Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра економічної та інформаційної безпеки
Навчально-наукового інституту права та підготовки фахівців
для підрозділів Національної поліції

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Матеріали
Всеукраїнської науково-практичної конференції
(м. Дніпро, 02 листопада 2023 р.)

Дніпро
2024

УДК 351.74+004
С 90

Рекомендовано до друку науковою радою Дніпропетровського державного університету внутрішніх справ (протокол № 8 від 20.03.2024)

С 90 Сучасні інформаційні технології в діяльності Національної поліції матеріали Всеукр. наук.-практ. конференції (м. Дніпро, 02 листопада 2023 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. 184 с.

ISBN 978-617-8035-96-9

Збірник містить матеріали однойменної Всеукраїнської науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.

ISBN 978-617-8035-96-9

З М І С Т

СОЛДАТЕНКО Аліна
курсант 3-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції,
Науковий керівник:
ПЕРВІЙ Віта
доктор філософії, викладач кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ

ЩОДО ЗНАЧЕННЯ ДІЇ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Успішність та ефективність роботи правоохоронних органів у боротьбі зі злочинністю залежать від якості, своєчасності та достатнього об'єму інформаційного та аналітичного забезпечення цієї сфери діяльності. У нормативних документах і науковій літературі, терміни «інформаційне забезпечення», «інформаційно-аналітична діяльність», «інформаційно-аналітична робота» та «аналітична діяльність» часто використовуються як синоніми для «інформаційно-аналітичного забезпечення». Термін «інформація» (походить від латинського «informatio», що означає «роз'яснення» або «виклад») має два основних значення: у повсякденному використанні, це відомості або повідомлення, що громадяни передають один одному усним, письмовим або іншими способами, щоб повідомити про щось; у науковому контексті, це обмін цими відомостями між громадянами, досліджуючи їх з різних точок зору.

Одним із видів правової інформації, що використовується в оперативно-розшуковій діяльності, є оперативно-розшукова інформація. Оперативно-розшукова інформація включає в себе фактичні дані, що мають поточне або майбутнє значення для вирішення стратегічних, тактичних та організаційних завдань в рамках оперативно-розшукової діяльності. Ця інформація зазвичай здобувається оперативними структурами з використанням як відкритих, так і секретних методів з різних джерел або через аналітичну обробку вихідних даних [1, с. 262].

У загальноприйнятих наукових твердженнях про природу та значущість оперативно-розшукової інформації, її основною цінністю дійсно є відображення змінливого соціального оточення та контексту, в яких проводиться оперативно-розшукова діяльність. Ця інформація також фіксує наслідки постійного впливу на це оточення, різних соціальних суб'єктів, незалежно від спрямованості та характеру їхньої діяльності (як правомірної,

так і протиправної). На цьому перетині оперативно-розшукова інформація, з одного боку – виникає, а з іншого боку – продовжує активно «функціонувати», тобто просуватися й розвиватися, включаючись в процеси безпосередньої роботи з оперативно-розшуковими діями та відображаючи зміни, які сталися в об'єктах оперативно-розшукової діяльності або в їхньому оточенні [2, с. 26].

Загалом інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції є важливою складовою, яка чітко допомагає в забезпеченні безпеки громадян та ефективності у протидії зі злочинністю. Ефективність протидії злочинності суттєво залежить від прав та повноважень, які надаються правоохоронним органам законодавцем. Оперативно-розшукова діяльність становить важливий компонент у загальній системі боротьби зі злочинністю та захисту інтересів громадян, суспільства та держави. Усі процесуальні дії правоохоронних і судових органів у сфері кримінального правосуддя спрямовані на об'єктивне, всебічне й повне розслідування обставин подій, незалежно від їхньої специфіки. Правовий статус і функції оперативно-розшукової діяльності регулюються законодавством України, що також визначає права та обов'язки суб'єктів, які здійснюють оперативно-розшукову діяльність та здійснюють контроль над цим процесом. Визначення ОРД як специфічного виду державної діяльності спеціальних служб правоохоронних органів, спрямованого на протидію злочинності, забезпечення національної безпеки і державної таємниці міститься в Законі України «Про оперативно-розшукову діяльність», де зазначено, що ОРД – це система гласних і негласних, пошукових і контррозвідувальних заходів, що здійснюються визначеними в законі оперативними підрозділами, із застосуванням оперативних та оперативно-технічних засобів [3, с. 328].

Отже, підкреслимо, що інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції має величезне значення. Вона є ключовим інструментом для забезпечення безпеки громадян, розкриття злочинів та встановлення справедливості. Інформація, що правильно зібрана та аналізована, допомагає оперативникам і слідчим приймати обґрунтовані рішення, прогнозувати можливі злочини та їхні наслідки, а також діяти передбачливо. Зважаючи на сучасний характер злочинів та загроз для суспільства, інформаційно-аналітична робота стає невід'ємною частиною боротьби зі злочинністю. Важливим фактором для досягнення успішності процесу збору оперативної інформації з боку працівників національної поліції є визначення джерел та місць її отримання, а також встановлення необхідного обсягу інформації, необхідної для виконання завдань щодо протидії злочинам та способів її отримання. Основним завданням Національної поліції є забезпечення безпеки, в якій інформаційно-аналітична робота грає ключову роль у досягненні цієї мети. Вона сприяє ефективній роботі правоохоронних органів, допомагає виявляти та припиняти злочинну

діяльність, та забезпечує правосуддя та справедливість.

1. Шинкаренко І.Р., Шинкаренко І.О., Кириченко О.В. Правове регулювання оперативно-розшукової діяльності та здійснення негласних слідчих (розшукових) дій (структурно-логічні схеми) : навч. посібник. Дніпропетровськ : ДДУВС, 2015. 320 с.

2. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів : ЛьвДУВС, 2017. 244 с.

3. Телійчук В.Г., Клешня В.В. Оперативні підрозділи як суб'єкти правоохоронної діяльності: проблеми правового регулювання. Дніпро : ДДУВС, 2021. С. 327-329.

ГОНТАР Анна
курсант 3-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
ТЕЛІЙЧУК Віталій
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ОПЕРАТИВНИХ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ: ДЕЯКІ АСПЕКТИ ТА ОСОБЛИВОСТІ

Від початку воєнного стану до чинного законодавства України було внесено цілу низку змін, що викликані реаліями сьогодення. Наскільки виправданими є такі зміни, чи не звужується об'єм прав осіб, щодо яких здійснюється оперативно-розшукова діяльність та чи не вплинув воєнний стан на здійснення оперативно-розшукової діяльності оперативними підрозділами Національної поліції – ці питання набувають особливої актуальності для сьогодення [1].

Основними суб'єктами оперативно-розшукової протидії злочинів є підрозділи карного розшуку. Зокрема, до функцій підрозділів карного розшуку належить попередження, виявлення, припинення і розкриття злочинів, вчинених учасниками організованих злочинних груп, злочинних організацій, бандитських формувань. Результативність діяльності оперативних підрозділів у боротьбі зі злочинами безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності [2].

У теорії оперативно-розшукової діяльності (далі ОРД) більшістю

вчених прийнято визначати, що суб'єкт ОРД - це спеціально уповноважений орган або підрозділ, що відповідно до визначеного законодавцем функціонального призначення, реалізовує комплексні повноваження щодо застосування спеціальних сил та засобів ОРД з пошуку і фіксації фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [3].

Наразі досить розповсюдженою є проблема того, що фундаментальних знань здобутих правоохоронцями в ході навчання та професійного становлення недостатньо для успішного вирішення професійних завдань, з якими вони зустрічаються під час виникнення незвичних обставин діяльності та непередбачуваних ситуацій в процесі виконання посадових обов'язків. Передусім, це пояснюється мобільністю правової системи, постійними законодавчими нововведеннями та мінливістю часу, що невпинно рухається в бік інновацій.

З метою якісного вирішення завдань професійного характеру, співробітникам правоохоронної системи усіх рівнів та підрозділів абсолютно необхідно на високому рівні опановувати основні аспекти та особливості організації інформаційно-аналітичної діяльності (далі ІАД), а також постійно їх застосовувати в практичній діяльності. Методику ІАД досліджували такі вчені як І.Т. Муковський, І.Р. Боднар, І.В. Захарова, В.М. Варенко та ін., проте проблематика ефективного опанування та застосування зазначених компетенцій залишається як недостатньо досліджуваною, так і нормативно не врегульованою.

Аспекти та особливості ІАД, як концепція методології підходів до опрацювання службових моментів чи вирішення професійних завдань побудована на одночасному опануванні трьох важливих складових професійної діяльності: опрацюванні інформації, документальному супроводженні та прийнятті управлінських рішень.

Методи здійснення ІАД, відносно часто, ототожнюють з іншими методами проведення аналізу та прийняття рішень, але вони мають і свою специфіку – їх зазвичай використовують під час вирішення нетипових ситуацій, проблем, складних і неструктурованих завдань. Різноманітність галузей діяльності співробітників Національної поліції України обумовлює широкий спектр методів, які класифікують за різними критеріями. Зокрема, виокремлюють методи теоретичного і матеріального підходів, що охоплюють цілу систему заходів, які реалізують з урахуванням конкретних умов.

Зокрема, до основної групи дієвих методів, що застосовують в процесі ІАД належать:

– аналіз, синтез, абстрагування, узагальнення, порівняння;

– опитування, спостереження, експеримент, статистичний аналіз;

моделювання, експертна оцінка;

– згортання змісту інформації (реферування, анотування) і узагальнення (створення оглядової інформації);

– довідково-інформаційний умовивід [4].

На нашу думку, варто окремо закцентувати увагу на методах безпосереднього аналізу та моделювання, що належать до аналітико-прогностичних методів та становлять сукупність комплексних методів, пов'язаних з опрацюванням, класифікацією, інтерпретацією інформації. Саме завдяки своєчасному їх застосуванню відбувається усвідомлення тих чи інших причинно-наслідкових подій, отримується своєчасне пояснення фактів та здійснюється логічне складання прогнозів можливих варіантів подальшого розвитку подій. Поступове застосування вище зазначеного беззаперечно сприятиме прийняттю найбільш зваженого адекватного рішення. Проте, важливу роль у цьому, відіграє також процес ухвалення рішення, що обов'язковим чином має здійснюватися на основі об'єктивного аналізу обставин, конкретних особливостей тієї чи іншої ситуації.

У підсумку, вважаємо доцільним нагадати про метод порівняння, що є фундаментально необхідним для формування висновку про подібність чи відмінність об'єктів згідно отриманого досвіду, фактів дійсності та особливостей конкретного випадку [5]. Цей метод є одним з найпоширеніших задля знаходження закономірностей, як загальних, так і локальних, притаманних одному або кільком об'єктам.

Таким чином, вивчення методів ІАД має фундаментальне значення у виконанні професійних функцій оперативних працівників, і є обов'язковим чинником для досягнення очікуваних результатів професійної діяльності, формуванні компетентностей та якісного досвіду, комплексному виконанню покладених повноважень. На наш погляд, така діяльність на постійній основі передбачає вдосконалення навичок як кожного окремого фахівця, так і усієї системи діяльності правоохоронних органів в цілому, що безпосередньо залежить від усвідомленості професіоналізму здійснюваних дій і сьогодні, і в майбутньому.

_____-

1. Особливості кримінального процесу в умовах воєнного стану. URL : https://jurliga.ligazakon.net/analitycs/212017_osoblivost-krimnalnogo-protsesuv-umovakh-vonnogo-stanu]

2. Телійчук В. Г. Оперативний аналіз як важливий елемент аналітичної підтримки оперативно-розшукової протиді корисливо-насильницьким злочинам. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі україни: матеріали міжвідомчої наук.-практ. конф., м. Київ 11.08.2022. С. 158-162.

3. Телійчук В.Г., Приступа Д.В., Щодо питання протидії розбоям підрозділами кримінальної поліції. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2019. №4. С.271-276

4. Стегній Б.Т., Методи інформаційно-аналітичного забезпечення трансферу та провайдингу інновацій у галузі ветеринарної медицин. Ветеринарна медицина, випуск

101, 2015. С. 236-237.

5. А. В. Ліпінська: «Вивчення методів ІАД майбутніми фахівцями з документознавства та інформаційної діяльності» (2017, Київ). URL : http://www.dy.nayka.com.ua/?op=1&z=109.

ГРЕБЕНЮК Андрій,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент;

ЗЛОЧИНИ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТИ

У сучасному світі розгортається невідома боротьба, яка не має меж та кордонів – це боротьба у кіберпросторі, де виявляються нові виклики та загрози для суспільства. Однією з найбільш серйозних проблем є кіберзлочинність, яка в умовах воєнного стану може стати ще більш небезпечною. Особливе місце серед цих загроз активно захоплює мережа Dark Web, де розвивається кіберзлочинність та економічні злочини. Для цього широко використовується криптовалюта.

Станом на вересень 2023 року у світі існує **22904** криптовалюти та є активними або цінними лише близько **8832** активних криптовалют. [1]

Тисячі криптовалют, що ми маємо сьогодні, можна найпростіше розділити на три категорії:

- **Bitcoin** – лідер ринку і оригінальна криптовалюта Процесс створення нових криптоблоків біткоїну дуже енергозатратний, підтвердження транзакцій потребує певного часу.
- **Альткойн** – альтернатива біткоіну (не обов’язково схожа), їх простіше видобувати, бо вони потребують менше енергії та мають нижчі збори за транзакції.
- Стейблкоїни – це альткоїни, курс яких чимось забезпечений. Наприклад, сильними фіатними валютами (доларом США, євро тощо), чи товарними цінностями (наприклад, золотом), чи іншими криптовалютами.
- **Токени** – цифровий сертифікат, який гарантує зобов’язання компанії перед його власником. Токени можна назвати криптовалютним аналогом акцій або цінних паперів, з тією різницею, що контроль за всіма транзакціями здійснюється через технологію блокчейн. Оборот токена відбувається саме у тому проекті, для якого він створений.

Найпопулярніші криптовалюти:

	Валюта	**Скорочення**	**Ціна,** доларів США
1	Bitcoin	BTC	27908,28
2	Perpetual Protocol	PERP	0,5615
3	Avalanche	AVAX	10,06
4	Decentraland	MANA	0,2976
5	Axie Infinity	AXS	4,4793
6	Bitcoin Gold	BTG	12,95
7	Aptos	APT	5,25
8	Monero	XMR	154,89
9	Internet Computer	ICP	3,11
10	Tether Gold	XAUt	1839,00

За даними, наданими Національною поліцією України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилась на 36 %.

До того ж, за законом в Україні єдиний законний засіб платежу – національна валюта гривня. Але й прямої заборони використання криптовалют в Україні не було. Тобто розрахунки у криптовалютах і не дозволялися, і не заборонялися.

17 лютого 2022 року, Верховна Рада прийняла Закон «Про віртуальні активи» Цей закон регулює галузь криптовалют. Але на даний час цей закон не набув чинності [1]. У більшості країн статус крипти досі залишається невизначеним. Її важко регулювати, оскільки вона має децентралізований характер. Додатково до цього транзакції у блокчейні анонімні, через що податкова не може їх відстежити. Щоб подивитися, скільки коштує Біткоін та інші криптоактиви, а також для їх купівлі та продажу, в основному використовують криптобіржі. Більшість таких майданчиків потребує проходження верифікації. Теоретично податківці можуть робити запити через суд, щоб біржі надавали особисті дані та історію операцій клієнта. Але насправді це досить складно зробити, тому подібне відбувається лише тоді, коли йдеться про відмивання грошей в особливо великих розмірах [2, 3].

Активізувалися шахраї при введенні воєнного стану в нашій країні та почали використовувати деякі схеми для ошукування населення. Частина нових шахрайських схем виникла на хвилі підтримки України представниками світової криптоіндустрії:

Схема 1: «безкоштовна» роздача грошей криптобіржею

Схема виглядає так: потенційній жертві пропонують зареєструватися на ноунейм біржі, ввести промокод «StopWar», після чого обіцяють нарахувати 0,24 ETH (близько 600 $) нібито на допомогу. Що цікаво, в акції можуть брати участь не лише українські користувачі, що, звісно, дуже

розширює поле діяльності аферистів.

Після реєстрації на біржі та проходження процедури повної верифікації обіцяна сума справді засвічується на рахунку новачка. Проте, щоб вивести її, «біржа» просить активувати обліковий запис і поповнити баланс на $100. Як тільки баланс поповнено на зазначену суму, обліковий запис блокується. В результаті в аферистів залишаються не лише гроші, а й документи, надані їм для ідентифікації.

Схема 2: «заробіток» на російських санкціях

Своїх жертв аферисти знаходять у численних крипточатах, до яких новачки (і не лише) приєднуються у пошуку торгових сигналів. Все починається з того, що жертва отримує листа від учасника групи, який через санкції нібито не може вивести свою криптовалюту з біржі, але ще не втратив права робити внутрішні перекази.

Далі жертві пропонується зареєструватися на біржі, де у відправника повідомлення нібито «застрягла» криптовалюта, отримати на свій рахунок умовні 1,5 BTC та вивести їх із біржі за 10-відсоткову винагороду.

Але для виведення коштів нібито необхідно верифікувати рахунок поповненням на $100. Щойно гроші надходять на рахунок, вас блокують. Так «комбінатор» позбавляється не лише дармової криптовалюти, а й своїх кровно зароблених.

Схема 3: шахрайської схеми Pump&Dump

Обирають найчастіше маловідомі криптовалюти (або відомі) і починають скуповувати потроху, щоб цей процес не вплинув на ринкову ціну.

Другий етап – це саме Pump – «накачування». Шахраї починають розповсюджувати «ексклюзивну» інформацію про те, що саме ця монета ось-ось зросте в ціні.

Робиться це через величезну кількість «експертних» телеграм-каналів, групи у соціальних мережах чи блогерів. Головне – створити ілюзію зростання активу.

Схема 4: «допомога» Україні

У цьому випадку аферисти грають на бажанні представників криптоспільноти допомогти українській армії, нашим біженцям або взяти участь в інших акціях, що дозволяють пом’якшити наслідки гуманітарної катастрофи через російське вторгнення.

Криптоінвестори одними з перших організували допомогу Україні. За перші сім днів війни у вигляді пожертвувань у криптовалюті, як пише сайт The art newspaper, було зібрано близько $40 млн.

Вже у перші дні війни у соціальних мережах було зафіксовано сплеск активності спам-розсилок від шахраїв. Які просили робити пожертвування у криптовалюті для допомоги Україні.

Деякі зловмисники для обману користувачів видають себе представниками громадських і гуманітарних організацій. часто шахраї

використовують різні методи емоційного тиску.

Шахраї можуть використовувати різні методи викачування грошей – від фішингових електронних листів, які нібито виходять із доменів Управління ООН з координації гуманітарних питань до повідомлень на форумах, що нібито пов'язані з рухом допомоги Україні.

Потрібно дотримуватись простих правил: завжди перевіряйте ресурси, на яких реєструєтеся, вивчайте відгуки, моніторте інформацію в офіційних джерелах і головне – не подавайтеся спокусі швидкого отримання легких грошей.

Не надсилати криптовалюту невідомим людям та організаціям, оскільки немає жодних гарантій, що гроші підуть за призначенням.

Якщо ви дійсно хочете допомогти Україні криптовалютою у боротьбі проти агресора, користуйтеся лише офіційними сайтами профільних організацій: пожертвування можна зробити через розміщені там посилання або з їхніх сторінок у соціальних мережах.

1. Закон України «Про віртуальні активи». URL : https://zakon.rada.gov.ua/laws/show/2074-20#Text

2. Драгоненко А.О., Ніколенко М.І. Проблеми кваліфікації шахрайства з використанням електронно-обчислюваних машин. Порівняльно-аналітичне право – електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет» № 1, 2018. С. 256-259.

3. Карчевський М.В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Науковий вісник Львівського державного університету внутрішніх справ. Серія «Юридична». Вип. 1. 2014. С. 272–281.

САЄНКО Денис
здобувач вищої освіти ступеня
магістра за спеціальністю
«Кібербезпека» факультету №6
Науковий керівник:
НОСОВ Віталій
професор кафедри кібербезпеки
та DATA-технологій факультету № 6
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОКРЕМІ АСПЕКТИ РЕАЛІЗАЦІЇ ПРИХОВАНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

Прихований віддалений доступ до комп'ютерної системи може реалізовуватись зловмисниками або через встановлення стандартних засобів віддаленого адміністрування (Remote Administartion Tool, RAT) або за допомогою спеціально створених RAT.

Клієнтські модулі стандартних RAT, до яких можна віднести NjRAT, VNC, TeamViewer, DarkComet RAT, Quasar, мають безпосереднє з'єднання з системою, що дозволяє при розслідуванні кіберінцидентів встановлювати IP адрес вузла, з якого відбувається прихований віддалений доступ.

За своїм функціоналом, такі засоби надають можливість: доступу до файлів і і системних налаштувань; графічного відображення робочого столу та окремих відкритих вікон; трансляції відео з веб-камери та навколишнього звуку з використанням мікрофону; отримання інформації, щодо встановлених браузерів, паролів, історії з'єднань, активних сесій авторизованих профілів до різних онлайн ресурсів; виведення графічних повідомлень різного характеру; модифікації сервісів системи з подальшим порушенням цілісності та роботи системи; завантаження і встановлення застосунків; тощо.

Використання стандартних RAT у зловмисних цілях зазвичай блокується міжмережними екранами та антивірусними системами, що вимушує зловмисників розроблювати спеціальні RAT, що здійснюють приховане з'єднання із системою через проміжний сервіс, наприклад, месенджеру Телеграм. Логічна схема такого прихованого віддаленого доступу до системи Windows зображена на рис. 1.

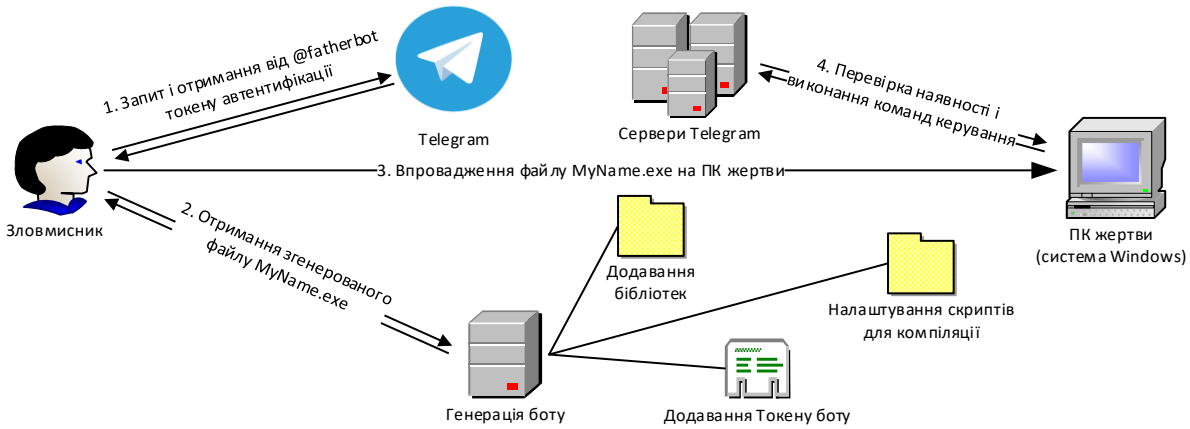

Рис. 1 – Логічна схема прихованого віддаленого доступу до комп'ютерної системи

Зловмисник створює у месенджері Телеграм приватний канал (чат), формально реєструє для каналу ще не створений застосунок автоматичного опрацювання запитів на віддалене керування системою – бот-керування, для якого від головного боту Телеграма @fatherbot отримує токен автентифікації на сервері Телеграм (Фаза 1) [1]. Далі (Фаза 2) зловмисник орендує віддалений сервер, встановлює одну із версій ОС Linux, завантажує базові бібліотеки мов програмування Nim [2], Python, додаткові бібліотеки Aiogram, Jsony, Nimcrypto, Sysinfo, Winim, Pixie, Nim_miniz, Quickcrypt, Puppy і інструменти Nimble та MinGW. У конструкторі застосунків експлуатації вразливостей (наприклад, Metasploit Framework) з використанням отриманого токену здійснює генерацію боту-керування у вигляді виконуваного файлу *.exe (наприклад, MyName.exe) для ОС Windows. За допомогою методів соціальної інженерії (Фаза 3) файл боту-керування доставляється і запускається в системі жертви. Використання спеціальних модулів і мов програмування при створенні боту-керування ускладнює його виявлення антивірусними системами ОС жертви. Бот-керування, зазвичай кожні 500 мс, за протоколом https з'єднується із сервером Телеграма і перевіряє наявність керуючих команд у відповідному приватному чаті (Фаза 4). За наявності таких команд виконує їх, а результати надсилає до цього ж чату. Зловмисник входить до приватного чату з будь-якого пристрою і віддає команди боту.

У зазначеній схемі сервери Телеграма виконують функцію посередника для забезпечення анонімності зловмисника, оскільки при здійсненні розслідувань фактів несанкціонованого доступу у комп'ютерну систему і виявлення каналу керування системою через сервіс Телеграму, офіційні запити на встановлення IP-адреси кінцевого отримувача повідомлень приватного чату адміністрація Telegram Messenger Inc. ігнорує. Зловмисник може підключатись до приватного чату через VPN, Proxy або мережу Tor, що забезпечує додатковий шар анонімності.

Для протидії описаній схемі прихованого віддаленого доступу до комп'ютерної системи користувачам, перш за все, необхідно: бути

обізнаними про методи соціальної інженерії; бути обережним під час завантаження і запуску файлів із мережі; мати антивірусне програмне забезпечення із регулярно оновленими базами; здійснювати моніторинг постійно відкритих з'єднань неідентифікованих (невідомих) компонентів системи із вебсерверами, зокрема із серверами Телеграма. У випадку виявлення прихованого віддаленого доступу потрібне фізичне відключення системи від комп'ютерної мережі і проведення досліджень із метою оцінки втрат, відновлення безпеки, ідентифікації причин ураження, збору доказів і покращення системи захисту від подібних кібератак.

1. Telegram team, 22.09.2023, «Telegram Bot API». URL : https://core.telegram.org/bots/api (дата звернення 25.10.2023).
2. Andreas Rumpf, Zahary Karadjov, 01.08.2023, «Nim Manual». URL : https://nim-lang.org/docs/manual.html (дата звернення 25.10.2023).

АНТОНЮК Владислав
курсант 4 курсу факультету №4
КОЛІСНИК Тетяна
доцент кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутр.ішніх справ,
кандидат педагогічних наук, доцент

ЗВІДКИ БЕРУТЬСЯ І ЯК ВПЛИВАЮТЬ НАШІ ОСОБИСТІ ДАНІ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ

В епоху цифрових технологій, коли сучасне суспільство переповнене смартфонами, соціальними мережами, та онлайн-сервісами, особисті дані стали справжньою скарбницею і, водночас, пунктом вразливості. Кожна наша онлайн-активність, будь-то пошук в Інтернеті, мобільні додатки чи спілкування в соціальних мережах, залишає сліди в цифровому просторі, які збираються та аналізуються корпораціями, урядами та іншими структурами. Тема впливу та походження наших особистих даних набула надзвичайної актуальності, оскільки це має надзвичайно важливий вплив на наше життя, економіку, політику, та суспільство загалом.

Питання обробки і захисту персональних даних є надзвичайно важливими для бізнесу, особливо через збільшену потребу в інформації про фізичних осіб і посилене законодавство про захист даних, яке було впроваджено Європейським Союзом. Будь-яка організація, яка працює з персональними даними, повинна відповідати закону і включати в роботу такі напрямки: збір даних за згодою суб'єктів, обробка та зберігання даних,

договірні відносини з іншими організаціями та заходи щодо захисту даних. Більшість цих завдань належать до компетенції юристів, і навіть технічні заходи краще узгоджувати з юристом [2].

В українському законодавстві немає спеціальної термінології «безпека приватності персональних даних», але існує поняття «інформаційна безпека». Інформаційна безпека визначається як захист важливих інтересів людини, суспільства і держави від можливих загроз, таких як неповна, нечасна, або невірогідна інформація, негативний вплив інформації, проблеми, пов'язані з використанням інформаційних технологій, та незаконне розповсюдження та використання інформації [1]. Важливо зауважити, що у цьому контексті не обговорюється конкретний процес захисту.

Згідно з Доктриною інформаційної безпеки України, інформаційна безпека включає конфіденційність (обмеження доступу до інформації), цілісність (запобігання змінам інформації без дозволу) і доступність (забезпечення доступу до інформації для відповідних осіб).

Зараз, завдяки розвитку інформаційних технологій і збільшеному збору та обробці персональних даних, концепція «приватності» стає складнішою, і важливо враховувати віртуальний аспект цього поняття. Більша кількість зібраних даних дозволяє створювати віртуальний образ особи, і розмова про приватність та конфіденційність стає більш віртуальною, але все ж важливою [1].

Використання даних у корпораціях та владних органах є важливим аспектом сучасного суспільства. Корпорації використовують дані для прийняття стратегічних рішень, покращення продуктів та послуг, а також оптимізації бізнес-процесів. Владні органи використовують дані для розробки політик, прийняття законів та забезпечення безпеки та громадського порядку [2].

Проте використання даних також вимагає збереження приватності та конфіденційності громадян. Для цього існують правила та регулювання щодо захисту персональних даних, а також механізми контролю за їх використанням [3]. Забезпечення балансу між використанням даних та збереженням приватності є важливою задачею сучасного управління даними.

Наразі в епоху цифрових технологій, наші особисті дані стають об'єктом інтенсивного збору та використання. Збір і обробка цих даних мають значущий вплив на наше щоденне життя, включаючи рекламу, персоналізовані послуги та наше відношення до приватності. Одночасно, це створює виклики щодо захисту особистих даних та етичного використання інформації. Правильне регулювання та освіта громадськості стають ключовими чинниками для забезпечення безпеки та збереження особистої приватності у цифровому світі.

---

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/card/47/2017 (дата звертання 12.10.2023).

2. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних (ст. 33-46). URL : https://ippi.org.ua/brizhko-vm-pilipchuk-vg-privatnist-konfidentsiinist-ta-bezpeka-personalnikh-danikh-st-33-46 (дата звертання 12.10.2023). Назва з екрана.

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 12.10.2023)

ТЕЛІЙЧУК Віталій
професор кафедри
оперативно-розшукової діяльності
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, старший
науковий співробітник, доцент

ОПЕРАТИВНО-РОЗШУКОВЕ ПРОГНОЗУВАННЯ ЯК ФОРМА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ

Сучасне і повне інформаційне забезпечення діяльності оперативних підрозділів з використанням як негласних, так і гласних відомостей з метою виявлення всіх обставин вчинення злочинів є однією з умов підвищення рівня організації оперативно-розшукової діяльності оперативних підрозділів у протидії злочинам. Слід погодитися з В. Ортинським, що отриману оперативно-розшукову інформацію щодо злочинів можна класифікувати на чотири групи: відомості, одержані: від осіб, яких конфіденційно залучено до виконання завдань ОРД; від інших (не оперативних) підрозділів правоохоронних органів; від працівників зарубіжних правоохоронних органів і організацій; від громадян у формі усних і письмових заяв (повідомлень) та ЗМІ. Також, необхідно зазначити, що перелічені вище джерела отримання оперативно-розшукової інформації в ході проведення оперативно-розшукових заходів всі без винятку використовуються у протидії злочинам, що вчиняються організованими злочинними структурами. Отримана із зазначених джерел інформація уможливлює прогнозування злочинів та визначення кількості сил і засобів оперативних підрозділів для протидії їм [1].

Потреба у прогнозуванні, виявленні та прогнозуванні тенденцій розвитку ситуації диктує застосування різноманітних аналітичних методів обробки вихідної інформації в сучасних умовах життя. Щоб з’ясувати

можливі шляхи розвитку ситуації необхідне не лише узагальнення оприлюдненої інформації, а й її оцінка. Наявність «вивідних знань» у вивченні та аналізі інформації робить її надійною основою для прийняття управлінських рішень [2]. Приналежність організації роботи оперативних підрозділів у процесі протидії організованій злочинності (далі ОЗ), як правило, повинно передувати проведення прогнозу, оскільки без обліку майбутнього розвитку (тобто без прогнозу) неможливе ефективне планування діяльності в оперативній роботі. Криміногенна ситуація, яка склалася у теперішній час потребує впровадження у практику правоохоронних органів сучасних прийомів і методів протидії злочинності, розроблення адекватних підходів до розв'язання проблем, що виникають у процесі цієї боротьби. Оперативно-розшукове прогнозування - один з таких підходів [3].

Оперативно-розшукове прогнозування це форма інформаційно-аналітичної роботи в ОРД, яка полягає в організації процесу наукового передбачення майбутнього на основі оперативного аналізу минулого та сьогодення на підставі раніше зібраної оперативної інформації. В умовах протидії організованій, транснаціональній злочинності особливої актуальності набуває вміння передбачити розвиток криміногенної ситуації, запобігти розвитку подій у небажаному напрямку. Зазначені чинники вимагають від правоохоронних органів застосування відповідних заходів, засобів і методів боротьби зі злочинністю, впровадження сучасних прийомів і форм інформаційно-аналітичної роботи. сьогодні однією з таких форм є оперативно-розшукове прогнозування. Прогнозування оперативної обстановки здійснюється шляхом висунення на основі інформації, що надходить, опе-ративно-розшукових версій про можливі дії осіб, схильних до скоєння правопорушень; щодо умов, сприяючих учиненню економічних і кримінальних правопорушень; про ймовірні методи приховування слідів учинених і здійснюваних злочинів тощо [4].

Таким чином, констатуємо, що оперативно-розшукове прогнозування є результатом мислення оперативного працівника, пошуку ним відповідей на питання про те, як може змінитися оперативно-тактична ситуація, як необхідно діяти в очікуваній ситуації, якою буде поведінка противника (особи, яка вчиняє чи буде вчиняти протиправні дії). Також зазначимо, що оперативно-розшукове прогнозування – це важливий елемент тактичного мислення, інформаційно-логічний процес, що передує прийняттю тактичного рішення та впливає на їх зміст і вибір засобів та методів реалізації в оперативно-розшукових діях (заходах, операціях).

1. Володимир Ортинський. Особливості інформаційного забезпечення оперативно-розшукового прогнозування у протидії злочинам у сфері обігу наркотичних засобів. URL : https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13118/4-9.pdf

2. Кандуєв Д. В. Інформаційно-аналітичне забезпечення підрозділів збройних сил України в умовах воєнного стану. URL : https://cutt.ly/SwEiicUI

3. Телійчук В. Г. Оперативно-розшукове прогнозування як спосіб виявлення організованих злочинних груп. URL : https://www.juris.vernadskyjournals.in.ua/journals/2013/2-1-2_2013/52.pdf.
4. Оперативно-розшукове прогнозування. URL : http://4ua.co.ua/pravo/ord/operativno-rozshukove-prognozuvannya.html.

ДУСЯК Олександра,
курсантка 3 курсу ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
ТЕЛІЙЧУК Віталій,
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ЩОДО ПИТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

За сучасних умов мінливої реальності закономірно виникає необхідність у якісному прогнозуванні, своєчасному виявленні, попередженні та нейтралізації загроз Національній безпеці Україні. Очевидно, що в боротьбі із зазначеною проблемою залучається максимально різноманітний спектр правоохоронних органів та організацій, однак, ми пропонуємо виокремити вагомість дослідження процесу здійснення саме стратегічного аналізу кримінальними аналітиками, його результатів, що полягають у створенні необхідного аналітичного продукту [1, с. 325-326].

Інформаційно-аналітична діяльність в сфері оперативно-розшукової діяльності є ключовим елементом забезпечення безпеки та викриття злочинів у сучасному світі. Зі зростанням обсягів і доступності інформації у цифрову еру, важливість розробки та використання аналітичних інструментів і технологій стає критичною для забезпечення суспільної безпеки та виявлення злочинців.

Згідно ст. 1 Закону України «Про оперативно-розшукову діяльність», завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою

припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [2].

Здійснений нами аналіз законодавчого та нормативного врегулювання оперативно-розшукової діяльності як частини державної діяльності, дає можливість зрозуміти, що держава має безпосередній інтерес у вирішенні своїх завдань, а право в цьому контексті стає ефективним інструментом для досягнення цих цілей, і це, на наш погляд, є дуже важливим. Норми законодавства, які стосуються оперативно-розшукової діяльності, мають різний ступінь юридичної обов'язковості і, відповідно, виконують різні регуляторні функції.

Погоджуємось із думкою А. В. Мовчана в тому, що інформаційно-аналітична робота в оперативно-розшуковій діяльності повинна базуватися на суворому дотриманні норм закону та підзаконних нормативних актів. Будь-яке неправомірне застосування оперативно-розшукових заходів не може бути виправдано ніякими оперативними, організаційними та іншими міркуваннями [3, с. 126].

Основною метою системи інформаційного-аналітичного забезпечення діяльності у боротьбі зі злочинністю є всебічна інформаційна підтримка практичної діяльності підрозділів МВС України, а саме Національної поліції України на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів [4, с. 323].

Інформаційно-аналітичне забезпечення відіграє дуже важливу роль у діяльності оперативних підрозділів Національної поліції України, зокрема, підрозділів кримінального аналізу і є комплексом організаційних, правових і технологічних засобів, що забезпечують збір, отримання, обробку, розповсюдження, аналіз та використання необхідних для реалізації інформаційних ресурсів, завдання та функції органів Національної полії, визначені чинним законодавством. У сучасних умовах інформаційно-аналітична діяльність стає необхідною потребою суспільства, що є одним із найважливіших і впливових факторів стабільності та життєздатності будь-якої країни. Загалом, кримінальний аналіз передбачає виявлення та точне визначення зв'язку між інформацією, що стосується подій злочинного характеру, фігурантів, і даних, отриманими з різних джерел, для того, щоб слідчі органи, прокуратура та суди могли їх оцінити і діяти з метою подальшого використання. Загальною метою кримінального аналізу є розробка нових напрямів ефективної слідчої роботи та досудового розслідування, кримінальних проваджень, отримати детальних аналітичних результатів за предметом кримінального аналізу, якісне планування окремих оперативно-розшукових та слідчих (гласних і негласних) дій, аналітичне забезпечення оперативно-розшукової діяльності та досудового розслідування, аналіз стану та ефективності досудового розслідування, оперативно-розшукової та профілактичної діяльності у боротьбі зі

злочинністю, оскільки необхідна обробка такої кількості інформації, факти неможливо відстежити та зв'язати без використання спеціальних аналітичних методів [5, с. 243].

Ми вважаємо, що для отримання інформації та вирішення завдань оперативно-розшукової діяльності, працівники підрозділів кримінальної поліції повинні взаємодіяти з іншими правоохоронними органами, національними та міжнародними службами, громадскістю. Завдяки цьому досягається більший успіх у сфері протидії злочинності, ефективна боротьба зі злочинністю та забезпечення безпеки громадян, суспільства і держави.

На нашу думку, інформаційно-аналітична діяльність в оперативно-розшуковій діяльності відіграє невід'ємну та ключову роль у сучасному правоохоронному процесі. Завдяки розвитку технологій і підвищенню кваліфікації фахівців, ця діяльність стала більш ефективною та продуктивною, сприяючи виявленню та припиненню злочинів. Однак важливо пам'ятати, що співпраця і обмін інформацією між різними органами та службами є ключовими складовими успіху в цій сфері. Тільки через спільні зусилля можна забезпечити ефективну боротьбу зі злочинністю та забезпечити безпеку громадян.

1. Калашнік Є. О.; Телійчук В. Г. Аналітичний продукт стратегічного аналізу як базовий інструментарій у боротьбі зі злочинністю. Реалізація державної антикорупційної політики в міжнародному вимірі: матеріали VII Міжнар. наук.- практ. конф. (Київ, 8–9 груд. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. с. 325-327

2. Закон України «Про оперативно-розшукову діяльність»: від 07.07.1992 № 2136-XII станом на: 31.03.2023 р. URL : https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 08.10.2023)

3. Мовчан А. В. Окремі аспекти законодавчого регулювання інформаційно-аналітичної роботи в оперативно-розшукової діяльності. Право і безпека, 2011 с. 125-128.

4. Телійчук В. Г.; М'яло А. О. Щодо питання удосконалення оперативно-розшукової діяльності у виявленні та розслідуванні кримінальних правопорушень в умовах воєнного стану. *The 13th International scientific and practical conference "Modern science: innovations and prospects" (September 18-20, 2022)* SSPG Publish, Stockholm, Sweden. 2022 pp. 320-327.

5. Пашкевич О. Я. *Актуальні питання діяльності підрозділів кримінальної поліції: збірник матеріалів Всеукраїнської науково-практичної конференції (м. Кропивницький, 14 квітня 2023 року).* Інформаційно-аналітичне забезпечення підрозділів Національної поліції України. Кропивницький : ДонДУВС, 2023 с. 243-245

ЗАЧЕК О.І.,
доцент кафедри інформаційного
та аналітичного забезпечення
діяльності правоохоронних органів
факультету № 2 ІПФПНП
Львівського державного університету
внутрішніх справ,
кандидат технічних наук, доцент

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ CLEARVIEW AI У НАВЧАЛЬНОМУ ПРОЦЕСІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Clearview AI – американська компанія з розпізнавання обличь, яка надає програмне забезпечення компаніям, правоохоронним органам, університетам і окремим особам. Алгоритм компанії зіставляє обличчя з базою даних із понад 20 мільярдів зображень, проіндексованих з Інтернету, включаючи додатки соціальних мереж [1]. Clearview AI використовують ФБР, Департамент внутрішньої безпеки США та більше 600 правоохоронних органів по всьому світі для виявлення підозрюваних [2]. За допомогою Clearview правоохоронні органи можуть завантажити зображення обличчя підозрюваного та порівняти його зі своєю базою даних зібраних фотографій. Потім програмне забезпечення надає посилання, яке дозволяє знайти «збіг» в Інтернеті. За словами помічника начальника поліції Маямі Армандо Агілара, цей інструмент штучного інтелекту допоміг розкрити кілька справ про вбивства [3].

Після початку повномасштабної війни в Україні компанія Clearview AI надала свою технологію Україні щоб допомогти захиститися від російського вторгнення, зокрема, для возз'єднання біженців, розлучених зі своїми сім'ями, виявлення російських агентів та допомоги уряду у спростуванні неправдивих повідомлень у соціальних мережах, пов'язаних з війною. Спочатку доступ до програми отримало Міністерство оборони України, а потім інші відомства, включаючи Національну поліцію України, приєдналися до проєкту [4].

У квітні 2022 року New York Times повідомила, що Clearview створила понад 200 облікових записів для користувачів у п'яти українських державних установах, які здійснили понад 5000 пошукових запитів, а також Clearview переклала свій додаток українською мовою. Були надані підтвердження від офіційних осіб трьох відомств в Україні, що вони використовували інструмент для ідентифікації загиблих солдатів і військовополонених [5].

Станом на липень 2022 року, через 4 місяці, 7 відомств та понад 600 співробітників активно використовували платформу Clearview AI,

здійснивши понад 60000 пошуків. Кожен пошук міг врятувати життя на блокпосту, допомогти ідентифікувати зниклу людину тощо. У небезпечних ситуаціях воєнного часу знання того, хто є другом, а хто ворогом, має вирішальне значення для забезпечення безпеки громадян і військовослужбовців. Clearview AI зібрав понад 2 мільярди зображень з публічних фотографій на російському сайті соціальних мереж «Вконтакте» і допомагає ідентифікувати потенційних російських солдатів і порушників на блокпостах, російських військових, які загинули або потрапили в полон, шукати зниклих безвісти [4].

У липні 2022 року доступ до даного програмного забезпечення отримали завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Сеник В.В. та доцент цієї кафедри Зачек О.І. Кафедра використовує це програмне забезпечення у навчальному процесі під час викладання навчальної дисципліни «Інформаційне забезпечення професійної діяльності», а саме теми «Інформаційно-пошукові системи МВС та Національної поліції України».

Головна сторінка, на яку попадаємо після входу до програми, містить історію пошуків (Рис.1). Ми використовували фото знайомих нам людей для перевірки роботи програми. Після відкриття одного з пошуків ми потрапляємо до вікна, де містяться відомості про цей пошук і результати пошуку у вигляді ряду фотографій, клацнувши по яким, ми попадаємо на соцмережу, де ці фотографії є. А це дозволяє встановити особу. Остаточне рішення про схожість осіб на фото є за нами, бо не всі фото є фотографіями особи, є фото схожих людей. Під час занять здобувачі вищої освіти завантажують своє фото, а ми разом з ними за допомогою програми знаходимо їх сторінки в соцмережах. Відповідно, вони таким чином навчаються роботі з програмою.

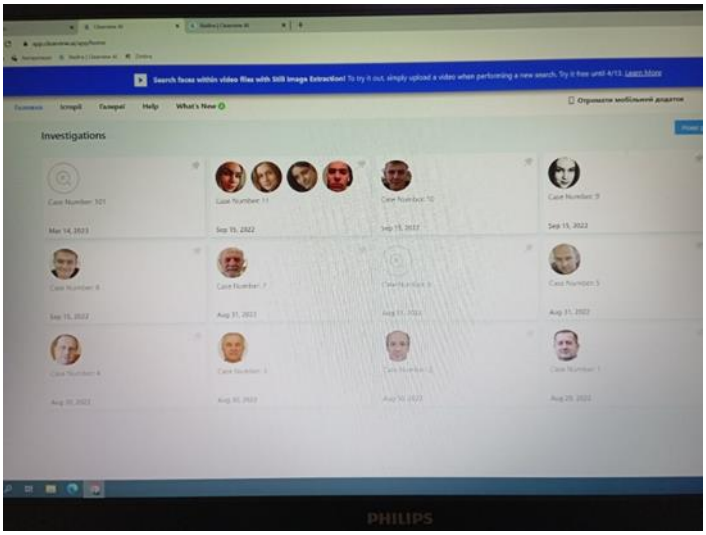

Рис. 1. Головна сторінка програми Clearview AI

Використання цієї програми поліцією має дуже гарні перспективи як в умовах воєнного стану, так і після нашої перемоги, тому підготовка курсантів до її використання має важливе значення.

1. Ryan Mac, Kashmir Hill. «Clearview AI settles suit and agrees to limit sales of facial recognition database». NY Times (May 9, 2022). URL : https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html (дата звернення: 27.10.2023).
2. «Twitter demands AI company stops ‘collecting faces’«. BBC News (January 23, 2020). URL: https://www.bbc.com/news/technology-51220654 (дата звернення: 27.10.2023).
3. James Clayton, Ben Derico. «Clearview AI used nearly 1m times by US police, it tells the BBC». BBC News, San Francisco (March 27, 2023). URL : https://www.bbc.com/news/technology-65057011 (дата звернення: 27.10.2023).
4. Війна в Україні. URL : https://www.clearview.ai/ukraine (дата звернення: 27.10.2023).
5. Kashmir Hill. «Facial Recognition Goes to War». NY Times (April 7, 2022). URL : https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html (дата звернення: 27.10.2023).

КАДІРОВА Аріна
курсантка 3 курсу ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
ТЕЛІЙЧУК Віталій,
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ОПЕРАТИВНИЙ ПОШУК ТА ЗНАЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ У ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

На теперішній час через введення воєнного стану на території України кардинально змінилось життя кожного українця. Також змінилось життя поліцейських, вони мають виконувати широкий спектр завдань, що не завжди є характерними для мирного часу. Чисельність кримінальних правопорушень також зростає, але їх характер змінюється. Зросла кількість злочинів проти основ національно безпеки, умисних вбивств, а також

військових злочинів. Наразі доля нетяжких правопорушень і кримінальних проступків, правопорушень проти власності зменшилась [1].

Розслідування зазначених правопорушень потребує нових шляхів для збирання, аналізу, обробки та зберігання доказової бази. Спеціалізовані підрозділи Національної поліції України які проводять оперативно-розшукову діяльність, окрім негласних (закритих) користуються і відкритими джерелами для пошуку слідів кримінального правопорушення, їх фіксації, тощо. Ми поєднуємо думку В. Телійчука і А. Антіпова, що до оперативно-розшукової інформації з відкритих джерел можна віднести:

– інформація яка міститься в мережі Інтернет. Це можуть бути веб-сайти, соціальні мережі, блоги, форуми, електронні дошки оголошень та інші.

– інформація, що міститься в ЗМІ. Це можуть бути газети, журнали, теле- та радіопрограми, а також соціальні мережі.

– інформація, що міститься в інших відкритих джерелах. Це можуть бути книги, статті, доповіді, звіти та інші.

Під час організації оперативного пошуку інформації з відкритих джерел існують певні особливості. Зокрема першою особливістю організації є залежність об’єкта оперативного впливу та виду оперативної інформації, що планується отримати, про:

– осіб, що готуються або вчиняють злочинну діяльність, або осіб що можуть мати інформацію про злочин;

– обставини підготовки та вчинення злочину;

– обставини, що сприяють вчиненню злочину, а також предмети, об’єкти або речі, що можуть становити значення для оперативно-розшукової діяльності або кримінального провадження.

Отже «оперативний пошук», це комплекс дій оперативного працівника, спрямований на отримання певних відомостей, передбаченим чинним законодавством [2, с.465].

Умовно оперативний пошук можна поділити на 4 певні етапи, такі як:

1. Визначення завдання. Першим кроком є визначення завдання, для якого потрібна інформація. Це допоможе сформувати правильний запит і знайти релевантні результати;

2. Формування запиту. Запит має бути чітким і зрозумілим. Він повинен містити ключові слова, пов’язані з завданням;

3. Вибір джерела інформації. Після того, як запит сформовано, потрібно вибрати джерела інформації. Це можуть бути веб-сайти, соціальні мережі, блоги та інші;

4. Аналіз результатів. Після того, як інформацію знайдено, її потрібно проаналізувати та перевірити на достовірність.

Оперативний пошук інформації в Інтернеті є важливим навиком, що може бути корисним у різних сферах діяльності. Він дозволяє швидко знаходити актуальну та необхідну інформацію, яка може бути використана

для вирішення конкретних завдань.

Інформація з відкритих джерел допомагає оперативним підрозділам виконувати їх обов'язки легше та швидше. У мережі Інтернет є велика кількість інформації, яка може бути використана для ідентифікації свідків і підозрюваних. Соціальні мережі, форуми блоги та інші онлайн-платформи дозволяють отримати доступ до профілів та публікацій осіб, які можуть бути причетні до злочину. Інформація про місцезнаходження, контакти та інші дані можуть бути важливим для розслідування.

Зазначимо, що оперативний пошук допомагає у зборі доказів. Фото, відео, повідомлення та інші дані, розміщені в мережі, можуть стати ключовими доказами в справах кримінального провадження. Оперативні працівники можуть використовувати ці дані для встановлення фактів і реконструкцій подій.

