентифікацію на основі маркерів, в якій автентифікація виконується один раз на початку сеансу. Система автентифікації видає підписаний маркер автентифікації до програми кінцевого користувача, і цей маркер додається до кожного запиту від клієнта [5].

Автентифікацію об'єктів для систем і процесів можна здійснювати за допомогою облікових даних машини, які працюють як ідентифікатор користувача та пароль, за винятком того, що дані облікового запису автоматично подаються відповідним пристроєм. Вони також можуть використовувати цифрові сертифікати, які були видані та перевірені центром сертифікації як частину інфраструктури відкритого ключа для автентифікації особи при обміні інформацією через Інтернет.

1.2 Види автентифікації

Традиційна автентифікація залежить від використання файлу паролів, в якому ідентифікатори користувачів зберігаються разом з хешами паролів, пов'язаних з кожним користувачем. Під час входу в систему пароль, що подається користувачем, змішується і порівнюється зі значенням у файлі паролів. Якщо два хеши збігаються, користувач автентифікується. Додавання факторів автентифікації до процесу автентифікації зазвичай покращує безпеку. Сильна автентифікація зазвичай відноситься до автентифікації, яка використовує принаймні два фактори, коли ці фактори мають різні типи. Відмінність важлива; оскільки і ім'я користувача, і пароль можна вважати типом фактора знань, можна сказати, що базове ім'я користувача та автентифікація паролем використовують два фактори знань для автентифікації - однак це не вважається формою двофакторної автентифікації. Так само для систем автентифікації, які покладаються на "питання безпеки", які також є "щось, що ви знаєте", для доповнення ідентифікатора користувача та паролів [15].

Деякі ресурси пропонують авторизувати із застосуванням автоматично згенерованого одноразового пароля, який відправляється користувачеві при відповідному запиті. Числова або текстова комбінація для здійснення входу

відправляється через SMS або за допомогою e-mail. Іноді одноразові паролі генеруються спеціальними пристроями eToken.

У системах, які потребують підвищеному рівні безпеки, часто використовується біометрична авторизація із застосуванням сканування райдужної оболонки ока або відбитка долоні. У деяких випадках застосовується технологія автоматичної експертизи почерку або голосу користувача.

Процес автентифікації в інтернеті застосовується на таких ресурсах, як веб-форуми, блоги, соціальні мережі. Авторизація із застосуванням різних способів здійснюється в платіжних системах, інтернет-банкінгу, інтернет-магазинах і на деяких корпоративних ресурсах. Залежно від ступеня захищеності сайту і важливості зберігається на ньому можуть бути реалізовані різні методи отримання доступу.

1.2.1 Парольна автентифікація

Одноразовий пароль - це автоматично створений числовий або буквено-цифровий рядок символів, що автентифікує користувача. Цей пароль дійсний лише для одного сеансу входу або транзакції

Такий підхід до автентифікації має ряд недоліків, особливо для ресурсів, розгорнутих в різних системах. По-перше, зловмисники, які можуть отримати доступ до файлу паролів для системи, можуть використовувати атаки грубої сили на хешовані паролі для вилучення паролів. З іншого боку, такий підхід вимагає декількох автентифікацій для сучасних додатків, які отримують доступ до ресурсів у різних системах [13].

Слабкі місця автентифікації на основі паролів можуть бути вирішені до певної міри розумнішими іменами користувачів і правилами паролів, такими як мінімальна довжина та умови для складності, наприклад, включаючи великі і символи.

Однак, автентифікація на основі паролів і автентифікація на основі знань є більш вразливими, ніж системи, які вимагають декількох незалежних методів.

1.2.2 Біометрична автентифікація

Біометричні технології засновані на біометрії, виміри унікальних характеристик окремо взятої людини. Це можуть бути як унікальні ознаки, отримані з народження, наприклад: ДНК, відбитки пальців, райдужна оболонка ока; так і характеристики, отримані з часом або здатні змінюватися з віком або зовнішнім впливом. Наприклад: почерк, голос чи ходу.

Ідентифікація полягає у розпізнаванні користувача за властивою або присвоєною йому ідентифікаційною ознакою. Перевірка належності користувачеві пред'явленої ним ідентифікаційної ознаки здійснюється у процесі автентифікації [18].

До складу апаратно-програмних систем входять ідентифікатори, пристрої введення-виводу (зчитувачі, контактні пристрої, адаптери, плати довіреного завантаження, роз'єми системної плати та ін.) та відповідне програмне забезпечення. Ідентифікатори призначені для збереження унікальних ідентифікаційних ознак. Крім того, вони можуть зберігати та обробляти різноманітні конфіденційні дані. Пристрої введення-виводу та програмне забезпечення пересилають дані між ідентифікатором і комп'ютером, що захищається.

Біометрична ідентифікація – це спосіб ідентифікації особи за окремими специфічними біометричними ознаками (ідентифікаторами), властивими конкретної людини.

Біометрична автентифікація - це упізнання індивідуума з урахуванням його фізіологічних показників та поведінки. Автентифікація проводиться за допомогою комп'ютерної технології без порушення особистої сфери людини.

Зібрані таким чином у базі даних прикмети людини порівнюються з тими, що актуально реєструються системами безпеки.

Біометричні технології активно застосовуються у багатьох галузях пов'язаних із забезпеченням безпеки доступу до інформації та матеріальних об'єктів, а також у завданнях унікальної ідентифікації особистості.

Застосування біометричних технологій різноманітні: доступ до робочих місць та мережевих ресурсів, захист інформації, забезпечення доступу до певних ресурсів та безпека. Ведення електронного бізнесу та електронних урядових справ можливе лише після дотримання певних процедур з ідентифікації особи. Біометричні технології використовуються у сфері безпеки банківських звернень, інвестування та інших фінансових переміщень, а також роздрібній торгівлі, охороні правопорядку, питаннях охорони здоров'я, а також у сфері соціальних послуг. Біометричні технології незабаром відіграватимуть головну роль у питаннях персональної ідентифікації у багатьох сферах. Застосовувані окремо або використовувані разом зі смарт-картами, ключами та підписами, біометрія незабаром буде застосовуватися у всіх сферах економіки та приватного життя. У таблиці 1.1 наведені основсі області застосування біометричної автентифікації та їх основні характеристики [11].

Крім цих основних секторів застосування, в даний час починається активне використання біометрії і в деяких інших областях, таких як:

– гральний бізнес. Біометрія використовується за двома напрямками: перевірка всіх "чорних списків" (аналог масової ідентифікації по особах, що використовується в аеропортах), а також як система ідентифікації та платіжний засіб постійних клієнтів;

– ідентифікація у мобільних пристроях, таких як мобільні телефони, компактні ПК тощо;

– у транспортній галузі як платіжний засіб;

– електронні системи голосування (використовуються замість карток);

Таблиця 1.1 - Області застосування біометричної автентифікації

Області застосування	Основні характеристики
Комп'ютерна безпека	У цій галузі біометрія використовується для заміни (іноді для посилення) стандартної процедури входу в різні програми пароля, смарт-карти, таблетки touch-memory і т.д. Найпоширенішим рішенням на основі біометричних технологій є ідентифікація (або верифікація) за біометричними характеристиками в корпоративній мережі або при вході на робочу станцію (персональний комп'ютер, ноутбук тощо).
Торгівля	Основні напрями: у магазинах, ресторанах та кафе біометричні ідентифікатори використовуються або безпосередньо як засіб ідентифікації покупця та подальшого зняття грошей з його рахунку, або для підтвердження права покупця на будь-які знижки та інші пільги; - у торгових автоматах та банкоматах як засіб ідентифікації людини замість магнітних карток або на додаток до них; - в електронній комерції біометричні ідентифікатори використовуються як засоби віддаленої ідентифікації через Інтернет, що значно надійніше за паролі, а в поєднанні з засобами криптографії дає електронним транзакціям дуже високий рівень захисту.

Продовження таблиці 1.1

Системи контролю та управління доступом	У системах контролю та управління доступом з мережевою архітектурою, коли в будівлі є кілька входів, обладнаних біометричними замками, шаблони біометричних характеристик усіх співробітників зберігаються централізовано, разом з інформацією про те, кому і куди (і, можливо, коли) дозволено вхід. У системах контролю та управління доступом реалізуються такі технології розпізнавання: відбиток пальця, обличчя, форма руки, райдужна оболонка ока, голос.
Автоматизовані дактилоскопічні інформаційні системи	Основним призначенням систем громадянської ідентифікації та автоматизованих дактилоскопічних інформаційних систем є управління правами, які надано державою громадянам та іноземцям. Права громадянства, голосування, місця проживання або роботи для іноземців, право на отримання соціального забезпечення тощо. визнаються та підтверджуються за допомогою документів та різноманітних карт. В даний час такі системи набули дуже широкого поширення, через деякі країни стали використовувати їх для перевірки особистості тих, хто виїжджає.
Комплексні системи	До систем даного типу відносяться рішення, що поєднують у собі системи перших трьох класів. Співробітник компанії реєструється в адміністратора системи лише один раз, і далі йому автоматично призначаються всі необхідні привілеї як на вхід у приміщення, так і на роботу в корпоративній мережі та з її ресурсами.

– медицини. Біометрія використовується для ідентифікації медичних працівників при отриманні доступу до закритих даних та електронного підпису записів в історії хвороби.

Розглянемо особливості біометричної автентифікації. Останні два десятиліття біометричні технології зробили великий крок уперед. Багато в чому сприяло поширення мікропроцесорних технологій. Ще у 80-ті роки систему контролю доступу, що використовує біометричні характеристики людини, можна було побачити лише у фантастичних фільмах. Сьогодні ж використання в системах контролю та управління доступом біометричних сканерів практично не ускладнює систему безпеки, і їх вартість для деяких біометричних методів дуже низька. Більше того, близько третини ноутбуків виходить зараз із вбудованою системою зчитування відбитка пальців, а якщо в ноутбуці є відеокамера, на нього можна встановити систему розпізнавання людини на обличчі.

Основними характеристиками будь-якої біометричної системи є два числа - FAR (False Acceptance Rate) та FRR (False Rejection Rate). Перше число характеризує можливість помилкового збігу біометричних показників двох людей. Друге – ймовірність відмови доступу людині, яка має допуск. Система тим краще, що менше значення FRR при однакових значеннях FAR. Стійкість до підробки - це емпірична характеристика, що узагальнює те, наскільки легко обдурити біометричний ідентифікатор. Стійкість до навколишнього середовища - характеристика, що емпірично оцінює стійкість роботи системи за різних зовнішніх умов. Простота використання показує, наскільки складно скористатися біометричним сканером, чи можлива ідентифікація на ходу. Важливими характеристиками є швидкість роботи, і вартість системи. Безсумнівно, суттєвим є те, як протягом часу поводиться біометрична характеристика. Якщо вона нестійка і може змінитися це значний мінус [16].

Фізіологічні (статичні) методи:

– сканування райдужної оболонки ока;

– сканування сітківки ока;

– геометрія кисті руки (малюнок вен, відбитки пальців – дактилоскопія, розмір, довжина та ширина долонь);

– розпізнавання рис обличчя (контур, форма; розташування очей та носа);

– зняття відбитків пальців;

– структура ДНК – сигнатура.

Поведінкові (динамічні) методи:

– аналіз підпису (форма літер, манера письма, натиск);

– аналіз тембру голосу;

– аналіз клавіатурного почерку.

У таблиці 1.2 наведені методи автентифікації та їх характеристики, що дозволяє нам їх порівняти.

