Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

22 грудня 2023 року

Львів 2024

УДК 004
І 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 8 від 31 січня 2024)

РЕДАКЦІЙНА КОЛЕГІЯ:

І 78 **Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України**: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2024. – 192 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 22 грудня 2023 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

Андрієнко І. А.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Грищенко Д. О.
старший викладач кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Штучний інтелект (ШІ) – це комп'ютерна система та програма, яка може виконувати завдання, які раніше виконували лише люди. Штучний інтелект може вчитися на даних, розпізнавати зображення та текст, приймати рішення та вирішувати проблеми. Це означає, що програми, що використовують штучний інтелект, можуть самостійно вивчати та аналізувати інформацію та приймати рішення на основі цієї інформації. Штучний інтелект використовується в багатьох галузях, включаючи охорону здоров'я, банківську справу, транспорт, виробництво, бізнес та стартапи [1].

Перші спроби створення штучного інтелекту з'явилися ще в 1950-х роках. Одним з перших, хто спробував створити штучний інтелект, був Джон Маккарті з Массачусетського технологічного інституту (MIT). Він вважається одним з батьків штучного інтелекту та створив термін «штучний інтелект» у 1956 році. Однак, перший повноцінний штучний інтелект був створений не однією особою, а командою дослідників під керівництвом Джона Маккарти, Марвін Мінски та інших вчених в MIT в 1960-х роках. Вони створили програму під назвою «Logic Theorist», яка могла доводити математичні теореми, що було вважалося складним завданням для комп'ютерів того часу.

По-перше, давайте розберемося, що таке критична інфраструктура. Критична інфраструктура включає інфраструктурні об'єкти, що забезпечують життєво важливу діяльність населення. Вони впливають на важливі фактори. Це включає в себе електроенергію, електрику, тепло, газ, водопостачання та каналізацію. Це також включає транспортну інфраструктуру, оскільки вона забезпечує доставку продуктів харчування, медикаментів та людей. [2]

Штучний інтелект, як і інші технології, може представляти як позитивні, так і негативні аспекти інформаційної безпеки в критичній інфраструктурі. Зловмисники можуть використовувати штучний інтелект для виявлення вразливостей і розробки складних і хитрих кібератак в обхід захисту. Маніпулювання рішеннями штучного інтелекту може призвести до неправильних рішень та неправильного використання систем безпеки.

Крім того, проблеми конфіденційності та етики можуть виникнути при використанні штучного інтелекту для збору та аналізу даних. Якщо організація занадто сильно покладається на штучний інтелект для захисту критичної інфраструктури, вона може стати вразливою, якщо їй не довіряють або якщо відбуваються атаки на ці системи. Тому важливо поєднувати штучний інтелект із традиційними методами захисту для розробки стратегії кібербезпеки, яка включає аналіз ризиків та застосування відповідних заходів безпеки.

Крім того, штучний інтелект виявив додатки для створення та управління бот-мережі, мережею скомпрометованих пристроїв, контрольованих кіберзлочинцями. Ці мережі можуть використовуватися для різних шкідливих дій, таких як розподілені атаки відмови в обслуговуванні (DDoS), розповсюдження спаму та крадіжка даних. ШІ відіграє

ключову роль у спрощенні координації та оптимізації діяльності цих бот-мережей, роблячи їх більш потужними та важкими для розуміння загрозами.

Незважаючи на потенційні загрози, пов'язані з використанням штучного інтелекту, він також може мати позитивний вплив на захист критичної інфраструктури. Штучний інтелект може допомогти виявити аномалії мережі та аномальну активність. Це може вказувати на кібератаку. Він також може бути використаний для прогнозування майбутніх загроз та підготовки до можливих атак. Автоматизовані системи, побудовані на основі штучного інтелекту, можуть швидко реагувати на кібератаки, блокувати шкідливі дії та відновлювати системи.

Щоб ефективно використовувати штучний інтелект для захисту критичної інфраструктури, необхідно враховувати кілька аспектів. Розробка надійних моделей і алгоритмів, здатних розпізнавати нові типи загроз, є важливим завданням. Також необхідно захистити сам ШІ від атак і маніпуляцій, щоб уникнути помилкових рішень і неправильного використання систем захисту.

Також важливо враховувати питання конфіденційності та етики при використанні штучного інтелекту для збору та обробки даних. Необхідно забезпечити належний рівень захисту та конфіденційності інформації про критично важливу інфраструктуру.

Загалом, штучний інтелект може бути потужним інструментом захисту критичної інфраструктури, але його використання вимагає комплексного підходу, ретельної оцінки ризиків та застосування відповідних заходів безпеки для забезпечення надійності та захисту системи.

Література

1. Що потрібно знати про штучний інтелект. bizmag. URL: http://surl.li/nppkr
2. Що таке інфраструктура: чим цивільна відрізняється від критичної. fakty. URL: https://fakty.com.ua/ua/ukraine/20221101-shho-take-infrastruktura-chym-czyvilna-vidriznyayetsya-vid-krytychnoyi/

Антощук С. А.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, доктор економічних наук, професор

КІБЕРШАХРАЙСТВО В УКРАЇНІ В УМОВАХ ВІЙНИ

Галузь інформаційних технологій вимагає від зловмисника відповідних навичок, але вчиняти такі злочини може практично будь-хто, хто має вільний доступ до інтернету – кібершахрайство є абсолютно новим явищем, оскільки воно безпосередньо пов'язане з останніми досягненнями.

