DOI 10.31558/2519-2949.2023.2.15
УДК 339.137.22:355.40

ORCID ID: https://orcid.org/0000-0002-7362-2666
Гунін В. Є., Воєнна академія імені Євгенія Березняка
ORCID ID: https://orcid.org/0000-0002-4222-813X
Смолянюк В. Ф., Воєнна академія імені Євгенія Березняка

БЕЗПЕКА СУБ'ЄКТІВ КОНКУРЕНТНОЇ РОЗВІДКИ ПІД ВПЛИВОМ СУЧАСНИХ БІОМЕТРИЧНИХ СИСТЕМ ІДЕНТИФІКАЦІЇ

У ході дослідження авторами статті вивчено можливості сучасних біометричних систем в провідних країнах світу. Проведено аналіз сучасних форм, методів та процедур опрацювання антропогенних біометричних показників державними органами та приватними структурами іноземної країни для ідентифікації та верифікації осіб за рисами обличчя. Визначено особливості використання правоохоронними органами іноземних країн сучасних біометричних систем ідентифікації за рисами обличчя для встановлення співробітників конкурентної розвідки під час виконання ними фахових завдань.

Дослідження показали, що в умовах глобалізації цифрового простору боротьба з економічними злочинами міжнародного характеру та організованою транснаціональною злочинністю в умовах сьогодення є актуальним питанням стабільності та безпеки для багатьох країн світу сьогодення. В значній мірі, ця боротьба є доволі ефективною завдяки поєднанню інформаційних технологій та біометричних систем на глобальному рівні. У цьому контексті варто відмітити, що правоохоронні органи багатьох країн світу почали успішно впроваджувати в свою практику сучасні біометричні системи ідентифікації та верифікації осіб за їх біометричними даними.

Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. У той же час посилюється небезпека несанкціонованого втручання в роботу інформаційних систем. Наслідки такого втручання дедалі стають непередбачуваними, а їх вагомість останнім часом значно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації закритого характеру та пошуків нових шляхів вирішення цих проблем. У той же час зростають можливості сучасних інформаційних технологій та спеціально навчених професіоналів, здатних отримати доступ до закритої інформації або акумулювати її з відкритих джерел.

Зміна форм і методів ведення іноземними правоохоронними органами своєї роботи завдяки використанню біометричних технологій, обумовлює протиріччя між формами і методами, які на теперішній час використовуються суб'єктами конкурентної розвідки для приховування діяльності її співробітників під час виконання фахових завдань розвідки, та умовами їх здійснення.

Оцінка можливостей сучасних біометричних систем ідентифікації та особливостей їх використання іноземними правоохоронними органами надали авторам статті можливість розробити і запропонувати суб'єктам конкурентної розвідки практичні рекомендації щодо організації протидії сучасним біометричним системам ідентифікації особи за рисами обличчя.

Ключові слова: *країна призначення, політична обстановка, автоматизована інформаційно-пошукова система, візова інформаційна система, єдина біометрична система, машинозчитувальний формат.*

Постановка проблеми в загальному вигляді. В умовах цифрової глобалізації, що створює можливості використання провідними країнами світу сучасних біометричних систем, перед суб'єктами конкурентної розвідки постає проблема безпечного та ефективного виконання фахових завдань.

Використання біометричних систем ідентифікації особи за рисами обличчям дає можливість правоохоронним органам іноземної країни досить легко встановити представника конкурентної розвідки, що перебуває на її території, навіть незважаючи на те, що він буде перебувати на офіційній

посаді, користуватися відповідними документами, що посвідчують його повноваження, зокрема документами, що засвідчують його особу, а також довідками, речами і предметами, які підтверджують його статус відповідно до займаної посади [1, 2].

Щоб забезпечити безпеку професійної діяльності суб'єктів конкурентної розвідки, що виконують професійні завдання на відповідних посадах за кордоном в інтересах національної безпеки в умовах використання іноземними правоохоронними органами біометричних систем ідентифікації особи за рисами обличчя, керівництво державних інституцій та приватних компаній конкурентної розвідки має знайти раціональні шляхи організації адекватної протидії таким системам ще на етапі підготовки її співробітників до виконання фахових завдань.

