Санакоєв Д. Б.,
завідувач кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

СУЧАСНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ: СВІТОВИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ У ПРОТИДІЇ ОРГАНІЗОВАНИМ ФОРМАМ ЗЛОЧИННОСТІ

Використання новітніх інформаційних та комунікаційних технологій організованими злочинними групами, терористичними організаціями чи окремими злочинцями є головною проблемою для держав загалом та правоохоронних органів зокрема через складність явища, кількість задіяних факторів та учасників, а також значну сукупність злочинних технологічних засобів, що використовуються для фінансування та підтримки злочинних і терористичних дій.

Використання сучасних технологій цими угрупованнями зміцнює їхні можливості для підтримки своєї діяльності (фінансування, відмивання грошей, вербування, планування терористичних атак, шахрайство з використанням особистих даних) та анонімного вчинення злочинів. Ці злочинні групи та організації часто знаходяться в авангарді технологічних інновацій для планування, вчинення та приховування своєї злочинної діяльності та доходів від неї.

Які з найбільш ефективних інструментів вже використовують правоохоронці у світі для забезпечення публічної безпеки та які перспективи подальшого впровадження технічних пристроїв у діяльності поліції?

Виконаний нами аналіз фахових джерел з цього питання дозволив виокремити ***світові тенденції, що становлять підґрунтя сучасної поліцейської діяльності***, спрощують можливості забезпечення публічної безпеки і порядку, вивільняють ресурси, забезпечуючи проактивну роботу поліції та надають її діяльності більшої прозорості:

1. Соціальні мережі. Сьогодні активно й ефективно використовуються поліцією для збирання та поширення інформації, залучення спільнот. Зі зростанням потреби у прозорості соціальні мережі стали одним із найкращих способів зв'язку з широкою публікою. Платформи соціальних мереж, як-от: Facebook, Twitter, Reddit дозволяють отримувати оновлення у режимі реального часу. Крім того, створення широкої мережі в соціальних мережах може допомогти розкрити злочини, оскільки поліція може ділитися інформацією з ширшою аудиторією.

2. BodyCam, що забезпечують більшу прозорість та зменшують

кількість скарг, пов'язаних із застосуванням сили. Проте такі питання, як вартість, конфіденційність, зберігання даних, публічне розкриття та загальна ефективність, продовжують залишатися предметом дискусій.

3. Програмне забезпечення для розпізнавання обличчя (наприклад, NGI, Rekognition та NeoFace Reveal від NEC, FaceFirst) ідеально підходить для віддаленого спостереження, оскільки його точність і складність зростають. Однак були деякі розбіжності щодо розпізнавання осіб та потенційних расових упереджень [1]. Внаслідок цих проблем закони про біометричну конфіденційність стануть актуальною темою, оскільки цей тип технологій стає дедалі популярнішим.

4. Алгоритми прогнозування у поліцейській діяльності. Штучний інтелект (далі – ШІ) пропонує фундаментальний прорив у роботі поліції, переходячи від реактивного до проактивного (попереджувального) контролю. Це стало можливим завдяки розширеній аналітиці та моделям втручання, які, по суті, можуть «прогнозувати» злочинність – системи ШІ можуть проактивно сканувати масиви інформації, щоб забезпечити точне прогнозування злочинності за допомогою прогнозної аналітики, яка може допомогти поліції активно координувати свої дії на стадії до вчинення злочину.

5. Додатки GPS. Використовуються правоохоронними органами для швидшого відстеження та визначення місцезнаходження підозрюваних та умовно-достроково звільнених. Кулі GPS, наприклад, можуть бути випущені в транспортний засіб, щоб дистанційно відстежувати його рухи, а пристрої GPS-стеження можуть використовуватися для рецидивних правопорушень для відстеження їхнього розташування [2].

