Umański Państwowy Uniwersytet Pedagogiczny imienia Pawła Tyczyny
NGO „Towarzystwo Pedagogów i Naukowców Ukrainy”

FINANSOWO-ANALITYCZNA GWARANCJA ROZWOJU GOSPODARKI NARODOWEJ

Monografia wieloautorska

Pod redakcją
M. Słatwińskiego

2017

UDK 338.24
F-59

Zespół autorów:

Berżanir A., Berżanir I., Biłoszkurśka N., Biłoszkurśkyj M., Czwertko L., Czyrwa O, Demczenko T., Demjanyszyna O., Kornijenko T., Sawczenko W., Słatwińskyj M. (redaktor), Stojka S.

Zarekomendowano do druku przez Radę Naukową
Umańskiego Państwowego Uniwersytetu Pedagogicznego
imienia Pawła Tyczyny
(protokół nr 4 z dnia 28 listopada 2017 roku)

Recenzenci:

Kurmajew P., doktor nauk ekonomicznych, profesor *(Umański Państwowy Uniwersytet Pedagogiczny imienia Pawła Tyczyny);*
Peńkowa O., doktor nauk ekonomicznych, profesor (*Umański Narodowy Uniwersytet Sadownictwa*);
Sus T., kandydat nauk ekonomicznych, docent *(Przykarpacki Uniwersytet Narodowy imienia Wasyla Stefanyka).*

F-59 **Finansowo-analityczna gwarancja rozwoju gospodarki narodowej**: monografia wieloautorska / [Słatwińskyj M., Czyrwa O., Biłoszkurśkyj M. i in.]; pod red. M. Słatwińskiego. – Warszawa: iScience sp z. o. o., 2017. – 218 str.

ISBN 978-83-949403-0-0

W monografii przedstawiono rezultaty badań zespołu profesorów i wykładowców Katedry Finansów, Rachunkowości oraz Bezpieczeństwa Ekonomicznego Umańskiego Państwowego Uniwersytetu Pedagogicznego imienia Pawła Tyczyny w zakresie „Problemów finansowych gwarancji rozwoju gospodarki oraz sfery społecznej" (numer w rejestrze państwowym 0116U000117).

Potwierdzono założenia teoretyczne oraz opracowano praktyczne rekomendacje dotyczące udoskonalenia narzędzi finansowo-analitycznej gwarancji rozwoju gospodarki narodowej. Przeprowadzono diagnostykę ekonomiczną współczesnego stanu kształtowania zasobów finansowych w gospodarce Ukrainy, dokonano monitoringu pozostałych kierunków polityki finansowej państwa oraz zaproponowano sposoby optymalizacji wykorzystania narzędzi finansowo-analitycznej gwarancji rozwoju gospodarki narodowej. Szczególną uwagę poświęcono opracowaniu odpowiednich przedsięwzięć w sferze polityki fiskalnej oraz inwestycyjnej, inwestycji giełdowych, udoskonaleniu narzędzi do stymulacji rozwoju rynku funduszy oraz ubezpieczeń w gospodarce państwowej, tworzeniu warunków bezpiecznego funkcjonowania sfery finansowej.

Poleca się Czytelnikom, którzy interesują się zagadnieniami z zakresu ekonomii, uczonym, specjalistom, doktorantom, wykładowcom oraz studentom.

ISBN 978-83-949403-0-0

2.2. Podniesienie poziomu bezpieczeństwa finansowo-ekonomicznego banków poprzez wprowadzenie nowoczesnych technologii ochrony

2.2. Підвищення рівня фінансово-економічної безпеки банків шляхом впровадження новітніх технологій захисту

Дослідивши ринок новітніх технологій та інноваційних ідей, виокремимо ті інновації, впровадження яких можна було б розпочати в Україні та отримати неймовірно позитивні результати.

Банки ділового району Лондона Сіті проводять випробування нової системи ідентифікації клієнта – порівняння зовнішності клієнта з його фотографіями в соціальних мережах.

Відповідну програму під назвою Perceive, що використовує біометричні параметри для авторизації, розробили фахівці з компанії Socure, що базується в Нью-Йорку. Система оцінює зображення, зняте клієнтом на смартфон, і визначає його особу. А для додаткової перевірки використовує його профілі в соцмережах типу Facebook, Twitter і LinkedIn. Після перевірки система або схвалює платіж, або включає сигнал тривоги.

У компанії Socure відзначили, що дану технологію в рамках боротьби з шахрайством по картах вже використовують кілька американських банків – правда, поки на рівні тестування.

Які саме лондонські банки будуть використовувати дану біометричну систему безпеки, поки не відомо, оскільки публічних заяв вони не робили.

За даними Британського статистичного управління (Office for National Statistics), в минулому році в країні було

зафіксовано 5,1 млн випадків фінансового шахрайств в онлайн-операціях.

Раніше MasterCard оголосив про запуск тестування системи використання відбитків пальців і селфі для підтвердження онлайн-платежів. Тестування пройде в деяких країнах Європи і в США.

Деякі американські банки почали використовувати новий спосіб верифікації клієнтів: тепер замість паролів і підписів для підтвердження операції досить зробити селфі на смартфон.