Українці воюють в інформаційному просторі, так як і на полі бою з 24 лютого 2022 року. Через вплив війни на свідомість та поведінку людей їх дії в більшості випадків є протиправними. В період війни не лише ворог провокує інформаційні атаки для підриву обороноздатності України, але й також ті, хто прагне скористатися перенавантаженістю правоохоронних органів і нажитися на коштах громадян. За перші півтора місяці війни кіберзлочинність в Україні неухильно зростала.

Зростання кількості онлайн-шахраїв, які маніпулюють вразливими українцями та іноземцями, є нагальною проблемою, з якою бореться наша правоохоронна система. Як наслідок, кіберзлочинність, зокрема, онлайн-шахрайство, зростає.

За статистикою, за 10 місяців 2023 року облікували 73160 кримінальних проваджень за ст. 190 про шахрайство. Цьогоріч зафіксували в 1,3 рази більше випадків, аніж загалом за попередні два 2021-2022 роки – 55933. Натомість від початку осені відкритих проваджень про шахрайство істотно поменшало на 17%. Восени середня кількість нових проваджень зменшилася на 17%.

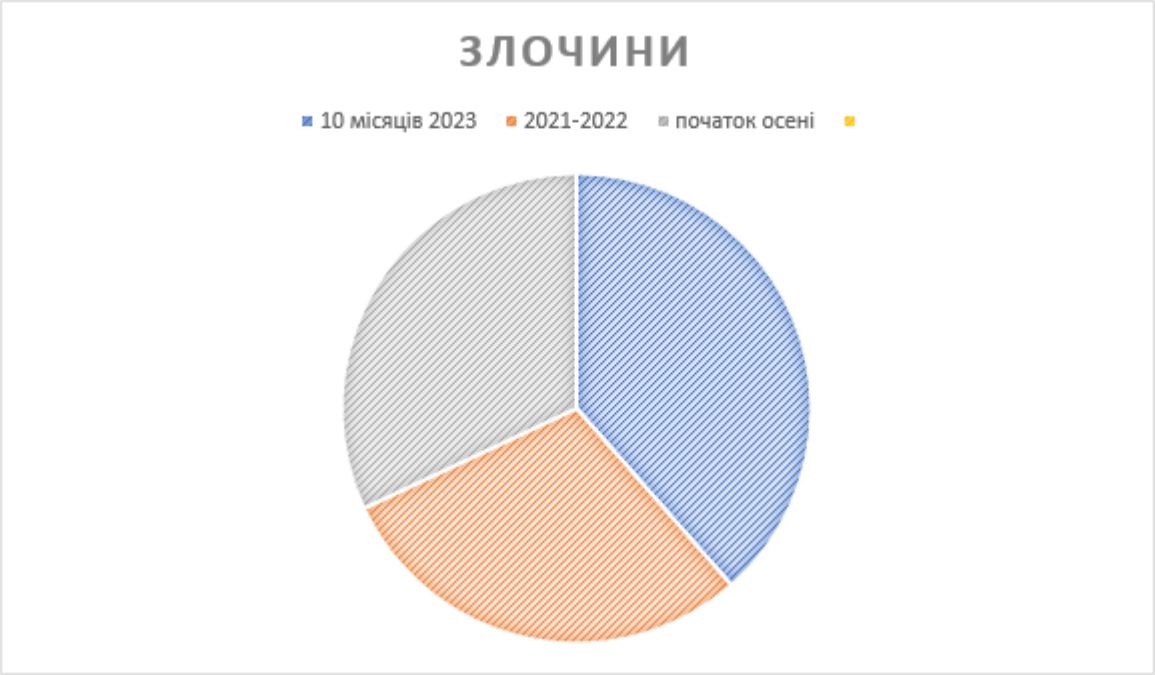

Рис. 1. Статистика скоєння кіберзлочинів за 2021-2023рр.

Відповідно до Кримінального кодексу України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (ст.190 КК України). Здійснення даного кримінального правопорушення в інтернеті науковці називають «кібершахрайством».

Відповідно до п. 8 ч. 1 ст. 1 [2], кіберзлочин (комп'ютерний злочин)– суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України. До того ж це кримінальні правопорушення, передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж».

Війна в інформаційному просторі завдає такої ж шкоди, як і на полі бою. Після початку війни парламент покращив Кримінальний та Кримінально-процесуальний кодекси, вдосконаливши підстави та процесуальні механізми притягнення до відповідальності кіберзлочинців. Ці зміни сконцентровані у двох законодавчих актах [4],[5].

Дійсно, посилення відповідальності за правопорушення, перелічені у відповідному законодавстві, підвищило ефективність боротьби з кіберзлочинністю.Розширення сфери діяльності правоохоронних органів, які розслідують кіберзлочини, посилення санкцій та додаткова криміналізація певних діянь стримують потенційних шахраїв, але

проблема полягає в тому, що кримінологічні дослідження ґрунтуються майже виключно на кримінальних даних, тоді як дослідження соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства є відсутність таких досліджень є проблемою.

Більшість випадків шахрайства сталися під час купівлі або продажу товарів онлайн (52,7%). Наступними за поширеністю були фішингові посилання (18,6%). Наступними за поширеністю були злом акаунтів у соціальних мережах (12%) та телемаркетинг (10,2%).

