Use of biometric technologies as a protection method of credit union activities

Використання біометричних технологій як спосіб захисту від шахрайства, пов'язаного з діяльністю кредитної спілки

Olga Kovalchuk

Key words:

biometric technologies, verification, identification, credit union, fraud.

Ключові слова:

біометричні технології, верифікація, ідентифікація, кредитна спілка, шахрайство.

Постановка проблеми. В умовах стрімкого розвитку економіки в Україні особливої гостроти набуло шахрайство у сфері фінансових відносин. Надання фінансових послуг на ринку зараз відбувається за активної участі посередників, якими є банківські та різноманітні небанківські фінансові установи, до яких, зокрема, належать і кредитні спілки (далі – КС). Це ставить перед криміналістикою завдання детально проаналізувати випадки шахрайства у сфері фінансових відносин та розробити найбільш сучасні методи захисту інформації.

Віднедавна дедалі більше уваги привертає до себе біометрія як одна з новітніх інформаційних технологій, що визначає розвиток засобів і систем ідентифікації і верифікації громадян, які можна використовувати в різних системах контролю і управління доступом для забезпечення безпеки у державній і приватній сферах. Використання біометричних технологій і є найбільш актуальним напрямом у галузі захисту інформації[1].

Стан дослідження. Проблемам використання біометричних технологій для захисту інформації присвячено достатньо публікацій, зокрема, таких вчених, як В.С. Барсуков, Ю.А. Брюхомицький, О.М. Гречишкіна, Г.А. Двоєносова, О.В. Дубчак, В.П. Захаров, А.І. Іванов, М.Н. Казарин, С.П. Козирев, А.О. Корченко, Г.А. Кухарев, Н.С. Мацьків, К.І. Підгайна, М.О. Полєнніков, В.І. Рудешко, І.В. Урсуленко та ін.

Метою цієї статті є розгляд сучасних тенденцій використання біометричних технологій та можливості їхнього застосування у системі протидії шахрайству, яке вчиняється у сфері діяльності КС.

Виклад основного матеріалу. Надзвичайно складна криміногенна обстановка, що складається в економіці України, не лише перешкоджає нормальному розвитку фінансової системи країни, але й вимагає підвищення ефективності діяльності правоохоронних органів і пошуку найбільш оптимальних підходів до вирішення проблем, що виникають у процесі виявлення та розслідування кримінальних правопорушень у кредитно-фінансовій сфері.

Аналіз судово-слідчої практики, чинного законодавства та спеціальної літератури дає підставу вважати, що вирішення зазначених завдань ускладнюється наявністю таких факторів: 1) недосконалістю банківського та кримінального законодавства; 2) суперечливістю судової практики; 3) відсутністю достатнього досвіду в більшості слідчих і працівників оперативних підрозділів; 4) відсутністю загальних положень методики розслідування цих кримінальних правопорушень, які б знайшли достатнє відображення у науковій літературі; 5) застарілістю існуючих методичних рекомендацій правоохоронних органів тощо.

Згідно зі ст. 190 Кримінального кодексу України (далі – ККУ), шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою[2]. Предметом шахрайства може бути не тільки майно, а й право на таке майно. Для відмежування шахрайства від інших видів по-

[1] Захаров В.П. Тенденції використання в діяльності правоохоронних органів біометричних технологій, які не входять до «трьох великих біометрик» / В.П. Захаров, О.І. Зачек // Науковий вісник Львівського державного університету внутрішніх справ. Серія: юридична. – 2015. – Вип. 2. – С. 286.

[2] Кримінальний кодекс України: чинне законодавство зі змінами та доповненнями на 25 січня 2017 р. – К. : Алерта, 2017. – С. 78.

сягань на власність важливо встановити наявність обману або зловживання довірою. Під обманом розуміється повідомлення неправдивих відомостей або приховування, замовчування певних обставин, повідомлення про які було обов'язковим у даних ситуаціях. Шахрайський обман є таким впливом на поведінку власника майна або особи, що відає майном чи охороняє його, який здатний ввести цю особу в оману щодо добровільних дій із передачі майна винному[3].

