УДК 339.137.22:355.40

БАЛІЦЬКИЙ В.В. Воєнна академія імені Євгенія Березняка.
ORCID: https://orcid.org/0000-0003-1272-7920.
ГУНІН В.Є. Воєнна академія імені Євгенія Березняка.
ORCID: https://orcid.org/0000-0002-7362-2666.

ДАКТИЛОСКОПІЧНИЙ ОБЛІК ЯК ФАКТОР ВПЛИВУ НА БЕЗПЕКУ СУБ'ЄКТІВ КОНКУРЕНТНОЇ РОЗВІДКИ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334235

Анотація. *Проаналізовано сучасні форми, методи та процедури застосування іноземними правоохоронними органами та заінтересованими комерційними структурами різних антропогенних біометричних показників. Виокремлено особливості використання ними біометричних систем ідентифікації та верифікації осіб за відбитками пальців. Дослідження показали, що в сучасних умовах широких масштабів набули міжнародні економічні злочини та транснаціональна організована злочинність. Безумовно, що вказані фактори деструктивно впливають на стабільність та безпеку в усіх сферах життя цивілізованого суспільства провідних країн світу. Тож перспектива нейтралізації зазначених факторів потребує якнайшвидшого вирішення. Але організація адекватної протидії цим факторам на сьогодні вимагає неабияких зусиль з боку відповідних державних структур і стає можливою лише завдяки поєднанню на глобальному рівні всіх наявних сил та засобів, насамперед спроможності сучасних інформаційних технологій та біометричних систем. Проте використання біометричних технологій іноземними правоохоронними органами, зокрема ідентифікації осіб за відбитками пальців, на сьогодні обумовлює певні протиріччя між формами і методами, які на теперішній час використовуються суб'єктами конкурентної розвідки для приховування своєї діяльності. Зокрема, з одного боку інтенсивне впровадження сучасних інформаційних технологій дає можливість правоохоронним органам багатьох країн світу ефективно здійснювати пошук міжнародних злочинців завдяки успішному застосовуванню в своїй практиці сучасних біометричних систем ідентифікації та верифікації осіб за їх біометричними показниками. З іншого, такі системи можуть становити певні загрози діяльності суб'єктів конкурентної розвідки. З огляду на рівень та характер таких загроз авторами статті визначено для оцінки систему ідентифікації осіб за відбитками пальців, складову якої становлять так звані дактилоскопічні обліки. Відомо, що на сьогодні правоохоронні органи постійно формують, наповнюють та використовують у своїх цілях дактилоскопічні обліки, до яких потрапляє певна категорія осіб. Насамперед мова йде про осіб, які мали порушення чинного законодавства тієї чи іншої країни або підозрюються у скоєнні кримінального злочину. Небезпеку діяльності суб'єктів конкурентної розвідки на території іноземних країн становить можливе потрапляння дактилоскопічних характеристик (параметрів) її співробітників до зазначених обліків. Проте процес формування, поповнення та використання цих обліків на сьогодні не є достатньо досконалим. Це дає можливість заінтересованим структурам, насамперед суб'єктам конкурентної розвідки, знаходити нові способи їх обходу (обману) і постійно вдосконалювати напрацьовані у цій сфері методики. Оцінка можливостей сучасних біометричних систем ідентифікації осіб за відбитками пальців та особливостей їх використання правоохоронними органами у своїй професійній діяльності дало можливість авторам статті розробити і запропонувати суб'єктам конкурентної розвідки окремі практичні рекомендації щодо організації ефективної протидії зазначеним системам під час виконання фахових завдань за кордоном.*

Ключові слова: конкурентна розвідка, країна комерційного інтересу, правоохоронні органи, комерційні структури, біометричні показники, біометрична система ідентифікації осіб за відбитками пальців, дактилоскопічний облік, дактилоскопічні параметри, сканери відбитків пальців.