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Висновки. Таким чином, боротьба з кібершахрайством в Україні здійснюється за трьома основними напрямами, а саме: запобігання кіберзлочинам; загальна організація боротьби з кіберзлочинністю; застосування кримінальної відповідальності та покарання осіб, які вчиняють кіберзлочини.

Література

1. Відкриті дані Опендатабот з посиланням на дані Генеральної прокуратури України. https://uworld.news/news/shakhrai-staly-aktyvnishymy-nizh-do-1006442.html
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 No 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. http://dspace.onua.Edu.ua/handle/11300/19993
4. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» No 2137-IX від 15 березня 2022 року. https://ips.ligazakon.net/document/view/T222137?an=1
5. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. https://zakon.rada.gov.ua/laws/show/2149-20#Text.
6. Стаття 12 із змінами, внесеними згідно із Законом України від 17.06.2020 р. N 720-IX. https://zakon.rada.gov.ua/laws/show/720-20#Text.

Баб'як А. В.

завідувач кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Вдосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності є одним із напрямів підвищення результатів діяльності оперативних підрозділів Національної поліції. Над окресленою проблемою працює чимало

вітчизняних учених: Бірюков Г.М. Бусол О.Ю. Никифорчук Д.Й. [1]; Захаров В.П. [2; 3]; Мовчан А.В. [4] та ін.

Як засвідчує вивчення оперативної ситуації на практиці, значення аналітичного забезпечення в організації оперативно-розшукової діяльності Національної поліції ще недостатньо усвідомлено не тільки особовим складом оперативних підрозділів, а й окремими їх керівниками.

Безперечно, аналітична робота має стати центральною координаційною ланкою інформаційно-аналітичного забезпечення оперативно-розшукової діяльності оперативних підрозділів Національної поліції для виконання таких завдань стратегічного характеру:

- встановлення інфраструктури стійких суспільно небезпечних злочинних груп ступеня їх впливу й проникнення у пріоритетні напрями економіки бюджетну сферу, діяльність державних інституцій, а також наявності корумпованих, міжрегіональних і міжнародних злочинних зв'язків, озброєності, технічної оснащеності тощо;
- виявлення криміногенних й антикриміногенних чинників, що впливають на характер протиправної діяльності злочинців;
- вивчення тенденцій розвитку злочинності, визначення нових механізмів протиправної діяльності груп, характерних ознак діяльності їх лідерів, а також їх уразливості;
- встановлення повного ланцюга економічних зв'язків як складової економічного підґрунтя злочинності, схем і механізмів одержання й легалізації доходів, отриманих злочинним шляхом;
- вивчення сучасного стану боротьби з корупцією і неправомірною винагородою у сферах, що мають стратегічне значення для економіки держави, серед осіб, які обіймають впливові посади,
- підготовка відповідних рекомендацій щодо вдосконалення організації роботи за основними напрямами діяльності оперативних підрозділів Національної поліції по виявленню кримінальних правопорушень у бюджетній сфері.

Отже, інформаційно-аналітичне забезпечення оперативно-розшукової діяльності оперативних підрозділів Національної поліції має функціонувати у трьох напрямах:

- підготовка регулярних аналітичних оглядів щодо змін оперативної обстановки, поточних подій і чинників, що на них впливають, для своєчасного інформування керівництва й прийняття необхідних управлінських рішень;
- довгострокова оцінка процесів і тенденцій, що відбуваються на окремій території чи об'єктах (у сферах, галузях), рівня розвитку й утворення ймовірних негативних наслідків;
- вивчення окремих питань за завданням оперативних підрозділів Національної поліції для заповнення прогалин в конфіденційно-оперативному й інформаційному супроводі матеріалів оперативно-розшукових справ, розробка в яких потребує додаткового використання заходів інформаційно-аналітичного забезпечення.

Реалізувати ці напрями можливо через такі види доведення інформації:

- **прогностичний аналіз** – вивчення стану й тенденцій розвитку злочинності в регіоні, чинників, що на них впливають, отримання ймовірних висновків (прогнозів) про можливі зміни оперативної обстановки й вироблення пропозицій до комплексу заходів щодо попередження наслідків. Проводячи

прогностичний аналіз, доцільно використовувати методи екстраполяції, експертних оцінок, аналогії, евристичні методи й ін;

- **проблемний аналіз** – дослідження (зокрема із залученням фахівців) конкретних проблем оперативно-розшукової діяльності у напрямі протидії злочинності й корупції в регіоні для надання пропозицій і рекомендацій щодо прийняття стратегічних і тактичних рішень у складних і трудомістких питаннях. При проведенні проблемного аналізу бажано використовувати методи експертних оцінок, економіко-правового, фінансового, системного, структурно-функціонального аналізу, контент-аналізу, аналізу мережі зв'язків й т. ін.;
- **комплексний аналіз** – вивчення оперативної обстановки в регіоні загалом або її окремих елементів за визначений період (квартал, півріччя, рік) для вироблення заходів щодо протидії злочинності й удосконалення оперативно-розшукової діяльності оперативних підрозділів Національної поліції. У процесі комплексного аналізу доцільно використовувати методи системного, структурно-функціонального, факторного аналізу, експертних оцінок, екстраполяції та ін.;
- **оперативний аналіз** – дослідження окремих елементів оперативної обстановки в регіоні, ґрунтуючись на поточній (добовій, декадній) інформації, щоб отримати дані для ситуаційного оперативного реагування та прийняття управлінських рішень з окремих питань оперативно-розшукової діяльності. Для оперативного аналізу застосовуються статистичні методи швидкої оцінки стану організованої злочинності, зокрема із застосуванням інформаційних технологій.