Результати аналізу нових форм та методів, що використовують іноземні правоохоронні органи для викриття співробітників конкурентної розвідки, вказують на те, що біометричні системи зі штучним інтелектом для розпізнавання особи дають можливість накопичувати й обробляти велику кількість біометричних показників щодо певної категорії осіб [3].

З огляду на це керівництво вищезазначених представництв конкурентної розвідки має визначити, які прийоми, форми і методи доцільно застосовувати для того, щоб протягом тривалого часу їх співробітники не потрапляти в поле зору іноземних правоохоронних органів або інших структур, що представляють загрозу їх діяльності на території країни призначення [4, 5].

Щоб успішно протидіяти сучасним біометричним системам ідентифікації особи за рисами обличчя, потрібно насамперед визначити слабкі місця цих систем, а також виявити недоліки їх використання іноземними правоохоронними органами, що дає співробітникам конкурентної розвідки нові можливості якісно та ефективно вести фахову діяльність на території країни призначення.

Зв'язок проблеми з важливими науковими і практичними завданнями. Обраний напрям дослідження тісно пов'язаний з виконанням положень Указу Президента України від 14 вересня 2020 року № 392/2020 «Про стратегію національної безпеки України», Указу Президента України від 15 жовтня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки», прискорення європейської та євроатлантичної інтеграції нашої країни [6], використання ресурсів конкурентної розвідки для досягнення цієї мети.

Проблеми застосування конкурентної розвідки в комерційній компанії не обмежуються лише забезпеченням інформаційної безпеки її суб'єктів. Важливим для розвідки насамперед є вирішення завдань менеджменту і маркетингу, що забезпечується наступними чинниками:

спостереження за репутацією компанії;

активна участь у формуванні іміджу компанії, інформаційного поля навколо компанії;

відстеження появи нового конкурента, технології або каналу збуту;

виявлення можливих злиттів і поглинань;

оцінка потенційних ризиків при інвестиціях;

випередження кроків конкурентів в рамках маркетингових кампаній;

випередження конкурентів в тендерах;

виявлення каналів витоку інформації.

Конкурентна розвідка як сфера діяльності має здійснюватися в рамках правового поля держави. Основою для цього є конституційні права на пошук, отримання, передачу і використання інформації в усіх цивілізованих державах. Проте на сьогодні між поняттями «конкурентна розвідка» і «промислове шпигунство» поки що проглядається хитка грань, що полягає в легітимності, законності методів і засобів, які використовуються в процесі збору цільової інформації [9]. Методи і способи ведення конкурентної розвідки стають дуже близькими до тих, що використовуються національними спецслужбами в ході проведення традиційної розвідувальної діяльності на території іноземної держави. Таким чином, безпосередньою загрозою професійній діяльності співробітників конкурентної розвідки стають контрзаходи іноземних правоохоронних органів, які широко використовують у своїх цілях сучасні біометричні системи ідентифікації особи. Тож для якісного та ефективного виконання фахових завдань за кордоном співробітники конкурентної розвідки мають навчитися протидіяти таким системам.

Аналіз останніх досліджень і публікацій. Можливості сучасних біометричних систем, що використовують провідні країни світу, розглянуто в [7]. Сучасні методи, форми та процедури опрацювання правоохоронними органами біометричних показників особи визначено в [8]. Особливості накопичення, обробки та використання персональних даних представників силових структур України викладено в [4]. Можливі шляхи та канали витоку інформації щодо співробітників конкурентної розвідки розглянуто в [5]. Проте, сьогодні недостатньо уваги приділено дослідженню

проблеми захисту співробітників конкурентної розвідки, які в ході виконання фахових завдань стикаються з такою небезпекою, як ідентифікація особи за рисами обличчя сучасними біометричними системами.

Метою статті є дослідження можливостей сучасних біометричних систем ідентифікації у провідних країнах світу, розроблення практичних рекомендацій співробітникам конкурентної розвідки щодо організації протидії сучасним біометричним системам ідентифікації особи за рисами обличчя.