Першим серед американських фінансових інститутів, що запропонували своїм клієнтам встановити на смартфон спеціальний додаток, що дозволяє використовувати селфі для ідентифікації при здійсненні банківських операцій, став USAA. Цей банк запустив даний сервіс в тестовому режимі ще в грудні минулого року. А вже з січня 2015 понад 100 тис. клієнтів кредитної організації у Флориді змогли скористатися новою послугою. Глава служби безпеки USAA Гарі Макалум розповів, що клієнт для своєї ідентифікації і проведення операції по рахунках повинен просто запустити відповідний додаток на мобільному телефоні, в меню вибрати «Камеру» і кліпнути один раз. Додаток фіксує особа клієнта, запускаючи процес його розпізнавання. Моргання було додано, щоб уникнути небажаних фотографій, пояснив Макалум.

Інший американський банк – Wells Fargo – став пропонувати своїм клієнтам робити селфі очей. Замість паролів і підписів клієнти кредитної організації можуть встановити на свої смартфони спеціальний додаток Eye Verify, яке вивчає структури склери і зіниці ока клієнта, звіряє з заведеними в базу даними і верифікує людину при здійсненні банківських операцій. Головне, не відсувати камеру смартфона занадто далеко, більш ніж на 8 дюймів.

Ізраїльські винахідники також нещодавно запропонували використовувати селфі для ідентифікації клієнта при здійсненні ним банківських операцій. Американці вважають, що в 2015 році можна буде спостерігати різке зростання попиту на такі мобільні додатки в США. Британський банк Halifax проводить випробування нової системи ідентифікації своїх клієнтів за допомогою моніторингу серцебиття, який дозволяє вкладникам отримувати доступ до свого рахунку без введення додаткових кодів і паролів. Експеримент банку ґрунтується на тому факті, що малюнок серцевого ритму у кожної людини так само індивідуальний, як відбитки пальців або райдужна оболонка ока. Для його визначення клієнтів банку забезпечать спеціальним браслетом, який буде з'єднуватися з домашнім комп'ютером носія і підтверджувати його особу, відкриваючи доступ до здійснення банківських операцій онлайн.

В'єтнамський об'єднаний експортно-імпортний комерційний банк Eximbank почав встановлювати на території країни біометричні банкомати. Ідентифікація клієнтів таких банкоматів здійснюється за відбитками пальців.

Користувачі банкоматів Eximbank позбавлені від необхідності запам'ятовувати і вводити PIN-код до своїх карт. Будь-які операції з коштами на поточному рахунку здійснюються за допомогою дотику пальця. Втім, враховуючи заклопотаність клієнтів тим, що нововведення може породити сплеск злочинності, адміністрація Eximbank зазначає, що сканери відбитків пальців здатні визначити, чи жива рука, після прикладання білої тканини до датчиків, і не дадуть доступ до фінансових операцій, якщо палець відтятий.

Однак, безпека ідентифікації по відбитку пальця нещодавно була скомпрометована. Дослідницька компанія SRLabs легко обійшла сканер відбитків пальців смартфона

Samsung Galaxy S5, використовуючи копію відбитка і тонер. Фахівці SRLabs відзначають, що простота злому є досить серйозною загрозою для користувача даних, адже компанія Samsung вирішила використовувати відбитки пальців для захисту інформації в системі платежів PayPal. Таким чином, викравши телефон і зламавши його сканер, злочинці мають змогу заволодіти всією інформацією з карток, тим самим безпроблемно робити покупки, а також пересилати куди завгодно кошти без відома і згоди реального власника. Ситуація ускладняється і через те, що смартфон не вимагає паролю після перезавантаження – вся безпека мобільного пристрою та збережених на ньому даних залежить виключно від сканера, який вдалося зламати за кілька хвилин.

Отже, новітні технології біометричної ідентифікації за рисами обличчя, відбитками пальців, даних кисті руки та серцевого ритму мають реальну основу для впровадження в банківські системи різних країн світу. Проходячи тестування, новинки вражають рівнем швидкості обробки інформації, надійності та захисту даних і коштів клієнта від протиправних посягань.

Біометричні системи на даний час формують нове покоління інформаційної безпеки. При визначенні біометрії (Biometrics) розуміємо технологію ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу тощо) для ідентифікації [12, с. 87].

Для банківської системи запровадження біометричних даних, як засобу ідентифікації, стане форпостом формування цілісної банківської системи захисту. Адже традиційним системам першого покоління притаманні такі ознаки, як однозначність та постійність ідентифікаційного параметра, у систем нового покоління якими є біометричні системи

параметри залежать від багатьох чинників та завжди змінні. В традиційних системах (ПІН-код, магнітна картка), доступ може бути виконаний будь-ким, оскільки система очікує наявність правильного коду, а не конкретної особи. Відтак втрата чи викрадення ключа дає можливість отримання несанкціонованого доступу до даних. Відсутність даного недоліку в біометричних системах надає ряд суттєвих переваг, оскільки використовуються унікальні ідентифікатори, притаманні конкретній особі. Алгоритм ідентифікації для систем першого покоління зазвичай набагато простіший ніж для біометричних систем ідентифікації.