Одним із завдань інформаційно-аналітичного забезпечення оперативно-розшукової діяльності оперативних підрозділів Національної поліції є автоматизація основних технологічних процесів із накопичення й обробки оперативно-важливої інформації, що сприятиме покращанню рівня та результативності проведення оперативно-розшукових заходів, спрямованих на викриття та припинення діяльності, окремих осіб, що становлять оперативний інтерес, дослідженню й прогнозуванню негативних тенденцій і подій, що відбуваються в соціальній сфері та певною мірою впливають на стан криміногенної обстановки, тощо.

На сучасному етапі системна обробка оперативно-значимої інформації здійснюється в рамках автоматизованих інформаційних систем, кожній з яких властиві наступні загальні характеристики:

- інформаційна система являє собою упорядковану сукупність елементів;
- елементи системи взаємозалежні, вони взаємодіють у рамках цієї системи та є її підсистемами;
- система виконує певну функцію;
- елементи системи можуть взаємодіяти із зовнішнім середовищем і змінювати при цьому свій зміст і внутрішню будову;
- кожна інформаційна система існує не тільки в часі, але й у просторі[5].

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності як самостійний і важливий напрям оперативно-службової діяльності оперативних підрозділів Національної поліції потребує детальнішої наукової розробки, проте увагу акцентовано на наявності проблем, запроваджено окремі шляхи їх розв'язання.

Література

1. Аналітична робота в оперативно-розшуковій діяльності: навчально-практичний посібник / Никифорчук Д.Й., Бусол О.Ю. Бірюков Г.М. – К., 2012. – 152 с.
2. Захаров В.П. Проблеми інформаційного забезпечення боротьби зі злочинністю: монографія / В.П. Захаров. – Львів. ЛьвДУВС, 2008. – 472 с.
3. Захаров В.П. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник / В.П. Захаров, В.І. Рудешко – 2-ге вид. доп. – Львів. ЛьвДУВС, 2015. – 492 с.
4. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А.В. Мовчан – Львів. ЛьвДУВС, 2017. – 244 с.
5. Галючек А.А. Інформаційне та аналітичне забезпечення оперативно-розшукової діяльності спеціальних підрозділів по боротьбі з організованою злочинністю ОВС: методичні рекомендації / А.А. Галючек, В.Ю. Журавльов. – Запоріжжя: Запорізький юридичний інститут ДДУВС, 2008. – 59 с.

Бондаренко В. А.

доцент кафедри іноземних мов та культури фахового мовлення факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ТЕОРЕТИКО-ПРАВОВА СУТНІСТЬ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ

Розвиток інформаційного суспільства та перехід до суспільства знань нерозривно пов'язані з посиленням значення достовірності інформації. Поширення фейкової інформації, необхідність повторної перевірки практично будь-якої інформації, що циркулює через засоби масової комунікації, детермінують осмислення проблем достовірності інформації вже на якісно іншому рівні з метою правового забезпечення інформаційної безпеки, виділеної як пріоритетне спрямування державної політики та визначеної Стратегією інформаційної безпеки України, спрямованої на формування безпечної середовища обороту достовірної інформації [1].

Питання реалізації національних інтересів в інформаційній сфері закріплені в національній Доктрині інформаційної безпеки України, що є документом стратегічного планування в даній галузі [2]. У правовій системі вимога достовірності інформації, що традиційно розглядається стосовно низки офіційних інформаційних процесів, починає переосмислюватися на якісно іншому рівні. Забезпечення достовірності інформації у суспільстві знань стає одним із критеріїв формування суспільства принципово нового типу.

Достовірна інформація є одночасно цінністю та умовою соціально-економічного розвитку державних та громадських інститутів. Очевидне збільшення потреб світової спільноти в об'єктивній, достовірній та своєчасній інформації про суспільні процеси є однією з важливих особливостей сучасного етапу глобалізації, широкого застосування глобальних інформаційних систем.

Відповідність фактам, що мали місце насправді – ось одна з властивостей інформаційного контенту, залежно від інформації визнається достовірною чи недостовірною.

Така категорія як «недостовірна інформація» може містити два елементи, – це хибні відомості, що ганьблять честь, гідність, добре ім'я та ділову репутацію, а також

відомості антидержавного характеру. Зауважимо, що мають рацію ті, хто вважає, що суспільні відносини у сфері обігу недостовірної інформації, як правило, врегульовані двома філософськими категоріями – мораллю і правом.

Диференціювання областей впливу кожної може здійснюватися залежно від завданих при обігу недостовірної інформації шкоди. Причому також важливе значення має приділятися об'єкту, якому така шкода завдається. У законі «Про доступ до публічної інформації» закріплено універсальний підхід до групі відносин, розглядають. Закон свідчить, що у разі, якщо внаслідок неправомірної відмови у доступі до інформації, невчасного надання, надання недостовірної або не відповідної змісту запиту інформації були заподіяні збитки, такі збитки підлягають відшкодуванню відповідно до цивільного законодавства [3].

Щодо окремих об'єктів протиправного посягання, здійснюваного при обороті недостовірної інформації, значність збитків має бути оцінена диференційовано, специфічно, з позиції ситуаційного підходу. Це знаходить відображення в адміністративно-юрисдикційній та кримінально-процесуальній практиці правоохоронних органів.