Виклад основного матеріалу.

Досліджуючи питання організації ефективної протидії сучасним біометричним системам, потрібно насамперед визначити, які саме загрози фаховій діяльності співробітників конкурентної розвідки становлять зазначені системи.

Що являє собою сучасна біометрія взагалі? Йдеться про ідентифікацію особи за її фізичними характеристиками або поведінковими рисами. Відбитки пальців, сітківка очей, голос і навіть хода – все це є біометричні показники (характеристики, параметри, маркери, тощо). На цей час біометричні системи ідентифікації особи різної складності використовуються майже в усіх провідних країнах світу. Наприклад, технологічний пристрій Touch ID, який встановлено на сучасному iPhone, використовується для біометричного розпізнавання власника цього засобу зв'язку. Така технологія розпізнавання вважається найбільш сучасною, оскільки ідентифікація особистості ведеться за унікальними показниками, які теоретично притаманні лише певній людині [10].

Зрозуміло, що будь-яка система ідентифікації не має жодної цінності, якщо її можна обійти (обманути). Іноді це зробити досить складно. Якщо співробітник конкурентної розвідки намагатиметься досягти результату без сторонньої допомоги, зростає ймовірність того, що адміністративний орган швидко виявить спроби його несанкціонованого доступу до захищеної системи, а під час превентивного службового розслідування стане очевидним, хто намагався дістати доступ до цієї системи. Щоб знизити ризик передчасного потрапляння в поле зору іноземного правоохоронного органу, співробітнику конкурентної розвідки доцільно встановити конфіденційні стосунки з тією посадовою особою режимного об'єкта, яка має офіційний доступ до закритої системи, що цікавить розвідку. Інший варіант: співробітник конкурентної розвідки намагається отримати доступ до закритої системи дистанційно. У такому разі біометричну систему ідентифікації можна обійти за допомогою спеціальних програм та засобів [11].

Сьогодні особливо актуальною стає проблема отримання співробітниками конкурентної розвідки доступу до будь-яких закритих баз даних (систем) як в Україні, так і за кордоном. Її розв'язання дасть можливість розвідникам вносити в разі службової необхідності окремі зміни до біометричних показників на ту чи іншу особу, що зберігаються в базах даних з обмеженим доступом. У цьому контексті співробітник конкурентної розвідки має приділяти особливу увагу прихованому вивченню особливостей використання іноземними правоохоронними органами Єдиної біометричної системи (ЄБС). Зокрема, для отримання доступу саме до цієї системи особа має пройти бімодальну ідентифікацію, тобто ідентифікацію за рисами обличчя та голосом. Слід зазначити, що в більшості країн світу ці дві модальності одночасно не використовуються [11, 12].

Особливості використання іноземними правоохоронними органами сучасних біометричних системи ідентифікації особи за окремими антропометричними даними. У більшості випадків в сучасних біометричних системах використовується одна з двох вищезазначених модальностей, зокрема ідентифікація особи за рисами обличчя або за голосом. Тож спочатку з'ясуємо, що являє собою ідентифікація особи за рисами обличчя.

Для біометрії найбільш надійною є 3D-ідентифікація рис обличчя. Йдеться про фотофіксацію об'ємного зображення обличчя тієї чи іншої людини. Таке зображення можна отримати лише за допомогою камер з достатньо високою роздільною здатністю, однак далеко не всі країни можуть собі дозволити такі камери. Сьогодні залишається невирішеним й інше питання – як працюватимуть біометричні системи ідентифікації за рисами обличчя, якщо обсяг одночасних звернень до них перевищуватиме мільйон і більше за хвилину.