Summary. *The article analyzed the modern forms, methods and procedures of processing various anthropogenic biometric indicators by foreign law enforcement agencies and interested private structures. The peculiarities of how they apply biometric systems of identification and verification of persons based on fingerprints are distinguished. Studies have shown that international economic crimes and organized transnational crime have become widespread in today's conditions. Undoubtedly, these factors have a destructive effect on stability and security in all spheres of life of the civilized society of the leading countries of the world. Therefore, the prospect of neutralizing the mentioned factors needs to be resolved as soon as possible. But the organization of adequate countermeasures against these factors today requires considerable efforts on the part of the relevant state structures and becomes possible only thanks to the combination of all available forces and means at the global level, primarily the capabilities of modern information technologies and biometric systems. However, the use of biometric technologies by foreign law enforcement agencies, in particular the identification of persons by fingerprints, today causes certain contradictions between the forms and methods currently used by competitive intelligence entities to hide their activities. In particular, on the one hand, the intensive implementation of modern information technologies enables law enforcement agencies of many countries of the world to effectively search for international criminals thanks to the successful use in their practice of modern biometric systems of identification and verification of persons based on their biometric indicators. On the other hand, such systems may pose certain threats to the activity of competitive intelligence entities. In view of the level and nature of such threats, the authors of the article selected for evaluation a system of identification of persons based on fingerprints, the component of which is the so-called dactyloscopic records. It is known that today foreign law enforcement agencies constantly create, fill and use for their own purposes dactyloscopic records, which include a certain category of persons. First of all, we are talking about persons who have violated the current legislation of one or another country or are suspected of committing a criminal offense. Therefore, the danger of the activities of the subjects of competitive intelligence on the territory of a foreign country is precisely the possible entry of dactyloscopic characteristics (parameters) of its employees into the specified records. However, the process of forming, replenishing and using these accounts is not sufficiently perfect today. This makes it possible for interested structures, primarily subjects of competitive intelligence, to find new ways to deceive (circumvent) them and to constantly improve the methods developed in this field. The assessment of the possibilities of modern biometric systems for the identification of persons based on fingerprints and the peculiarities of their use by foreign law enforcement agencies in their professional activities gave the authors of the article the opportunity to develop and offer to the subjects of competitive intelligence separate practical recommendations for the organization of effective countermeasures against those systems during the performance of professional tasks abroad.*

Keywords*: competitive intelligence, country of commercial interest, foreign law enforcement agencies, private structures, biometric indicators, biometric system of identification of persons based on fingerprints, dactyloscopic accounting, dactyloscopic parameters, fingerprint scanners.*

Постановка проблеми. На сьогодні визначення “конкурентна розвідка” дуже близько асоціюється з таким поняттям як “промислове шпигунство”. Якщо промислове шпигунство в багатьох країнах світу передбачає кримінальну відповідальність, то конкурентна розвідка, як специфічна сфера діяльності, загалом здійснюється в рамках правового поля. Зокрема, суб’єкти конкурентної розвідки діють легітимно, дотримуються принципів законності, використовують ті методи і засоби, які залучаються до процесу збору цільової інформації.

Основою легітимності конкурентної розвідки є конституційні права на пошук, отримання, передачу і використання в своїх інтересах здобутої легітимним шляхом інформації. Проте в сучасних умовах зазначені методи і засоби стають дуже близькими до тих, що використовуються спецслужбами в ході ведення традиційної розвідувальної (шпигунської) діяльності на території іншої країни. Тож на заваді легітимній діяльності суб'єктів конкурентної розвідки можуть стати іноземні правоохоронні органи, які в окремих випадках спроможні навіть довести незаконність такої діяльності [1].

Серед іншого загрозу діяльності суб'єктів конкурентної розвідки можуть становити сучасні біометричні системи ідентифікації осіб, зокрема за відбитками пальців. Основою використання зазначених систем є створення, формування, наповнення (оновлення) і застосування правоохоронними органами так званих дактилоскопічних обліків для своєчасної ідентифікації певної категорії осіб. Вказані обліки зазвичай містять в собі відбитки пальців осіб, які мали проблеми із законом, або підозрювалися у причетності до скоєння злочину. Також до цих обліків потрапляють дактилоскопічні параметри осіб, причетних до промислового шпигунства. З огляду на зазначені обставини співробітники конкурентної розвідки під час виконання фахових завдань в країнах комерційного інтересу мають навчитися якісно та ефективно обходити (обманювати) системи ідентифікації осіб за відбитками пальців. Зокрема розвідники мають створювати навколо себе такі умови, які унеможливлюють або ускладнюють їх ідентифікацію іноземними правоохоронними органами через використання зазначених вище систем ідентифікації.