Відповідно до чинного законодавства, КС – це неприбуткова організація, заснована з метою задоволення потреб її членів у взаємному кредитуванні та наданні фінансових послуг за рахунок об'єднаних грошових внесків членів КС[4]. Як суб'єкти фінансового ринку, КС надають послуги, які подібні до банківських, а також цілу низку нефінансових послуг, а саме: залучення коштів шляхом прийняття депозитів; надання кредитів усіх видів; надання гарантій за членів спілки; платіжно-розрахункові операції; колективна закупівля необхідних для членів спілки товарів; сприяння бізнесу членів КС; надання певних видів страхових послуг; здійснення контролю за ефективним використанням отриманих фінансово-кредитних ресурсів[5]. Із цього можна зробити загальний висновок, що предметом посягання у злочині, що розглядається, є грошові внески, специфічною ознакою яких є те, що вони належать членам КС. Крім того, КС є юридичною особою, яка має самостійний баланс та банківські рахунки, може укладати договори, набувати майнових та немайнових прав. Їй належить майно, у межах якого кредитна спілка несе відповідальність за своїми зобов'язаннями, тому предметом посягання також може бути майно КС.

Враховуючи вищенаведене, можна стверджувати, що під час діяльності КС можливі факти вчинення шахрайських дій, пов'язаних із наданням фінансових і нефінансових послуг, із метою заволодіння грошовими коштами, які добровільно надаються громадянами-учасниками КС. Тому для захисту від шахрайських дій необхідно використовувати найновіші технології захисту. Найбільш сучасним напрямом є використання біометричних технологій.

Нині системи доступу і захисту інформації, які використовують біометричні технології, за висновками фахівців, є не тільки найнадійнішими, але і найзручнішими для користувачів – не потрібно запам'ятовувати складні паролі, постійно носити із собою смарт-карти або апаратні ключі. Потрібно лише прикласти до сканера палець або руку, підставити для сканування в інфрачервоному промінні око, обличчя, руку або палець, що-небудь сказати, щоб була виконана ідентифікація особи та була надана можливість проходу на територію об'єкта, що знаходиться під охороною, або доступу до комп'ютерних мереж та інформації з обмеженим доступом.

Причини популярності біометричних технологій загальновідомі: їх достатня надійність, безпечність, ефективність і комфортність. На відміну від інших технологій, біометрія працює безпосередньо з людьми й ідентифікує їх індивідуальні ознаки. Порівняно з традиційними, біометричні методи ідентифікації особи мають низку переваг, а саме:

– біометричні ознаки дуже складно фальсифікувати;
– через унікальність біометричних ознак достовірність ідентифікації дуже висока;
– біометричний ідентифікатор не можна забути, як пароль, або втратити, як пластикову картку[6].

Згідно з визначенням Г.А. Двоєносової, біометрія – це наукова дисципліна, що вивчає способи вимірювання різних параметрів людини з метою встановлення подібності або різниці між людьми та виділення однієї конкретної людини з множини інших людей. Слово «біометрія» переводиться з грецької мови як «вимірювання життя»[7].

Методи біометричної автентифікації поділяються на *статичні* та *динамічні*. ***Статичні методи*** біометричної автентифікації ґрунтуються на фізіологічній (статичній) характеристиці фізичної особи, тобто

---

[3] Кримінальне право України: особлива частина : [підручник] / [Ю. Александров, О. Дудоров, В. Клименко та ін.] / за ред. М. Мельника, В. Клименка // Київ. нац. ун-т внутр. справ, Київ. міжнар. ун-т. – К. : Атіка, 2008. – С. 213.

[4] Про кредитні спілки: Закон України від 20 грудня 2001 р. (зі змінами) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2908-14.

[5] Кредитні спілки в Україні: [навч. посіб.] / уклад. О.І. Гриценко, Б.А. Дадашев. – Суми : ДВНЗ «УАБС НБУ», 2011. – С. 56.

[6] Захаров В.П. Використання біометричних технологій в системах захисту інформації правоохоронних органів України / В.П. Захаров, О.І. Зачек // Наукові записки Львівського університету бізнесу та права. – 2013. – Вип. 11. – С. 109.

[7] Двоеносова Г., Двоеносова М. Биометрия как наука, метод и способ документирования / Г. Двоеносова, М. Двоеносова // Журнал «Управление персоналом». – 2009. – № 11. – [Електронний ресурс]. – Режим доступу : http://www.top-personal.ru/issue.html?2039.