У зв'язку із розвитком та поширеністю біометричних технологій, їх почали активно використовувати в багатьох сферах пов'язаних із захистом доступу до конфіденційної інформації, до матеріальних цінностей, при перетині державного кордону і т. п. Біометричні технології широко використовуються в області безпеки банківських оборотів, інвестування та інших фінансових траншів, а також роздрібній торгівлі, охороні правопорядку, питаннях охорони здоров'я, останнім часом активно використовуються у сфері соціальних послуг. В недалекому майбутньому біометричні технології відіграватимуть чи не головну роль в багатьох сферах персональної ідентифікації, застосовувані окремо або використовуються спільно зі смарт-картками, ключами та підписами [13].

Як правило, на даний час, найпоширенішими біометричними системами за типом біометричних параметрів є: відбитки пальців, геометрія руки, зображення обличчя, райдужна оболонка ока, дослідження акцентується на методах розпізнавання обличчя.

Розпізнавання за відбитком пальця [13]. 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 (рис. 2.4). Для кожної особливості, крім її типу, запам’ятовуються також відносні розташування та інші параметри, наприклад, для точки закінчення лінії – її напрямок. Сукупність таких даних особливостей та їхніх характеристик утворює шаблон БХЛ.

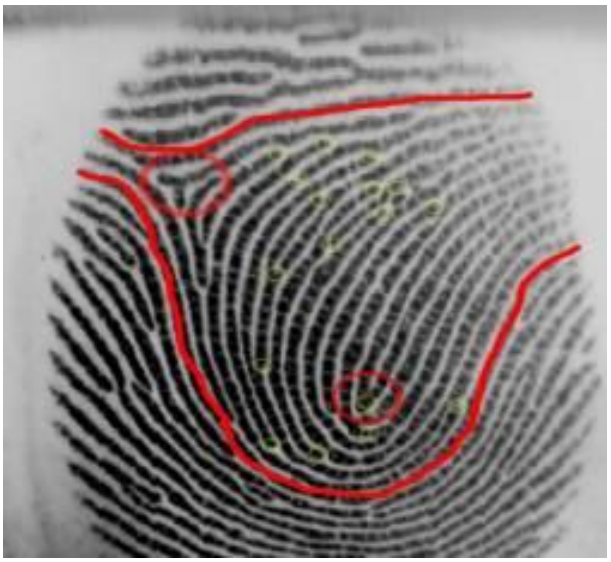

Рис. 2.4. ***Процес дактилоскопічного розпізнавання***
Джерело: [13].

При розпізнаванні особи використовується порівняння одержуваного шаблону відбитку пальця з раніше отриманими. При певному рівні відповідності робиться висновок про ідентичність шаблонів і відбувається верифікація чи ідентифікація представленого відбитка. Цей метод є найбільш поширеним у світі. Він застосовується як у діловому житті, наприклад, доступ до комп’ютерної системи, так і в побуті, наприклад, для дверних замків. Перевагами цього методу є відносна дешевизна та висока ефективність, простота у використані, легкість встановлення, компактність форми. Слід зауважити, що дактилоскопічна ідентифікація за

застосовністю та доступністю з фінансової точки зору перевершує всі інші технології (табл. 2.4).

До недоліків можна віднести недостатню стійкість до підробки відбитку пальця та до дії зовнішніх факторів – забруднення сканера або чистоти пальця.

Таблиця 2.4

Порівняння біометричних методів автентифікації особи

Параметри, що вимірюються	**FRR**	**FAR**	**Вартість (середня)**
Рисунок покровів пальців рук, долонь	0,05	10-6	$200
Рисунок кровоносних судин дна ока	0,01	10-9	$5000
Рисунок кровоносних судин кисті руки	0,05	10-4	$2000
Райдужна оболонка ока	0,05	10-5	$2000
Геометрія руки	0,02	10-3	$500

Джерело: сформовано та проведено розрахунки за даними, наведеними у [22; 25].

Розпізнавання за формою долоні [23]. Даний метод побудований на основі геометрії кисті руки людини. Від користувача отримують кілька силуетів руки за допомогою підсвічувальних діодів, будується тривимірне зображення (рис. 2.5).

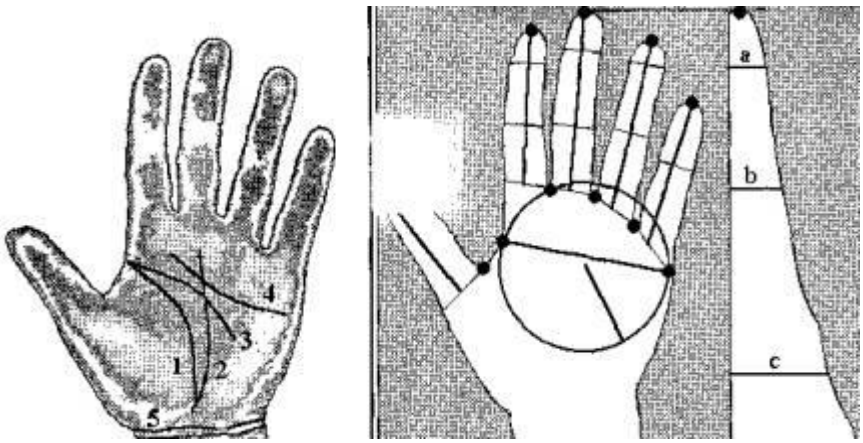

Рис. 2.5. ***Відбиток руки (ліворуч) та 3D-геометрія руки (праворуч)***

Джерело: [23].