Таблиця 1.2 - Порівняння методів біометричної автентифікації

Метод	Насій біометричної інформації	Ймовірність помилки	Надійність	Сфера використання
Розпізнавання райдужної оболонки ока	Візерунок веселки	1/1200000	Висока	Критичні до кількості помилок послуги
Дактилоскопія	Відбитки пальців	1/1000	Середня	Універсальна

Продовження таблиці 1.2

Форма руки	Розмір, довжина та ширина долонь	1/700	Низька	Некритичні до кількості помилок послуги
Розпізнавання особи	Контур, форма; розташування очей та носа	1/100	Низька	Некритичні до кількості помилок послуги
Підпис	Форма букв, манера письма, натиск	1/100	Низька	Некритичні до кількості помилок послуги
Розпізнавання голосу	Характеристики голосу	1/30	Низька	Телефонні сервери

Новим напрямком є використання біометричних характеристик в інтелектуальних розрахункових картках, жетонах-перепустках та елементах стільникового зв'язку. Наприклад, при розрахунку в магазині пред'явник картки кладе палець на сканер на підтвердження, що картка справді його [9].

Відбитки пальців

Дактилоскопія (розпізнавання відбитків пальців) - найбільш розроблений на сьогоднішній день біометричний метод ідентифікації особистості. Каталізатором розвитку методу стало його широке використання у криміналістиці XX століття.

Кожна людина має унікальний папілярний візерунок відбитків пальців, завдяки чому і можлива ідентифікація. Зазвичай алгоритми використовують характерні точки на відбитках пальців: закінчення лінії візерунка, розгалуження лінії, одиночні точки. Додатково залучається інформація про морфологічну структуру відбитка пальця: відносне положення замкнених ліній папілярного візерунка, арочних та спіральних ліній. Особливості папілярного візерунка перетворюються на унікальний код, який зберігає інформативність зображення відбитка. І саме «коди відбитків пальців» зберігаються в базі даних, яка використовується для пошуку та порівняння. Час перекладу зображення відбитка пальця код і його ідентифікація зазвичай не перевищують 1с, залежно від розміру бази. Час, витрачений на піднесення руки, не враховується. У таблиці 1.3 наведені переваги та недоліки даного методу.

Таблиця 1.3 - Переваги та недоліки біометричного методу автентифікації за допомогою відбитків пальцав.

Переваги	Недоліки
1) Висока достовірність – статичні показники метода вище показників способі автентифікації за обличчам, голосом 2) Низька вартість пристрою,. Що сканує зображення відбитків пальців 3) Достатньо проста процедура сканування відбитку	1) Папілярний візерунок відбитку пальця дуже легко пошкоджується маленькими подряпинами, порізами 2) Недостатня захищеність від підробки зображення відбитку, що частично визвана широким розповсюдженням метода

Райдужна оболонка

Райдужна оболонка ока є унікальною характеристикою людини. Малюнок райдужної оболонки формується на восьмому місяці

внутрішньоутробного розвитку, остаточно стабілізується у віці близько двох років і практично не змінюється протягом життя, крім як внаслідок сильних травм або різких патологій. Метод є одним із найбільш точних серед біометричних технологій.

Система ідентифікації особистості по райдужній оболонці логічно ділиться на дві частини: - пристрій захоплення зображення, його первинної обробки та передачі обчислювачу; обчислювач, який здійснює порівняння зображення із зображеннями в базі даних, що передає команду про допуск виконавчого пристрою.

Час первинної обробки зображення в сучасних системах приблизно 300-500 мс, швидкість порівняння отриманого зображення з базою має рівень 50000-150000 порівнянь за секунду навіть на звичайному персональному комп'ютері. Така швидкість порівняння не накладає обмежень застосування методу великих організаціях під час використання у системах доступу. При використанні спеціалізованих обчислювачів і алгоритмів оптимізації пошуку стає навіть можливим ідентифікувати людину серед жителів цілої країни.

У таблиці 1.4 наведені переваги та недоліки даного методу.

Таблиця 1.4 - Переваги та недоліки біометричного методу автентифікації за допомогою райдужної оболонки

Переваги	Недоліки
1) Статистична надійність метода 2) Захват зображення райдужної оболонки можливо проводити на відстані від декількох сантиметрів до декількох метрів, при цьому фізичний контакт з пристроєм не відбувається 3) Райдужна оболонка ока захижена від пошкоджень рогівницею	1) Ціна системи для захвату райдужної оболонки вище вартості сканера відбитків пальців та камери для захвату 2D зображення обличчя

Геометрія обличчя

Існує безліч методів розпізнавання геометрії обличчя. Усі вони засновані на тому, що риси обличчя та форма черепа кожної людини індивідуальні. Ця область біометрії багатьом здається привабливою, тому що ми впізнаємо один одного в першу чергу по обличчю. Дана область ділиться на два напрямки: 2D-розпізнавання та 3D-розпізнавання. У кожного з них є переваги та недоліки, проте багато що залежить ще й від галузі застосування та вимог, пред'явлених до конкретного алгоритму.

2D-розпізнавання обличчя

2D-розпізнавання особи — один із найстатистично неефективних методів біометрії. З'явився він досить давно і застосовувався в основному в криміналістиці, що й сприяло його розвитку. Згодом з'явилися комп'ютерні інтерпретації методу, внаслідок чого він став надійнішим, але, безумовно, поступався і з кожним роком дедалі більше поступається іншим біометричним методам ідентифікації особистості. В даний час через погані статистичні показники він застосовується, в основному, в мультимодальній або, як її ще називають, перехресній біометрії. У таблиці 1.5 наведені переваги та недоліки даного методу.

Реалізація цього методу є досить складне завдання. Незважаючи на це, в даний час існує безліч методів 3D-розпізнавання обличчя. Нижче розглядається один із найпоширеніших [7].

Метод проектування шаблону у тому, що у об'єкт (обличчя) проектується сітка. Далі камера робить знімки зі швидкістю десятки кадрів за секунду, і отримані зображення обробляються спеціальною програмою. Промінь, що падає на викривлену поверхню, згинається - чим більша кривизна поверхні, тим сильніший вигин променя.

Таблиця 1.5 - Переваги та недоліки біометричного методу автентифікації за допомогою 2D-розпізнавання особи

Переваги	Недоліки
1) При 2D розпізнаванні, на відміну від більшості біометричних методів, не потребується дороге обладнання 2) Можливість розпізнавання обличчя на відстані від камери	1) Низька статистична достовірність 2) Вимоги до освітлення 3) Для багатьох алгоритмів неприйнятність зовнішніх перешкод, як, наприклад, окуляри, борода, деякі деталі зачіски 4) Обов’язкове фронтальне зображення обличчя, з дуже незначними відхиленнями 5) Багато алгоритмів не враховують можливі зміни міміки обличчя

Спочатку при цьому застосовувалося джерело видимого світла, що подається через жалюзі. Потім видиме світло було замінено інфрачервоним, який має низку переваг. Зазвичай на першому етапі обробки відкидаються зображення, на яких особи не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3D-модель особи, на якій виділяються та видаляються непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі - виділяються антропометричні особливості, які в результаті записуються в унікальний код, що заноситься в базу даних. Час захоплення та обробки зображення становить 1-2 с для кращих моделей. У таблиці 1.6 наведені переваги та недоліки даного методу.

Таблиця 1.6 - Переваги та недоліки біометричного методу автентифікації за допомогою 3D-розпізнавання особи

Переваги	Недоліки
1) Відсутність необхідності контакти- рувати зі скануючим пристроєм; 2) Низька чутливість до зовнішніх факторам, як на людині: (поява окулярів, бороди, зміна зачіски) таки в його оточенні (освітлення щенность поворот голови); 3) Високий рівень надійності, порівняно- нимий з методом ідентифікації відбиткам пальців.	1) Дорожнеча обладнання; «Зміни міміки особи і перешкоди хіна обличчі погіршують статистичні ну надійність методу; 2) Метод ще недостатньо добре шо розроблений, особливо в орівнянні нянні з давно застосовується дактилосколією, що утруднює його широке застосування.

Венозний малюнок руки

Це нова технологія у сфері біометрії. Інфрачервона камера робить знімки зовнішнього або внутрішнього боку руки. Малюнок вен формується завдяки тому, що гемоглобін крові поглинає ІЧ-випромінювання. В результаті ступінь відображення зменшується і вени видно на камері у вигляді чорних ліній. Спеціальна програма на основі отриманих даних створює цифрову згортку. Не потрібен контакт людини з скануючим пристроєм. Малюнок вен на долоні не змінюється із дворічного віку.

Технологія можна порівняти за надійністю з розпізнаванням по райдужній оболонці ока, але має ряд мінусів, вказаних нижче у таблиці 1.7.

Таблиця 1.7 - Переваги та недоліки біометричного методу автентифікації за допомогою венозного малюнка руки

Переваги	Недоліки
1) Відсутність необхідності контактувати з скануючим пристроєм 2) Висока достовірність - статистичні показникиметода можна порівняти з показниками райдужної оболонки ока	1) Недопустиме засвічення сканера сонячними промінями та промінями галогенових ламп 2) Деякі вікові захворювання, наприклад артрит 3) Метод менш вивчений порівняно з іншими статичними методами біометрії

Сітківка ока

До останнього часу вважалося, що найнадійніший метод біометричної ідентифікації та автентифікації особистості – це метод, що базується на скануванні сітківки ока. Він містить у собі найкращі риси ідентифікації за райдужною оболонкою та венами руки. Сканер зчитує малюнок капілярів на поверхні сітківки ока. Сітківка має нерухому структуру, незмінну в часі, крім як внаслідок очної хвороби, наприклад катаракти.

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Сканери сітківки ока набули широкого поширення в системах контролю доступу на особливо секретні об'єкти, так як у них один із найнижчих відсотків відмови у доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу.

На жаль, цілий ряд труднощів виникає при використанні цього методу біометрії. Сканером тут є дуже складна оптична система, а людина має значний час не рухатися, доки система наводиться, що спричиняє неприємні відчуття. У таблиці 1.8 наведені переваги та недоліки даного методу.

Таблиця 1.8 - Переваги та недоліки біометричного методу автентифікації за допомогою сітківки ока

Переваги	Недоліки
1) Високий рівень статистичної надійності 2) Через низьку розповсюдженність системи мала ймовірність розробки способа їх обману 3) Безконтактний метод отримання данних	1) Складна в використанні система з довгим часом обробки 2) Висока вартість системи 3) Відсутність широкого ринку пропозиції та, як слідство, недостатня інтенсивність розвитку метода

Термічний образ обличчя. Системи дозволяють ідентифікувати людину з відривом до десятків метрів. У комбінації з пошуком даних по базі даних такі системи використовуються для пізнання авторизованих співробітників та відсіювання сторонніх. Однак при зміні освітленості сканери мають відносно високий відсоток помилок.

Голос. Перевірка голосу зручна для використання у телекомунікаційних програмах. Необхідні для цього 16-розрядна звукова плата та конденсаторний мікрофон коштують менше 25$. Можливість помилки становить 2 – 5%. Ця технологія підходить для верифікації по голосу по телефонних каналах зв'язку, вона більш надійна, ніж частотний набір особистого номера. Зараз розвиваються напрями ідентифікації особи та її стану за голосом – збуджений, хворий, каже правду, не в собі тощо.

Введення із клавіатури. Тут при введенні, наприклад, пароля відстежуються швидкість та інтервали між натисканнями.

Підпис. Для контролю рукописного підпису застосовуються дигітайзери.