Для безпечного та ефективного виконання завдань конкурентної розвідки в умовах тотальної діджиталізації суспільства перед суб'єктами конкурентної розвідки постає проблема щодо пошуку нових способів забезпечення безпеки співробітників з огляду на використання іноземними правоохоронними органами біометричних систем ідентифікації особи за відбитками пальців [2]. Означені системи дають можливість накопичувати і обробляти велику кількість біометричних показників, зокрема дактилоскопічних характеристик (параметрів) на осіб, які становлять певний інтерес для іноземних правоохоронних органів або навіть специфічних приватних структур [3].

Безпосередню небезпеку професійній діяльності співробітників конкурентної розвідки становить потрапляння їх відбитків пальців до дактилоскопічних обліків, які зазвичай використовуються правоохоронними органами в країні комерційного інтересу. При цьому розвідники мають враховувати, що такий виток їх дактилоскопічних параметрів може статися навіть випадково. Наприклад, під час перебування співробітника конкурентної розвідки за кордоном у приватних справах, в ході навчання або стажування в іноземних навчальних закладах, за участі в різних міжнародних конференціях. Виток означених параметрів сприяє процесу встановлення правоохоронними органами іноземної країни особи співробітника конкурентної розвідки під час виконання ним професійних завдань за кордоном. Водночас співробітники конкурентної розвідки повинні усвідомлювати, що володіючи відповідними формами і методами моніторингу інформаційного простору країни комерційної зацікавленості, вони можуть таємно заволодіти дактилоскопічними параметрами іншої особи, яка може представляти певний розвідувальний інтерес [4].

З огляду на використання іноземними правоохоронними органами біометричних систем ідентифікації осіб за відбитками пальців, автори визначили доцільним розробити окремі практичні рекомендації щодо організації сучасної протидії біометричним системам ідентифікації особи за відбитками пальців під час виконання співробітниками конкурентної розвідки професійних завдань за кордоном.

Обраний напрям у цій роботі тісно пов’язаний з виконанням положень Закону України “Про національну безпеку України”, Указу Президента України “Про рішення Ради національної безпеки і оборони України “Про Стратегію інформаційної безпеки” від 15.10.21 р. № 685/2021, Указу Президента України № 56/2022 “Про рішення Ради національної безпеки і оборони України “Про Стратегію забезпечення державної безпеки” від 30.12.21 р. щодо прискорення європейської та євроатлантичної інтеграції нашої країни, використання ресурсів конкурентної розвідки для досягнення визначеної мети.

Застосування сил та засобів конкурентної розвідки в комерційних компаніях не обмежується забезпеченням лише інформаційної безпеки її суб’єктів. Тому безпосередню загрозу виконанню її співробітниками професійних завдань за кордоном становлять контррозвідувальні заходи іноземних правоохоронних органів. Відомо, що правоохоронні органи іноземних країн для боротьби із внутрішнім криміналом та міжнародною злочинністю повсякчасно використовують сучасні біометричні системи ідентифікації осіб. З огляду на це співробітники конкурентної розвідки мають навчитися протидіяти таким системам, щоб не потрапляти у поле зору того чи іншого правоохоронного органу в країні комерційного інтересу під час виконання професійних завдань за кордоном [4].

Результати аналізу наукових публікацій. Можливості сучасних біометричних систем, що використовують провідні країни світу, розглянуто в [2]. Сучасні форми, методи та процедури опрацювання біометричних показників певної особи правоохоронними органами визначено в [3]. Особливості накопичення, обробки та використання персональних даних в [4]. Можливі шляхи та канали витоку персональних даних на представників українських силових структур розглянуто в [5; 6].

Проте на цей час недостатньо приділено уваги дослідженню проблем забезпечення безпеки співробітників конкурентної розвідки під час виконання фахових завдань за кордоном з огляду на особливості використання правоохоронними органами іноземних країн сучасних біометричних систем ідентифікації особи, зокрема за відбитками пальців.

Метою статті є визначення можливостей сучасних біометричних систем ідентифікації осіб за відбитками пальців у провідних країнах світу, особливостей формування дактилоскопічного обліку місцевого населення та іноземців, зокрема подальша розробка для співробітників конкурентної розвідки окремих практичних рекомендацій з організації протидії зазначеним системам під час виконання фахових завдань за кордоном.