Водночас GPS дозволяє краще координувати та відстежувати місцезнаходження (у т.ч. фізіологічний стан) офіцерів та транспортних засобів. Це може допомогти ефективніше реагувати на інциденти, а також дозволяє отримувати більш точну інформацію про місцезнаходження для координації викликів та безпечніше і швидше скеровувати працівників поліції до цих інцидентів.

6. Використання **робототехніки** у роботі поліції продовжує розширюватися [3]. Наприклад, маленькі роботи у формі танків, оснащені датчиками, використовуються для проникнення у місця, куди небезпечно входити поліцейському, а потім надсилають аудіо- і відеопотік групі затримання, що відповідає за проведення заходу (операції). Дедалі досконаліші роботи зі знешкодження вибухових пристроїв також допомагають правоохоронцям, виконуючи небезпечні завдання, пов'язані з вибуховими речовинами.

7. Дрони. Допомагають у спостереженні, оскільки поліцейські підрозділи знаходять нові застосування для безпілотних літальних апаратів (БПЛА), оснащених оптичними, зумуючими та/або тепловізійними камерами [4]. Наприклад: пошукові та рятувальні операції, затримання зі стрілянинӧю, перестрілка між злочинцями, дорожньо-транспортні пригоди, огляд місця

події, візуальне спостереження та моніторинг натовпу.

8. Поліцейська діяльність, керована аналітикою [5], поєднує вирішення проблем, спостереження, обмін інформацією та підзвітність поліції з поліпшеними розвідувальними операціями та даними для інформування поліцейських зусиль, спрямованих на найбільш ймовірні сценарії та ситуації.

9. Система ShotSpotter, що впроваджується в США, яка використовує датчики для виявлення пострілів та залучає аналітиків для відстеження даних та миттєвої передачі їх у поліцію, що дозволяє їм прибути на місце події швидше, ніж будь-коли раніше [6].

10. Хмарні застосунки. Перехід до операцій із забезпечення безпеки у хмарному середовищі набув значного поширення: зокрема, Пентагон поставив 10 мільярдів доларів на свій гучний контракт на хмарну інфраструктуру спільного захисту підприємства (JEDI) [7]. У діяльності підрозділів поліції та ФБР США активно використовуються програмні продукти ApprissSafety та Fusus у так званих хмарних середовищах Центрів контролю злочинності в реальному часі у хмарах (RTC^3 – Real-Time Crime Center in the Cloud). Наприклад, технологія Fusus дозволяє будь-якому виду пристрою (БПЛА, камери контролю дорожнього руху, телефони або інші види пристроїв Інтернету речей та пристроїв, орієнтованих на публічну безпеку), перехоплювати і передавати дані про події в режимі реального часу. Інтегруючи всю цю інфраструктуру безпеки в безпечну хмару, Fusus змогла зробити RTC^3 доступним для більшості підрозділів, які можуть отримати доступ до цієї інформації з метою забезпечення публічної безпеки [8].

11. Програмне забезпечення для керування розслідуванням, кадрами (наприклад, Case Jacket, Forensics Capture, HooYu Investigate, Omnigo, Cerebral, SceneDoc, HR Acuity, програмні продукти InTime тощо). Дедалі очевиднішим є той факт, що використання електронної таблиці або олівця більше не допоможе. Це може призвести до негативних наслідків для підрозділів, зокрема високих понаднормових витрат, підвищеного ризику, високої плинності кадрів через низький моральний дух персоналу та неефективність. Крім того, ризик неукомплектованості або укомплектування співробітниками без достатньої мотивації може завдати шкоди безпеці працівників та громадськості. Забезпечити управління ризиками та економити на витратах агентств дозволяє впровадження спеціалізованого програмного забезпечення [9].

12. Використання негласних джерел та легендованих підприємств. Ми не випадково розмістили цей напрям діяльності поліції у нашому переліку останнім, оскільки переконані – людський фактор у поєднанні з негласними формами та методами роботи у протидії злочинності та, передусім, її організованим проявам, дозволить підняти ефективність такої протидії на якісно вищий рівень.