унікальній характеристиці, яка надана їй від народження, яка є невід'ємною складовою частиною індивіда і яка не змінюється з часом. Це такі методи, які засновані на розпізнанні:

1) відбитка пальця. В основі цього методу лежить унікальність для кожної людини малюнка папілярних узорів на пальцях. Відбиток, знятий за допомогою спеціального сканера, перетворюється на цифровий код (згортку), і порівнюється зі збереженим контрольним еталонним зразком, який був отриманий раніше. Апаратно-програмна технологія, яка використовує папілярні узори пальців, була, є і залишається найпоширенішою за обсягом продажу на ринку порівняно з іншими методами біометричної автентифікації;

2) форм долоні (геометрія долоні, кисті руки або пальця – використовується в доволі вузькому сегменті ринку). Цей метод ґрунтується на суто індивідуальній геометрії долоні, кисті руки або пальця. За допомогою спеціального пристрою, що складається з камери та декількох підсвічувальних діодів (вмикаючись почергово, вони дають різні проекції об'єкта), вибудовується тривимірне зображення долоні (кисті руки або пальця), за яким формується згортка і відбувається розпізнавання індивіда;

3) малюнка вен на долоні або пальці руки (відповідна технологія стає більш поширеною, але, зважаючи на досить високу вартість необхідного обладнання, поки що незначно поширилася). За допомогою інфрачервоної камери зчитується малюнок вен на лицьовій стороні долоні (кисті руки) або пальця, отримане зображення обробляється, і за схемою розташування вен формується відповідна цифрова згортка;

4) райдужної оболонки ока. Малюнок райдужної оболонки ока є унікальною характеристикою людини, причому для її сканування достатньо портативної камери та спеціалізованого програмного забезпечення, за допомогою яких сканується відповідна частина обличчя і виділяється зображення ока, з якого відокремлюється малюнок райдужної оболонки і формується відповідний цифровий ідентифікаційний код людини. Розповсюдження технології ідентифікації за райдужною оболонкою ока стримувалося патентними обмеженнями фірм-виробників і досить високою ціною необхідного устаткування;

5) сітківки ока. Це спосіб ідентифікації за малюнком кровоносних судин очного дна. Для того, щоб цей малюнок став видимим і його можна було зафіксувати, людині потрібно подивитися на віддалене світлове джерело-цятку, і тоді очне дно, що підсвічується, сканується спеціальною камерою. Нині цей спосіб із низки причин майже не застосовується для ідентифікації;

6) форми обличчя. У цьому методі ідентифікації формується двовимірне або тривимірне зображення обличчя людини. На обличчі виокремлюються контури брів, очей, носа, губ і т. д., вираховується відстань між ними і формується не просто образ обличчя, а ще й велика кількість його варіантів на випадки повороту обличчя або нахилу, а також зміни виразу. Кількість образів формується і записується у базу даних залежно від мети використання цього способу (для автентифікації, верифікації, віддаленого пошуку на великих територіях тощо);

7) за термограмою обличчя, термографією руки або пальця (засновані на використанні цих ідентифікаторів технології застосовуються, в основному, у банківській сфері та не отримали поки що поширення). Основою цього способу автентифікації є унікальність розподілу на кожній частині людського тіла артерій, які забезпечують постачання крові на вибрану ділянку шкіри та формують на ній специфічний тепловий фон. Для отримання термограм використовуються спеціальні камери інфрачервоного діапазону. Цей метод дозволяє розрізнити навіть близнят;

8) ДНК. Переваги цього способу загальновідомі, проте нині методи отримання й обробки ДНК досить трудомісткі й довготривалі (поки що відсутня можливість роботи у режимі реального часу), тому системи, які застосовують цей метод, використовуються тільки для спеціалізованих експертиз;

9) за допомогою інших методів. Окрім наведених методів, існують ще інші унікальні способи – автентифікація за підігтьовим шаром шкіри, за кількістю відібраних для сканування пальців, формою вуха, запахом тіла та низкою інших характеристик. Але головним недоліком усіх цих не дуже поширених способів є те, що автоматичних систем і баз даних для можливого масового розпізнавання індивідів, які використовували б ці ідентифікатори, практично ще не створено. Насамперед це стосується автентифікації за запахом тіла і формою вуха.

Динамічні методи автентифікації ґрунтуються на аналізі поведінкових характеристик особи – особливостей, властивих кожному індивіду під час виконання будь-яких рухливих дій. Вони побудовані на особливостях, характерних для підсвідомих рухів під час відтворення будь-якої дії. Динамічні методи істотно поступаються статичним у точності й ефективності, тому, як правило, використовуються як допоміжні або додаткові. Методи автентифікації цієї групи такі:

1) за рукописним почерком. Як правило, для цього виду автентифікації або ідентифікації фізичної особи використовується її підпис (іноді написання кодового слова). Цифровий ідентифікаційний код формується залежно від необхідного ступеня захисту і наявності необхідного устаткування (графічний планшет, екран кишенькового комп'ютера тощо). Ідентифікація за рукописним почерком буває двох типів:

– за самим підписом, тобто для ідентифікації використовується просто ступінь збігу двох картинок;
– за динамічними характеристиками написання підпису (динаміка підпису), тобто для ідентифікації формується цифрова згортка, в яку входить інформація за безпосередньо часовим режимом підпису, тобто часовими характеристиками ставлення підпису і статистичними характеристиками динаміки натискання на поверхню матеріалу, на якому ставиться підпис;

2) за клавіатурним почерком (динаміка клавіатурного набору). Метод аналогічний попередньому, але замість підпису використовується набір якогось кодового слова (коли для цього застосовується особистий пароль користувача, таку автентифікацію називають двофакторною) і не потребує ззовні жодного спеціального устаткування, окрім переобладнаної і дооснащеної стандартної клавіатури. Основною характеристикою, за якою формується згортка для ідентифікації, є динаміка набору кодового слова;

3) за голосом. Одна з найстаріших технологій, нині її розвиток вийшов на новий рівень, оскільки виникла потреба її більш широкого використання. Існує багато способів формування кодів ідентифікації за голосом, але, як правило, це різні поєднання частотних і статистичних характеристик голосу;

4) за допомогою інших методів. Окрім вищеперелічених найпоширеніших динамічних методів, існують ще такі унікальні способи, як: ідентифікація за рухом губ під час відтворення кодового слова, за ходою, за динамікою повороту ключа в дверному замку тощо[8].

Біометрична система може працювати в двох режимах:

1) верифікації – порівняння біометричних шаблонів. Так перевіряється, чи є людина тим, за кого себе видає. Іншими словами, верифікація ставить питання: «Ви той, за кого себе видаєте?». Відповідь на це питання будь-яка біометрична система надає в режимі верифікації, порівнюючи одного з одним. Користувач вводить своє ім'я, пароль або пін-код, пред'являє електронну картку або іншим способом оголошує системі, хто він. Її завдання в цьому випадку – перевірити правдивість отриманої інформації, тобто звірити відповідність вимірюваної біометричної характеристики записаному раніше шаблону заявленого індивіда;
2) ідентифікації – порівняння одного з багатьма: після «захоплення» біометричних даних триває з'єднання з біометричною базою даних для визначення особистості. Ідентифікація особистості успішна, якщо біометричний зразок уже є в базі даних. Іншими словами, ідентифікація відповідає на питання: «Хто ви?». Відповідаючи на нього, будь-яка біометрична система працює в режимі ідентифікації, порівнюючи одного з багатьма. У цьому випадку користувач «пред'являє біометрику» (обличчя, райдужну оболонку ока, відбиток пальця) сканеру, і завдання алгоритму – прийняти рішення, чи належить користувач до відомих індивідів. Якщо так, то хто він? У цьому випадку вимірюється біометрична характеристика, порівнюється з базою раніше записаних шаблонів усіх «відомих» системі людей[9].

Переваги біометричних систем безпеки очевидні: унікальні людські якості добрі тим, що їх важко підробити, важко залишити фальшивий відбиток пальця за допомогою свого власного або зробити райдужну оболонку свого ока схожою на чиюсь іншу. На відміну від паперових ідентифікаторів (паспорт, водійські права, посвідчення особи), пароля або персонального ідентифікаційного номера (ПІН), біометричні характеристики не можуть бути забуті або втрачені, завдяки своїй унікальності вони використовуються для запобігання крадіжці або шахрайству.

На українському ринку вже присутня пропозиція біометричних пристроїв із програмним забезпеченням для обмеження доступу до комп'ютерних систем, мережних ресурсів і матеріальних об'єктів. Засновані на методах ідентифікації за відбитками пальців, невеликих розмірів, зручні й прості в користуванні, ці системи унеможливлюють неавторизований доступ до підконтрольних ресурсів. Наприклад, у

[8] Біометричні технології в XXI столітті та їх використання правоохоронними органами : [посібник] / В.П. Захаров, В.І. Рудешко. – Львів : Львівський державний університет внутрішніх справ. – 2015. – С. 234–238.

[9] Гнідець Т.Я. Біометрія: сильні та слабкі сторони / Т.Я. Гнідець // Науковий вісник Львівського державного університету внутрішніх справ. Серія: юридична. – 2014. – Вип. 2. – С. 274.

Комерційному Індустріальному Банку для контролю доступу до службових приміщень використовується поєднання традиційних безконтактних карток доступу та пристрою для сканування двох пальців співробітника. Програма порівнює зчитані та збережені дані на чипі карти, що дозволяє зробити неможливим використання викраденої картки[10].