Отже, на наш погляд, оперативний пошук та відкриті джерела інформації є невід'ємною складовою роботи сучасних поліцейських у розкритті кримінальних правопорушень. Інтернет є великою банкою даних, які можуть бути важливими для виявлення та переслідування злочинців.

1. ДС редакція. Ще один бік медалі: як війна вплинула на рівень злочинності – DSnews.ua. «Ділова столиця» українською – найсвіжіші новини України та світу. URL : https://www.dsnews.ua/ukr/politics/shche-odin-bik-medali-yak-viyna-vplinula-na-riven-zlochinnosti-27022023-475107 (дата звернення: 22.10.2023).

2. Телійчук, Віталій, and Антон Антіпов. «ОПЕРАТИВНО-РОЗШУКОВА ПРОТИДІЯ РОЗПОВСЮДЖЕННЮ НАРКОТИЧНИХ ЗАСОБІВ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ: ДЕЯКІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ ДЖЕРЕЛ ІНФОРМАЦІЇ.» Наука і техніка сьогодні. 2022. №5(5). URL : http://perspectives.pp.ua/index.php/nts/issue/view/58/84 (дата звернення: 23.10.2023).

КОПИЛОВ Едуард
викладач кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ

ОБГРУНТУВАННЯ ЕТАПІВ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ВОЄННОГО СТАНУ

Одним із пріоритетних напрямків діяльності підрозділів Національної поліції в умовах воєнного стану є інформаційно-аналітична діяльність, який є дослідницьким процесом управління, що охоплює широкий комплекс заходів і методичних прийомів вивчення та оцінки інформації про стан, структуру та динаміку злочинності, рівень громадського порядку, стану оперативної

обстановки, результати практичної діяльності органів і підрозділів поліції з виконання поставлених перед ними завдань, а також умови, в яких ці завдання виконуються, що забезпечує оцінку ефективності роботи у розкритті та попередженні злочинів. Якість та повнота розкриття злочинів безпосередньо пов'язана з умінням застосовувати розвідувальну аналітику та проводити кримінальний аналіз, а саме - накопичувати, використовувати, обробляти та аналізувати оперативну інформацію, отриману з різних джерел.

Головною метою інформаційно-аналітичної діяльності є забезпечення процесу управління публічною, оперативною і оперативно-розшуковою діяльністю структур виконавчого механізму держави і суб'єктів господарювання шляхом постачання необхідної відкритої та закритої інформації, надання консультативно-прогностичної допомоги при прийнятті ними рішень.

Розумово-аналітична діяльність полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язку між даними, отриманими в ході розслідування, і даними, що мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальше проведення оперативно-стратегічного аналізу називається кримінальним аналізом [1, с.8].

В умовах воєнного стану кримінальний аналіз удосконалює методи роботи аналітика, оскільки його алгоритми допомагають успішно обробляти великі масиви даних різноманітних джерел з метою вилучення та використання необхідної інформації. Тож, кримінальний аналіз відіграє значну роль в розкритті та попередженні злочинів.

Процес кримінального аналізу – це ланцюжок оперативних дій або процедур, що ведуть до найбільш точного та обґрунтованого висновку з цієї інформації. Аналітичний етап процесу починається з отримання відповідних даних і організації їх у формі, яка дозволяє зрозуміти їх значення. Цей крок, опис даних, полегшує ідентифікацію відсутньої інформації та допомагає спрямовувати подальші зусилля зі збору даних [2, с.33].

Слід зазначити, що кримінальний аналіз як вид інформаційно-аналітичної діяльності в розкритті злочинів дає можливість отримання оперативно-значимої інформації не лише про події та об'єкти, але і про причинно-наслідкові зв'язки, додаткові кваліфікуючі ознаки (стійкість, згуртованість, розподілення ролей тощо). Крім того, у аналітика з'являється реальна можливість оперативного прогнозування ймовірних подій та прийняття відповідних рішень.

Збір даних є цілеспрямованим збором інформації з різних джерел відкритими та негласними методами, після чого її необхідно оцінити. Саме оцінка вимагає достовірності джерела інформації та правдивості її змісту. Упорядкуванням є саме зберігання інформації та система індексованих посилань для її пошуку. Мета опису даних передбачає узагальнення наявної інформації, щоб її значення стало більш зрозумілим для аналітика.

Критичним елементом аналізу є застосування індуктивної логіки для формування висновків про злочинну діяльність, її методи, ключових осіб, ступінь злочинної діяльності чи впливу.

Під час даного етапу виникає основа для введення індуктивного висновку з метою розробки однієї чи кількох гіпотез щодо основних сторін злочинної діяльності. Гіпотези перевіряються повторним збором, впорядкуванням, оцінкою, описом даних і циклом індуктивного обґрунтування. Кінцевою метою цього процесу є надання висновку – підсумку, передбачення чи розрахунку, на основі якого можна впевнено діяти [3, с.24].

Підсумовуючи вищевикладене, зазначимо, що заходи, які вживаються правоохоронними органами повинні бути більш ефективними, тому необхідно ретельно вивчати та реалізовувати на практиці концептуальні положення кримінального аналізу.

Отже, кримінальний аналіз відіграє значну роль у встановленні особи, яка причетна до вчинення злочину та безпосередньо його розкриття, має превентивну загальну методологію, даючи змогу провоохоронним органам бути на крок попереду злочинців, визначати тенденції та закономірності реагування, швидкому та ефективному запобіганню та розслідуванню кримінальних правопорушень.

1. Основи кримінального аналізу : підручник / А. М. Бабенко, О. М. Заєць, В. А. Некрасов, К. Ю. Ісмайлов, Д. О. Пефтієв та ін.; за заг. ред. О. Є. Користіна. Одеса, 2019. С.296.

2. Бараненко Р.В. Застосування сучасних аналітичних методів для оптимізації оперативно-розшукової діяльності підрозділів Національної поліції. Кримінальна розвідка: методологія, законодавство, зарубіжнийдосвід: матеріали Міжнародної науково-практичної конференції (м. Одеса, 29 квітня 2016 р.). – Одеса: ОДУВС, 2016. С. 33-34.

3. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. С.288.

КРУТЬ Тимур
курсант 1-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри інформаційних
та комунікативних технологій
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВОЄННОГО СТАНУ

Під час військового стану в Україні питання інформаційно-економічної безпеки є надзвичайно актуальним з тієї причини, що більшість населення нашої Батьківщини не є достатньо обізнаними у сфері інформаційної безпеки і можуть стати жертвами соціальної інженерії як з боку шахраїв, так і з боку держави-агресора.

Введення воєнного стану має значний вплив на інформаційне середовище суспільства, оскільки призводить до обмеження свободи слова та доступу до незалежної інформації. Під час воєнного стану часто спостерігаються цензурні обмеження, які можуть призвести до поширення пропагандистської інформації. Воєнний стан у країні сприяє поширенню дезорганізації та хакерських атак на системи збереження інформації, що, у свою чергу, може призвести до порушень безпеки даних.

Важливо підкреслити, що під час воєнного стану необхідно бути критичним до отриманої інформації та шукати джерела з різних джерел, щоб отримати об’єктивне уявлення про події.

Окрім власне громадян України, за інформаційною безпекою також стежать окремі Державні органи: однією з їх ключових ролей є забезпечення інформаційної безпеки країни. Державні органи виконують функцію координації та контролю за захистом інформаційних систем та даних в Україні. Вони встановлюють правову базу для регулювання сфери інформаційної безпеки та розробляють стратегічні плани щодо протидії кіберзагрозам. Державним органам також належить право проведення аудиту та перевірок систем безпеки.

Під час воєнного стану існує велика загроза для безпеки інформації, оскільки хакери та кіберзлочинці можуть використовувати цей період нестабільності, щоб зламати системи, викрасти конфіденційну інформацію або проникнути у мережеву інфраструктуру. Один з способів боротьби з

цими загрозами - установлення сильних паролів та шифрування даних, щоб запобігти несанкціонованому доступу до конфіденційної інформації. Регулярне оновлення програмного забезпечення та застосунків також є важливим для запобігання експлойтам та вразливостям, які можуть бути використані хакерами. Налагодження бекап-копій даних та зберігання їх на різних носіях одночасно може допомогти уникнути значних втрат інформації у разі кібератаки або несприятливих обставин, пов'язаних із воєнним станом.

Окрім проблем на інформаційному фронті, під час воєнного стану виникає багато викликів і загроз економічній безпеці, так як держава і її громадяни може зазнати серйозних збитків у сфері бізнесу та інвестицій. У такому нестабільному періоді можлива неконтрольована інфляція, що призводить до падіння купільної спроможності населення і загострення соціально-економічних проблем, зокрема, наявність погрози збройної агресії може призвести до припинення торговельних операцій і порушення ланцюжка постачання товарів, що, в свою чергу, негативно вплине на економіку країни. Змушена зупинка промислових підприємств, скорочення робочих місць та зниження споживчого попиту можуть спричинити загострення економічної кризи. В умовах воєнного стану, важливо приймати державні заходи для забезпечення економичної стабільності, привертання інвестицій та захисту прав бизнесменів і споживачів.

У перший тиждень жовтня кількість нових вакансій суттєво зросла, що може свідчити про пожвавлення ринку праці; втім, треба стежити за подальшою динамікою. Кількість поданих резюме є меншою, ніж у цей час рік тому. Від початку повномасштабного вторгнення Держстат не публікує даних щодо безробіття. Дослідницька агенція Info Sapiens робить власні оцінки його рівня. Відповідно до них, у вересні 2023 року рівень безробіття становив 15,9%. Безробіття трохи зросло порівняно з серпнем, коли його рівень становив 15,1%. Проксі-показник рівня бідності – частка опитаних людей, що змушена економити на їжі – у вересні 2023 року становив 24,7%. Індекс очікувань ділової активності НБУ за вересень зріс до 50,1 з 49,3 у серпні, перевищивши «нейтральне» значення на 50 пунктів. Це означає, що позитивні очікування широко поширені серед опитаних компаній. За даними НБУ, ділові очікування включають «поступове відновлення темпів виробництва, встановлення нових шляхів постачання продукції, зниження темпів зростання витрат на сировину та енергію, покращення інфляційних та курсових очікувань, а також стабільний внутрішній попит». є важливим суб'єктивним показником стану економіки, що свідчить про поступове відновлення діяльності. За попередніми даними НБУ, сальдо товарів і послуг у вересні 2023 року склало від'ємне 3,6 млрд доларів. У вересні імпорт товарів ($5,5 млрд) перевищив експорт товарів ($2,5 млрд), а імпорт послуг ($2 млрд) перевищив експорт послуг ($1,4 млрд). Що стосується обсягу депозитів населення, то строкові депозити в гривні залишилися без змін, а вклади на місцях зменшилися. Натомість строкові депозити в іноземній

валюті знову зафіксували зростання вперше з березня 2023 року. Такі зміни можуть бути пов'язані з девальвацією гривні в серпні.

Роль державних органів у забезпеченні економічної безпеки полягає у формуванні та реалізації стратегічної політики, що сприяє економічній стабільності та зростанню. Державні органи мають на меті захистити економіку від негативних впливів зовнішнього середовища, таких як підробка продукції, контрабанда чи недобросовісна конкуренція. Вони також здатні реагувати на кризові ситуації та проводити необхідний аналіз законодавства для покращення умов для ведення бізнесу та інвестиційного клімату. Державні органи також мають повноваження сприяти розвитку державно-приватного партнерства для прискорення економічного зростання та стимулювання інновацій. Загальною місією державних органів є забезпечення сталого економічного розвитку, захист добробуту громадян, підтримка соціальної та економічної стабільності.

Умови воєнного стану можуть поставити економіку країни під загрозу, тому важливо мати механізми для захисту її функціонування. Один із таких механізмів – обмеження зовнішньоекономічної діяльності, що дозволяє контролювати і регулювати експорт та імпорт товарів. Додатковий захист може бути забезпечений шляхом введення фінансових обмежень, таких як капіталові контролі або обмеження на операції з готівкою. Серйозний нагляд і регулювання банківської сфери можуть бути іншим ефективним механізмом для захисту економіки в умовах воєнного стану. Наведення спеціальних заходів по підготовці до можливостей серединних загроз економіці, таких як посилена підтримка секторів, що залежать від експорту, або стимулювання внутрішнього споживання, також може бути корисним механізмом захисту.

Однак, окрім охорони та підтримання стабільності економічної та інформаційної безпеки, їх ще потрібно розвивати Рекомендації щодо політичних та економічних питань, спрямовані на покращення інформаційної та економічної безпеки, можуть включати розширення контролю над поширенням дезінформації і фейкових новин. Важливо забезпечувати прозору та надійну інформаційну базу для прийняття політичних та економічних рішень, включаючи доступ до достовірних даних та статистики. Одним з ключових аспектів покращення економічної безпеки є розвиток сильної правової системи, що гарантуватиме захист прав власності і боротиметься з корупцією. Залучення кваліфікованих фахових кадрів у сферу політики та економіки може позитивно впливати на формулювання стратегій І рекомендації для забезпечення інформаційної та економічної безпеки. Координація між політичними і економічними органами, включаючи співпрацю з міжнародними партнерами, може сприяти впровадженню рекомендацій щодо політичних та економічних питань з метою покращення інформаційної та економічної безпеки.

1. Д. Смотрич, Л. Браілко, Інформаційна безпека в умовах воєнного стану / Том 2 № 77 (2023): Науковий вісник Ужгородського національного університету. Серія: Право. URL : http://visnyk-pravo.uzhnu.edu.ua/article/view/284104
2. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. URL : https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v
3. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. URL : https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku
4. Тетяна Богдан, Фінансово-економічні наслідки війни. URL : https://lb.ua/blog/tetiana_bohdan/550614_finansovoekonomichni_naslidki.html
5. Толошна Н. В. Вплив інформаційного простору на національну безпеку в умовах воєнного стану. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VII Міжнар. наук.-практ. конф. (м. Дніпро, 17 бер. 2023 р.). Дніпро : ДДУВС, 2023. С. 555-557 https://er.dduvs.in.ua/handle/123456789/11208
6. Максим Самойлюк, Трекер економіки України під час війни. URL : https://ces.org.ua/tracker-economy-during-the-war/

КУРИЛО Дмитро
курсант 2 курсу факультету №4
Науковий керівник:
СВІТЛИЧНИЙ Віталій
кандидат технічних наук, доцент,
доцент кафедри протидії
кіберзлочинності факультету №4
Харківського національного
університету внутрішніх справ

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ БОРОТЬБИ З ПРАВОПОРУШНИКАМИ КОМЕНДАНТСЬКОЇ ГОДИНИ

Вступ: Під час широкомасштабної агресії російської федерації проти українського народу та територіальної цілісності, дуже гостро постало питання що до забезпечення правопорядку у державі. З 24 лютого 2022 року, було зафіксовано більш ніж 330 кримінальних проваджень за фактом крадіжок, що вчинені під час венного стану [1]. Більшість з цих правопорушень були скоєні у нічний час доби, що могло бути менш помітним як для громадян, так і для працівників правоохоронної діяльності. Також, хотілось додати про те, що з 2022 року діяльність правоохоронних органів здійснювалась в умовах підвищеного навантаження, що пов'язано з виконанням як безпосередньо функцій з протидії злочинності, так і з

виконанням завдань з відсічі та стримування збройної агресії російської федерації в слідстві чого, поліція не могла швидко реагувати на повідомлення від громадян [2]. Також, постало питання, щодо громадян, які через "кураторів", які пропонували їм по 4 тисяч гривень за координати чи фото місця знаходження Збройних сил України або багатолюдних місць, про виявлення їх та притягнення до покарання. Офіційне число розглянутих справ та притягнення таких громадян до відповідальності не розгладшають, але явно одне, вони працюють теж у нічну пору доби як і мародери.

На мою думку, щоб підвищити ефективність у виявленні правопорушників під час комендантської години (у тому числі після воєнного стану), треба застосовувати безпілотні літальні апарати (далі. БПЛА) у патрулюванні зі спеціальними налаштуваннями та зміненою системою польоту, навігації та камерою.

По-перше, хотів би змінити його навігаційну систему та систему геолокаційного трекінгу. Безпілотник має завантажену карту вулиці, за якою він закріплений, де кілька антен, розміщенні на телекомунікаційних антенах, що знаходяться на дахах багатоповерхівок. Ці ж антени, могли б прискорити передачу даних між дроном та оператором. Сам дрон, який автономною системою навігації, рухався по заздалегідь зазначеному маршруту.

По-друге, звичайну камеру, замінити на тепловізійну камеру з датчиком руху. Як тільки камера фіксувала рух, вона передавала координати до оператора. Оператор, своєю чергою, доповідає до найближчої патрульної машини про те, що поступи сигнал від дрона про виявлення правопорушника комендантської години. Патрульна поліція одразу прибуває на визначенні координати такими шляхами, щоб правопорушник не міг змогу втекти. У весь час, БПЛА транслює координати підозрюваного, поки патрульна поліція не наблизиться до нього.

По-третє, треба буде змінити систему польоту. Якщо для тих цілей взяти дрони як DJI Mavic 3, якого середня тривалість польоту приблизно 40 хвилин [3], то тоді треба буде використовувати тихий режим польоту, що означає більше витрат на батарею, що, своєю чергою може привести до скородження тривалості польоту до 30 хвилин. Якщо використовувати або взагалі створити спеціальний дрон, який буде вузько спрямований тільки на ці дії, то тоді треба робити його габарити менше DJI Mavic 3 у 1,5 раза, та використовувати 6-сть лопатей, що в теорії може вплинути на гучність та більш мобільність його. Що до камери, то тоді краще застосувати тепловізійну камеру GSTiR COIN417G2+9.1 9,1 мм [4]. Він компактний зі спектральним діапазон: 8-14 мкм та напруга живлення: 4~5,5 В, що, в теорії, може працювати від декількох батарейок, що своєю чергою, дає змогу зробити два, не важких для дрона по вазі, джерела живлення.

Висновки: Наша держава має значну базу літакобудування та технологічний потенціал, а також можливість стати одним з ключових гравців у виробництві та розвитку безпілотних літальних апаратів не лише у

військовій сфері, а й сфери забезпечення громадської безпеки та порядку, в тому числи в умовах військового стану.

1. ЗВІТ Національної поліції України про результати роботи у 2022 році : Звіт. URL : https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf (дата звернення: 22.10.2023).

2. Лотоцька Н. За фактами мародерства зареєстровано понад 330 кримінальних проваджень, Клименко. LB.ua. URL : https://lb.ua/society/2022/03/28/511392_faktami_maroderstva.html (дата звернення: 22.10.2023).

3. GSTiR COIN417G2+9.1 тепловізійна камера з об'єктивом 9,1мм для дронів, 384×288/17мкм, 8-14мкм – ТОВ «Селток Фотонікс». ТОВ «Селток Фотонікс» – перший професійний каталог оптоелектроніки. URL : https://seltokphotonics.com/catalog/gstir-coin417g2-9-1-teploviziyna-kamera-z-ob-ektyvom-9-1mm-dlya-droniv-384-288-17mkm-8-14mkm/ (дата звернення: 22.10.2023).

4. Mavic 3 - Technische Daten - DJI. DJI Official. URL : https://www.dji.com/global/mavic-3/specs (date of access: 22.10.2023).

МОРДВИНЦЕВ Микола
провідний науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у
кіберпросторі,
кандидат технічних наук, доцент
ХЛЄСТКОВ Олексій
старший науковий співробітник
науково-дослідної лабораторії з
проблем інформаційних технологій та
протидії злочинності у кіберпросторі
Харківського національного
університету внутрішніх справ

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТАХ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Для ефективного застосування засобів фото- та відеозапису які базуються на безпілотних літальних і використовуються в Національній поліції України (далі – НП України) в структурі центрального органу управління поліції створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (далі – УПВП), основними завданнями якого є організація, координація, методичне забезпечення й контроль службової діяльності підрозділів поліції на воді та забезпечення

повітряної підтримки підрозділів Національної поліції України.

Виконання завдань, покладених на НП України в умовах воєнного стану, вимагає підвищення ефективності використання наявних, а також розвиток нових сил і засобів у сферах: охороні громадського порядку, публічної безпеки та безпеки дорожнього руху; – виявленні, припиненні та протидії адміністративним та кримінальним правопорушенням; припиненні терористичної чи розвідувальної діяльності, діяльності незаконних воєнізованих або збройних формувань, колабораціонізму ,терористичних організацій, організованих груп та злочинних організацій; забезпечення охорони прав і свобод людини, інтересів суспільства та держави, протидії злочинності, підтримання публічної безпеки і порядку, а також надання поліцейських послуг; співпраці в питаннях захисту державного кордону й охорони суверенних прав України; цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню; громадянства та міграції тощо. Воно об'єктивно передбачає запровадження нової моделі управління, координації та контролю, визначення концептуальних засад її розбудови [1 с. 27].

Відповідно до Плану розвитку Національної поліції України, УПВП розроблено низку заходів для створення системи повітряної підтримки. Основою такої системи є застосування авіаційної техніки (вертольотів і безпілотних авіаційних комплексів (далі – БпАК) для виконання завдань, покладених на поліцію.

Згідно з вимогами п. 30 ст. 1 Повітряного кодексу України авіація НП України належить до державної авіації. Відповідно до Правил виконання польотів державної авіації України та наказом НП України «Про допуск до експлуатації (прийняття на озброєння) в органах та підрозділах Національної поліції України безпілотних літальних апаратів» від 27.02.2019 № 196 УПВП визначено органом управління безпілотної авіації Національної поліції.

Сьогодні безпілотні літальні апарати (далі – БпЛА) широко використовують в Національній поліції України, зокрема в УПВП. Окрім того, УПВП координує діяльність п'яти підрозділів центрального органу управління поліції (ДПП, ДЗТ, ДОС, ДОТЗ, УПВП) та двадцяти чотирьох головних управлінь Національної поліції в областях з питань використання БпЛА.

Основними напрямками використання БпЛА підрозділами поліції під час виконання завдань є:

повітряна розвідка, відстеження оперативної обстановки під час виконання службових (поліцейських) завдань;

висотне спостереження під час проведення культурно-масових, суспільно-політичних і спортивних заходів, а також під час припинення масових заворушень і загрози блокування об'єктів;

супроводження розслідування в межах єдиного реєстру досудових розслідувань;

виявлення злочинів та адміністративних правопорушень, фото- та відеодокументування, забезпечення зв'язку й управління наземними нарядами поліції, їх взаємодія з іншими силовими підрозділами;

моніторинг для забезпечення безпеки дорожнього руху;

порятунок і пошук зниклих людей.

У будь-який час, у складних умовах і в максимально короткі терміни застосування зазначеної техніки дає можливість здійснювати моніторинг обстановки в режимі реального часу, забезпечує якісний і своєчасний обмін інформацією між підрозділами Національної поліції, а також оперативне прийняття ними рішень.

З метою підвищення ефективності службової діяльності УПВП розроблено Методичні рекомендації щодо виконання польотів безпілотними авіаційними комплексами НП України та їх технічної експлуатації відповідно до вимог та нормативно-правових актів державної авіації України, а також Програму навчання зовнішніх пілотів (операторів) безпілотних літальних апаратів І класу за базовим кваліфікаційним рівнем І, схвалену Управлінням регулювання діяльності державної авіації Міністерства оборони України і затверджену Головою Національної поліції України.

Названа Програма є основним документом, який визначає порядок, послідовність, зміст, обсяг, умови здійснення підготовки екіпажу БпАК до виконання завдань за призначенням. Вона складається з курсу теоретичної та практичної підготовки зовнішніх пілотів (операторів), охоплює базові знання з авіаційної метеорології, аеродинаміки, впливу людського чинника, безпеки польотів, правил польотів і правил використання повітряного простору державної авіації під час експлуатації БпАК.

Враховуючи перспективи використання БпЛА в органах і підрозділах поліції, з метою належного виконання покладених на поліцію завдань і функцій заплановано провести підготовку/перепідготовку поліцейських, які у службовій діяльності використовують БпЛА.

Одним із пріоритетних напрямів діяльності УПВП на сьогодні є протидія правопорушенням, які вчиняються за допомогою БпЛА, зокрема попередження несанкціонованих польотів зазначених повітряних суден над територією стратегічних об'єктів енергокомплексу України, критичної інфраструктури, недопущення вчинення терористичних актів, диверсій, ведення розвідки уздовж прикордонних смуг, у тому числі в районах проведення ООС. Поліцейські постійно залучаються до забезпечення заходів з протидії правопорушенням під час проведення масових заходів державного рівня та спеціальних поліцейських операцій, до проведення роботи, що гарантує безпеку громадян, захист інтересів держави, її суспільних інститутів. Розробляються й упроваджуються рішення, спрямовані на подальший ефективний розвиток системи повітряної підтримки НП України.

Основні середньострокові цілі УПВП: ініціювання змін, спрямованих на вдосконалення нормативно-правової бази, у тому числі у сфері

застосування БпЛА і засобів контр-БпЛА в правоохоронній діяльності, протидії правопорушенням на воді, забезпечення безпеки на морському та річковому транспорті;

відбір, підготовка поліцейських відповідно до вимог та специфіки завдань, функцій і практичної спрямованості системи підрозділів поліції повітряної підтримки.

1. Мордвинцев М. В. та ін. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції . МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 44 с.

НЕКЛЕСА Олександр
викладач кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЗАХОДУ ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У ВИГЛЯДІ АРЕШТУ МАЙНА

Недоторканність права власності є однією із засад кримінального провадження, реалізація якої регламентується окрім ст.ст. 7, 16 Кримінального процесуального кодексу України, також ст. 40 Конституції України, Протоколом 1 до Конвенції про захист прав людини і основоположних свобод (ратифікований Верховною Радою України 17.07.1997 року), правовими позиціями Європейського суду з прав людини, що відповідно до ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» та згідно зі ст. 8, 9 КПК України, визнаються джерелом права, а їх застосування та врахування є обов’язковим під час здійснення кримінального провадження для усіх правозастосувачів.

Аналіз вищезазначених нормативних джерел дозволив зробити висновок, що попри те, що держава і гарантує забезпечення права власності, однак в окремих випадках дозволяє його обмежувати або навіть позбавляти. Так, відповідно до ч.2 ст. 170 КПК України, арешт майна допускається з метою забезпечення: 1) збереження речових доказів; 2) спеціальної конфіскації; 3) конфіскації майна як виду покарання або заходу кримінально-правового характеру щодо юридичної особи; 4) відшкодування шкоди, завданої внаслідок кримінального правопорушення (цивільний позов), чи стягнення з юридичної особи отриманої неправомірної вигоди [1].

Оскільки право приватної власності охороняється законом згідно з

Конституцією України, а накладення арешту на майно обмежує дане право, то застосування цього примусового заходу можливе лише за судовим рішенням. Згідно ч.1 ст. 170 КПК України, арешт майна у кримінальному провадженні здійснюється за ухвалою слідчого судді або суду [1].

Слід зазначити, при прийнятті рішення про застосування арешту майна слід враховувати не тільки питання, пов'язані з обмеженням прав підозрюваної особи щодо можливості відчуження, розпорядження та/або користування майном, а й питання, пов'язані з реалізацією прав потерпілого на відшкодування шкоди, заподіяної кримінальним правопорушенням. Так, несвоєчасний арешт майна, спрямований на забезпечення цивільного позову, може призвести до того, що шкоду, заподіяну кримінальним правопорушенням, взагалі буде складно відшкодувати у зв'язку з тим, що на момент заявлення цивільного позову майно буде знищено, пошкоджено, приховано тощо. Така ситуація, у свою чергу, загрожує порушенням прав потерпілого [2; с.120].

Також слід звернути увагу на забезпечення належного зберігання майна, на яке накладено арешт. Наприклад, під час вирішення питання щодо передачі нерухомого майна на відповідальне зберігання, метою якого є збереження майна до скасування його арешту у встановленому КПК України порядку, потрібно враховувати, що така передача майна не спричиняє наслідків, що негативно позначаються на інтересах будь-яких інших фізичних або юридичних осіб. Зокрема, передачу майна на відповідальне зберігання можна розцінювати як найменш обтяжливий спосіб арешту, тобто зміну способу арешту майна у відповідності до положення ч. 4 ст. 173 КПК України. У такому випадку власник (законний володілець) майна зобов'язується прийняти нерухоме майно на відповідальне зберігання та забезпечити зберігання майна до скасування арешту у встановленому КПК України порядку [3; с.58].

Таким чином, інститут накладення арешту на майно є одним із інструментів захисту конституційних прав осіб, залучених до кримінального судочинства, від наслідків вчиненого кримінального правопорушення. Однак, разом з цим, процедура застосування арешту майна потребує подальшого наукового дослідження та вдосконалення на законодавчому рівні.

---

1. Кримінальний процесуальний кодекс України від 13.04.2012 року № 4651-VI. URL : http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення 03.10.2023).

2. Гарасимів О., Захарова О., Ряшко О. Арешт майна у кримінальному провадженні. Юридичний вісник № 2. 2022. с. 118-123. URL : http://yuv.onua.edu.ua/index.php/yuv/article/view/2329/2621 (дата звернення 02.10.2023).

3. Якових Є. В. Актуальні питання передання майна на відповідальне зберігання під час кримінального провадження. Кримінальна юстиція сучасної України: виклики та перспективи: матеріали Міжнар. наук.-практ. конф., присв. до 75-річчя д.ю.н., проф. Ю. П. Аленіна (м. Одеса, 20 лист. 2021 р.) / відп. ред.: Л. І. Аркуша, О. О. Торбас, В. А. Завтур; НУ «ОЮА». Одеса, 2021. С. 55-59.

НЕКЛЕСА Олександр
викладач кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ГАРАНТІЙ ЗАБЕЗПЕЧЕННЯ ЗАКОННОСТІ ТА ОБГРУНТОВАНОСТІ ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Однією з фундаментальних категорій науки кримінального процесу вважаються кримінальні процесуальні гарантії, які прийнято розглядати як елемент кримінальної процесуальної форми поряд із закріпленими законом юридичними процедурами та умовами [1, с. 16].

Аналізуючи вимоги щодо наявності підстав проведення НСРД, звернемось до ст. 246 КПК, виходячи з нормативного змісту якої проведення НСРД є законним за наявності фактичної, матеріальної та юридичної підстав.

Ч. 2 ст. 246 КПК встановлює матеріальну підставу для проведення НСРД – можливість проведення переважної більшості цього різновиду слідчих (розшукових) дій лише у кримінальному провадженні щодо тяжких та особливо тяжких злочинів. Але якщо на момент проведення НСРД існували достатні підстави для припущення щодо вчинення діяння, яке кваліфікується як тяжкий або особливо тяжкий злочин, а при проведенні подальшого розслідування кваліфікацію було змінено на злочин середньої тяжкості, то фактичні дані, отримані в результаті проведення НСРД, можуть бути доказами в даному кримінальному провадженні. Якщо на момент проведення НСРД вказані достатні підстави для кваліфікації діяння як тяжкого чи особливо тяжкого злочину не існували, то отримані в їх результаті фактичні дані не можуть бути визнані доказами [2, с. 160].

Переходячи до характеристики вимог щодо кола суб'єктів, уповноважених на проведення НСРД, відзначимо, що згідно з ч. 6 ст. 246 КПК проводити вказані дії має право слідчий, який здійснює досудове розслідування злочину, або за його дорученням - відповідні уповноважені оперативні підрозділи. На думку А. П. Глушка та І. В. Строкова, розширення можливостей слідчого завдяки об'єднанню слідчої і розшукової діяльності та запровадження нових засобів збирання ним доказів шляхом проведення НСРД забезпечує досягнення позитивних результатів [3, с. 140-145].

Отже, закон має з чіткістю визначати межі такої переваги, наданої компетентним органам, і порядок її здійснення, з урахуванням законної мети заходу, щоб забезпечити особі належний захист від свавільного втручання.

1. Трофименко В. М. Теоретичні та правові основи диференціації процесу-альної форми у кримінальному судочинстві: монографія. Харків : ТОВ «Оберіг», 2016. 304 с.

2. Панова А. В. Визнання доказів недопустимими у кримінальному прова-дженні: монографія. Харків : Право, 2017. 256 с.

3. Глушко А. П., Строков І. В. Негласні слідчі (розшукові) дії в криміналь-ному провадженні: проблемні питання проведення. Право і суспільство. 2013. №3/2013. С. 140-145.

ГАБОРЕЦЬ Ольга
доцент кафедри
оперативно-розшукової діяльності
та інформаційної безпеки
Донецького державного університету
внутрішніх справ, доктор філософії

РОЛЬ І ВАЖЛИВІСТЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ В СУЧАСНІЙ ПРАВООХОРОННІЙ СИСТЕМІ

Сучасна правоохоронна система, знаходячись в умовах постійних трансформацій у суспільстві та технологічного розвитку, стикається з низкою викликів та завдань, які вимагають адаптації та удосконалення. Один із основних аспектів, що домінує в сучасній правоохоронній системі, полягає в обробці та аналізі великої кількості інформації, що надходить з різних джерел. Роль та важливість інформаційно-аналітичної діяльності в цьому контексті стають неабияк актуальними й важливими для забезпечення ефективності та ефективності діяльності правоохоронних органів.

З розвитком інформаційних технологій та зростанням доступності інформації стало можливим збирати, зберігати та обробляти великі обсяги даних. Проте, інформаційна рівень в сучасному суспільстві не тільки відкриває нові можливості, але й створює складні завдання у сфері правоохоронної діяльності. Інформація стала критичним ресурсом, який впливає на прийняття стратегічних рішень і ефективність заходів, спрямованих на підтримання законності та забезпечення громадської безпеки.

Інформаційно-аналітична діяльність в правоохоронній системі включає в себе збір, обробку, аналіз та інтерпретацію даних, а також передбачення подій та загроз. Вона спрямована на надання правоохоронним органам інформації, яка стає відомою шляхом збору та аналізу різних джерел, включаючи відкриті джерела, інформацію від інформаторів, внутрішні дані та багато інших.

Діяльність інформаційно-аналітичних служб правоохоронних органів

включає в себе також розробку аналітичних моделей, використання інформаційних технологій для обробки великих обсягів даних, включаючи машинне навчання та штучний інтелект, а також співпрацю з іншими національними та міжнародними організаціями у сфері обміну розвідувальною інформацією та боротьби з транскордонною злочинністю.

Специфіка правоохоронної діяльності вимагає не лише реакції на події, а й активного аналізу, передбачення та попередження можливих загроз. У цьому контексті, роль і важливість інформаційно-аналітичної діяльності стають важливими аспектами сучасної правоохоронної системи, які допомагають забезпечити безпеку громадян, реагувати на злочини та забезпечувати додержання закону. Тому дослідження ролі цієї діяльності має велике значення для розвитку та модернізації правоохоронних органів та забезпечення громадської безпеки в умовах сучасного світу.

Сприяючи правоохоронним органам у зборі та аналізі інформації, інформаційно-аналітична діяльність стає інтегральною складовою виявлення та розслідування злочинів, їх прогнозування та запобігання. Ця діяльність допомагає розкривати складні взаємозв’язки між злочинними об’єктами та суб’єктами, ідентифікувати мережі злочинності та незаконні зв’язки, а також оцінювати потенційні загрози для національної та глобальної безпеки.

Здатність аналізувати велику кількість даних, розуміти їх значення та виявляти тенденції є ключовим елементом в успішній роботі правоохоронних органів у сучасному світі. Важливість інформаційно-аналітичної діяльності розкривається не лише на рівні національних структур, але й на міжнародному рівні, де спільна обмін інформацією та аналітичними даними між країнами стає ключовим інструментом в боротьбі з транснаціональною злочинністю та тероризмом.

Таким чином, дослідження ролі й важливості інформаційно-аналітичної діяльності в сучасній правоохоронній системі є актуальним завданням, спрямованим на покращення роботи правоохоронних органів та підвищення рівня безпеки суспільства.

ПАНЧЕНКО Ілля
курсант 1-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри інформаційних
та комунікативних технологій
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ

Тема 1. Мета, завдання, предмет навчальної дисципліни «Інформаційно-аналітична діяльність» та її специфіка

Основні етапи інформаційно-аналітичної діяльності включають:

1. Збір інформації: Цей етап включає пошук, вибір і отримання інформації з різних джерел, таких як документи, бази даних, Інтернет, опитування тощо. Важливо акумулювати достовірну інформацію, яка є релевантною для конкретних цілей.

2. Аналіз інформації: На цьому етапі проводиться ретельний розгляд зібраної інформації з метою виявити потенційні залежності, зв'язки, тенденції та інші важливі фактори. Використовуються різні методи інтерпретації даних, статистичного аналізу, моделювання та інші методи.

3. Оцінка та інтерпретація результатів: На цьому етапі висуваються висновки, пропозиції та рекомендації на основі виявлених залежностей та аналізу результатів. Інтерпретація результатів може охоплювати оцінку потенційних ризиків, можливостей, перспектив розвитку та інших аспектів.

4. Використання результатів: Отримані знання та висновки можуть бути використані для прийняття рішень в різних сферах діяльності, включаючи бізнес, політику, науку, освіту, розробку стратегій тощо. Інформаційно-аналітичні результати можуть допомогти удосконалити роботу організації, спрогнозувати ризики та виявити можливості.

В рамках курсу майбутні фахівці познайомляться з системою знань про інформацію, інформаційне забезпечення та джерела інформації, знаннями про інформаційні ресурси, особливості інформаційних процесів, властивості та способи отримання необхідної інформації, типи та види інформаційних продуктів і послуг, про основи формування у здобувачів уміння виявляти джерела необхідної інформації, дізнаються як здійснювати моніторингові дослідження з використанням усіх доступних джерел інформації, аналізом достовірності отриманої інформації, специфікою основних принципів комплектування, познайомляться з колом нормативно-правових актів, які

регулюють правовідносини в інформаційній галузі, оволодіють навичками підготовки та редагування аналітичних матеріалів, створення інформаційних масивів за певною тематикою, здійснення експертного оцінювання і підготовки експертного висновку для прийняття рішення, дізнаються про сучасні тенденції розвитку інформаційного забезпечення й аналітичного опрацювання інформації на потребу держави і суспільства, що дасть можливість визначити модель управлінської структури інформаційного суспільства XXI ст

Основна мета інформаційно-аналітичної діяльності полягає в тому, щоб мати доступ до якісної та орієнтованої на результат інформації, розуміти її і використовувати для досягнення поставлених цілей. Це важливий процес, який допомагає організаціям і людям діяти на основі обґрунтованих даних та розуміння ситуації.

Завдання курсу:

• з’ясувати місця і ролі інформаційно-аналітичної діяльності в практичній діяльності;

• допомогти в опануванні специфіки методології, структури та видової

• розгалуженості інформаційно-аналітичних процесів; ознайомити з базовими інформаційно-аналітичними технологіями;

• навчити застосовувати окремі інформаційно-аналітичні технології для аналізу

• інформаційних процесів та явищ.

• окреслити та розкрити коло нормативно-правових актів, які регулюють

• правовідносини у інформаційній галузі розкрити форми та методи створення інформаційної бази, моніторингу подій, оцінки інформації;

• навчити орієнтуватись у складних соціокультурних процесах, аналізувати їх перебіг,

• моделювати та прогнозувати розвиток подій, обґрунтовувати прийняті рішення;

• сформувати у студентів уміння виявляти джерела необхідної інформації,

• здійснювати моніторингові дослідження з використанням усіх доступних джерел інформації, аналізувати достовірність отриманої інформації, готувати та редагувати аналітичні матеріали, створювати інформаційні масиви за певною тематикою, здійснювати експертне оцінювання і підготовку експертного висновку для прийняття рішення;

• сформувати знань і уміння щодо підготовки оглядів з актуальних соціальних,економічних питань, аналітичних доповідей, довідок та інших матеріалів, використовуючи інформаційно-пошукові системи.

У результаті вивчення навчальної дисципліни «Інформаційно-аналітична діяльність в державних і недержавних структурах» студент буде:

знати:

1. структуру та особливості функціонування сфери публічного управління та адміністрування; стандарти, принципи та норми діяльності у сфері публічного управління та адміністрування; основні нормативно-правові акти та положення законодавства у сфері публічного управління та адміністрування;

2. технології вироблення, прийняття та реалізації управлінських рішень; теоретичні, методологічні і практичні аспекти здійснення моніторингу соціально-політичної ситуації у країні з метою прийняття ефективних управлінських рішень

вміти:

1. здійснювати пошук та узагальнення інформації, робити висновки і формулювати рекомендації в межах своєї компетенції; налагодити комунікації між громадянами та органами державної влади і місцевого самоврядування; корегувати професійну діяльність у випадку зміни вихідних умов;

2. використовувати дані статистичної звітності, обліку та спеціальних досліджень у професійній діяльності; застосовувати різні технології прийняття управлінських рішень, враховуючи інтереси й потреби громадян, представників певної спільноти, суспільства та держави; розробляти рекомендації для органів державної влади та місцевого самоврядування щодо упередження та нівелювання чинників дестабілізації суспільно-політичних процесів.

Інформаційно-аналітична діяльність - це процес, що включає збір, аналіз і оцінку інформації з метою формування корисних знань, розуміння поточної ситуації і прийняття свідомих рішень. У сучасних умовах специфіка інформаційно-аналітичної роботи полягає в забезпеченні особи, яка приймає рішення (управлінця), необхідною і достатньою кількістю аналітичної інформації для прийняття єдино правильного, ефективного в умовах непередбаченості і кризових явищ управлінського рішення.

Таким чином, інформаційно-аналітична діяльність певною мірою убезпечує, захищає керівників, управлінців від ризиків, небезпек і викликів сьогодення, рекомендуючи те чи інше ефективне управлінське рішення, прогнозуючи наперед наслідки його прийняття чи неприйняття, чи бездіяльності. Зокрема, вказуються як позитивні так і негативні наслідки прийняття/неприйняття таких рішень.

Тема 2. Інформаційно-аналітичні послуги: різновиди, характеристика

Інформаційно-аналітичні послуги складають значний відсоток в межах загального поняття “інформаційні послуги”, оскільки для процесу та результату їх створення притаманні саме методи та засоби “інформаційної аналітики”

Інформаційно-аналітичні послуги включають в себе різноманітні сервіси, які надаються для збору, обробки, аналізу та поширення інформації з метою допомоги клієнтам в прийнятті рішень. Ці послуги можуть бути

надані як зовнішнім провайдером, так і внутрішньою аналітичною службою компанії. Основні різновиди інформаційно-аналітичних послуг включають:

1. Збір та агрегація даних: ця послуга включає збір інформації з різних джерел, які можуть бути внутрішніми або зовнішніми, а також її узагальнення і структурування. Це може включати моніторинг ринків, дослідження конкурентів, збір соціальної інформації та багато іншого.

2. Аналіз даних: ця послуга включає обробку і аналіз зібраних даних з метою виділення корисної інформації і виявлення тенденцій і патернів. Це може включати статистичний аналіз, лінійну алгебру, машинне навчання та інші методи аналізу даних.

3. Візуалізація даних: ця послуга надається для візуального представлення зібраної і проаналізованої інформації шляхом використання діаграм, графіків, інфографіків та інших методів візуалізації. Це допомагає клієнтам легше сприймати і розуміти складну інформацію.

4. Прогнозування та моделювання: ця послуга включає прогнозування майбутніх подій і результатів на основі наявних даних та створення моделей для аналізу різних сценаріїв. Це може бути корисно для розробки стратегій та планування дій.

5. Презентація результатів: після аналізу інформації та отримання результатів, ця послуга надає можливість презентувати інформацію клієнту у зрозумілій та доступній формі. Це може включати підготовку звітів, презентацій, дашбордів та інших інструментів для передачі даних.

Тема 3. Інформаційна аналітика як засіб одержання знань. Інформаційно-аналітичний процес: суть, принципи.

Інформаційна аналітика є процесом, який включає збір, аналіз та інтерпретацію інформації з метою отримання цінних знань і розробки висновків. Вона допомагає приймати обґрунтовані рішення, розробляти стратегії і виявляти тенденції.

Суть інформаційно-аналітичного процесу полягає у перетворенні великого обсягу інформації у зрозумілу і корисну форму. Це включає збір даних і фактів, їх аналіз, методи інтерпретації та моделювання, а також виведення висновків і рекомендацій.

Принципи інформаційно-аналітичного процесу включають:

1. Об’єктивність – основані на фактах інформація і аналіз мають бути безпристрасними і недискримінаційними.

2. Точність – надійна і перевірена інформація, яка базується на достовірних джерелах.

3. Комплексний підхід – урахування всіх аспектів проблеми, включаючи економічні, соціальні, технологічні й інші фактори.

4. Аналітична дисципліна – застосування систематичного підходу до збору і аналізу інформації.

1. URL : https://subj.ukr-lit.com/osnovi-informacijno-analitichno%D1%97-diyalnosti-zaxarova-i-v-5-2-informacijno-analitichni-poslugi-riznovidi-xarakteristika/
2. URL : http://megalib.com.ua/book/22_Informaciino_analitichna_diyalnist. html
3. URL : https://r.donnu.edu.ua/bitstream/123456789/1516/1/22_%D0%9C%D0%B0%D0%BA%D0%B5%D1%82_%D0%9A%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%86%D0%90%D0%94.pdf

ПАШКЕВИЧ Ольга
здобувач вищої освіти 3 курсу
спеціальність 262 «Правоохоронна діяльність» факультету підготовки фахівців для підрозділів кримінальної поліції
ЧОРНА Аліна
старший викладач кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ

У зв’язку з повномасштабним вторгненням рф в Україну 24 лютого 2022 року в Україні введено воєнний стан[1].Дана тема наразі є особливо актуальною в Україні, адже в умовах воєнного стану кіберзлочинці активно займаються зломом державних серверів, дезінформацією населення, використанням фейкових профілів у соціальних мережах. На сьогодні широко поширені кібершахрайства, під час яких зловмисники під виглядом різноманітних платежів мають намір дізнатися банківські реквізити громадян, щоб заволодіти грошима. Визначення поняття «Злочинність у сфері інформаційних технологій»- це сукупність правопорушень, які вчиняються за допомогою комп’ютерних систем, мереж та програмного забезпечення з метою незаконного доступу до інформації, крадіжки даних, шахрайства, поширення шкідливих програм тощо.

Вивченням історичного походження та причин злочинності у сфері інформаційних технологій, розвитку цього виду системи запобігання злочинності дослідники почали займатися порівняно недавно. До таких вчених можна віднести О.С. Алавердова, Ю.М. Батуріна, П.Д. Біленчука, А.В. Войцехівського, М.Д. Діхтяренка, К.Ю. Ісмайлова, С.М. Круля та ін.

Варто зазначити, що кіберзлочинність, порівняно з традиційними видами злочинності в Україні (вбивства, корисливі кримінальні

правопорушення тощо), є відносно новим явищем і найбільшою загрозою XXI століття водночас, адже інформаційні технології також є способом вчинення багатьох традиційних кримінальних правопорушень[2, с.442]. Такий злодій стає бойовою силою, а основним його засобом є кібератаки та хакерство. Зокрема, в умовах війни інформаційний простір використовуватимуть не лише супротивники для підриву обороноздатності України, а й можуть зазнати атак ті, хто прагне нажитися на ситуації перевантаженості правоохоронних органів. Із кожним днем кількість кіберзлочинів зростає, і їх кількість значно зростає. Збільшуються нові види злочинів, кожен з яких вимагає вибору відповідного методу боротьби, але це створює певні проблеми. Основна причина полягає в тому, що кіберзлочинців набагато важче зловити, ніж звичайних злочинців.

Після повномасштабного вторгнення рф на територію України різко зросла кількість злочинів у сфері інформаційних технологій. Держава-агресор використовує інтернет-технології для поширення дезінформації, ворожої ідеологічної пропаганди про вторгнення в Україну. Тому відбулося удосконалення притягнення до кримінальної відповідальності таких злочинців і зміни в законодавстві відбулися саме в Законі України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 №2149-IX внесено зміни до Розділу XVI [3]. Передбачається кримінальна відповідальність в ч.1 ст.361 за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; в ч.2 ст.361 вчинені повторно або за попередньою змовою групою осіб. Раніше дії передбачені в ч.1 ст.361 вважалися основним складом кримінального правопорушення, а тепер ч.3 ст.361 стали його особливо кваліфікованим складом. Тож відповідні зміни стосуються посилення кримінальної відповідальності за злочини у сфері інформаційних технологій та розширення обмежень щодо діяльності правоохоронних органів щодо розкриття таких злочинів.

Зрозуміло, що Україна перебуває на ранніх етапах впровадження інституцій та механізмів у сфері кібербезпеки, але вже створено певну законодавчу базу, яку необхідно дотримуватися та вдосконалювати. З розвитком інформаційних технологій кіберзлочинність також покращилася, і вона проявляється в різних сферах особистого життя та діяльності, а також суспільства в цілому.

Аби запобігти таким злочинам потрібно встановити сучасні засоби кіберзахисту, які допоможуть виявити та запобігти кібератакам, це може включати використання антивірусного програмного забезпечення, систем виявлення вторгнень та інших заходів.Також навчання та підвищення кваліфікації: організовувати навчальні курси та семінари для спеціалістів у галузі кібербезпеки.Це допоможе покращити їхні навички та знання, а також

підготувати нових фахівців. Важливим залишається співпраця з правоохоронними органами, важливо підтримувати співпрацю з поліцією та іншими правоохоронними органами, це допоможе виявити та розслідувати злочини у сфері інформаційних технологій. Встановити ефективну систему відповідальності. Законодавство повинно передбачати відповідальність за злочини у сфері інформаційних технологій. Це може включати штрафи, покарання та інші більш серйозніші санкції.

Отже, запобігання злочинності в сфері інформаційних технологій є важливим завданням, особливо в умовах воєнного стану. Україна потребує подальшого розвитку своїх інформаційних технологій, оскільки такі злочинці принаймні на крок випереджають механізми, які мають відповідні державні інституції для боротьби з цим видом злочинності. Тому лише завдяки належному рівню, можливе нормальне функціонування мереж і систем, які з кожним днем все більше і більше інтегруються в наше соціальне життя.

1. Про введення воєнного стану в Україні: Указ Президента України № 64 від 24.02.2022 р. URL : https://www.president.gov.ua/documents/642022-41397.

2. Бодунова О.М Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. Електронне наукове видання «Аналітично-порівняльне правознавство». 2023 р. С.441-445

3. Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» 2149- IX від 24.03.2022 р. URL : https://zakon.rada.gov.ua/laws/show/2149-20#Text

ПЕКАРСЬКИЙ Сергій
к. ю. н., доцент, доцент кафедри
оперативно-розшукової діяльності та
інформаційної безпеки факультету № 3
Донецького державного
університету внутрішніх справ

БАЗА ДАНИХ «РОЗШУК» У ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

В умовах повномасштабної агресії росії проти України актуалізувалося питання розшукової роботи підрозділів кримінальної поліції Національної поліції України. Починаючи з кінця лютого 2022 року підрозділи кримінальної поліції у складі сил безпеки та оборони залучаються до проведення безпекових та стабілізаційних заходів. На нашу думку доцільним

є акцентуація розшукової роботи підрозділів кримінальної поліції в системі стабілізаційних заходів, які проводять на деокупованих територіях уповноважені органи та підрозділи.