Окремі біометричні системи налаштовані на ідентифікацію особи за райдужною оболонкою її очей. Проте коштує таке обладнання занадто дорого, тому не кожна держава може його придбати. Розробка технологій (алгоритмів) ідентифікації особи за вимірами в інфрачервоному спектрі, зокрема за малюнком вен на щоках, вилицях або в ділянці очей, за реакцією звуження або розширення зіниць на відблиски, особливостями райдужної оболонки очей тощо допоки перебуває

на стадії наукових досліджень. Наразі, щоби обійти зазначену систему, достатньо їй показати, що перед нею жива людина із венами під шкірою обличчя, зіниці ока якої реагують на зміни зовнішнього освітлення. Проблемним для розвідників поки що залишається питання щодо організації протидії біометричним технологіям ідентифікації особи за голосом. Якщо співробітнику конкурентної розвідки потрібно підробити чийсь голос або змінити свій, він має брати до уваги те, що за допомогою сучасних програмних технологій можна здійснювати шумоочищення й відновлювати аудіосигнали, зокрема мовлення [10].

На безпеку діяльності співробітників конкурентної розвідки та організацію адекватної протидії сучасним біометричним системам позитивно впливають такі чинники: багато біометричних систем, що використовують іноземні правоохоронні органи, потребує високої професійної підготовки їх користувачів; ці системи мають певне відставання в інтерфейсі від вимог, що висуваються до сучасних операційних систем; системи мають певні обмеження у виборі типу електронно-обчислювальної техніки, що може працювати тільки в одній операційній системі і тільки з одним видом звукових кварт; під час використання цих систем існують певні обмеження через неможливість їх регулярного технічного супроводження, постійного підтримання в належному стані, оновлення тощо [8].

Для співробітників конкурентної розвідки, звичайно, важливо знати особливості використання адміністративними та правоохоронними органами іноземної країни тієї чи іншої біометричної системи для пошуку та ідентифікації певних осіб, але набагато важливіше досконало вивчити її технічні характеристики. Ці знання допоможуть розвідникам знайти оптимальне рішення, як протидіяти тій чи іншій біометричній системі, зокрема із застосуванням програмних або технічних засобів. Наприклад, провідний американський експерт у галузі створення і розпізнавання діпфейків (відеопідробок) Хао Лі (Hao Li) стверджує, що з початку 2020 року підроблені зображення обличчя вже майже не відрізняються від реальних фотографій та відеозаписів [11]. Тож у разі оперативної потреби співробітнику конкурентної розвідки достатньо завчасно створити діпфейк, що дасть змогу на певний час приховати своє обличчя від правоохоронних органів відповідно до офіційної посади прикриття.

Особливості організації протидії біометричним системам ідентифікації особи за райдужною оболонкою очей. Поки що в сучасних біометричних системах застосовується алгоритм ідентифікації особи за безпосереднім підтвердженням самого факту наявності на обличчі вен під шкірою або реакції зіниць у відповідь на зміни зовнішнього освітлення. Зрозуміло, що обійти таку систему, використовуючи лише звичайну фотографію, буде важко. Більшість сучасних ІТ-компаній велику увагу приділяють розробці алгоритму ідентифікації (аутентифікації) особи за райдужною оболонкою очей. Основний закон діалектики підказує нам, що той, хто щось виробляє, краще за будь кого знає слабкі місця свого винаходу, тому, організувати протидію сучасним біометричним системам буде достатньо легко, якщо співробітник конкурентної розвідки знайде підхід до фахівця, який бере участь у створенні або експлуатації тієї чи іншої системи. Крім того, малюнок райдужної оболонки можна, так би мовити, вкрасти в її власника на відстані, не заглядаючи в його очі. Для цього потрібно мати якісні фотоапарат та 3D-принтер з великими роздільними здатностями. Найпростіший спосіб обійти таку систему – це зробити знімок райдужної оболонки за допомогою цифрової камери в режимі нічної зйомки або видаливши з цієї камери інфрачервоний фільтр. Технічні характеристики такої камери дають змогу на відстані до 5 метрів зробити якісний фотознімок, на якому буде зафіксовано райдужну оболонку очей тієї особи, що становить оперативний інтерес для розвідки [7].