Переважна більшість людей вважають, що в пам'яті комп'ютера зберігається зразок відбитка пальця, голосу людини або картинка райдужної оболонки його ока. Але насправді у більшості сучасних систем це не так. У

спеціальній базі даних зберігається цифровий код довжиною до 1000 біт, який асоціюється з конкретною людиною, яка має право доступу. Сканер або будь-який інший пристрій, який використовується в системі, зчитує певний біологічний параметр людини. Далі він обробляє отримане зображення або звук, перетворюючи їх на цифровий код. Саме цей ключ і порівнюється із вмістом спеціальної бази даних для ідентифікації особи [10].

1.2.3 Багатофакторна автентифікація

Двофакторна автентифікація зазвичай залежить від фактора знання, що поєднується з біометричним фактором або фактором володіння, наприклад, маркером безпеки. Багатофакторна автентифікація може включати будь-який тип автентифікації, що залежить від двох або більше факторів, але процес автентифікації, який використовує пароль, плюс два різних типи біометричних даних, не вважатиметься трьохфакторною автентифікацією, хоча, якщо процес вимагає фактора знання, володіння фактор і фактор невідповідності, було б. Системи, які викликають ці три фактори плюс географічний чи часовий фактор, вважаються прикладами чотирьохфакторної автентифікації.

2 АВТЕНТИФІКАЦІЯ В МОБІЛЬНИХ ПРИСТРОЯХ

Популярність мобільних пристроїв зростає з кожним днем. Смартфони, планшети, "розумний" годинник - сьогодні ці легкі портативні "міні-ПК" перевершують за популярністю традиційні настільні комп'ютери та ноутбуки. Ця тенденція продиктована темпом сучасного життя, насиченого перельотами та переїздами – часто на інший кінець земної кулі. Сьогодні багато людей працюють віддалено, не в звичайному офісі, а вдома чи під час подорожей. А невеликий, легкий мобільний пристрій зручно мати під рукою.

У такій ситуації для доступу до особистих і, особливо, робочих облікових записів гостро необхідні надійні способи автентифікації. Тому мобільна автентифікація набуває значення, яке неможливо переоцінити.

До сучасних методів автентифікації відноситься перевірка автентичності на основі біометричних показників. При біометричній автентифікації секретними даними користувача можуть бути як очна сітківка, так і відбиток пальця. Ці біометричні образи є унікальними кожного користувача, що забезпечує високий рівень захисту доступу до інформації. Згідно з попередньо встановленими протоколами, біометричні зразки користувача реєструються в базі даних.

Мобільна автентифікація - це процес перевірки користувачів через пристрої або самі пристрої. Процес мобільної аутентифікації включає багатофакторну аутентифікацію, яка може містити одноразові паролі, біометричну аутентифікацію або перевірку QR-коду.Сучасна біометрична автентифікація ґрунтується на двох методах:

- статичний метод автентифікації - розпізнає фізичні параметри людини, якими вона має протягом усього життя: від свого народження і до самої смерті (відбитки пальців, відмінні характеристики райдужної оболонки ока, малюнок

сітківки очей, термограма, геометрія обличчя, геометрія кисті руки і навіть фрагмент генетичного коду);

- динамічний метод - аналізує характерні риси, особливості поведінки користувача, які демонструються в момент виконання будь-якої звичайної повсякденної дії (підпис, клавіатурний почерк, голос та інше).

Статичний метод завжди був основою світового ринку біометричної безпеки. Динамічна автентифікація та комбіновані системи інформаційної безпеки захопили лише 20% ринку. Проте останніми роками активно розвиваються методи динамічного захисту. Особливий інтерес для мережевих технологій становлять методи аутентифікації клавіатурного почерку та підписи.

Досить швидкий розвиток сучасних біометричних технологій порушує найважливішу проблему – визначення загальних стандартів достовірності для біометричних систем безпеки. Продукти, що пройшли сертифікацію якості Міжнародної асоціації комп'ютерної безпеки (ICSA), цінуються професіоналами [4].

2.1 Статичний метод автентифікації

2.1.1 Дактилоскопія

Дактилоскопія - найпопулярніша технологія біометричної автентифікації, заснована на скануванні та розпізнаванні відбитків пальців.

Цей метод активно просувається правоохоронними органами з метою включення електронних зразків до своїх архівів. Крім того, метод сканування відбитків пальців простий у використанні та забезпечує надійну універсальність даних. Основним інструментом для цього методу біометричної аутентифікації є сканер, який сам собою невеликий і недорогий. Така автентифікація відбувається досить швидко, оскільки система не вимагає розпізнавання та порівняння кожного рядка зразка з оригінальним зразком, що

є основою. Системі достатньо визначити збіг блоків шкали та проаналізувати розгалуження, розриви та інші спотворення ліній (хвилин).

Унікальність кожного відбитка дозволяє використовувати даний метод біометричної автентифікації як у криміналістиці, процесах серйозних бізнес-операцій, так і в побуті. Останнім часом з'явилося багато ноутбуків із вбудованим сканером відбитків пальців, клавіатур, комп'ютерних мишей, а також смартфонів для автентифікації користувача.

Ця, здавалося б, незаперечна і справжня автентифікація має недоліки. Складні алгоритми виявлення дрібних папілярних ліній можуть призвести до того, що система аутентифікації сигналізуватиме про помилки, якщо пальці недостатньо стикаються зі сканером. Пристрій аутентифікації та саму систему безпеки можна обдурити за допомогою муляжу (дуже добре зробленого) або мертвого пальця.

За принципом роботи, що використовуються для автентифікації сканери, поділяються на три види:

- оптичні сканери, що функціонують на технології відображення або за принципом просвіту. З усіх видів, оптичне сканування не здатне розпізнати муляж, однак завдяки своїй вартості і простоті, саме оптичні сканери найбільш популярні;

- напівпровідникові сканери - поділяються на радіочастотні, ємнісні, термочутливі та чутливі до тиску сканери. Теплові (термосканери) та радіочастотні сканери найкраще здатні розпізнати справжній відбиток і не допустити автентифікацію по муляжу пальця. Напівпровідникові сканери є більш надійними, ніж оптичні;

- ультразвукові сканери. Даний вид пристроїв є найскладнішим та найдорожчим. За допомогою ультразвукових сканерів можна здійснювати автентифікацію не тільки за відбитками пальців, але й за деякими іншими біометричними параметрами, такими як частота пульсу та ін.

2.1.2 Автентифікація сітківки ока

Цей метод стали використовувати ще в 50-х роках минулого сторіччя. На той час, якраз, було вивчено і визначено унікальність малюнка кровоносних судин очного дна.

Сканери сітківки ока набагато більші і дорожчі, ніж сканери відбитків пальців. Однак надійність цього типу аутентифікації набагато вища, ніж у відбитків пальців, що виправдовує вкладення. Характер крові у фундусі такий, що він не повторюється навіть у близнюків. Тому така автентифікація забезпечує максимальний захист. Обдурити сканер сітківки ока практично неможливо. Помилки у розпізнаванні образів очей незначні – близько мільйона випадків. Якщо користувач не має серйозних захворювань очей (наприклад, катаракти), він може впевнено використовувати систему аутентифікації по сітківці для захисту доступу до різних сховищ, приватних офісів та секретних об'єктів.

Сканування сітківки ока передбачає використання інфрачервоного низькоінтенсивного випромінювання, яке прямує до кровоносних судин очного дна через зіницю. Сигнал відображає кілька сотень характерних точок, які записуються до шаблону. Найсучасніші сканери замість інфрачервоного світла спрямовують лазер м'якої дії.

Щоб пройти аутентифікацію, людина повинна бути якомога ближче до сканера особи (очі повинні бути на відстані не більше 1,5 см від пристрою), бути зафіксованим в одному положенні і дивитися на дисплей сканера, спеціальний знак. Ви повинні знаходитись у такому положенні біля сканера близько однієї хвилини. Саме стільки часу потрібно сканер для виконання операції сканування, після чого системі знадобиться ще кілька секунд для порівняння отриманого зразка з встановленим шаблоном. Основним недоліком використання цього виду ідентифікації є тривалість перебування в одному положенні та фіксація погляду на спалаху світла. Крім того, через тривале сканування сітківки та обробки результатів цей пристрій не може бути

використаний для аутентифікації великої кількості людей (наприклад, перехожих) [13].

2.1.3 Автентифікація по райдужній оболонці ока

Цей метод автентифікації заснований на розпізнаванні унікальних особливостей райдужної оболонки ока.

Як і сітківка, хитромудра схема переміщення мембрани між задньою і передньою камерами ока унікальна для райдужної оболонки. Він формується до народження та не сильно змінюється протягом життя. Надійність перевірки шляхом сканування райдужної оболонки ока допомагає відрізнити ліве око від правого. Ця технологія практично виключає помилки та похибки при аутентифікації.

Однак пристрої, які зчитують зображення райдужної оболонки ока, важко назвати сканером. Можливо, це спеціальна камера, яка робить 30 знімків за секунду. Потім один із записів оцифровується і переводиться в спрощений формат, з якого вибирається близько 200 характерних точок і інформація про них заноситься в шаблон. Це набагато надійніше, ніж сканування відбитків пальців – для створення таких візерунків використовується лише 60-70 точок ознак.

Даний вид автентифікації передбачає додатковий захист від підроблених очей - у деяких моделях пристроїв, для визначення "життя" ока, змінюється потік світла, спрямований у нього і система відстежує реакцію і визначає чи змінюється розмір зіниці.

Ці сканери вже широко використовуються, наприклад, в аеропортах багатьох країн для аутентифікації співробітників при вході до зони обмеженого доступу, а також були використані у пілотних банкоматах у Великій Британії, Німеччині, США та Японії. Слід зазначити, що на відміну від сканування сітківки ока, камера, що сканує, може знаходитися на відстані від 10 см до 1 м від ока, а процес сканування і розпізнавання відбувається

набагато швидше. Ці сканери дорожчі, ніж вищезгадані пристрої біометричної аутентифікації, але останнім часом вони стали доступнішими.

2.1.4 Автентифікація по геометрії руки

Автентифікація по геометрії руки - даний метод біометричної автентифікації передбачає вимірювання певних параметрів людського пензля, наприклад: довжина, товщина та вигини пальців, загальна структура кисті, відстань між суглобами, ширина та товщина долоні.

Руки людини є унікальними, тому для надійності даного виду автентифікації необхідно комбінувати розпізнавання відразу за декількома параметрами.

Імовірність помилок при розпізнаванні геометрії пензля становить близько 0,1%, а це означає, що при забитому місці, артриті та інших захворюваннях і пошкодженнях кисті, швидше за все, пройти автентифікацію не вдасться. Отже, даний метод біометричної автентифікації не підходить для забезпечення безпеки об'єктів високого ступеня секретності.

Проте цей метод широко використовується, оскільки він зручний для користувача з низки причин. Одна з цих причин полягає в тому, що інструмент розпізнавання руки не завдає незручності користувачеві і не займає багато часу (весь процес аутентифікації займає кілька секунд). Ще одна причина популярності аутентифікації з геометрії руки полягає в тому, що ні температура, ні бруд, ні вологість не впливають на процес аутентифікації. Цей метод зручний ще й тим, що його можна використовувати для розпізнавання кисті за низькоякісними зображеннями - розмір шаблону, що зберігається в базі даних, становить 9 байт. Процедура порівняння пензля користувача з встановленим шаблоном дуже проста і легко автоматизується.