Основна ж слабкість біометрії, на думку фахівців, полягає в тому, що біометричні дані можливо викрасти після їх отримання. Тож можна зробити висновок, що біометричні характеристики добре працюють тільки тоді, коли оператор має змогу перевірити дві речі: по-перше, що біометричні дані отримані від конкретної особи саме під час перевірки; по-друге, що ці дані збігаються зі зразком, який зберігається в картотеці. Якщо система не може цього зробити, вона не буде працювати. Біометричні характеристики є унікальними ідентифікаторами, але питання їх надійного зберігання і захисту від перехоплення, як і раніше, залишається відкритим[11].

Висновки. Біометрія та засновані на її принципах біометричні технології можуть стати ефективним засобом убезпечення власності та захисту особи від шахрайства та інших протиправних дій, що може стосуватися діяльності КС. І хоча міжнародні експерти погоджуються з думкою, що біометричні системи знаходяться в зародковому стані, їх подальше впровадження в різні галузі є актуальним завданням для суспільних інституцій, що зможе забезпечити створення зручних і надійних інструментів як для державного сектору, індустріальних і комерційних структур, так і для громадян держави, ставши засобом подолання багатьох негативних чинників у нашому суспільному укладі.

Анотація

Стаття присвячена дослідженню поняття біометрії, її режимів, класів, основним видам біометричних систем, відомостям про сильні сторони біометрії, її застосування у діяльності кредитних спілок. Проаналізовано питання використання біометричних технологій для захисту від шахрайств, що можуть вчинятися у сфері діяльності кредитних спілок.

Summary

The article is devoted to the study of the concept of biometrics, its modes, classes, the main types of biometric systems, information about the strengths of the biometrics, its use in the activities of credit unions. The questions of use of biometric technologies for protection against fraud, which can be carried out in the field of activity of credit unions, are analyzed.

Використана література:

1. Біометричні технології в XXI столітті та їх використання правоохоронними органами : [посібник] / В.П. Захаров, В.І. Рудешко. – Львів : Львівський державний університет внутрішніх справ, 2015. – 492 с.
2. Бродкевич В.М. Біометрія та захист основних прав людини / В.М. Бродкевич, М.В. Гуцалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – Вип. 23. – С. 293–301.
3. Гнідець Т.Я. Біометрія: сильні та слабкі сторони / Т.Я. Гнідець // Науковий вісник Львівського державного університету внутрішніх справ. Серія: юридична. – 2014. – Вип. 2. – С. 273–282.
4. Двоеносова Г., Двоеносова М. Биометрия как наука, метод и способ документирования / Г. Двоеносова, М. Двоеносова // Журнал «Управление персоналом» – 2009. – № 11. – [Електронний ресурс]. – Режим доступу : http://www.top-personal.ru/issue.html?2039.
5. Захаров В.П. Використання біометричних технологій в системах захисту інформації правоохоронних органів України / В.П. Захаров, О.І. Зачек // Наукові записки Львівського університету бізнесу та права. – 2013. – Вип. 11. – С. 108–110.

[10] Бродкевич В.М. Біометрія та захист основних прав людини / В.М. Бродкевич, М.В. Гуцалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – Вип. 23. – С. 300.

[11] Швець В. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації / В. Швець, А. Фесенко // Безпека інформації. – 2013. – Т. 19. – № 2. – С. 102.

6. Захаров В.П. Тенденції використання в діяльності правоохоронних органів біометричних технологій, які не входять до «трьох великих біометрик»/ В.П. Захаров, О.І. Зачек // Науковий вісник Львівського державного університету внутрішніх справ. Серія: юридична. – 2015. – Вип. 2. – С. 285–291.
7. Кредитні спілки в Україні: [навч. посібник] / уклад. О.І. Гриценко, Б.А. Дадашев. – Суми : ДВНЗ «УАБСНБУ», 2011. – 196 с.
8. Кримінальний кодекс України: чинне законодавство зі змінами та доповненнями на 25 січня 2017 р. – К. : Алерта, 2017. – 194 с.
9. Кримінальне право України: особлива частина : [підручник]. / [Ю. Александров, О. Дудоров, В. Клименко та ін.]; за ред. М. Мельника, В. Клименка // Київ. нац. ун-т внутр. справ, Київ. міжнар. ун-т. – К. : Атіка, 2008. – 711 с.
10. Про кредитні спілки: Закон України від 20 грудня 2001 р. (зі змінами) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2908-14.
11. Швець В. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації / В. Швець, А. Фесенко // Безпека інформації. – 2013. – Т. 19. – № 2. – С. 99–111.

Olga Kovalchuk,
Adjunct of the Department of Criminology,
Forensic Medicine and Psychiatry
Lviv State University of Internal Affairs