Наразі реєструються численні порушення норм міжнародного гуманітарного права, зокрема випадки незаконної депортації громадян України, в тому числі і дітей різних вікових категорій на територію країни-агресора. Окрім того після деокупації населених пунктів пошуковими групами з пошуку осіб, зниклих безвісти за особливих обставин виявляються місця масових поховань військовослужбовців та цивільних громадян України з ознаками тортур та насильства. У свою чергу встановлення місцезнаходження полонених захисників та їх повернення на територію України знаходиться в постійному полі зору органів державної влади України. Не залишаються поза увагою і загальні питання розшукової роботи підрозділів кримінальної поліції щодо розшуку злочинців, які ухиляються від органів досудового розслідування, слідчого судді, суду, відбування кримінального покарання, а також розшук осіб, зниклих безвісти за особливих обставин [1].

Законом України «Про правовий статус осіб, зниклих безвісти за особливих обставин» від 12 липня 2018 року № 2505-VIII регламентовано наповнення та ведення Єдиного реєстру осіб, зниклих безвісти за особливих обставин (далі – Реєстр, прим. автора). Під зазначеним Реєстром розуміємо електронну базу даних, яка призначена для зберігання, захисту, обробки, використання і поширення інформації про осіб, зниклих безвісти за особливих обставин, їх невпізнані останки, наявність чи відсутність рішення суду про визнання осіб, зниклих безвісти, безвісно відсутніми або оголошення померлими, а також інших даних, що використовуються для забезпечення обліку осіб, зниклих безвісти, з метою їх розшуку [1].

Держателем Реєстру є Міністерство внутрішніх справ України, яке має право отримувати інформацію (включаючи персональні дані) від інших органів державної влади, у тому числі шляхом інформаційної взаємодії між Реєстром та іншими державними інформаційними ресурсами в електронній формі інформаційно-комунікаційними засобами з використанням засобів технічного та криптографічного захисту інформації відповідно до вимог законодавства з питань захисту інформації [1, ст. 12]. Окрім того необхідно зазначити, що наказом МВС України від 28.06.2023 № 534 затверджена Інструкція з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» [2].

Основними термінами, які зазначені в даній Інструкції є:

- база даних «Розшук» (далі – БД «Розшук», прим. автора) – автоматизований банк відомостей, у якому обробляється інформація щодо розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування покарання, зниклих

безвісти, зокрема за особливих обставин, підлягають психіатричній допомозі у примусовому порядку, є боржниками за виконавчими документами, відповідачами у справах про стягнення аліментів або про відшкодування шкоди, завданої каліцтвом, іншим ушкодженням здоров'я або смертю фізичної особи, є дітьми, стосовно яких за виконавчим документом про відібрання дитини за поданням виконавця судом винесено ухвалу про їх розшук, осіб, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком, установлення осіб невпізнаних трупів;

- користувач БД «Розшук» – поліцейський та/або представник іншого органу державної влади, зокрема суб'єкта наповнення БД «Розшук», яким у встановленому порядку надано доступ до БД «Розшук»;
- суб'єкти наповнення БД «Розшук» – працівники оперативних підрозділів, які здійснюють оперативно-розшукову діяльність [2], зокрема це працівники підрозділів кримінальної поліції Національної поліції України.

Відповідно, до положень зазначеної Інструкції завданням та призначенням БД «Розшук» є:

1) забезпечення наповнення та підтримання в актуальному стані реєстрів та баз (банків) даних, що входять до єдиної інформаційної системи МВС (ЄІС МВС), стосовно осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування покарання, зниклих безвісти, зокрема за особливих обставин, підлягають психіатричній допомозі у примусовому порядку, є боржниками за виконавчими документами, відповідачами у справах про стягнення аліментів або про відшкодування шкоди, завданої каліцтвом, іншим ушкодженням здоров'я або смертю фізичної особи, є дітьми, стосовно яких за виконавчим документом про відібрання дитини за поданням виконавця судом винесено ухвалу про їх розшук, осіб, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком, установлення осіб невпізнаних трупів;

2) інформаційно-аналітичне забезпечення оперативно-розшукової діяльності суб'єктів наповнення БД «Розшук»;

3) автоматизована перевірка підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду, осіб, зниклих безвісти, зокрема за особливих обставин, людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком, а також виявлених невпізнаних трупів за реєстрами та базами (банками) даних, що входять до ЄІС МВС, для встановлення їх місцезнаходження або визначення осіб [2].

Необхідно вказати, що БД «Розшук» формується та ведеться засобами системи «Інформаційний портал Національної поліції» [3] із застосуванням її комплексної системи захисту інформації з підтвердженою відповідністю.

БД «Розшук» формується за наступними групами:

- оголошені в розшук особи;

- невстановлені особи;
- невпізнані трупи.

До групи оголошених в розшук відносяться особи, які:

- переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування покарання;
- зникли безвісти, зокрема за особливих обставин;
- підлягають психіатричній допомозі у примусовому порядку;
- є боржниками за виконавчими документами, відповідачами у справах про стягнення аліментів або про відшкодування шкоди, завданої каліцтвом, іншим ушкодженням здоров'я або смертю фізичної особи;
- є дітьми, стосовно яких за виконавчим документом про відібрання дитини за поданням виконавця судом винесено ухвалу про їх розшук [2].

До групи невстановлених осіб відносяться особи, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком [2]. У свою чергу до групи невпізнаних трупів відносяться тіла (останки) осіб, персональні дані яких на момент виявлення невідомі та встановлення яких потребує проведення пошукових заходів [2].

Отже, на підставі викладеного висновуємо про те, що в загальному розумінні у базі даних «Розшук» може міститися та оброблятися інформація, яка сприятиме підрозділам кримінальної поліції у встановленні місцезнаходження особи, яка розшукується, або її визначенню, а також установленню особи невпізнаних трупів. Це надасть можливість в конкретних випадках підрозділам кримінальної поліції виявляти та затримувати осіб, які розшукуються за державну зраду, колабораційну діяльність, вчинення військових злочинів тощо. Одночасно накопичена інформація в БД «Розшук» може сприяти працівникам кримінальної поліції у розшуці особи, зниклої безвісти за особливих обставин, зокрема щодо визначення її місцеперебування, а також місця поховання або місцезнаходження останків померлої особи та ідентифікації невпізнаного трупа чи останків.

1. Про правовий статус осіб, зниклих безвісти за особливих обставин: Закон України від 12 липня 2018 року № 2505-VIII (редакція від 27.04.2022). Відомості Верховної Ради України. URL : https://zakon.rada.gov.ua/laws/show/ 2505-19#Text.

2. Інструкція з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: затв. наказом МВС України від 28.06.2023 № 534. URL : https://ips.ligazakon.net/document/RE33710.

3. Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: затв. наказом МВС України 03.08.2017 № 676. URL : https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

ПИЛИПЧУК Владислав
курсант 4 курсу факультету №4
КОЛІСНИК Тетяна Петрівна
доцент кафедри протидії
кіберзлочинності факультету №4
Харківського національного
університету внутрішніх справ,
кандидат педагогічних наук, доцент

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРАЦІВНИКАМИ ПОЛІЦІЇ

Останнім часом безпілотні літальні апарати займають особливу популярність серед сучасних роботизованих комплексів та новаторських технологій, які можуть бути ефективно використані правоохоронними органами у боротьбі зі злочинністю [1]. Ця популярність пояснюється їхнім широким функціоналом, який дозволяє в реальному часі поєднувати автоматичну систему пілотування з одночасним збором та передачею криміналістично-важливої інформації.

Поліцейські в США стали одними з перших, хто почав використовувати безпілотні літальні апарати у своїй правоохоронній роботі. Зокрема, Федеральне управління цивільної авіації (FAA) авторизувало вже 74 урядові агентства з використання БпЛА у повітряному просторі країни, 17 з яких – правоохоронні. Найбільш відомі серед них такі: Montgomery County в Техасі, Mesa County Sheriff›s Department в Колорадо і Grand Forks в Північній Дакоті. Дозвіл FAA надав можливість правоохоронним органам США використовувати дрони для детального обстеження місць скоєння злочину і пошуку потерпілих [2].

Безпілотні літальні апарати мають великий різновид класифікацій. Вони відрізняються за характеристиками та цільовим призначенням. Наприклад, є мікродрони, які зазвичай використовуються в цивільному житті; безпілотники середньої дальності, які здійснюють розвідку на тактичних рівнях, саме до них відносяться БпЛА української розробки «Лелека-100» та «Фурія»; оперативно-тактичні безпілотники, які можуть безперервно літати до 10 годин, мають збільшений радіус дії, використовуються для спостереження за противником і планування військових дій; стратегічні або ударні БпЛА, один із найпоширеніших – турецької розробки Bayraktar TB-2.

Національна поліція України вдосконалює свої методи боротьби зі злочинністю, включаючи створення підрозділу аеророзвідки. Цей підрозділ призначений для виявлення злочинів та можливої затримки зловмисників за допомогою використання безпілотних літальних апаратів. Дрони

використовуються не лише для виявлення незаконних посівів маку та конопель, але й для виявлення браконьєрів, незаконного видобутку бурштину та вугілля, незаконних вирубок лісу та моніторингу дорожньої ситуації на трасах, тощо [2]. З війною в Україні функціонування БпЛА кардинально розширилися, та їх почали використовувати як військові так і поліцейські для розвідки з повітря ворожих позицій, фіксації воєнних злочинів, нанесення ударів по ворожим силам та знищення техніки, оцінка обсягів руйнувань та стану пошкоджених будівель та споруд. Державна прикордонна служба також використовує безпілотники для моніторингу кордонів України. Необхідність використання безпілотників в Україні сьогодні обумовлена тим, що вони дозволяють проводити роботи в місцях небезпечних для життя людей – на замінованих територіях, при загрозі обстрілів, обвалів, підриву боєприпасів, що не вибухнули, в зонах ймовірного хімічного та радіоактивного забруднення тощо.

Таким чином, підводячи підсумки, наразі важливою задачею різних країн залишається вирішення юридичних аспектів, пов’язаних із застосуванням дронів. Наразі є очевидним, що можливості поліції та військових із використанням безпілотних літальних апаратів будуть лише зростати.

1. Особливості застосування безпілотних літальних апаратів органами та підрозділами поліції: метод. рек. / А. А. Саковський, С. М. Науменко, С. І. Кравченко, І. М. Єфіменко та ін. Київ: Нац. акад. внутр. справ. 2022. 72 с. URL : https://www.naiau.kiev.ua/files/naukova-diyalnist/naukovi-laborator/lab_nni2/2023/metod_bpla.pdf (дата звертання 10.10.2023).

2. Використання безпілотних літальних апаратів у діяльності правоохоронних органів: метод. рек. / А. В. Мовчан, М. А. Мовчан Львів: Львівський держ. універ. внутр. справ. 2020. 104-110 с. URL : https://dspace.lvduvs.edu.ua/bitstream/1234567890/3244/1/16.pdf (дата звертання 10.10.2023). Назва з екрана.

3. Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : Наказ МВС України від 18.12.2018 р. № 1026, зареєстрований в Міністерстві юстиції України 11 січня 2019 р. за № 28/32999 // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/z0028-19#Text (дата звернення 10.10.2023).

ПІЩЬ Артем
курсант 2 курсу факультету №4
КОЛІСНИК Тетяна
кандидат педагогічних наук, доцент,
доцент кафедри протидії
кіберзлочинності факультету №4
Харківського національного
університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕНІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Використання інформаційних технологій у забезпеченні економічної безпеки України є важливим аспектом сучасного розвитку країни. Інформаційні технології допомагають підвищити ефективність економічних процесів, забезпечити захист від кібератак та зловживань, а також забезпечити конкурентоспроможність на міжнародному ринку.

Основні напрямки використання інформаційних технологій у забезпеченні економічної безпеки України включають:

Кібербезпека: Захист інформаційних систем та мереж від кібератак є одним з найважливіших аспектів економічної безпеки. Використання сучасних технологій кібербезпеки, таких як вогнепровідні стіни, антивірусне програмне забезпечення, системи виявлення вторгнень та шифрування даних, допомагає запобігти кібератакам та зберегти конфіденційність інформації [1].

Електронна комерція: Використання інформаційних технологій у сфері електронної комерції сприяє розвитку бізнесу та забезпечує безпеку електронних транзакцій. Застосування шифрування даних, електронного підпису та інших технологій дозволяє забезпечити конфіденційність та цілісність електронних операцій.

Біг-дата та аналітика: Використання інформаційних технологій дозволяє збирати, аналізувати та використовувати великі обсяги даних для прийняття обґрунтованих рішень. Аналітика даних допомагає виявляти тенденції, прогнозувати ризики та виявляти можливості для розвитку економіки [1].

Електронне урядування: Використання інформаційних технологій у сфері урядування сприяє покращенню ефективності державних послуг та забезпечує прозорість та відкритість управління. Електронні системи урядування дозволяють забезпечити швидкий доступ до інформації, автоматизувати процеси та зменшити корупцію [1].

Інтернет в розвитку бізнесу: Використання інформаційних технологій у забезпеченні економічної безпеки України є важливим аспектом сучасного розвитку країни. Інформаційні технології допомагають підвищити

ефективність економічних процесів, забезпечити захист від кіберзагроз та забезпечити конкурентоспроможність українських підприємств на міжнародному ринку.

Суб'єкти ринкової економіки здійснюють свою діяльність в умовах, коли інформація, інформаційні взаємовідносини, тай взагалі, всі основні складові процесу інформатизації набувають все більшої значущості. Тому комплексна інформаційна безпека виступає запорукою забезпечення економічної безпеки. Вони органічно доповнюють одна одну і нерозривно пов'язані не тільки з практичної точки зору, але і в понятійному відношенні [2].

Основні аспекти використання інформаційних технологій у забезпеченні економічної безпеки України включають:

Кібербезпека: Захист інформаційних систем від кібератак є одним з найважливіших аспектів економічної безпеки. Використання сучасних інформаційних технологій дозволяє виявляти, запобігати та реагувати на кіберзагрози.

Електронна комерція: Розвиток електронної комерції дозволяє українським компаніям розширити свої ринки збуту та залучити нових клієнтів. Використання інформаційних технологій у цій сфері допомагає забезпечити безпеку електронних транзакцій та захист персональних даних.

Біг-дата та аналітика: Збір та аналіз великих обсягів даних дозволяє уряду та бізнесу приймати обґрунтовані рішення щодо розвитку економіки. Використання інформаційних технологій у цій сфері допомагає виявляти тенденції, прогнозувати ризики та покращувати ефективність управління.

Електронне урядування: Використання інформаційних технологій у державному управлінні допомагає забезпечити прозорість, ефективність та доступність послуг для громадян та бізнесу. Це також сприяє боротьбі з корупцією та підвищенню довіри до державних інституцій.

Інновації та стартапи: Використання інформаційних технологій сприяє розвитку інноваційного підприємництва та створенню нових робочих місць. Це допомагає зміцнити економічну безпеку.

---

1. Застосування інформаційно-комунікаційних технологій у забезпеченні економічної безпеки держави | Літопис Волині. Літопис Волині. URL : http://litopys.volyn.ua/index.php/litopys/article/view/179 (дата звернення: 18.10.2023).

2. Інформаційно-економічна безпека як фактор стабільного розвитку держави | Публічне урядування. Наукова періодика Міжрегіональної Академії управління персоналом. URL : http://journals.maup.com.ua/index.php/public-management/article/view/152 (дата звернення: 18.10.2023).

ПРОКОПОВИЧ-ТКАЧЕНКО Дмитро
В.о. завідувача кафедри кібербезпеки Університету митної справи та фінансів, кандидат технічних наук
КОСТЕНКО Олексій, завідувач наукової лабораторії теорії цифрової трансформації та права науково-дослідного центру цифрових трансформацій і права науково дослідного інституту інформатики і права Національної академії правових наук України, доцент кафедри права Державного університету «Київський авіаційний інститут»,
доктор філософії з права, доцент
ХРУШКОВ Борис
Студент 2 курсу гр. К22-1М
Університету минтної справи
та фінансів

КОМУНІКАЦІЯ ОБ'ЄКТІВ ІЗ ВМОНТОВАНИМИ ДАТЧИКАМИ ТА ПРИСТРОЯМИ, ЩО Є СКЛАДОВОЮ ІНТЕРНЕТ РЕЧЕЙ ТА ВПЛИВОМ ШТУЧНОГО ІНТЕЛЕКТУ

Об'єктом дослідження є інформаційно -технічні системи промислового інтернету речей, що забезпечують безпечну експлуатацію техногенно-небезпечних елементів промислового інтернету речей.

Предмет дослідження це процес комплексного програмно апаратного тестування критично важливих , техногенно-небезпечних елементів інтернету речей.

Метою роботи є підвищення забезпечення безпеки найбільш небезпечних елементів промислового інтернету речей шляхом додаткового програмно апаратного тестування таких елементів та отримання інтегрального композитного ефекту .

Проведено аналіз проблем безпеки промислового інтернету речей , розглянуті основні теноглогічні інциденти , що відбулись у світі за останні 5 років. Деякі інциденти , що стосуються програмних помилок , помилок давачів та фізичних проблем активаторів на та техногенно небезпечних елементах , і пропонована оригінальна вдосконалена система програмно-апаратного тестування техногенно небезпечних елементів з використанням штучного інтелекту та хмарних сервісів , що сформувало блок пропозицій до вдосконалення відповідних міжнародних стандартів ISO/IEC.

З метою практичної реалізації в роботі пропоновано макетування програмно апаратного комплексу на базі платформи Raspberry PI та ARDUINO.

З метою наукової апробації опубліковані тези на відповідних науково-практичних конференціях за напрямом промисловий інтернет речей,

Світова наукова спільнота жваво спостерігає перехід від сьогоднішнього Інтернету речей (IoT) до включення більшої кількості промислового обладнання та систем метрології, утворюючи промисловий Інтернет речей (HoT). Однак це призводить до багатьох проблем, пов'язаних із конфіденційністю, цілісністю, доступністю, конфіденційністю та невідмовністю. Отже, існує потреба у забезпеченні сучасних телекомунікаційних технологій , щоб забезпечити безпечний промисловий інтернет речей з розумними інформаційно телекомунікаційними мережами , розумною метрологією , промисловими підприємствами та безпечними містами , що використовують безпечні елементи промислового інтернету речей. З кожним днем екосистеми промислового інтернету речей все більш охоплюють сфери життя суспільства та людини в тому рахунку і в захисті прав та свобод людини, своєчасному документуванню соціально небезпечних подій пов'язаних як і з діяльністю людини так і техногенно небезпечними подіями та природними явищами.

Тому важливо досліджувати технології HoT і створювати сучасні стандарти особливо коли йдеться про захист зв'язку, стійкі бездротові мережі, захист промислових даних і безпечне зберігання промислової інтелектуальної власності в хмарних системах. Таким чином, наше дослідження визначає виклики, потреби та вимоги промислових застосувань програмно апаратних елементів найбільш техногенно небезпечних програмно апаратних елементів інтернету речей.[1]

Сьогодні ми можемо спостерігати великі глобальні тенденції цифровізації всіх аспектів нашого повсякденного життя. Зокрема, ми бачимо програми, які можуть використовувати інформацію від датчиків, прикріплених до речей, щоб забезпечити більш персоналізовану, автоматизовану та інтелектуальну поведінку [2]. Цю концепцію зазвичай називають Інтернетом речей (IoT) . IoT – це загальний термін для розробки машин, транспортних засобів, товарів, приладів, одягу тощо, оснащених маленькими вбудованими датчиками та приводами, які також можуть спілкуватися між собою через Інтернет. Це означає, що ці пристрої можуть сприймати своє оточення, спілкуватися з іншими, мати ситуативну поведінку та створювати нові форми розумних, інтелектуальних та автономних послуг. Цей розвиток важливий не лише для цифрового та пов'язаного суспільства, але й для промисловості та економіки в цілому. Поточні оцінки стверджують, що вже до 2023 року в Інтернеті буде понад 100 мільярдів підключених пристроїв, і багато з цих пристроїв будуть давачами, актуаторами [3].

Усі ці пристрої IoT разом створюватимуть нові типи послуг, повсюдно

обмінюючись інформацією датчиків один з одним у глобальному масштабі та керуючи різними типами приводів. Таким чином, для отримання інформації з датчиків значною мірою покладаються на метрологічні системи.

З цього ми також бачимо тенденції в хмарних обчисленнях IoT для великомасштабного зберігання даних, аналітики великих даних на величезній кількості даних, зібраних з джерел IoT, і включення кіберфізичних систем у системи «машина-машина», які керуються штучним інтелектом.[4]

У зв'язку з цим багато роботи виконується в рамках ініціативи Industrie 4.0 [5], включаючи розумні міста, розумну промисловість, фабрики майбутнього та розумне виробництво. Зокрема, оскільки Індустрія 4.0 розвивається швидше, ніж будь-коли можна було собі уявити, промислова автоматизація не лише стає розумнішою завдяки використанню методів штучного інтелекту, але й звільняється від дротових компонентів завдяки використанню бездротових технологій.[6] Це стає можливим завдяки використанню HIoT стандартизованим способом і пошуку технологічного прориву від дослідників промислової автоматизації. [7]Отже, формується потреба в дослідженнях промислового IoT (HoT) [8]. Однак промислові вимоги суттєво відрізняються від послуг, які не є гарячими, особливо коли йдеться про критичність часу та надійність [9]. Наприклад, промисловий процес може швидко реагувати на невеликі зміни значень датчика, щоб підтримувати високу якість продукту або уникнути катастрофічного збою. Через це промислові системи зв'язку часто розглядають доступність як п'ять дев'яток [10], [11], що означає час безвідмовної роботи щонайменше 99,999%. Промислові додатки та HOT мають набагато вищі вимоги до безпеки, щоб уникнути простою та захистити конфіденційну інформацію, пов'язану з промисловим процесом. Включно із захистом мереж від атак на відмову в обслуговуванні, захистом даних і конфіденційністю конфіденційних промислових даних, а також своєчасними оновленнями, щоб уникнути використання слабких місць різними онлайн-атаками. Саме ця область буде в центрі уваги цієї статті, де опитування та пов'язані з ними роботи , а посилання в ньому добре вводять і підсумовують поточний стан техніки. Загальна мета цього дослідження полягає в тому, щоб зрозуміти, як захистити HoT, зосередивши особливу увагу на ланцюжку створення вартості інтернету речей . Що варіюється від генерації значень датчиків і передачі через Інтернет до хмарних серверів і додатків для кінцевих користувачів. Надзвичайно важливо вирішити та звернути увагу на аспекти безпеки Інтернету речей і гарячих речей, якщо це бачення виходить за рамки простих програм, які ми бачимо сьогодні. [12]

Щоб досягти цього, дослідження необхідно ґрунтувати на існуючих роботах щодо міжнародних стандартів з безпеки, інфраструктур промислової безпеки, принципів безпеки за проектом для екосистем, безпечного віддаленого виконання коду, гомоморфного шифрування та розширень програмного захисту. Отже, мета полягає в дослідженні недоліків

та обмежень хмарних підходів, що наразі використовуються. Додаткова мета цього дослідження полягає в тому, щоб представити більш життєздатний і перспективний підхід. Нарешті, цей проект допоможе створити критичну масу в дослідженнях IoT та HoT для підвищення обізнаності, повноти та масштабності[13]

Незважаючи на те, що безпека в промислових системах та IoT досліджується вже деякий час, це приносить новинку в цю сферу завдяки цілісному погляду на ланцюжок створення цінності HoT. Захищає як пристрої, так і промислові дані в реальних системах HoT. Таким чином, дослідницька робота, прагне відповісти на наступні два дослідницькі питання:

1. Які вимоги можна визначити та висвітлити, щоб показати виклики безпеки та довіри з цілісної точки зору на всіх етапах галузевого ланцюжка створення вартості, що включає гарячі речі та систему вимірювання.

2. Які майбутні напрямки досліджень безпеки є найважливішими для поширення Industry 4.0 і HoT, і які основні перешкоди, на яких слід зосередити майбутню роботу таких систем.

Виходячи з цих двох дослідницьких питань, наш внесок полягає в тому, щоб висвітлити проблеми, виклики під час забезпечення безпеки найбільш техногенно небезпечних елементів інтернету речей . Отже тези нададуть огляд сучасних проблем і короткі пояснення можливих рішень, оскільки вирішення цих проблем є дуже актуальною в різноманітних сферах життя людини, що забезпечують сучасні цифрові екосистеми.

Решта нашого дослідження організована таким чином: у першому розділі дослідження описані та представлені виклики, з якими стикається HoT, розподілені на низку областей. У другої частині представлено приклад використання, який показує, як ці проблеми можуть з’явитись та будуть вирішені в сучасних системах інтернету речей зокрема в промисловому інтернеті речей. В третьої частині нашого дослідження зроблені висновки та пропозиції щодо вдосконалення світових стандартів міжнародних інституцій ISO/IEC, NIST.

Отже, використання пропонованих алгоритмів тестування значно підвищує технологічну надійність промислового інтернету речей, що використовується у спеціальних системах та системах подвійного призначення. Підвищує час роботи таких елементів без заміни комплектуючих.

---

1. CISCO IoT Market Estimates, avaialble online at: http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html (retrieved 30/04/2016).

2. Gartner IoT Hype Cycle, available online at: http://www.gartner.com/newsroom/id/3165317 (retrieved 30/04/2016).

3. Constrained Application Profile (CoAP), RFC-7252, available online at: https://tools.ietf.org/html/rfc7252 (retrieved 30/04/16).

4. REpresentational State Transfer (REST), available online at: http://rest.elkstein.org/

(retrieved 30/04/16).

5. Message Queueing Telemetry Transport (MQTT), avaialble online at: http://mqtt.org/ (retrieved 30/04/16).

6. D. Hughes, K. Thoelen, W. Horré, N. Matthys, J. Del Cid, S. Michiels, C. Huygens, and W. Joosen. 2009. LooCI: a loosely-coupled component infrastructure for networked embedded systems. In Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09). ACM, New York, NY, USA, 195-203.

7. IPSO Data Model, available online at: https://www.iab.org/wpcontent/IAB-uploads/2016/03/ipso-paper.pdf (retrieved 30/04/16).

8. SenML Smart Object Data Model, available online at: https://datatracker.ietf.org/doc/draft-jennings-senml/ (retrieved 30/04/16).

9. The Web Sockets protocol (RFC-6455), available online at: https://tools.ietf.org/html/rfc6455 (retrieved 30/04/16).

10. F. Yang, N. Matthys, R. Bachiller, S. Michiels, W. Joosen, and D. Hughes. 2015. PnP: plug and play peripherals for the internet of things. In Proceedings of the Tenth European Conference on Computer Systems (EuroSys '15). ACM, New York, NY, USA, 14 pages.

11. Erbium CoAP Server, available online at: http://people.inf.ethz.ch/mkovatsc/erbium.php (retrieved 30/04/16)

12. Californium CoAP Server, available online at: http://www.eclipse.org/californium/ (retrieved 30/04/16)

13. VoCore IoT Gateway, available online at: http://www.eclipse.org/californium/ (retrieved 29/08/16)

РИЖКОВ Едуард
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
к.ю.н., професор

ВДОСКОНАЛЕННЯ АНАЛІТИЧНОЇ СКЛАДОВОЇ СИТУАЦІЙНИХ ЦЕНТРІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ

Вдосконалення аналітичної складової ситуаційних центрів Національної поліції України за допомогою засобів штучного інтелекту у найближчий час повинно стати невід'ємною частиною стратегії їх вдосконалення. Штучний інтелект може великою мірою полегшити та удосконалити аналітичний процес, забезпечуючи збільшення ефективності та точності роботи працівників ситуаційних центрів. Поява самих ситуаційних центрів у 2017-2019 роках стала значною подією у правоохоронному відомстві, як результат певного прогресу управлінської та науково-технічної думки [1].

Проте, потрібно також враховувати й проблеми, що залишаються

актуальними: недостатня кількість кадрів (програмістів, аналітиків), засобів обчислювальної техніки, ліцензованих програм, засобів відеоспостереження і т.ін. Серед перспектив розвитку ситуаційних центрів – це використання систем відеоаналітики, але це потребує значних фінансових витрат [2, с. 144].

Не зважаючи на те, що кількість відеокамер у комунальній власності по країні в останні 5 років неухильно зростає, відсоток тих, що обладнані штучним інтелектом залишається мізерним, а сама відеоаналітика залишається одним із найслабкіших сегментів функціонування вказаних підрозділів.

У процесі виконання своїх функцій ситуаційний аналітик досі вимушений у ручному режимі передивлятись по черзі відеоконтент з кількох відеокамер, що відображають картину відеоспостереження з різних ракурсів для того, щоб встановити конкретні обставини чи об'єкт нашого інтересу. Така робота інколи займає неприпустимо значний обсяг часу, стримуючи оперативність реагування, потребує зайвих фізичних зусиль та суттєво залежить від суб'єктивних факторів працівника (неувага, втома та інш.).

Автоматизована відеоаналітика в Ситуаційних центрах НПУ повинна стати ключовим елементом для забезпечення оперативності та ефективного вирішення ситуацій в реальному часі. Ця технологія поєднує в собі різноманітні технічні рішення та програмні засоби, які спрямовані на автоматизацію аналізу великої кількості відеоданих для виявлення подій, взаємодії з ними та швидкого реагування на виникаючі ситуації.

Однією з ключових складових автоматизованої відеоаналітики є використання розпізнавання облич, руху та об'єктів. За допомогою продуктивних алгоритмів та штучного інтелекту системи автоматично впізнають особи, рухомі об'єкти та потенційно небезпечні ситуації. Це дозволяє операторам отримувати інформацію в реальному часі та приймати рішення швидше та ефективніше.

Окрім того, системи відеоаналітики в ситуаційних центрах мають використовувати технології глибинного навчання для автоматичного класифікування подій та об'єктів. Аналізуючи широкий спектр даних, вони повинні розпізнавати нестандартні або підозрілі сценарії, що сприяє зниженню часу реакції та удосконаленню процесу прийняття рішень.

Забезпечення високої ефективності автоматизованої відеоаналітики вимагає інтеграції цих систем з іншими технологіями та інформаційними базами даних правоохоронних органів. Це дозволяє створювати цілісні інформаційні системи, що об'єднують різноманітні дані для максимально точного аналізу та прогнозування ситуацій.

Зокрема, важливою є інтеграція з системами відеоспостереження на об'єктах громадського значення, такими як аеропорти, вокзали, міські камери спостереження тощо. Це дозволяє операторам центру моніторингу отримувати комплексну інформацію та оперативно реагувати на будь-які події, які можуть виникнути в цих місцях.

Камери зі штучним інтелектом (як елемент сегменту відеоаналітики – Р.Е.) приносять більше користі, ніж їхні традиційні аналоги. Але вони також вимагають більше ресурсів з точки зору даних і апаратного забезпечення.

Нові камери відеоспостереження зараз розробляються для обробки декількох відеопотоків і більш високої роздільної здатності (4K і вище), щоб надати алгоритмам штучного інтелекту великий набір даних детальних зображень і відео, необхідних для їх аналізу. На додаток до цього, все більше метаданих фіксується і зберігається на пристрої, щоб оператори могли швидко шукати і знаходити відповідні відеоматеріали. Значна частина обробки тепер відбувається на рівні пристрою, а більша обчислювальна потужність нових чипсетів дозволяє проводити глибоку нейромережеву обробку на самій камері для забезпечення периферійного інтелекту [3].

Одним із важливих аспектів автоматизованої відеоаналітики потенційно є також можливість інтеграції з системами штучного інтелекту та аналізу великих обсягів даних. Використання цих технологій дозволить робити прогнози, виявляти тенденції та попереджати можливі загрози, що важливо для стратегічного планування та управління правоохоронною діяльністю.

Таким чином, автоматизована відеоаналітика в ситуаційних центрах Національної поліції України повинна відігравати критичну роль у підвищенні ефективності та швидкості реагування на потенційні загрози та події в реальному часі. Інтеграція різноманітних технічних рішень та засобів програмного забезпечення із використанням штучного інтелекту повинно сприяти створенню цілісних інформаційних систем, які поліпшать ефективність роботи поліції в цілому.

---

1. Косянчук І. Ситуаційний центр Нацполіції працює цілодобово: Урядовий кур’єр. 7 лютого 2018. URL : https://ukurier.gov.ua/uk/articles/situacijnij-centr-nacpoliciyi-pracyuye-cilodobovo/

2. Кудінов В.А. Проблеми впровадження ситуаційних центрів в органах Національної поліції України // Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. Міжнар. наук.- практ. конф. (м. Харків, 30 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Консультат. місія Європейського Союзу. Харків, 2018. С. 143-145

3. Потенційні можливості відеокамер зі штучним інтелектом. URL: https://tvtdigital.com.ua/potentsiyni-mozhlyvosti-videokamer-zi-shtuchnym-intelektom/

4. Що таке штучний інтелект у відеоспостереженні? URL : https://worldvision.com.ua/chto-takoe-iskusstvennyy-intellekt-v-videonabludenii/

ЛІСОВА Єлизавета
здобувач вищої освіти 4 курсу ННІ
права та підготовки фахівців для
підрозділів Національної поліції
Науковий керівник:
ГІДЕНКО Євгеній
старший викладач кафедр
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

СУЧАСНА ПРОБЛЕМАТИКА ТА РОЗВИТОК ІНфОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сьогодні неможливо уявити роботу будь-якого підрозділу поліції без інформаційного забезпечення. Інформаційне забезпечення діяльності поліції є основою для планування, прогнозування та здійснення оперативно-розшукової, профілактичної діяльності, прийняття оптимальних управлінських рішень, контролю за їх виконанням. Автоматизовані інформаційні системи є найважливішим елементом організації діяльності установ і підрозділів НПУ. Важливою передумовою створення єдиного інформаційного простору правоохоронних органів є забезпечення високого рівня інформаційного забезпечення правоохоронних органів та розробка нових методів і засобів боротьби зі злочинністю [1, С.397]. Інформаційне забезпечення правоохоронної діяльності в поєднанні з перевагами єдиного інформаційного простору відкриває нові можливості для попередження злочинності та сприяє прийняттю ефективних і точних рішень щодо розкриття правопорушень.

Незаперечним є той факт, що використання інформаційного простору та інформаційних технологій може стати чи не головним чинником зміцнення законності, забезпечення національної обороноздатності, соціально-політичної стабільності та розвитку демократичних засад державного управління. У сучасних умовах рівень розвитку інформаційного забезпечення Національної поліції України безпосередньо впливає на криміногенну ситуацію, впливає на дотримання прав і свобод людини і громадянина, створює сприятливі умови для впровадження економічно інтенсивних методів управління, відкидає використання екстенсивних економічно ефективних методів, це вплинуло на процес інтеграції нашої країни у світовому інформаційну просторі [2, С. 148]. Важливою передумовою для створення єдиного інформаційного простору правоохоронних органів має стати забезпечення високого рівня

інформованості національної поліції та розробка нових методів і засобів боротьби зі злочинністю. До того ж, інформаційне забезпечення Національної поліції є важливою складовою її діяльності. Слід зазначити, що, описуючи стан розвитку інформаційних систем у сучасних умовах, можна дійти висновку, що впроваджувані на сьогодні інформаційні системи не повною мірою виконують своє призначення в процесах діяльності правоохоронних органів і потребують вдосконалення на всіх рівнях. У цьому контексті особливо актуальним є вдосконалення законодавства щодо інформаційного забезпечення правоохоронними органами [3, С.76].

Основними джерелами інформації, які використовуються під час інформаційно-аналітичної діяльності поліції, є:

а) бази даних оперативно-розшукових записів, створені інформаційно-аналітичним відділом кримінальної поліції;

б) Інформаційні масиви оперативних довідок, довідок та статистичного обліку

в) Інформаційна база даних промислових служб МВС України.

Для ефективного інформаційного забезпечення у межах окремих територіальних органів поліції необхідно об'єктивно розробити стандарти збору інформації та розробити процедури обробки інформації. Варто зазначити, що технології збору та обробки даних мають охоплювати всі сфери діяльності складових системи національної поліції, як визначено Законом України «Про Національну поліцію» і компонентами Міністерства внутрішніх справ України (Державна служба України з питань надзвичайних ситуацій, Державна міграційна служба України, Державна прикордонна служба України, Національна гвардія України), індикатори надійності, актуальності та інших зовнішніх і внутрішніх властивостей зібраної та обробленої інформації [4, С.170]. Оптимізація завдань пошуку, відбору та систематизації необхідної для роботи поліції інформації здійснюється на основі розвитку єдиного інформаційного простору системи МВС України, який логічно визначається як сукупність спеціалізованих баз даних і як основа для здійснення дій на основі загальних принципів і загальних правил. Інформаційно-аналітичні заходи забезпечують інформаційну взаємодію МВС України з громадянами. Щоб розкрити поточний стан інформаційного забезпечення Національної поліції України, насамперед необхідно звернути увагу на питання вдосконалення нормативно-правової бази інформаційного забезпечення правоохоронних органів та інформаційного забезпечення в цілому[5, С.147]. До того ж було б доречне створення єдиної бази з даними на кожного громадянина та окремим доступом для Національної поліції, щоб база містила всі дані на громадянина. Така база значно б полегшила та прискорила роботу правоохоронних органів. Існує багато реєстрів, що зберігають певну інформацію про кожну людину, але не всі вони можуть повно та всебічно надати інформацію про особу. Як зробити таку базу, щоб вона відповідала законодавству? Таке питання виникає щоразу, коли мова

заходить про використання особистих даних. Нікому б не хотілося, наприклад, аби інформацію про борги знали всі. Річ у тім, що дані про борги, суди, нерухомість та автомобілі громадян давно відкриті і зберігаються у державних реєстрах. Тобто люди самі віддали цю інформацію державі і погодилися з тим, що вона буде відкритою.

Однак, незважаючи на таку велику кількість інформаційно-аналітичних систем, вони ще не можуть відповідати вимогам сучасного інформаційного обігу, тому необхідні вдосконалення на всіх рівнях від збору інформації до обробки інформації. Зазначимо, що в умовах стрімкого розвитку інформаційних технологій, усі сфери суспільного життя, відповідні технології, які використовують правоохоронні органи, не можуть відставати від технологій, які можуть бути використані для вчинення кримінальних правопорушень в інформаційній сфері [6, С.576]. Безперечно, причинами цієї проблеми є недостатність коштів на розвиток інформатизаційного забезпечення правоохоронних органів і нерівномірний стан програмно-технічного забезпечення територіальних підрозділів. Важливим аспектом у подоланні цієї проблеми в умовах загострення кризи є фінансова підтримка міжнародних партнерів, особливо ЄС, у контексті реформ правоохоронної системи [7,С.379]. Також потребують удосконалення технічна та програмна складові інформаційного забезпечення Національної поліції з метою впровадження новітніх технологічних засобів, підвищення рівня якості програмних продуктів, постійного вдосконалення можливостей інформаційних бібліотек, інформаційно-обчислювальних центрів, комп'ютеризації систем управління, та створювати системи захисту інформації. У межах технічної та процедурної складових особливо важливим є забезпечення того, щоб інформація не витікала через технічні канали, оскільки від цього залежить якість та ефективність правоохоронних органів, а також інформаційний суверенітет і національна безпека [8, С.202]. Захист інформаційних технологій регламентується національними стандартами України та нормативними документами системи захисту інформаційних технологій, які не є уніфікованими нормативними документами, але є обов'язковими для керівництва та керівного персоналу всіх рівнів. Окрім того, нагляд здійснюється відповідно до положень технічного захисту, які не відображені в постановах вищого рівня, а регламентуються внутрішніми наказами, розпорядженнями, інструкціями із захисту інформаційних технологій [9, С.130].

Вважаємо, що особливого значення набуло питання вдосконалення інформаційного забезпечення діяльності правоохоронних органів. Дуже важливими характеристиками зібраної інформації повинні бути повнота, достовірність, доступність, актуальність, точність. Це може стати чи не головним чинником активізації діяльності поліції, адже в умовах розвитку якісне інформаційне забезпечення правоохоронних органів є запорукою їх ефективної діяльності, а отже захисту стану удосконалення прав і свобод

людини і громадянина в нашій державі.

1. Гіденко Є.С. Зарубіжний досвід та українські реалії в боротьбі зі злочинністю. Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід : матеріали ІІ Міжнар. наук.-практ. конф. (м. Дніпро, 15 березня 2018 р.). Дніпро : ДДУВС, 2018. С.397-401.

2. Попович М. І. Організація інформаційного забезпечення оперативно-розшукової діяльності підрозділів МВС України у протидії незаконному обігу наркотичних засобів. Європейські перспективи. 2014. №. 7. С. 145–151.

3. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналіт. доп. Київ : НІСД, 2014. 76 с.

4. Нефедова Н. А. Інформаційне забезпечення спеціальної поліцейської діяльності. Адміністративне право і процес. 2014. № 2(8). 167–173.

5. Петровський О. М. Проблемні питання формування єдиного інформаційного простору правоохоронних органів. Підприємництво, господарство і право. 2017. № 8. С. 145–149.

6. Беляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення : монографія. Київ : КВІЦ, 2008, 576 с.

7. Катеринчук І.П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України. Форум права. 2011. № 2. С. 376–380.

8. Шорохова Г.М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. Шоста міжнародна науково-практична конференція НАНР Економіко-правові виклики 2016 року (12 січня 2016 року). Львів : НАНР Національна академія наукового розвитку, 2016. Том 2. 202 с.

9. Цимбалюк В.І., Олексін Ю.П., Міщук І.В., Петровський О.М., Сахнюк В.В. Проблеми та перспективи удосконалення законодавства щодо інформаційного забезпечення правоохоронних органів. Достижения современных ученых. Серія юриспруденція. 2017. С. 127- 137.

ВАСИЛЕНКО Максим
курсант 1-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри інформаційних
та комунікативних технологій
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Кібербезпека та боротьба з кіберзлочинністю в умовах військового стану XXI століття – це одні з найбільш важливих питань особливо в нашій країні, коли противостояння двух сторін переходить в кібергібридну війну.

Операції з якими потребують глибокого аналізу, розробок та впровадження високотехнологічних рішень з метою запобігання та викриття кіберзагроз в цій галузі. Інформаційна та економічна безпека допомагають забезпечити функціонування держави, захистити інтереси нації та зберегти стабільність у складних умовах військового конфлікту. Я вважаю, що інформаційна безпека в контексті війни стає дуже важливою, оскільки інформація має мегазначення у стратегічному плануванні, розвідці, веденні операцій і впливі на громадську думку [1].

Інформаційна безпека в війні охоплює такі аспекти:

Захист від кіберзагроз: Військові та військово-політичні системи піддаються кібератакам. Забезпечення кібербезпеки є критично важливим, оскільки кіберзагрози можуть завдати серйозної шкоди військовим операціям та інфраструктурі країни.

Розвідка і контррозвідка: Збір інформації про дії супротивника і виявлення спроб проникнення власних військових систем є важливими аспектами інформаційної безпеки.

Вплив на громадську думку: Використання інформаційної війни для маніпулювання громадською думкою власної або супротивника є способом вплинути на психологічний стан суспільства та військових підрозділів.

Захист від дезінформації: Розповсюдження неправдивої інформації та фейків може призвести до невірного рішення влади. Тому важливо мати механізми виявлення та реагування на дезінформацію.

Захист комунікаційних інфраструктур: Забезпечення надійності та стійкості комунікаційних систем у військових операціях дозволяє зберігати зв’язок та обмін інформацією.

Інформаційна готовність: Готовність до обробки та аналізу інформації, яка надходить з різних джерел, є важливою для швидкого реагування на зміни на полі бою.

Забезпечення інформаційної безпеки в війні вимагає інтеграції технологій, політики та психологічних аспектів. Інформація може бути важливою зброєю в сучасних конфліктах, тож її захист і використання становлять складний завдання для військових та політичних лідерів.

та відновлення економіки після закінчення конфлікту. Ось деякі ключові аспекти, які слід враховувати:

Макроекономічна стабільність: Забезпечення стабільності фінансового сектору та управління інфляцією є важливими аспектами в економічній безпеці під час війни.

Управління фінансами: Надзвичайні фінансові заходи можуть бути введені для фінансування військових операцій. Важливо контролювати та маніпулювати фінансами, щоб уникнути гострої інфляції та інших негативних наслідків.

Забезпечення основних потреб населення: Забезпечення доступу до основних життєвих потреб, таких як харчування, медичні послуги та житло, є

критично важливим для збереження соціальної стабільності.

Управління ресурсами: Збереження та ефективне використання ресурсів, таких як енергія, вода та продовольство, має важливе значення.

Податкова політика: Податкова система може бути змінена для забезпечення додаткових доходів для фінансування військових потреб.

Міжнародні відносини: Співпраця з міжнародними партнерами, а також дотримання міжнародних домовленостей, може вплинути на економічну безпеку під час військового стану.

Відновлення після війни: Після завершення конфлікту важливо розробити плани для відновлення економіки та суспільства, включаючи відшкодування шкідливих наслідків війни.

Запобігання війні та розумне управління конфліктом також можуть відігравати важливу роль у збереженні економічної безпеки. Під час військового стану важливо співпрацювати з різними галузями уряду, а також зв'язаними організаціями та експертами для ефективного управління економічними аспектами конфлікту та його наслідками.[2]

Висновок про кібербезпеку в війні можна сформулювати так:

Сучасні військові конфлікти вимагають надзвичайної уваги до кібербезпеки. Кібератаки можуть наносити значні збитки інфраструктурі, військовим системам та комунікаціям, і навіть впливати на геостратегічну ситуацію. Тому забезпечення високого рівня кібербезпеки стало невід'ємною складовою військової стратегії країн та міжнародних організацій. Ефективна кібероборона та здатність до кібернаступів стали важливими елементами військової підготовки та готовності країн у сучасному світі. Таким чином, кібербезпека стала критичною складовою національної та міжнародної безпеки в умовах військових конфліктів[3].

---

1. Теоретичні аспекти інформаційних війн та національна безпека. URL : https://core.ac.uk/download/pdf/268616887.pdf

2. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика (Анотація). Автор Пєтков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. Видавництво ЦУЛ Рік видання 2022

3. «Макроекономічна стабільність: складові, кількісний вимір та фактори забезпечення». Міждисциплінарна курсова робота з Економічної теорії. URL : http://dspace.wunu.edu.ua/bitstream/316497/32467/1/Чипурка%20Х.Б.%20ЕЕП-21.pdf

СНІСАР Владислав
курсант 3-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції,
Науковий керівник:
ПЕРВІЙ Віта
викладач кафедри
оперативно-розшукової діяльності
факультету підготовки фахівців
для підрозділів кримінальної поліції,
доктор філософії

ОСОБЛИВОСТІ КОНФІДЕНЦІЙНОГО СПІВРОБІТНИЦТВА ПРИ ЗДІЙСНЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Упродовж історії правоохоронні, розвідувальні та контррозвідувальні установи країн світу використовували осіб, які були готові надавати конфіденційну інформацію та сприяти в проведенні різних заходів та операцій в умовах таємності. Навіть при стрімкому прогресі науки та технології, значних досягненнях у сфері інформаційних технологій і швидкому розвитку інформатизації суспільства, цей вид діяльності залишається ключовим для запобігання та виявлення злочинів, а часто й для їх розслідування. Різні країни використовують різні терміни для позначення цього виду діяльності. Навіть в українських наукових та практичних колах використовуються різні терміни, щоб визначити саме цей вид співпраці: конфіденційне співробітництво, негласне співробітництво, конфіденційне (негласне) співробітництво, агентурна робота, агентурно-оперативна робота, агентурний метод, робота з негласними працівниками і таке інше.

Важливо відзначити, що аспект цього дослідження ґрунтується на повноваженнях, наданих оперативним підрозділам згідно зі статтею 8 Закону України «Про оперативно-розшукову діяльність». Ці повноваження охоплюють наявність як гласних, так і негласних штатних та позаштатних працівників (пункт 13, частина 1); можливість використовувати конфіденційне співробітництвом згідно з положеннями статті 275 Кримінального процесуального кодексу України (пункт 14, частина 1); отримувати від юридичних чи фізичних осіб безкоштовно або за винагороду інформацію про кримінальні правопорушення, що готуються або вчинені, та про загрозу безпеці суспільства і держави (пункт 15, частина 1) [1, 2].

Особи, які бажають співпрацювати з оперативним підрозділом, можуть оформити цю співпрацю у письмовій угоді з гарантією конфіденційності. Угоду про надання підтримки оперативним підрозділам у проведенні

оперативно-розшукової діяльності може бути укладено з особою, яка має повну цивільну дієздатність. Порядок укладання такої угоди визначається Кабінетом Міністрів України. Таким чином, законодавець використовує два основних терміни - «конфіденційне співробітництво» та «сприяння здійсненню оперативно-розшукової діяльності», не надаючи їх визначень. Водночас, посилання на норми Кримінального процесуального кодексу України, що стосуються права використання конфіденційного співробітництва, створює враження, що саме ці норми містять визначення та розкривають сутність конфіденційного співробітництва. Однак законодавець просто вказує на те, що під час проведення негласних слідчих (розшукових) дій слідчий має право використовувати інформацію, отриману внаслідок конфіденційного співробітництва з іншими особами, або залучати цих осіб до проведення негласних слідчих (розшукових) дій у випадках, передбачених цим Кодексом.

Термін «конфіденційне співробітництво» можна розглядати в такому контексті: це співробітництво між уповноваженими посадовими особами правоохоронних органів та особами, які залучені до виконання завдань правоохоронної діяльності. Це співробітництво здійснюється зі збереженням конфіденційності обміну інформацією, проте не обов'язково передбачає таємницю самого факту такої співпраці.

Проаналізувавши визначення конфіденційного співробітництва, можна прийти до висновку, що існують дві форми надання громадянами допомоги під час проведення негласних слідчих (розшукових) дій:

1) Використання інформації, яку отримано від конфідента під час проведення негласних слідчих (розшукових) дій.

2) Залучення конфідента до участі у негласних слідчих (розшукових) діях [3, с. 103].