Виклад основного матеріалу. Під час дослідження сучасних біометричних систем ідентифікації особи за відбитками пальців виникає низка проблемних питань, у тому числі: які саме загрози фаховій діяльності співробітників конкурентної розвідки становлять зазначені системи, якими силами і засобами можна організувати протидію цим системам та як використати інформаційний простір країни комерційного інтересу для видалення або заміни дактилоскопічних характеристик обраної особи в інтересах конкурентної розвідки. Зокрема, за певних умов та рівня професійної підготовки співробітник конкурентної розвідки має винайти можливість отримати негласний доступ до іноземних баз даних для прихованого вилучення або заміни дактилоскопічних параметрів на ту особу, яка представляє певний комерційний інтерес для конкретного суб’єкта конкурентної розвідки.

Системи сканування (дактилоскопії) відбитків пальців набули поширення в 1990-ті роки. Проте вони одразу зазнали атак з боку заінтересованих осіб щодо можливого

обходу (обману). Вже на початку 2000-х років, хакери винайшли та вдосконалили механізм виготовлення силіконових копій відбитків пальців за наявним рисунком. Виготовлення таких копій дає можливість обійти будь-яку систему розпізнавання за відбитками пальців, наприклад, наклеївши тонку плівку копії відбитка пальця однієї особи на палець іншої і прикласти її до сканера. Якщо система розпізнавання відбитків пальців має інші сенсори, то таку систему також можна обійти (зламати). Наприклад, біометрична система розпізнавання за відбитками пальців додатково налаштована на перевірку температури людського тіла. У такому разі сканер визначить, що прикладено палець живої людини, а не силіконову роздруківку відбитка. При цьому сканер не помітить тонку плівку з іншим візерунком, наприклад, наклеєну на палець співробітника конкурентної розвідки. За потреби співробітник також може використати аналогічні плівки для маскування інших пальців [4].

Актуальним залишається питання, чи можна отримати відбитки пальців іншої людини, зокрема об’єкта зацікавленості комерційної розвідки, для їх подальшого використання в інтересах комерційної структури. Як краще це зробити? Класичним посібником з виготовлення штучних відбитків пальців можна вважати японського криптографа Цутому Мацумото (Tsutomu Matsumoto) від 2002 року. У ньому докладно пояснюється, як співробітник конкурентної розвідки має обробити палець іншої, так званої жертви комерційного інтересу, графітовим порошком або парами ціаноакрилата (суперклею), щоб зняти з нього якісний відбиток. Окрім того детально викладено порядок обробки скопійованого співробітником конкурентної розвідки візерунку відбитка пальця цієї особи перед виготовленням його штучної копії. Наприкінці посібника докладно описано, як можна виготовити випуклу маску цього пальця за допомогою желатину, латексного молочка чи клею для дерева [7].

Результати дослідження свідчать, що найбільша складність у виготовленні копії пальця “жертви” – це якісно скопіювати його оригінал. Фахівці у цій сфері стверджують, що найякісніші відбитки пальців залишаються на скляних поверхнях та ручках дверей [6]. Проте в сучасному світі з’явився ще один спосіб копіювання відбитка пальця, зокрема завдяки роздільній здатності деяких фотографій. Йдеться про відновлення рисунка пальця безпосередньо з його фотографії [8].

У 2017 році фахові зарубіжні ЗМІ оприлюднили результати наукового проекту Національного інституту інформатики Японії. Зокрема, дослідники цього закладу довели можливість відтворення рисунка відбитка пальця з фотографій, які було зроблено цифровим фотоапаратом на відстані трьох метрів. Того ж року на Хакаській конференції (Chaos Communication Congress) дослідники в цій сфері продемонстрували відбитки пальців Міністра оборони Німеччини Жан-Клода Юнкера, які було відтворено за допомогою офіційних фотографій високої роздільної здатності, отриманих з відкритих джерел інформації. За аналогією діяв німецький хакер Ян Кесслер. Він використав дві фотографії Урсули фон дер Ляєн (одну з відкритого прес-релізу міністерства оборони Німеччини, іншу – зробив самостійно на одному з офіційних прийомів за участі У. Ляєн) та спеціальний програмний продукт Microsoft, створивши модель відбитків її пальців.

Подібний метод обходу (обману) системи розпізнавання відбитків пальців також використали співробітники компанії Vkansee. Прикладом став розрекламований пристрій фірми Apple – сенсор Touch ID, який розпізнає лінії на подушечках пальців, але не визначає матеріал, на якому вони зберігаються.

Дослідники цієї компанії з’ясували, що такий сенсор однаково реагує як на палець власника, так і на зліпок цього пальця. Експеримент проводили з двома різновидами

матеріалу – дитячим пластиліном і стоматологічним силіконом, який зазвичай використовують для виготовлення зліпків зубів. Як не дивно, але в обох випадках означений сенсорний пристрій не зміг розпізнати підробки пальця [8].