Для кожного з них обчислюють вектор значень. Всі вектори ознак однієї людини об’єднуються в окремий клас. Ознаки еталонного образу складають середні значення ознак всього класу, тобто визначають його центр. Вихідні ознаки модифікуються перерахуванням у нові або редукуються скороченням їх кількості. І, таким чином, на основі вибірки утворюється шаблон кисті. Отриманий образ переводиться в клас вихідних або модифікованих ознак при порівнянні з еталоном. Переваги методу: не пред’являються вимоги до чистоти кисті, її температури та вологості. Недоліки: громіздкість пристроїв, невисока стійкість до підробки [22, с. 54].

Розпізнавання за райдужною оболонкою ока [23]. 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 (рис. 2.6).

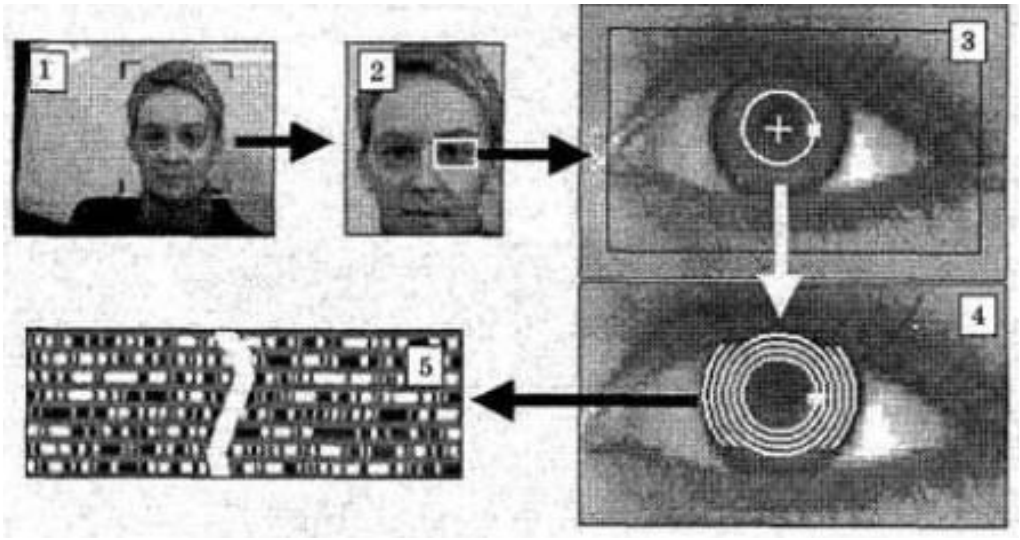

Рис. 2.6. ***Етапи процесу розпізнавання особи за райдужною оболонкою ока***

Джерело: [13].

На цьому етапі може знадобитися інтерполяція зображення, тому що цілочисельні декартові координати не завжди відповідають полярним. Перевагами даного способу є висока ступінь розпізнавання, безконтактний спосіб сканування, невеликий обсяг бази даних, що в принципі є характерним для більшості біометричних систем, та невелика кількість помилок першого і другого роду (табл. 2.4). До недоліків можна віднести високу вартість пристроїв та деякі незручності користувачів, пов’язані з необхідністю зосереджувати погляд.

Розпізнавання за голосом [23]. Автентифікація 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. Інтерес у цій області пов’язаний ще й з прогнозами повсюдного впровадження голосових інтерфейсів. Принцип дії базується на наступному: кожен сплеск голосового сигналу відповідає деякому фрагменту мовлення. Це може бути одна літера, їх поєднання або коротке слово. Після фрагментації слідує оцифрування фрагментів відповідно до частотних показників (рис. 2.7).

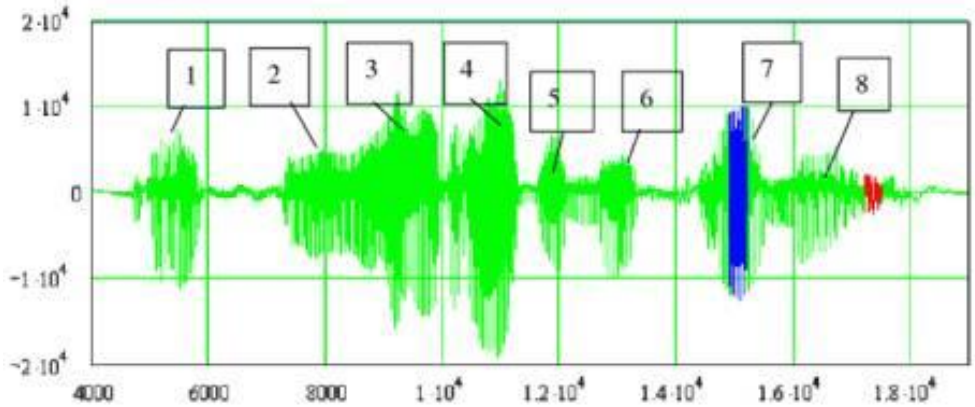

Рис. 2.7. ***Процес розпізнавання особи за голосом***

Джерело: [13].