Пристрої даного виду біометричної автентифікації можуть мати різний зовнішній вигляд і функціонал - одні сканують лише два пальці, інші роблять

знімок усієї руки, а деякі сучасні пристрої за допомогою інфрачервоної камери сканують вени і зображують автентифікацію.

Цей метод вперше був використаний на початку 70-х років минулого століття. Сьогодні подібні пристрої можна зустріти в аеропортах та різних підприємствах, де необхідно формувати достовірні відомості про присутність тієї чи іншої людини, обліку робочого часу та інших процедур контролю.

2.1.5 Автентифікація з геометрії особи

Цей біометричний метод автентифікації є одним із «трьох великих біометрик» поряд з розпізнаванням по райдужній оболонці та сканування відбитків пальців.

Цей метод аутентифікації поділяється на двовимірне та тривимірне розпізнавання. Двовимірне (2D) розпізнавання осіб використовується вже давно, в основному в галузі криміналістики. Однак цей метод удосконалюється рік у рік, що підвищує рівень його надійності. Однак до досконалості двовимірного розпізнавання осіб ще далеко – ймовірність помилкових спрацьовувань при такій перевірці коливається між 0,1 та 1%. Частота помилок нерозпізнавання ще вища.

Набагато більше надій покладається новий метод - тривимірне (3D) розпізнавання осіб. Оцінки надійності цього методу поки що немає, оскільки він відносно молодий. Близько десяти провідних світових IT-компаній розробляють системи тривимірного розпізнавання облич. Більшість із цих розробників продають свої сканери разом із програмним забезпеченням. І лише деякі працюють над створенням та випуском сканерів..

При тривимірному розпізнаванні осіб використовується ряд складних алгоритмів, ефективність яких залежить умов застосування. Процес сканування займає близько 20-30 секунд. У цей момент особа повертається щодо камери, змушуючи систему компенсувати рухи та проекції рис обличчя, таких як брови, очі, ніс, губи тощо. Потім система визначає відстань з-поміж

них. В основному, шаблон складається з фіксованих характеристик, таких як глибина очниць, форма черепа, дуги брів, висота і ширина вилиць, та інших акцентованих рис, які дозволяють системі розпізнавати навіть бородаті особи, особи в окулярах, шрамах, капелюхах і т.д. Загалом, для створення шаблону використовується від 12 до 40 характеристик особи та голови користувача.

Міжнародний підкомітет зі стандартизації в галузі біометрії (IS0/IEC JTC1/SC37 Biometrics) останнім часом займається розробкою єдиного формату відомостей для розпізнавання людських осіб на основі дво- та тривимірних зображень. Швидше за все, два даних методу об'єднають один біометричний метод автентифікації.

2.1.6 Термографія особи

Цей біометричний метод автентифікації виявляється у встановленні людини за її кровоносними судинами.

Особа користувача сканується інфрачервоним світлом, і формується термограма – температурна карта обличчя, абсолютно унікальна. Цей метод надійніший, ніж автентифікація за відбитками пальців. За такої аутентифікації сканування особи може здійснюватися з відстані до десяти метрів. Цей метод може розпізнавати близнюків (на відміну геометрії обличчя), людей, які перенесли пластичні операції, використовує маску і ефективний, попри температуру тіла, і старіння.

Однак, цей метод не поширений широко, можливо через невисоку якість одержуваних термограм осіб [11].

2.2 Динамічні методи біометричної автентифікації

2.2.1 Метод розпізнавання голосу

Біометричний метод автентифікації користувача за голосом є найдоступнішим для реалізації.

Цей метод дозволяє ідентифікувати та аутентифікувати людину за допомогою одного мікрофона, підключеного до записуючого пристрою. Цей метод корисний у судових справах, коли єдиним доказом проти підозрюваного є запис телефонної розмови. Метод розпізнавання голосу дуже зручний - користувачеві достатньо вимовити слово без додаткових дій. Нарешті, величезною перевагою цього є право виконання секретної аутентифікації. Користувач не завжди може бути поінформований про включення додаткових елементів управління, що ще більше ускладнює зловмисникам отримання доступу.

Персональний портрет ґрунтується на низці характеристик голосу. Це може бути тон, інтонація, модуляція, вимова певних звуків і т.д. Якщо система автентифікації правильно проаналізувала всі характеристики голосу, можливість сторонньої автентифікації дуже мала. Однак у 1-3% випадків система може відмовити реальному власнику до певного голосування. Факт, що голос людини може змінитись під час хвороби (наприклад, застуди), психічного стану, віку тощо. Тому біометричний метод голосової автентифікації небажаний для об'єктів із високим рівнем безпеки. Його можна використовувати для доступу до комп'ютерних класів, бізнес-центрів, лабораторій та подібних захищених приміщень. Технологія розпізнавання голосу може використовуватися не тільки для аутентифікації та ідентифікації, але як незамінний помічник для голосового введення даних.

2.2.2 Метод розпізнавання клавіатурного почерку

Розпізнавання рукописного тексту клавіатури - одне із перспективних методів сучасної біометричної аутентифікації. Почерк клавіатури - це біометрична характеристика поведінки кожного користувача, а саме - швидкість набору тексту, час утримання натиснутої клавіші, інтервали між натисканнями, частота помилок при наборі тексту, кількість накладень між

клавішами, використання функціональних клавіш та комбінацій, ступінь арифметики при наборі тексту та інші.

Ця технологія є універсальною, проте, найкраще, розпізнавання клавіатурного почерку підходить для автентифікації віддалених користувачів. Розробкою алгоритмів розпізнавання клавіатурного почерку активно займаються як зарубіжні, і IT-компанії.

Автентифікація за клавіатурним почерком користувача має два способи:

- уведення відомої фрази (паролю);

- введення невідомої фрази (генерується випадковим чином).

Обидва способи автентифікації передбачають два режими: режим навчання та режим самої автентифікації. Режим навчання полягає у багаторазовому введенні користувачем кодового слова (фрази, пароля). У процесі повторного набору система визначає характерні особливості введення тексту і формує шаблон показників користувача. Надійність такого виду автентифікації залежить від довжини фрази, що вводиться користувачем.

До переваг цього методу аутентифікації відносяться простота використання, можливість проведення процедури аутентифікації без спеціального обладнання та можливість прихованої аутентифікації. Недоліком цього методу, як і у разі розпізнавання голосу, є залежність відмови системи від віку та стану здоров'я користувача. Адже рухливість, яка набагато сильніша за голос, залежить від стану людини. Навіть проста втома людини може вплинути на автентифікацію. Зміна клавіатури також може призвести до збоїв у роботі системи - користувач може не відразу адаптуватися до нового пристрою введення, тому при наборі тестового виразу почерк клавіатури може не відповідати зразку. Зокрема це може вплинути на темпи реалізації. Хоча дослідники рекомендують підвищити ефективність за рахунок використання ритму. Штучне додавання ритму (наприклад, вставка користувачем слова під відому мелодію) забезпечує стабільність клавіатурного почерку та надійніший захист від шкідливих факторів.

2.2.3 Верифікація підпису

У зв'язку з популярністю та масовим використанням різних пристроїв із сенсорним екраном, біометричний метод автентифікації за підписом стає дуже затребуваним.

Використання спеціальних прозорих ручок забезпечує найточнішу перевірку підпису. У багатьох країнах електронні документи, підписані біометричним підписом, мають таку саму юридичну силу, як і паперові. Це дозволяє обробляти документи набагато швидше та безперешкодно. На жаль, справжнім є лише документ, підписаний на папері, або електронний документ із офіційно зареєстрованим електронним цифровим підписом (ЕЦП). Однак ЕЦП можна легко передати іншій людині, чого не можна зробити з біометричним підписом. Тому перевірка біометричного підпису є більш надійною.

Біометричний метод автентифікації за підписом має два способи:

- з урахуванням аналізу візуальних характеристик підпису. Даним способом передбачається порівняння двох зображень підпису на відповідність ідентичності це може здійснюватися як системою, так і людиною;

- метод комп'ютерного аналізу динамічних параметрів написання підпису. Автентифікація у такий спосіб відбувається після ретельного дослідження відомостей про сам підпис, а також про статистичні та періодичні характеристики його написання.

Формування шаблону підпису здійснюється залежно від необхідного захисту. Усього, один підпис аналізується підлогу 100-200 характерних точок. Якщо ж, підпис ставиться з допомогою світлового пера, крім координат пера, враховується і кут його нахилу, натискання пера. Кут нахилу пера обчислюється щодо планшета та за годинниковою стрілкою.

Цей метод біометричної автентифікації, як і розпізнавання клавіатурного почерку, мають спільну проблему залежність від психофізичного стану людини [14].

2.3 Комбіновані рішення біометричної автентифікації

Мультимодальна або комбінована система біометричної аутентифікації - це пристрій, який поєднує кілька біометричних технологій. Комбіновані рішення по праву вважаються найнадійнішими у плані захисту з використанням біометричних показників користувача, оскільки підробити відразу кілька показників набагато складніше, ніж один токен, що практично не під силу зловмисникам. Комбінації "райдужна оболонка ока + палець" або "палець + рука" вважаються найбільш надійними.

Хоча останнім часом популярність набирають системи типу «обличчя + голос». Це пов'язано з широким поширенням комунікаційних засобів, які поєднують у собі модальності аудіо та відео, наприклад, мобільні телефони з вбудованими камерами, ноутбуки, відеодомофони та інше.

Комбіновані системи біометричної автентифікації значно ефективніші за мономодальні рішення. Це підтверджує безліч досліджень, у тому числі досвід одного банку, який встановив спочатку систему автентифікації користувачів по обличчю (частота помилок за рахунок низької якості камер 7%), потім голосом (частота помилок 5% через фонові шуми), а після, комбінувавши ці два методи, досягли майже 100% ефективності.

Біометричні системи можуть бути об'єднані різними способами: паралельно, послідовно або згідно з ієрархією. Головним критерієм при виборі способу об'єднання систем має бути мінімалізація співвідношення кількості можливих помилок на час однієї автентифікації.

Крім комбінованих систем автентифікації, можна використовувати багатофакторні системи. У системах з багатофакторною автентифікацією біометричні дані користувача використовуються разом з паролем або електронним ключем.

2.4 Захист біометричних даних

Біометрична система автентифікації, як і багато інших систем захисту, у будь-який момент може бути піддана нападу зловмисників. Відповідно, починаючи з 2011 року, міжнародна стандартизація в галузі інформаційних технологій передбачає заходи щодо захисту біометричних даних – стандарт IS0/IEC 24745:2011.

Найбільш поширеним напрямом у галузі сучасних методів біометричної аутентифікації є розробка стратегій безпеки для баз даних біометричних шаблонів. Одним із найпопулярніших кіберзлочинів у всьому світі сьогодні є "крадіжка особистих даних". Витік шаблонів з бази даних робить злочин більш небезпечним, оскільки зловмисник може легко відновити біометричні дані, розробивши зворотний шаблон. Оскільки біометричні характеристики є невід'ємною частиною носія інформації, вкрадений шаблон може бути повторно замінений без компрометації, на відміну пароля. Ризик крадіжки шаблону полягає в тому, що зловмисник може отримати доступ до секретної інформації про людину, крім доступу до захищених даних або організувати проти нього приховане спостереження.