Співробітник конкурентної розвідки має усвідомлювати, що під час виконання ним фахових завдань за кордоном є багато варіантів потрапляння його дактилоскопічних параметрів до баз даних правоохоронних органів країни комерційного інтересу, де він вже не зможе легко їх видалити чи підмінити без спеціального програмного забезпечення або фізичного втручання в цю систему. Зокрема, виток дактилоскопічних параметрів співробітника конкурентної розвідки може статися через розміщення ним своїх фотографій у соціальних мережах. Як доведено вище, роздільна здатність сучасних фотоапаратів дає можливість правоохоронним органам або зацікавленим приватним структурам виділити на окремих фотографіях маленькі деталі, наприклад, відбитки пальців. Тож, як тільки співробітник конкурентної розвідки поділиться своїми фотографіями в соцмережах, він стає надто вразливим для правоохоронних органів країни комерційного інтересу.

Для уникнення цієї проблеми (окрім випадків навмисного розповсюдження своїх фотографій в соціальних мережах) розвідник має винайти всі можливі способи, як не залишати свої відбитки пальців у місцях громадського користування. Особливо, коли йдеться про місце, обране співробітником конкурентної розвідки для отримання цільової інформації. Проте, в разі гострої потреби, завдяки завчасно підготовленим копіям відбитків пальців іншої особи, розвідник може навмисно залишити їх в обраному громадському місці і у такий спосіб відволікти увагу іноземного правоохоронного органу на хибний об’єкт. Таким чином співробітник конкурентної розвідки суттєво знизить або навіть унеможливить ризик імовірної ідентифікації його особи правоохоронним органом країни комерційного інтересу через залишені ним чужі відбитками пальців, оскільки їх порівняння з наявними в дактилоскопічних базах даних відбитками пальців не дасть позитивних результатів.

Знання співробітником конкурентної розвідки особливостей функціонування систем розпізнавання особи за відбитками пальців також може відіграти для нього іншу позитивну роль. Йдеться про те, що в разі потреби розвідник може непомітно викрасти відбитки пальців у тієї особи, яка представляє певний комерційний інтерес для суб’єкта конкурсної розвідки і раніше згадувалася авторами як “жертва”. Для цього розвіднику зовсім не обов’язково запрошувати свою “жертву” на зустріч у приватній обстановці, під час якої він начебто випадково змусить співрозмовника взяти до рук пластилін або скляну пляшку. На початку йому достатньо лише добре вивчити особливості формування відбитків пальців цієї “жертви”, дослідити можливості і способи їх сканування в дистанційному режимі, а також всі чинники, які сприятимуть або заважатимуть цьому процесу.

Співробітники конкурентної розвідки повинні зважати на те, що відбитки пальців – папілярні візерунки (рисунки, які є неповторними для кожної людини) зазвичай формуються у людини випадково і це триває до шести місяців від її народження. Можна легко побачити неозброєним оком так звані арки, петлі, спіралі на подушечках пальців, інші деталі – так звані островки, розгалуження, закінчення ліній у кожному візерунку – тільки через оптичні прилади. Результати сучасних дослідів свідчать, що навіть у близнюків з ідентичною ДНК відбитки пальців різняться. Вірогідність їх співпадіння становить приблизно один випадок на 64 мільярди. Рисунок на подушечках пальців може трохи мінятися і слабшати з часом. Причиною тому є будь-яке пошкодження, опік або інші травми пальців. Наприклад, рисунок на подушечках пальців може затертися,

коли людина протягом тривалого часу працює муляром. Встановлено, що в секретарів, які постійно контактують із папером, цей рисунок може зазнати певних змін. Але в цілому, за основними ознаками, візерунок пальців залишається незмінним. Тому повністю позбутися від нього неможливо. Навіть після хімічного опіку відбитки пальців через декілька тижнів відновлюються і починають проступати зовні. При цьому рубці, що залишаються після таких опіків, можуть додати відбиткам травмованих пальців певну унікальність (неповторність), що сприятиме ідентифікації їх власника.