Переваги методу: звичний для людини спосіб розпізнавання, низька вартість, безконтактність. Недоліки: високий рівень помилок 1-го і 2-го роду, висока чутливість до завад, що викликає необхідність у спеціалізованому звукоізольованому приміщенні для проходження розпізнавання, можливість несанкціонованого перехоплення фрази. Якість розпізнавання залежить від багатьох факторів, таких як інтонація, швидкість мовлення, захворювання та психологічний стан джерела тощо [22, с. 37].

Слід зазначити, що кожний з розглянутих видів біометричної автентифікації характеризується певними особливостями, які залежать від вимог до простоти його використання, вартості та точності методу. Причому точність містить три складові:

- FRR (False Rejection Rate) – коефіцієнт помилкової відмови в доступі – доступ заборонений користувачеві, зареєстрованому в системі; іменується «помилка 1- го роду»;

- FAR (False Acceptance Rate) – коефіцієнт помилкового допуску, ураховує випадки надання системою доступу неавторизованому користувачеві – процентний поріг, що визначає ймовірність того, що один користувач може бути прийнятий за іншого; іменується «помилка 2- го роду»;

- ймовірність того, що система взагалі не зможе прийняти жодного рішення, називається «помилка 3- го роду» [28].

Зазвичай в біометричної системі є певний баланс між помилками першого та другого роду: при зниженні числа хибно-позитивних спрацьовувань зростає ймовірність хибно-негативних і навпаки. Підвищити обидва показники надійності можна тільки принциповим удосконаленням біометричної методики.

Помилки третього роду схожі на помилки другого роду – користувачеві відмовляють в доступі, так як система не змогла його розпізнати. Однак природа цих помилок інша і пов'язана не з вадами алгоритмів розпізнавання, а із зовнішніми причинами. Наприклад, нерозпізнавання особи, яка втратила або з якихось інших причин не змогла пред'явити необхідні для перевірки БХЛ: поріз або опік пальця, нежить тощо.

Усі основні види технологій розпізнавання обличчя розробляються з метою проведення пошуку потрібного суб'єкта в режимі «один до багатьох», тобто ідентифікувати обличчя у базі даних.

Якісні характеристики таких систем залежать від технологічних можливостей відео-камер, які мають розподільну здатність не менше 320x240 пікселів на дюйм при швидкості відеопотоку не менше 3-5 кадрів на секунду та об'єднаних у мережу з персональними комп'ютерами [25, с. 145].

Існують три основні методи розпізнавання обличчя, вони включають аналіз зображень з метою встановлення відмінних характеристик обличчя: а) аналіз «відмінних рис обличчя» – найрозповсюджений та адаптований до змін міміки; б) аналіз на основі «нейронних мереж» – побудований на порівнянні «особливих точок», здатних ідентифікувати обличчя у важких умовах; в) метод «автоматичної обробки зображення обличчя» – визначення відстані та відносин відстані між встановленими особливими рисами обличчя людини [26].

Теоретичні основи методів розпізнавання облич, в силу складності проблеми, включають різноманітні математичні підходи. Серед основних методів розпізнавання облич можна вказати наступні:

Геометричний метод: після одержання картинки, формуються бінарні образи. При роботі з кольоровою камерою перетворення з кольору в чорно-білий колір йде по стандартній формулі Y:=0.3*R+0.59*G+0.11*B. Далі встановлюється деяка порогова оцінка. Якщо значення відтінку сірого вище за поріг, тоді він вважається білим, якщо нижче – вважається чорним. При обчисленні ряду морфометричних ознак, використовуються поняття механіки твердого тіла. Зокрема, це відноситься до довжин осей інерції об'єкта.

Метод головних компонент: один із способів зниження розмірності, що полягає у переході до нового ортогонального базису. Метод головних компонент широко використовується при вирішенні задачі розпізнавання облич на зображенні. Для усього набору зображень облич обчислюються власні вектори. За допомогою обчислених матриць вхідне зображення розкладається на набір лінійних коефіцієнтів, що називаються головними компонентами. Для кожного зображення обличчя обчислюються його головні компоненти. Процес розпізнавання полягає в порівнянні головних компонент невідомого зображення з компонентами усіх інших зображень. Метод на основі перетворення Габора: фільтр Габора – лінійний електронний фільтр, імпульсна перехідна характеристика якого визначається у вигляді гармонійної функції, помноженої на функцію Гауса. Набір фільтрів Габора з різними частотами й орієнтаціями можуть бути корисні для вилучення корисних функцій, з зображення. Фільтри широко використовуються для аналізу образів.

Метод Віоли-Джонса: алгоритм, дозволяє виявляти об'єкти на зображеннях в реальному часі. Запропоновано в 2001 році Paul Viola і Michael Jones. Хоча алгоритм може розпізнавати різні класи зображень, основним завданням при його створенні було виявлення осіб. Існує безліч реалізацій, в

тому числі у складі бібліотеки комп'ютерного зору OpenCV (функція cvHaarDetectObjects).