Доцільно класифікувати недостовірну інформацію, заклавши в основу критерії: спосіб обороту інформації; сфера дезорганізованих суспільних відносин; суб'єкт поширення відомостей, наявності спеціального правового статусу; суб'єктивна сторона інформаційного делікту, яка може виражатися за допомогою поінформованості адресанта інформації про її недостовірність; наявність спеціального правового статусу в отримувача недостовірної інформації (наприклад, неповнолітній); наявність додаткових об'єктів зазіхання (честь, гідність, добре ім'я чи ділова репутація); наявність несприятливих матеріальних наслідків поширення недостовірної інформації.

Недостовірна інформація – це будь-які відомості, які не відображають об'єктивну дійсність, обіг яких загрожує конституційним засадам країни, зазіхає на права та законні інтереси особи, оборону держави та її безпеку.

Необхідною є конкретизація переліку об'єктів-носіїв честі, гідності та ділової репутації, які можуть постраждати від поширення недостовірної інформації. Збитки від негативного впливу недостовірної інформації зумовлюються багато в чому та рівнем соціально-культурного, економічного та інформаційно-технологічного розвитку соціуму та держави.

Чим активніше залучення різних верств населення до інформаційних правовідносин, чим доступніші технічні засоби комунікації, тим вища небезпека зловживання свободою слова та інформації, пов'язаного з обігом шкідливої інформації. Відповідно, інтенсивності комунікаційних систем має відповідати темпу інтенсивності розробки та прийняття правових засобів регулювання таких непростих інформаційних відносин.

Література

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL. https://zakon.rada.gov.ua/laws/show/685/2021#Text
2. 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. URL. https://zakon.rada.gov.ua/laws/card/47/2017
3. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL. https://zakon.rada.gov.ua/laws/card/2939-17

Борисова К. Є.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Світличний В. А.
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У OSINT

Технологія **OSINT (Open Source Intelligence)** знайшла застосування в різних галузях. Вона складається з різноманітних публічних джерел, таких як: наукові публікації, джерела ЗМІ, веб-контент та публічні дані. В нашій роботі увагу буде приділено веб-контенту, а саме використанню соціальних мереж.

Питання конфіденційності та поширення даних турбують кожного, адже щоденний обіг інформації, що поширюється та транслюється, за допомогою доступних платформ, набирає значимих обертів та надає поштовх до розгляду тематики використання соціальних мереж як джерела інформації, відкритої для громадськості.

Розглядаючи дану тему, слід зазначити аспекти використання соціальних мереж у вирішенні завдань OSINT (інформація, яку можна здобути):

- **Визначення зв'язків та мереж взаємодії.** Використання соціальних мереж для встановлення взаємозв'язків між особами та виявлення ключових фігур або груп.
- **Геолокаційний аналіз через геотеги та місцезнаходження.** Використання інформації про місцезнаходження у соціальних мережах для визначення фізичного положення користувачів..
- **Моніторинг інтересів та активності.** Аналіз публікацій, взаємодій та інтересів користувачів для розуміння їхнього ставлення та поведінки.
- **Детекція дезінформації та фейкових акаунтів.** Використання соціальних мереж для виявлення штучно створених профілів та розповсюдження дезінформації.
- **Побудова психологічного профілю за допомогою соціальних мереж.** Використання поведінкових відомостей на платформах соціальних мереж для аналізу психологічних характеристик осіб.

Зазначаючи вказані аспекти використання загалом ми говоримо про ідентифікацію та аналіз інформації, яку користувачі розміщають у своїх профілях, на персональних сторінках. Слід пам’ятати, що вище перелічена інформація, може використовуватися як правоохоронними органами, так й зловмисниками.

Вказавши та розглянувши основні аспекти використання соціальних мереж у OSINT розуміємо, що технологія зводиться до того, що ви просто аналізуєте всю доступну інформацію про когось в Інтернеті. Існує два способи аналізу: ручний пошук і автоматизація.

Дуже небагато ситуацій, коли ручний пошук інформації справді доречний, лише коли вам потрібно шукати на дуже конкретному веб-сайті або чітко окресленому ряду сторінок, які не аналізуються доступними інструментами (або вам потрібно проаналізувати одне чи два джерела, і немає сенсу у використанні інструментів).

У більшості випадків спосіб «автоматизації» є більш затребуваним та доцільний, адже фреймворк (посередник між шукачем і процесором) має кращі та більш ефективніші результати. Автоматизація включає в себе програмні інструменти, різноманітні утиліти. Вбачаємо необхідним аналіз сучасного набору інструментів для

виконання вказаних загальних завдань. На сьогоднішній день, можемо запропонувати вашій увазі наступний перелік [1]:

- **Maltego** – це графічний інструмент для збору та аналізу інформації з різних джерел, включаючи соціальні мережі. Він дозволяє користувачам візуалізувати дані та взаємозв'язки між різними об'єктами.
- **Spiderfoot** – це інструмент розвідки з відкритим вихідним кодом, що володіє безліччю функцій, включаючи можливість отримувати та аналізувати IP-адреси, діапазони CIDR, домени та піддомени, ASN, адреси електронної пошти, телефонні номери, імена та імена користувачів, адресу BTC та багато іншог.
- **Alfred** – утиліта для збору інформації та ідентифікації акаунтів у соціальних мережах.
- **Social Searcher** – безкоштовний інструмент для моніторингу соціальних мереж.
- **Google Alerts** – повідомляє вас про появу в інтернеті вказаної інформації.
- **Телеграм чат-боти**, тощо.