Захист біометричних шаблонів базується на трьох основних вимогах:

- незворотність - ця вимога орієнтована на збереження шаблону таким чином, щоб зловмиснику було неможливо відновити обчислювальним шляхом біометричні характеристики зі зразка, або створити фізичні підробки біометричних характеристик;

- розрізнення - точність системи біометричної автентифікації не повинна бути порушена схемою захисту шаблону;

- скасовуваність - можливість формування декількох захищених шаблонів з одних біометричних даних. Дана властивість надає біометричній системі можливість відкликати біометричні шаблони і видавати нові

компрометації даних, а також запобігає зіставленню відомостей між базами даних, зберігаючи цим приватність даних користувача.

Основне завдання при оптимізації надійного захисту шаблону полягає у тому, щоб знайти прийнятне розуміння між цими вимогами. Захист біометричних шаблонів заснований на двох принципах: біометричні криптосистеми та перетворення біометричних ознак. Останні зміни у законі забороняють оператору біометричної системи самостійно змінювати персональні дані без присутності людини. Відповідно, прийматимуться системи, що зберігають біометричні дані у зашифрованому вигляді. Ця інформація може бути зашифрована двома способами: зашифрована звичайним ключем та зашифрована біометричним ключом – доступ до даних надається лише у присутності власника біометричних ідентифікаторів. У традиційній криптографії ключ для розшифровки та зашифрований шаблон - це дві абсолютно різні сутності. Шаблон вважається захищеним, якщо ключ захищений. У біометричний ключ одночасно вбудовується шаблон криптографічного ключа. При такому шифруванні біометрична система зберігає лише часткову інформацію із шаблону. Це називається безпечним ескізом. Для відновлення вихідного шаблону використовується безпечний шаблон, наприклад, представлений під час реєстрації, та інші біометричні шаблони.

ІТ-фахівці, які займаються дослідженнями схем захисту біометричних шаблонів, позначили два головні методи створення захищеного ескізу:

- нечітке зобов'язання (fuzzy commitment);

- нечіткий сейф (fuzzy vault).

Перший метод підходить для захисту біометричних шаблонів, що мають вигляд двійкових рядків певної довжини. А другий може бути корисним для захисту шаблонів, які є набором точок.

Впровадження криптографічних та біометричних технологій надає позитивний вплив на розробку інноваційних рішень у галузі інформаційної

безпеки. Особливо перспективною є багатофакторна біометрична криптографія, яка поєднує технології порогової криптографії з поділом секрету, багатофакторної біометрії та методи перетворення нечітких біометричних ознак у базові послідовності.

Неможливо зробити однозначний висновок у тому, який із сучасних методів біометричної автентифікації чи його комбінації є найефективнішим у тому чи іншого комерційного підприємства з погляду ціна/надійність. Вочевидь, що з багатьох комерційних завдань нелогічно використовувати складні комбіновані системи. Але такі системи взагалі не слід розглядати. Комбінована схема аутентифікації може бути активована з урахуванням рівня безпеки, необхідного в даний час, з можливістю активації додаткових методів у майбутньому [2].

2.5 Мобільна автентифікація як складова двохфакторної автентифікації

Отримання Одноразового пароля в SMS-сообщении.

При вході в аккаунт з комп'ютера або ноутбука користувач отримує тимчасовий пароль, надісланий SMS на його мобільний телефон для підтвердження особи. SMS-автентифікація вважається дуже зручною, оскільки для отримання пароля не потрібне втручання користувача. Вам не потрібно йти до банку або поштового відділення, щоб отримати додатковий пристрій автентифікації користувача – апаратний токен. Також не потрібно встановлювати окреме програмне забезпечення: функція SMS вбудована у всі телефони за замовчуванням. Все, що потрібно користувачеві - це мобільний телефон, який сьогодні є практично у кожного.

Але, як відомо, у кожної медалі з двох сторін — є свій «реверс» і подібний спосіб автентифікації. У тому, що канали мобільного зв'язку захищені досить слабко і теоретично мошенники можуть підключатися до з'єднання та перехоплювати пароль OTP. К тому же, якість сигналу може бути

низьким. А значить, SMS просто не прийде в термін і одноразовий пароль, дійсний тільки впродовж короткого часу, утратить свою актуальність.

Смартфон в ролі генератора одноразових паролей.

Існує більш сучасний та надійний спосіб отримання пароля OTP. На смартфон встановлюється спеціальна програма, яка генерує одноразові паролі та перетворює пристрій на повноцінний OTR-токен. Розробники створили кілька подібних програм, придатних для різних мобільних операційних систем. Protectimus також має таку назву – він називається Protectimus Smart. Його можна безкоштовно встановити на смартфони під керуванням Android та iOS, а також на годинник Android Wear. Програмний токен має досить широкі можливості: вибір довжини пароля, алгоритму його генерації, підтримка функції підпису даних.

Однак такий спосіб отримання одноразових паролів є вразливістю безпеки - відсутність захисту даних в операційних системах, що працюють на мобільних пристроях. Більше того, якщо раніше iOS вважалася практично невразливою для вірусів і зломів, то сьогодні хакери дісталися навіть дітища Стіва Джобса: експерти підтверджують, що в її захисті є "дірки". Вразливості Android вже давно не дають спокою хакерам.

Незважаючи на деякі недоліки, мобільна автентифікація дуже зручна для користувачів — раніше всього тому, що не вимагає проведення перевірки протяжності жодних додаткових пристроїв. Слід визнати, що багаточисленні достоїнства цього способу автентифікації з вибуттям компенсують недочети, які маються.

2.6 Види автентифікації в мобільних пристроях

Методи автентифікації також умовно можна поділити на однофакторні та двофакторні.

Однофакторні методи діляться на:

– логічні (паролі, ключові фрази, які вводяться з клавіатури комп’ютера чи клавіатури спеціалізованого пристрою);

– ідентифікаційні (носієм ключової інформації є фізичні об’єкти: дискета, магнітна карта, тарт-карта, штрих-кодова карта тощо. Недоліки: для зчитування інформації з фізичного об’єкта (носія) необхідний спеціальний рідер; носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію);

– біометричні (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліки: біометричні методи дорогі і складні в обслуговуванні; чутливі до зміни параметрів носія інформації; володіють низькою достовірністю; призначені тільки для автентифікації людей, а не програм або інших ресурсів) [15].

2.7 Методи біометричної автентифікації

Аутентифікація щодо відбитків пальців. Ця біометрична технологія, ймовірно, найбільш широко використовуватиметься в майбутньому. Переваги доступу по відбитку пальця - простота використання, зручність та надійність. Весь процес ідентифікації відбувається досить швидко і вимагає від користувачів великих зусиль. Імовірність помилки при ідентифікації користувача набагато нижча, ніж під час використання інших біометричних методів.

Використання ручної геометрії. В даний час цей метод використовують понад 8000 організацій, включаючи законодавчий орган Колумбії, міжнародний аеропорт Сан-Франциско, лікарні та імміграційні служби. Переваги геометричної ідентифікації по долоні перед ідентифікацією відбитків пальців з точки зору надійності, хоча зчитувач відбитків пальців

займає більше місця. Найсучасніший інструмент Handkey сканує як внутрішню, так і бічні сторони руки.

Аутентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що малюнок плям на оболонці розташований на поверхні ока і користувачеві не потрібно докладати особливих зусиль. Фактично відеозображення ока можна сканувати з відстані до одного метра, що дозволяє використовувати такі сканери в банкоматах. Параметри ідентифікації можуть бути прочитані і закодовані, особливо для людей з вадами зору з неушкодженою райдужкою.

Перевірка сітківки ока. Сітківка сканується низькоінтенсивним інфрачервоним світлом, яке спрямовується через зіницю на кровоносні судини в задній частині ока. Сканери сітківки широко використовуються у надсекретних системах контролю доступу, оскільки вони є одним із пристроїв автентифікації з одним із найнижчих показників повернення та практично нульовою помилкою доступу для зареєстрованих користувачів.

Аутентифікація по обличчю (геометрія особи) - одна з областей біометричної індустрії, що найбільш швидко розвиваються. Розвиток цієї області пов'язаний із швидким зростанням мультимедійних відеотехнологій. Однак більшість розробників все ще намагаються досягти високого рівня продуктивності для таких пристроїв. Однак очікується, що в найближчому майбутньому з'являться пристрої для ідентифікації певних рис особи в залах аеропортів, для захисту від терористів тощо.

Двофакторні методи автентифікації отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: «пароль + дискета», «магнітна карта + PIN».

Кожен клас методів має свої переваги і недоліки. Майже всі методи автентифікації страждають на один недолік - вони, насправді, автентифікують не конкретного суб’єкта, а лише фіксують той факт, що автентифікатор

суб’єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації автентифікатора.

3 ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ

Важливо, щоб захистити файли та вміст вашої компанії неможливо переоцінити. За оцінками, до 2021 року глобальні збитки від кіберзлочинів досягнуть близько 6 трлн доларів на рік. До втрат, пов'язаних з кіберзлочинністю, можна віднести знищення або неправильне використання даних, крадіжку коштів, переривання роботи після кібератаки, крадіжки інтелектуальної власності та зниження продуктивності праці. Вам також слід взяти до уваги потенційні витрати, пов'язані з відновленням зламаних даних або систем, судовою експертизою та заподіянням шкоди репутації. Хоча загрози стають все більш витонченими, а двофакторна автентифікація в усьому світі впроваджується як стандарт безпеки, підприємства, які не звертають уваги на ризики, можуть виявитися вразливими для атак хакерів. Це як не пристібати ремінь безпеки, тому що машина обладнана подушками безпеки. Технічно ви захищені, але не так надійно, як могло б бути.

Недостатній захист даних, зокрема повідомлень електронної пошти, клієнтських баз даних, бібліотек документів, може серйозно вплинути на репутацію організації. Саме тому необхідно використовувати різні варіанти двофакторної автентифікації для додаткового захисту облікових записів співробітників. Зазвичай, використовується автоматичне надсилання SMS-повідомлень або окрема програма, яка генерує коди доступу. Після стандартного пароля користувачеві потрібно також ввести ще код, а в деяких системах використовується програма для введення коду.

Незважаючи на можливості покращення безпеки організації, двофакторна автентифікація використовується нечасто. Поширеними причинами є страх складності застосування для користувачів або небажання розуміти, як цей рівень безпеки може бути використаний для досягнення найкращого ефекту.

Варто зазначити, що на ринку рішень для двофакторної автентифіції є різні цінові пропозиції. Однак під час вибору продукту потрібно пам’ятати, що вартість втрачених даних облікових записів може у кілька разів перевищувати витрати на впровадження рішення.

вофакторна автентифікація в поєднанні з традиційною системою паролів забезпечує більш надійний захист, ніж використання тільки облікових даних для входу. Саме завдяки наявності двофакторної автентифікації багатьох атак за останні місяці можна було б запобігти.

Рішення потрібне для компаній будь-якого розміру, оскільки щоденно співробітники здійснюють вхід на декілька платформ. В першу чергу двофакторну автентифікацію необхідно забезпечити для облікових записів з правами адміністратора та тих, хто має доступ до конфіденційної інформації. Це є потужним кроком до запобігання крадіжці даних і можливим фінансовим втратам.

В основі двофакторної автентифікації лежить використання не тільки традиційної зв'язки «логін-пароль», а й додаткового рівня захисту - так званого другого фактору, володіння яким потрібно підтвердити для отримання доступу до облікового запису або до інших даних.