Співпраця осіб з правоохоронними органами повинна бути винятково добровільною. Згідно зі статтею 19 Конституції України, правовий порядок в Україні ґрунтується на засадах, відповідно до яких, ніхто не може бути примушений робити те, що не передбачено законодавством. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачений Конституцією та законами України [4]. При цьому мотивація для такої співпраці може бути різноманітною:

- власне бажання надати безкоштовну допомогу правоохоронним органам, ґрунтуючись на своїх ідеологічних і моральних переконаннях;
- потреба поліпшити умови перебування в кримінально-виконавчих установах;
- мотивація, такі як помста, заздрість, конкуренція в кримінальному середовищі, особиста симпатія чи вдячність до конкретного працівника правоохоронних органів;
- бажання приймати ризик, або потреба завдати шкоду конкурентові в

сфері бізнесу і таке інше.

У висновку важливо відзначити, що конфіденційне співробітництво є важливим і необхідним інструментом для правоохоронних органів у запобіганні та розкритті злочинів. Історично цей вид діяльності виявився невід'ємною складовою діяльності правоохоронних, розвідувальних та контррозвідувальних установ у багатьох країнах світу. Незважаючи на швидкий технологічний прогрес і зростання ролі інформаційних технологій, конфіденційне співробітництво залишається невід'ємною складовою сучасного суспільства, яка спрямована на забезпечення безпеки громадян та держави.

Отже, конфіденційне співробітництво залишається важливим елементом діяльності правоохоронних органів і допомагає у забезпеченні безпеки громадян та суспільства в цілому.

1. Про оперативно-розшукову діяльність : закон України від 18.02.1992 року № 2135-XII із змін. URL : https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення 22.10.2023).

2. Кримінально-процесуальний кодекс України від 13.04.2012 року № 3341-IX із змін. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 22.10.2023).

3. Гольдберг Н. Проблеми регулювання конфіденційного співробітництва при здійсненні негласних слідчих (розшукових) дій. Національний юридичний журнал: теорія і практика. 2016 р. С. 100-103.

4. Конституція України від 28.06.1996 року № 254к/96-ВР URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text (дата звернення 22.10.2023).

ГЛЯН Тетяна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
ВАРАВА Володимир
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ЗАХИСТ ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ЗАПОБІГАННЯ ЇЇ РОЗПОВСЮДЖЕННЮ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Україна переживає важкі часи, оскільки з 24 лютого 2022 року в країні оголошено воєнний стан у зв'язку з повномасштабним вторгненням російської федерації. У таких умовах збереження цифрової інформації та

запобігання її розповсюдженню стає критично важливим завданням.

Одним із перших кроків у захисті цифрової інформації є забезпечення безпеки інфраструктури. Це включає в себе кіберзахист критично важливих об'єктів, які можуть бути спрямовані нашими противниками. Важливо розглядати кожен об'єкт, як потенційну мішень для кібератак і забезпечувати їхню максимальну захищеність.

Під час воєнного стану, увага до кібербезпеки стає надзвичайно важливою. Запобігання несанкціонованому доступу до цифрової інформації починається з використання надійних паролів. Громадяни та організації повинні усвідомлювати важливість створення складних паролів, які включають букви, цифри та символи. Також рекомендується регулярно змінювати паролі [1, с.98].

Шифрування є ключовим елементом забезпечення конфіденційності цифрової інформації. Під час воєнного стану, особливо важливо шифрувати конфіденційну інформацію, щоб ускладнити можливим загрозам доступ до неї. Застосування ефективних шифрувальних методів допомагає зберегти цінні дані в надійності.

Один з важливих аспектів кібербезпеки - це обмеження доступу до конфіденційних даних. Це може включати в себе розробку політик доступу, які обмежують права користувачів лише до тих ресурсів, які їм необхідні для виконання їхніх обов'язків.

Громадяни та організації повинні бути освічені щодо потенційних кіберзагроз та сценаріїв атак. Це допомагає вчасно виявляти підозрілу діяльність та реагувати на неї. Спільнота повинна бути обізнаною щодо соціальної інженерії та методів атак, щоб уникнути попадання в пастки зловмисників.

Кіберзагрози постійно зростають в своїй складності і винахідливості. Тому ініціативи з підвищення кібербезпеки повинні бути постійно оновлюваними і вдосконалюваними, відповідаючи новим тенденціям та технологіям [2, с.76].

Також зазначимо, що системи моніторингу та виявлення загроз є важливим компонентом військової кібербезпеки, особливо під час воєнного стану. Їх роль полягає у постійному нагляді за цифровим простором та реагуванні на можливі кібератаки і порушення безпеки. Наведемо кілька ключових характеристик цих систем:

1. Оперативне реагування. Системи моніторингу та виявлення загроз реагують на події в режимі реального часу. Вони виявляють підозрілі або несподівані активності в мережах і системах та надсилають сповіщення про це відповідним службам безпеки. Це дозволяє приймати швидкі заходи для зниження можливих наслідків атаки.

2. Аналіз та ідентифікація загроз. Системи моніторингу аналізують зібрані дані для ідентифікації потенційних загроз. Вони використовують алгоритми та сигнатури для розпізнавання відомих атак, а також аномалії в

активності, які можуть свідчити про нові загрози.

3. Широке охоплення мереж. Системи моніторингу можуть охоплювати різні рівні мереж, включаючи локальні мережі, сервери, хмарні обчислення та великі системи. Вони надають загальний огляд інфраструктури та дозволяють виявляти загрози на різних рівнях.

4. Реалізація реагування. Після виявлення загрози, системи моніторингу можуть надавати рекомендації або навіть автоматично виконувати дії для зменшення ризику атаки. Це може включати в себе блокування зловмисників, відключення вразливих систем або ізоляцію уражених мереж.

5. Збільшення свідомості про загрози. За допомогою систем моніторингу та виявлення загроз можна підвищити свідомість про потенційні кіберзагрози в організаціях та владних структурах. Це допомагає підготувати персонал до вчасної реакції на загрози та розуміти важливість кібербезпеки.

У військових умовах, коли цифрова інформація та інфраструктура піддаються великому тиску, системи моніторингу та виявлення загроз грають критичну роль у забезпеченні безпеки. Вони допомагають вчасно виявляти кібератаки, знижувати їх вплив і забезпечувати стійкість цифрових ресурсів під час воєнного стану.

У воєнний час, регулярні кібератаки на державні та військові системи можуть бути значною загрозою. Щоб захистити цифрову інформацію, слід використовувати відповідні кіберзаходи, включаючи вогнені стіни, антивірусні програми та інші заходи безпеки [3, с.116].

Під час воєнного стану, зловмисники можуть використовувати соціальну інженерію для отримання доступу до цифрової інформації. Освіта та навчання громадян щодо виділення підозрілих повідомлень та спроб маніпуляції можуть значно зменшити ризики.

Отже, умови воєнного стану створюють значні виклики у сфері кібербезпеки. Захист цифрової інформації вимагає комплексного підходу, що охоплює технічні, організаційні та освітні заходи. Необхідно надавати пріоритет цій сфері, оскільки велика частина важливих рішень та інформації зберігаються в цифровому вигляді.

Нація має бути об’єднаною і визначеною у своєму прагненні захистити свою цифрову інформацію в умовах воєнного стану. Захист цифрової інформації є важливим елементом національної безпеки та вимагає постійного удосконалення та адаптації до нових загроз.

1. Інформаційна безпека. Підручник. Під ред. В. В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с

2. Лизанчук В. В. Інформаційна безпека України: теорія і практика: підручник. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

3. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків : Вид. ХНЕУ, 2018. 196 с.

БУЛДАКОВА Анастасія
курсант IV курсу ННІ права
та підготовки фахівців
для підрозділів Національної поліції
ГРЕБЕНЮК Андрій,
завідувач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ВПЛИВ ДЕЗІНФОРМАЦІЇ ТА ФЕЙКОВИХ НОВИН НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ: ПРОТИДІЯ ТА ЗАХИСТ

Інформаційна безпека стає дедалі важливою складовою національної безпеки, і ця тенденція стає особливо актуальною у зв'язку з поширенням дезінформації та фейкових новин. На сучасному етапі інформація є цінністю великого масштабу. Її інтегрітет і надійність визначають рівень стійкості суспільства та держави перед загрозами. Однак, разом із зростанням значення інформації, ми спостерігаємо також і збільшення кількості дезінформації, фейкових новин і маніпуляцій інформацією.

Ці явища загрожують національній безпеці України. Дезінформація може викликати паніку серед населення, впливати на громадську думку, викривати національний потенціал перед ворогами, та порушувати державні процеси. Фейкові новини можуть спричиняти соціальні конфлікти, підривати довіру до державних інституцій, та завдавати значної шкоди національним інтересам. У світлі цих викликів, суспільство зобов'язано знати як розрізняти та захищати себе від фейків, інструменти та методи протидії.

Фейкова новина – це інформаційне вкидання спеціально підготовленої інформації свідомо провокаційного та резонансного характеру. При цьому сам фейк може містити як свідомо хибну, так і справжню (верифіковану) інформацію, вирвано з контексту конкретної бесіди, розмови або виступу. Мета фейкової новини – створення ажіотажу навколо уявного інформаційного приводу, створюваного закидом наперед провокаційної інформації, що має резонансний характер [1, с. 12].

Походження дезінформації та фейкових новин вельми складне і різноманітне. Ці явища можуть виникати з різних мотивацій та від різних суб'єктів. Деякі з основних джерел та факторів, що призводять до поширення дезінформації та фейкових новин: Деякі країни можуть

використовувати дезінформацію та фейкові новини як інструмент гібридної війни для впливу на інші країни. Засоби масової інформації можуть створювати та поширювати фейкові новини. В інтернеті анонімні користувачі можуть створювати та поширювати фейкові новини без відома своєї ідентичності.

Розповсюдження дезінформації та фейкових новин є серйозною загрозою для суспільства, оскільки вони можуть впливати на громадську думку, вибори, та створювати паніку. Боротьба з цими явищами вимагає спільних зусиль держав, медіа, технологічних компаній та громадянського суспільства.

Дезінформація може викликати такі наслідки: Дезінформація може викликати збурення громадської думки та створити атмосферу недовіри та паніки серед населення, підірвати довіру громадян до медіа, інформаційних джерел, та навіть державних інституцій, впливати на політичні рішення та вибори, оскільки фейкові новини можуть викликати негативні переконання та стереотипи, викликати паніку та хаос серед громадян, стимулювати міжнаціональні та міжсоціальні конфлікти.

Щоб захиститися від дезінформації та фейкових новин, суспільству варто бути не тільки достатнім чином мати гарний рівень володіння сучасними технологіями, чи бути інформаційно грамотною особою. Також варто притримуватися деяким правилам поводження з інформаційним простором а саме: перевіряти джерело новин, перевіряти факти, постійно підвищувати свою інформаційну грамотність, перевіряти дати публікації, уникати спекуляції і чуток, і т. д.

В Україні існують ініціативи з фактчекінгу. Серед них – StopFake.org, заснований 2 березня 2014 року. Ініціаторами його створення стали викладачі, випускники та студенти Могилянської школи журналістики та програми для журналістів і редакторів Digital Future of Journalism. До проєкту долучилися журналісти, редактори, програмісти, перекладачі та ін. В опублікованому звіті проєкту за 2014–2018 роки було проаналізовано і спростовано 919 неправдивих повідомлень. При цьому 85 зі 178 джерел поширення фейкових новин про Україну – російські ЗМІ (Річний звіт StopFake.org, 2018) [2, с. 13].

Таким чином, дезінформація та фейкові новини становлять серйозну загрозу національній безпеці. Вони можуть роз’єднувати суспільство, порушувати довіру до інформації та державних інституцій, а також викликати паніку та соціальні конфлікти. Проте, існують способи протидії цим загрозам. Важливо зосередитися на підвищенні інформаційної грамотності населення, зміцненні правових та етичних стандартів у журналізмі, та активному впровадженні заходів безпеки та контролю на рівні держави.

1. Вакуленко, А. О. «Фейкові новини та дезінформація, як загроза національній безпецІ.» конференції «Актуальні проблеми соціальних комунікацій» 30 травня 2022 р.: с. 12-14.

2. Дементьєва Л. , і Сукова, Д. (2023) «Вплив фейкових новин та дезінформації в аудіовізуальних медіа», Вісник Київського національного університету культури і мистецтв. Серія: Аудіовізуальне мистецтво і виробництво, 6(1), с. 8–19.

БОЙКО Володимир
курсант 3-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції,
Науковий керівник:
ПЕРВІЙ Віта
викладач кафедри
оперативно-розшукової діяльності
факультету підготовки фахівців
для підрозділів кримінальної поліції,
доктор філософії

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

У зв’язку з подіями у нашій країні, однією зі значущих проблем є зростання рівня злочинності в умовах воєнного стану. Це має негативний вплив на економічну та соціальну стабільність держави, загрожує національній безпеці та порушує права та свободи громадян. У зв’язку з збройною агресією Російської Федерації проти України, значні зміни відбулися у кримінально-процесуальних, криміналістичних та оперативно-розшукових аспектах організації розслідування злочинів.

Відповідно до чинного законодавства, оперативно-розшукова діяльність – це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів. Завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [1].

Сучасний рівень злочинності став однією з ключових складових розвідувально-підривної та диверсійної діяльності спеціальних служб

Російської Федерації. Це вимагає вдосконалення організації оперативно-розшукової роботи для виявлення та розслідування кримінальних порушень в умовах воєнного стану.

Суть поняття «організація оперативно-розшукової діяльності» у теорії полягає у вдосконаленні специфічного механізму, що має забезпечувати ефективне використання оперативно-розшукових можливостей оперативних підрозділів та досягнення високої результативності у протидії злочинності [2, с. 117].

Організація оперативно-розшукової діяльності офіційно відображена у положеннях нормативно-правових актів, що регулюють суспільні відносини у сфері оперативно-розшукової роботи. Сутність цієї організації проявляється у вчинках уповноважених посадових осіб, таких як створення керованих систем (організаційних структур) у сфері оперативно-розшукової діяльності, упорядкування (розвиток) цих систем до рівня, який забезпечує найвищу ефективність вирішення завдань оперативно-розшукової діяльності в конкретних умовах; упорядкування (налагодження) процесу управління (його окремих стадій) у сфері оперативно-розшукової діяльності та створення оптимальних умов для ухвалення та реалізації відповідних управлінських рішень; управлінського циклу, тобто самого процесу управління оперативно-розшуковою діяльністю; створення необхідних умов для конкретних оперативно-розшукових заходів [3, с. 147].

Для забезпечення ефективності кримінального провадження та виконання повноважень поліції в умовах воєнного стану, Верховною Радою прийнято низку законів, включаючи №2123-IX від 15 березня 2022 року, що вносять зміни до законів України «Про Національну поліцію» та «Про Дисциплінарний статут Національної поліції України». Головна мета цих змін - оптимізація роботи поліції, включаючи період воєнного стану. Що стосується оперативно-розшукової діяльності, вони вносять якісні зміни у взаємодію оперативних підрозділів Національної поліції з державними та місцевими органами самоврядування, юридичними особами, зокрема утримання військовополонених, конвоювання затриманих осіб, розмінування та допуск поліцейських до спеціальних вибухотехнічних робіт. Зміни також стосуються збору біометричних даних осіб, включаючи дактилоскопіювання, а також розширення підстав для зупинки та перевірки транспортних засобів поліцейськими, а також перевірки водіїв та пасажирів [4].

Незважаючи на внесені зміни у законодавство після введення режиму воєнного стану, на наш погляд, деякі аспекти удосконалення взаємодії між слідчими та оперативними підрозділами в умовах воєнного стану залишаються невирішеними. Зокрема, активні бойові дії на території України, масовані обстріли, загроза, що пов’язана з визволенням міст та інші фактори ускладнюють проведення оперативно-розшукових заходів та обмежують комунікацію між слідчим та працівниками оперативних підрозділів. Це вимагає врегулювання надання права оперативному

підрозділу у невідкладних ситуаціях проводити такі заходи в рамках відкритого кримінального провадження без відповідного рішення слідчого. Крім того, ці зміни повинні враховувати питання щодо термінів виконання оперативними працівниками завдань слідчого, особливо в разі об'єктивної неможливості їх виконання у встановлені строки через обставини, пов'язані з воєнним станом.

Отже, деякі аспекти організації оперативно-розшукової діяльності в умовах воєнного стану потребують адекватної відповіді та нормування на рівні законодавства. Це вимагає ухвалення спеціального законодавства, яке має включати положення, що регулюють особливі процедури здійснення оперативно-розшукових заходів в умовах введеного режиму.

1. Про оперативно-розшукову діяльність : закон України від 18.02.1992 № 2135-XII із змін. URL : https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення 21.10.2023)

2. Павленко С.О. Основи оперативно-розшукової тактики: монографія. Київ : «Видавництво Людмила», 2022. 624 с

3. Князєв С. М. Загальна характеристика організації оперативно-розшукової діяльності та негласної роботи національної поліції України. Південноукраїнський правничий часопис. 4. 2019, Ч. 3. С. 146-151.

4. Про внесення змін до законів України «Про Національну поліцію» та «Про Дисциплінарний статут Національної поліції України». Закон України №2123- IX від 15 березня 2022 року URL : https://zakon.rada.gov.ua/laws/show/2123-20#Text. (дата звернення 21.10.2023)

РИБАЛЬЧЕНКО Людмила,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ГЕНДЕРНА НЕРІВНІСТЬ В ОПЛАТІ ПРАЦІ В КРАЇНАХ СВІТУ ТА В УКРАЇНІ

Гендерна нерівність між чоловіками та жінками в усьому світі відбувалася завжди і спостерігається нині в багатьох сферах життєдіяльності. Для її подолання необхідно пройти значно складний шлях, але це не є питанням навіть десятків років, а суттєвого тривалого періоду.

Актуальним питанням в цьому напрямі є оплата праці. За даними дослідження всесвітньої організації Global Gender Gap Report 2023, гендерний розрив в оплаті праці становить близько 20%. Найбільшою є нерівність в оплаті праці між чоловіками та жінками в Південній Кореї, де

розрив становить 31,06%, далі йде Ізраїль 24,32%, Японія 22,1%, Латвія 19,76%, Естонія 19,6%, Україна 18,6% та США 16,86% (рис. 1). Серед країн, де відбувається найменший розрив в оплаті праці між чоловіками та жінками є Норвегія 4,6%, Колумбія 4%, Бельгія 3,8%, Румунія 3,3% та Болгарія 2,55% [1].

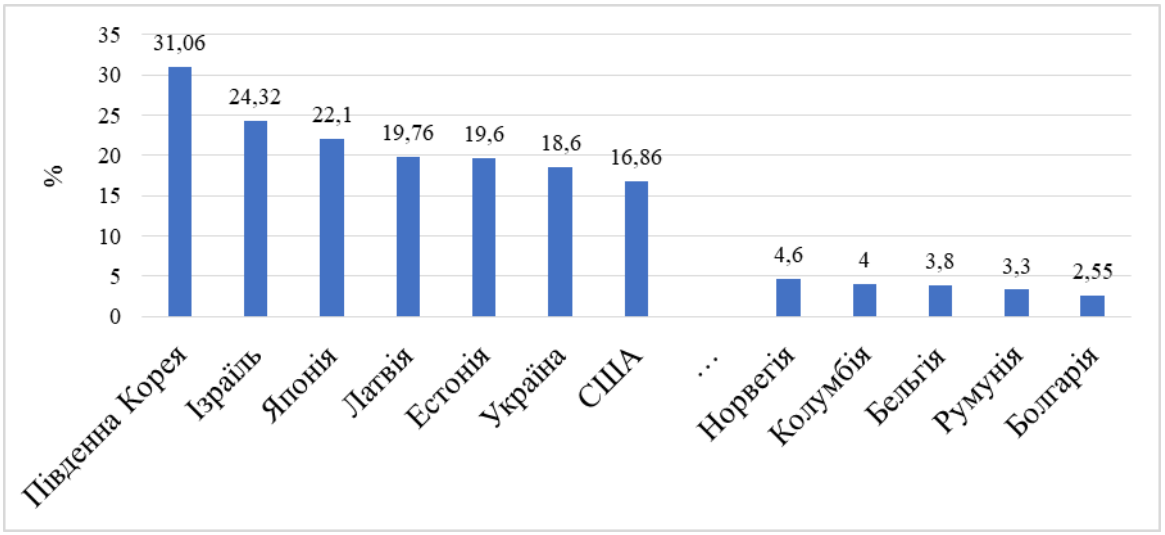

Рис. 1. Нерівність в платі праці в країнах світу, (%)

Розглядаючи гендерну нерівність Південної Кореї, необхідно сказати, що тут жінки працюють в таких секторах, де їх труд є низькооплачуваним і залежить від стажу роботи.

Друге та третє місця у рейтингу посіли Ізраїль та Японія. В Ізраїлі гендерний розрив оплати праці становить 24,32%, у Японії – 22,11%.

У Японії однією з причин гендерного розриву є велика кількість жінок, які є непостійними працівниками та займають мало місць у професіях з високим статусом, тому і отримують нижчу за інших заробітну плату.

В Україні розрив в заробітній платі між жінками та чоловіками становить 18,6%. Національною стратегією України до 2030 року є подолання гендерного розриву в оплаті праці, скоротивши його розрив до 13,6%.

Гендерний розрив в оплаті праці в США та Канаді становить 16,86% та 16,67% відповідно, на Кіпрі – 16,58%, в Фінляндії – 15,98%, Австралії – 15,31%, Британії – 14,35%, Німеччині – 14,2%, Швейцарії – 13,8%, Нідерланди – 13,33%, Ісландія – 12,9%, Мексика – 12,5%, Австрія – 12,38%, Угорщина – 12,35%, Франція – 11,82%, Португалія – 11,72%, Словаччина – 11,7%, Чехії – 11,52%, Мальті – 11,09% та інші [1].

За дванадцять років в Україні гендерна нерівність в оплате праці між чоловіками та жінками суттєво змінилася (рис. 2).

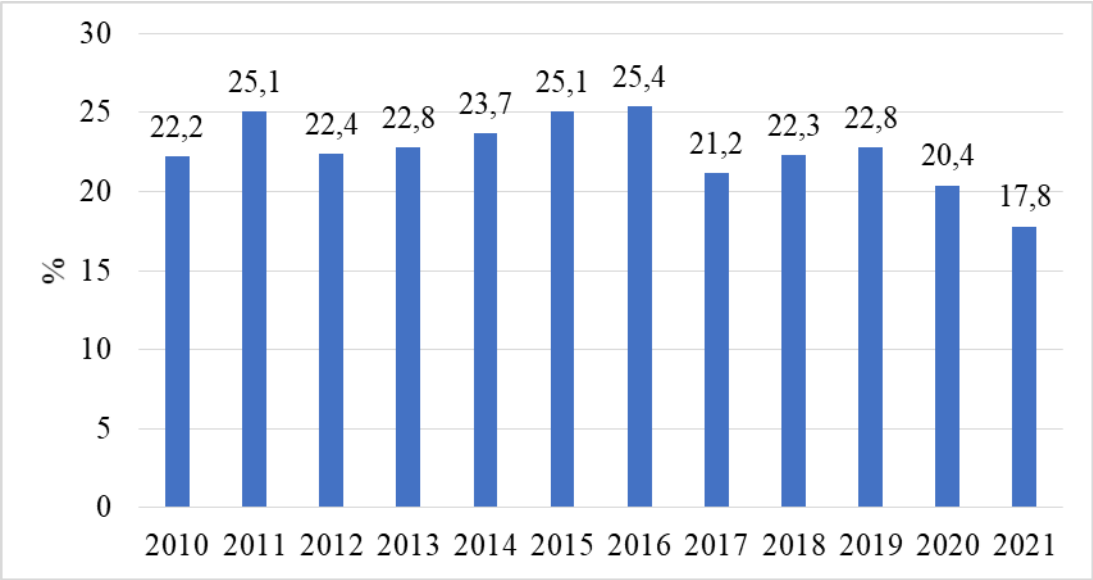

Рис. 2. Гендерна нерівність в Україні у 2010-2021 рр.

Гендерний розрив в оплаті праці в Україні у 2010-2020 рр. був більшим за 20% і лише із 2021 року зменшився. Виконуючи майже однакові види робіт, жінки отримували меншу заробітну плату, ніж чоловіки.

Так, із 2010 року розрив між середньомісячним заробітком чоловіків і жінок скоротився до 22,2%. В Україні чоловіки заробляли близько 2 тис. 538 грн. за місяць, а жінки – 1 тис. 974 грн. У 2014 році жінки заробляли близько 3 тис. 37 грн за місяць, що на 23,7% менше, ніж чоловіки (3 тис. 979 грн). Розрив збільшився до 2016 року, коли чоловіки заробляли трохи більше 6 тис. грн, а жінки – 4 тис. 480 грн. У 2018-му різниця між середньомісячним заробітком жінок і чоловіків становила -22,3%: чоловіки – 10 тис. 83 грн, жінки – 7 тис. 830 грн.

Середня зарплата чоловіків в 2019 році становила 11 тис. 961 грн на місяць, у жінок – 9 тис. 237 грн. У минулому році гендерний розрив в оплаті праці трохи скоротився: чоловіки на місяць отримували в середньому 13 тис. 35 грн, жінки – 10 тис. 373 грн. Лише у 2021 році жінки стали отримувати в середньому на 18% меншу зарплату, ніж чоловіки [2].

---

1. Всесвітній економічний форум (World Economic Forum) Global Gender Gap Report 2023. INSIGHT REPORT. JUNE 2023.
2. Гендерний розрив в оплаті праці: як відрізняється середня зарплата жінок і чоловіків в Україні. URL : https://www.slovoidilo.ua/2021/06/10/infografika/suspilstvo/hendernyj-rozryv-oplati-praczi-yak-vidriznyayetsya-serednya-zarplata-zhinok-cholovikiv-ukrayini

ЛИМАНСЬКА Ірина
курсант 1-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри інформаційних
та комунікативних технологій
Дніпропетровського державного
університету внутрішніх справ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Актуальність правового аспекту інформаційної культу¬ри визначається тим, що всі соціальні процеси – еко¬номічні, психологічні, інформаційні, технологічні та, що виникають, відбуваються і припиняються в суспільстві, державі потребують правового регулювання. Ці процеси з'являються, розвиваються, удосконалюються і відмира¬ють чи ліквідуються у правовому середовищі (правовому полі), на його базі. При цьому виникає потреба урегулю-вання суспільних відносин з урахуванням необхідності визначення правил поведінки людей, співвідношення їхніх, потреб та інтересів з потребами та інтересами окремих со¬ціальних корпорацій, суспільства, держави, міжнародно¬го співтовариства.

Сьогодні в розвинених країнах світу приділяється велика увага питанням інформатизації суспільства. Все більшим стає розуміння того, що країна, яка буде володіти потужними інформаційними ресурсами, ефективною системою їх реалізації, буде знати динаміку й перспективи їх розвитку, опиниться на гребні науково-технічного прогресу і зможе його ефективно використовувати. Тому сучасний етап розвитку суспільства в цих країнах характеризується переходом до всеохоплюючої інформатизації усіх соціальних інституцій і процесів, пов'язаних із формуванням інформаційних ресурсів і передачею знання. У світі спостерігається бурхливий розвиток засобів інформатизації (комп'ютерів, комп'ютерних мереж, всіляких електронних пристроїв) і, в зв'язку з цим, поява нових інформаційних технологій обробки, передачі, одержання і збереження інформації.

Не залишається осторонь цих процесів і Україна, в якій відбувається інтенсивне впровадження сучасних інформаційних технологій майже в усі сфери життєдіяльності суспільства, зокрема, в правоохоронній та юридичній діяльностіь. Створюються та успішно використовуються різноманітні інформаційно-пошукові системи, бази та банки даних, системи електронного документообігу. Сучасні інформаційні технології надають працівникам

правоохоронних органів можливість отримати багатоцільову довідкову, аналітичну та статистичну інформацію, що сприяє ефективному виконанню ними різноманітних оперативно-службових завдань.

Однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій.

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: 1) удосконалення форм та методів управління системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків; 4) розбудова та широке використання ефективних та потужних комп'ютерних мереж; 5) застосування спеціалізованих засобів захисту інформації; 6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [1, с. 12].

Підбиваючи підсумки, можливо зазначити те, що враховуючи сучасні світові тенденції збільшення ролі інформаційного забезпечення в оперативному обслуговуванні, варто розширити функції аналітичних підрозділів у рамках здійснення оперативно-розшукової діяльності.

1. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. Київ : НАВСУ, 2013. 82 с.

БОЖКЕВИЧ Анастасія
здобувач ступеня вищої освіти магістр
за спеціальністю «Кібербезпека»
факультету № 6
Науковий керівник:
ОНИЩЕНКО Юрій
доцент кафедри кібербезпеки та
DATA-технологій факультету № 6
Харківського національного
університету внутрішніх справ,
кандидат наук з державного
управління, доцент

БЕЗПЕЧНЕ КОРИСТУВАННЯ ГРОМАДСЬКОЮ ТА ДОМАШНЬОЮ МЕРЕЖЕЮ WI-FI

Сьогодні мережа Wi-Fi широко поширена по всій земній кулі і неможливо уявити і дня без користування нею. Бездротова мережа сучасності дозволяє нам незалежно від місця знаходження завжди бути

онлайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в мережі Інтернет.

Бездротові мережі зручні і добре захищені, що дає можливість використання мережевих технологій цього типу і в домашніх умовах [1] .

Користування Wi-Fi вдома передбачає наявність роутера, що, власне, «роздає» Wi-Fi. Саме налаштування цього пристрою є необхідною умовою безпеки. Якщо не приділити увагу цьому важливого питанню, зловмисники можуть отримати контроль над каналами передачі даних, вкрасти конфіденційну інформацію, гроші, обмежити та/або позбавити користувача доступу до мережі Інтернет.

Безпека домашньої мережі – це набагато більше, ніж встановлення пароля для домашнього Wi-Fi. Члени вашої родини дивляться свої улюблені шоу на Smart TV, купують різні товари в інтернеті, грають в мережеві ігри або працюють вдома. При цьому всі види важливих даних – особиста інформація, паролі, адреси, приватні фотографії тощо – постійно підключені до інтернету через домашню мережу.

Більшість користувачів мережі Інтернет знає про такі поняття, як «фішинг» та «шкідливе програмне забезпечення», які хакери використовують, щоб замаскувати себе та отримати доступ до домашньої мережі для крадіжки або знищення персональних даних. Але чи справді усі користувачі обізнані з тим, що це насправді і як з цим боротися? Безпека домашньої мережі – це фундаментальна основа для захисту себе та родини від загроз з боку зловмисників. Існують певні правила, дотримуючись яких, можна з легкістю захистити власну інформацію від витоку у мережі.

Перш за все, налаштовуючи роутер, треба зважати на такі аспекти, що є складовими високого рівня кібербезпеки «домашньої» мережі, адже визначають те, як і коли роутер буде дозволяти пристроям користуватися Wi-Fi:

1. Спершу змініть стандартні налаштування логіна і пароля, що встановленні виробником із заводу. Ідеальний варіант – щомісячна, тобто регулярна зміна паролів.

2. Змініть тип шифрування на WPA2 / WPA, що зробить передачу даних мережею більш захищеною.

3. Керуйте списком пристроїв що користуються Вашою Wi-Fi мережею через визначення MAC-адрес пристроїв що можуть до неї під’єднуватися.

4. Вимкніть функцію WPS (QSS) – ця функція спрощує підключення нових пристроїв до мережі. Якщо Wi-Fi користуються з одних і тих самих гаджетів, краще відключити цю функцію, оскільки вона має серйозні уразливості.

5. Приховайте свою мережу від пристроїв які сканують простір в пошуках мереж. Ідея полягає у тому, що якщо Wi-Fi мережу не бачать, то вірогідність того що її захочуть «зламати» суттєво знижується [2].

Слід зауважити, що сучасні технології дають нам можливість користуватись мережею Wi-Fi не лише вдома, а й в громадських місцях.

Сьогодні підключитися до безкоштовних мереж Wi-Fi можна у багатьох закладах харчування, в парках, громадському транспорті, торговельних центрах і навіть в укриттях. Для багатьох українців це зручний та вигідний спосіб отримати доступ до мережі Інтернет та бути постійно на зв'язку [3].

Однак, варто пам'ятати, що переважна більшість Wi-Fi мереж у громадських місцях мають дуже низький рівень захисту від злому. Отже, отримавши доступ до керування ними, шахраї можуть отримати доступ до конфіденційної інформації користувачів у тому числі до логінів та паролів від облікових записів, якими кожен з нас активно користується.

Для того, щоб не потрапити на гачок шахраїв, необхідно дотримуватися простих правил безпеки при роботі з громадськими Wi-Fi мережами. Ці правила стосуються всіх видів пристроїв – ПК, планшетів, смартфонів:

1. Встановіть антивірус.
2. Використовуйте VPN-сервіси.
3. Краще підключатися до мереж Wi-Fi вручну.
4. Обмежте можливість автоматичного підключення пристрою. Це можна зробити в налаштуваннях ноутбука або смартфону.
5. Якщо є можливість, уточніть назву мережі, до якої маєте намір під'єднатися. Пам'ятайте – кібершахраї можуть створювати фейкові мережі для заволодінням інформацією.
6. Вимкніть функцію надання спільного доступу до файлів через локальну мережу на всіх пристроях. При підключенні до громадського Wi-Fi вони можуть стати доступними зловмисникам.
7. Уникайте здійснення грошових операцій: перекази, покупки, регулярні платежі. Не використовуйте загальнодоступні мережі Wi-Fi для обміну чутливою конфіденційною інформацією і вирішення важливих справ. Краще скористатися перевіреною стаціонарною мережею або мобільним інтернетом.
8. Відвідуйте сайти, що використовують безпечний протокол з'єднання HTTPS.
9. Вимкніть загальний доступ до файлів і папок на пристрої що буде приєднуватися до відкритої Wi-Fi мережі.

Отже, можна зробити висновок, що сьогодні більшість користувачів перебувають онлайн майже цілодобово. Значною мірою на це вплинула наявність загальнодоступних Wi-Fi у громадських місцях та активним користуванням мережею в домашніх умовах [4]. Враховуючи той факт, що протягом наступних кількох років Wi-Fi обіцяють зробити безпечнішим, наразі досі залишається актуальним питання щодо збереження своєї цифрової безпеки в кіберпросторі.

1. Бездротові мережі (Wi-Fi). URL : https://i-help.us/adjustment/wifi/
2. Wi-Fi безпека: вдома та в громадських місцях. URL :

https://zillya.ua/index.php?q=wi-fi-bezpeka-vdoma-ta-v-gromadskikh-mistsyakh

3. Чи безпечно користуватися громадським безкоштовним Wi-Fi – роз'яснення Держспецзв'язку. URL : https://armyinform.com.ua/2022/08/04/chy-bezpechno-korystuvatysya-gromadskym-bezkoshtovnym-wi-fi-rozyasnennya-derzhspeczzvyazku/

4. Топ-10 порад для безпечного використання відкритих Wi-Fi. URL : https://www.eset.com/ua/about/newsroom/blog/data-protection/top-10-sovetov-dlya-bezopasnogo-ispolzovaniya-otkrytykh-wi-fi/

БОЖКЕВИЧ Микола
здобувач магістерського
ступеня вищої освіти
за спеціальністю «Кібербезпека»,
Науковий керівник:
СТРУКОВ Володимир
завідувач кафедри інформаційних
технологій Харківського
національного університету
внутрішніх справ,
кандидат технічних наук, доцент,

ПЕРЕВАГИ ТА НЕДОЛІКИ БЕЗДРОТОВОЇ СИГНАЛІЗАЦІЇ

Дротова сигналізація нам добре зрозуміла: ось дроти, по них іде сигнал. Сьогодні ж такий захист радше ілюзорний. Дротові системи безпеки – це клубок проблем. Вони забирають багато сил у процесі установки та нервів під час експлуатації.

Виробники Ajax прагнули створити ідеальну охоронну систему, тому дроти з усіма їхніми недоліками замінили власною радіотехнологією Jeweller – неприступною, стабільною, енергоефективною. Створювачі хотіли, щоб вона не поступалася дротам у надійності, однак результат перевершив всі розрахунки [1].

Бездротова сигналізація – це така охоронна система, в якій усі вузли взаємодіють між собою по радіозв'язку, а саме по певних технологіях, таких як WIFI, Bluetooth та ін. При цьому сигнал тривоги може передаватись як по дротовому каналу (інтернет, міський телефон), так і по радіоканалу (GSM сигналізація). Без дротів – без вразливостей [2].

Датчики Ajax працюють на відстані до 2000 метрів відкритого простору від хаба. У приміщеннях ця дальність гарантує, що зміна планування або перестановка меблів не зможуть порушити зв'язок. Сигнал все одно буде доставлено до хаба.

Щоб розуміти роботу системи, перш за все необхідно розібрати всі її складові, а саме - будову бездротової сигналізації:

Бездротова сигналізація складається з таких вузлів: центральний блок (хаб), пульт управління дозвонщик, бездротові датчики, сповіщувачі, брелоки і т.д. Також сучасні сигналізації мають спеціальний додаток для мобільного телефона, який дозволяє моніторити об'єкт та управляти окремими його елементами.

Всі вузли такої сигналізації працюють по спеціальному протоколу. Такий протокол крім передачі інформації від датчиків сигналізації на центральний блок, забезпечує також захист цієї інформації від завад, здійснює її шифрування та перешкоджає можливість дистанційного злому охоронної системи. Тому чим надійніший протокол, тим дорожчою буде охоронна сигналізація.

Протокол передачі даних – набір угод інтерфейсу логічного рівню, які визначають обмін даними між різними програмами. Ці угоди задають однаковий спосіб передачі повідомлень і обробки помилок при взаємодії програмного забезпечення рознесеного на просторі апаратної платформи, з'єднаної тим чи іншим інтерфейсом.

Переваги бездротової сигналізації:

Всупереч тому, що бездротові сигналізації є дорожчими, вони набувають широкої популярності, оскільки коштують дорожче дротових, але більш популярні, оскільки вони простіші в монтажі та не потребують укладки кабелів. Тому такі сигналізації легко монтуються на об'єктах, де вже був зроблений ремонт. Крім того, бездротові системи легко масштабуються та розширюються. Демонтаж такої системи або зміна положення окремих датчиків також є не складними операціями.

Недоліки бездротової сигналізації:

1. Бездротова сигналізація є дорожчою за дротову, оскільки бездротові датчики коштують дорожче дротових. Це суттєво здорожчує систему сигналізації для великого об'єкта. Проте, для малого об'єкта (наприклад квартири) бездротова сигналізація не буде сильно дорожчою в порівнянні з дротовою, оскільки в такому випадку буде мало безпровідних датчиків, а основний вклад в загальну ціну буде йти від централі та пульта управління.

2. Бездротові датчики мають живлення від батарейок чи акумуляторів. Оскільки батарейки з часом розряджаються, то вони потребують періодичної діагностики й заміни. Звичайно, сучасні бездротові сигналізації для дому та офісу самостійно моніторять заряд батарейок на усіх датчиках і повідомляють власника при їх розрядці. Проте все одно потрібно заміняти "сівші" батарейки вручну.

3. Можливе зникнення сигналу внаслідок радіозавад. Радіозавади від різних пристроїв можуть впливати на сигнал від датчика та його спотворювати. Це може приводити до відсутності сигналу від датчиків, і навіть до хибних спрацювань в дешевих китайських сигналізаціях. Імовірність втрати сигналу внаслідок завад збільшується зі зростанням відстані безпровідного датчика від центрального блоку.

Відомі моделі бездротових сигналізацій:

Бездротові сигналізації виробляються багатьма виробниками, що представлені різними брендами, таким як Ajax, Xiaomi, Kerui, Fibaro, ATIS, Aoke, Astrel, PoliceCam, JA, Siren, ОКО, Intervision, Jablotron, Smart system та ін. Кожна модель має своє особливе програмування та особливості у використанні. Слід завжди пам'ятати, що чим новіший засіб експлуатації тим надійніший протокол з'єднання. На сьогоднішній день – це є важливим елементом для охорони нами обраних об'єктів, адже від цього безпосередньо залежить наш захист.

Таким чином, враховуючи всі переваги та недоліки бездротової сигналізації, очевидно, що перед нами максимально ефективне та надійне рішення. Все, що потрібно – віддавати перевагу відомим брендам, які зможуть гарантувати стабільність та ефективність роботи та найновіші протоколи передачі даних [3].

1. Радіотехнологія Jeweller. URL : https://ajax.systems/ua/jeweller/

2. Бездротова сигналізація. URL : https://oxorona.com/no-wires-signalling/

3. Переваги та недоліки бездротових сигналізацій для дому. URL : https://www.volynnews.com/news/all/perevahy-ta-nedoliky-bezdrotovykh-syhnalizatsiy-dlia-domu/

ЛУНГОЛ Ольга
доцентка кафедри
оперативно-розшукової діяльності
та інформаційної безпеки,
к.пед.н., доцент
МАКАРИНСЬКА Анна
курсантка 210 н.вз. факультету
підготовки фахівців для підрозділів
кримінальної поліції Донецького
державного університету
внутрішніх справ

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ВДОСКОНАЛЕННІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

Сучасний світ вимагає від правоохоронних органів не тільки реакції на злочини, але й їх передбачення та запобігання. Інформаційно-аналітична діяльність в правоохоронній сфері відіграє ключову роль в цьому напрямку. Вона полягає у зборі, обробці, аналізі та використанні інформації для прийняття обґрунтованих рішень, запобігання злочинам і забезпечення безпеки громадян. Інформаційно-аналітичні підрозділи опрацьовують значні

масиви даних, перетворюючи їх у корисну для правоохоронних органів інформацію. Вони ретельно аналізують великі обсяги інформації для виявлення зразків та відомостей, які можуть бути корисними в розслідуванні злочинів. Інформаційно-аналітичні методи допомагають в передбаченні можливих випадків порушення закону, що дозволяє правоохоронцям приймати запобіжні заходи та попереджати потенційної загрози. Важливо відзначити, що інформаційно-аналітична діяльність не лише допомагає у запобіганні злочинам, але й в оперативному реагуванні на події.

Інформаційно-аналітична діяльність є важливим і невід'ємним компонентом правоохоронної роботи, тому її постійне вдосконалення, підвищення продуктивності та ефективності, є актуальним завданням для забезпечення безпеки громадян. Саме тут штучний інтелігент (ШІ) знаходить своє застосування та відіграє ключову роль у вдосконаленні інформаційно-аналітичного процесу.

З використанням штучного інтелекту інформаційно-аналітичні системи можуть швидко та результативно аналізувати великі обсяги даних, виявляти відхилення та вести моніторинг. Засоби ШІ дозволяють автоматично відсіювати незначущу інформацію та виділяти ключові відомості. Завдяки алгоритмам машинного навчання, ШІ використовують у розробці прогностичних моделей, які допомагають передбачити події на основі аналізу минулих даних. ШІ вміє розпізнавати образи на зображеннях, відеозаписах, і навіть в тексті, що важливо для відстеження та ідентифікації об'єктів або осіб. ШІ використовують в процесі аналізу соціальних медіа для виявлення зв'язків між особами, встановлення деталей, моніторингу громадської думки на певну тему. ШІ допомагає створювати системи категоризації даних та класифікації інформації, що робить її більш доступною та структурованою для фахівців правоохоронних органів. Завдяки можливості обробляти дані в режимі реального часу, ШІ дозволяє оперативно реагувати на події надаючи швидкі та обґрунтовані рішення.

На важливості та актуальності використання ШІ в роботі правоохоронних органів наголошують як вітчизняні, так і зарубіжні науковці. Так, Демура М.І. [1] описує напрями використання ШІ в роботі італійських правоохоронців з попередження злочинності та підвищення безпеки в містах, поліцейських Сполученого Королівства в рамках проекту з прогнозування можливих місць крадіжок зі зломом, розкрадання і нападу за допомогою ШІ. Лаврик Н.С. та Неклеса О.В. [2] зазначають, що сучасна діяльність НП України вже активно застосовує можливості ШІ для розпізнавання обличчя, яке дозволяє правоохоронцям порівнювати отримане зображення обличчя із системою відеоспостереження та даними, які вже є в інформаційних базах, а також відповідно до біометричних показників. Як приклад, наводять автоматизовану систему контролю безпеки на дорогах, яка фіксує правопорушення в автоматичному режимі, а також полегшує діяльність правоохоронців щодо документування порушень Правил дорожнього руху.

Отже, інформаційно-аналітична діяльність є важливою складовою різних сфер сучасного суспільства, включаючи бізнес, науку, та, безперечно, правоохоронні органи. Роль ШІ у вдосконаленні інформаційно-аналітичної діяльності важлива, оскільки він допомагає отримати цінну інформацію з великих обсягів даних та прискорює процес прийняття рішень. Таким чином, впровадження ШІ є необхідним етапом у розвитку інформаційно-аналітичної сфери.

1. Демура М.І. Міжнародний досвід використання алгоритмів штучного інтелекту у кримінальному провадженні. Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 24 – 28.

2. Лаврик Н.С., Неклеса О.В. Аспекти використання штучного інтелекту під час проведення кримінального аналізу в підрозділах Національної поліції України. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України. 2022. С. 268-269. URL : http://elar.naiau.kiev. ua/jspui/ handle/123456789/24907.

3. Шаєц Є., Лунгол О. Перспективи використання штучного інтелекту в проведенні кримінального аналізу. Актуальні питання діяльності підрозділів кримінальної поліції: Всеукр. наук.-практ. конф. (м. Кропивницький, 14 квітня 2023 р.). Кропивницький: ДонДУВС, 2023. С. 422–424.

СЕМЧИШИН Володимир
перший заступник начальника
Управління СБУ
в Івано-Франківській області
ЯЦЮК Тарас
аспірант кафедри права та публічного
управління Університету
Короля Данила,
начальник відділу Управління СБУ
в Івано-Франківській області
ТКАЧЕНКО Павло
аспірант кафедри кримінально-
правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
член Асоціації правників України

КРИМІНАЛЬНА АНАЛІТИКА ЯК СКЛАДОВА КІБЕРБЕЗПЕКИ

Кібербезпека – це сукупність заходів, технологій, практик та процедур, спрямованих на захист комп’ютерних систем, мереж, даних та інформації від несанкціонованого доступу, зміни, руйнування чи розповсюдження. Основна

мета кібербезпеки – забезпечення конфіденційності, цілісності та доступності цифрових ресурсів. Водночас кібербезпека держави – це комплексний підхід та система заходів, спрямованих на захист інформаційних, технологічних та комунікаційних ресурсів країни від кіберзагроз та кібератак. Це важливий аспект національної безпеки, оскільки сучасна держава значною мірою залежить від функціонування своїх інформаційних систем та технологічної інфраструктури. Саме забезпечення захисту інформаційної та кібернетичної безпеки держави покладається на спеціальний підрозділ Служби безпеки України (далі – СБУ). В структурі СБУ ефективно функціонує департамент захисту інтересів держави в сфері інформаційної безпеки, який цілодобово забезпечує кібербезпеку особливо важливих інформаційно-телекомунікаційних мереж держави. Спектр діяльності забезпечення кібербезпеки сьогодні не обмежений виключно на інформаційні платформи, а й охоплює об'єкти критичної інфраструктури, державні інформаційний ресурси, кібервійськові операції, навіть кібердипломатію та міжнародне співробітництво. Зважаючи на вищевикладене, підрозділи забезпечення інформаційної та кібернетичної безпеки держави мають бути цілком забезпечені відповідними методичними та прикладними напрямками, серед яких зокрема аналітичне.

Наразі аналітичне забезпечення відіграє ключову роль в діяльності підрозділів кібербезпеки, однак в більшості своїх, на належному рівні, не надається увага такому напрямку роботи, як кримінальна аналітика. Отже, кримінальна аналітика – це складна та мультидисциплінарна область, яка використовує методи та техніки аналізу даних для виявлення та розкриття злочинів. Ця дисципліна орієнтована на дослідження кримінальної діяльності, злочинних тенденцій, а також на розробку стратегій та заходів для їх запобігання та припинення.

На думку більшості вчених, кримінальна аналітика, за умови отримання правильних завдань та ефективного використання її потенціалу, виступає головною зброєю в арсеналі правоохоронних органів. Збір, аналіз і поширення аналітично опрацьованих даних забезпечують набуття правоохоронними органами знань, необхідних для нейтралізації будь-яких проявів злочинності або запобігання їм. Кримінальна аналітика є результатом аналізу злочинців і даних про злочини, чи то на оперативному, тактичному чи стратегічному рівні [1, с. 27].

Діяльність аналітиків з підготовки аналітичних продуктів передбачає дослідження інформації та даних, отриманих з різноманітних джерел за визначеним алгоритмом, який характерний для усіх рівнів аналітичних досліджень. Цей алгоритм називають аналітичним процесом, і він складається з таких етапів: формування аналітичного завдання, збирання відомостей, їх оцінювання, накопичення та збереження (упорядкування), інтеграція та візуалізація для проведення аналізу, підготовка висновку, оцінка висновку, поширення (доведення продукту аналітики замовникові).

Під час проведення аналітичного процесу для отримання аналітичного продукту можуть застосовуватись різні методи: аналіз взаємозв'язків, аналіз злочинних мереж, аналіз телефонних з'єднань, аналіз подій, аналіз дій, аналіз обігу (руху), аналіз фінансових транзакцій, порівняльний аналіз справ, аналіз злочинних моделей (серій), картографування криміногенної інформації (ГІС), статистичний аналіз злочинів, SWOT аналіз, аналіз ризиків, PEST аналіз; SOCTA, OSINT, аналіз злочинних моделей, аналіз тенденцій тощо. Результати аналітичного дослідження виражаються у вигляді письмових аналітичних звітів, досьє на фізичну або юридичну особу, об'єкт (предмет), організовану групу чи злочинну організацію, подію, профілів, аналітичних орієнтувань та інших аналітичних документів (довідки, інформаційні зведення, аналітичні огляди) [1, с. 27].

До принципів кримінально-аналітичної діяльності варто віднести: законність, функціональна спеціалізація, розумна достатність, взаємодія, професійна компетентність, об'єктивність, сумісність форм і методів, цілеспрямованість, незалежність, системність та безперервність. Водночас за видами кримінального аналізу виділяють операційний, тактичний та стратегічний. Безумовно кожний з напрямків – це частка інформаційно-аналітичної діяльності.

Операційний кримінальний аналіз – це інформаційно-аналітична діяльність за конкретними кримінальними провадженнями або оперативними справами стосовно інформації, що становить інтерес для підрозділів кібербезпеки щодо ознак та інших відомостей, які характеризують осіб, об'єктів, організованих груп чи злочинних організацій, що в подальшому сприятиме розслідуванню правопорушень. У процесі операційного кримінального аналізу здійснюється встановлення тенденцій злочинності, з'ясовуються місця концентрації вчинення злочинів, визначається профіль підозрюваного та потерпілого. До цих дій вдаються з метою підготовки управлінських рішень щодо розподілу сил та засобів і проведення операційного аналізу.