Всі розглянуті методи біометричної ідентифікації розвивають ідею, спрямовану на комплексний розгляд внутрішніх характеристик біометричних систем та їх зовнішніх проявів, найбільш зримо виявляючи переваги біометрії в порівнянні з іншими технологіями. Перелік цих переваг очевидний: розпізнавання саме людини, а не пароля або матеріального носія; неможливість відмови від дій, підтверджених пред'явленням біометричних ідентифікаторів; є фактом те, що ідентифікатори невіддільні від конкретної особистості і не можуть бути втрачені, викрадені або обмінені. І щоб дане перерахування не залишалося декларацією, розглянемо конкретний приклад того, які наслідки може мати застосування інших технологій.

Аналіз діяльності Жерома Керв'єля, який завдав банку Societe Generale збиток в 5 млрд євро, виявив, що цей трейдер запозичив паролі своїх колег і під їх іменами брав участь у торгах, маніпулював банківською інформаційною системою, видаляючи відомості про проведені транзакції, а потім знову відновлюючи їх. Цими діями список правопорушень Керв'єля не вичерпується, але вже вищевказаного достатньо для того, щоб зробити висновок про серйозні недоліки системи ідентифікації користувачів і управління їх доступом до інформаційних ресурсів [22, с. 59].

Однак бізнес-замовників крім принципових аспектів цікавить ще й економічна віддача від впровадження біометричних систем, і бажано, щоб вона була виражена в конкретних показниках. Для їх визначення часто використовуються методики, засновані на аналізі ROI (Return On Investment – окупність інвестицій), і вже проводяться розрахунки стосовно до біометрії.

За оцінками консалтингової компанії Nucleus Research, що спеціалізується на аналізі окупності інформаційних технологій, впровадження біометричної системи в банках призводить до економії $ 800 за рік на одного співробітника. Спосіб визначення ROI полягає у встановленні розрахункового ефекту, який виражається у зменшенні операційних витрат, збільшенні кількості клієнтів та (або) зростання відвідуваності і т. д. Аналізуючи діяльність біометричних платіжних систем, експерти виявили (згідно з інформацією CNN Money), що застосування біометрії удвічі знижує операційні витрати з обслуговування платежів і на 15% збільшує відвідуваність магазинів, на касах яких діють біометричні банківські термінали [1].

Інтерпретувати показники ROI можна і в термінах ефекту економії часу і зростання продуктивності, точності й прозорості платежів. Прямий взаємозв'язок економії часу та підвищення економічної ефективності простежується і на прикладах використання біометрії для обслуговування клієнтів. Так, вже на перших етапах тестування експлуатації біометричних платіжних терміналів час введення інформації про платника скоротився до 1-2 секунд (при використанні сканера відбитків пальців), і на 30% зросли обороти, які забезпечували згадані біометричні термінали.

Отже, стрімкий розвиток інформаційних технологій, необхідність використання локальних та глобальних мереж зв'язку спричинили зростання уваги до проблем захисту інформації. Переважна більшість систем захисту інформації орієнтовані на використання біометричних ознак. Застосування біометричних ознак для захисту банківських операцій дасть потужний розвиток системі безпеки банку. А це, в свою чергу, призведе до мінімізації різного роду ризиків для фізичних та корпоративних клієнтів та банку загалом.

Отже, в результаті вивчення перспектив використання новітніх технологій для вдосконалення систем захисту банківських операцій сформовані наступні висновки:

1. Здійснивши аналіз теоретичної сутності систем захисту банківських операцій, можна стверджувати, що безпека банківських операцій є малодослідженою вченими-економістами. Більшість інформації про системи захисту банківських операцій можна почерпнути в науково-популярних та публіцистичних статтях, на сайтах банків, але не в наукових авторитетних працях. Загальні висновки та дублювання загальновідомої інформації, закритість більшості інформації та статистики для дослідження безпеки банківських систем є проблемою для розвитку самостійного та ґрунтовного напряму в економічній думці. Правове регулювання безпеки банківських операцій є складовою частиною загального правового регулювання банківської діяльності. В українському законодавстві немає чітких норм, які регламентували б механізми захисту банківських операцій, а поняття, які фігурують в українському законодавстві та пов'язані з банківською сферою, можна трактувати по-різному. Цим користуються багато економічних злочинців, яким вдається легко уникнути правосуддя.

2. В результаті дослідження сучасних методів захисту банківських операцій встановлено, що сучасний розвиток банківських технологій захисту операцій орієнтується на розвиток та вдосконалення ДБО (дистанційного банківського обслуговування). Інтернет-банкінг, СМС-банкінг та інші є новими технологіями, які значно скорочують ризики шахрайства банківських працівників та економлять час, кошти клієнту банку. Банки запроваджують нові технології захисту інформації від зловмисників (ЕЦП – електронний цифровий підпис, та ін.). Але в кожного новітнього методу є

як свої переваги, так і недоліки. Людський фактор є одним з основних чинників, який провокує загрози на банківському ринку. Системи захисту банківських операцій в більшій мірі орієнтовані на інформаційні та комп'ютерні системи. Але найбільший захист своїх фінансів на банківських рахунках може здійснити сама людина, дотримуючись правил безпеки та, будучи уважною й обережною в користуванні своїм банківським рахунком.