На цей час сканери відбитків пальців є достатньо компактними. Їх почали використовувати в багатьох технічних пристроях, зокрема в ноутбуках, клавіатурах, "мишах", смартфонах, засобах захисту інформаційних баз даних, різних технічних пристроях обмеження доступу до секретних приміщень тощо. На багатьох комерційних підприємствах зазвичай використовують оптичний спосіб сканування відбитку пальця, який дає можливість проаналізувати його рисунок завдяки видимому світлу. Так, коли система сканує зображення пальця, вона порівнює рисунок його гребенів і впадин з тими параметрами, що є в базі цього підприємства. У такому разі помилки в порівнянні трапляються рідко. Але обійти (обманути) такі системи можна без особливих зусиль. Для цього достатньо силіконових муляжів пальців. Проте можуть бути й більш складні випадки. Зокрема, на важливих засекречених об'єктах зазвичай застосовують термічні сканери, які аналізують людське тепло, або тактильні сканери, що аналізують тиск людського тіла. Сканери такого типу можуть навіть фіксувати світло, яке проходить крізь шкіру пальця, вловлюють на ньому пульс і визначають частинки поту. Наприклад, у системах контролю доступу PERCo використовують високоточне обладнання – вбудований OEM-модуль серії CBM від компанії IDEMIA, завдяки якому відбувається ідентифікація особи за декількома показниками одночасно. Але такі системи застосовують дуже рідко, оскільки вони дороговартісні [8-10].

З огляду на результати проведеного аналізу авторами статті запропоновано окремі практичні рекомендації суб'єктам конкурентної розвідки щодо організації ефективної протидії сучасним біометричним системам ідентифікації особи за відбитками пальців під час виконання їх представниками фахових завдань за кордоном.

На першому етапі співробітник конкурентної розвідки має визначити, яку саме загрозу його професійній діяльності несе та чи інша біометрична система розпізнавання особи за відбитками пальців, чи можна обійти цю систему без внутрішнього втручання в її роботу. На цьому етапі виконання фахових завдань за кордоном розвідник має дотримуватися таких заходів безпеки:

вивчати систему розпізнавання за відбитками пальців, зокрема її можливості (характеристики, параметри тощо), особливості та порядок використання цієї системи іноземними правоохоронними органами, насамперед слабкі місця в її функціонуванні, конкретні чинники, що стають на заваді виконання співробітником конкурентної розвідки фахових завдань через дію такої системи;

визначати місця розташування аналогічних систем в усіх районах можливого виконання фахових завдань в країні комерційного інтересу;

знаходити місця проведення спеціальних фахових заходів поза дією таких систем.

На другому етапі, в разі якщо співробітник усвідомив, що йому не уникнути деструктивної дії тієї чи іншої системи без втручання в її внутрішню роботу, він має виконати такі заходи:

визначити можливі варіанти обходу (обману, злому) конкретної системи, що стає йому на заваді;

обрати ресурси, за допомогою яких він це зможе зробити.

Одним із варіантів обходу розвідником визначеної ним системи ідентифікації особи за відбитками пальців може стати той спосіб, коли він винайде умови, що сприятимуть прихованому викраденню і подальшій підробці відбитків пальців тієї особи, яка має офіційний доступ до цієї системи.

Такий спосіб співробітник конкурентної розвідки може реалізувати: через застосування програмних засобів і спеціальної техніки; через безпосереднє механічне втручання в роботу конкретної, визначеної ним системи.

У разі застосування програмних засобів і спеціальної техніки розвідник має отримати від комерційної структури, інтереси якої він представляє, таке програмне забезпечення, яке дасть йому можливість:

непомітно дистанційно (через застосування комп'ютерних мереж) втрутитися в роботу обраної системи розпізнавання і змінити її параметри на свою користь;

особисто фізично втрутитися в роботу обраної системи розпізнавання, яка на деякий час за якихось причин і обставин залишилася без відповідного контролю, після чого застосувати отримане від комерційної структури програмне забезпечення для зміни параметрів цієї системи на свою користь. Для цього співробітник також може використати завчасно виготовлені відбитки пальців тієї посадової особи, яка має офіційний доступ до визначеної співробітником для злому системи;

залучити до втручання в роботу системи третіх (заінтересованих) осіб, які мають можливості офіційного доступу до неї.

Тож насамперед розвідник має визначитися, що йому доцільніше зробити: зламати обрану систему розпізнавання за відбитками пальців за допомогою наданого заінтересованою комерційною структурою програмного забезпечення; заволодіти відбитками пальців особи, яка має офіційний доступ до цієї системи, або залучити таку особу до співпраці з комерційною розвідкою.