Тактичний кримінальний аналіз – це аналіз злочинності та злочинів на конкретній території за невеликий проміжок часу, за певним видом злочину чи протиправної діяльності певної групи з метою напрацювання тактичних заходів із затримання злочинців, виявлення ризиків і попередження конкретних правопорушень.

Стратегічний кримінальний аналіз – це ідентифікація та оцінювання кримінальних загроз особі, суспільству, державі, метою яких є визначення вразливості правоохоронної системи або середовища, та формування управлінських рішень щодо запобігання вчиненню кримінальних правопорушень і протидії злочинності (виявлення тенденцій, закономірностей, прогнозування розвитку встановлених загроз за великий період часу). Проводиться з метою підготовки стратегічних управлінських рішень та визначення ризиків розвитку криміногенної ситуації [1, с. 30].

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» (ILP), як моделі, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних. Основні складові розвитку моделі ILP є такими: нормативно-правова база для врегулювання; інформаційні ресурси; система наповнення інформаційних ресурсів; система оцінювання джерел та достовірності інформації; спеціальне програмне забезпечення; інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами та іншими джерелами інформації; тренінги для аналітиків практичних підрозділів; стандартизовані форми аналітичних продуктів.

Разом з цим, варто підкреслити, що кримінальний аналітик повинен співпрацювати з оперативними підрозділами в рамках оперативно-розшукової діяльності та виконувати покладені на нього завдання. Швидко та оперативно знайдена інформація дасть змогу та можливості швидко розслідувати кримінальне провадження, спираючись на отриману інформацію.

Отже, зважаючи на вищевикладене можливо визначити, що кримінальна аналітика є невід'ємною складовою кібербезпеки. Шляхом аналізу кіберзлочинів, їхньої характеристики та особливостей, а також ідентифікації злочинців та прогнозування їхньої діяльності, оперативні підрозділи в змозі ефективно захищати інформаційно-телекомунікаційні системи та державні інформаційні ресурси. Вдосконалення стратегій та політик кібербезпеки на основі аналітичних даних допоможе побудувати більш безпечне цифрове майбутнє.

1. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

ФЕДЧАК Ігор
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент

ПРАКТИЧНІ АСПЕКТИ ВИРІШЕННЯ ПРОБЛЕМ ЧЕРЕЗ ВИКОРИСТАННЯ SWOT-АНАЛІЗУ ПІД ЧАС РЕАЛІЗАЦІЇ МОДЕЛІ ЗДІЙСНЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ, ОРІЄНТОВАНОЇ НА ПОТРЕБИ ГРОМАД (community policing)

У процесі щоденної поліцейської діяльності, спрямованої на вирішення широкого спектру проблемних питань виконання своїх завдань з протидії та запобігання злочинності правоохоронні органи у різних країнах використовують різні стратегічні підходи, які переважно базуються на досвіді керівників, і є недостатньо науково обґрунтованими. Це значно ускладнює процес досягнення мети стабільного підтримання позитивного стану криміногенної ситуації. Вчений О. Гуменюк стверджує, що одним із основних інструментів стратегічного управління, з допомогою якого керівники та управлінці оцінюють у комплексі внутрішні і зовнішні чинники функціонування органу, підрозділу чи організації є SWOT-аналіз [1, с. 282-283]. SWOT-аналіз це організаційна стратегія, яка була розроблена Альбертом Хамфрі (Albeit S. Humphrey) в 1960-х роках, визнаного спеціаліста з ділового управління.

Назва цього методу походить від перших літер сфери чинників, які підпадають під аналіз. Strengths (S – сильні сторони) Weaknesses (W – слабі сторони) Opportunities (O – можливості) та Threats (T – загрози). SWOT-аналіз – це групування факторів середовища функціонування організації на зовнішні та внутрішні, їх аналіз із позиції визначення позитивного чи негативного впливу на діяльність цієї організації [2].

На етапі виникнення SWOT-аналіз був заснований на визначенні та структуризації знань про поточну ситуацію і наявні тенденції, проте згодом став використовуватися в ширшому значенні – для розробки та формулювання управлінських стратегій.

SWOT-аналіз – це метод, за допомогою якого можна зрозуміти сильні та слабкі сторони у організації діяльності, а також можна зрозуміти можливості й загрози, з якими стикаються підрозділи поліції, кожен з яких працює в індивідуальних умовах з індивідуальними можливостями в окремих громадах, яким властива індивідуальна криміногенна картина. SWOT-аналіз – це фактично фундаментальна, проста модель, яка аналізує те, що може

зробити підрозділ поліції, а що не може, а також імовірні можливості та загрози, які можуть мати місце в поточній та майбутній криміногенній ситуації. Техніка SWOT-аналізу завжди полягає в тому, щоб проаналізувати внутрішні умови – сильні та слабкі сторони підрозділу поліції, а також зовнішні елементи діяльності поліції – це можливості та загрози. Проведення SWOT-аналізу не займає багато часу, проте дає змогу роздивитися свою організацію з нової точки зору. SWOT-аналіз – це структурований звіт про поточні основні сильні сторони, слабкі місця, можливості та загрози. Проведений кримінальними аналітикам SWOT допомагає визначити, що може посприяти поліції у досягненні її цілей в окремих громадах, а також які обмеження потрібно подолати або, можливо, зменшити для досягнення очікуваних результатів.

Сильні сторони є внутрішніми чинниками, і здебільшого правоохоронна організація має повний контроль над ними. Сильні сторони – це унікальні навички та компетенції, які є важливими та цінними. Слабкі сторони слід позиціонувати як внутрішні фактори, якими може керувати правоохоронний орган чи підрозділ, і це найважливіші моменти, які заважають організації працювати краще в плані досягнення стратегічних цілей та завдань. Можливості – це зовнішні фактори, які орган чи підрозділ не контролює, або контролює частково, проте вони сприятливі для органу чи підрозділу поліції. Поточні тенденції та зміни можуть суттєво вплинути на орган чи підрозділ, і потрібно визначити ці сили та розробити план дій, як скористатися цими можливостями. Загрози – це також зовнішні сили, які зазвичай неможливо контролювати. Загрози бувають різними: технологічні, політичні, економічні, демографічні тощо. Як правило, загрози повністю усунути не вдасться, проте слід розробляти стратегію і тактику, щоб мінімізувати ризик, або максимально уникнути загроз.

Методо SWOT-аналізу особливо цінний під час реалізації моделі діяльності Community policing, оскільки дозволяє індивідуально до кожної громади визначити: яких загроз потрібно уникати; які шанси треба використати; які слабкі сторони необхідно виправити та на які сильні сторони слід опертися?

Розробляючи рекомендації під час реалізації моделі Community policing потрібно сконцентруватись на: 1. посилення міцності; 2. захисті слабких сторін; 3. використанні можливостей; 4. нейтралізації загроз [3, с. 208-213].

Основна ідея застосування SWOT-аналізу може бути визначена для реалізації моделі Community policing таким чином:

- розробка комплексу заходів по перетворенню слабкості в силу і загрозу в можливості;
- укріплення та розвиток сильних сторін фірми з урахуванням її обмежених можливостей;
- повне використання всіх переваг, виявлених на основі аналізу навколишнього середовища.

Проведення SWOT-аналізу створює передумови розроблення окремих

стратегій діяльності, зокрема:

1) підтримка та розвиток сильних сторін правоохоронного органу використовуючи можливостей зовнішнього середовища;

2) боротьба із загрозами використовуючи внутрішній потенціал;

3) використання можливостей для нейтралізації слабких сторін;

4) зміцнення правоохоронного органу та нейтралізація потенційних загроз від зовнішнього середовища [4, с. 221].

Застосування методології SWOT-аналізу для ідентифікації, вивчення, розробки заходів з обмеження впливу проблем на стан криміногенної ситуації дозволяє ефективно та якісно, з обмеженим застосуванням правоохоронних ресурсів досягати максимального результату при нейтралізації першопричин проблем у сфері забезпечення правопорядку, а також дієво послаблювати вплив існуючих проблем з метою більш ефективного виконання покладених на правоохоронні органи завдань [5, с. 187].

---

1. Гуменюк О. Г. Використання SWOT-аналізу як основного інструменту стратегічного управління. Миколаївський національний університет імені В.О. Сухомлинського. Глобальні та національні проблеми економіки. 2017. Вип. 17. С. 281–285.

2. Балабанова Л. В., Сардак О. В. Управління персоналом : навч. посіб. Донецьк : ДонДУЕТ, 2006. 471 с.

3. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

4. Балабанова Л. В. SWOT-аналіз – основа формування маркетингових стратегій : навч. посіб. 2-ге вид., випр. і доп. Київ : Знання, 2005. 301 с.

5. Федчак І. А. Практичні аспекти вирішення проблем через використання методології “Трикутник злочинності” та методології SWOT-аналізу під час реалізації моделі здійснення правоохоронної діяльності, орієнтованої на потреби громад (Community Policing). Дніпровський науковий часопис публічного управління, психології, права. 2023. Вип. 3. С. 183–187. URL : DOI https://doi.org/10.51547/ppp.dp.ua/2023.3.30 (дата звернення: 30.08.2023).

ЛИСЮК Ярослав
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри інформаційних
та комунікативних технологій
Дніпропетровського державного
університету внутрішніх справ

ГЕНДЕРНА НЕРІВНІСТЬ НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ СУСПІЛЬСТВА

Вперше термін гендерна нерівність виник у 1980 році, завдяки появі поняття гендер, як основи феміністської концепції (Джейн Скотт). Гендерну нерівність можна визначити як одну з характеристик громадського устрою, згідно з якою диференційовані соціальні групи (жінки та чоловіки) мають стійкі відмінності, які виникли через нерівні можливості в суспільстві.

Для більшого розуміння необхідно визначитись, що таке гендерна рівність. Гендерна рівність – це рівність у реалізації прав людини незалежно від її статі у будь-якій сфері суспільного життя. Правовий принцип рівності означає відсутність будь-якої нерівності чи обмежень у реалізації своїх прав та свобод у будь-якій сфері. Але нажаль і на теперішній час незважаючи на певний прогрес у сфері подолання гендерної нерівності вона так чи інакше має свої прояви у кожному суспільстві [1].

Традиційна модель суспільства визнає, що жіноча та чоловіча моделі поведінки не схожі, так наприклад, поведінці чоловіка властиві такі риси як: рішучість, активність, агресивність, розважливість, лідерство, а жінці властиві пасивність, залежна поведінка, емоційність, творче мислення. Але с розвитком сучасності та з плином часу загальноприйнята модель набуває зовсім іншого характеру. Деякі риси, властиві чоловікам, переймають жінки і навпаки. З часом гендерні ролі мають властивість змінюватись й різнитися в контексті конкретних культур та верств. Гендерні ролі можуть варіюватися залежно від статусу, класу, етнічної групи, неплатоспроможності, віку або інших чинників. Оскільки гендер є соціальним явищем, він набуває значущості в процесі модифікації ознак, притаманних політиці певної держави [3].

Гендерна нерівність - складна і не вирішена проблема, тому що ця вона бере свій початок в далекому минулому, завдяки стереотипному мисленню наших пращурів. Часто визначення біологічного та соціального гендеру не відрізняють один від одного. Дискримінація за статевими відмінностями,

супроводжується дискримінацією за віком, рівнем освіти, національністю.

Ступінь та причини виникнення гендерної нерівності обумовлені такими факторами [2]:

1. Чинником розвитку соціуму (демографічного, технологічного, соціально-економічного);

2. Фактором гендерного порядку (дискримінаційним фактором);

3. Поведінковим фактором.

Наразі, світові організації прагнуть створити якомога кращі умови життя для людей, вирішити глобальні суспільні проблеми, а також позбавитися від будь-яких проявів нерівності: гендерної, расової, етнічної, релігійної. Викорінення гендерної нерівності – це елементарна умова соціальної справедливості, яка забезпечить розвиток демократичних відносин, а також сталий економічний розвиток країни.

Як висновок, ми можемо зауважити, що нерівність гальмує розвиток суспільства, вона впливає на економічні, політичні, технологічні та багато інших сфер розвитку соціуму. Тому проблема, гендерної нерівності у сучасності, є важливою проблемою, вирішення якої потребує багато зусиль та часу.

---

1. Крочук М. І. Гендерна рівність як складова загального принципу рівності. Науковий вісник. 2011. №4. С. 464 – 471

2. Смачило В.В., Дюжова Т.О. Гендерна рівність та її вплив на розвиток громадянського суспільства. Молодий вчений. 2018. №5.1. С.62-67.

3. Німець О. Гендерна рівність та ii розвиток в історичному аспекті / О. Німець, О.Нагорна // Роль національного права України в умовах глобалізаційних викликів : матеріали Всеукр. наук.-практ. онлайн-конф. (м. Дніпро, 18 листопада 2021 р.). - Дніпро : ДДУВС, 2021. – С. 60-63

ТКАЧЕНКО Дар'я
курсант 3-го курсу ННІ права
та підготовки фахівців для підрозділів
Національної поліції
Науковий керівник:
ВАРАВА Володимир
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ СТРАТЕГІЧНИХ РОЗСЛІДУВАНЬ ЩОДО ЗАХИСТУ ЕКОНОМІКИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ

Забезпечення економічної та фінансової безпеки, соціально-економічного добробуту, попередження можливих загроз в економіці, виявлення існуючих ризиків, викриття осіб причетних до дестабілізації економічної ситуації в нашій державі – все це лиш невеликий перелік завдань, що виконуються працівниками Департаменту стратегічних розслідувань (далі – ДСР) Національної поліції України. Визначальним документом у діяльності ДСР НП України є Стратегія боротьби з організованою злочинністю (далі – Стратегія), схвалена розпорядженням Кабінету Міністрів України від 16 вересня 2020 року № 1126-р, якою визначено напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики у відповідній сфері в сучасних умовах [1, с. 17].

Зосередження уваги на виявленні, ліквідації кримінальних мереж, відстеженні грошових потоків і поверненні активів, одержаних від корупційних та інших злочинів [2] – є одним із керівних принципів реалізації Стратегії, виконання завдань з метою реалізації зазначених положень покладено на підрозділи ДСР. Виконання таких завдань потребує не лише високого рівню професіоналізму відповідних працівників ДСР, компетентності та кваліфікованості, а й належного рівня матеріально-технічного забезпечення, оперативного ресурсу, агентурного апарату, спеціальних технічних засобів та інформаційно-аналітичного забезпечення у відповідності до вимог сьогодення, враховуючи тенденції програмного та технічного прогресу.

Для вирішення завдань боротьби з організованою злочинністю підрозділи Служби безпеки України та підрозділи органів Національної поліції мають право збирати, накопичувати і зберігати інформацію про події і

факти, що свідчать про організовану злочинну діяльність, її причини та умови, про осіб, які беруть участь в організованій злочинній діяльності [3]. Зазначені положення Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» зумовлюють потребу формування відповідними підрозділами ДСР, що здійснюють протидію злочинності у сфері господарської діяльності та фінансово-економічному блоці, обліків, підсистем, систем, аналітичних зведень та статистичних показників, результатів розвідки з відкритих інтернет-джерел, які містять в собі інформацію, що може свідчити про стан та наявні економічні загрози.

Р. Коваль переконаний, що під інформаційно-аналітичним забезпеченням розуміється «процес створення оптимальних умов задля задоволення інформаційних потреб та реалізації посадових обов'язків органів державної влади на основі формування та використання інформаційних ресурсів» [4].

Інформаційно-аналітична та інформаційна пошукова діяльність – важливий напрям роботи структурних підрозділів ДСР, необхідність у своєчасному виявленні потенційних загроз, існуючих ризиків та факторів, що є своєрідним каталізатором процесів, які являють собою небезпеку для стану захищеності економіки нашої держави.

Формування статистично-аналітичних блоків (зведень), щодо поточного стану та рівня економічної злочинності, протиправних діянь у сфері службової діяльності, вчинення яких може слугувати наслідком у вигляді створення загрози економічній безпеці держав, кримінальних правопорушень у сфері господарської діяльності – має здійснюватися у синергії з відповідними підрозділами органів досудового розслідування, якими мають надаватись відповідні дані щодо зареєстрованих кримінальних проваджень, їх стану, повідомленим підозрам, встановлених досудовим розслідуванням обсягів завданих збитків, варіативністю організованості зазначеної злочинності (організовані групи, злочинні організації, злочинні спільноти). Зазначена взаємодія може надати можливість здійснювати якісні інформаційно-аналітичні дослідження з метою встановлення передумов, причин та наслідків вчинення зазначених кримінально-протиправних дій. Виходячи з аналізу вже існуючої злочинності, використовуючи інформаційно-аналітичний ресурс, підрозділами ДСР має здійснюватися діяльність з дослідження наявних ризиків у вигляді існування схожих передумов у відповідних регіонах, у якій здійснює свою діяльність певний підрозділ стратегічних розслідувань, метою такого аналізу має бути – встановлення подібних фактів здійснення суспільно небезпечної діяльності, що загрожує економіці держави та викриття осіб причетних до її здійснення.

Отже, економічна безпека держави, що перебуває у стані повномасштабної війни – це запорука не лише належного рівня функціонування державних інституцій та забезпечення потреб населення держави, а й один із фундаментальних показників обороноздатності держави,

можливості забезпечення Сил безпеки й оборони матеріальним ресурсом, який необхідний для оборони та забезпечення територіальної цілісності держави. Стан захищеності вітчизняної економіки – це відповідальність уповноважених правоохоронних підрозділів, завданням яких є забезпечення економічної безпеки держави, авангардним, на нашу думку, підрозділом, що здійснює таку діяльність є ДСР Національної поліції, а для належного функціонування зазначеного підрозділу особливо важливим у час новітніх технологій є його інформаційно-аналітичне забезпечення як запорука стану захищеності фінансово-економічного блоку.

1. Нормативно-правове забезпечення діяльності підрозділів стратегічних розслідувань: метод. рек. / уклад. : Д. Б. Санакоєв, О. В. Неклеса, В. В. Єфімов, Д. С. Юр'єв. Дніпро : ДДУВС, 2021. 84 с.

2. Про схвалення Стратегії боротьби з організованою злочинністю : Розпорядж. Каб. Міністрів України від 16.09.2020 р. № 1126-р. URL : https://zakon.rada.gov.ua/laws/show/1126-2020-р#Text (дата звернення: 22.10.2023).

3. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30.06.1993 р. № 3341-XII : станом на 31 берез. 2023 р. URL : https://zakon.rada.gov.ua/laws/show/3341-12#Text (дата звернення: 23.10.2023).

4. Коваль Р.А. Інформаційно-аналітичне забезпечення діяльності органів державної влади. Теорія та практика державного управління. 2006. № 1(113).

УСТИМЕНКО Владислава
курсантка 3-го курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
ТЕЛІЙЧУК Віталій
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ЕКОНОМІЧНА СТІЙКІСТЬ ПІД ЧАС ВІЙНИ: РОЛЬ КОНТРРОЗВІДУВАЛЬНИХ ОПЕРАЦІЙ

Широкомасштабна війна, спровокована Російською Федерацією, чинить фундаментальний негативний вплив на економічну безпеку України. Економічна безпека – це стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі і характеризує здатність національної економіки до сталого та збалансованого

зростання.

За визначенням, яке пропонується в довіднику ООН, стійкість означає здатність системи, суспільства або громади, які піддаються ризикам, ефективно та своєчасно протистояти їм, поглинати, адаптуватися та відновлюватися після їхніх наслідків, включаючи збереження та відновлення основних структур і функцій [1, с. 24]. Під час війни економічна стійкість вкрай важлива, і контррозвідувальні операції можуть відігравати ключову роль у забезпеченні її. Контррозвідка допомагає виявляти та припиняти економічні загрози, такі як: шпигунство, кібератаки, саботаж і контрабанду. Вона також допомагає захищати важливі господарські об'єкти та забезпечувати безпеку постачання ресурсів. Збереження економічної стійкості під час війни може мати велике значення для успішного ведення конфлікту та подальшого відновлення країни після нього [2, с. 9]. Як зазначено у статті 1 Закону України «Про контррозвідувальну діяльність» контррозвідувальна діяльність це спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України.

Структурна організація контррозвідувальної діяльності як вияв методологічної основи є системою ідей, поглядів, цілеспрямувань на діяльність контррозвідки з метою убезпечення особистості, держави та суспільства від протиправної діяльності спеціальних служб іноземних держав, окремих організацій, груп та осіб, що пов'язані з ними в інформаційній сфері життєдіяльності суспільства. Така здатність системи контррозвідки як суспільних відносин є забезпеченням оптимального функціонування її інститутів у суспільстві країни і за його межами у вирішенні життєво-важливих інтересів.

У концептуальній конструкції контррозвідувальної системи відповідно до визначених напрямів варто закласти такі елементи як: конституційні, соціально-політичні, основні, спеціальні, оперативно-тактичні та організаційні. При цьому, акцентуємо увагу на структурну організацію, яка визначається діяльністю органу, що спрямована на досягнення результату, визначеного його основним функціональним завданням; структура органу відповідає характеру його діяльності та грунтується на направленості на конкретні об'єкти; елементи цієї структури можуть об'єднуватися для створення підрозділів за принципом подібності об'єктів діяльності та методів і засобів, що зокрема використовуються. Підпорядкованість і взаємодія елементів у контррозвідувальній системі забезпечується як результат діяльності кожного з них, що є керуючою інформацією для структурних елементів наступного рівня ієрархії (знизу – вгору і навпаки).

Законодавець у ст. 1 Закону України «Про оперативно- розшукову діяльність» визначив, що завданням оперативно- розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [3]. Контррозвідувальні заходи вживають оперативні підрозділи в межах визначеної чинним законодавством компетенції зокрема, оперативні підрозділи Служби безпеки України. У системі Національної поліції України, зазвичай, ці заходи здійснюються підрозділами внутрішньої безпеки з метою попередження, виявлення та припинення будь-яких форм протидії організованих груп чи злочинних організацій оперативним підрозділам, а також виявлення корумпованих працівників Національної поліції [4]. Одним із основних завдань контррозвідки є припинення економічних злочинів і запобігання їх подальшому розвитку. Це може включати в себе затримання злочинців, конфіскацію майна, що було отримане злочинним шляхом, та надання підтримки у проведенні судових розглядів. Контррозвідувальні служби здійснюють збір інформації про підозрюваних осіб, компанії та організації, які можуть бути причетні до економічних злочинів. Ця інформація може бути зібрана з відкритих джерел, свідчень свідків або з інших джерел [5, с. 102].

Отже, вважаємо, що економічна безпека – це стан, за якого економічні інтереси, ресурси і інфраструктура країни захищені від ризиків, загроз і небезпек, що можуть спричинити збитки або загрозу стійкості економіки. Тому контррозвідувальна діяльність є важливою складовою боротьби з економічними злочинами. Основним завданням контррозвідки у цьому контексті є виявлення та припинення діяльності осіб або груп, що здійснюють економічні злочини, такі як корупція, відмивання грошей, шахрайство, викрадення комерційної інформації та інші.

1. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с

2. Економічна безпека держави: навчально-методичний посібник / Живко З.Б., Черевко О.В., Копитко М.І., Зачосова Н.В., Живко М.О., Середа В.В., Занора В.О., Бієвець А.В.; за ред. Живко З.Б. Черкаси : видавець Чабаненко Ю.А., 2019. 240 с.

3. Про оперативно-розшукову діяльність: Закон України від 18.02.1992. № 2136-XII. Відомості Верховної Ради України (ВВР), № 22, ст.304. URL : https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення 24.10.2023)

4. Про контррозвідувальну діяльність: Закон України від 03.04.2003. № 662-IV. Відомості Верховної Ради України (ВВР), 2003, № 12, ст.89. URL : https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення 24.10.2023)

5. Лісовський П. М., Подоляка С. А., ЛісовськаЮ. П. Спецслужби держав світу: ентропія, балістика, логістика : навчальний посібник. Київ : Видавничий дім «Кондор», 2019. 212 с.

ЦУРАНОВ М.В.
старший викладач кафедри
кібербезпеки та DATA-технологій
факультету №6 Харківського
національного університету
внутрішніх справ

ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЙНИХ МЕТОДІВ БОРОТЬБИ З ФІШИНГОВИМИ АТАКАМИ

У зв'язку з військовими діями, значна кількість користувачів мережі Інтернет перейшла на режим дистанційної роботи. Навантаження на сервери істотно зросло, через те що, більшість користувачів почали робити звичайні речі за допомогою мережі Інтернет, (відвідувати онлайн кінотеатри замість звичайних, купувати продукти харчуванні та інше). Цим скористалися Інтернет шахраї, що призвело до збільшення кількісті випадків витоку конфіденційної інформації за допомогою фішинг атак. Тема протидії фішинговим атакам ненова, але її не можливо вирішити раз і назавжди, оскільки з кожним місяцем йде адаптація під сучасні тренди інформаційно-телекомунікаційних мереж. Спираючись на статистику антивірусних рішень, слід зазначити, що в першому кварталі 2021 року, лише одна з систем протидії фішингових атак , а саме SecureList, запобігла близько 79 608 185 спроб несанкціонованого доступу [1].

Фішинг являє собою атаку, яку порушник здійснює через сучасні месенджери, e-mail листи та соціальні мережі, аби спонукати потенційну жертву до розголошення певної конфіденційної інформації під приводом її «перевірки». Наразі є спеціальні інструменти для автоматизованого створення фішингових сторінок, які схожі на реальний ресурс, але всі дані, введені користувачем, – передаються зловмиснику.

Фішингова атак не потребує наявності глибоких технічних знань. Реалізація успішної атаки залежить від комунікаційних навиків зловмисника та від його вміння аналізувати останні новини. Вразливим об'єктом найзахищеної системи – є людський розум. Таким чином фішинг стоїть поряд з соціальною інженерією. За звичай саме від довірливості працівника, залежить конфіденційність, цілісність та доступність навіть об'єктів критичної інфраструктури. Власне потужним інструментом зловмисника – є гра на людських вадах, що реалізується за допомогою навиків соціальної інженерії.

Існує два види фішинга: цільовий та безадресний. Під безадресним розуміється, масова атака, направлена на залучення якомога більше людей. Сучасні антивіруси вже навчилися розпізнавати більшість таких атак, тому 95% шкідливих листів знищується ще до моменту відкриття листа жертвою

[2]. Однак, наразі при цільовій атаці, жоден сканер не зможе зі значною вірогідністю розпізнати фішинг. На відміну від безадресової атаки, для цільової атаки зловмисник проводить OSINT-розвідку, використовує реальні сторінки соціальних мереж, надсилає повідомлення зі шкідливими посиланнями в залежності від вподобань жертви. В України є декілька популярних ресурсів, в яких зловмисники шукають жертв, більшість з них пов'язанні з сайтами продажу. Прикладом є веб-додаток для продажу речей olx. Зловмисник починає розмову з жертвою, та намагається перенести спілкування з нею у месенджер. Після чого розповсюджує фейкову сторінку з оплатою під виглядом olx, звісно усі дані та грошовий переказ йде на пряму зловмиснику.

Відповідно до спільного звіту дослідницької фірми Cyentia Institute та компанії Elevate Security, традиційні методи підвищення безпеки, такі як навчання та імітація фішингу, слабко впливають на реальну захищеність співробітників від кібератак [2]. Так відбувається, тому що користувач не заохочений на проходження даних курсів. Проводити мотивацію працівника необхідно здалеку. Пояснити працівникам, що таке ІБ і чому це так важливо в 21 столітті. Одним із переконливих аргументів для проходження курсу є підтримка конфіденційності персональних даних самого працівника, оскільки тренінги допоможуть йому захистити не тільки корпоративні дані, але й особисті.

Також, заздалегідь необхідно продумати інтеграцію з вже існуючим державним порталом навчанням, а саме «Цифрова Освіта», який був розроблений командою Дії за підтримки Міністерства Цифрової Трансформації України [3].

Важливим фактором мотивації розвитку даної тематики, є навчання громадян розпізнавати дезінформацію в період війни.

Важливо розглянути вразливості українських користувачів мережі Інтернет. Користуючись важким положенням України в момент Російської агресії, слід зазначити, що істотна кількість зловмисників залишаються безкарними при атаці на громадян України. При проведені розслідувань як приватних детективів, так і державним департаментом кіберполіції, виявляється, що більшість атак відбувається зі сторони тимчасово непідконтрольної території, що унеможливлює пошук та покарання зловмисників. Тому наразі, в край важливо бути пильними при повсякденній роботі в мережі.

Основна цільова аудиторія представлених методів є, керівники відділу безпеки, власники компаній та представники державного сектору, які зацікавлені в нерозголошенні конфіденційної інформації. Аналізуючи роботу, керівник відділу безпеки або власник компанії, має змогу розглянути метод захисту від фішинг атаки та на основі представленого методу впровадити свій або існуючий тренінг з розпізнавання фішингу.

Низка новин по розкриттю конфіденційної інформації, мотивує на

розробку та впровадження представленого рішення. Однак, до розробки такого класу програмних засобів, необхідно підходити з повною відповідальністю, адже від якості освітніх процесів, буде залежати в тому числі інтереси України на міжнародній арені в сфері інформаційних технологій.

1. Спам и фишинг в I квартале 2021 года, SECURE LIST. URL : https://securelist.ru/spam-and-phishing-in-q1-2021/101270/ (дата звернення: 05.09.2023);
2. Verizon, Data Breach Investigations Report 2021. Verizon. ES2090521. 2021;
3. Цифрова освіта, Дія. URL : https://osvita.diia.gov.ua/ (дата звернення: 07.09.2023).

ЧОРНИЙ Данило
студент 3-го курсу
факультету № 2 КННІ
Донецького державного
університету внутрішніх справ
Науковий керівник:
ГРАНКІНА Валентина
доцент кафедри
кримінально-правових дисциплін
факультету № 2 КННІ Донецького
державного університету внутрішніх
справ, доктор філософії

ДО ПИТАННЯ НЕЦІЛЬОВОГО ВИКОРИСТАННЯ БЮДЖЕТНИХ КОШТІВ ПІД ЧАС ВОЄННОГО СТАНУ

Стале функціонування економіки держави у період воєнного стану має суспільну важливість для забезпечення життєвого рівня населення, військових потреб і ведення військових операцій, а також для забезпечення національної безпеки. Тому вкрай необхідно використовувати кошти державного бюджету за призначенням, оскільки вірно розподілені бюджетні кошти – запорука нормального та стабільного функціонування всього суспільства.

У контексті проведення дослідження, вважаємо за доцільне розглянути поняття бюджетних коштів та нецільового використання бюджетних коштів. До бюджетних коштів належать кошти, що включаються до державного бюджету і місцевих бюджетів незалежно від джерела їх формування [3, с.117]. Нецільовим використанням бюджетних коштів, відповідно дост.119 Бюджетного кодексу України, є їх витрачання на цілі, що не відповідають:

– бюджетним призначенням, встановленим законом про Державний бюджет України (рішенням про місцевий бюджет);

– напрямам використання бюджетних коштів, визначеним у паспорті бюджетної програми або в порядку використання бюджетних коштів (включаючи порядок та умови надання субвенцій);

– бюджетним асигнуванням (розпису бюджету, кошторису, плану використання бюджетних коштів) [1].

Суспільна небезпечність нецільового використання бюджетних коштів, здійснення видатків бюджету чи надання кредитів з бюджету без встановлених бюджетних призначень або з їх перевищенням полягає в тому, що внаслідок вчинення таких діянь безпідставно знижується рівень фінансування суспільних потреб. Як наслідок, не забезпечуються на належному рівні бюджетне фінансування обороноздатності, внутрішньої безпеки, охорони здоров'я, освіти, культури тощо [5, с.298].

Контроль за витрачанням бюджетних коштів здійснюють Контрольно-ревізійна служба, Рахункова палата, а також фінансові управління та відділи. Практика перевірок контрольно-ревізійними органами говорить про системність та повторюваність бюджетних правопорушень, а результати проведених контрольних заходів засвідчують продовження негативної практики незаконного та нецільового використання бюджетних коштів [2]. Така практика незаконного та нецільового використання бюджетних коштів не зменшилась навіть під час повномасштабного російського вторгнення в Україну. Яскравим прикладом нецільового використання бюджетних коштів, на нашу думку, є закупівля музичних інструментів для психологічного розвантаження дітей в укриттях під час повітряних тривог [4].

За нецільове використання бюджетних коштів ст. 210 Кримінального кодексу України, передбачено відповідальність [3, с.117]. На нашу думку, суспільна небезпечність таких дій істотно підвищується в умовах воєнного або надзвичайного стану. Зогляду на вищевикладене, вважаємо за доцільне пропонувати внесеннязмін до кримінальногозаконодавства:

– диспозицію частини другої статті 210 КК України доповнити та викласти у наступній редакції: «Ті самі діяння, предметом яких були бюджетні кошти в особливо великих розмірах або вчинені повторно, або за попередньою змовою групою осібабо вчинені в умовах воєнного або надзвичайного стану, або щодо коштів виділених на посилення цивільного захисту або посилення обороноздатності України»

Запропоновані зміни до Кримінального кодексу України є запорукою більш чіткої кваліфікації кримінальних правопорушень проти зловживань у сфері господарської діяльності та визначення справедливого покарання за делікти,що є особливо актуальним у період надзвичайного та воєнного стану.Оскільки під час дії правового режиму воєнного стану та надзвичайного режиму всі зусилля держави спрямовані на підтримку на достатньому рівні обороноздатності та забезпеченні основних потреб населення, то нецільове використання бюджетних коштів у ці періоди набуває більшої суспільної небезпеки.

1. Бюджетний кодекс України : Закон України від 08.07.2010 № 2456-VI URL : https://zakon.rada.gov.ua/laws/show/2456-17#n1797 (дата звернення: 08.10.2023)

2. Здирко Н.Г. Контроль за використанням бюджетних коштів в Україні. URL : http://repository.vsau.org/getfile.php/1921.pdf (дата звернення: 08.10.2023)

3. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.

4. Музичні інструменти для психологічного розвантаження дітей в укриттях під час повітряних тривог. Електронна система публічних закупівельProzorro. URL : https://prozorro.gov.ua/tender/UA-2023-04-20-004546-a (дата звернення: 08.10.2023)

5. Кримінальний кодекс України. Науково-практичний коментар: за заг. ред.Тація В.Я, Пшонки В. П., Борисова В. І., Тютюгіна В. І. 5-те вид., допов. Харків : Право, 2013.1040 с.

ШУВАЛОВ Владислав
курсант 4 курсу
КОЛІСНИК Тетяна
доцент кафедри протидії
кіберзлочинності Харківського
національного університету
внутрішніх справ,
кандидат педагогічних наук, доцент

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ: ПРОГРАМИ ВИМАГАЧІ

У сучасному світі інформаційних технологій та цифрового зв'язку одним з найбільш руйнівних та небезпечних видів кіберзагроз є атаки, пов'язані з використанням шкідливого програмного забезпечення, відомого як «ransomware». Цей вид кіберзлочинності не тільки вражає індивідуальних користувачів, а й становить серйозну загрозу для організацій, урядів та навіть критичної інфраструктури.

Програма вимагач – це різновид шкідливого програмного забезпечення, що зашифровує файлову систему користувача та вимагає викуп за дешифрування даних, зазвичай у криптовалюті. Перша відома в світі атака програмою вимагачем, «троян СНІД», написаний Джозефом Поппом у 1989 році, мала такий серйозний провал, що платити здирникові взагалі не довелося. Його пейлоад приховував файли на жорсткому диску та шифрував лише їхні імена, а також відображав повідомлення про те, що термін дії ліцензії користувача на використання певного програмного забезпечення закінчився. Але на теперішній час програми вимагачі стали набагато складнішими. Та більш скритними. Деякі програми-вимагачі використовують проксі-сервери, прив'язані до прихованих служб Tor, для підключення до

своїх командних і контрольних серверів, що ускладнює відстеження точного місцезнаходження зловмисників. Корпорація Symantec класифікувала програми-вимагачі як найнебезпечнішу кіберзагрозу [2].

Атаки програм-вимагачів зросли більш ніж на 37% у 2023 році, а середня сума викупу підприємства перевищила 100 000 доларів США при середньому попиті в розмірі 5,3 мільйона доларів США. 2023 рік став свідком кількох резонансних інцидентів, які розкрили конфіденційні дані та спричинили збої в різних галузях [1]. Наприклад Reddit, відомий технічний дискусійний форум, став однією з жертв порушення безпеки. Було здійснено несанкціонований доступ до корпоративних документів, програмних кодів і метаданих, відповідальність за які взяла на себе група BlackCat Ransomware, також відома як Alphv. Хакери вимагали чималий викуп у розмірі 4,5 мільйона доларів США за ключ дешифрування після отримання доступу та викрадення близько 80 ГБ конфіденційних даних [3].

Рівень небезпеки певних програм вимагачів може змінюватися з часом у міру нових варіантів експлуатації цільової системи і нових загроз.

Найпопулярніші програми вимагачі, які були особливо небезпечними та помітними в минулому:

• WannaCry (також відомий як WannaCrypt): WannaCry привернув увагу всього світу в травні 2017 року завдяки швидкому та широкому зараженню комп'ютерів. Він націлений на вразливості в Microsoft Windows для проникнення у систему та шифрування усієї файлової системи, вимагаючи викуп за її дешифрування [4].

• NotPetya (ExPetr, Petya та інші): NotPetya, що вперше з'явився у 2016 році, поширювався через скомпрометовані оновлення програмного забезпечення. Його основною метою було знищення файлів, і він завдав широкомасштабної шкоди комп'ютерним системам в Україні та за її межами [5].

• Ryuk відомий тим, що націлений на організації в сфері охорони здоров'я та фінансах. Він шифрує файли та вимагає значні викупи. Ryuk поширювався через фішингові електронні листи [6].

• DarkTequila – програма була відкрита в 2018 році і в основному націлена на користувачів у Мексиці. Вона використовувала комбінацію методів фішингу для викрадення фінансової інформації та облікових даних [7].

---

1. 2023 ThreatLabz State of Ransomware Report | Zscaler. Cybersecurity and Zero Trust Leader | Zscaler. URL : https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report#:~:text=Thanks!&text=Ransomware%20attacks%20increased%20by%20over,the%20world's%20largest%20security%20cloud. (date of access: 16.10.2023).
2. Contributors to Wikimedia projects. Ransomware - Wikipedia. Wikipedia, the free encyclopedia. URL : https://en.wikipedia.org/wiki/Ransomware#:~:text=Ransomware%20is%20a%20type%20of,unle

ss%20a%20ransom%20is%20paid. (date of access: 16.10.2023).

3. Top 10 Ransomware Attacks in 2023 - Cybersecurity Insiders. Cybersecurity Insiders. URL : https://www.cybersecurity-insiders.com/top-10-ransomware-attacks-in-2023-so-far/ (date of access: 16.10.2023).

4. Учасники проектів Вікімедіа. WannaCry – Вікіпедія. Вікіпедія. URL : https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 16.10.2023).

5. Учасники проектів Вікімедіа. Petya – Вікіпедія. Вікіпедія. URL : https://uk.wikipedia.org/wiki/Petya (дата звернення: 16.10.2023).

6. Contributors to Wikimedia projects. Ryuk (ransomware) - Wikipedia. Wikipedia, the free encyclopedia. URL : https://en.wikipedia.org/wiki/Ryuk_(ransomware) (date of access: 16.10.2023).

7. Dark Tequila Añejo. Securelist | Kaspersky's threat research and reports. URL : https://securelist.com/dark-tequila-anejo/87528/#:~:text=Dark%20Tequila%20is%20a%20complex,storage%20accounts%20and%20domain%20registrars. (date of access: 16.10.2023).

ПИРІГ Ігор
доктор юридичних наук, професор,
професор кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

НАПРЯМКИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-ДОВІДКОВОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Розслідування кримінальних правопорушень є специфічним видом діяльності суб'єктів, які його проводять, що полягає у збиранні, дослідженні, оцінці та використанні доказів з метою вирішення завдань кримінального провадження. У свою чергу, доказами є фактичні дані, отримані у встановленому порядку, тобто інформація щодо події кримінального правопорушення, осіб, причетних до нього, мети та мотивів вчинення злочину та інших обставини, що підлягають доказуванню. Тобто, процес розслідування є ні чим іншим, як діяльністю з отримання доказової інформації, від кількості та якості якої залежить кінцевий результат. Інформаційно-довідкове забезпечення розслідування злочинів є діяльністю суб'єктів розслідування, спрямована на пошук та одержання, а в необхідних випадках оновлення та коригування інформації, яка міститься в інформаційних системах незалежно від їх відомчої належності, з метою використання її в процесі розслідування злочинів [1, с. 390].

Основу інформаційно-довідкового забезпечення розслідування складають криміналістичні обліки, що являють собою засновану на наукових даних та узагальненні практики протидії злочинності сукупність

інформаційних та інформаційно-пошукових систем, які складаються з об'єктів або відомостей про них, що створені, функціонують та використовуються суб'єктами розслідування кримінальних правопорушень для вирішення завдань кримінального провадження [2, с. 7]. Загальноприйнятим є поділення криміналістичних обліків за призначенням на інформаційно-довідкового, що знаходяться у Департаменті інформаційно-аналітичної підтримки Національної поліції України та оперативно-розшукового, зосередженого в Експертній службі МВС України [3, с. 359]. Організація формування та ведення криміналістичних обліків регламентується Наказом МВС України від 10.09.2009 № 390, що затверджує Інструкцію з організації функціонування криміналістичних обліків експертної служби МВС України [4].

Підрозділи Департаменту інформаційно-аналітичної підтримки Національної поліції України забезпечують функціонування криміналістичних обліків інформаційно-довідкового призначення. На сьогодні їх об'єднано в інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», що стала складовою частиною єдиної інформаційної системи МВС України. Означена система налічує більш ніж 40 різноманітних обліків, що використовуються як для розслідування кримінальних правопорушень, так і для забезпечення функціонування всієї системи Національної поліції України. Інформаційно-пошукові системи Департаменту інформаційно-аналітичної підтримки Національної поліції України останніми роками постійно вдосконалюються, додаються нові інформаційні системи, забезпечується нормативно-правове регулювання їх ведення та використання, що підвищує ефективність використання облікової інформації в ході розслідування злочинів.

На наш погляд, більшої уваги на сьогодні потрібно приділити формуванню та використанню оперативно-розшукових обліків. Саме ці обліки призначені для отримання інформації про особу, яка причетна до вчинення злочину та її ідентифікації; ідентифікації знаряддя вчинення злочину: транспортного засобу, зброї, обладнання тощо, що використовувалися під час учинення злочину; установлення спільної групової належності матеріалів та речовин; інших фактичних даних, що свідчать про вчинення злочинів конкретною особою; отримання іншої інформації щодо вчинених злочинів та запобігання їм. Обліки формуються з об'єктів (їх копій, зображень) та відомостей про них, вилучених під час огляду місця події чи при проведенні інших слідчих (розшукових) дій, а також отриманих під час реєстрації дактилокарт, фото-, відеозображень, записів голосів і мовлення осіб, ДНК-профілів тощо.

На сьогодні основним обліком оперативно-розшукового призначення є дактилоскопічний, що реалізується в автоматизованій інформаційно-пошуковій системі «Дакто-2000». Практика використання даного обліку свідчить, що на сьогодні його ефективність значно знизилась. Це пояснюється як об'єктивними причинами: обізнаністю злочинців та використанням ними гумових рукавичок при вчиненні злочинів, що зменшує

отримання дактилоскопічної інформації при оглядах місць події, так і суб'єктивними: застарілість програмного забезпечення, незважаючи на багаточисельні її модифікації.

У зв'язку з означеним вище, потрібно, на нашу думку, змінити підхід до формування оперативно-розшукових обліків впровадженням нових, заснованих на сучасних досягненнях науки і техніки. Такими, на нашу думку, на сьогодні є обліки геномної інформації людини та ознак її зовнішності.

У 2022 році було прийнято Закон України «Про державну реєстрацію геномної інформації людини», який визначив правові засади обробки геномної інформації людини з метою її державної реєстрації в Україні, що сформувало правові підстави формування та ведення Центрального обліку генетичних ознак людини (ЦОГОЛ), до якого вносяться дані ДНК-профілів, отриманих після проведення досліджень у стаціонарних лабораторіях експертних установ. Однією з переваг обліку генетичних ознак людини є можливість ідентифікації особи навіть при отримання невеликої кількості біологічного матеріалу, за умови дотримання вимог до збирання та дослідження біологічного матеріалу. Аналізом практики використання генетичних обліків встановлено, що вони допомагають не тільки у викритті злочинців, а й у відсіюванні осіб, які не причетні до вчинення злочинного діяння.

Актуальним під час збройної агресії росії стало питання забезпечення проведення молекулярно-генетичних досліджень для ідентифікації загиблих військових та цивільних осіб на деокупованій території, в тому числі з місць масових поховань. Стаціонарні лабораторії експертних установ, зважаючи на значну кількість таких досліджень, на сьогодні не в змозі в повному обсязі забезпечити їх проведення. На практиці позитивних результатів у цьому напряму набув пристрій «ANDE Rapid DNA», призначений для створення ДНК-ідентифікатора для швидкої ідентифікації людини (протягом 90-100 хвилин). Нещодавно такими пристроями було забезпечено всі обласні слідчі підрозділи поліції з техніко-криміналістичного забезпечення розслідування. Проблема формування бази даних ДНК профілів, що підлягає вирішенню, полягає у тому, що кожний пристрій ANDE має власну базу даних, яка не реєструються у Центральному обліку генетичних ознак людини.

Іншим, перспективним напрямком вдосконалення інформаційно-довідкового забезпечення розслідування є створення обліку, заснованого на фіксації та обробці ознак зовнішності людини, зокрема рис обличчя. На сьогодні існує достатня кількість програмного забезпечення розпізнання обличчя людини, що підтверджено практикою його застосування. Наприклад, прикордонники за допомогою американської програми розпізнавання обличчя «Clearview AI» змогли встановити особи понад 10 000 осіб, які брали участь у воєнних злочинах російської федерації [6]. Як система контролю співробітників підприємств та організацій зарекомендувала себе система розпізнавання обличчя «Visible Light», що має велику продуктивність і надійність та підходить як для загального застосування, так

і здатна розпізнавати людину у динамічному середовищі [7]. З наведеного зрозуміло, що на сьогодні технічні можливості дозволяють створити загальнонаціональну систему ідентифікації людини за ознаками зовнішності.

Визначені нами системи реєстрації не мають заміняти дактилоскопічний облік, а повинні доповнювати один одного, створюючи єдину систему реєстрації, засновану на обліку біометричних параметрів людини, про що неодноразово зазначалось науковцями.

1. Бирюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів : монографія. Луганськ : Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка, 2009. 664 с.

2. Приходько В. О. Теоретичні та практичні основи функціонування та використання криміналістичних обліків МВС України. Автор. на здобуття наукового ступеня канд. юрид. наук. 12.00.09. Нац. Наук. центр «Ін-т суд. експертиз ім. Засл. проф. М. С. Бокаріуса». Харків, 2021. 20 с.

3. Пиріг І.В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування : монографія. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. 432 с.

4. Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС України : Наказ МВС України від 10.09.2009 р. № 390. URL : https://zakon.rada.gov.ua/laws/show/z0963-09/conv**.**

5. Про державну реєстрацію геномної інформації людини. Закон України від 09.07.2022 № 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text

6. Clearview AI – система розпізнавання обличчя, яка допомагає прикордонникам виявляти людей, причетних до злочинів. URL : https://www.ukrinform.ua/rubric-technology/3694894-zavdaki-programi-rozpiznavanna-oblic-vstanovili-osobi-10-tisac-rosijskih-voennih-zlocinciv.html.

7. Система розпізнавання обличчя Visible Light. URL : https://zktecoua.com/ua/solutions/sistema-raspoznavaniya-lits-visible-light/

ВОЛІКОВ Тарас
кандидат юридичних наук,
докторант Дніпропетровського
державного університету
внутрішніх справ

ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ ОБЛІКІВ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ВЛАСНОСТІ

Використання різних видів криміналістичних обліків при розслідуванні кримінальних правопорушень залежить від завдань та етапів розслідування, а також слідчої ситуації, що склалася на певний момент. у зв’язку з

різноманітність криміналістичних обліків та їх функціональним призначенням у слідчих (дізнавачів) виникають питання щодо використання інформації, що міститься в них у конкретній слідчій ситуації. Криміналістикою не можливо передбачити кожну слідчу ситуацію та дії слідчого щодо її вирішення, але розробка рекомендацій щодо можливостей використання криміналістичних обліків у типових ситуаціях розслідування є перспективним напрямком підвищення результативності слідчої діяльності.

Під типовою слідчою ситуацією розуміють абстраговану штучна модель, що відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування [1, с. 111]. Інформація, що міститься у криміналістичних обліках використовується, в основному, на початковому етапі розслідування. У залежності від слідчої ситуації, використовується сукупність інформаційних даних, що містяться у базах даних як інформаційно-довідкового призначення, так і оперативно-розшукових обліках.

Розглянемо типові слідчі ситуації розслідування злочинів проти власності та можливість використання інформаційних баз даних для їх вирішення. У типовій слідчий ситуації, що є найбільш несприятливою для розслідування, а саме: є ознаки злочину (залишені матеріальні сліди, зникло майно), відсутні свідки та очевидці, особа злочинця невідома. Для вирішення основного завдання розслідування – встановлення особи злочинця у такій ситуації використовуються криміналістичні обліки залежно від виду слідів, виявлених на місці події. При виявленні слідів рук, вони перевіряються за дактилоскопічним обліком, а саме автоматизованою інформаційно-пошуковою системою «Дакто 2000». Якщо особа була раніше засуджена або затримана та її дактилокарта є у базі даних перевірка слідів, вилучених на місці події, дає позитивні результати. В залежності від вилучених при огляді місця події слідів, у цій ситуації, поряд з дактилоскопічним використовуються обліки слідів взуття, знарядь зламу та інструментів, транспортних засобів та ін. Всі означені сліди вносяться до інформаційної підсистеми «СЛІД» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі – ІПНП) та перевіряються за даними цієї системи. Облік у зазначеній системі ведеться за такими категоріями: фотозображення слідів рук; фотозображення слідів підошов взуття; фотозображення слідів знарядь зламу; фотозображення слідів структури матеріалу (рукавичок); фотозображення слідів протекторів шин транспортних засобів; мультимедійна інформація (фото-, відео-, звукозапис) щодо осіб, які причетні до вчинення кримінального правопорушення; мультимедійна інформація (фото-, відеозапис) обстановки події, що сталася; інформація про кулі, гільзи і патрони зі слідами зброї; інформація про об’єкти біологічного походження; інформація про інші вилучені матеріальні об’єкти, які були знаряддям вчинення кримінального правопорушення та зберегли на собі його сліди або містять інші відомості,

що можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [2].