3. Провівши пошук шляхів підвищення ефективності та удосконалення системи захисту банківських операцій з картками, виявлено, що стрімкий розвиток інформаційних технологій, необхідність використання локальних та глобальних мереж зв'язку спричинили зростання уваги до проблем захисту інформації. Переважна більшість систем захисту інформації орієнтовані на використання біометричних ознак. Тому ми пропонуємо новий підхід до організації захисту банківських операцій – застосування біометричних технологій задля визначення унікальних ознак людини, які є не піддаються підробці. Впровадження біометричних банкоматів, зчитувачів біометричної інформації при здійсненні банківських операцій, мінімізує ризики, пов'язані з кібератаками, махінаціями з пластиковими картками та підвищить рівень захисту банківської системи загалом. Застосування біометричних ознак для захисту банківських операцій в Україні дасть потужний розвиток системі безпеки банківського сектору, збільшить довіру населення до банківських установ. Впровадження новітніх технологій біометричної ідентифікації за рисами обличчя, відбитками пальців, даних кисті руки та серцевого ритму мають реальну основу для впровадження в банківські системи різних країн світу, зокрема й української банківської системи. Проходячи тестування, новинки вражають рівнем швидкості

обробки інформації, надійності та захисту даних і коштів клієнта від протиправних посягань. А відношення вартості впровадження біометричних систем ідентифікації до їх користі дозволяє нам стверджувати, що біометрична система захисту банківських операцій є ліквідною та прибутковою. Тож, завдяки унікальним та дієвим розробкам, через короткий проміжок часу нас чекає повне переформатування системи безпеки банківських операцій на українському та світовому ринках.

2.3. Sposoby udoskonalenia rachunkowej i analitycznej gwarancji optymalizacji procesów biznesowych przedsiębiorstw przemysłowych

2.3. Шляхи вдосконалення обліково-аналітичного забезпечення оптимізації бізнес-процесів промислових підприємств

Організовуючи будь-яку справу, суб'єкт підприємницької діяльності, звичайно ж, перш за все, ставить за мету отримання прибутку. Для цього він вивчає кон'юнктуру ринку, зважає на наявність попиту того чи іншого товару (робіт, послуг) у регіоні, де буде здійснюватися діяльність, шукає свого клієнта, покупця.

Фармацевтичний бізнес – одна з найприбутковіших сфер діяльності. На аптечний товар завжди і повсюди є попит, адже люди все ж не схильні економити на своєму здоров'ї. Проте фармацевтична фірма повинна ставити за мету не лише отримання прибутку, основним завданням має бути забезпечення населення лікарськими засобами та товарами медичного призначення. Оскільки тут справа стосується охорони здоров'я, то держава здійснює особливий контроль та в якійсь мірі послаблює «податковий тягар» у

Spis tekstów źrodłowych wykorzystanych w rozdziale 2

Список використаних джерел до розділу 2

1. Аналіз окупності біометричних технологій. За даними консалтингової компанії Nucleus Research [Електронний ресурс]. – Режим доступу : http://nucleusresearch.com.
2. Аптечный рынок Украины по итогам 2015 г. : Helicopter View [Електронний ресурс]. – Режим доступа : http://www.apteka.ua/article/358052.
3. Бержанір І. А. Теоретико-методичні аспекти аудиту фінансової звітності суб'єктів господарювання / І. А. Бержанір, Н. І. Гвоздєй, О. А. Демянишина // Економіка. Фінанси. Право. – 2017. – № 2. – С. 7-10.
4. Білошкурська, Н. В. Порівняльний аналіз IPO з іншими інвестиційними джерелами / М. В. Білошкурський, Н. В. Білошкурська // Вісник Київського інституту бізнесу та технологій. – 2017. – № 2(33). – С. 3-4.
5. Білошкурський, М. В. До проблеми економічної діагностики стану розвитку інноваційної діяльності підприємств / М. В. Білошкурський // Соціально-економічні трансформації в умовах глобалізації: світовий та вітчизняний виміри : матеріали міжнародної науково-практичної конференції (м. Херсон, 1-2 березня 2013 р.) ; ред. кол. : К. С. Шапошников [та ін.]. – Херсон : Видавничий дім «Гельветика», 2013. – С. 56-58.
6. Гасюк, Г. Д. Фармацевтичний маркетинг: теоретичні та прикладні засади / Г. Д. Гасюк, Б. П. Громовик, О. Р. Левицька.– Вінниця, 2004. – 204 с.
7. Горбунова, К. Аптеки світу - 2017: перетворення фармринку після кризи [Електронний ресурс] // К. Горбунова / Газета «Аптека. ua-online». – Режим доступу : http://www.br.com.ua/referats/Managment/107719-2.html.
8. Дем'янишина О. А. Бухгалтерський облік як інформаційна підсистема зовнішньоекономічних відносин у системі міжнародних фінансів / О. А. Дем'янишина, О. В. Бутенко // Фінансово-кредитна система: вектор розвитку : збірник

