УДК

О. Р. Демедюк

ПОРІВНЯННЯ МЕТОДІВ ЗАХИТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ ІДЕНТИФІКАЦІЇ

Вінницький національний технічний університет

Анотація

Проаналізовано методи захисту персональних даних від несанкціонованого доступу за допомогою ідентифікації користувачів.

Ключові слова: безпека життєдіяльності, персональні дані, користувач, біометрична ідентифікація, голосова ідентифікація, несанкціонований доступ.

Abstract

Methods of protection of personal data from unauthorized access by identification of users was analyzed.

Keywords: life safety, personal data, user, biometric identification, voice identification, unauthorized access.

Вступ

Сучасна концепція безпеки життєдіяльності в Україні базується на досягненні допустимого ризику, а не недосяжної абсолютної безпеки. Її сутність полягає у прагненні створити такий малий ризик, який сприймає суспільство у певний час, виходячи з рівня життя, соціально-політичного та економічного становища, розвитку науки та техніки. Безпека ж інформації, а особливо персональних даних сьогодні потребує максимального захисту.

Існує велика кількість технічних, інженерних, криптографічних та організаційних методів захисту інформації. Автентифікація користувачів є невід'ємною частиною будь-якої політики безпеки, метою якої є захист від несанкціонованого доступу до даних шляхом підтвердження особи користувача. Існують різні способи здійснення автентифікації, серед яких введення користувачем паролів доступу, PIN кодів, маркерів доступу, методи біометричної автентифікації, тощо.

У зв'язку зі збільшенням кількості потоків інформації, які потребують надійного та ефективного захисту від, в першу чергу, несанкціонованого доступу, виникла потреба в системах ідентифікації користувачів персонального комп'ютера. На сьогоднішній день не існує простих у використанні та максимально ефективних способів, які могли б абсолютно точно розпізнати користувача, який знаходиться за комп'ютером. Саме тому є потреба у розробці ефективного методу автентифікації користувача задля захисту персональних даних від несанкціонованого доступу.

Результати дослідження

Автентифікація – це процес розпізнавання користувача системи і надання йому певних прав та повноважень.

Методи автентифікації умовно можна поділити на однофакторні та двофакторні. Однофакторні методи в свою чергу діляться на:

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

2) ідентифікаційні (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, смарт-карта, штрих-кодова карта тощо);

3) біометричні (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя). [1]

Надійна ідентифікація і автентифікація уповільнюється низкою принципових причин. По-перше, комп'ютерна система ґрунтується на інформації в тому вигляді, в якому вона була отримана; строго кажучи, джерело інформації залишається невідомим. По-друге, майже всі автентифікаційні відомості можна почути, вкрасти чи підробити. По-третє, є протиріччя між надійністю автентифікації з одного боку, і зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки

необхідно з певною частотою просити користувача повторно вводити автентифікаційну інформацію (адже на його місце могла сісти інша людина), але це а це підвищує вірогідність підглядання за введенням. По-четверте, чим надійніший засіб захисту, тим він дорожчий.

Найбільш поширеним засобом автентифікації є паролі. Система порівнює введений і раніше заданий для даного користувача пароль; у разі збігу справжність користувача вважається доведеною. Інший засіб, поступово набирає популярність і забезпечує найбільшу ефективність, – секретні криптографічні ключі користувачів. [2]

Необхідно шукати компроміс між надійністю, зручністю, доступністю за ціною адміністрування на ідентифікацію і автентифікацію. Зазвичай компроміс досягається з допомогою комбінування двох перших з вище перерахованих базових механізмів перевірки справжності.

Перелічені заходи доцільно застосовувати завжди, навіть якщо поруч із паролями використовуються інші методи автентифікації, засновані, наприклад, на застосуванні токенів.

Токен – це предмет чи пристрій, володіння яким підтверджує справжність користувача. Токен – це компактний пристрій у вигляді USB-брелока, яке призначений для авторизації користувача, захисту електронного листування, безпечного віддаленого доступу до інформаційних ресурсів, а також надійного зберігання будь-яких персональних даних. Ці пристрої мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT). Розрізняють токени з пам'яттю (пасивні, які лише зберігають, але з обробляють інформацію) і інтелектуальні токени (активні).

Найпоширенішим різновидом токенів з пам'яттю є картки з магнітною стрічкою. Для використання цих токенів необхідно також мати пристрій читання. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих токенів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. [3]

Пристрої контролю біометричних характеристик складні, і недешеві, тому вони як правило застосовуються лише у специфічних організаціях з високими вимогами до безпеки.

Останнім часом здобуває популярність автентифікація шляхом з'ясування координат користувача. Ідея у тому, щоб користувач посилав координати супутників системи GPS (Global Positioning System), що знаходяться у зоні прямої видимості. Оскільки орбіти супутників не завжди стабільні, передбачити які дуже складно, підробка координат виявляється практично неможливою. Нічого не дає і перехоплення координат – вони постійно змінюються. Безперервна передача координат не потребує від користувача будь-яких додаткових зусиль, і тому він може легко багаторазово підтверджувати свою справжність. Апаратура GPS порівняно недорога і апробована, у тому випадку, коли легальний користувач має перебувати у певному місці, даний метод перевірки справжності є досить привабливим.