Найпростіший приклад двофакторної автентифікації, з яким постійно стикається кожен з нас - це зняття готівки через банкомат. Щоб отримати гроші, потрібна карта, яка є тільки у вас, і РШ-код, який знаєте тільки ви. Отримавши вашу карту, зловмисник не зможе зняти готівку не знаючи РШ-коду і точно так само не може отримати гроші знаючи його, але не маючи карти. За таким же принципом двофакторної автентифікації здійснюється доступ до ваших акаунтів в соцмережах, до пошти та інших сервісів. Багатофакторна автентифікація забезпечує додатковий рівень безпеки, вимагаючи більш ніж одного способу автентифікації, щоб перевірити ідентифікацію користувача для входу або виконання суттєвих транзакцій. Окрім паролів, які історично були одним з факторів, інший фактор може

включати те, що ви маєте, наприклад унікальний токен, щось що змінюється кожні 30 секунд (одноразовий пароль на основі часу) або щось таке, як, наприклад, відбиток пальця користувача.

Таким чином двофакторна автентифікація забезпечить додатковий захист файлів від зловмисників. Незалежно від розміру підприємств, ефективність цього рівня безпеки не слід недооцінювати, особливо у випадку використання спільної корпоративної мережі для співробітників [13].

3.1 Особливості двофакторної автентифікації (переваги та недоліки)

Основна перевага двофакторної автентифікації - наявність другого етапу перевірки, який дуже складно або неможливо викрасти. Зазвичай другий фактор є фізичним. Навіть якщо користувач використовує автентифікацію по СМС, або за допомогою спеціальної програми використовується фізичний пристрій, наприклад смартфон, який практично весь час користувач тримає при собі і не помітити його втрату майже не можливо.

Чому це важливо? Щодня у світі відбуваються витоки баз даних, що містять персональні дані мільйонів користувачів. В так званому “дарк-неті” вони масово продаються за символічні гроші. З їх допомогою хакери можуть отримати доступ навіть до облікових записів, а це наражає нас на нові ризики адже більшість сучасних користувачів звикли робити покупки в інтернеті. В разі компрометації облікового запису під цілком реальною загрозою можуть опинитись і ваші фінансові дані, рахунки або комерційні таємниці.

Звісно ж, у двофакторній автентифікації існують і певні недоліки. Тут я зупинюсь трішки детальніше, адже недоліки у всіх видів двофакторної автентифікації різні.

Під час використання OTP-автентифікації вразливою частиною є сервер, який генерує одноразові паролі для всіх користувачів. У разі вдалої на нього атаки будуть скомпрометовані всі користувачі. Разом з цим, в разі

використання автентифікації за допомогою СМС одноразові паролі передаються у відкритому, незашифрованому вигляді та можуть бути перехоплені зловмисниками. Крім того, зараз існують фішингові сайти, які можуть імітувати в тому числі і двофакторну автентифікацію. За допомогою цих сайтів та простих прийомів соціальної інженерії, хакери отримують доступ і до захищених, шляхом двофакторної автентифікації, профілів.

Зручною альтернативною двофакторній автентифікації є біометрична автентифікація. Біометрична автентифікація базується на використанні унікальних біологічних параметрів людини, таких як відбиток пальця або райдужна оболонка ока. Використання біометричної автентифікації дуже популярне на мобільних пристроях. А от щодо її надійності ситуація трішки складніша. Стійкість до зламу визначається правильністю реалізації зчитування біометричних даних. Наприклад, китайські зчитувачі зазвичай не надійні та можуть бути зламані або навмисно містити вразливості. У деяких телефонах використовується технологія FaceID, яка базується не на апаратних датчиках, а на програмних алгоритмах і тому може бути зламана шляхом використання звичайної фотографії. Навіть дорогі смартфони не захищені від такого методу взлому. У подібні скандали вже потрапляли флагманські пристрої компаній Apple, Samsung, Huawei та Nokia.

Щодо захисту смартфонів методом відбитку пальця теж все дуже неоднозначно. Здавалось би, як можна підробити відбиток, який у кожної людини є унікальним? А от все не так просто. Смартфон може бути зламаний з використанням систем штучного інтелекту. Конструкція сучасних смартфонів не дозволяє здійснити зчитування повного відбитка пальця, натомість здійснюється зчитування невеликої частини відбитка, що в свою чергу суттєво полегшує взлом смартфона.

Станом на сьогодні, найнадійнішим видом двофакторної автентифікації фахівці визначають саме використання апаратних ключів з використанням засобів криптографії. Світові корпорації також обрали цей шлях. Зазвичай,

апаратний ключ виглядає як звичайна флешка, однак його конструкція практично не дозволяє здійснити взлом для несанкціонованого доступу до ваших облікових засобів [15].

Крім того, нині існують різні форми апаратних ключів. Він може бути і у вигляді пластикової картки, яку зручно помістити в гаманець. Також її без проблем можна використовувати як пропуск в офіс. Навіть в разі втрати, мало хто зрозуміє, що це апаратний ключ безпеки, адже на вигляд він буде як звичайна перепустка до офісного центру.

3.2 Методи двофакторної автентифікації

В останнє десятиліття Інтернет перетворився на основний спосіб зв’язку нашого сучасного життя. Він, безсумнівно, буде основним інструментом для здійснення покупок та інших фінансових операцій. Поява цих технологій створила суспільний попит на методи автентифікації, основані не тільки на традиційних криптографічних способах (шифрування, гешування, цифровий підпис), а й на методи, основані на використанні декількох чинників забезпечення достовірності особи, яка здійснює фінансову операцію. Двофакторна система безпеки основана на тому, що користувач, крім того, що знає пароль доступу до певного імені користувача (“логіна”), володіє й інструментом для отримання відповідного йому ключа доступу. Останнім може слугувати збережений на комп’ютері електронний сертифікат безпеки або код, який надходить на особистий телефон як СМС з кодом підтвердження, або ж відбиток пальця, знятий електронним пристроєм [2].

3.2.1 Комбінація логіна і пароля

Першим фактором є комбінація логіна і пароля, а в ролі другого може виступати один з приведених нижче конкретних методів двофакторної автентифікації, розглянемо їх переваги та недоліки.

Підтвердження за допомогою 8М8-кодів працює дуже просто. Ви, як завжди, вводите свій логін і пароль, після чого на ваш номер телефону приходить 8М8 з кодом, який потрібно ввести для входу в обліковий запис. Це все. При наступному вході відправляється вже інший 8М8-код, дійсний лише для поточної сесії.

Переваги:

Генерація нових кодів при кожному вході. Якщо зловмисники перехоплять ваш логін і пароль, вони нічого не зможуть зробити без коду.

Прив'язка до телефонного номеру. Без вашого телефону вхід неможливий.

Недоліки:

– при відсутності сигналу мережі ви не зможете залогінитися;

– вснує теоретична ймовірність підміни номера через послугу оператора або працівників салонів зв'язку;

– якщо ви авторізуетесь і отримуєте коди на одному і тому ж пристрої (наприклад, смартфоні), то захист перестає бути двухфакторной.

3.2.2 Додатки-автентифікатори

Цей варіант багато в чому схожий на 8М8, з тією лише відмінністю, що, замість отримання кодів по 8М8, вони генеруються на пристрої за допомогою спеціального додатку (Ооодіе АиШепїісаїш, АиШу). Під час налаштування ви отримуєте первинний ключ (найчастіше - у вигляді ^К-коду), на основі якого за допомогою криптографічних алгоритмів генеруються одноразові паролі з терміном дії від 30 до 60 секунд. Навіть якщо припустити, що зловмисники зможуть перехопити 10, 100 або навіть 1 000 паролів, передбачити з їх допомогою, яким буде наступний пароль, просто неможливо.

Переваги:

– для автентифікатора не потрібен сигнал мережі, тобто достатньо підключення до інтернету лише при первинному налаштуванні;

– підтримка декількох акаунтів в одному автентифікаторі.

Недоліки:

– якщо зловмисники отримають доступ до первинного ключа на вашому пристрої або шляхом злому сервера, вони зможуть генерувати паролі в майбутньому;

– при використанні автентифікатора на тому ж пристрої, з якого здійснюється вхід, втрачається двухфакторність.

3.2.3 Перевірка входу за допомогою мобільних додатків

Даний тип автентифікації можна назвати збірною солянкою з усіх попередніх. В цьому випадку, замість запиту кодів або одноразових паролів, ви повинні підтвердити вхід з вашого мобільного пристрою з встановленим додатком сервісу. На пристрої зберігається приватний ключ, який перевіряється при кожному вході. Це працює в Тшіїег, 8парсЬаї-і та різних онлайн-іграх. Наприклад, при вході в ваш Тшіїег-аккаунт в веб-версії ви вводите логін і пароль, потім на смартфон приходить повідомлення із запитом про вхід, після підтвердження якого в браузері відкривається ваша стрічка.

Переваги:

– не потрібно нічого вводити при вході;

– незалежність від мережі;

– підтримка декількох акаунтів в одному додатку.

Недоліки:

– якщо зловмисники перехоплять приватний ключ, вони зможуть видавати себе за вас;

– сенс двофакторної автентифікації втрачається при використанні одного і того ж пристрою для входу.

3.2.4 Апаратні токени

Фізичні (або апаратні) токени є самим надійним способом двофакторної автентифікації. Будучи окремими пристроями, апаратні токени, на відміну від всіх перерахованих вище способів, ні при якому розкладі не втратять своєї двохфакторної складової. Найчастіше вони представлені у вигляді ШВ-брелоків з власним процесором, що генерує криптографічні ключі, які автоматично вводяться при підключенні до комп'ютера. Вибір ключа залежить від конкретного сервісу. Ооодіе, наприклад, рекомендує використовувати маркери стандарту РГОО ШР, ціни на які починаються від 6 доларів без урахування доставки.

Переваги:

– ніяких 8М8 і додатків;
– немає необхідності в мобільному пристрої;
– є повністю незалежним девайсом.

Недоліки:

– потрібно купувати окремо;
– підтримується не у всіх сервісах;
– при використанні декількох акаунтів доведеться носити цілу в'язку токенов.

3.2.5 Резервні ключі

По суті, це не окремий спосіб, а запасний варіант на випадок втрати або крадіжки смартфону, на який мають приходити одноразові паролі або коди підтвердження. При налаштуванні двофакторної автентифікації в кожному сервісі вам дають кілька резервних ключів для використання в екстрених ситуаціях. З їх допомогою можна увійти в ваш акаунт, відв'язати налаштовані пристрої та додати нові. Ці ключі варто зберігати в надійному місці, а не у вигляді скріншоту на смартфоні або текстового файлу на комп'ютері. Обличчя, голос, відбиток пальців Розпізнавання обличчя, розпізнавання

голосу та сканування відбитків пальців підпадають під категорію біометричних даних. Системи використовують біометричну автентифікацію, коли потрібно, щоб ви дійсно були тими, за кого себе видаєте, часто в областях, де потрібна перевірка безпеки (наприклад, уряд).

Переваги:

– Біометрію надзвичайно важко підробити. Навіть відбиток пальців, який, можливо, найпростіший для копіювання, вимагає певного фізичної взаємодії.

– Розпізнавання голосу потребує певного твердження сказаного вашим голосом

– Розпізнавання обличчя потребує чогось радикального, такого як пластична хірургія. Він не незламний, але досить близький до цього.

Недоліки:

– Найбільший недолік і причина, чому біометрія рідко використовується як двофакторний метод, полягає в тому, що скомпрометований біометричний пристрій може ставити під загрозу саме життя.

3.3 Приклади двофакторної та багатофакторної автентифікації

Методика автентифікації за допомогою SMS заснована на використанні одноразового пароля: перевага такого підходу, згідно з постійним паролем в тому, що цей пароль не можна використовувати повторно. Навіть якщо припустити, що злоумышленнику вдалося перехопити дані в процесі інформаційного обміну, він не вдасться ефективно використати український пароль для отримання доступу до системи.