Підсумовуючи зробимо наступний висновок: тема «Використання соціальних мереж у OSINT» є важливою для розгляду у сучасному світі, адже обсяги інформації, яку можна отримати у вільному доступі є суттєвими. Існує безліч інструментів для автоматизованого пошуку та певні алгоритми ручного, все це використовується як правоохоронними органами, так й зловмисниками, тому більш детальний розгляд та постійне приділення уваги вказаному питанню є важливим превентивним заходом, на котрий слід звернути увагу.

Література

1. Найкращі інструменти для розвідки на основі відкритих джерел (OSINT) у 2023 році | TheTransmitted. URL: https://thetransmitted.com/security/najkrashhi-instrumenti-dlya-rozvidki-na-osnovi-vidkritih-dzherel-osint-u-2023-roczi/

Боровікова В. С.
аспірант кафедри загально-правових дисциплін Інституту права Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНИЙ ОБЕРТ ЯК ПРАВОВЕ ЯВИЩЕ

Інформація виступає важливим компонентом розвитку суспільства. Сучасне громадянське суспільство поступово перетворюється в інформаційне. Інформаційне суспільство розвивається стрімкими темпами, цей розвиток позначається на характері суспільних відносин, які формуються між людьми, а також між населенням та державою.

Створення єдиного інформаційного простору, формування та розвиток якого необхідне для забезпечення оперативного доступу громадян до відомостей, які є в інформаційних системах, у тому числі в Єдиних та державних реєстрах, а також з метою реалізації повноважень органів публічного управління у сфері управління економікою, безпекою особи, суспільства та держави з переважним використанням інформаційних систем.

При правовому регулюванні використання інформаційних систем важливу роль відіграє проблема встановлення порядку оберту інформації. Інформація, як об'єкт

діяльності, носить різноманітний характер, але з правової точки зору може бути визначена як – відомості, повідомлення, дані незалежно від форми подання. Права на маніпуляції з інформацію закріплені у низці статей Конституції України, що передбачає важливість і значущість захисту державою, але, водночас, обсяг інформаційного простору, де реалізуються дані права дуже широкий, що ускладнює процес регламентації інституту інформаційного оберту.

У межах інформаційних правовідносин існує певна правова невизначеність, виражена у відсутності формального, легітимного визначення низки явищ, які існують у межах інформаційних правовідносин. До них можна віднести інформаційний оберт. В інформаційному праві інформаційний оберт використовується у контексті наукових досліджень, але даний термін не знайшов відображення в законодавчих правових актах.

Інформаційний оберт – це процес виробництва, зміни, накопичення, поширення інформації незалежно від її природи, носія, масовості, правового обмеження доступу.

Залежно від специфіки інформаційний оберт можна розділити на декілька видів: оберт бібліотечної інформації, цивільно-правовий оберт інформації, оберт інформації, що відноситься до таємниці, оберт публічної інформації. Цей перелік можна продовжувати. Особливості оберту інформації висвітлюються у наукових працях та нормативно-правових актах, наприклад, у законі України «Про доступ до публічної інформації» [1].

Розуміння формування регуляції інформаційного оберту у загальному значенні дано у законі «Про інформацію» [2]. Цей нормативно-правовий акт не є першим у цій галузі. Закон «Про електронні комунікації» визначає правову основу технічних особливостей функціонування мережі Інтернет, визначає режим доступу до інформації, правову основу обмеження доступу, що дає уявлення про оберт інформації в мережі Інтернет, соціальних мережах [3].

Закон «Про публічні електронні реєстри» визначає доступ до інформаційних ресурсів, створює матеріальну основу для низки статей адміністративного і кримінального кодексу, визначає права та обов'язки окремих суб'єктів інформаційного оберту, інші особливості функціонування інститутів інформаційного права [4].

Загальні засади оберту інформації визначає закон «Про медіа» [5]. У контексті даного закону інформаційний оберт як явище може бути представлений як: законний – коли оберт інформації не порушує законодавства та розглядається як природна властивість функціонування суспільства держави; незаконним – якщо законодавство порушується. Незаконний інформаційний оберт завдає шкоди певним групам населення, або державі.

Складно говорити про форму регламентації деяких суміжних суспільних відносин, що безпосередньо чи опосередковано стосуються даного інституту, наприклад, право людини на виробництво, зміну, зберігання та поширення інформації, оскільки ці процеси спрямовані на входження у єдиний європейський інформаційний простір та пов'язані з реалізацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [6].

Інформаційний оберт є динамічним і безперервним явищем. Дієвими нормами регламентації даних відносин будуть ті, що не торкаються приватної сфери, тобто інформація розмішується в публічному просторі, де її поширення свідомо спрощено через її природу – в мережі Інтернет. Це реалізується у межах регламентації інформаційного оберту. Важливим аспектом інформаційного оберту є залежність від чинного законодавства. Цифровізація впливає на розвиток публічно-правового регулювання оберту інформації, яке розширюється у сфері використання цифрової

інформації та застосування інформаційних технологій фізичними і юридичними особами, органами публічної влади.