Під час розслідування злочинів проти власності перевірка здійснюється майже по всіх зазначених категоріях. На наш погляд, недостатньо уваги приділяється слідам біологічного походження, особливо у процесі розслідування крадіжок і майнових злочинів, не пов'язаних із застосуванням насилля. Це пов'язано зі значною вартістю проведення молекулярно-генетичних досліджень для виділення із слідів біологічного походження профіля ДНК та його внесення в базу даних.

Зокрема, у такій ситуації за даними інформаційних підсистем ІПНП «Особа» та «Оперативно-довідкова картотека» перевіряються всі особи, які проживають у районі вчинення кримінального правопорушення та були раніше засуджені за вчинення злочинів проти власності. Серед них особливу увагу приділяють тим з них, які нещодавно повернулись з місць позбавлення волі та не мають постійного заробітку. Також перевіряються за обліками викрадені речі, особливо якщо серед них є номерні речі або культурні цінності, що підлягають реєстрації в окремій інформаційній підсистемі.

Типова слідча ситуація, у якій присутні ознаки кримінального правопорушення, є свідки (очевидці), які запам'ятали правопорушника та можуть його описати та впізнати, або є його відеозображення, зафіксоване відеокамерою спостереження. У цьому випадку зі слів свідків-очевидців потрібно скласти суб'єктивний портрет підозрюваного за допомогою автоматизованого програмного комплексу «Фоторобот». Складений композиційний портрет може бути перевірений автоматизованою системою портретної ідентифікації «Портрет». Система також дозволяє завантаження зображень, отриманих з відеокамер спостереження, графічних файлів та сканерів. Незважаючи на відносно невелику вартість та простоту у використанні цієї ідентифікаційної системи, вона поки що не знайшла застосування на центральному рівні. Окремі підрозділи її використовують, але база зображень правопорушників є незначною, а звідси й ідентифікаційні можливості встановлення злочинця за його зображенням зменшуються. Окрім цієї системи, на сьогодні існує достатня кількість програмних продуктів розпізнання обличчя людини, що вже знайшли апробацію на практиці. Наприклад, прикордонники за допомогою американської програми розпізнавання обличчя «Clearview AI» змогли встановити особи понад 10 тисяч осіб, які брали участь у воєнних злочинах російської федерації [3].

Також можливо використання даних інформаційної підсистеми «Розшук» ІПНП, що містить інформацію про осіб, які ухиляються від відбування покарання або переховуються від слідства чи зникли безвісти. В інформаційній підсистемі «Пізнання» ІПНП містяться відомості про підозрюваних, підсудних та осіб, які ухиляються від вироку суду або відбування покарання; зниклих безвісти; осіб, які не здатні через стан здоров'я чи вік повідомити інформацію про себе; невпізнаних трупів.

Більш сприятливою для розслідування є типова слідча ситуація, коли особу правопорушника встановлено, але не затримано і його місцезнаходження невідомо. У цій ситуації випадку потрібне комплексне використання інформації оперативно-розшукових обліків та інформаційно-довідкових обліків на центральному та регіональному рівнях. Також можуть використовуватись інформаційні бази інших відомств, зокрема: Державної міграційної служби, СБУ, прокуратури, НАБУ та ін. Поряд з цим, можливо використання баз даних різних підприємств та організацій, банківської системи, медичних установ, транспортних підприємств тощо.

У сприятливій для розслідування типовій слідчій ситуації коли є ознаки кримінального правопорушення та особу затримано з викраденим майном при його вчиненні. Зокрема, особа перевіряється для встановлення: можливого вчинення ним інших кримінальних правопорушень за інформаційною підсистемою «Особа», вчинення правопорушень у минулому за інформаційною підсистемою «ОДК». Інформація зазначених підсистем при наявності судимості, містить дані про час і місце затримання, прояви агресивності, протидії працівникам поліції, наявності при затриманні викрадених речей, наркотичних засобів, зброї тощо, а також особистісну інформацію: спосіб життя, звички, нахили, стосунки з членами сім'ї, товаришами, колегами по роботі, сусідами тощо.

Проаналізувавши можливості використання криміналістичних обліків при розслідуванні кримінальних правопорушень проти власності, можна зазначити, що об'єм необхідної інформації визначається слідчим залежно від слідчої ситуації, що склалась на певному етапі, об'єму та значимості вилучених об'єктів та наявності інших фактичних даних, що знаходяться у матеріалах кримінального провадження. Від швидкого та професійного використання інформації, що міститься в криміналістичних обліках на початковому етапі залежить успіх всього розслідування.

---

1. Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України // Право і безпека. 2013. № 3 (50). С. 110-115.

2. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України». Наказ МВС України від 16.03.2020 р. № 257. URL : https://zakon.rada.gov.ua/laws/show/z0319-20#Text.

3. Clearview AI – система розпізнавання обличчя, яка допомагає прикордонникам виявляти людей, причетних до злочинів. URL : https://www.ukrinform.ua/rubric-technology/3694894-zavdaki-programi-rozpiznavanna-oblic-vstanovili-osobi-10-tisac-rosijskih-voennih-zlocinciv.html.

ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

АНАЛІЗ ВІДКРИТИХ ПЛАТФОРМ ДЛЯ ПОШУКУ ОСІБ ПО ФОТОЗОБРАЖЕННЯМ В МЕРЕЖІ ІНТЕРНЕТ

Працівникам Національної поліції в рамках завдань, покладених на правоохоронні підрозділи, доволі часто виникає необхідність збирання інформації на певних фігурантів. Для отримання необхідної інформації, в першу чергу, використовуються відомчі бази даних, основу яких складає Інформаційний портал Національної поліції. Однак у багатьох випадках, коли фігурант раніше не контактував з правоохоронними органами, підсистеми ІПНП не містять інформації про цю особу. В даному випадку приходиться збирати інформації з відкритих джерел. Існує багато джерел та механізмів отримання подібної інформації використовуючи можливості пошукових та мета пошукових машин, державних реєстрів, соціальних мереж, розроблені методи OSINT-розвідки. [1, с. 328]. В даній доповіді пропонується розглянути відкриті інформаційні платформи для пошуку осіб по фотозображенням в мережі Інтернет. Також ми проаналізуємо їх функціональність та можливості.

Найбільш потужною серед платформ для пошуку осіб по фотозображенням є пошукова система зі штучним інтелектом Clearview AI. Вона використовується правоохоронними підрозділами багатьох держав. Керівництво цієї платформи дуже ретельно слідкує за користувачами своєї інформаційно-пошукової системи, право користування базою Clearview AI надається виключно суб'єктам правоохоронної діяльності. Після початку війни в Україні 24.02.2022 року деяким правоохоронним підрозділам України було надано безкоштовний доступ до можливостей пошукової системи зі штучним інтелектом Clearview AI. Вони ефективно використовують систему Clearview AI для ідентифікації осіб на основі їхніх фотографій з відкритих джерел для розкриття злочинів, в першу чергу пов'язаними з військовими діями, та пошуку військових злочинців. Система найбільш ефективна для ідентифікації російських загарбників та колаборантів України за рахунок використання фотозображень з російської соціальної мережі «Вконтакте», яких у платформи 2 млрд. [2].

Однак, важливо відзначити, що цей процес може породжувати етичні та правові питання. Перш за все, це питання приватності громадян, оскільки система здатна ідентифікувати осіб за їхніми фотографіями без їхньої згоди. Це може призвести до недоречних порушень особистої сфери. Це підкреслює

необхідність обговорення та регулювання використання таких технологій в Україні з метою забезпечення балансу між правоохороною та правами людини. Крім того, необхідно враховувати ризики недостатньої точності системи Clearview AI, яка може спричинити помилкові ідентифікації та неправильне заподіяння шкоди невинним особам.

З подальшим розвитком соціальних мереж, онлайн-фотоальбомів та інших веб-сервісів, де користувачі завантажують свої фотографії, з'явилася необхідність у засобах для пошуку та ідентифікації осіб на фотографіях. Розглянемо систему пошуку осіб по фотозображенням TinEye, це одна з перших платформ, яка пропонує послуги з пошуку фотографій за зображенням. Сервіс дозволяє завантажити фото або ввести URL зображення та шукає інші варіанти цієї фотографії в Інтернеті. Використовуючи технології розпізнавання облич, TinEye може бути корисним для пошуку схожих зображень. Розглянемо можливості веб-ресурсу оболонки TinEye (рис. 1) [3]:

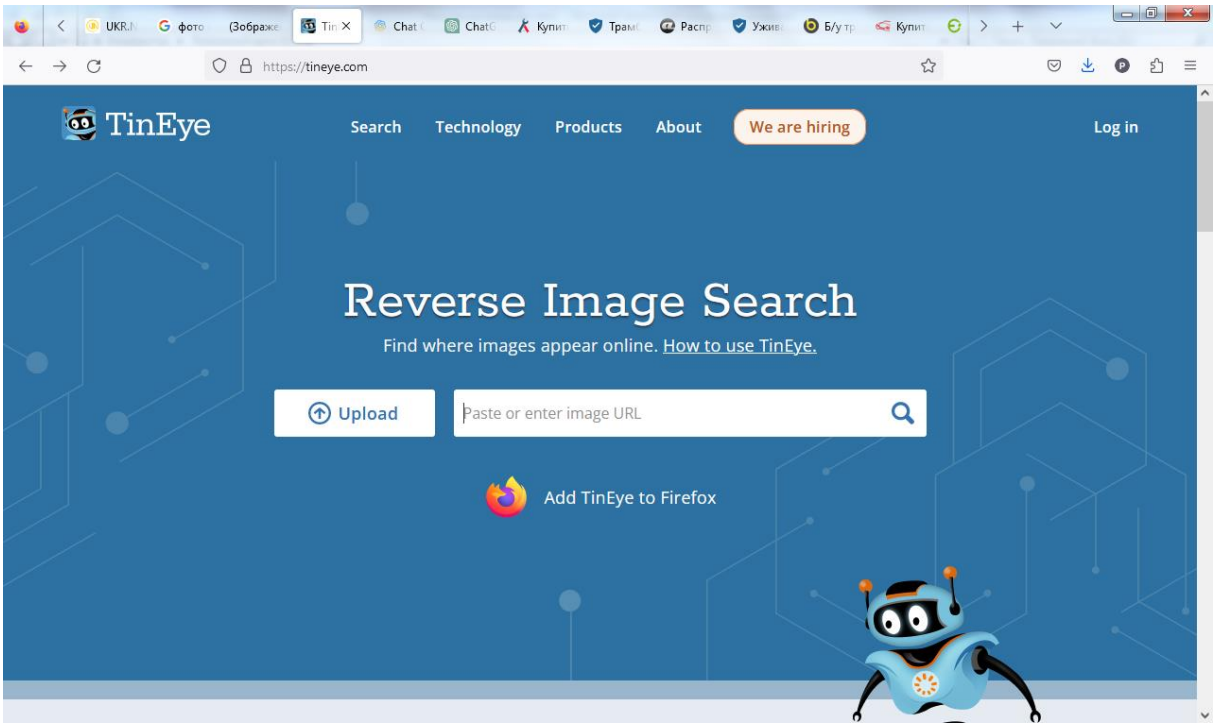

Рис. 1. Загальний вигляд веб-ресурсу оболонки TinEye.

Після введення у платформу TinEye фотозображення зрадника України Олега Царьова, отримуємо результат пошуку системи (рис. 2):

Тобто дана оболонка знайшла абсолютно ідентичні введеному фото фотозображення на 14 інтернет-ресурсах. Тобто дана система не аналізує безпосередньо обличчя особи, а проводить аналіз загального фотозображення. Вона не пригідна для пошуку різних фото особи, інформацію на яку ми збираємо.

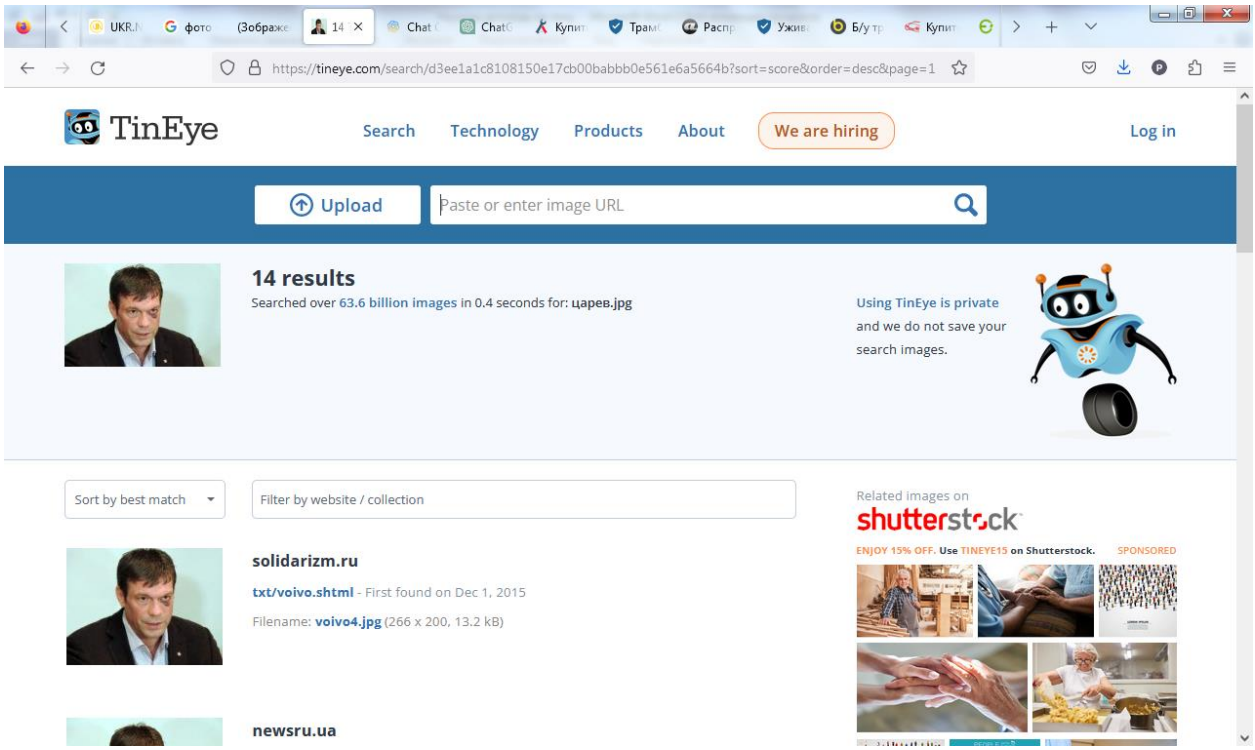

Рис.2. Результат пошуку системи TinEye.

Розглянемо платформу Google Images [4], що надає можливість пошуку фотографій в Інтернеті, використовуючи ключові слова або зображення. Також вона має функцію пошуку за зображенням, яка дозволяє завантажити фотографію та знайти інші сторінки, на яких ця фотографія зустрічається. Результат пошуку фігуранта Царьова у цій системі має наступний результат (рис. 3):

Ця оболонка для пошуку облич за фотозображеннями Google Images показала значно кращий результат, вона ідентифікувала фігуранта за введеним фото. Також знайшла понад 40 різних фотозображень фігуранта в мережі Інтернет. Можна зробити висновок, що ця система може використовуватись правоохоронцями для ідентифікації осіб та пошуку інформації за фотозображеннями в мережі Інтернет.

Розглянемо наступну платформу для пошуку осіб по фотозображенням PimEyes. Вона є сервісом, спеціалізованим на пошуку осіб за їх фотографіями. Він використовує технології розпізнавання облич та може вказувати, де і коли знайдену фотографію було опубліковано в Інтернеті

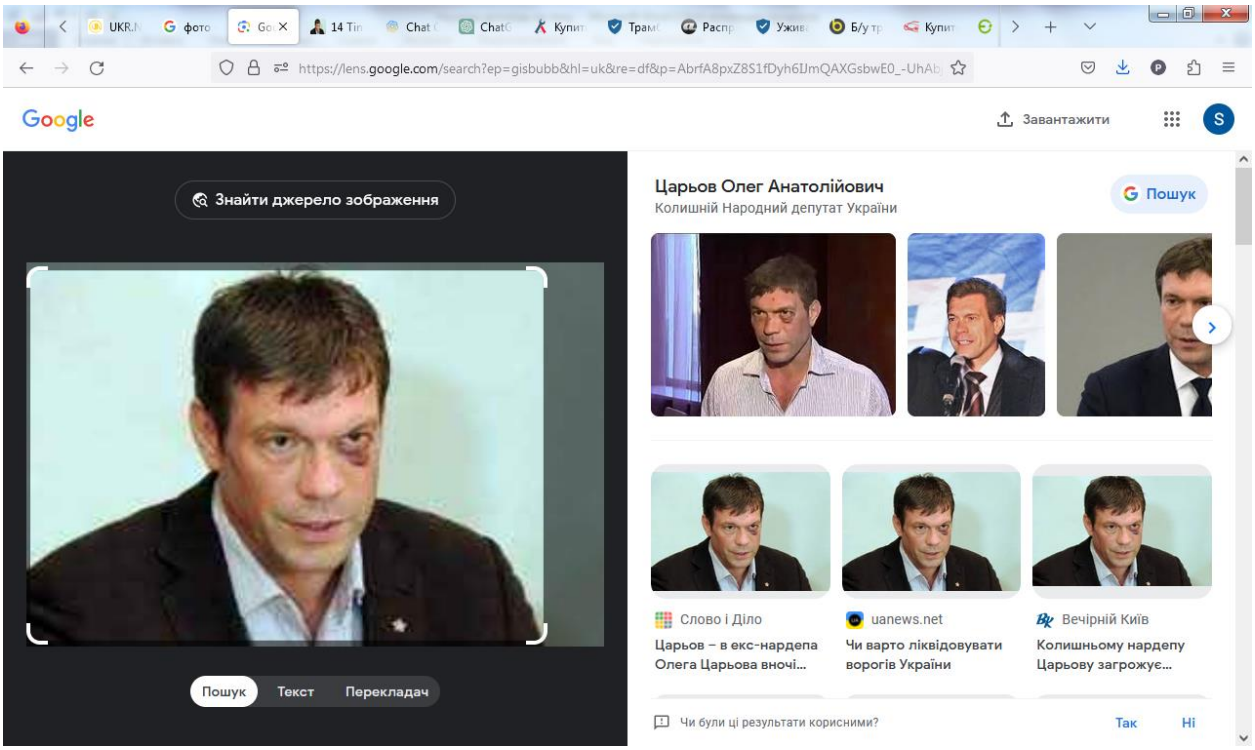

Рис. 3. Результат пошуку фігуранта системою Google Images.

За допомогою можливостей вбудованого в пошукову систему PimEyes штучного інтелекту, даному пошуковику вдається спочатку розпізнати обличчя людини на вхідному зображенні, а потім здійснити пошук цього обличчя на інших фотозображеннях, які розміщені у відкритому доступі мережі Інтернет. Для використання PimEyes не потрібна реєстрація, але ви не зможете переглянути зображення повністю та отримати посилання на сайт, на якому воно було знайдено, якщо не заплатите за право користування цією системою. Крім того, ви не зможете використовувати сповіщення при появі нових фото в мережі **[2].**

У результаті пошуку фігуранта по фото системою PimEyes було знайдено 247 інтернет-ресурсів з ідентифікованим Царьовим (рис. 4) [5]:

Ця система з початку проводить аналіз обличчя з фотозображення, а вже потім здійснює його пошук у мережі Інтернет з вражаючою точністю. Дана система є найбільш ефективною для пошуку осіб за фотозображенням і може використовуватись правоохоронцями для збору необхідної інформації при виконанні службових обов'язків. Суттєвим недоліком є те, що вона платна.

Використання відкритих платформ для пошуку осіб за фотозображеннями в мережі Інтернет стає все більш актуальним завдяки поширенню цифрових зображень та технологіям розпізнавання облич.

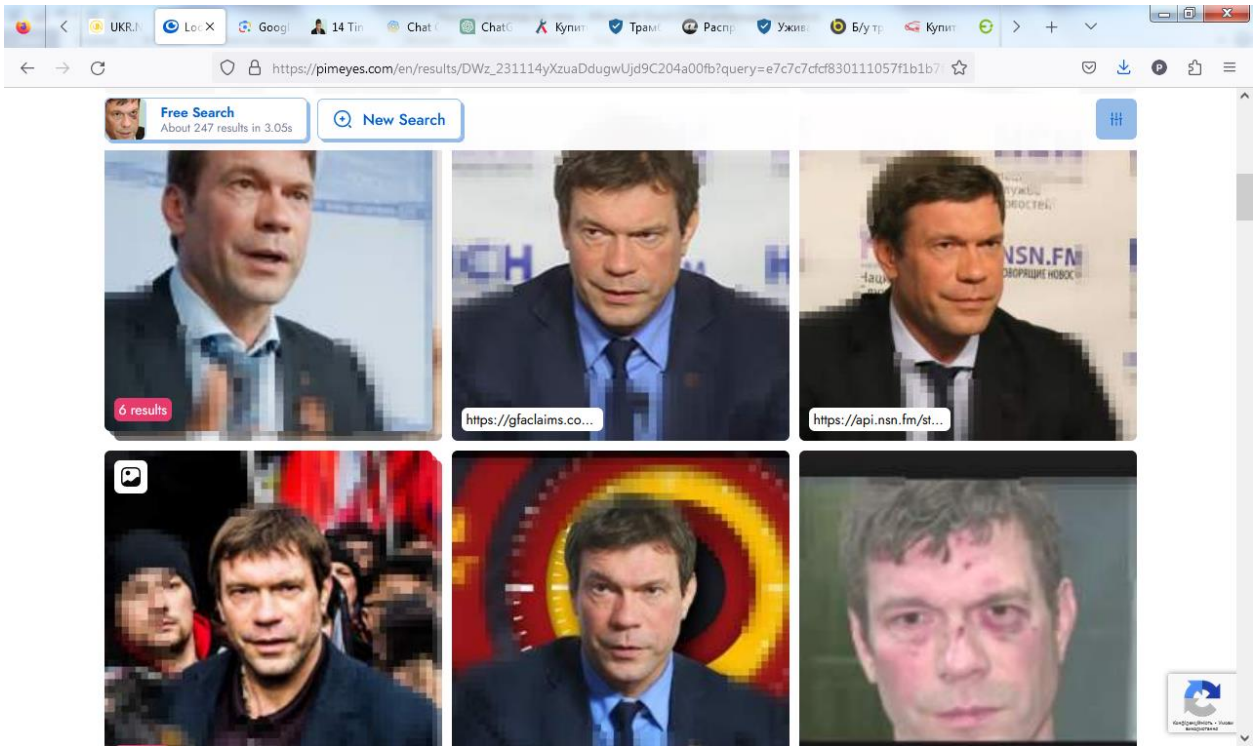

Рис. 4. Результат пошуку фігуранта системою PimEyes.

Зазначені сервіси надають правоохоронцям можливість відшукати фотографії або інформацію про осіб на основі доступних зображень.

Проведений аналіз відкритих платформ для пошуку осіб за фотозображеннями у мережі Інтернет буде корисним як для практичних працівників Національної поліції з метою/у процесі/під час ефективного збору інформації під час досудового розслідування, контрольно-пропускного режиму та виконання інших функціональних обов'язків, особливо під час війни.

1. Інформаційні технології : підручник / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий та ін. Дніпро : ДДУВС, 2021. 492 с. URL : https://er.dduvs.in.ua/handle/123456789/6820

2. Використання технологій розпізнавання обличчя на видео та фотозображеннях: метод. рекоменд. / А.М. Гребенюк, С.О. Прокопов, Л.В. Рибальченко Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 42 с.

3. Веб-сайт пошукової системи TinEye. URL : https://tineye.com/

4. Веб-сайт пошукової системи Google Images. URL : https://images.google.com/

5. Веб-сайт пошукової системи PimEyes. URL : https://pimeyes.com/en

БАЗУКІН А. С.
курсант 3 курсу факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ТРЕНІНГ «ЛІНІЯ 102» У ДНІПРОПЕТРОВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

Програмно-технічні комплекси інформаційного забезпечення діяльності Національної поліції як «ЦУНАМІ», Інформаційний портал та інші, нажаль відсутні у вищих навчальних закладах системи Міністерства внутрішніх справ, що негативно впливає на рівень інформаційної підготовки майбутніх правоохоронців. Тому виникає необхідність розроблення навчальної інформаційно-технічної платформи, яка максимально відображує реально діючі системи інформаційного забезпечення Національної поліції, тобто є їх емулятором. Інформаційно-технічна платформа супроводження професійно-орієнтованої ділової гри «Лінія 102» розроблена та впроваджена авторським колективом кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ [1, с. 461].

Як яскравий приклад власного досвіду, я брав участь у тренінгу «Лінія 102» від Дніпропетровського державного університету внутрішніх справ. Інтерактивні методичні рекомендації інформаційно-технічної платформи професійно-ділової гри «Лінія 102» розміщені на веб-вузлі 102.dduvs.in.ua, доступ до якого мають всі поліцейські навчальні заклади [2].

Ми заходили на Емулятор лінії 102, вибирали емблему ДДУВС. Та реєструвалися у системі відповідно до ролі. За найкоротший час, а саме до 2 хвилин, я ввів всі дані про місце події, які мені казав напарник, який був заявником. На наступному занятті, я у ранзі патрульного прибув на місце події, склав звіт про свої дії та додав до нього фото. Цей тренінг видався доволі цікавим та допоміг справити моє враження як працює «Лінія 102»

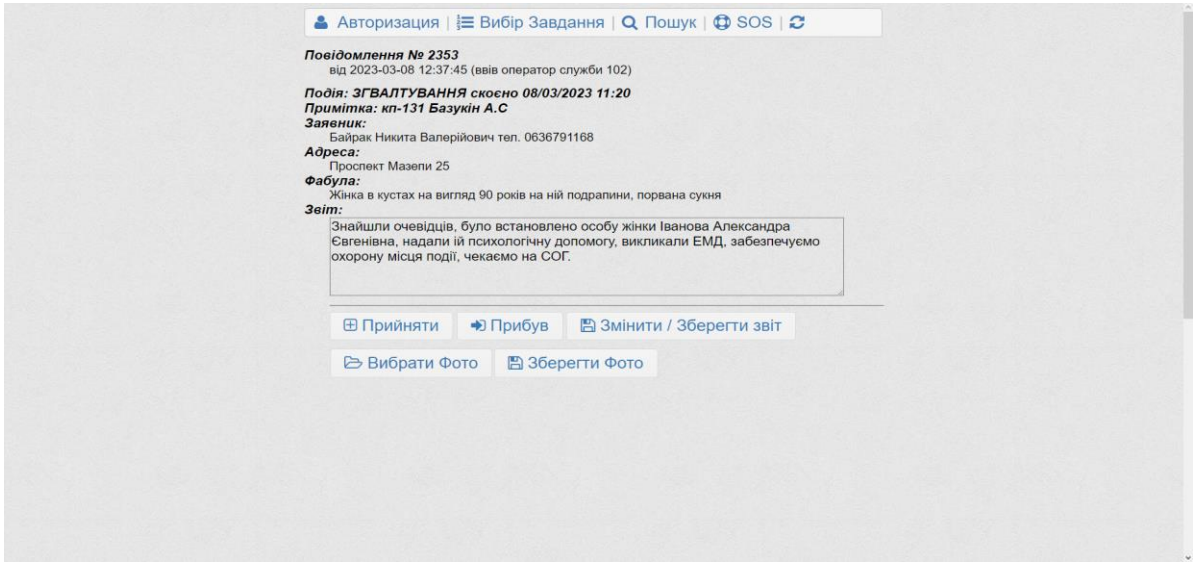

Рис.1 Робоче місце патрульного

Для початку роботи у ролі оператора 102 я по-перше авторизувався у системі, ввів ім’я користувача та пароль. Після авторизації з’являється графічний інтерфейс робочого місце оператора, де в правій частині екрана розташований список подій з сортуванням за датою занесення цієї події в базу даних, а в лівій частині розташована форма для створення нової події. Для того, щоб створити картку події я виконав наступне:

1. Заповнив пункт Подія.
2. Ввів час та дану скоєння злочину
3. Далі ввів інформацію про місце скоєння злочину, для цього заповняється поля адреси (місто, вулиця, будинок)
4. Наступним увів інформацію про заявника, його номер телефону, прізвище, ім’я та по-батькові
5. У полі Зміст стисло вніс опис події з описом деталей скоєного правопорушення
6. Для того, щоб закінчити введення даних та створити картку події, натиснутив на кнопку – Зберегти. Введена інформація потрапляє в базу даних загальних подій.

Також, на вкладці Карта є можливість здійснити пошук адреси за допомогою Google карт.

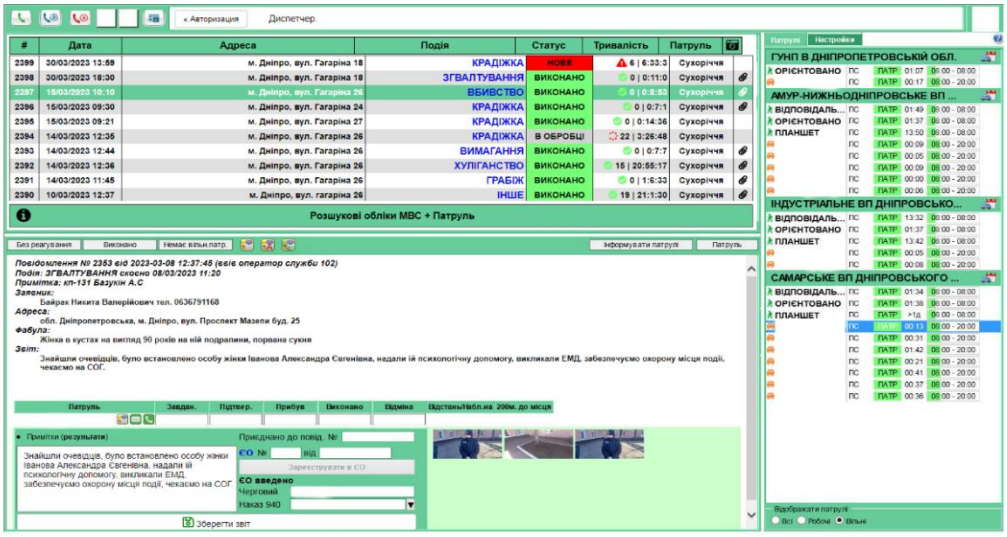

Рис. 2 Робоче місце оператора 102

У диспетчера 102 на екрані розташована таблиця з подіями, занесеними базами даних оператором 102. Диспетчер має можливість вибрати будь-яку подію і натиснувши на нею один раз правою кнопкою мишки побачити подробиці про подію, а також звіт патруля про виконану роботу. У таблиці подій, напроти кожної події відображається її статус. Існує чотири статуси події. Статус «Новий» – це новий запис у базі даних подій. Статус «В обробці» – екіпаж патрульної поліції прийняв завдання та прямує до місце події. Статус «Прибув» – патруль прибив до місця події та вже виконує свої функції на місце події. «Виконано» – патруль впорався зі своїм завданням, написав короткий звіт про дані події та зберіг його у систему. Коли з'являється подія зі статусом «Нове», диспетчер зв'язується по рації з патрулем і оголошує патрулю, що саме вони беруть в обробку подію з відповідним номером. Коли патруль прийняв цю подію в обробку на робочу місці диспетчера Статус події «Нове» змінюються на статус «В обробці», що означає, що патруль прямує на місце події. Після прибуття патруля на місце події статус завдання змінюється на «Прибув». Коли патруль завершив свою роботу статус змінюється на «Виконано» та диспетчер може переглянути звіт, який склав патруль.

Отже, створений авторським колективом ДДУВС емулятор лінії 102 дуже допомагає в розвитку інформаційної підготовки курсантів університету. Курсанти, можуть спробувати себе у ролі оператора, диспетчера та патрульного, отримати базові знання роботи з програмно-технічними комплексами інформаційного забезпечення діяльності Національної поліції та дали набуті навички зможуть застосувати вже на службі. А також, викладачі відповідної навчальної дисципліни проводять практичні заняття, що позитивно впливає на професійні якості майбутніх правоохоронців.

1. Інформаційні технології : підруч. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніп- роп. держ. ун-т внутр. справ, 2021. 492 с. URL : http://er.dduvs.in.ua/handle/123456789/6820

2. Прокопов С.О. Удосконалення інформаційно-технічної платформи професійно-ділової гри «Лінія 102». Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 28 листоп. 2019 р.). Дніпро : ДДУВС, 2019. С. 54-57 URL : https://er.dduvs.in.ua/handle/123456789/4992

ЛЕЩЕНКО Д. Д.,
курсант 3 курсу факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ЗАРУБІЖНИЙ ДОСВІД ФОРМУВАННЯІНФОРМАЦІЙНОГО ПРОСТОРУ У СИСТЕМІ ПРАВООХОРОННИХ ОРГАНІВ

Система правоохоронних органів Україні постійно потребує пристосовуватись до нових потреб забезпечення правопорядку державі та боротьби з правопорушеннями, необхідно підвищувати якісний рівень інформаційного забезпечення. Аналіз інформаційного забезпечення правоохоронних органів України свідчить про постійну необхідність його вдосконалення.

Як зазначає О.В. Бочковий, автоматизовані інформаційно-пошукові системи широко використовуються правоохоронними органами у багатьох зарубіжних країнах та сприяють оптимізації процесів розкриття та розслідування злочинів, скоєних членами організованих угруповань. В умовах активізації процесів обміну інформацією та загального ритму життя, в тому числі і злочинного, необхідно постійно удосконалювати методи та способи роботи зі зростаючими масивами даних. З цією метою функціонують інформаційно-аналітичні системи, основна перевага яких полягає у здійсненні аналізу та прогнозування [1, с. 227].

Варто звернути увагу, перш за все всього, Звернемо увагу на досвід застосування інформаційних технологій у діяльності правоохоронних органів країн ЄС, адже в умовах євроінтеграції співробітництво в галузі юстиції,

свободи та безпеки є одним із важливих векторів руху нашої держави до набуття статусу повноцінної держави-члена ЄС.

В умовах реформування системи правоохоронних органів важливим для підвищення ефективності її інформаційно-аналітичного забезпечення є вивчення досвіду успішного функціонування інформаційних систем країн ЄС, а не лише гармонізація законодавства у цій сфері. Наразі, вивчаючи досвід країн ЄС у сфері застосування інформаційних технологій правоохоронними органами, науковці особливу увагу приділяють передовому досвіду Великобританії.

У цій державі було введено систему нових комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств, що сприяє підвищенню рівня попередження правопорушень та швидкого їхнього розкриття. Сучасні технічні засоби відеоспостереження, які застосовують поліція Великобританії, мають здатність здійснювати нагляд під час стеження за громадянами, особливістю якого є моментальне сканування особи та перевірка у файлах поліції. Впроваджена корпоративна об'єднана інформаційна модель даних для потреб поліції ґрунтується на створення каталогу інформаційних об'єктів, завдяки якому встановлюються та наочно демонструються ієрархічні взаємини між інформаційними об'єктами [2, с. 169].

Серед інформаційних систем Великобританії насамперед необхідно звернути увагу на основну Національну комп'ютерну систему поліції Великобританії – Police National Computer (PNC), яка введена з метою сприяння здійсненню розслідування та обміну інформацією. До того ж, ця система містить розширені відомості про людей, транспортні засоби, злочини та майно, які доступні в межах захищеної мережі та включають мобільні перевірки даних на місці злочину або проведення розслідування [3].

Заслуговує на увагу також досвід застосування інформаційних технологій правоохоронними органами Франції. Інформаційно-аналітична система ANACRIM, якою користуються не лише французькі правоохоронні органи, а також багатьох інших країн ЄС, використовується Національною жандармерією Франції з метою проведення аналізу стану злочинності у країні. ANACRIM містить інформацію про осіб, місця, подіях, зокрема номери телефонів або автомобілів. За допомогою ANACRIM французькі правоохоронці встановити зв'язок між усіма записами в базі даних, а висновок надається у вигляді графічної презентації. На основі цього аналітики визначають відповідні гіпотези або складають запити з метою заповнення прогалин або перевірки деяких інтелектуальних припущень. Відповідно до французького законодавства до бази даних ANACRIM можуть бути внесені також відомості, які вимагають доказування на розсуд слідчого.

Проте інформація до бази даних інформаційної системи ANACRIM може бути внесена лише тоді, коли існують вагомі та послідовні докази підозри або вчинення особою особливо тяжкого злочину. Правоохоронні

органи Франції також використовують у своїй діяльності автоматизовані інформаційно-пошукові системи, зокрема JUDEX - це система, з допомогою якої здійснюється реєстр кримінальних правопорушників та потерпілих, у якій міститься близько 3 млн записів; Fichier National Automatisé des Empreintes Génétiques (FNAEG) – автоматизований національний банк даних генетичних відбитків ДНК; L'application digestion des dossiers des ressortissants etrangersen France (AGDREF AGEDREF) – база даних, у якій зосереджується інформація про іноземців; автоматична інформаційно-пошукова система «Касіопея», яка містить інформацію про скарги зареєстрованих суддів у ході судового розгляду, обвинувачених, свідків, потерпілих та цивільних позивачів [4, с. 5]

Правоохоронні органи Федеративної Республіки Німеччина (ФРН) Не менш активно, ніж розглянуті вище країни-члени ЄС, застосовують новітні інформаційні комп'ютерні технології з метою покращення якості інформаційного забезпечення своєї службової діяльності. Так, єдиним центром збору та електронної обробки необхідної для німецької поліції інформації є Федеральна кримінальна поліція – Bundeskriminalamt (BKA). На Bundeskriminalamt покладається завдання встановлення взаємодії між усіма поліцейськими органами та службами держави у сфері запобігання та протидії злочинності.

Як зазначає М. Криштанович, за допомогою використання інформаційно-аналітичних систем правоохоронні органи ФРН виконують важливі завдання, зокрема здійснюють реєстрацію та обробку оперативних даних, що надходять до структурних підрозділів управління у вигляді письмових відомостей, поліцейських протоколів, радіоповідомлень; проводять реєстрацію та обробку повідомлень про здійснення правопорушень та злочинів; здійснюють передачу у земельний кримінальний розшук оперативних повідомлень щодо кримінальних злочинів; здійснюють інформаційний пошук згідно з запитами співробітників управлінь та ін [5, с. 347].

Отже, правоохоронні органи зарубіжних країн приділяють велика увага створенню та забезпеченню функціонування інформаційних систем як важливого інструменту забезпечення ефективності запобігання та протидії злочинності. Аналіз інформаційного забезпечення багатьох країн-членів ЄС, США, Ізраїлю дозволяє зробити висновок про те, що вітчизняна система інформаційного забезпечення потребує вдосконалення, зокрема приведення у відповідність до міжнародних стандартів. Порівняно із зарубіжними аналогами введені вітчизняні інформаційні системи потрібно вдосконалювати відповідно до технологічного рівня та потребами розвинених країн. Необхідно вводити нові програмні комплекси, які дозволять встановлювати зв'язок між інформацією про особу, яка підлягає перевірці з метою побудови версій чи передбачення поведінки. У сучасних умовах зростання транснаціональної злочинності, тероризму важливим

напрямом міждержавного співробітництва правоохоронних органів виступає формування єдиного інформаційного простору, зокрема введення в рамках міжнародних поліцейських організацій (Європола, Інтерполу) комп'ютеризованих систем обміну.

1. Бочковий О.В. Ігнорування інформаційно-технічного прогресу органами досудового розслідування в Україні: хронічна риса чи тимчасове явище? / О.В. Бочковий // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2016. Вип. 3. С. 223. URL: http://nbuv.gov.ua/UJRN/Vlduvs_2016_3_26 .

2. Нефедова Н.А. Інформаційне забезпечення спеціальної поліцейської діяльності. Адміністративне право і процес. 14. № 2(8). С. 167–173 URL : http://applaw.knu.ua/indexphp/holovna/item/download/220_925e37796a97ae5941a1a6e59018065f

3. The PNC or Police National Computer URL : http://www.inbrief.co.uk/police/police-national-computer/

4. Катеринчук І.П. Світовий досвід застосування інформаційних технологій у діяльності правоохоронних органів. Роль та місце правоохоронних органів у розбудові демократичної правової держави: матеріали VIII міжнар. наук.-практ. конф., м. Одеса, 25 березня 2016 р. Одесса : ОДУВС, 2016. 356 с.

5. Криштанович М.Ф. Модернізація механізмів державного управління в системі органів внутрішніх справ сучасної України: дис. ... д-ра наук з держ. упр. : 25.00.02 / М.Ф. Криштанович ; Чорномор. нац. ун-т ім. Петра Могили. Миколаїв, 2016. 474 с. URL : https://chmnu.edu.ua/wp-content/uploads/2016/09/Kryshtanovych_dis.pdf.

ЛЕЩЕНКО Максим
курсант гр. ДР-344 ННІППФПНП
Науковий керівник:
РИБАЛЬЧЕНКО Людмила
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ГЕНДЕРНА НЕРІВНІСТЬ В УКРАЇНІ ТА ЄВРОПІ

Термін «гендер» вказує на різноманітні соціальні ролі, обов'язки і ідентичності, які призначені жінкам і чоловікам, а також на взаємовідносини між ними в конкретному суспільстві. Гендерні ролі та відносини різняться в різних країнах і культурах, і можуть відрізнятися навіть серед різних груп в межах одного суспільства.

Гендерна нерівність виникає, коли існують фактичні відмінності у правах, можливостях та сприйняттях жінок і чоловіків через наявність сексизму. Досі спостерігається нерівна представленість жінок у різних

сферах, таких як безпека, освіта, доступ до робочих можливостей, участь у політиці, оплата за рівноцінну роботу (гендерний розрив у зарплаті), а також випадки гендерного насильства, зокрема насильства проти жінок.

Гендерна статистика визначається як збір і аналіз інформації, що точно відображає відмінності та нерівності у становищі жінок і чоловіків у різних сферах життя (згідно з визначенням Організації Об'єднаних Націй у 2006 році).

Гендерна інтеграція у національній статистиці передбачає, що аспекти, пов'язані з ґендером, та ґендерні упередження системно враховуються під час створення всієї офіційної статистики на всіх етапах її виробництва.
Перший крок у виробництві ґендерної статистики полягає в визначенні показників, які необхідні для досягнення та розуміння цілей, пов'язаних із ґендерними питаннями.

Гендерна статистика повинна мати наступні характеристики: а) збір, ідентифікація та поширення даних здійснюється з розподілом за ознакою статі;

б) дані ґендерної статистики ґрунтуються на визначеннях, які правильно відображають суспільні відмінності між жінками та чоловіками, охоплюють всі аспекти їхнього життя та є доступними як вихідні дані;

в) методи збору даних враховують соціальні та культурні чинники, а також стереотипи, які можуть викликати ґендерно зумовлені викривлення в даних.

Створення національної системи індикаторів на основі даних ґендерної статистики та їх аналіз сприятиме активізації заходів та відстеженню змін у ґендерній сфері, а також підготовці публікацій, присвячених ґендерним питанням.

Дані ґендерної статистики є основою для розробки стратегічних рішень органами влади в напрямках реалізації принципу рівноправності у суспільстві, запобігання та протидії гендерній дискримінації, підтримки сімей, формування відповідального батьківства та культури поведінки.

У 2021 році Данія виокремилася серед європейських країн як лідер за гендерною рівністю з індексом 0,013. Країна відзначається низьким рівнем материнської смертності (4 випадки на 100 тисяч новонароджених) та невеликим показником підліткових вагітностей (1,9 на тисячу жінок). Практично рівна кількість чоловіків і жінок мають як мінімум середню освіту (понад 95%), а зайнятість становить 57,7% для жінок та 66,7% для чоловіків. Жінки займають 39,7% місць у парламенті.

На другому місці в Європі розташувалася Норвегія із показником 0,016. У країні відзначається значно нижчим ризиком материнської смерті та вищим показником підліткових вагітностей (2,3). Понад 99% чоловіків і жінок мають як мінімум середню освіту, а роботу мають 60,3% жінок та 72% чоловіків. Жінки у парламенті складають 45%.

На третьому місці з індексом 0,018 розташувалася Швейцарія. Країна

має коефіцієнт материнської смертності 5 на 100 тисяч народжених і 2,2 підліткових пологи на тисячу жінок. Зайнятість становить 61,7% для жінок та 72,7% для чоловіків, а практично всі (понад 96%) мають як мінімум середню освіту. Жінки у парламенті складають 39,8%.

У період воєнних дій спостерігається значне погіршення цієї тенденції, оскільки в умовах воєнного конфлікту та зростання складності побутових проблем (відсутність електроенергії, водопостачання, зв'язку, руйнування житла і т.д.) жінки змушені пріорітетно вдаватися до розв'язання справ, пов'язаних із виживанням домогосподарств. Це часто веде до відмови від власної кар'єри та інших можливостей самореалізації. Особливо це стосується тих родин, де чоловіки мобілізовані, загинули чи отримали серйозні травми, і які залишилися в Україні.

У зв'язку з прямими втратами, переважно серед працездатних чоловіків під час війни в Україні, ймовірно, буде спостерігатися збільшення участі жінок на ринку праці. Повномасштабні конфлікти найчастіше породжують необхідність у прискоренні процесу забезпечення гендерної рівності у сфері зайнятості. Тому актуальною стає необхідність розробки державних програм, які б дозволяли жінкам отримати новий досвід і знання, а також отримувати моральну підтримку під час навчання новій професії або перекваліфікації.

Завдяки ефективній державній підтримці та належному орієнтуванню на професійному рівні, жінки матимуть можливість отримувати справедливу заробітну плату. Удосконаленню нормативно-правової бази з питань гендерної рівності сприятиме прийняття Закону України «Про рівне винагородження за однакову працю», проєкт якого вже розроблено Міністерством економіки України.

Крім того, важливо активно проводити інформаційно-комунікаційні заходи, зокрема серед молоді, з метою подолання гендерних стереотипів у відношенні «жіночих» та «чоловічих» професій і протидії професійній сегрегації. Також слід створювати умови для злагодження сімейних і професійних обов'язків для працівників з дітьми.

Забезпечення гендерної рівності на ринку праці буде сприяти швидшому економічному відновленню, зміцненню стабільності економіки та активізації процесу повоєнного відновлення, що в свою чергу поліпшить умови та якість життя громадян України.

---

1. Резолюція Ради Безпеки ООН 1325 "Жінки, мир, безпека". Режим доступу: https://nssu.gov.ua/genderna-rivnist
2. Індекс гендерної нерівності в Україні та Європі. Слово і дело. Режим доступу: https://www.slovoidilo.ua/2023/03/08/infografika/ suspilstvo/indeks-hendernoyi-nerivnosti-ukrayini-ta-yevropi
3. Гендерні диспропорції в Україні під час війни. Національний інститут стратегічних досліджень. Режим доступу: https://niss.gov.ua/news/komentari-ekspertiv/henderni-dysproportsiyi-v-ukrayini-pid-chas-viyny

ЛИТВИНЕНКО О. О.,
курсантка 3 курсу факультету
підготовки фахівців для підрозділів
кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ ВІДЕОАНАЛІТИКИ В РОБОТ І НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Сьогодні системи відеоспостереження широко використовуються для забезпечення безпеки банків, торгових центрів, розважальних закладів, промислових підприємств та інших комерційних і некомерційних організацій. Системи відеоспостереження використовуються для швидкого реагування на небезпечну ситуацію, контролю за персоналом та відвідувачами, а системи відеореєстрації широко застосовуються і мають потенціал у моніторингу дорожнього руху тощо. Відеоаналіз - це комплекс дій, які використовують ситуаційні центри для швидкої та ефективної обробки відеоданих з метою виявлення правопорушень та осіб, причетних до скоєння злочинів.

Основними завданнями, які можна та доцільно вирішувати за допомогою відео технологій, є:

– розпізнавання, адже найчастіше розпізнаються обличчя людей і номери автомобілів або вагонів;

– завдання, пов’язані з аналізом поведінки людини, автомобіля або іншого рухомого об’єкту;

– реалізація охоронних функцій на різноманітних об’єктах [1, с.6].

Наразі в Україні існує потреба у підготовці та вдосконаленні професійних знань ситуаційних центрів для проведення сучасних розслідувань, адже наприклад відеоспостереження дуже погано розвинуте в Україні та потребує вдосконалення, а також у подальшому розвитку практичних можливостей використання результатів, отриманих під час відеоаналізу, для ефективного виконання завдань Національною поліцією. Наразі ця тема має велике значення в потоці різноманітних технологій, які допомагають правоохоронним органам, особливо поліції, виявляти, розслідувати та запобігати злочинній діяльності.

Сучасний світ має можливість використовувати технології для миттєвого отримання необхідної інформації про правопорушника.

Використання інформації, отриманої в результаті аналізу відеоматеріалів департаментом кримінального аналізу, є важливим підґрунтям для вирішення інших важливих питань, таких як припинення, розкриття та попередження злочинів Національною поліцією.

Інформаційна система — Гарпун регламентується наказом НПУ від 13.06.2018 No 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

Інформаційна підсистема «Геопортал – Гарпун» інформаційно – телекомунікаційної системи «ІПНП» дає можливість отримати дані про перес вання транспортного засобу (ТЗ) автошляхами України. Треба заповнити параметри пошуку: ДНЗ транспортного засобу і період часу та відомості про ініціатора пошуку.

У результаті позитивного результату на екран виводиться інформація про час фіксації відповідного ТЗ. Натиснувши на відповідний номер, на карті виводиться вікно з інформацією та фотозображенням з відеокамери [2].

Сучасні інформаційні технології мають вражаючі можливості і можуть як покращити життя пересічних громадян, так і сприяти ефективній роботі Національної поліції. Адже, завдяки сучасним технологіям обробки інформації та новітній техніці, можна легко та швидко виконувати поставлені завдання. Основними завданнями, які можна і потрібно вирішувати за допомогою відеоаналізу, є наступні - завдання, пов’язані з аналізом поведінки людини, автомобіля або іншого рухомого об’єкта; Завдяки сучасним методам відеоаналізу можна виявити підозрілих осіб у людському потоці, покинуті предмети, які можуть становити небезпеку для оточуючих, а також виявити ознаки злочину. Завдяки сучасним можливостям розпізнавання облич стає все простішим і простішим. Ми знаємо, що людина має індивідуальну (унікальну) зовнішність і відносно стабільні характеристики. Процес ідентифікації передбачає порівняння двох (або більше) наборів характеристик. Тому для ідентифікації необхідно виділити ці ознаки. Умови низької освітленості часто є основною проблемою при використанні відеотехніки в роботі поліції.