Особливості організації протидії біометричним системам ідентифікації особи за рисами обличчя. Співробітник конкурентної розвідки має усвідомлювати: якщо він коли-небудь потрапляв у поле зору правоохоронного органу іноземної країни, його фотографія може опинитися в накопичувальній базі оперативної інформації. Проте, якщо співробітник конкурентної розвідки зможе внести якомога більше дрібних змін до рис свого обличчя, це набагато ускладнить або навіть унеможливить його ідентифікацію через порівняльний аналіз фотографії «нового» обличчя з тими, що раніше потрапили до оперативних баз. Важливою умовою протидії таким біометричним системам є саме збільшення кількості незначних змін окремих параметрів обличчя на противагу декільком радикальним змінам. Щоб ефективно протидіяти тій чи іншій біометричній системі ідентифікації за рисами обличчя, співробітник конкурентної розвідки насамперед має приховано вивчати новітні досягнення державних та приватних ІТ-компаній, що ведуть розробку та вдосконалення таких систем і водночас тестують їх з метою виявлення слабких місць. Звісно, результати випробувань таких систем на стійкість до впливу сторонніх чинників програмного

або технічного характеру розробники ретельно приховують. Однак відомі випадки, коли за допомогою точної 3-D копії обличчя іншої особи можна уникнути ідентифікації [13]. Наприклад, з'ясувалося, що за допомогою гіпсової копії голови керівника компанії «Bkav», виконаної у форматі 3D, було розблоковано п'ять сучасних моделей смартфонів: «LG G7 ThinQ», «Samsung S9», «Samsung Note 8», «OnePlus 6» и «iPhone X», які було захищено системою розпізнавання за рисами обличчя. Для створення такої 3-D копії варто скористатися фотографіями або відеоматеріалами, які можна дістати в достатній кількості із соціальних мереж. Отже, знаючи можливості цих біометричних систем, співробітник конкурентної розвідки зможе протидіяти навіть мультимодальним біометричним системам ідентифікації обличчя і радужної оболонки очей, що діють одночасно завдяки використанню технічних або програмних рішень [14].

Висновки. Аналіз можливостей сучасних біометричних систем ідентифікації за рисами обличчя вказує на те, що завжди можна підібрати способи та методи ефективної протидії їм. У сучасному цифровому світі біометричні системи анітрохи не безпечніші, ніж класичні коди та паролі. Наприклад, якщо співробітник конкурентної розвідки буде використовувати для входу в цифрову систему спеціальний пароль – число, предмет, умовну фразу, знак, він може добре їх завчити або зберігати у прихованому місці. Дізнатися від розвідника пароль можливо лише в разі застосування сильних психотропних засобів або фізичного впливу. Зазвичай підготовлений розвідник готовий протидіяти усім заходам, що можуть застосовувати іноземні правоохоронні органи. Проблемним питанням для нього є те, як сховати від оточення чи правоохоронних органів свої очі та відбитки пальців, щоб вони не потрапили до накопичувальних баз даних. Звичайно, найпростіший спосіб їх приховати – постійно носити темні окуляри і рукавички, але саме це може привернути увагу оточення. Інша проблема для розвідника – унікальність тієї чи іншої біометричної системи ідентифікації особи, яку використовують іноземні правоохоронні органи для виявлення осіб, що збирають інформацію економічного характеру, виток якої може завдати шкоди інтересам країни призначення. Щоб адекватно протидіяти такій системі, співробітник конкурентної розвідки має постійно вивчати її параметри (характеристики). Наприклад, у разі зламу паролю, яким користується розвідник, він завчасно може передбачити, як можна замінити його іншим у потрібний момент. А чим замінити обличчя співробітника конкурентної розвідки або відбиток його пальця, щоб убезпечити їх потрапляння до баз даних правоохоронного органу? Для цього керівництво суб'єкта конкурентної розвідки насамперед має визначити, які саме показники (риси обличчя) його співробітника могли потрапити до інформаційних баз іноземних правоохоронних органів, ідентифікація яких може призвести до його розкриття під час виконання ним фахових завдань в країні призначення.

Перспективи подальших досліджень. Деталізувати особливості організації протидії біометричним системам ідентифікації особи за відбитками пальців.

Бібліографічний список:

1. Про порядок заповнення машинозчитуваної зони паспортних та візових документів: Постанова Кабінету міністрів України від 28 червня 1997 року № 636. URL: https://zakon. rada.gov.ua/laws/show/636-97-п#Text (2023, березень, 23).