Ось приклад, реалізований із застосуванням біометричних пристроїв і методів автентифікації: використання сканера для відбитка пальця, який міститься в ряді моделей ноутбуків. При вході в систему користувач повинен

пройти процедуру сканування пальця, а потім підтвердити свою повноту паролем. Успешно завершена автентифікація дасть йому право на використання локальних даних конкретного ПК. Тим не менш, регламентом роботи в ІС може бути передбачена окрема процедура автентифікації для доступу до сетевих ресурсів компанії, яка, поміжуючи вводу іншого пароля, може включати в себе весь ряд вимог до представлення автентифікаторів суб'єкта. Але навіть при такій реалізації, захищеність системи, несомненно, усилюється.

Аналогічним чином можуть бути використані та інші біометричні автентифікатори:

– відбитки пальців;
– геометрія кисті руки;
– контури та розміри особи;
– характеристики голосу;
– візерунок райдужної оболонки та сітківки очей;
– малюнок вен пальців

При цьому звичайно застосовується відповідне обладнання та програмне забезпечення, а витрати на його придбання та підтримку можуть відрізнятись у рази.

Проте, варто розуміти – біометричні автентифікатори є абсолютно точними даними. Відбитки одного пальця можуть відрізнятися під впливом зовнішнього середовища, фізіологічного стану організму людини і т.п. Для успішного підтвердження цього автентифікатора достатньо неповної відповідності відбитка стандарту. Методи біометричної автентифікації містять визначення ступеня ймовірності відповідності автентифікатора діючого еталону. Що стосується біометричної автентифікації та віддаленого доступу до ІС, то поки сучасні технології не мають можливості передати по незахищеним каналам достовірні дані - відбиток пальця або результат сканування сітківки ока.

Ці технології переважно підходять для використання в корпоративних мережах.

Найбільш популярною технологією в цьому напрямку в недалекому майбутньому може стати голосова автентифікація та ознаки цього очевидні. Значна кількість розробок у цій сфері є вже сьогодні, проекти запровадження подібних механізмів управління/контролю знайшли місце у ряді великих банків. Як приклад практичного застосування систем голосової біометричної автентифікації, можна вказати автентифікацію за ключовою фразою, що застосовується в ряді кол-центрів, аудіо-паролі для доступу до систем інтернет-банкінгу і т.п., підтвердження дій персоналу при здійсненні важливих операцій доступу до інформації , контроль фізичного доступу та присутності у приміщенні.

Крім технологій, пов'язаних з використанням біометричних аутентифікаторів, існують також програмні та апаратні рішення, такі як автономні ключі для генерації одноразових паролів, зчитувачі RFID-міток, криптокомп'ютери, програмні та апаратні токени, різні типи електронних ключів - Touch Memory та ключ/інтелектуальні карти, а також біометричні ідентифікаційні картки. Усі перелічені у цій статті системи та методи багатофакторної аутентифікації, а також системи контролю та управління доступом (СКУД) можуть бути інтегрованими, комбінованими, взаємозамінними та складними. Це призводить до невтішного висновку: на ринку достатньо пропозицій щодо посилення захисту інформаційних систем від внутрішніх та зовнішніх вторгнень. Компанії обмежені у своєму виборі лише розміром своїх бюджетів.

Методам захисту, заснованим на методиках багатофакторної автентифікації, сьогодні довіряє велика кількість зарубіжних компаній, серед яких організації хай-теку, фінансового та страхового секторів ринку, великі банківські установи та підприємства держсектору, незалежні експертні організації, дослідницькі фірми.

При цьому, приватні компанії та організації у світі, в цілому, не дуже охоче поширюються про впровадження у себе технологічних новинок у сфері безпеки та захисту інформації з цілком зрозумілих причин. Набагато більше відомо про проекти у державному секторі – з 2006 року публічно відомі успішно реалізовані технологічні рішення у державних установах Канади, Саудівської Аравії, Іспанії, Данії та інших країн [16].

4 ПЕРЕВАГИ ТА НЕДОЛІКИ МЕТОДІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Двофакторна автентифікація, як і всі інші рішення в галузі безпеки, може бути обійдена кіберзлочинцями, але це складніше, ніж використання імен та паролів. Для отримання двофакторної аутентифікації зловмисник повинен або придбати фізичний апаратний аутентифікатор токенів, або, у разі програмних аутентифікаторів, отримати доступ до токенів, згенерованих аутентифікатором на пристрої. Зловмисники роблять це двома способами. Для кожного з них ми включаємо рішення щодо забезпечення безпеки для запобігання наступним типам атак.

– Соціальна інженерія / фішинг: Одна з найбільших уразливостей будь-якої системи безпеки - це люди, задіяні в її експлуатації. Соціальна інженерія та фішинг - це схеми мошенничества, розроблені для експлуатації людського фактора. Визиваючи себе для надійної організації чи окремої особи в телефонному дзвінку, електронній пошті чи іншому обговоренні, фішери намагаються обманом закрити користувача розкрити конфіденційну інформацію, яка дозволить злоумышленнику знайти проблеми двохфакторної автентифікації.

– Вредоносне програмне забезпечення : Вредоносне програмне забезпечення також може виявляти автентифікацію токена з різними способами. Наприклад, шкідлива програма для кейлоггерів може відстежувати натискання клавіш, вводимих користувачів, а потім видаляти передачу маркера автентифікації злоумышленника.

4.1 Переваги двофакторної автентифікації

Її здатність захищати інформацію може бути обумовлена як внутрішніми, і зовнішніми загрозами. Необхідність використання додаткового програмного та апаратного забезпечення, зберігання даних та обчислювальних ресурсів може розглядатися як недолік. У той же час статистика зі злому систем, що використовують двофакторну автентифікацію, нині відсутня або знищена.

Багатофакторна або розширена автентифікація вже використовується багатьма компаніями фінансового сектора для надання кінцевим користувачам рішень в галузі інтернет-банкінгу, мобільного банкінгу, обміну файлами тощо. Вона заснована на спільному використанні кількох факторів аутентифікації (знання інформаційним компонентом, носієм інформації або об'єктом легітимних процедур аутентифікації), що значно підвищує інформаційну безпеку принаймні для сторін, підключених до інформаційних систем, захищених або не захищених каналів зв'язку.

Прикладом може бути процес двофакторної аутентифікації користувача у банківській сфері: вхід у особистий кабінет користувача здійснюється через Інтернет після введення пароля на сайті, а потім (у разі підтвердження) на мобільний телефон раніше зареєстрованого користувача передається штамп часу та дати (SMS) [12].

Аналогічні схеми контролю та управління повноцінністю користувача, його подальші дії в корпоративних чи інших інформаційних системах, можуть бути реалізовані із застосуванням самих різних засобів і методів, вибір яких досить широкий, як за технологіями, коштами, виконанням, так і за можливими комбінаціями перелічених властивостей.

Користувальницька сесія також може відстежуватися за відповідями, як за IP-адресою останньої успішно завершеної сесії, так і за MAC-адресою відповідного мережевого пристрою. Потім можна зробити дії для

підтвердження або заборони доступу до джерела інформації, але покладатися на ці два параметри контролю не слід через їхню технологічну слабкість: IP-адреси можуть бути змінені, MAC-адреси можуть бути просто переписані під час роботи системи і навіть без перезавантаження. Однак ця інформація може бути використана як довідкова.

Аналіз сучасних систем автентифікації показав, що вони вимірюють свою безпеку шляхом поділу різниці між вартістю атаки та вигодою для атакуючого на вартість захисту від неї. Саме з цієї причини дорогі, хоч і більш безпечні методи, такі як криптографічні PKI з власними захищеними каналами зв'язку, екранами та клавіатурами, оцінюються так низько за шкалою безпеки, в той час як банківські системи все ще в основному засновані на найдешевших і, здавалося, б, найменш безпечних. Через загальну вартість і складність розгортання таких пристроїв вони часто краще криптографічних систем безпеки.

4.2 Недоліки багатофакторної автентифікації.

Загрози мережевої безпеки можна розділити на мережеві атаки (інформація від віддалених агентів) та локальні атаки, які походять від шкідливих програм, вже встановлених на клієнтській системі, таких як трояни, руткіти і т.д. Оцінки безпеки автентифікації часто фокусуються в основному на мережевих атаках, що передбачає, що термінал користувача (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є безпечною платформою [1-5]. Однак часті випадки, коли зловмисники отримують повний доступ до комп'ютера жертви через приховані повідомлення, залишені шкідливим програмним забезпеченням, що використовує непропатчені вразливості в ліцензійному програмному забезпеченні.

Типовими методами атак є:

– виламування онлайнових баз даних – викрадення інформації, що зберігається в торгових базах даних.

– “Людина посередині”/фішинг – третя сторона втручається і уособлює клієнта і сервер, змушуючи записувати та/або змінювати повідомлення один одного.

– Атаки в області соцінженерії – клієнтів обманюють, щоб вивідати їхні особисті дані й передати хакеру.

– “Людина в браузері” – шкідлива програма, яка встановлена на комп’ютері жертви, для повідомлення про мережеву активність, натискання клавіш, а також дані, захоплені з екрана хакером, що дає йому змогу перехоплювати дані про переказ коштів, в яких кошти можуть бути мимоволі спотворені шляхом зміни інформації, що відображається в браузері користувача.

– Атака повним перебором паролів користувачів – сервер опитується з усіма можливими комбінаціями паролів.

– Проста крадіжка – подробиці про автентифікацію записані або на картці можуть бути фізично прийняті та скопійовані.

– Спостереження зі спини – зловмисник може непомітно спостерігати, як користувач вводить деталі своєї угоди.

Термін "SMS-системи на базі мобільних телефонів" або "системи двофакторної аутентифікації" є некоректним, точнішим терміном є "позасмугова" аутентифікація. Однак з поширенням GSM, смартфонів та підключених планшетів навіть ця перевага в безпеці може бути втрачена, якщо автентифікація транзакцій користувача здійснюється на мобільному пристрої. Крім того, розповсюдження шкідливого програмного забезпечення на мобільних пристроях тепер дозволяє зловмисникам отримувати доступ до кодів автентифікації, що надсилаються в SMS-повідомленнях, не лише шляхом традиційного перехоплення шкідливих програм, а й шляхом перехоплення та розшифровування даних через телекомунікаційну мережу

GSM. Атаки на мобільну автентифікацію можуть бути успішними без таких технологій. Натомість зловмисник просто видає себе за користувача пристрою та просить, щоб усі SMS-повідомлення в рамках атаки були відправлені на другий номер телефону. Інший метод аутентифікації використовує камеру мобільного пристрою для сканування зображення штрих-коду на робочій станції користувача, де зашифрована інформація про транзакцію OTP. Цей метод містить недолік, який передбачає, що операційна система мобільного пристрою користувача не така вразлива для шкідливого ПЗ, як всі інші види мережного програмного забезпечення.

При використанні біометричної аутентифікації система пропонує дані користувача онлайн-аутентифікації. Однак засоби біометричної автентифікації не можуть взаємодіяти з локальними пристроями або мережею, не зазнаючи атак шкідливих програм та/або проксі-атак. Цей метод може бути змінено повторно, навіть якщо зловмисник видав себе за користувача, який використовує біометричну аутентифікацію.