Для роботи загального відеоспостереження, яким зазвичай користуються громадяни, освітлення може бути достатнім, але, наприклад, матеріал відеозапису, отриманий відповідно до кримінально-процесуального законодавства, може бути використаний як доказ у кримінальній справі, оскільки є додатком до протоколів слідчих дій та обвинувачення, речовим доказом і об’єктом дослідження для фахівців у галузі відеоаналізу з метою встановлення осіб, причетних до злочину. Для розпізнавання обличчя освітленість повинна бути від 300 до 400 люкс. Це створює низку проблем для фахівців з відеоаналізу. У будь-якому випадку їм доводиться шукати нове, нестандартне рішення цієї проблеми. Слід враховувати, що збільшення кількості камер вимагає збільшення ресурсів для обробки інформації. Це

питання матеріальних і людських ресурсів [3].

Отже, використання відповідного обладнання та пристроїв для відеоспостереження, які мають розширені технічні характеристики та налаштування для якісної фіксації в денний або темний час зйомки, відеотехнологій обробки отриманої таким чином інформації у роботі Національної поліції має величезне значення у розкритті та попередженні злочинів і у профілактиці правопорушень.

1. Використання відеоаналітики у роботі Національної поліції. Методичні рекомендації. – Мирошниченко В.О, Кочеткова . І. Б.Махницький О.В. – Дніпропетровський державний університет внутрішніх справ.– Дніпро, 2020 – 34 с. URL: https://er.dduvs.in.ua/handle/123456789/5570

2. Інформаційні технології : підруч. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніп- роп. держ. ун-т внутр. справ, 2021. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820

3. Наказ Міністерства внутрішніх справ України 23.05.2017 року №440 (у редакції наказу Міністерства внутрішніх справ України від 08.02.2022 № 103)/ URL: https://zakononline.com.ua/documents/show/383825___689404

ЛУКОМСЬКА Аліна
слухач магістратури І курсу
ННІП ПФПНП
Науковий керівник:
ГРЕБЕНЮК Андрій
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

СКАНУВАННЯ МОЗКУ ЯК ІННОВАЦІЙНИЙ МЕТОД РОЗКРИТТЯ ЗЛОЧИНІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

Розкриття будь-якого кримінального правопорушення неможливе без роботи з різними видами слідів. Як відомо, робота зі слідами складається з кількох етапів, а саме: виявлення, фіксація, вилучення, дослідження, оцінка та використання. Відповідний процес відбувається не швидко, а тому займає достатню кількість часу. Адже без правильної роботи на перших трьох, тобто без грамотного, процесуально правильного збирання слідів, неможливе повне дослідження та використання у процесі доведення.

Сліди біологічного походження у цьому сенсі дуже специфічні та

робота з ними має низку особливостей. Складність роботи зі слідами біологічного походження полягає в тому, що вони можуть дуже швидко змінюватися, зазнаючи деструктивних змін, що, у свою чергу, унеможливлює їх використання і для вирішення ідентифікаційних завдань. Сліди біологічного походження можуть бути утворені кров'ю, спермою, слиною тощо. До них належать також волосся, органи та тканини людського організму, кістки та їх фрагменти. Джерелом слідів біологічного походження є тіло людини, зокрема її мозок [2, с. 235-236].

Неврологи заявили, що функції, які виконуються розумом, такі як навчання, пам'ять і свідомість, обумовлені чисто фізичними і електрохімічними процесами у мозку. Наприклад, Крістоф Кох і Джуліо Тононі заявили в журналі «IEEE Spectrum»: «Свідомість є частиною природного світу. Вона залежить від того, як мислимо, тільки з точки зору математики, логіки і відомих законів фізики, хімії і біології; вона не виникає з якоїсь магічної або потойбічної якості.» [1].

Видатні вчені-програмісти і неврологи передбачили, що спеціально запрограмовані комп'ютери будуть здатні мислити і навіть зможуть досягти свідомості. Незважаючи на те, що завантаження впливає на загальні можливості, воно концептуально відрізняється від загальних форм в тому, що є результатом динамічної реанімації інформації, яка була одержана від конкретного людського розуму, так що розум зберігає почуття історичної самобутності. Перенесена і відновлена інформація стане формою штучного інтелекту.

Багато теоретиків представили моделі мозку і встановили діапазон оцінок обсягу обчислювальних потужностей, необхідних для часткової і повної симуляції. Використовуючи ці моделі, вчені підрахували, що завантаження свідомості може стати можливим протягом десятиліть.

У теорії, якщо інформацію і процеси розуму можна відокремити від біологічного тіла, вони більше не будуть прив'язані до окремих меж і тривалості служби цього органу. Окрім того, інформація в мозку можу бути частково або повністю скопійована чи передана одному або кільком іншим субстратам (у тому числі для цифрового зберігання), отже, з механічної точки зору, відбудеться зниження або усунення «ризику смертності» такої інформації.

Супер-комп'ютер зможе моделювати людський мозок на рівні нервової системи і на більшій швидкості, ніж має біологічний мозок. До цього часу, транзистори досягнуть субатомних розмірів. До того ж, навіть якщо моделювання на таких швидкостях буде можливе, точну дату важко вирахувати через обмежене розуміння необхідної точності, і обчислювальна швидкість не єдина вимога для отримання максимально повної моделі людського мозку.

Враховуючи, що електрохімічні сигнали, які мозок використовує для досягнення думки, подорожують на швидкості близько 150 метрів в секунду,

в той час як електронні сигнали в комп'ютерах відправляються на 2/3 швидкості світла (триста мільйонів метрів в секунду), це означає, що електронний аналог людського біологічного мозку в теорії міг би думати в тисячі, а то й мільйони разів швидше. Зокрема, нейрони можуть генерувати максимум від 200 до 1000 потенціалів дії, в той час як тактова частота мікропроцесорів сягала 5,5 ГГц в 2013 році, що є швидше приблизно в п'ять мільйонів раз.

Відтак, людський мозок містить приблизно вісімдесят шість мільярдів нейронів із вісімдесятьма шістьма трильйонами синапсів їх з'єднань. Реплікація кожного з них у вигляді окремих електронних компонентів з використанням мікрочипів на основі напівпровідникової технології потребують комп'ютер, значно більший у порівнянні з сьогоднішніми супер-комп'ютерами.

Пам'ять нейрона, з областей із сірою речовиною мозку – це нейромедіаторна постсинаптична відповідь певної концентрації глутамату до сусідніх нейронів, що виникає при внутрішньойронній синхронізації візикул на відгук, що надходить від рецепторів даного нейрона, який у свою чергу відгукуються на нейромедіатор передсинаптичних нейронних зв'язків. Пам'ять нейрона здатна змінюватися, якщо нейрон зазнає змін у щільності глії, що оточує нейрон, за одночасного повторення величини передсинаптичного сигналу, якому піддається даний нейрон [3, с. 124].

Таким чином, пам'ять з оцифрованого мозку можна перенести спочатку лише в цифровому вигляді на диск, де він зберігатиметься до появи комп'ютерних програм аналізу оцифрованих зрізів мозку, тому що комп'ютер не здатний у принципі на повноцінне аналітичне мислення, як людський мозок, а лише на обробку інформації по заздалегідь створеному програмістами алгоритму. Ідея полягає в тому, що після сканування мікроскопом мікронних зрізах шарів мозку, отриманих нарізанням мозку на мікронні шари, створюється карта мозку з повним описом на ній щільності рецепторів на дендритах.

Узагальнюючи усе вищевикладене варто наголосити на тому, що точна комп'ютерна симуляція людського мозку дозволить вченим краще зрозуміти принципи, за якими він діє, і розібратися в механізмах розвитку психічних розладів серійних убивць для подальшого запобігання вчинення злочинів. Крім того, штучний аналог стане ідеальним об'єктом для випробувань нових методів розслідування злочинів. Однак складності сканування мозку наразі полягає в тому, що неможливо швидко здійснити аналіз нейронних мереж використовуючи сучасні комп'ютерні програми, адже/оскільки сучасні навіть гібридні штучні нейронні мережі не здатні працювати з великим обсягом даних, а сама карта мозку складається протягом 6 років. Тому без тимчасової заморозки мозку, під час процедури завантаження свідомості не обійтися, але можна не складати комп'ютерну карту мозку, а обійтися фотографіювання зрізів з мозку. Зберігання об'ємних фотографій зрізів з мозку, отриманих у

процесі фотографувань цих зрізів під різним кутом, дало можливість зберегти пам'ять мозку в хмарному сховищі чи на компактдиску. Потрібні мікроскопи, що спеціалізуються лише на вивченні мозку, потрібні програми, які вміють відділяти рецептори в цій каші/у цьому безладі/мішанині/суміші глії та нейронів і співвідносити їх з іншими зрізами, формуючи загальну картину розташування нейронів, аксонів, дендритів і тип нейронів, до яких належать рецептори.

Отже, немає особливої потреби виокремлювати тип рецептора, основне – визначити тип нейронів.

1. Koch, Christof; Tononi, Giulio (2008). Can machines be conscious?. *IEEE Spectrum* 45 (6): 55. URL : https://cutt.ly/mwGPQrvs (дата звернення 25.10.2023).

2. Кун Д. Основы психологии. Все тайны поведения человека. 10-е международное издание. СПб.: Прайм-Еврознак, 2005. 720 с.

3. Галян І. М. Психодіагностика. *Навчальний посібник*. Київ : «Академвидав». 2009. 463 с.

СОЛОП І. О.
курсант 3 курсу факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ МЕРЕЖ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Одним з ключових факторів для збільшення ефективності боротьби зі злочинністю є широке застосування передових досягнень науково-технічного прогресу, особливо в галузі інформаційних технологій, які останнім часом зробили значний прогрес. У сучасних умовах Національна поліція України не може успішно виконувати свої службові завдання без допоміжних видів діяльності, які не є безпосереднім об'єктом їхньої роботи, але необхідні для досягнення поставлених цілей [1, с.23].

Згідно зі статтею 25 Закону України «Про Національну поліцію», одним з таких видів діяльності є інформаційно-аналітичне забезпечення. Під цим терміном розуміється постійна робота з отримання інформаційних продуктів або надання інформаційних послуг.

Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система «Інформаційного порталу Національної поліції України» є функціональною підсистемою єдиної інформаційної системи Міністерства внутрішніх справ[2,с.105].

Необхідність інформаційно-аналітичного забезпечення випливає з інформаційної невизначеності окремих службових завдань Національної поліції України. Це означає, що поліцейські не мають достатньої інформованості про фактичний стан справ і оточуючу дійсність, що ускладнює вирішення окремих завдань їхньої службової діяльності.

Наприклад, на сьогоднішній день Національна поліція України не має доступу до інформаційних ресурсів митниці, які є необхідними для здійснення перевірок щодо законності перебування іноземців на території України або автомобілів із закордонною реєстрацією тощо.

Сучасні інформаційні технології надають працівникам правоохоронних органів можливість отримати багатоцільову довідкову, аналітичну та статистичну інформацію, що сприяє ефективному виконанню ними різноманітних оперативно-службових завдань.

Сучасні інформаційні технології є сукупністю методів, процесів і програмно-технічних засобів, що поєднані для збирання, обробки, зберігання, передачі, відтворення та використання інформації у потребах її користувачів. Основні види сучасних інформаційних технологій включають:

- технологію обробки даних;
- керування інформацією;
- технологію підтримки процесу прийняття рішень;
- технологію експертних систем [3, с.96].

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

1) вдосконалення форм та методів управління системами інформаційного забезпечення;

2) централізація та інтеграція комп’ютерних баз даних;

3) впровадження передових комп’ютерних інформаційних технологій для збереження кримінологічних та криміналістичних даних;

4) розбудова та широке використання потужних комп’ютерних мереж;

5) застосування спеціалізованих засобів захисту інформації;

6) налагодження ефективного обміну кримінальною інформацією на міжнародному рівні. Все це сприяє значному підвищенню рівня боротьби зі злочинністю.

Таким чином, всі системи інформаційного забезпечення, що використовуються в Національній поліції України, незалежно від їх архітектури та сфери застосування, зазвичай містять однаковий набір

компонентів: функціональні, організаційні та оброблення даних.

Використання інформаційно-аналітичних систем і технологій надає можливість Національній поліції України більш ефективно оптимізувати та раціоналізувати свої управлінські функції за допомогою сучасних засобів отримання, генерації, обробки та передачі інформації.

Для поліпшення якості та своєчасності виконання службових завдань поліцейськими важливо забезпечити більш ефективний обмін інформацією між Національною поліцією України та іншими органами, що підпорядковані центральним органам виконавчої влади.

1. Узлов Д.Ю., Струков В.М. Про новий підхід до взаємодії поліції з населенням на основі сучасних інформаційних технологій. «Сучасні проблеми правового, економічного та соціального розвитку держави» : тези доп. V Міжнародної науково-практичної конференції (м. Харків, 18 листопада 2016 року). МВС України, Харківський національний університет внутрішніх справ. Харків, 2016. 472 с. URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/ 2d0a051b-ce45-4531-8fdc-29e81826076f/content

2. Інформаційні технології : підруч. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніп- роп. держ. ун-т внутр. справ, 2021. 492 с. URL **:** http://er.dduvs.in.ua/handle/123456789/6820

3. Спеціальна техніка в правоохоронній діяльності: навч.посібник / Ю.П. Синиціна, С.О. Прокопов Е.В. Рижков. Дніпро: Дніпроп. Держ. Унтв. нутріш. справ, 2021. 96с. URL : https://er.dduvs.in.ua/handle/123456789/8735

СОЛОМИНА В. О.,
курсант 3 курсу факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Використання систем штучного інтелекту правоохоронними та судовими органами здатне забезпечити якісне оновлення їх діяльності. У зарубіжних країнах до практики правоохоронних органів впроваджені проекти, пов’язані із класифікацією та розпізнаванням об’єктів, розпізнаванням звукових сигналів (мови або, наприклад, системи визначення

пострілів). Запропоновані технічні рішення для аналізу великих обсягів даних на основі алгоритмів машинного навчання. У такий спосіб здійснюється аналіз відомостей про телефонні або інтерент-з'єднання, про використання платіжних систем тощо. Подібні рішення використовуються як потужні інструменти розслідування злочинів. Розробляються системи прогнозування злочинності та оцінки ризику індивідуальної протиправної поведінки на основі штучного інтелекту. [1].

Так використання штучного інтелекту надає Національній поліції України засоби для прогнозування та запобігання злочинам. Аналітика даних з використанням штучного інтелекту може допомогти у виявленні злочинних схем, прогнозуванні місць та часу вчинення злочинів і вчасного реагування на них [2]. Наразі штучний інтелект може допомогти в автоматичному аналізі великих обсягів даних, що допоможе у швидкому розслідуванні кримінальних справ та ідентифікації злочинців.

Упровадження штучного інтелекту в роботу Національної поліції України також може поліпшити оперативне реагування на події. Системи автоматичного розпізнавання образів можуть допомогти у виявленні автомобілів, які були викрадені або пов'язані зі злочинами. Зокрема, штучний інтелект може бути використаною для аналізу відео- та аудіоматеріалів, що допоможе у швидкому знаходженні та арешті підозрюваних осіб.

Національна поліція України може використовувати штучний інтелект для покращення системи контролю. Автоматизовані системи можуть допомогти у моніторингу та аналізі соціальних мереж з метою виявлення та запобігання поширенню нелегальної та шкідливої інформації. Крім того, використання штучного інтелекту може сприяти виявленню організованої злочинності та боротьбі зі зловживаннями у сфері фінансів.

Із використанням штучного інтелекту в роботі Національної поліції України виникають етичні проблеми, пов'язані зі збором та аналізом особистих даних. Однак, ці проблеми можуть бути вирішені за допомогою правових норм та процедур, що забезпечують конфіденційність і захист особистих даних. Реалізація таких норм і забезпечення етичної та прозорої роботи систем Штучний інтелект є важливим аспектом розвитку та використання штучного інтелекту у роботі Національної поліції України.

Можна зробити такі висновки, що використання штучного інтелекту в роботі Національної поліції України є важливою та перспективною ініціативою, яка може привести до покращення безпеки громадян, підвищення ефективності оперативного реагування, поліпшення системи контролю та забезпечення етичних стандартів та конфіденційності. Штучний інтелект може сприяти підвищенню ефективності Національної поліції та усуненню різних викликів, що виникають у сучасному суспільстві. Однак, для успішної реалізації цієї ініціативи необхідно розробити законодавчу базу, яка врегулює використання штучного інтелекту та забезпечить захист прав та

свобод громадян.

1. Штучний інтелект та протидія злочинності. Сайт професора Карчевського. URL : https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://karchevskiy.com/2020/11/06/ai-vs-crime/&ved=2ahUKEwidz4DzlIyAAxXY_7sIHYrsCUUQFnoECCYQAQ&usg=AOvVaw2KXzZu0pqZ1rreqL4y45d0

2. Шевчук Т.А., Свистун Я.В. Використання штучного інтелекту у протидії злочинності. Вісник кримінологічної асоціації України. 2021. № 2 (25) URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/26d850e6-49ce-4cc6-bf59-a0f14b6b4d40/content

ТАРАСЮК Д. О.,
курсант 3 курсу факультету
підготовки фахівців для підрозділів
кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

КІБЕРБЕЗПЕКА КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Із поширенням інформаційних технологій та цифрової трансформації суспільства зростає значення кібербезпеки. Комп'ютерні системи та мережі стають невід'ємною частиною нашого повсякденного життя, використовуються у сфері бізнесу, уряду, охорони правопорядку та багатьох інших галузях. Проте, ця цифрова залежність приносить і нові виклики, пов'язані зі збільшенням кількості кібератак, крадіжок даних та порушенням приватності. Розглянемо виклики, з якими стикається сучасна кібербезпека, та стратегії, які науковці в інформаційних технологіях використовують для захисту від цих загроз. [1]

Сучасні кібератаки стають все більш складними та витонченими. Злочинці використовують різноманітні методи, такі як фішинг, введення в оману користувачів, вразливості програмного забезпечення та атаки на мережеві інфраструктури. Кіберзагрози можуть походити як від окремих хакерів, так і від організованих груп або навіть державних структур. Виклик полягає в тому, щоб забезпечити ефективний захист від таких широкомасштабних і різноманітних атак.

Навіть найбільш технологічно продумані системи можуть стати жертвами соціальної інженерії. Кіберзлочинці використовують психологічні методи для маніпулювання користувачами та здійснення атак. Фішингові електронні листи, шахрайські дзвінки та соціальні мережі є засобами, якими злочинці намагаються отримати конфіденційну інформацію або навіть переконати людей здійснити певні дії, які можуть веде до порушення безпеки. [2]

Злочинці постійно шукають нові способи атаки, щоб уникнути виявлення та захисту. Вони активно використовують розробки в галузі штучного інтелекту, машинного навчання та автоматизації для створення більш складних та непередбачуваних кіберзагроз. Наприклад, атаки з використанням штучного інтелекту можуть автоматично адаптуватись до захисних заходів та швидко знаходити нові уразливості. [3]

Освіта та підвищення свідомості про кібербезпеку є першим кроком у захисті від кіберзагроз. Користувачі повинні бути навчені розпізнавати фішингові атаки, використовувати сильні паролі, оновлювати програмне забезпечення та дотримуватися основних правил безпеки в Інтернеті.

Використання сучасних технологій безпеки: Застосування передових технологій інформаційної безпеки, таких як антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень та шифрування даних, є необхідною умовою для захисту від кібератак.

Розробка та впровадження стандартів безпеки: розробка та впровадження стандартів безпеки в галузі інформаційних технологій є важливим кроком у забезпеченні кібербезпеки. Це включає стандартизацію процесів розробки програмного забезпечення, аудиту безпеки та захисту даних.

Розробка систем моніторингу та виявлення кіберзагроз є важливою стратегією кібербезпеки. Ці системи виявляють незвичайну активність, аномальні зміни в мережі та інші показники, що можуть свідчити про потенційні атаки. Вони дозволяють реагувати на загрози швидко і ефективно.

Постійне оновлення та підвищення безпеки: кіберзагрози постійно змінюються, тому важливо постійно оновлювати та підвищувати безпеку інформаційних систем. Це включає оновлення програмного забезпечення, виявлення та виправлення вразливостей, а також стеження за новими трендами та інноваціями в галузі кібербезпеки.

Отже, кібербезпека користувачів комп’ютерної техніки в епоху цифрової трансформації стає все більш важливою задачею. Виклики, пов’язані зі зростанням кількості та складності кібератак, недостатньою кібербезпекою в Інтернеті речей, соціальною інженерією та розробкою інноваційних кіберзагроз, вимагають комплексного підходу та стратегій кібербезпеки. Для ефективного захисту інформаційних технологій в епоху цифрової трансформації, необхідно поєднувати технічні, організаційні та освітні заходи.

1. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. 2022. № 1 (84). С. 13–20. URL : https://doi.org/10.26906/EiR.2022.1(84).2540.

2. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. Інформаціяіправо. 2018. No 1(24). С. 127-132. URL : http://nbuv.gov.ua/UJRN/Infpr_2018_1_15

3. Гуцалюк М. В. Окремі аспекти боротьби з організованою кіберзлочинністю. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук.-практ. конф. (м. Київ, 4 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 199-201. URL : https://academy.ssu.gov.ua/uploads/p_57_54325835.pdf

ТИХЕНКО Я. В.
курсант 3 курсу факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ОРГАНІЗАЦІЯ БОРОТЬБИ З ІНФОРМАЦІЙНИМИ ЗАГРОЗАМИ ПІД ЧАС ВІЙСЬКОВИХ ДІЙ

З 24 лютого 2022 року, російська Федерація вторглася на територію України, порушуючи її незалежність, суверенітет та правовий статус. Паралельно з цією агресією розпочався новий етап інформаційної війни. Україна бореться з російськими наративами, пропагандою та повною дезінформацією вже з 2014 року, але сьогодні ця проблема стає ще більш актуальною й загостреною [1] .

Інформаційна війна – це стратегічна та цілісна сукупність дій, спрямованих на досягнення інформаційної переваги в рамках національної військової стратегії. Її основна мета полягає у впливі на інформацію та інформаційні системи супротивника, одночасно зміцнюючи та захищаючи власну інформацію та інформаційні системи.

Ця концепція, яка часто приписується командувачу інформаційних військ США, визнає важливість і цінність інформації в плануванні, управлінні та виконанні військових операцій, а також реалізації національної політики. Інформаційна війна використовує всі можливості та націлена на вразливі фактори, які виникають через залежність від інформації [2].

Отже, інформаційна війна – це комплексна стратегія, спрямована на ефективне використання інформаційних ресурсів для досягнення своїх військових та політичних цілей, включаючи вплив на опонента, захист власної інформації та забезпечення національної безпеки.

Упродовж періоду з 2014 до 2022 року пропагандистська «машина Кремля» активно працювала на формування підґрунтя для вторгнення на територію України. Вона створювала інструменти, які виправдовували дії росії на міжнародній арені та блокували потік інформації з зовнішнього європейського та американського світу для російських громадян. Усі ці кроки були і залишаються частиною інформаційної війни.

Ця інформаційна війна стимулювала в громадян та військовослужбовців російської Федерації ідеї проведення так званих «спеціальних операцій» та «денацифікації та демілітаризації» України. Це дозволило формувати певну думку серед російських громадян і військових про необхідність здійснення таких дій.

В інформаційній війні можна виділити три основні цілі:

1. Контроль інформаційного простору та захист власної інформації від ворожих дій. Це означає забезпечення контролю над потоком інформації, що поширюється в медіа та онлайн, а також захист власних інформаційних ресурсів від несанкціонованого доступу та кібератак.

2. Використання контролю над інформаційним простором для проведення інформаційних атак на противника. Це передбачає розповсюдження пропагандистської інформації, дезінформацію, маніпуляцію інформацією, створення фейкових новин та інших методів, що спрямовані на вплив на думку та переконання опонента, дискредитацію або зменшення довіри до противника.

3. Підвищення загальної ефективності збройних інформаційних функцій. Це також використання інформаційних ресурсів та технологій для покращення комунікації, координації та співпраці внутрішніх військових структур, підвищення свідомості та тренування військових осіб з питань кібербезпеки, інформаційної аналітики та електронної війни.

Отже, основні цілі в інформаційній війні полягають у контролі інформаційного простору, проведенні інформаційних атак на противника та підвищенні ефективності інформаційних функцій військових структур.

Україна вирішила передати свої тактики кібернаступу користувачам мережі, створивши «ІТ-армію» хакерів, які активно беруть участь у цифровій боротьбі з російськими організаціями. Навіть до масових кібератак, за якими Росія стала відомою, українські кібер- та інформаційні професіонали вже вели цифрову війну. Вони здійснювали атаки на офіційні російські веб-сайти, збирали розвідувальні дані, протидіяли дезінформації та поширювали загальні повідомлення.

Одним із недавніх прикладів активності на кібер-фронті був злам російського веб-сайту з метою опублікування статті з посиланням на

російське міністерство оборони, у якій повідомлялось про втрати російської армії. Згідно з цим повідомленням, близько 20 000 російських солдатів було вбито, а понад 20 000 отримали поранення [3].

Ці дії свідчать про активну роль українських хакерів у проведенні кібератак та інформаційних операцій проти російських цілей.

У сучасному світі кіберпростір є полем битви, де проводяться кібератаки, крадіжки даних, дезінформаційні кампанії та інші злочинні дії. Це ставлять під загрозу не лише комп'ютерні системи і мережі, але й нашу приватність, економічну безпеку, національну обороноздатність та навіть демократичні процеси. У зв'язку з цим, важливо мати науковий підхід до розуміння цієї проблематики та пошуку рішень для захисту в кіберпросторі.

Також значущим аспектом цієї проблематики є розуміння та аналіз кібератак, що дає змогу прогнозувати нові загрози та розробляти ефективні заходи для їх запобігання. Також важливо досліджувати технологічні вразливості інформаційних систем та розробляти методи їх усунення або компенсації.

Одним із основних напрямків нашої роботи є розробка інноваційних методів виявлення та відповіді на кібератаки. Це включає в себе використання штучного інтелекту, машинного навчання та аналізу великих обсягів даних для виявлення незвичайних активностей, аномалій і підозрілих з'єднань в мережі.

Після оцінки ситуації, можна зробити висновок, що інформаційна війна, що розгортається російською Федерацією проти України, є складовою частиною загальної агресії, спрямованою проти українського народу та світового співтовариства загалом. Незважаючи на те, що пропагандистські та дезінформаційні дії з боку росії впливають на їх внутрішній простір, варто відзначити, що Україні вдається давати відсіч на інформаційному фронті.

Наразі питання боротьби та забезпечення безпеки в контексті інформаційної війни стали надзвичайно актуальними. У сучасному світі інформація поширюється надзвичайно швидко, і дезінформувати населення стало надзвичайно просто. Ворог намагається відвернути увагу суспільства та всього світу від реальної ситуації в Україні за допомогою масового поширення фейкових новин та пропаганди [2].

Для забезпечення якісного захисту інформаційного простору України, потрібно вживати заходи на законодавчо-нормативному рівні. Знищення таких складових інформаційної війни, як маніпуляції, фейки та пропаганда, має стати пріоритетом на найвищому рівні державного регулювання. Такі заходи допоможуть забезпечити якість інформаційного простору, захистити населення від маніпуляцій і зберегти національну безпеку.

---

1. Щеголь, А. В. Інформаційна війна в умовах міжнародного збройного конфлікту на території України, викликаного агресією російської федерації. *конференції «Актуальні проблеми соціальних комунікацій» 30 травня 2022 р.*, 138. URL : https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved

=0CAIQw7AJahcKEwiYqf6yz42AAxUAAAAAHQAAAAAQAw&url=https%3A%2F%2Fjrnl.nau.edu.ua%2Findex.php%2FUV%2Farticle%2Fview%2F15596%2F22843&psig=AOvVaw2aFMmjTFIVEogtEozz7Dnd&ust=1689404248043327&opi=89978449

2. Brzhevska, Z., Dovzhenko, N., Kyrychok, R., Gaidur, G., & Anosov, A. (2019). Інформаційні війни: проблеми, загрози та протидія. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(3), 88- 96. URL : https://doi.org/10.28925/2663-4023.2019.3.8896**.**

3. М. П. Требін. Феномен інформаційної війни у світі, що глобалізується. М. П. Требін. 2013. URL : https://lib.nadpsu.edu.ua/eldocs/BooksShow4/Vnyua_2013_2_24.pdf**.**

ТІТОВА А. С.,
курсантка 3 курсу факультету
підготовки фахівців для підрозділів
кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ПІД ЧАС ВОЄННОГО СТАНУ

Останній період часу в Україні характеризується швидким розвитком інформаційних технологій, що невід'ємно пов'язаний з збільшенням кількості кіберзлочинів. Кіберзлочини стали найбільш динамічною та небезпечною групою протиправних діянь, оскільки з кожним роком вони стають все поширенішими та загрозливішими.

Хоча терміни «кіберзлочинність» та «комп'ютерна злочинність» часто використовуються як синоніми, вони мають свої відмінності. «Кіберзлочинність» є більш широким поняттям, яке точніше відображає природу злочинності в інформаційному просторі. У той час як «комп'ютерна злочинність» обмежується злочинами, вчиненими за допомогою комп'ютера.

Мережа Darknet стала відомим явищем, де злочинці знаходяться і створюють чорний ринок для торгівлі наркотиками, зброєю, краденими товарами та іншими незаконними продуктами. Однак, законодавство не встигає за розвитком технологій, що сприяє поширенню кіберзлочинності [1].

Україна має правову базу для забезпечення інформаційної безпеки, у складі якої включає Конституцію, Кримінальний кодекс, закони про кібербезпеку, інформацію, захист інформації в інформаційно-телекомунікаційних системах, національну безпеку та інші. Зокрема, існують

доктрина інформаційної безпеки та міжнародні договори, які регулюють кіберзлочинність і які Україна прийняла.

Стратегія кібербезпеки України підкреслює, що безпечний кіберпростір є ключовим для успішного розвитку країни. Забезпечення кібербезпеки визначається як пріоритетна мета національної безпеки України. Заходи з підвищення кібербезпеки передбачають зміцнення потужностей національної системи кібербезпеки для протидії сучасним кіберзагрозам [2].

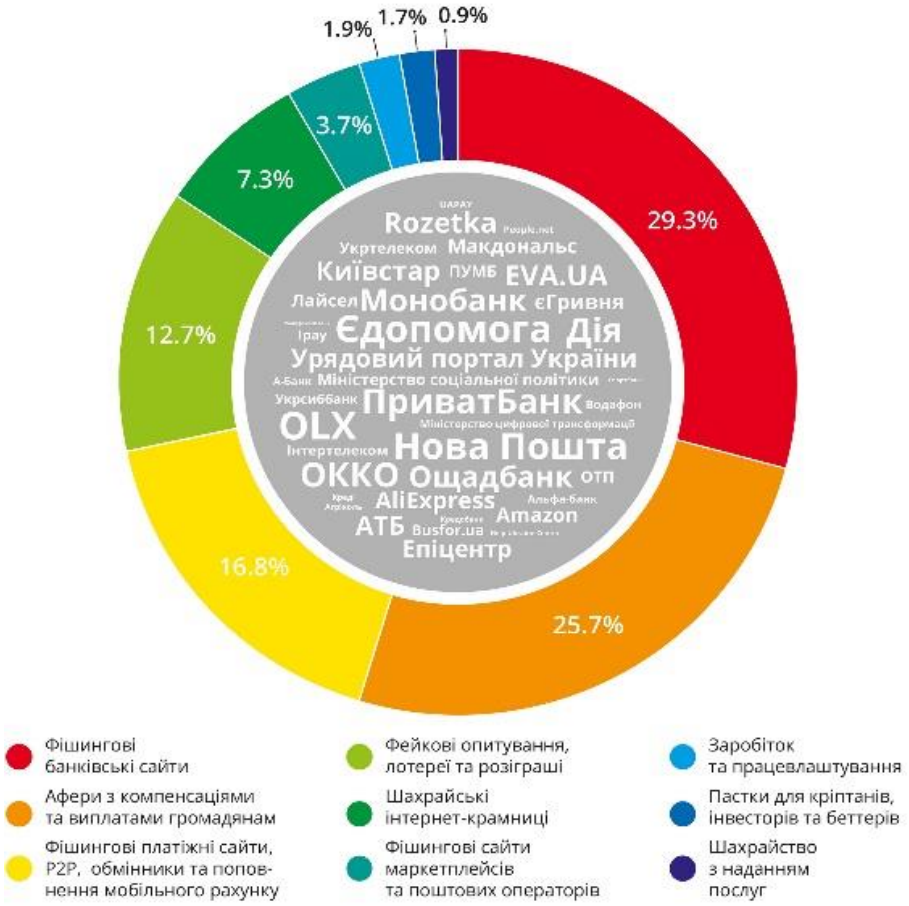

Рис. 1. Види кіберзлочинів в Україні станом на 2022 рр.

З огляду на виклики та загрози в кіберпросторі, роль кібербезпеки стає критично важливою в процесах цифрової трансформації країни. Оскільки все більше послуг та покупок здійснюються онлайн, зростає кількість випадків шахрайства в Інтернеті стосовно громадян. Використання сучасних інформаційних технологій та безготівкових розрахунків полегшує життя як громадянам, так і зловмисникам, які вигадують нові схеми для шахрайства та обману довірливих людей. Наведемо статистику кіберзлочинів за 2022 рік (рис. 1):

Щоб захистити себе від шахрайства, слід дотримуватися простих

рекомендацій. Важливо не розголошувати інформацію про свою платіжну карту та персональні дані, і уникати передачі банківської картки постороннім особам для оплати товарів або послуг. Під час здійснення покупок в Інтернеті краще сплачувати за товар після його отримання та уникати передоплати. Також слід здійснювати платіжні операції лише на «захищених» сайтах, адреса яких починається з «https»[3].

Не рекомендується здійснювати покупки, оплачувати комунальні послуги або входити в онлайн-банкінг за допомогою Wi-Fi в публічних місцях. Важливо встановити складний пароль для інтернет-банкінгу і уникати використання персональної інформації в паролі. Корисним буде підключення SMS-інформування для отримання повідомлень про операції з платіжними картками та утримуватися від переходу за сумнівними посиланнями, які надходять у повідомленнях. Особливо важливо ігнорувати будь-які повідомлення про виграші.

Підводячи підсумок можна сказати, що кіберзлочинність являється наслідком глобалізації інформаційних процесів, а отже, вона становить основну загрозу для соціогуманітарних та інших компонентів. У контексті гібридної війни та широкого використання засобів масової інформації та комунікацій, особливо важливим стає попередження основних загроз, пов’язаних з кіберзлочинністю.

1. Кіберзлочинність: проблеми боротьби і прогнози. URL : http://anticyber. com.ua/article_detail.php?id=140.

2. Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted. Statista. URL : https://www.statista.com/statistics/991304/ worldwidecybersecurity-spending/.

3. Юлія Газізова. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL : https://uz.ligazakon.ua/ua/magazine_article/EA013606.

ТОПЧІЙ К. К.,
курсантка 3 курсу факультету
підготовки фахівців для підрозділів
кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

Успіх будь-якої діяльності, у тому числі правоохоронних органів, багато в чому залежить від того, наскільки вона спирається на знання дійсного стану, структури та динаміки суспільних відносин, що сприяють та перешкоджають причинам та умовам, процесам та явищ, що відбуваються у цій сфері. Недарма фахівці в сфері управління зазначають, що координація забезпечує цілісність та стійкість управління діяльністю, що неможливо як без достовірної інформації, так і без її аналітичної обробки.

Окремі аспекти правового регулювання аналітичної діяльності стали об'єктом наукового дослідження таких учених, як С. Алексєєв, Ф. Брецко, В. Горшенєв, О. Зайчук, В. Копєйчиков, С. Лисенков, Ю. Максименко, М. Марченко, Н. Оніщенко, П. Рабінович, О. Скакун та ін.

У діяльності поліції переломлюється інформація соціального характеру, що обумовлено областю та специфікою самої поліції. Інформація складається насамперед у змістовній характеристиці різноманітних відомостей про явища, факти, події, значимих у житті. Інформація виступає як основний предмет діяльності і, по суті, характеризує її результати. Наразі соціальна інформація, яку використовують поліція, включає, з одного боку, відомості, які можуть бути отримані в результаті дослідження навколишньої дійсності та долучені до вже існуючої об'єктивної системи знань про оперативну обстановку відповідної території, а з іншого – бути об'єктом пошуку, виробленого конкретним органом задля досягнення його цілей [1]. Не знаючи реального стану справ на місцях, не можна оперативно керувати силами та засобами, своєчасно надавати допомогу підлеглим структурам, впливати на організацію діяльності та кінцеві результати роботи. І чим складніша оперативна обстановка, динамічніші соціально-економічні та демографічні процеси, що відбуваються, тим вищі вимоги до інформації та її аналізу. Без достовірної та повної інформації, всебічного та глибокого її вивчення не може нормально функціонувати жоден управлінський апарат.

Обґрунтованість та ефективність його рішень перебувають у прямій залежності від стану інформаційно-аналітичної роботи.

З метою організації інформаційно-аналітичної підтримки поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України». Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичної підтримки [2 с. 105].

Розпорядником системи «Інформаційний портал Національної поліції України» є Національна поліція України, який вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи. Адміністратором системи Інформаційного порталу Національної поліції України є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України, який забезпечує:

- вирішення організаційних питань щодо забезпечення функціонування системи;
- ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється;
- захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації [2 с. 107];

Функціонування інформаційної системи поліції забезпечується інформаційним забезпеченням, під яким розуміється діяльність з розробки, організації функціонування та вдосконалення інформаційних систем, спрямована на організацію забезпечення суб’єкта сукупністю відомостей як систематизованої інформації, необхідної йому реалізації покладених на нього завдань та функцій процесу управління.

Слід зазначити, що вирішення завдань пошуку, відбору та систематизації інформації, необхідної правоохоронним органами у процесі виконання поставлених перед ними завдань, передбачає використання інтегрованої інформаційної системи, можливості якої дозволяють суттєво розширити інформаційну базу, необхідну для інформаційно-аналітичного забезпечення, знизити витрати часу на пошук та відбір вихідної інформації, своєчасно визначати аспекти, за якими слід проводити аналіз інформації, а основне – у процесі аналітичної обробки даних забезпечити виявлення сутності та динаміки просторово-часових та причинно-наслідкових зв’язків між досліджуваними фактами, явищами, процесами [3]. У результаті спочатку наявні дані перетворюються на нову, вивідну інформацію, яка дозволяє готувати пропозиції щодо нейтралізації кримінальних загроз, приймати обґрунтовані оперативні та управлінські рішення, готувати плани

дій, правильно розподіляти сили та засоби, здійснювати координацію та взаємодію.

Інформаційно-аналітична діяльність є цілісною частиною відомчого механізму управління правоохоронними органами, що проявляється у наявності єдиних цілей, єдиного комплексу функцій, єдиних основних методів їх реалізації, єдиного класу об'єктів управління, у існуванні стійких зв'язків між елементами середовища, при переважанні внутрішніх зв'язків над зовнішніми, що забезпечує відносну автономність системи. Як невід'ємний елемент управлінської діяльності, вона має бути спрямована на досягнення конкретних результатів, до яких можна віднести насамперед забезпечення дотримання режиму законності та правопорядку в суспільстві [4].

Таким чином, інформаційно-аналітичне забезпечення діяльності поліції є системою, що включає в себе два взаємопов'язані компоненти. Перший – це інформаційне забезпечення, що полягає у вивченні інформаційного попиту споживачів, підтримці сталого стану інформаційних зв'язків, збиранні, накопиченні, обробці, зберіганні та видачі інформації споживачам у максимально короткі терміни. Другий – аналітичне забезпечення, що полягає у дослідженні кримінальних загроз, виявленні причин та умов, що впливають на формування обстановки, прогнозування її розвитку, вивчення проблемних ситуацій у сфері забезпечення законності та правопорядку в суспільстві. Кінцевою метою реалізації двох вищезгаданих складових інформаційно-аналітичного забезпечення є створення умов для реалізації завдань забезпечення режиму законності та правопорядку у суспільстві.

1. Сурмін Ю. П. Аналітика державного управління: сутність і тенденції розвитку. URL : http:// www. academy.gov.ua/ej/ej5/txts/06sypdsv.htm.

2. В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Інформаційні технології : підруч. Дніпро : Дніп-роп. держ. ун-т внутр. справ, 2021. 492 с. URL : https://er.dduvs.in.ua/handle/123456789/6820

3. Аналітична складова інформаційної діяльності: уточнення сутності, ознак і процесів / Л. Я. Філіпова, І. В. Захарова // Вісник ХДАК. Випуск 28. С. 44–52. URL : https://periodica.nadpsu.edu.ua/index.php/legal/article/view/327

4. Телешун С. О. Основи інформаційно-аналітичної діяльності в публічному управлінні : навчальний посібник / С. О. Телешун. Київ : НАДУ. 2021. 168 с. URL : https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/39122/1/52%20 Metod._КАФЕДРА-ТокарМ-текст-21.pdf

ТІЦЬКА І.Г.,
курсантка 3 курсу факультету
підготовки фахівців для підрозділів
кримінальної поліції
Науковий керівник:
ПРОКОПОВ Сергій
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНІЧНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Впровадження систем відеоспостереження має значний вплив на рівень злочинності в країні і сприяє створенню безпечних умов для громадян. Це сприяє організації безпечного середовища, профілактиці правопорушень та їх розкриттю.

Наявність і використання систем відеоспостереження сприяють позитивній динаміці у розкритті злочинів та запобіганні правопорушенням у всіх напрямках. Наприклад, тільки протягом 2022 року у місті Києві було розкрито понад 3500 правопорушень завдяки використанню відеокамер. Встановлення системи відеоспостереження сприяло зниженню загального рівня злочинності у публічних місцях, де вони були впроваджені, на понад 60% [1].

Однак на сьогоднішній день в Україні не існує єдиної системи відеоспостереження. В різних областях країни та в структурних підрозділах Національної поліції України діють незалежні системи відеоспостереження, які часто використовують застарілі технології та обладнання [2, с. 27].

Національна поліція України використовує різні засоби відеоспостереження, такі як портативні відеореєстратори, системи встановлені на службових транспортних засобах, автомобільні системи, стаціонарні системи та навіть засоби відеозапису на безпілотних літальних апаратах (БпЛА). Патрульна поліція України також використовує нагрудні відеокамери (відеореєстратори), системи встановлені на службових транспортних засобах та стаціонарні системи відеоспостереження [3].

Впровадження та розвиток систем відеоспостереження в Україні є важливим кроком для забезпечення безпеки громадян та боротьби зі злочинністю. Необхідно зосередити зусилля на створенні єдиного та сучасного інтегрованого підходу до системи відеоспостереження, щоб забезпечити ефективну роботу поліції та забезпечити безпеку громадян у всіх

регіонах країни.

Управління діями патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби, відомої як «ЦУНАМІ» . Ця система містить/має стаціонарну систему відеоспостереження, що забезпечує швидкий візуальний контроль за основними злочинними місцями, вулицями, майданами, транспортними потоками та охоронюваними об'єктами. Інформація, отримана з систем відеоспостереження, дозволяє старшому черговому слідкувати за оперативною ситуацією та коригувати роботу нарядів поліції. Зокрема, вона може використовуватись для надання вказівок під час переслідування підозрюваних. Записані дані можуть бути використані як докази під час розслідування злочинів.[3]

В Інформаційній підсистемі «Гарпун» ІПНП ведеться облік відомостей про транспортні засоби та їх державні номерні знаки, які розшукуються у рамках кримінального, адміністративного або виконавчого провадження, а також у рамках оперативно-розшукової діяльності. Система «Гарпун» виявляє використання одного номерного знака на різних транспортних засобах, виявлення фактів використання пошкоджених номерних знаків і автоматичного повідомлення про ці факти черговим диспетчерам патрульної служби. «Гарпун» є підсистемою інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» і постійно оновлюється новою інформацією. Нажаль, система «Гарпун» не може виявляти реєстраційний номер, вид, марка, модель та колір транспортного засобу, яким незаконно заволоділи,чи який покинув місце дорожньо-транспортної пригоди. [4, с. 194].

Однією з найсучасніших систем відеоспостереження, які були впроваджені в Україні, є UASC, що належить до Єдиного аналітичного сервісного центру Головного управління Національної поліції в Донецькій області . В UASC вже використовуються інтелектуальні відеокамери, що представляють собою окремий апаратно-програмний комплекс. Вони можуть діяти самостійно або в межах внутрішньої підмережі з подібними комплексами. Камера має вбудовані аналітичні функції, що використовують програмні датчики руху, функції інфрачервоного спостереження, вимірювання швидкості та інші детектори, які можуть викликати тривогу. Крім того, камера передає відеопотік до головного центру UASC, де проводиться глибокий аналітичний аналіз.[3]

Отже, один із найважливіших пріоритетів подальшого розвитку Національної поліції України – створення єдиної системи відеоспостереження та відеоаналітики в Україні. Ця система є важливою умовою для ефективного функціонування і передбачає оновлення і розгортання нових «розумних» систем відеоспостереження. Основним чинником для існування і подальшого розвитку цієї системи є використання штучного інтелекту з використанням нейронних мереж.

Під час будівництва систем відеоспостереження в країні потрібно враховувати світові тенденції їх розвитку, спрямовані передусім на попередження злочинів, а потім на їх реєстрацію. Тому варто використовувати системи штучного інтелекту, що виявлятимуть поведінкові аномалії людей, реєструватимуть мікрорухи і аналізуватимуть психологічний стан на їх основі.

Це дозволить отримати інформацію про особу, яка наміряє вчинити злочин. Зокрема, системи штучного інтелекту повинні мати здатність здійснювати біометричне розпізнавання осіб, фіксувати появу і зникнення предметів, розпізнавати державні номери автомобілів, визначати їх тип, марку і колір, фіксувати маршрути їх руху. За допомогою аналізу цих факторів можна проводити розшук підозрюваних і автомобілів на території міста та інше.

1. Deng I. This state-backed AI unicorn has helped Chinese police arrest 10,000 criminals // South China Morning Post : сайт. 28.03.2019. URL : https://www.scmp.com/tech/start-ups/article/3003686/ state-backed-ai-unicorn-has-helped-chinese-police-arrest-10000

2. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : метод. матеріали для працівників підрозділів поліції МВС України / В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов та ін. Харків : Харків. нац. ун-т внутр. справ, 2020. 44с. URL : https://dspace.univd.edu.ua/items/ae7803e4-c7b6-4caa-bb32-9a64e0873190

3. Пефтієв О. В. Єдиний аналітичний сервісний центр Головного управління Національної поліції в Донецькій області // Актуальні питання забезпечення публічної безпеки, порядку в сучасних умовах: поліція та суспільство – стратегії розвитку і взаємодії : тези доп. Всеукр. наук.-практ. конф. (м. Маріуполь, 12 трав. 2018 р.) / МВС України, ДВНЗ «Приазовський державний технічний університет». Маріуполь, 2018. С. 345–351. URL : https://univd.edu.ua/science-issue/issue/3956

4. Інформаційні технології : підруч. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніп- роп. держ. ун-т внутр. справ, 2021. 492 с. URL : http://er.dduvs.in.ua/handle/123456789/6820

ПЕТРУШИН Олексій
курсант 2 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
СИНИЦІНА Юлія
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

НОВІТНІ ЗАСОБИ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

У наш час важко уявити ефективну протидію злочинності без використання поліцією спеціальної техніки та сучасних інформаційних технологій. До популярних технічних засобів, які зараз активно впроваджуються вдіяльність поліції багатьох країн світу, у тому числі в Національній поліції України, можна віднести [1]:

1) безпілотні літальні апарати, які в останні роки почали активно використовуватися правоохоронними органами багатьох країн світу для:

– спостереження;

– збирання доказів;

– контролю за натовпом;

– відслідковування біженців;

2) GPS-трекери, що за допомогою супутникової навігації передають через мобільний зв'язок дані на сервер про місцезнаходження певного рухомого об'єкту. За допомогою цього сучасного приладу поліція має змогу:

– відслідковувати злочинців;

– здійснювати моніторинг за правильним виконанням працівниками поліції покладених на них обов'язків;

– координувати та відслідковувати місцезнаходження працівника поліції та їх транспортні засоби в режимі реального часу;

– встановлення місця перебування вкраденого транспорту;

3) системи виявлення вогнепальної зброї, які, використовуючи звуковідатчики та відеокамери, надають змогу працівникам поліції швидко виявляти та реагувати на випадки застосування вогнепальної зброї.

Дослідженням актуальних питань у сфері використання безпілотних літальних апаратів підрозділами Національної поліції України під час виконання спеціальних завдань присвячено певна кількість наукових робіт видатних вчених, таких як: Головань О.М., Грідіна К.О., Кузьменко Є.В.,

Глотов В.М., Трубніков Г.В., Мовчан А.В. [2] та інших.

У наукових працях розглядаються наступні актуальні питання:

– перспектива використання БПЛА для виконання завдань у військовій сфері;

– аспекти використання безпілотних комплексів для ведення різного виду моніторингу;

– організаційно-правові засади використання безпілотних літальних апаратів у діяльності правоохоронних органів;

– аналіз нормативних актів, що регулюють застосування безпілотних літальних апаратів у діяльності Національної поліції України і т. інш.

В Україні поліцейські для забезпечення публічного порядку під час проведення масових заходів можуть застосовувати сучасний гелікоптер та спеціально обладнані автомобілі. Вони обладнані спеціальною відеоапаратурою, що має можливості фіксації правопорушень та оперативної передачі інформації до Ситуаційних центрів Національної поліції. Спеціально укомплектованіавтомобілі розміщувалися неподалік масового скупчення громадян, що дозволило досконало володіти обстановкою та миттєво реагувати на будь-які події.

Україна також не відстає в інтеграції новітніх інформаційних технологій у діяльність правоохоронних органів, утому числі у діяльність Національної поліції України. У зв’язку з тим, що у діяльності поліції одну знайважливішихролей відіграє інформація (накопичення банків даних, їхобробка та аналіз), останнім часом в діяльність поліції починають активно впроваджувати хмарні технології обробки інформації. Сучасні інтернет-технології дозволяють швидконадати доступ до центральної системи обробки та зберігання інформації, що знаходиться у «хмарі», з будь-якої частини світу, що у свою чергу дає змогу поліцейському швидко реагувати на надзвичайні події, які виникли і були зафіксовані шляхом відеофіксації, направляти на місця виникнення надзвичайної ситуації відповідні сили ізасоби.

Отже, з вище наведеного можна зробити висновок, що застосування новітніх засобів спеціальної техніки та технологій у діяльності правоохоронних органів допомагає забезпечувати безпеку населення на більш вищому рівні та зробити діяльність поліції більш ефективною.