2. Бригинець С. Біометричні дані: збір і захист у Європі, США та Україні. *Юридична Газета*. 2019. № 40 (694). URL: https://yur-gazeta.com/publications/practice/ inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (2023, березень, 25).

3. Біометричний контроль іноземців // WikiLegalAid довідково-інформаційна платформа правових консультацій. URL: https://wiki. legalaid.gov.ua/index.php/ (2023, березень, 27).

4. Персональні дані представників силових структур України. URL: https:// myrotvorets2.org/index.html (2023, березень, 30).

5. У відкритий доступ злили біометричні дані більше мільйона українців. *Новини «То є Львів»*. 2015–2021. URL: https://inlviv.in.ua/ ukraine/u-vidkrytyj-dostup-zlyly-biometrychni-dani-bilshe-miljona-ukrayintsiv (2023, квітень, 03).

6. Питання європейської та євроатлантичної інтеграції: Указ Президента України від 20 квітня 2019 року № 155/2019.

7. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. Львів: ЛьвДУВС, 2015. 492 с.

8. Колотушкин С. М., Лосева С. Н. Биометрические технологии в правоохранительной деятельности: международный и отечественный опыт. *Социально-политические науки*. 2018. № 2. С. 226–228. URL: https://cyberleninka.ru/article/n/biometricheskie-tehnologii-v-pravoohranitelnoy-deyatelnosti-mezhdunaro-dnyy-i-otechestvennyy-opyt (2023, квітень, 06).

9. Ландэ Д. В, Прищепа В. П Школа веб-разведки. Инструменты и источники. *Телеком.* 2007. № 7–8. С. 46–49.

10. Швець В. А., Фесенко А. О. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації. *Ukrainian Scientific Journal of Information Security*, 2013, vol. 19, issue 2. С. 99–111. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/ view/4882 (2023, квітень, 12).

11. Как обмануть системы распознавания лиц. URL: https://www.vedomosti.ru/ technology/articles/2018/03/ 28/755116-obma-ut-sistemi (2023, квітень, 15).

12. Шесть способов защиты от камер видеонаблюдения. URL: https://pramen.io/ru/2016/04/6-sposobov-zashhititsya-ot-kamer-videona/ (2023, квітень, 17).

13. Как затруднить идентификацию, обмануть видеоаналитику и скрыть лицо от камер. URL: https://habr.com/ru/company/ivideon/blog/373255/ (2023, квітень, 19).

References:

1. Pro poriadok zapovnennia mashynozchytuvanoi zony pasportnykh ta vizovykh dokumentiv: Postanova Kabinetu ministriv Ukrainy vid 28 chervnia 1997 r. № 636. URL: https://zakon. rada.gov.ua/laws/show/636-97-p#Text (accessed on: 23/03/2023).

2. Bryhynets S. Biometrychni dani: zbir i zakhyst u Yevropi, SShA ta Ukraini. Yurydychna Hazeta. 2019. № 40 (694). URL: https://yur-gazeta.com/publications/practice/ inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (accessed on: 25/03/2023).

3. Biometrychnyi kontrol inozemtsiv // WikiLegalAid dovidkovo-informatsiina platforma pravovykh konsultatsii URL: https://wiki. legalaid.gov.ua/index.php/ (accessed on: 27/03/2023).

4. Personalni dani predstavnykiv sylovykh struktur Ukrainy. URL: https:// myrotvorets2.org/index.html (accessed on: 30/03/2023).

5. U vidkrytyi dostup zlyly biometrychni dani bilshe miliona ukraintsiv. *Novyny «To ye Lviv»*. 2015–2021. URL: https://inlviv.in.ua/ ukraine/u-vidkrytyj-dostup-zlyly-biometrychni-dani-bilshe-miljona-ukrayintsiv (accessed on: 03/04/2023).