Біометрична автентифікація надає користувачеві зручний спосіб генерувати ім'я користувача в Інтернеті, але якщо мережа перехоплена або мобільний пристрій скомпрометовано, загальна ефективність безпеки таких методів не перевищує використання стандартного імені користувача та пароля.

Електронні апаратні токени бувають декількох типів і мають різні функції безпеки аутентифікації. Найчастіше апаратні токени використовують криптографічні алгоритми з внутрішнім секретним ключем для генерації одноразових паролів (OTP) або, що поширеніше, генерують секретний ключ на основі загального синхронізованого значення системного часу. Користувачі сканують номери, що відображаються пристроєм, та вручну вводять їх у свої термінали, щоб зв'язати їх із сервером аутентифікації. Цей простий метод генерації електронного OTP, як і раніше, вразливий для проксі-атак, оскільки

користувачі повинні публікувати OTP без перевірки середовища аутентифікації.

У відповідь на це багато виробників маркерів додали невелику цифрову клавіатуру, помітно збільшивши розмір маркера, але дозволяючи користувачу вводити інформацію про конкретні транзакції, зашифровані за допомогою секретного ключа, перш ніж користувач вводить результат у своєму терміналі. Це є одним з типів перевірки або підписання транзакції, і справді забезпечує деякий захист від атаки “посередника”.

Проте цей метод, як і раніше, уразливий для атак через використання трудомісткого процесу ручного підписання транзакції. Час і увага, які необхідні для виконання ручної операції, успішно використовуються для відволікання користувача від контексту інформації про угоди, які користувач приймає, і, отже, атаки можуть бути успішно здійснені в масовому масштабі [1].

Друковані списки OTP/сітки чисел. Старіший метод надання одноразових паролів – друковані списки випадково згенерованих кодів зв’язку або кодів авторизації транзакцій на аркуші паперу або скетч-картці. Кожен код доступу запитується у послідовності та використовується для перевірки справжності однієї транзакції.

Ці методи залишаються вразливими для повного спектра атак “посередника” з тих самих причин, що і всі методи автентифікації з невідомим контекстом.

Перша проблема багатофакторної автентифікації є способом її реалізації. В даний час самим популярним фактором, використовуваним постачальниками сервісу, є одноразовий пароль одноразового пароля — OTP [1].

Призначений цей тип 2FA користувач вводить на першому рівні автентифікацію персонального пароля. На наступному етапі він повинен ввести маркер OTP, зазвичай відправляється за допомогою SMS на його

мобільний пристрій. Ідея способа понятна. OTP буде доступний тільки тому, хто, як передбачається в теорії, вельми недоступний постороннього паролю.

Однак, уви, відправляйте OTP в SMS, взагалі кажу, небезпечно, так як часто повідомлення відправляються відкритим текстом. Навіть починаючи хакери можуть прочесть подібні текстові повідомлення, насправді все, що їм потрібно — цільовий номер телефону.

Крім того, багатофакторна автентифікація не дозволяє запобігти атакам класу MitM, які часто використовуються в ході фішингових компаній за допомогою електронної пошти. У разі успіху користувач перейде на мошенническую ссилку і попаде на сайт, схожий на онлайн-портал банку. Там користувач вводить інформацію про вхід в систему та інші конфіденційні дані, які будуть використовуватися злоумышленником, щоб отримати доступ до реального сайту.

І хоча дана атака буде можлива для здійснення лише обмеженого періоду часу, вона все можлива [16].

4.3 Адаптивний метод багатофакторної автентифікації

Розглянувши в минулих пунктах та розділах методи автентифікації ми можемо зробити висновок, що в наш час більш доцільним є використання багатофакторного методу автентифікації користувачів. Та чи завтжди для кожної авторизації доцільно вводити велику кількість данних? Можливо в деяких ситуаціях це непотрібно?

Тому мною запропоновано використання адаптивного методу багатофакторної автентифікації. Далі пропоную розглянути більш детально що таке адаптивна автентифікація, та які саме методи автентифікації більш доцільно використовувати для багатофакторної автентифікації.

Використання однофакторної автентичності або системи захисту, заснованої лише на використанні пароля, створює значну загрозу для безпеки

підприємств та організацій. Цей метод не становить серйозної перешкоди для хакерів, і наслідки їх дій можуть призвести до появи пролому в системі безпеки, фінансових втрат і втрат важливої інформації, наприклад, такої як персональні дані (PII). При цьому велика кількість IT-підрозділів займається вирішенням завдань щодо розширення доступу до корпоративних додатків та надання його для більш широкої аудиторії, включаючи постачальників, партнерські компанії та клієнтів.

4.3.1 Адаптивний метод автентифікації

Концепція адаптивної аутентифікації вирішує складні проблеми традиційних середовищ управління аутентифікацією та подолання бар'єрів на шляху до підвищення продуктивності користувачів. Якщо не включати до процесу аутентифікації додаткові фактори ризику, такі як місцезнаходження, тип мережі або операційна система, традиційні структури стають застарілими.

Адаптивна аутентифікація - це спосіб налаштування та розгортання двофакторної або багатофакторної аутентифікації. Це метод вибору відповідних факторів аутентифікації залежно від профілю ризику користувача та тенденцій – для адаптації типу аутентифікації до ситуації.

Мистецтво адаптивної аутентифікації є досить ефективним у визначенні відповідних рівнів ризику та представленні відповідних рівнів аутентифікації у реальних сценаріях. На відміну від стандартів, що впливають на зручність використання, безпеку, ефективність та відповідність вимогам, адаптивна автентифікація дозволяє уникнути надто обтяжливих чи надмірно ризикованих операцій із низьким рівнем ризику.

Коротше кажучи, цей підхід нестатичної автентифікації використовує профіль агента, якому потрібен доступ до системи, визначення профілю ризику, пов'язаного з транзакцією. Профіль ризику потім використовується визначення складності завдання. Як згадувалося раніше, цей підхід є адаптованим, дозволяючи проводити ретельніше тестування профілів з

високим рівнем ризику, у той час як для профілів з низьким рівнем ризику може знадобитися статичне ім'я користувача/пароль.

Коли йдеться про реалізацію адаптивної аутентифікації у промисловому середовищі, стає ясно, що для досягнення різних можливостей процесу адаптивної аутентифікації використовувалися різні підходи. Однак модель, що базується на машинному навчанні, може бути визначена як ефективний механізм реалізації, враховуючи характер проблеми.

У традиційному контексті очевидно, що людські фактори та питання зручності використання емпірично ігнорувалися у дослідженнях з безпеки та розробки безпечних систем. Завжди існував компроміс між безпекою та зручністю використання. Однак такий компроміс не може довго існувати в комерційних системах, оскільки він, як і раніше, актуальний у сучасну епоху. Саме тому такі підходи, як адаптивна автентифікація, роблять своєчасним вступ до сфери управління ідентифікацією та доступом.

4.3.2 Методи автентифікації для використання у адаптивній багатофакторній автентифікації

У пунктах 1.2 та 2 були розглянуті існуючі методи автентифікації в цілому та в мобільних пристроях. На основі таблиць, що слугують висновками у розділі 1.2 ми можемо зробити висновок, який саме метод автентифікації доцільно обрати для нашої адаптивної автентифікації. Також з пункту 2 ми можемо винести методи, що більш підходять для автентифікації в мобільних пристроях.

Тому саме за розглядом цих методів можемо зробити висновок, що для більш надійного захисту доцільніше використовувати комбінування таких методів як парольна автентифікація, автентифікація за допомогою відбитків пальців та за допомогою розпізнавання обличчя, перевірка місцезнаходження користувача за допомогою GPS.

Комбінування даних методів можливо за такою схемою:

1) Введення пароля
2) Перевірка відбитку пальця
3) Перевірка місцезнаходження користувача за допомогою GPS

Якщо ві пункти вище співпадають, то можлива автентифікація та допуск до користування пристроєм. Якщо є сумніви або відсутній якийсь з перерахованих методів, то необхідно додатково провести автентифікацію за допомогою розпізнавання обличчя, що буде 4м пунктом в схемі.

Данний метод дозволить надійно захистити данні та перешкодить доступ зловмисників до них.

ВИСНОВКИ

Під час написання даної роботи були розкриті чотири досить великі теми: поняття про автентифікацію, автентифікація в мобільних пристроях, двофакторна автентифікація та загрози методів двофакторної автентифікації. Були проаналізовані методи автентифікації, розглянутий такий великий пласт, як двофакторна автентифікація.

Ціль даної роботи була досягнута, результатами цієї роботи є аналіз методів автентифікації та методів двофакторної автентифікації. Визначили методи реалізації даної послуги та їх переваги та недоліки.

У третьому розділі були розглянуті методи двофакторної автентифікації, що дає змогу визначити більш доцільний.

В ході аналізу були виявлені загрози методів двофакторної автентифікації та іх типи. Детально ці моменти описані у четвертому розділі.

Також в четвертому розділі був запропонований метод автентифікації за допомогою адаптивної багатофакторної автентифікації, він дозволить більш надійно захистити данні та інформацію, що знаходиться на мобільному пристрої.

СПИСОК ЛІТЕРАТУРИ

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.- СПб.: Изд-во СПбГУЭФ, 2010.- 267 с.

2. Галатенко В.А. Идентификация и автентификация, управление доступом лекция из курса «Основы информационной безопасности». - Интернет Университет Информационных Технологий, 2010г.

3. Двухфакторная автентификация [Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/solutions/ authentication/.

4. Двухфакторная автентификация при удаленном доступе [Электронный ресурс]. – Режим доступа: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166/.

5. Евсеев С. П. Исследование методов двухфакторной автентификации / С. П. Евсеев, О. Г. Король // Системи обробки інформації. – 2014. – № 2(118). – С. 81– 87.

6. Настройка двухфакторной автентификации [Электронный ресурс]. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factorauthentication-gransden.html?locale=ru.

7. Зиновьев А. Ю., Визуализация многомерных данных, Красноярск, Изд. КГТУ, 2000.

8. Метод главных компонент - Википедия. [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/ Метод_главных_компонент.

9. Распознавание лиц [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/Распознавание_лиц.

10. Семь методов двухфакторной автентификации [Электронный ресурс]. – Режим доступа: http://www.infosecurityrussia.ru/news/29947.

11. Тихонов И.А. Информативные параметры биометрической автентификации пользователей информационных систем 2010. № 9. С. 26-32.

12. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - Феникс, 2008 г.

13. Face Recognition. [Электронный ресурс]. - Режим доступа: https://play.google.com/store/apps/details?id=com.vinisoft.facesdk.demo&hl=ru.

14. Hyvdrinen A, Karhunen J., and Oja E., Independent Component Analysis, A Volume in the Wiley Series on Adaptive and Learning Systems for Signal Processing, Communications, and Control. — John Wiley & Sons, Inc., 2001.

15. Muresan D. D., Parks T. W., Adaptive Principal Components and Image Denoising, in: Image Processing, 2003, Proceedings 2003 IEEE International Conference on Image Processing (ICIP), 14-17 Sept. 2003, V. 1, pp. I-101-104

16. Rao, K., Yip P. (eds.), The Transform and Data Compression Handbook, CRC Press, Baton Rouge, 2001.

17. Scholz M., Fraunholz M., Selbig J., Nonlinear Principal Component Analysis: Neural Network Models and Applications, In: Gorban A. N. et al (Eds.), LNCSE 58, Springer, 2007 ISBN 978-3-540-73749-0

18. Zinovyev A., Cluster structures in genomic word frequency distributions, 14- 17 Sept. 2003, V. 1, pp. I-101-104.