Проблеми надійності та безпеки системи контролю доступу на основі біометрії

Дмитро Піддубний, студент [1], ORCID: 0009-0008-0405-1928,
Ольга Ізмайлова, канд.техн.наук, доц.[1], ORCID: 0000-0002-2905-1827.

[1] *Київський національний університет будівництва і архітектури, Київ, Україна*

АНОТАЦІЯ

У роботі виділено основні проблеми надійності біометричних систем контролю доступу, серед яких якість зчитування біометричних даних, похибки ідентифікації, зміни фізіологічних характеристик користувачів з часом, а також збої в роботі обладнання. Крім того, проаналізовано загрози безпеки: підробку біометричних даних, атаки на програмне забезпечення, компрометацію баз даних, соціальну інженерію та уразливості каналів передачі даних.

Ключові слова: біометрія, система контролю доступу, FAR, FRR,EER, підробка, загроза, користувач.

1. ВСТУП

На сьогодні системи контролю доступу відіграють ключову роль у забезпеченні безпеки інформації. Методи аутентифікації, засновані на паролях або смарт-картках, мають суттєві недоліки: можливість втрати, крадіжка чи підбір даних для доступу. Біометричні технології є альтернативою, яка базується на унікальних фізіологічних та поведінкових характеристиках людини. Перевага систем контролю доступу, що базуються на біометричних методах, полягає у високій стійкості до підробок та неможливості передачі ідентифікатора третім особам.

2. МЕТА РОБОТИ

Кожна біометрична ознака має свої особливості впровадження та специфічні проблеми безпеки, проте існують і загальні недоліки, притаманні більшості біометричних систем контролю доступу. Робота присвячена вивченню проблем надійності та безпеки біометричних систем контролю доступу, основних загроз їх функціонування та аналізу можливих помилок з метою подальшого удосконалення цих систем.

3. ОСНОВНІ ВИЗНАЧЕННЯ

Система контролю доступу (СКД) – це комплекс технічних та програмних засобів, які призначені для управління та обмеження доступу до приміщень, інформаційних ресурсів чи інших об’єктів які потребують захисту.

Біометрія – це технологія, яка використовує фізіологічні або поведінкові характеристики людини для її ідентифікації та аутентифікації особи.

Біометричні системи контролю доступу – це системи надання доступу, які здійснюють ідентифікацію або верифікацію користувача за допомогою однієї або декількох різних біометричних ознак.

Ідентифікація – це процес встановлення особи серед усієї бази зареєстрованих користувачів.

Верифікація – це процес підтвердження відповідності між біометричною ознакою, яку надає користувач та біометричним шаблоном, який зберігається в базі.

FAR (False Acceptance Rate) – це показник помилкового прийняття, тобто надання доступу неавторизованим користувачам.

FRR (False Rejection Rate) – це показник помилкового відхилення, тобто ймовірність відмови в доступі легальному користувачу.

EER (Equal Error Rate) – це точка рівноваги між показниками FAR та FRR, в якій вони мають однакове значення. EER використовується для оцінки ефективності біометричної системи.

4. ПРОБЛЕМИ НАДІЙНОСТІ БІОМЕТРИЧНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1. **Якість зчитування біометричних даних**. Сканери що зчитують біометричні дані особи можуть некоректно розпізнавати користувача через ряд факторів, таких як: пошкодження шкіри пальців, забруднення сенсора, вплив навколишнього середовища, освітлення тощо. Некоректне зчитування біометричної ознаки призводить до проблем з доступом, або навіть відмові в доступі.

2. **Похибки ідентифікації.** Існує два ключових показника ефективності біометричної системи, це показник FAR та FRR. Баланс між цими двома показниками впливає на зручність користування системою та на надійність роботи системи.

3. **Вплив часу та зміна біометричних характеристик.** Біометричні характеристики людини, які вважаються унікальними та відносно стабільними протягом життя, насправді схильні до поступових змін під впливом фізіологічних, медичних та зовнішніх чинників. Наприклад, відбитки пальців можуть втрачати чіткість через старіння шкіри, зниження еластичності епідермісу, формування зморшок чи мікропошкоджень. Додатковими факторами є фізична праця, травми, хімічний вплив, які здатні призвести до порушення рисунку папілярних ліній.

У випадку інших біометричних методів спостерігаються аналогічні проблеми: зміна тембру голосу, зниження точності розпізнавання обличчя через появу зморшок чи зміну міміки, варіації у формі райдужної оболонки через офтальмологічні захворювання тощо. Ці зміни знижують стабільність біометричних ознак, що призводить до зростання показника FRR. Таким чином, фактор старіння та біологічна мінливість потребують врахування при проектуванні алгоритмів адаптивної ідентифікації та регулярного оновлення біометричних шаблонів у системі.

4. **Збої в роботі обладнання.** Функціонування біометричних систем значною мірою залежить від технічної справності сенсорів та обчислювальних модулів. Біометричні датчики є високочутливими пристроями, що можуть зазнавати впливу зовнішніх факторів:

- механічні пошкодження;
- електромагнітні завади, які порушують роботу електронних схем і призводять до некоректного зчитування сигналу;

- нестабільність живлення, що може спричинити втрату даних, зависання або помилки в алгоритмах обробки.