Незалежно від виду оберту інформації процес буде регламентований загальними принципами, які можна описати так:

- забезпечення прав громадян на маніпуляції з інформацією – цей принцип передбачає можливість виробляти, змінювати, накопичувати, публікувати інформацію вільно, у межах чинного законодавства;
- забезпечення свободи вибору засобів отримання інформації – державна монополія виробництва інформації не може бути метою даного інституту, метою є формування інформаційного простору, у якому використовуються різні форми (електронна та матеріальна) і джерела;
- збереження традиційних для громадян (відмінних від цифрових) форм отримання інформації про товари та послуги – важливий аспект здорового інформаційного клімату, є збереження різних форм інформації, оскільки перехід до виключно віртуальних форм надання інформації розуміється як заміщення реальних передумов та джерел віртуальними;
- забезпечення законності та розумної достатності при збиранні, накопиченні та розповсюдженні інформації про фізичних та юридичних осіб – цей принцип передбачає правову обґрунтованість збору даних за умови достатніх підстав;
- забезпечення державного захисту інтересів фізичних і юридичних осіб в інформаційній сфері – цей принцип є важливим в аспекті формування інформаційного суверенітету, оскільки виходить із реальних обов'язків держави, передбачених Стратегією інформаційної безпеки України [7].

Резюмуючи вище зазначене, інформаційний оберт – це ще не сформована категорія, визначення якої можливе при наявності науково обґрунтованих принципів даного інституту інформаційного права. Позитивні тенденції у формуванні інституту інформаційного оберту очевидні, але норми мають формальний характер, оскільки їх застосування обмежене не визначеністю прав суб'єктів подібних відносин, обсягом інформаційного середовища.

Література

1. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL. https://zakon.rada.gov.ua/laws/card/2939-17
2. Про інформацію: Закон України від 02.10.1992 р.№ 2657-XII. URL. https://zakon.rada.gov.ua/laws/card/2657-12
3. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL. https://zakon.rada.gov.ua/laws/show/1089-20#Text
4. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL. https://zakon.rada.gov.ua/laws/show/1907-20#Text
5. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. URL. https://zakon.rada.gov.ua/laws/show/2849-20#Text
6. Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL. https://zakon.rada.gov.ua/laws/show/984_011#Text
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL. https://zakon.rada.gov.ua/laws/show/685/2021#Text

Бортник Н. П.
професор кафедри теорії та історії держави і права Національного кораблебудівного університету, доктор юридичних наук, професор
Єсімов С. С.
професор кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ВІРТУАЛЬНИХ АКТИВІВ І ЦИФРОВИХ ГРОШЕЙ

Світова валютна система характеризується масовим поширенням цифрових грошей, що використовуються для опосередкування товарно-грошових відносин, у спекулятивних цілях отримання короткострокової прибутку з допомогою високої волатильності, і навіть анонімної передачі коштів. Можливості цифрових валют дозволяють використовувати для опосередкування виробництва, споживання, розподілу, інвестиційної та трейдингової діяльності, відмивання прибутків, отриманих незаконним шляхом.

У 2020-2021 роках в окремих країнах почали випускати цифрові валюти центральних банків, які мають потенціал трансформації світової валютної системи на новій соціально-економічній та науково-технічній базі.

З розвитком сучасних технологій, з'явилася можливість проводити грошові угоди у реальному часі. Виникла потреба у поліпшенні платіжної системи. З кожним роком відбувається дедалі більше змін, пов'язаних із грошовими операціями. Величезний стрибок у цьому питанні стався в період пандемії 2020 року. Оскільки більшість компаній були змушені працювати в режимі реального часу, то угоди, пов'язані з фінансовими операціями, відбувалися в безготівковому форматі. Ситуація, що склалася в усьому світі показала, що кожна держава, що розвивається, потребує модернізації механізму грошової платіжної системи.

Цей механізм повинен швидко і ефективно вирішувати питання, пов'язані з фінансовими операціями в режимі реального часу. На законодавчому рівні порушуються питання альтернативного грошового обігу, розвиток цифрових грошей та запровадження її як нового фінансового інструменту для здійснення платіжних операцій. Проблеми правового регулювання віртуальних активів та цифрових грошей знаходять своє відображення у науці фінансового права. У зв'язку з цим питання про проблеми правового регулювання віртуальних активів та цифрової фінансової валюти є актуальним.

З метою регулювання віртуальних активів було ухвалено закон «Про віртуальні активи» (не набрав чинності) [1]. Цей закон регулює відносини, що виникають під час випуску, обліку та обігу цифрових фінансових активів. У законах було закріплено поняття «віртуальні активи» та «цифрові гроші Національного банку України» [2].

Відповідно до закону «Про віртуальні активи», віртуальними активами визнаються цифрові права, що включають грошові вимоги, можливість здійснення прав з емісійних цінних паперів, права участі в капіталі непублічного акціонерного товариства, внесення записів до інформаційної системи на основі розподіленого реєстру, а також в інші інформаційні системи.

Аналіз особливостей правового регулювання віртуальних активів дозволяє зробити ряд висновків: випуск, облік та звернення здійснюється шляхом додавання записів до інформаційної системи на основі розподіленого реєстру; права, засвідчені цифровими віртуальними активами, виникають у їхнього першого власника з моменту

внесення до системи запису про зарахування таких активів (право на внесення таких записів виникають тільки ц фізичних осіб-підприємців та юридичних осіб); Закон передбачає можливість укладати угоди з купівлі-продажу віртуальних активів, а також обмін одного виду цифрових віртуальних активів на такі ж активи іншого виду. Закон допускає вчинення інших угод, але при цьому не конкретизує (це можуть бути, наприклад, надання як забезпечення зобов'язань, дарування та інше); угоди з віртуальними активами укладаються через операторів обміну віртуальних активів, якими можуть бути банки та інші юридичні особи.

