К.О. Гончаренко
О.В. Волик

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧА ЗА РОЗПІЗНАВАННЯМ ЕЛЕКТРОННОГО ПІДПИСУ

Вінницький національний технічний університет

Анотація

Розглянуто актуальність задачі аутентифікації користувача за допомогою біометричних технологій. Розглянуто найбільш розвинені на даний момент БТ розпізнавання за статичними характеристиками.

Ключові слова: аутентифікація, електронний підпис, біометричні технології.

Abstract

The relevance of the problem of user authentication using biometric technology. Considered the most advanced at the moment BT recognition for static characteristics.

Keywords: authentication, electronic signature, biometric technologies.

Вступ

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні і некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках.

Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є Електронний цифровий підпис (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Огляд існуючих методів

Розпізнавання за відбитком пальця. Для даного методу необхідно отримати зображення папілярного візерунка одного або декількох пальців. Далі це зображення обробляється, в процесі чого знаходяться його характерні особливості, такі як розгалуження, закінчення або перетинання ліній.

Розпізнавання за формою долоні. Даний метод побудований на основі геометрії кисті руки людини. Від користувача отримують кілька силуетів руки за допомогою підсвічувальних діодів, будується тривимірне зображення.

Розпізнавання за райдужною оболонкою ока. Райдужна оболонка ока також є унікальною БХЛ. Для її сканування достатньо портативної камери зі спеціалізований програмним забезпеченням, що дозволяє охоплювати зображення частини обличчя, з якого виділяється зображення ока. З останнього, в свою чергу, виділяється рисунок райдужної оболонки, за яким будується цифровий код для розпізнавання особи, а саме перетворенням кожного пікселя з декартової системи координат у полярну.

Розпізнавання за голосом. Аутентифікація людини за голосом - один з традиційних способів розпізнавання особи. Оскільки цей метод безконтактний і не вимагає від людини особливих зусиль, ведуться роботи зі створення голосових замків і систем обмеження доступу до інформації.

Електронний цифровий підпис

Електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього

набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Програма електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Висновки

Електронний цифровий підпис — це просто термін одного технологічно специфічного типу електронного підпису. Створення цифрового підпису — вельми трудомістке та дороге заняття, що потребує застосування технічних засобів та професійних консультантів, а також окремого законодавчого регулювання.

Так, електронний цифровий підпис створюється внаслідок криптографічної операції з використанням технології PKI2, що гарантує цілісність даних і неможливість відмови від підпису.

Цифровий підпис практично неможливо скопіювати, підробити або змінити. Водночас є безліч видів інших, простіших видів електронного підпису, поданих у формі тексту, цифрового зображення власноручного підпису, «відбитка голосу», символу тощо, які легко підробити і скопіювати. Нецифрові види електронного підпису широко використовуються при спілкуванні за допомогою мережі.

Цифровий підпис використовується з тих самих причин, із яких підписуються паперові документи. Цифровий підпис використовується для автентифікації цифрових відомостей — зокрема шаблонів форм, повідомлень електронної пошти та документів — за допомогою комп’ютерної криптографії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. http://ru.wikipedia.org/wiki/Электронная_цифровая_подпись.
2. "Методы и средства защиты информации" (курс лекций) Беляев А.В.
3. И.Д. Горбенко, С.И. Збитнев, А.А. Поляков Криптографические преобразования в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. науч-тех. сб 2001. Вып. 119. С. 43-50.
4. И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ПОЛЯКОВ, С.И. ЗБИТНЕВ, ПРОТОКОЛЫ – ПРИМИТИВЫ УПРАВЛЕНИЯ КЛЮЧАМИ В ГРУППАХ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Волик Олексій Вадимович — студент групи 2КН-13б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: alex12486@gmail.com

Гончаренко Костянтин Олександдрович — студент групи 1КН-13б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: kostinadress@gmail.com

Науковий керівник – Суприган Олена Іванівна — канд. техн. наук, доцент, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Oleksii Volyk — student of Information Technologies and Computer Engineering Department, 2CS - 13b, Vinnytsia National Technical University, Vinnytsia, e-mail: alex12486@gmail.com

Kostiantyn Honcharenko — student of Information Technologies and Computer Engineering Department, 1CS - 13b, Vinnytsia National Technical University, Vinnytsia, e-mail: kostinadress@gmail.com

Supervisor – Olena Suprygan — Cand. Sc., Assistant Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.