Яскравим прикладом вважаємо спеціальну операцію OTF Greenlight /

Trojan Shield (Зелене світло / Троянський щит), що проводилась з 2019 року Федеральним бюро розслідувань США (ФБР), Національною поліцією Нідерландів (Politie) та Управлінням поліції Швеції (Polisen) у співпраці з Управлінням боротьби з наркотиками США (DEA) та 16 іншими країнами за підтримки Європолу [10].

Сутність довготривалої операції полягала в тому, що ФБР у тісній співпраці з Федеральною поліцією Австралії стратегічно розробило та таємно керувало компанією з виробництва зашифрованих пристроїв під назвою ANOM, яка розвинулась та обслуговувала понад 12 000 зашифрованих пристроїв більше ніж 300 злочинних синдикатів у понад 100 країн, включно з італійською організованою злочинністю, злочинні банди мотоциклістів та міжнародні організації, що займаються незаконним обігом наркотиків.

Мета нової платформи полягала в тому, щоб спрямовуватись на глобальні організації, що займаються організованою злочинністю, незаконним обігом наркотиків та відмиванням коштів незалежно від того, де вони розташовані, і переконати злочинні організації звернутися до цього зашифрованого пристрою із функціями, що зацікавлять мережі організованої злочинності, такими як, наприклад, віддалене стирання та примусове видалення паролів.

ФБР та 16 інших країн міжнародної коаліції за підтримки Європолу та в координації з Управлінням боротьби з наркотиками США потім використали розвіддані з 27 мільйонів отриманих повідомлень і переглянули їх протягом 18 місяців, тоді як злочинці-користувачі ANOM обговорювали свою злочинну діяльність.

Протягом червня 2021 року було проведено понад 700 обшуків будинків, здійснено понад 800 арештів та вилучено понад 8 тонн кокаїну, 22 тонни канабісу та смоли канабісу, 2 тонни синтетичних наркотиків (амфетамін та метамфетамін), 6 тонн прекурсорів синтетичних наркотиків, 250 одиниць вогнепальної зброї, 55 автомобілів еліт-класу та понад 48 млн доларів США у різних валютах та криптовалютах. Ця операція дозволить Європолу ще більше поліпшити розвідувальну картину про організовану злочинність, що впливає на ЄС, завдяки якості інформації, що збирається. Ця поліпшена розвідувальна картина підтримуватиме постійні зусилля щодо виявлення чинних важливих злочинних цілей у глобальному масштабі.

Отже, виконаний нами аналіз сучасних інноваційних інформаційно-комунікаційних технологій, що використовуються повністю або частково правоохоронними органами розвинених країн світу (передусім США та Європи), свідчить про тенденцію до їх швидкого розвитку й постійного удосконалення. Зважаючи на сучасний стан розвитку та впровадження інноваційних технологій в діяльність підрозділів правоохоронних органів, зокрема й щодо протидії організованим формам злочинності, перспективними для України вважаємо такі напрями:

1) *розширення можливостей впровадження поліцейської діяльності,*

керованої аналітикою (Intelligence-Led Policing). Вбачаємо можливості реалізації цього напряму в контексті створення Центрів контролю злочинності в реальному часі у хмарних середовищах;

2) *оптимізація поліцейських технологій у хмарних середовищах*. Хмарні рішення не лише надзвичайно дешеві, порівняно зі старими локальними рішеннями, вони також пропонують можливість дефрагментувати свою технологічну інфраструктуру та оптимізувати свої операції. З огляду на те, що хмарні системи сьогодні мають переваги над локальними у сенсі захищеності та більш низькі показники втручань, згідно з політикою безпеки даних CJIS, ймовірне їх впровадження найближчим часом [11];

3) *використання можливостей БПЛА*, зокрема й у протидії організованим проявам злочинності (огляд місця події; огляд закритих об'єктів і територій; аеророзвідка; візуальне спостереження за особою, місцем або річчю; контроль за діяльністю ОГ у місцях позбавлення волі, контроль натовпу тощо);