6. Pytannia yevropeiskoi ta yevroatlantychnoi intehratsii: Ukaz Prezydenta Ukrainy vid 20 kvitnia 2019 roku № 155/2019.

7. Biometrychni tekhnolohii v KhKhI stolitti ta yikh vykorystannia pravookhoronnymy orhanamy: posibnyk. 2-he vyd., dop. / V. P. Zakharov, V. I. Rudeshko. Lviv: LvDUVS, 2015. 492 s.

8. Kolotushkyn S. M., Loseva S. N. Byometrycheskye tekhnolohyy v pravookhranytelnoi deiatelnosty: mezhdunarodnыi y otechestvennыi opыt. Sotsyalno-polytycheskye nauky. 2018. № 2. S. 226–228. URL: https://cyberleninka.ru/article/n/biometricheskie-tehnologii-v-pravoohranite lnoy-deyatelnosti-mezhdunaro-dnyy-i-otechestvennyy-opyt (accessed on: 06/04/2023).

9. Landie D. V, Pryshchepa V. P. Shkola veb-razvedky. Ynstrumentы y ystochnyky. Telekom. 2007. № 7–8. S. 46–49.

10. Shvets V. A., Fesenko A. O. Osnovni biometrychni kharakterystyky, suchasni systemy ta tekhnolohii biometrychnoi autentyfikatsii. Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2. S. 99-111. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/ view/4882 (accessed on: 12/04/2023).

11. Kak obmanut systemы raspoznavanyia lyts. URL: https://www.vedomosti.ru/technology/articles/2018/03/ 28/755116-obma-ut-sistemi (accessed on: 15/04/2023).

12. Shest sposobov zashchyty ot kamer vydeonabliudenyia. URL: https://pramen.io/ru/2016/04/6-sposobov-zashhititsya-ot-kamer-videona/ (accessed on: 17/04/2023).

13. Kak zatrudnyt ydentyfykatsyiu, obmanut vydeoanalytyku y skrыt lytso ot kamer. URL: https://habr.com/ru/company/ivideon/blog/373255/ (accessed on: 19/04/2023).

Hunin V. E., Smolianiuk V. F. Security of subjects of competitive intelligence under the influence of modern biometric identification systems

In the course of the research, the authors of the article studied the possibilities of modern biometric systems in the leading countries of the world. An analysis of modern forms, methods and procedures for processing anthropogenic biometric indicators by state bodies and private structures of a foreign country for the identification and verification of persons by facial features was carried out.
The peculiarities of the use of modern biometric systems of identification by facial features by law enforcement agencies of foreign countries to identify employees of competitive intelligence during their professional tasks have been determined.

Studies have shown that in the conditions of globalization of the digital space, the fight against economic crimes of an international nature and organized transnational crime in today's conditions is an urgent issue of stability and security for many countries of the world today. To a large extent, this fight is quite effective thanks to the combination of information technology and biometric systems on a global level. In this context, it is worth noting that the law enforcement agencies of many countries of the world

have begun to successfully implement modern biometric systems of identification and verification of persons based on their biometric data into their practice.

Recently, there have been qualitative changes in management processes in the world, due to the intensive implementation of modern information technologies. At the same time, the danger of unauthorized interference in the operation of information systems is increasing. The consequences of such an intervention are becoming more and more unpredictable, and their importance has increased significantly recently. As a result, in many countries, more and more attention is paid to the problems of protecting information of a closed nature and to the search for new ways of solving these problems. At the same time, the possibilities of modern information technologies and specially trained professionals who can gain access to closed information or accumulate it from open sources are growing.

The change in the forms and methods of conducting their work by foreign law enforcement agencies due to the use of biometric technologies causes a contradiction between the forms and methods currently used by entities of competitive intelligence to hide the activities of its employees during the performance of professional intelligence tasks, and the conditions of their implementation.

The evaluation of the capabilities of modern biometric identification systems and the peculiarities of their use by foreign law enforcement agencies gave the authors of the article the opportunity to develop and offer the subjects of competitive intelligence practical recommendations on the organization of countermeasures against modern biometric systems of facial identification.

Keywords: *country of destination, political situation, automated information search system, visa information system, unified biometric system, machine-readable format.*