Збої обладнання безпосередньо впливають на FAR та FRR, викликаючи як помилкові відмови у доступі, так і несанкціоновані пропуски. В умовах критичної інфраструктури (банківська сфера, державні установи, військові об'єкти) навіть короткочасний збій може призвести до значних ризиків безпеці. Тому технічна надійність сенсорів має оцінюватися на етапі впровадження СКД, а експлуатація повинна супроводжуватися регулярним технічним обслуговуванням, калібруванням обладнання та резервуванням системних компонентів.

5. ПРОБЛЕМИ БЕЗПЕКИ БІОМЕТРИЧНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1. **Загроза підробки біометричних даних.** Однією з найсерйозніших вразливостей біометричних систем є можливість обману сенсора шляхом використання штучних біометричних зразків. Наприклад, для сканерів відбитків пальців зловмисники можуть виготовити фальшиві копії з силікону. Такі зразки здатні відтворювати рельєф папілярних ліній і в окремих випадках успішно проходять аутентифікацію.
2. **Атаки на програмне забезпечення.** Програмні модулі біометричних систем, які здійснюють обробку, нормалізацію та порівняння біометричних шаблонів, є потенційними об'єктами атак. Зловмисники можуть модифікувати алгоритми розпізнавання, підмінювати вхідні дані або впроваджувати шкідливе програмне забезпечення. Прикладом є атаки повторного відтворення, коли попередньо записані біометричні дані повторно подаються в систему з метою обходу автентифікації. Така уразливість особливо небезпечна для систем, що не використовують криптографічний захист або контроль цілісності програмного коду.
3. **Компрометація бази даних.** Бази даних, у яких зберігаються біометричні шаблони користувачів, становлять стратегічну ціль для кібератак. На відміну від паролів чи смарт-карт, які можна змінити у випадку компрометації, біометричні ознаки є незмінними протягом життя. Викрадення таких шаблонів створює довготривалу загрозу, адже один і той самий зразок може використовуватися зловмисниками для генерації підробок у різних системах. Тому компрометація бази біометричних даних має більш критичні наслідки, ніж витік традиційних реквізитів автентифікації.
4. **Соціальна інженерія.** Біометричні системи, навіть за високого рівня технічного захисту, залишаються вразливими до методів психологічного впливу. Зловмисники можуть примушувати користувача надати доступ шляхом шантажу, фізичного тиску або маніпуляцій.
5. **Вразливість каналів передачі даних.** Передача біометричних даних між сенсором, контролером і сервером є критичною ланкою системи. У випадку використання незахищених каналів існує загроза їх перехоплення або модифікації в процесі передачі (атаки типу Man-in-the-Middle). Зловмисники можуть впроваджувати підроблені пакети з біометричними шаблонами або здійснювати ін'єкцію даних для обходу аутентифікації. Відсутність криптографічного шифрування та механізмів автентифікації каналів передачі значно підвищує ризики компрометації системи.

6. ШЛЯХИ ПІДВИЩЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ БІОМЕТРИЧНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Розглянуті вище проблеми надійності та безпеки біометричних систем є визначальними факторами під час прийняття рішення щодо вибору конкретної біометричної ознаки для побудови системи контролю доступу. Однак для підвищення загальної ефективності та мінімізації ризиків необхідно застосовувати додаткові підходи.

1. Використання багатофакторної аутентифікації. Найвищим рівнем захисту є забезпечення системи багатофакторної аутентифікації, що поєднує біометрію з традиційними методами — паролями, смарт-картами, токенами чи одноразовими кодами. Це дозволяє створити багаторівневий бар'єр: навіть у випадку компрометації біометричних даних зловмисник не зможе отримати доступ без додаткового фактора. Такий підхід особливо актуальний для критично важливих об'єктів та банківської сфери.
2. Політики доступу та аудит. Забезпечення безпеки біометричних систем неможливе без організаційних заходів. Запровадження багаторівневих політик доступу дозволяє розмежувати права користувачів, мінімізуючи ризики зловживань. Регулярний аудит системних журналів, контроль дій адміністраторів та застосування принципу найменших привілеїв знижують вірогідність внутрішніх загроз.
3. Криптографічний захист. Збереження та передача біометричних шаблонів повинні супроводжуватися криптографічним захистом. Найбільш поширеними підходами є використання AES (Advanced Encryption Standard) для шифрування баз даних та TLS (Transport Layer Security) для захищеної передачі даних мережею

7. ВИСНОВОК

Біометричні системи контролю доступу є одним із найбільш перспективних напрямів забезпечення кібербезпеки завдяки унікальності фізіологічних характеристик людини. Проте вони не є повністю захищеними від технічних збоїв та кіберзагроз. Для забезпечення високої надійності та безпеки необхідно поєднувати сучасні технологічні рішення, криптографічний захист і багаторівневі методи аутентифікації. Подальші дослідження повинні бути спрямовані на вдосконалення захисту на основі різних біометричних ознак, підвищенню точності ідентифікації та мінімізацію ризиків компрометації біометричних даних.

Список літератури

[1] Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. / В. П. Захаров, В. І. Рудешко. – Львів: 2015. – 492 с.

[2] О. Петров, В. Кузнецов Біометричні технології в системах інформаційної безпеки: навч. посібник /. – Київ: КНУ, 2020.