1. Мовчан А.В. Використання безпілотних літальних апаратів у діяльності правоохоронних органів. Мовчан М.А. Соціально-правові студії Науково-аналітичний журнал, Львів – 2020. Випуск 3 (9). С. 104–110

2. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності Навч. посібн. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с. URL : https://er.dduvs.in.ua/handle/123456789/8735

КАДІРОВА Аріна,
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
СИНИЦІНА Юлія,
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПОТРЕБА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Упровадження інформаційних технологій у діяльність Національної поліції України має ключове значення для покращення ефективності роботи та забезпечення високого рівня обслуговування та безпеки громадян.

Серед українських дослідників проблеми інформаційного забезпечення Національної поліції України ми виділяємо науковий внесок В. Антоненка, В. Вишні, Л. Гліненко, О. Комісарова, І. Краснобрижого, М. Криштановича, С. Мамченка, В. Мирошниченка, Н. Морзе, В. Павлиша, Ю. Синиціна, Ю. Рогушиної, І. Шевчука та інших. Однак динаміка сучасного розвитку всього інформаційного суспільства, зокрема і діяльності Національної поліції України, змушує нас поглиблювати дослідження цієї проблеми, яка недостатньо проаналізована в науковому співтоваристві.

Відповідно до Закону України «Про Національну програму інформатизації» – інформаційно-комунікаційні технології – результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг [1].

Нижче наведемо деякі аспекти, що демонструють потребу застосування інформаційних технологій у поліційній діяльності:

1. Електронний звіт та аналітика:

Можливість ведення електронних звітів поліцейськими спрощує збір і аналіз статистичних даних, що може використовуватися для планування стратегій безпеки.

Електронний звіт та аналітика в поліції відіграють ключову роль у забезпеченні ефективності та прозорості правоохоронної діяльності. Електронний звіт та аналітика включають в себе: автоматизацію збору даних; аналіз та прогнозування; планування стратегій безпеки; взаємодію з

громадськістю; кыбербезпеку;

Автоматизація збору даних: електронні системи дозволяють поліції автоматизувати процес збору різноманітних статистичних даних, включаючи злочини, інциденти, затримання та інші події. Це спрощує рутинні завдання з введення та обробки інформації, дозволяючи працівникам поліції сконцентруватися на більш важливих завданнях.

Аналіз і прогнозування: застосування аналітичних інструментів до електронних звітів дозволяє виявляти тенденції та патерни в злочинності. Прогнозування можливих подій стає більш точним завдяки використанню алгоритмів і штучного інтелекту.

Планування стратегій безпеки: отримана інформація дозволяє керівникам поліції ефективніше планувати стратегії безпеки та розподіляти ресурси для боротьби з конкретними видами злочинів. Аналіз ефективності різних заходів дозволяє вдосконалювати підходи до протидії злочинності.

Взаємодія з громадськістю: електронні звіти можуть бути відкритими для громадськості, що забезпечує прозорість та взаємодію з громадою. Громадяни можуть отримувати доступ до статистики та аналізу, що сприяє залученню громади у питання безпеки та допомагає створювати більш безпечне середовище.

Кібербезпека: оскільки електронні системи містять конфіденційну інформацію, забезпечення кібербезпеки є критично важливим аспектом використання електронних звітів. Заходи безпеки мають на меті захищати дані від несанкціонованого доступу та забезпечувати конфіденційність.

2. Електронна база даних:

Створення і управління централізованою електронною базою даних злочинів, затриманих осіб та інших подій дозволяє поліції швидше отримувати доступ до інформації та вести кращий облік злочинів. Електронна база даних є ключовим інструментом для ефективного управління і моніторингу злочинності та дій правоохоронних органів. Ця система дозволяє збирати, зберігати та аналізувати різноманітну інформацію про злочини, затримані особи та інші події. Створення та управління централізованою електронною базою даних включає в себе: централізованість інформації; ефективне управління ресурсами; інтеграцію з іншими системами;

Централізованість інформації: Електронна база даних об’єднує дані з різних джерел, таких як поліцейські відділи, служби безпеки, судові установи тощо, у єдиний центральний ресурс. Це полегшує обмін інформацією та дозволяє швидше реагувати на злочини. Швидкий доступ до інформації: Електронна база даних дозволяє поліції отримувати необхідну інформацію в режимі реального часу. Це допомагає в оперативному розслідуванні злочинів та ухваленні стратегічних рішень.

Аналіз і статистика: Система може автоматично проводити аналіз інформації, виокремлюючи тенденції та патерни злочинності. Це надає

можливість прогнозувати ризики та приймати ефективні заходи для їх запобігання.

Ефективне управління ресурсами: Централізована база даних дозволяє оптимізувати використання ресурсів, забезпечуючи більш ефективну роботу правоохоронних органів. Захист інформації: Забезпечення безпеки і конфіденційності інформації є критичним аспектом. Сучасні технології шифрування та захисту даних гарантують, що лише авторизовані особи можуть отримати доступ до конфіденційної інформації.

Інтеграція з іншими системами: Електронна база даних має бути здатна інтегруватися з іншими інформаційними системами, такими як системи медичного обліку, бази даних паспортів тощо, для повноти та точності інформації. Створення та управління електронною базою даних є важливим етапом у модернізації правоохоронної системи, забезпечуючи більш ефективний контроль над злочинністю та забезпечуючи безпеку громадян.

3. Система відеоспостереження:

Встановлення систем відеоспостереження в публічних місцях та на важливих об’єктах допомагає в обліку порушень та забезпеченні громадської безпеки. Системи відеоспостереження грають ключову роль у забезпеченні безпеки в сучасних містах та на важливих об’єктах. Ось деякі аспекти, які варто розглянути при обговоренні цієї теми: це облік порушень: Встановлення камер спостереження у публічних місцях, на вулицях, в об’єктах громадського призначення дозволяє фіксувати порушення громадського порядку, вандалізму, злочинів тощо. Відеозаписи можуть служити як докази при розслідуванні і допомагати правоохоронним органам у виявленні та карантинуванні злочинців.

Запобігання злочинам: Відомість про те, що місце обладнане системою відеоспостереження, може відлякувати потенційних злочинців. Це може зменшити кількість злочинів та підвищити рівень безпеки в громаді.

Швидка реакція на події: Сучасні системи відеоспостереження часто обладнані розумними технологіями, такими як розпізнавання облич, руху чи детектори звуку. Це дозволяє автоматично виявляти підозрілі події та сповіщати операторів або правоохоронні органи для швидкої реакції.

Об’єктивність і довіра: Відеозаписи можуть служити об’єктивними доказами в судових процесах. Це сприяє підвищенню довіри до правоохоронних органів та системи правосуддя загалом.

Громадська безпека: Важливо встановлювати системи відеоспостереження в областях з великою концентрацією людей, таких як транспортні вузли, торгові центри, парки тощо. Це сприяє ефективному моніторингу громадської безпеки та вчасному реагуванню на непередбачені ситуації.

Співпраця з іншими технологіями: Системи відеоспостереження можуть інтегруватися з іншими технологіями, такими як штучний інтелект для аналізу поведінки або системи автоматизованого виявлення вибухових

пристроїв.

Загальносистемні підходи до впровадження систем відеоспостереження допомагають забезпечити повноцінний облік порушень, запобігання злочинам та підвищення громадської безпеки. При цьому важливо дотримуватися відповідних етичних та конфіденційних стандартів у збиранні та використанні отриманих даних.

Також потрібно врахувати наступні напрями це: використання мобільних додатків, автоматизацію службових процесів; системи розпізнавання обличчя; створення та використання електронних сервісів для громадян.

Отже, застосування інформаційних технологій у діяльності національної поліції України допомагає покращити якість роботи правоохоронних органів та забезпечити високий рівень безпеки в суспільстві.

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/95-ВР. поточна редакція 01.07.2022. URL : https://zakon.rada.gov.ua/ laws/show/80/94-вр#Text.

2. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності Навч. посібн. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с. URL : https://er.dduvs.in.ua/handle/123456789/8735

КИСЕЛЬОВА Єлизавета
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
СИНИЦІНА Юлія,
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

На сьогодні спостерігається досить значна інтеграція інформаційних технологій у діяльність правоохоронних органів. У цілому застосування штучного інтелекту, як напряму інформаційних технологій, в правоохоронній діяльності є доволі важливим та актуальним аспектом для України.

Один із надпотужних та складних штучних інтелектів на сьогоднішній

день є ChatGPT (Generative Pre-trained Transformer), розроблений компанією OpenAI, який може виконувати різні завдання, включаючи розпізнавання мови, розуміння запитів та формувати відповідь на запитання, здійснювати генерацію тексту, музики тощо. Завдяки таким можливостям ChatGPT може бути використаний у боротьбі із злочинністю на різних рівнях та у різних контекстах.

Дослідженням актуальних питань використання високих технологій, і зокрема, штучного інтелекту для підвищення ефективності правоохоронної діяльності займалися вітчизняні та закордоні вчені, такі як Р.І. Благута, О.І. Бугера, В.В. Голіна, М.В. Карчевський, В.А. Мисливий, А.В. Мовчан, В.М. Струков, Д.Ю. Узлов, К.В. Юртаєва та ін. Також, це питання вивчали зарубіжні дослідники Dupont B., Eliot L, Kashmir Hill, Stevens Y., Westermann H., Joyce M. [1].

Проте, швидкий розвиток технологій штучного інтелекту потребує постійного відслідковування його можливостей у галузі правоохоронної діяльності, удосконалення та розроблення нормативних документів, що регламентують їх застосування правоохоронними органами України.

Застосування штучного інтелекту у підрозділах національної поліції відіграє значущу роль у вдосконаленні різних аспектів правоохоронної діяльності. Розглянемо деякі ключові особливості та можливості штучного інтелекту в діяльності національної поліції, а саме використання штучного інтелекту у превентивній діяльності, а також для ефективного ведення розслідувань та для аналізу великих обсягів інформації (Big DATA).

Наступним напрямом застосування штучного інтелекту у формуванні громадської безпеки та відеоспостереження, а також з питань оптимізації патрулювання та ресурсів та створення електронних сервісів та формування електронної звітності, що в свою чергу призведе до оптимізації патрулювання та ресурсів, за рахунок застосування автономних патрульних систем.

Також штучний інтелект може бути використано для боротьби з кіберзлочинністю та тероризмом за рахунок аналізу текстів та мовлення та аналізу поведінки в інтернеті та виявлення загроз

Превентивна діяльність: аналіз даних для передбачення злочинів: Використання алгоритмів і аналітичних інструментів штучного інтелекту для обробки великої кількості даних дозволяє визначати тенденції в злочинності та передбачати можливі події.

Ефективне ведення розслідувань: розпізнавання обличчя та об’єктів: Використання технологій розпізнавання обличчя та об’єктів допомагає в ідентифікації підозрюваних та виявленні важливих слідів.

Аналіз великих обсягів інформації: системи штучного інтелекту можуть швидко аналізувати та категоризувати великі обсяги даних, що допомагає розслідуванням здійснювати більш ефективні запити та визначати потенційно важливу інформацію.

Громадська безпека та відеоспостереження: інтеграція систем відеоспостереження: Штучний інтелект може бути використаний для підвищення ефективності систем відеоспостереження, автоматично виявляючи підозрілу діяльність та реагуючи на неї.

Електронні сервіси та звітність, а саме розробка мобільних додатків для поліції. Розробка мобільних додатків, які використовують елементи штучного інтелекту, для поліції дозволяє ефективно взаємодіяти з громадою та забезпечує зручні онлайн-сервіси це в свою чергу призведе до оптимізації патрулювання та ресурсів, а саме застосування автономних патрульних систем. Використання автономних транспортних засобів чи роботів для патрулювання визначених районів, що може допомогти в оптимізації розподілу поліцейських ресурсів.

Боротьба з кіберзлочинністю, а саме аналіз поведінки та виявлення загроз. Використання алгоритмів штучного інтелекту для аналізу поведінки в Інтернеті та виявлення підозрілих або загрозливих дій.

Боротьба з тероризмом може розглядатися з точки зору аналізу текстів та мовлення. Використання алгоритмів машинного навчання для аналізу текстової інформації та мовлення для виявлення можливих загроз.

Автоматизована обробка доказів, а саме аналіз зображень та звуків. Інструменти штучного інтелекту можуть використовуватися для автоматизованого аналізу зображень та звуків, що може полегшити обробку доказів.

Важливо враховувати етичні та правові аспекти використання штучного інтелекту в правоохоронній діяльності та забезпечувати високий рівень захисту приватності громадян при впровадженні таких технологій.

1. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності DOI : https://doi.org/10.32782/2311-8040/2023-3-19

2. Milov O. et al. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. Eastern-European Journal of Enterprise Technologies. 2020. Т. 6. №. 2. PP. 30-32. DOI: 10.15587/1729-4061.2020.218660.

ПАНШИН Володимир,
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
СИНИЦІНА Юлія,
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РИЗИКИ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

Сучасні конфлікти внаслідок глобальної інформатизації почали використовувати інформацію як зброю, охопивши до цього недоступні засоби завдати значної шкоди противнику. Отже, використовуючи інформаційні впливи, маніпуляцію, пропаганду та інші інформаційні компанії існує критична потреба в забезпеченні надійної інформаційної безпеки. У той час як в контексті ескалації конфлікту в Україні потреба в забезпечення воєнно-інформаційної безпеки стала найбільш актуальною за всі останні роки дослідження проблематики. [1]

Доктрина інформаційної безпеки України визначає інформаційну безпеку як важливу самостійну сферу забезпечення національної безпеки (Про Доктрину інформаційної безпеки України 2017). Указом Президента України № 685/2021 від 15.10.2021 р. було схвалено Стратегію інформаційної безпеки (Про рішення Ради національної безпеки і оборони України 2021). Її метою є регулювання інформаційної безпеки на нормативно-правому рівні, посилення можливостей щодо забезпечення інформаційної безпеки України, інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, охорони суверенітету та цілісності України, демократії, прав та свобод людини і громадянина. Таким чином закладалися основи національної та інформаційної безпеки в інформаційній сфері. [2, 3]

Умови воєнного стану вносять значні виклики у сферу інформаційної безпеки держави. Забезпечення інформаційної безпеки стає стратегічно важливим завданням в умовах конфлікту. Основні ризики та напрями забезпечення інформаційної безпеки в умовах воєнного стану включають:

- кібератаки;
- дезінформація та психологічна війна;
- захист інформаційних мереж, контроль над комунікаціями;

- захист персональних даних;
- забезпечення кібербезпеки військових об’єктів;
- безпека суспільства та громадян;
- готовність до реагування на кіберзагрози.

Розглянемо кожен ризик коремо:

1. Кібератаки, а саме шпигунство та кібершпигунство. Держави можуть використовувати кібератаки для отримання доступу до конфіденційної інформації та розвідки. Знищення критично важливої інфраструктури: Кібератаки можуть бути спрямовані на енергетичні системи, телекомунікаційні мережі, банківські установи тощо.

2. Дезінформація та психологічна війна. До даного ризику можна віднести розповсюдження шейків та маніпуляція інформацією: Дезінформація може використовуватися для впливу на громадську думку, зміни настрої та психологічного ставлення громадян. Психологічний тиск та дестабілізація: Розповсюдження негативної або хибної інформації може спричинити паніку та створити атмосферу невпевненості в суспільстві.

3. Захист інформаційних мереж, а саме кіберзахист критично важливих об’єктів: Захист інформаційних систем енергетичних об’єктів, комунікаційних мереж, об’єктів управління та інших критично важливих об’єктів від кіберзагроз.

4. Контроль над комунікаціями, в данному випадку цензура та обмеження свободи слова. Введення цензури для контролю над потоком інформації та обмеженням свободи слова в опозиційних чи критичних медіа.

5. Захист персональних даних. Саме витоки конфіденційної інформації, є одним з головних ризиків безпеки держави в умовах воєнного стану. Ризик витоку конфіденційної інформації внаслідок хакерських атак чи внутрішніх угруповань, які можуть використовувати інформацію для здійснення тисків чи шантажу.

6. Забезпечення кібербезпеки військових об’єктів, а саме захист військових систем та комунікацій. Гарантування безпеки військових мереж, систем управління та комунікацій від потенційних кібератак противника.

7. Безпека суспільства та громадян, в першу чергу тісно пов’язана з захистом від інформаційного впливу. До основних заходів для запобігання психологічному впливу та дезінформації на суспільство в умовах військового конфлікту.

8. Готовність до реагування на кіберзагрози. До етапу готовності реагування на кібербезпекку потрібно віднести тренування персоналу. Проведення навчань та тренувань для персоналу в сфері кіберзахисту для ефективної реакції на можливі загрози.

Ефективна інформаційна безпека в умовах воєнного стану вимагає комплексного підходу, включаючи технологічні заходи, вдосконалення правового регулювання та підвищення інформаційної грамотності громадян.

1. Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіакомунікативні інструменти: матеріали міжнародної науково-практичної конференції. м. Київ : 18 квітня 2019 року. Київ. 2019. С. 17–22.

2. Про Доктрину інформаційної безпеки України: Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL : https://www.president.gov.ua/documents/472017- 21374

3. Про рішення Ради національної безпеки і оборони України 2021: Указ Президента України № 685/2021 від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL : https://www.president.gov.ua/documents/6852021-41 069

РИНДИЧ Анастасія
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
СИНИЦІНА Юлія,
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦМЕРЕЖАХ. ПРАВОВІ АСПЕКТИ

Актуальні питання інформаційної безпеки в соціальних мережах породжують численні виклики та вимагають уваги з боку як користувачів, так і законодавців.

Інформаційні права людини стали предметом праць таких науковців, як Ж. П. Вірна, А. І. Марущак, І. В. Алєксєєнко, Н. І. Ткачук, В. Вітів, О. О. Тихомиров, О. М. Селезньова, В. В. Ткаченко, Л. К. Орел та інших. Водночас доступність соціальних мереж зумовлює вразливість людини до нових викликів і загроз інформаційній безпеці, що потребує наукового аналізу та виявлення напрямів ефективного забезпечення інформаційних прав у соціальних мережах [1, с. 211].

Свобода думки, свобода слова, масової інформації та право на доступ до інформації від органів державної влади гарантують можливість людини мати переконання та не піддаватися дискримінації, висловлювати свою думку та доносити її іншим, обстоювати ідеї та впливати на їх облік, контролювати функціонування політичних інститутів та організацій [2, с. 211]

До основних аспектів та правових питань, пов'язані з інформаційною безпекою у соціальних мережах можна віднести наступні: конфіденційність та приватність, безпека облікових записів, поширення дезінформації, булінг та кіберзлочинність, рекламні та маркетингові практики, авторські права та інтелектуальна власність, механізми судового захисту, легітимність обміну інформацією, політичний вплив та етика.

До аспекту «конфіденційність та приватність» можна віднести процеси збору та обробки персональних даних. Соціальні мережі зазвичай збирають великі обсяги персональної інформації. Питання пов'язані з тим, як ці дані збираються, зберігаються і обробляються.

Безпека облікових записів включає в себе захист від хакерських атак та фішингу. Користувачі соціальних мереж стають об'єктом хакерських атак, спрямованих на отримання несанкціонованого доступу до їхніх облікових записів.

До аспекту поширення дезінформації потрібно віднести боротьбу з фейками та маніпуляціями. Соціальні мережі часто використовуються для розповсюдження дезінформації та фейків. Дезінформація та фейки, що розповсюджуються через соціальні мережі, стали серйозним викликом для сучасного суспільства. Боротьба з цими явищами вимагає уваги та дієвих заходів. Сучасні соціальні платформи стали плацдармами для розповсюдження неправдивої інформації, що може значно вплинути на громадську думку та формування поглядів.

Щоб впоратися із цим явищем, важливо вдосконалювати механізми виявлення та блокування фейків. Розробка та впровадження алгоритмів машинного навчання, спрямованих на виявлення недостовірної інформації, може стати ефективним інструментом в цьому процесі. Додатково, співпраця з фактчекерськими організаціями та створення механізмів для повідомлення про сумнівні матеріали можуть сприяти збільшенню обізнаності користувачів та ефективній боротьбі з дезінформацією.

Крім того, необхідно звертати увагу на розвиток інформаційної грамотності серед користувачів соціальних мереж. Навчання розпізнаванню маніпуляцій та вивчення навичок перевірки достовірності інформації може допомогти зменшити поширення дезінформації та підвищити рівень свідомості серед інтернет-користувачів. Булінг та кіберзлочинність:

Захист від кібербулінгу та онлайн-злочинів: Соціальні мережі можуть бути місцем для кіберзлочинності та ворожнечі. У сучасному цифровому віці, соціальні мережі стали не тільки місцем спілкування, але і платформою для зростаючих випадків кібербулінгу та онлайн-злочинності. Захист від цих явищ стає надзвичайно важливим завданням, оскільки вони можуть серйозно впливати на психічне здоров'я та безпеку користувачів.

Для протидії кібербулінгу, необхідно впроваджувати ефективні механізми звітування та блокування образливого контенту. Співпраця із платформами та правоохоронними органами для швидкого реагування на

ситуації кібербулінгу є ключовою. Посилення правового регулювання та визначення відповідальності за онлайн-злочини може створити відстрашуючий ефект та сприяти безпеці користувачів.

Крім того, навчання медіаграмотності та етики в інтернеті може допомогти користувачам убезпечити себе від потенційних загроз. Важливо підкреслювати важливість усвідомленості стосовно безпеки в онлайн-середовищі та вчати стратегії захисту своєї приватності.

Загальний захист від кібербулінгу вимагає спільних зусиль платформ, законодавців, та самих користувачів для створення безпечного та позитивного інтернет-середовища. Рекламні та маркетингові практики: Таргетована реклама та персоналізація. Таргетована реклама та персоналізація відіграють ключову роль у сучасному маркетингу. Ці стратегії дозволяють адаптувати пропозиції до індивідуальних інтересів та потреб кожного користувача. За допомогою аналізу даних, платформи можуть точно визначити цільову аудиторію, забезпечуючи більш ефективне спілкування між брендами та споживачами. Однак, важливо забезпечувати прозорість та захист конфіденційності даних, щоб уникнути можливих етичних питань та підтримувати довіру споживачів.

Авторські права та інтелектуальна власність. Законність використання контенту. Проблеми виникають, коли користувачі або компанії використовують чужий контент без відповідної дозволу. Механізми судового захисту та вирішення спорів та порушень: Механізми судового захисту та вирішення спорів є важливою складовою правової системи. Ці механізми забезпечують можливість оскарження та вирішення конфліктів у визначених правилах та рамках закону. Судові інстанції використовуються для розгляду цивільних та кримінальних справ, а також для вирішення спорів між сторонами. Забезпечення справедливого та ефективного судочинства є важливим аспектом правової системи, сприяючи розвитку правопорядку та захисту прав громадян.

Легітимність обміну інформацією та контроль за розповсюдженням особистої інформації. Легітимність обміну інформацією та контроль за розповсюдженням особистої інформації визначаються прозорими та етичними стандартами. Захист особистої інформації стає пріоритетом у сучасному цифровому світі, де обмін даними стає невід’ємною частиною інтернет-спільнот. Визначення правил, згода на обробку даних та суворий контроль з боку організацій є ключовими аспектами, що забезпечують легітимність обміну інформацією та дотримання приватності користувачів

Політичний вплив та етика та запобігання впливу на вибори та політичну маніпуляцію. Політичний вплив та етика у цифровому просторі стають важливими питаннями. Запобігання впливу на вибори та політичну маніпуляцію вимагає суворих стандартів дотримання правил у виборчих кампаніях. Транспарентність у фінансуванні, обмеження використання алгоритмів для спрямування інформації та ефективні механізми виявлення та

припинення дезінформації є ключовими складовими етичної політичної поведінки в цифровій ері.

Вирішення цих питань вимагає комплексного підходу, який включає в себе розробку та вдосконалення законодавства, активну участь соціальних мереж у захисті прав користувачів та навіть залучення міжнародних організацій для розробки стандартів безпеки в цій сфері

1. Токарєва К. Забезпечення інформаційних прав людини в соціальних мережах Актуальні проблеми правознавства. 4 (32)/2022 DOI :10.35774/app2022.04.088

2. Вірна Ж. П. Інформаційні права і свобода в структурі правового статусу сучасної людини. Особистісне зростання: теорія і практика: зб. наук. праць IV Міжнар. наук.-практ. Інтернет-конф. (м. Житомир, 21 квітня 2020 р.). Житомир, 2020. С. 210–213.

СИНИЦІНА Юлія
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сучасному етапі розвитку України інформаційні технології набули поширення в усіх сферах людської діяльності. Виникла й стрімко розвивається потужна індустрія отримання, систематизації та поширення інформації. Кількість працівників в інформаційному секторі у більшості країн світу до яких відноситься й Україна неухильно збільшується. Інформація набуває значення одного з найбільш затребуваних державних ресурсів.

Суттєві зміни відбуваються і в діяльності правоохоронних органів. Зокрема на основі інформаційних технологій упроваджуються потужні інформаційно-пошукові системи, удосконалюється система управління та інформаційно-аналітичного забезпечення Національної поліції, розробляються нові методи збирання й аналізу інформації, розширюються можливості спеціальних технічних засобів тощо. Водночас сучасними інформаційними технологіями оснащується й кримінальне середовище [1].

Проблемі формування моделі фахівця присвячено дослідження І.Д. Беха, І. А. Зязюна, Г.В. Єльникової, Л.В. Козак, А.К. Маркової, О.І. Мармази, О.О. Романовського, В.А. Семиченко, С.О. Сисоєвої, О.М. Спіріна, Н.Ф. Тализіної, В.В. Ягупова та інших науковців. Окремі аспекти

підготовки фахівців у галузі інформаційних технологій для правоохоронних органів розглядалися в наукових працях С.І. Апухтіна, О.М. Бандурки, О.М. Барановської, В.В. Бачила, В.О. Голубєва, В.Є. Козлова, В.А. Кудінова, Г.Ю. Маклакова, А.С. Овчинського, Ю Ю. Орлова, В.Л. Ортинського, В.Д. Поливанюка, та інших науковців.

Актуальні питання підготовки фахівців у галузі інформаційних технологій для органів національної поліції України включають ряд важливих аспектів:

1. Кібербезпека та кіберзахист:

– Організація тренінгів з кібербезпеки для ефективного захисту інформаційних систем поліції від кібератак.

– Розробка та впровадження політик кіберзахисту для запобігання витокам конфіденційної інформації.

Забезпечення кібербезпеки поліції – пріоритетна задача. Організація тренінгів у сфері кібербезпеки дозволяє підвищити навички фахівців та ефективно захищати інформаційні системи від кібератак. Розробка та впровадження політик кіберзахисту визначає рамки для запобігання витокам конфіденційної інформації, забезпечуючи надійний захист важливих даних та дотримання стандартів безпеки.

2. Комп'ютерна криміналістика:

– Навчання фахівців сучасним методам дослідження комп'ютерних злочинів та цифрового доказування.

– Підготовка до розслідування електронних слідів інтернет-злочинів.

Навчання фахівців у галузі комп'ютерної криміналістики включає ознайомлення із сучасними методами дослідження комп'ютерних злочинів та навичками цифрового доказування. Спеціалісти отримують знання для ефективного розслідування електронних слідів інтернет-злочинів, що стає дуже важливим у сучасній цифровій ері, де кіберзлочини стають все поширенішими. Таке навчання сприяє вдосконаленню методів виявлення та протидії комп'ютерній злочинності [2].

3. Аналіз використання великих баз даних:

– Вивчення методів та інструментів аналізу великих обсягів даних для виявлення закономірностей та трендів у кримінальній діяльності.

– Забезпечення навичок роботи з аналітичними платформами.

Навчання аналізу використання великих баз даних включає вивчення методів та інструментів для виявлення закономірностей та трендів у кримінальній діяльності. Фахівці отримують навички роботи з аналітичними платформами, що дозволяє їм ефективно обробляти та інтерпретувати великі обсяги даних. Це допомагає виявляти ключові відомості та сприяє більш ефективному розслідуванню кримінальних подій через використання сучасних технологій аналізу.

4. Електронне слідство:

– ***Навчання ефективному збору та аналізу електронних доказів у судових справах.***

– ***Застосування сучасних методів для виявлення та вивчення цифрових слідів.***

Навчання електронного слідства передбачає отримання навичок ефективного збору та аналізу електронних доказів у судових справах. Спеціалісти вивчають сучасні методи для виявлення та вивчення цифрових слідів, що є важливим у контексті розслідувань кримінальних подій. Використання новітніх технологій у сфері електронного слідства сприяє об'єктивному та ефективному процесу здобуття та представлення доказової бази у судових процедурах.

5. Захист від кіберзагроз:

– ***Організація навчань щодо виявлення та протидії кіберзагрозам, які можуть впливати на діяльність поліції.***

– ***Постійне оновлення захисних заходів та політик безпеки інформаційних систем.***

Захист від кіберзагроз включає організацію навчань, спрямованих на виявлення та протидію потенційним кіберзагрозам, які можуть впливати на діяльність поліції. Фахівці отримують необхідні навички для ефективної реакції на кібератаки. Постійне оновлення захисних заходів та політик безпеки інформаційних систем є важливим елементом стратегії, що гарантує високий рівень кібербезпеки та надійність функціонування поліцейських інформаційних структур.

6. Етичні аспекти використання технологій:

– ***Поглиблення знань щодо етичних норм використання технологій у роботі правоохоронних органів.***

– ***Розробка стандартів та директив, які враховують етичні вимоги до застосування новітніх технологій у роботі поліції.***

Зосередження на етичних аспектах використання технологій у сфері правоохоронних органів є ключовим завданням. Навчання фахівців стосовно етичних норм використання технологій у роботі правоохоронців допомагає поглибити їхні знання та визначити етичні межі застосування новітніх засобів. Розробка стандартів і директив, які враховують етичні вимоги, є необхідною для забезпечення відповідального та прозорого використання технологій у діяльності поліції.

Навчання фахівців у сфері інформаційних технологій для національної поліції важливо спрямоване на забезпечення ефективного використання сучасних інструментів у боротьбі з кримінальністю та забезпечення безпеки громадян.

---

1. Анісімов К.І. Сутність та значення концепції «community policing» у діяльності органів національної поліції України Правовий часопис Донбасу № 3 (76) 2021. DOI : https://doi.org/10.32366/2523-4269-2021-76-3-169-174

2. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності Навч. посібн. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с. URL : https://er.dduvs.in.ua/handle/123456789/8735

ГАЙВАНЮК Іветта
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИЖКОВ Едуард
ппрофесор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Основою національної безпеки є економічна безпека. Вона охоплює у себе фінансові ресурси України, людські ресурси та усю економічну систему в цілому. Інформаційна безпека, в свою чергу, захищає кіберпростір нашої держави. Економічна безпека включає в себе охорону економіки на національному та на міжнародному рівнях, тому є досить важливою складовою держави. Інформаційні технології, які використовуються задля вироблення, обробки та передавання інформації, зокрема, мають забезпечувати економічну безпеку України. До них належить опрацювання та надійне зберігання інформації, яка знаходиться в усіх інформаційних системах. Для подібних дій потрібне обов'язкове залучення технологій, таких, як сервери, сховища даних та надійне програмне забезпечення.

Забезпечення економічної та інформаційної безпеки відбувається за допомогою кіберзахисту, кібергігієни, аналітики даних, шифрування даних, моніторингу, їх надійних баз та ін. Акценти воєнної боротьби зміщуються в бік практичної реалізації інформаційних технологій [1]. Тому наразі коли на території України триває війна, інформаційна та економічна безпека мають бути основними питаннями, що мають бути розглянуті державою, адже інформаційний простір – це також зброя.

Захист інформаційних даних в Україні має бути надійним та комплексним для охорони систем даних, особливо під час війни. Військовий стан зараз дає змогу розвитку кіберзахищенності держави саме у військовій сфері. Збройні сили України, з моменту повномасштабного вторгнення

російської федерації, почали використовувати різні методи ведення бойових дій за допомогою засобів інформаційних технологій. Цими засобами є захист, управління зв'язком, розвідка та інше. Також зовсім нещодавно новими термінами у військовій справі ЗС України та світі став «кібероборона» та «кіберзахист», що зазначені у Законі України «Про основні засади забезпечення кібербезпеки України» [2].

Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, що здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Кіберзахистом є сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Складовою інформаційної безпеки є особиста інформаційна безпека. Вона направлена на захист конфіденційної інформації громадянина. Кожна людина має право на захист особистої інформації, особливо під час воєнного стану. Треба зазначити, що основними знаряддями інформаційної російської війни проти України є пропаганда, дезінформація та намагання змінити думку. Це означає, що кожен громадянин України повинен вміти фільтрувати всю інформацію, яка надходить з різноманітних інтернет-джерел.

Економічна безпека України під час військового стану є важливою. Національна безпека фактично залежить від економіки країни. Держава на даний момент зазнає великих втрат, руйнувань і збитків. Тому економічна безпека зараз тримається на забезпеченні фінансової підтримки Збройних сил України: уряд фінансує оборонні витрати. Але, на жаль, навіть під час військового стану фінансова система має низку загроз у вигляді корупції, високого рівня тіньової економіки, рейдерства та інших.

У забезпеченні економічної безпеки грають роль: фінансування оборони, що підтримує усі оборонні потреби; економічна співпраця з іншими країнами, направлена на отримання Україною фінансової підтримки від держав-партнерів; боротьба з корупцією, яка захищає економіку від негативних наслідків.

Серед найважливіших національних економічних інтересів, що визначають майбутнє України, добробут і процвітання нації, входять побудова потужної національної економіки з надійною системою економічної безпеки, розв'язання урядом соціальних проблем, розвиток науково-технічного потенціалу України, розвиток підприємництва, забезпечення зайнятості та гідної оплати праці людей [3].

У березні 2021 року урядом було ухвалено проект Стратегії економічної

безпеки України на період до 2025 року, у якому зазначено основи для формування державної політики у сфері забезпечення економічної безпеки. У Стратегії проведено детальну оцінку стану економічної безпеки та ідентифіковано загрози за основними складовими економічної безпеки – фінансовою, виробничою, інвестиційно-інноваційною, зовнішньоекономічною, макроекономічною. Важливе місце в безпековому напрямі займають виклики, пов'язані зі збройною агресією російської федерації та тимчасовою окупацією частини території України [4].

У підсумку зазначимо, що інформаційна та економічна безпека під час військового стану є надзвичайно важливою як для кожного громадянина, так і усієї держави в цілому. Ці два види допомагають зберегти суспільну цифрову безпеку та фінансову стійкість, що в умовах війни є досить важливими аспектами. Наша задача як громадян підтримувати заходи задля їх зміцнення: підтримувати громадські організації, брати участь у освітніх програмах тощо. Важливо розуміти, що економічна та інформаційна безпека сприяє стабільності України, що є найважливішим у воєнний період.

1. Інформайційно-воєнна безпека як елемент національної безпеки України / В.Ю. Артемов, В.О. Хорошко, Ю.Є. Хохлачова, В.В. Погорелов // Захист інформації. 2022. Т. 24, № 1. С. 21-29 : іл. Бібліогр.: 19 назв.

2. Закон України «Про основні засади забезпечення кібербезпеки України». URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text\

3. Eduard Ryzhkov Modeling economic component of national security / L. Rybalchenko, E. Ryzhkov, S. Ohrimenco // Philosophy, Economics and Law Review : Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. 2021. Volume 1 (1). P. 25-36

4. Проект Стратегії економічної безпеки України на період до 2025 року. URL : https://www.kmu.gov.ua/news/uryad-shvaliv-proekt-strategiyi-ekonomichnoyi-bezpeki-ukrayini-na-period-do-2025-roku

ЖЕЛНОВАЧ Ілля
курсант 3 курсу факультету №4
Науковий керівник:
СВІТЛИЧНИЙ Віталій.
доцент кафедри протидії
кіберзлочинності
факультету №4 Харківського
національного університету
внутрішніх справ, к.т.н. доцент

ДЕЗІНФОРМАЦІЯ В ЦИФРОВОМУ ПРОСТОРІ В УМОВАХ ВОЄННОГО СТАНУ: МЕТОДИ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ

Вступ. Цифровий простір - це віртуальне середовище в Інтернеті, де відбувається обмін інформацією, спілкування та взаємодія через різні онлайн-платформи і ресурси. На даний час, комунікація в глобальній павутині є також засобом впливу та маніпуляцією. Україна, що стоїть на передовій боротьби проти дезінформації, особливо відчуває цей вплив.

Виклад основного матеріалу. За інформацією, яку надає Центр Протидії Дезінформації, ЗМІ російської федерації неодноразово намагаються вплинути на громадян України, шляхом надання фейкової інформації та вигородити свої незаконні акти. Глобальним прикладом дезінформації є ряд джерел, в яких описуються напади рф на територію України, де ініціаторами смертей є конкретно Збройні Сили України (далі ЗСУ). Російські ЗМІ намагаються виправдати власні терористичні акти, шляхом надання недостовірної інформації, в якій нібито ЗСУ навмисно обстрілюють свою територію, займають будинки громадян України в своїх корисних цілях. **У відповідь,** керівництво України завжди пояснюють кожен крок ЗСУ фактами, при яких ця чи інша подія не могла б відбутися [1].

Виходячи з вищеперерахованих даних, російська пропаганда навмисно перекладає відповідальність задля налаштування громадян проти ЗСУ та поширення паніки серед цивільних осіб.

Важливим завданням є забезпечення точності та достовірності інформації, особливо в контексті воєнного конфлікту між Україною та рф. Базується це на комплексному підході до обробки та аналізу інформаційних потоків. Аналіз джерел, де основна ідея методу полягає в систематичному вивченні джерел інформації з метою визначення їхньої надійності та об'єктивності. В Україні це особливо актуально, оскільки країна є мішенню численних кампаній дезінформації, часто з орієнтацією на конфлікт на Сході. Аналіз може включати перевірку фактів, вивчення історії публікацій джерела, його власників та фінансування.

Big Data та AI, в якому розвитком технологій, зокрема великих даних та штучного інтелекту, з'явилася можливість автоматизованого аналізу інформаційних потоків. Спеціалізовані алгоритми можуть шукати шаблони, аномалії або незвичні тренди в соціальних мережах, новинах, блогах тощо. В Україні це може бути використано для виявлення та відслідковування кампаній дезінформації, спрямованих на підрив стабільності або дискредитацію ЗСУ.

Громадський моніторинг, насамперед, включає активне залучення громадян до процесу виявлення фейкових новин та дезінформації. В Україні це може включати в себе такі ініціативи як громадські спостерігачі, волонтери, журналісти, а також спеціалізовані платформи для колективного виявлення та маркування дезінформації. Це допоможе не лише збільшити обсяги виявленої дезінформації, але й підвищити рівень медіаграмотності серед населення [2].

Після роз'яснення етапів, в яких громадяни України розуміють порядок дій, щоб не стати жертвою дезінформації, потрібно передати ці знання на план боротьби із дезінформацією. Цей порядок включає в себе ряд взаємодоповнюючих методів, від освітніх програм до законодавчих ініціатив і створення авторитетних медіа-платформ.

Однією з ключових стратегій протидії дезінформації є масове просвітництво з питань медіаграмотності. В рамках цієї ініціативи можуть проводитися тренінги, воркшопи, та освітні курси, які навчають людей розпізнавати фейкові новини, маніпулятивні заголовки, та інші форми дезінформації [3].

Висновки. Щоб більше контролювати простір дезінформації, держава може вжити законодавчих заходів. Це може включати в себе введення штрафів, адміністративних або навіть кримінальних санкцій для осіб чи організацій, що займаються систематичним розповсюдженням дезінформації. У Україні такі механізми потребують особливої уваги, враховуючи їх можливий вплив на національну безпеку. Створення авторитетних і незалежних медіа-платформ може служити суттєвою противагою в екосистемі дезінформації. Ці платформи можуть пропонувати альтернативний, об'єктивний погляд на події, що відбуваються, тим самим зменшуючи ризик маніпуляції громадською думкою. В Україні це може включати в себе також спеціалізовані портали та платформи, які фокусуються на воєнних злочинах, гуманітарних питаннях, та ін.

Отже, боротьба з дезінформацією в Україні потребує комплексного підходу, який включає як технологічні, так і соціальні методи виявлення та нейтралізації. Важливо розуміти, що дезінформація є не лише засобом психологічної війни, але й загрозою національній безпеці країни.

1. Огляд провокацій та дезінформації рф. Частина 1. URL https://voxukraine.org/oglyad-provokatsij-ta-dezinformatsiyi-rf (дата звернення: 20.09.2023).

2. Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis. URL: https://www.mdpi.com/2673-5172/4/2/43 (дата звернення: 20.09.2023).
3. Tactics of Disinformation - CISA URL: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf (дата звернення: 21.09.2023).

КУНДО Богдан
курсант 2 курсу факультету №4
Науковий керівник:
КАЛЯКІН Сергій
викладач кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНО-ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВОЄННОГО СТАНУ

Під час військового стану, інформаційна та економічна безпека стають особливо важливими аспектами для забезпечення функціонування держави та захисту її інтересів.

Інформаційна безпека передбачає захист інформації, яка є важливою для функціонування держави та її обороноздатності. Під час військового стану, інформаційна безпека має на меті запобігти проникненню ворожих агентів, хакерських атак і дезінформації. Для цього можуть застосовуватись такі заходи, як заборона розповсюдження конфіденційної інформації, підвищення кібербезпеки, контроль за засобами масової інформації та запобігання поширенню ворожої пропаганди. Держава також може вживати заходів для забезпечення безпеки критично важливої інфраструктури, такої як електроенергетика, транспортні системи та зв'язок [1].

Під час військових конфліктів можуть бути введені економічні санкції проти ворожих держав, обмеження зовнішньої торгівлі та імпорту, а також мобілізація ресурсів для потреб оборони. Держава також здійснює заходи для забезпечення стабільності фінансової системи та банківської сфери, щоб уникнути фінансових збитків та зловживань.

Усі ці заходи спрямовані на забезпечення безпеки держави та її громадян під час військових дій. Вони допомагають зменшити вразливість держави перед зовнішніми загрозами, забезпечують стабільність функціонування ключових секторів інформаційної та економічної сфери та підтримують внутрішню безпеку та обороноздатність.

Під час військового стану для забезпечення інформаційної безпеки можуть бути вжиті такі додаткові заходи [2]:

1. Мобілізація кіберзаходів: Держава може змобілізувати кіберзаходи та залучити експертів з кібербезпеки для посилення захисту від хакерських атак та кібершпигунства. Це включає моніторинг мережі, виявлення потенційних загроз, вдосконалення захисних систем та розробку планів реагування на кіберінциденти.

2. Захист критичної інфраструктури: Для забезпечення інформаційної безпеки під час військового стану, держава може звернути особливу увагу на захист критичної інфраструктури, такої як електроенергетика, водопостачання, транспортні системи та зв'язок. Застосування технологій шифрування, використання вогнеповітрозахисних систем та підвищення фізичної безпеки можуть бути вжиті для запобігання можливим атакам на ці об'єкти.

3. Контроль за засобами масової інформації: Держава може встановити контроль за засобами масової інформації, щоб запобігти поширенню неперевіреної або ворожої пропаганди, яка може спричинити паніку серед населення або дезорієнтацію військових сил. Це може включати перевірку та регулювання інформаційного матеріалу, вимогу до засобів масової інформації про поширення точних та достовірних новин, а також заборону розповсюдження конфіденційної і військової інформації.

4. Запобігання дезінформації: Умисне поширення дезінформації може бути великою загрозою під час військового стану. Держава може вжити заходів для контролю та боротьби з дезінформацією, зокрема шляхом підвищення обізнаності громадськості про феномен дезінформації, сприяння розпізнаванню та відповіді на дезінформаційні кампанії та сприяння прозорості та достовірності інформації.

5. Міжнародне співробітництво: У ситуації військового стану важлике міжнародне співробітництво для забезпечення інформаційної безпеки. Держава може співпрацювати з іншими країнами та міжнародними організаціями для обміну інформацією про потенційні загрози, спільного розроблення кіберзаходів та координації заходів інформаційної безпеки. Таке співробітництво може сприяти виявленню та протидії загрозам, які мають транскордонний характер, та підвищити загальний рівень інформаційної безпеки.

Висновки. Інформаційну та економічну безпека під час військового стану **потрібно розглядувати** як спроможність національної економіки зберігати стійкість та невразливість до внутрішніх і зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі, стале та збалансоване зростання – важливі критерії оцінювання якісних параметрів національної економіки, стратегічної ефективності економічної політики держави в економічній сфері. Тому постійний експертно-аналітичний моніторинг рівнів та загроз економічної безпеки та її складових частин зберігає значну актуальність, а в умовах різкого

розширення та посилення потужності загроз, зумовлених повномасштабною агресією рф проти України, набуває особливого значення.

1. Нові правила: інформаційна безпека під час війни. Одеська національна наукова бібліотека. Офіційний веб-сайт. URL: http://odnb.odessa.ua/view_post.php?id=4286 (дата звернення: 13.10.2023).

2. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв'язку. URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku (date of access: 13.10.2023).

СИНЖЕРЯН Андрій
курсант 3 курсу факультету №4
Науковий керівник:
СВІТЛИЧНИЙ Віталій.
доцент кафедри протидії
кіберзлочинності факультету №4
Харківського національного
університету внутрішніх справ,
к.т.н. доцент

КІБЕРТЕРОРИЗМ: СУЧАСНІ ТЕНДЕНЦІЇ ТА МЕТОДИ ПРОТИДІЇ

Кібертероризм – нове, малодосліджене, але без того, поширене явище. Підтвердженням цьому слугує, зокрема, класична атака мережевого "черв'яка" Хелкерн, що розпочалася 26 січня 2003 року та стала безпрецедентним випадком, зашкалюючи у швидкості розповсюдження та розмірі спричиненої та потенційної шкоди. За експертними оцінками, загальна вартість шкоди склала понад 10 мільярдів доларів. В результаті атаки було інфіковано 80 тисяч веб-серверів, і Інтернет-трафік уповільнився на 25% у всьому світі [1]. Серед сучасних випадків кібертероризму можна зазначити комп’ютерний вірус “WannaCry”, який у період із 2017 по 2020 роки наніс шкоди більше ніж 230 тис. комп’ютерів у 150 країнах світу, вимагаючи викуп за дешифрацію зашифрованих внаслідок зараження даних у розмірі від 300 до 600 доларів [2]. Тож *метою* цього дослідження є аналіз сучасних тенденцій в кібертероризмі та методів протидії йому.

Щоб кібертероризм вважався формою тероризму, він повинен відповідати основним принципам і елементам тероризму. З цієї точки зору, кібертероризм — це не самостійний злочин, а скоріше форма тероризму, характеризована унікальним методом виконання, що здійснюється в кіберпросторі.

Це визначення можна критикувати, порівнюючи кібертероризм з іншими формами тероризму, як-то терактами з захопленням літаків або автомобільними атаками. Спостерігається тенденція перенесення "реальних" явищ в кіберпростір, як, наприклад, "кіберактивізм" або "кіберзнущання".

Тож у цій роботі пропонується, власне, трактування терміну “кібертероризм” — це форма терористичної діяльності, яка здійснюється в кіберпросторі із метою завдання значущої матеріальної, соціальної або психологічної шкоди. Він може включати в себе атаки на інформаційні системи, несанкціонований доступ до даних, а також розповсюдження дезінформації. Відмінністю кібертероризму від звичайного тероризму є його виконання через кібернетичні засоби, а не фізичні дії, хоча обидва види можуть бути взаємопов'язані [3].

Згідно із дослідженнями видання Fortinet найпопулярнішими видами кібератак, які можна віднести до кібертероризму, є:

1. DDoS-атаки;
2. фішинг та соціальна інженерія;
3. віруси та шкідливе програмне забезпечення;
4. атаки на критичну інфраструктуру;
5. розповсюдження дезінформації;
6. кібершпигунство;

Кібертероризм може призвести до знешкодження систем управління критичною інфраструктурою, фінансових втрат для корпорацій та загроз для державної безпеки [4].

Основні методи протидії кібертероризму включають в себе ряд стратегій та заходів. Базовим елементом є освіта та підготовка персоналу, яка зосереджена на навчанні з основ кібербезпеки, включаючи ідентифікацію фішингових атак та безпечне використання паролів. Для забезпечення захисту, активно використовуються фаєрволи, антивірусні програми та інші технічні механізми. Значну роль відіграє і регулярна актуалізація систем безпеки та програмного забезпечення. Систематичний моніторинг та аудити витрат на інформаційну безпеку дозволяють ідентифікувати та виправляти вразливості. Додатковий рівень захисту забезпечується через резервне копіювання критичних даних та розробка планів відновлення після аварій.

На законодавчому рівні, співпраця з державними органами може значно покращити правову базу в сфері кібербезпеки. Також не менш важливою є міжнародна співпраця, яка дозволяє об'єднати зусилля для протистояння глобальним кіберзагрозам. І, нарешті, ефективність протидії кібертероризму залежить від розробки як проактивних методик виявлення та блокування атак, так і реактивних стратегій для мінімізації наслідків. [5].

В умовах невизначеності терміну "кібертероризм", консенсус щодо його небезпеки очевидний. Атаки типу Хелкерн та WannaCry підкреслюють велику потенційну шкоду, яку може спричинити кібертероризм. Ефективні методи протидії включають освіту персоналу, технічні засоби захисту,

моніторинг, та міжнародну співпрацю. Швидкий розвиток технологій постійно створює нові виклики, вимагаючи адаптації методів протидії та законодавства. Тому кібертероризм залишається однією з ключових загроз сучасності, яка вимагає незмінної уваги.

1. Широкова-Мурараш О.Г., Акчурін Ю.Р. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/38938/14-Shirokova.pdf?sequence=1 (дата звернення: 21.09.2023).

2. Malwarebytes. WannaCry. URL: https://www.malwarebytes.com/wannacry (дата звернення: 21.09.2023).

3. Laura M.L. Defending cyberterrorism. URL: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005 (дата звернення: 21.09.2023).

4. Fortinet. Types of Cyber Attacks. URL: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (дата звернення: 21.09.2023).

5. Lee Jarvis. Stuart Macdonald. Lella Nouri. The Cyberterrorism Threat: Findings from a Survey of Researchers. URL: https://www.researchgate.net/publication/261513630_The_Cyberterrorism_Threat_Findings_from_a_Survey_of_Researchers (дата звернення: 21.09.2023).

Наукове видання

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Матеріали
Всеукраїнської науково-практичної конференції
(м. Дніпро, 02 листопада 2023 р.)

Редактор, оригінал-макет – *А. В. Самотуга*
Редактор *О. М. Врублевська*

Підп. до друку 06.05.2024. Формат 60х84/16. Друк – цифровий. Папір офісний.
Гарнітура – Times. Ум.-друк. арк. 10,70. Обл.-вид. арк. 11,50. Зам. № 13/24-зб

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua

Свідоцтво про внесення до Державного реєстру ДК № 6054 від 28.02.2018