Біометричні системи ідентифікації включають системи доступу по відбитку пальця, запаху, ДНК, формі вуха, геометрії особи, температурі шкіри обличчя, клавіатурного почерку, відбитку долоні, малюнку вен долоні, структурі сітківки ока, малюнку веселкової оболонки ока, підпису та голосу.

Перевага біометрії полягає в тому, що ці параметри завжди знаходяться при людині, їх не можна забути, втратити, передати комусь, вкрасти і досить важко відтворити.

Принциповий недолік всіх методів біометрії, крім мовного, полягає у сталості використовуваного біометричного коду, тому відбитки пальців або долонь, малюнок райдужної оболонки і риси обличчя незмінні для індивідуума. Цей недолік перешкоджає застосуванню цих методів у випадках, що вимагають особливо високої надійності ідентифікації особистості, оскільки незмінний біометричний код може бути лічений шляхом зловмисного вторгнення в програму розпізнавання. [4, 5]

Пристрої контролю біометричних характеристик складні, і недешеві, тому вони як правило застосовуються лише у специфічних організаціях з високими вимогами до безпеки.

Системи голосової біометрії не вимагають дорогої апаратної підтримки, універсальність полягає в можливості використання як при безпосередньому контакті з реєструючої апаратурою, так і при віддаленому доступі, наприклад, по каналах телефонних дротових або мобільних ліній. Це дає можливість легко адаптувати системи автентифікації на основі голосової біометрії до різних умов використання і сферам застосування. Автентифікація диктора за довільним текстом застосовується в криміналістиці для встановлення належності різних мовних висловлювань одному й тому ж дикторові,

при сегментації записів стенограм або інтерв'ю на ділянки мовлення, що належать кожному з учасників розмови, а також при встановленні особи без зазначення його ідентифікатора серед порівняно невеликої кількості дикторів.

Тому голосова біометрія є перспективним методом верифікації особистості як з точки зору надійності, так і з точки зору широти областей застосування та зручності, оскільки використовувати голосову автентифікацію можна навіть на значній відстані використовуючи телефон. Сьогодні це значно полегшує життя багатьох ділових людей.

Проблема параметризації мовного сигналу в контексті створення автоматичних систем розпізнавання мови (АСРМ) актуальна і потребує вирішення. Аналізуючи сучасні методів параметризації мови, відсоток слів, які вірно розпізнаються, коливається в широкому діапазоні від 20% до 99%. Такий результат вони дають тому, що не враховують безліч факторів, які впливають на зміну вхідних даних голосу диктора. Цього явно недостатньо для створення ефективних АСРМ, в яких максимально припустима помилка розпізнавання не повинна перевищувати 2%. [5]

Висновки

На основі розглянутих методів захисту персональних даних за допомогою ідентифікації користувачів найбільш доступним та ефективним є метод голосового підтвердження дійсності особи. Враховуючи недоліки існуючих методів постала необхідність у розробці нового підходу розпізнавання голосу диктора, що ляже в основі ефективної АСРМ. Розроблений підхід повинний забезпечувати автентифікацію голосу користувача як у тихій так і у шумній місцевості, та можливість розпізнати записаний голос користувача від живого (можна здійснити за допомогою певного словника, що буде використовувати система для створення довільних фраз-ключів), легкість у користуванні системою (невеликі та легкі фрази-ключі). Адже кінцевою метою створення автоматичних систем розпізнавання мови є здатність машини розпізнавати слова в акустичному сигналі з ефективністю, не меншою в порівнянні з аналогічною здатністю людини.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Hautamäki V. Approaching Human Listener Accuracy with Modern Speaker Verification. Interspeech / V. Hautamäki, 2010. – 1476 c.
2. Mak M. Utterance partitioning with acoustic vector resampling for GMM–SVM speaker verification. Speech Communication / M. Mak, 2011.
3. Wang D. Bayes Factor Based Speaker Segmentation for Speaker Diarization. Interspeech / D. Wang, 2010. – 1408 c.
4. Laskowski K. Modeling instantaneous intonation for speaker identification using the fundamental frequency variation spectrum / K. Laskowski. – M.: Proc. Internat. Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2009), Taipei, Taiwan, April 2009.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин – М.: ДМК Пресс, 2012. – 592 с.

Демедюк Олександра Русланівна — студентка групи 2УБ-13б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: lexa_333@mail.ru.

Науковий керівник: Кобилянська Ірина Миколаївна – канд. пед. наук, доцент кафедри безпеки життєдіяльності, Вінницький національний технічний університет, м. Вінниця, e-mail: jen4u@mail.ru.

Demediuk Oleksandra R. – Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: lexa_333@mail.ru.

Supervisor: Kobylyanska Irina M. – Cand. Sc. (Ped.), Assistant Professor of Department of Life Safety, Vinnytsia National Technical University, Vinnitsia, e-mail: jen4u@mail.ru.