4) *впровадження систем організації роботи підрозділу.* Стратегічними пріоритетними напрямами можуть стати скорочення кількості випадків із застосуванням сили, виявлення додаткових потреб у навчанні всередині підрозділів, тактика зниження шкоди, що підвищує безпеку співробітників та громад, а також стійке планування нагляду та підзвітності, що зміцнює зв'язки між поліцією та громадянським суспільством;

5) *впровадження у освітній процес* підготовки та підвищення кваліфікації поліцейських *систем і технологій VR*, що дозволить майбутнім та наявним працівникам поліції навчитись керувати кризовими ситуаціями та знижувати ескалацію небезпечних. Хоча може бути складно відтворити ці важливі ситуації у реальному житті, VR уможливлює відтворення будь-якого сценарію (наприклад, продукція компаній WRAP Reality, ApexOfficer, Axon, InVeris, та ін.), розробляючи та використовуючи під час підготовки поліцейських тренінги VR, що фокусуються на навчанні скорочення застосування сили тощо.

Бібліографічні посилання

7. https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/
8. https://www.starchase.com/
9. https://www.roboticstomorrow.com/story/2020/07/security-never-sleeps-robotics-in-law-enforcement/15449/
10. https://www.thedrive.com/article/15092/drones-in-law-enforcement-how-where-and-when-theyre-used
11. https://www.policechiefmagazine.org/changing-the-face-crime-prevention/
12. https://www.forbes.com/sites/elizabethmacbride/2018/10/30/the-scientist-the-investor-and-the-ceo-how-shotspotter-turned-a-profit-after-22-years/?sh=564739b0468c
13. https://www.businessinsider.com/jedi-jwcc-cloud-contract-legacy-pushing-multi-cloud-future-2021-8

14. https://www.fusus.com/rtc3-products/fusus-real-time-crime-center-in-the-cloud
15. https://www.capterra.com/investigation-management-software/s/free/
16. https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication
17. https://www.fusus.com/blog/infographic-why-cloud-based-solutions-are-the-future-of-law-enforcement

Сарахман О. М.,
доцент кафедри облікових
технологій та оподаткування,
кандидат економічних наук, доцент
Сідельник О. П.,
доцент кафедри фінансового
консалтингу та банківництва,
кандидат економічних наук, доцент
(Університет банківської справи)

ВПЛИВ ДІДЖИТАЛІЗАЦІЇ НА ОПЕРАЦІЙНІ РИЗИКИ БАНКІВ

З початку пандемії Covid-19 більшість банків України адаптувалися до віддаленого режиму роботи і обслуговування клієнтів у нових реаліях. Затрати на побудову нової сервісної моделі не закладалися повною мірою у бюджет витрат банків і стали відображенням збитків від однієї загальної події операційного ризику під назвою – Covid-19. Одним із фундаментальних елементів формування сучасної інформаційної економіки є цифрові платформи, які базуються на розвиненій IT- інфраструктурі [1].

Діджиталізація банківського сектора – довгостроковий процес, що має ознаки глобальної тенденції і позначається на розвитку банків у низці країн. Український банківський сектор активно долучається до цього процесу, намагаючись у такий спосіб утримувати клієнтів і підвищувати рівень своєї конкурентоспроможності на ринку фінансових послуг [2].

Зі свого боку, банки можуть оптимізовувати свої процеси, скорочувати бюрократичні процедури, впроваджувати сучасні послуги, підвищувати конкурентоспроможність. Важливою під час пандемії також є мінімізація соціальних контактів, яку забезпечує впровадження онлайн-послуг.

У банківській сфері ризик є цілком нормальним явищем, оскільки з метою отримання істотного прибутку необхідно ризикувати [3, 149–150].

Операційні ризики за типом наслідків і частотою прояву можна поділити на чотири категорії подій: що виникають із малою частотою і спричиняють невеликі збитки; що виникають часто та спричиняють невеликі