матеріалів ІІ Міжнародної науково-практичної конференції (м. Ужгород, 26 квітня 2017 р.). – Ужгород : Видавництво УжНУ «Говерла», 2017. – С.273-274.
9. Дем'янишина О. А. Удосконалення обліково-аналітичного забезпечення інвестиційно-інноваційного розвитку підприємств харчової промисловості / О. А. Дем'янишина // Адаптивні стратегії розвитку підприємств харчової промисловості в умовах мінливого світу : матеріали наукового симпозіуму з міжнародною участю (19 травня 2017 р., м. Одеса). – 2017. – С. 157-161.
10. Звіт Антимонопольного комітету України за результатами дослідження фармацевтичних ринків за 2016 рік [Електронний ресурс]. – Режим доступу : http://www.amc.gov.ua/amku/doccatalog/document?id=12257.
11. Кірсанов, Д. Бриф-анализ фармрынка: итоги мая 2017 г. [Електронний ресурс] // Д. Кірсанов / Газета «Аптека. ua-online». – 2017. – Режим доступу : http://www.apteka.ua/article/414502.
12. Лисенко, А. М. Застосування біометричних систем для ідентифікації особи / А. М. Лисенко // Вісник Київського нац. ун.-ту ім. Т.Шевченка. Юридичні науки.– 2004. – № 60/62. – С. 87-91.
13. Мицко, А. Є. Програмний сервіс розпізнавання облич з використанням 3D-сенсора Prime Sense Carmine 1.08 [Електронний ресурс] / А. Є. Мицко, Я. С. Парамуд. – Режим доступу : eom.lp.edu.ua/seminar/spr/mytsko.doc.
14. Мнушко, З. Н. Международный маркетинг в фармации : монография / З. Н. Мнушко, Н. В. Чмыхало, Н. М. Мусиенко. - Харьков, 2006. – 344 с.
15. Основи економіки та системи обліку у фармації : [навч. посіб. для студ. вищ. навч. закл.] / [А. С. Немченко, Г. Л. Панфілова, В. М. Чернуха та ін.] ; ра ред. А. С. Немченко. – Харків : Вид-во НФаУ ; Золоті сторінки, 2005. – 504 с.
16. Посилкіна, О. В. Методичні підходи до оцінки інтелектуальних ресурсів у фармації : [наук.- метод. рек.] / О. В. Посилкіна, О. В. Літвінова. – Харкыв : Вид-во НФаУ, 2014. – 34 с.
17. Про бухгалтерський облік та фінансову звітність в Україні / Закон України від 16.07.1999 р. № 996-XIV (зі змінами та

доповненнями). – [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/996-14.
18. Про затвердження переліку наркотичних засобів, психотропних речовин і прекурсорів / Постанова Кабінет Міністрів України від 6 травня 2000 р. № 770 (зі змінами та доповненнями). – [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/770-2000-%D0%BF?lang=uk.
19. Про затвердження Порядку державної реєстрації (перереєстрації) лікарських засобів і розмірів збору за їх державну реєстрацію (перереєстрацію) / Постанова Кабінет Міністрів України від 26.05.2005 р. № 376 (зі змінами та доповненнями). – [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/376-2005-%D0%BF.
20. Про лікарські засоби / Закон України від 04.04.1996 р. № 123/96-ВР (зі змінами та доповненнями). – [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/123/96-%D0%B2%D1%80.
21. Реформування сфери охорони здоров'я в Україні: організаційне, нормативно-правове та фінансово-економічне забезпечення [Електронний ресурс] : аналітична доповідь. – Режим доступу : http://www.niss.gov.ua/content/articles/files/Zdorovya_Popchenko-2a6db.pdf.
22. Романов, В. О. Технології аутентифікації особи за біометричними характеристиками / В. О. Романов, І. Б. Галелюка, П. С. Клочан // Комп'ютерні засоби, мережі та системи. – 2010. – № 9. – С. 54-61.
23. Російський біометричний портал [Електронний ресурс]. – Режим доступу : http://www.biometrics.ru.
24. Федорова, А. Організація та облік аптечної діяльності [Електронний ресурс] / А. Федорова // Аптека.ua. – Режим доступу: http://www.apteka.ua/article/14360/
25. Чередниченко, В. Б. Біометричні методи у системах захисту інформації / В. Б. Чередниченко, К. Е. Чередниченко // Системи обробки інформації. – 2012. – Вип. 4(1). – С. 145-148.
26. Erez, J. Real time vehicle license plate recognition system [Електронний ресурс] – Режим доступу : http:/visl.technion.ac.il/projects/2002 w03(2002).

27. IPO календарь // Фондовый рынок fixygen [Електронний ресурс]. – Режим доступу : http://www.fixygen.ua/calendar/ipo.
28. Marčelja, S. Mathematical description of the responses of simple cortical cells / S. Marčelja // Journal of the Optical Society of America. – 1980. – vol. 70(11). – [Електронний ресурс] – Режим доступу : http://dx.doi.org/10.1364/ JOSA.70.001 297.
29. PwC: IPO Watch Europe 2016 [Електронний ресурс]. – Режим доступу : https://www.pwc.co.uk/audit-assurance/assets/pdf/ipo-watch-europe-annual-review-2016.pdf.
30. PwC: Обзор рынка IPO в Европе во втором квартале 2016 года [Электронный ресурс]. – Режим доступа : http://www.oilru.com/news/524239.