Висновки. За результатами проведених досліджень встановлено, що жодна система розпізнавання відбитків пальців, навіть в оптимальних лабораторних умовах, вочевидь не є 100 % точною (із нульовими показниками хибно-позитивних і хибно-негативних спрацьовувань). Тож на цей час наявні способи захисту комерційних структур з використанням систем ідентифікації за відбитками пальців дуже вразливі, оскільки виробники цих систем передусім думають про низьку вартість та зручність використання, аніж про їх надійність.

Аналіз можливостей сучасних біометричних систем ідентифікації за відбитками пальців вказує на те, що завжди можна підібрати способи та методи їх обходу (обману). Але проблемним для співробітників конкурентної розвідки залишається питання, як вони мають приховати від оточення чи правоохоронних органів країни комерційного інтересу свої відбитки пальців, таким чином унеможливити їх потрапляння до накопичувальних баз даних (дактилоскопічних обліків). Для вирішення зазначеної проблеми співробітники конкурентної розвідки мають передусім визначитися, чи можна обманути сканер відбитків пальців - основу функціонування системи розпізнавання за відбитками пальців? Яким чином краще обійти визначену конкретну систему? Як не допустити потрапляння своїх відбитків пальців до дактилоскопічних обліків (баз даних) правоохоронних органів країни комерційної зацікавленості? Як їх можна замінити (видалити) у разі такого потрапляння? Як непомітно для оточення можна заволодіти відбитками пальців особи, що представляє комерційний інтерес для конкурентної розвідки, щоб наприклад розблокувати таку систему тощо?

Для вирішення цих проблемних питань співробітники конкурентної розвідки насамперед мають дотримуватися наданих вище окремих практичних рекомендацій з

організації протидії біометричним системам розпізнавання особи за відбитками пальців під час виконання фахових завдань за кордоном і водночас шукати інноваційні способи забезпечення безпеки в цій сфері.

Перспективи подальших досліджень. Визначення можливостей використання суб'єктами конкурентної розвідки штучного інтелекту у протидії біометричним системам ідентифікації за різними біометричними параметрами під час виконання фахових завдань за кордоном.

Використана література

1. Ланде Д.В. Правові питання конкурентної розвідки. *Інформація і право*. № 2(33)/2020. С. 51-68.

2. Біометричний контроль іноземців. WikiLegalAid: довідково-інформаційна платформа правових консультацій. URL: https://legalaid.wiki/index.php/Біометричний_контроль_іноземців (дата звернення: 15.10.2024).

3. Відбитки пальців і Eurodac. 2021. 4 с. URL: https://www.migracija.lt/documents/20123/55049/Dublin-874c-781c-8726-7bae71b2ebea?t=1562575380576 (дата звернення: 20.10.2024).

4. Волошенко О.В. Способи зміни та підміни відбитків пальців. *Вісник Академії адвокатів України.* Т. 11. № 1(29) 2014. С. 148-151.

5. Персональні дані представників силових структур України. URL: https://myrotvorets2.org/index.html (дата звернення: 28.10.2024).

6. Криміналістика. Академічний курс: підручник / Т.В.Варфоломеєва, В.Г. Гончаренко, В.І. Бояров, С.В. Гончаренко, В.О. Попелюшко. Київ: Юрінком Інтер, 2011. 504 с.

7. Методи обходу біометричного захисту. – (Блог компанії GlobalSign, 14.01.2019). URL: https://habr.com/ru/companies/globalsing/435978 (дата звернення: 30.10.2024).

8. Учені довели, що селфи можуть бути небезпечні (рос.). URL: https://bykvu.com/ua/movie/ 62191-uchenye-dokazali-chto-selfi-mogut-byt-nebezopasny (дата звернення: 5.11.2024).

9. У відкритий доступ злили біометричні дані більше мільйона українців. "То є Львів". 2015 – 2021. URL: https://inlviv.in.ua/ukraine/u-vidkrytyj-dostup-zlyly-biometrychni-dani-bilshe-miljona- ukrayintsiv (дата звернення: 8.11.2024).

10. Гункель Е. МВС рф буде збирати біометричні дані росіян і іноземців у спеціальному банку. – (Deutsche Welle, 22.11.2020, рос.). URL: https://www.dw.com/ru/mvd-rf-budet-sobirat-biometricheskie-dannye-rossijan-i-inostrancev-v-specialnom-banke/a-55689754 (дата звернення: 10.11.2024).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~