Під цифровими грошима розуміється сукупність електронних даних (цифрового коду або позначення), що містяться в інформаційній системі, які пропонуються і можуть бути прийняті як засіб платежу, який не є грошовою одиницею України, грошовою одиницею іноземної держави або міжнародною грошовою або розрахунковою одиницею, і як інвестицій, щодо яких відсутня особа, зобов'язана перед кожним власником таких електронних даних, за винятком оператора та вузлів інформаційної системи, зобов'язаних забезпечувати відповідність порядку випуску електронних даних та здійснення щодо них дій для внесення записів до такої інформаційної системи за її правилами. Легалізацію цифрових грошей в Україні здійснено Законом України «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг» [3].

Можна виділити такі особливості цифрових грошей: представляє сукупність електронних даних у системі; цифрові гроші не ставитиметься до грошової одиниці держави; її можна сприйняти як інвестиції або засіб платежу, який не є грошовою одиницею; потенційно цифрові гроші можуть виконувати всі фінансові функції; щодо цифрових грошей за загальним правилом немає особи, зобов'язаної перед кожним власником таких електронних даних; цифрові гроші визнається майном. Це в практичному плані означає, що вона може бути предметом розкрадання, неправомірної вигоди, засобами легалізації доходів, отриманих злочинним шляхом, може включатися до складу майна, за рахунок якого формується конкурсна маса та погашаються борги; юридичним особам, які діють за правом України, філіям, представництвам та іншим відокремленим підрозділам міжнародних організацій та іноземних юридичних осіб, компаній та інших корпоративних утворень, створених на території України, а також фізичним особам забороняється приймати цифрові гроші як платежу за товари, роботи, послуги у межах національної юрисдикції; судовий захист вимог, пов'язаних із володінням цифровими грошима, можливий лише у разі повідомлення про факти володіння цифровими грошима та вчинення цивільно-правових угод і операцій з цифровими грошима у порядку, встановленому законодавством про податки та збори; забороняється поширювати відомості про пропозицію та прийом цифрових грошей як спосіб оплати товарів, робіт і послуг.

Є два види активів: віртуальні активи, які мають цифрові права певного виду, та цифрові гроші. Віртуальні активи відрізняються від цифрових грошей тим, що вони випущені конкретною фізичною або юридичною особою, яка має виконати вимоги, закріплені законодавством про віртуальні активи. За змістом Цивільного кодексу України, який закріплює види об'єктів цивільних прав, цифрові активи є різновидом цифрових прав [4]. Цивільний кодекс України не передбачає поняття цифрових грошей, швидше за все це поняття потрапляє до категорії іншого майна.

Аналіз законодавчих норм у сфері правового регулювання віртуальних активів виявив проблеми: на сьогоднішній день законодавство не регулює купівлю-продаж крипто-активів фізичними особами без посередників; регулювання можливе лише для певних видів цифрових активів; відсутність публічних звітів для учасників крипто ринку; відсутність страхування під час інвестиції у віртуальні активи.

На даний момент немає одноманітної правозастосовної практики щодо визначення правової природи цифрових грошей. Незважаючи на те, що цифрові гроші активно використовуються учасниками господарського обороту, їх використання не позбавлене значних недоліків: атаки хакерів: дана проблема вважається другою за масштабністю і часто з'являється в країнах, що розвивають цифрові гроші та крипто валюту; існують юридичні ризики: інвестори підлягають великим ризиком, оскільки на законодавчому рівні не передбачено страхування вкладників, які не можуть претендувати на відшкодування збитків; втрата секретного коду: код-ключ до биткоен-гаманця. Втрата коду означає втрату всіх активів у гаманці.

Цифрові гроші є новим фінансовим інститутом. Інтерес до цифрових грошей зростає з кожним днем. Для повного регулювання цього питання необхідно, щоб усі необхідні положення були закріплені на законодавчому рівні.

Література

1. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX.URL. https://zakon.rada.gov.ua/laws/card/2074-20
2. Про платіжні послуги: Закон України від 30.06.2021 р. № 1591-IX.URL. https://zakon.rada.gov.ua/laws/card/1591-20
3. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг: Закон України від 12.01.2023 р. № 2888-IX. URL. https://zakon.rada.gov.ua/laws/card/2888-20
4. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL. https://zakon.rada.gov.ua/laws/show/435-15#Text

Ботнаренко І.А.

старший науковий співробітник наукової лабораторії з проблем протидії злочинності навчально-наукового інституту № 1 Національної академії внутрішніх справ, кандидат юридичних наук

КРИТИЧНА ІНФРАСТРУКТУРА В УКРАЇНІ ТА ЇЇ СКЛАДОВІ: ПОНЯТТЯ, ЗМІСТ ТА ЗАКОНОДАВЧЕ ВИЗНАЧЕННЯ

Термін «критична інфраструктура» вперше зафіксовано у директиві PDD-63 (Presidential Decision Directive), підписаній у 1996 році президентом Сполучених Штатів Америки (далі – США) Б. Клінтоном. Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі, а також закладено вимогу щодо забезпечення безпеки критичних елементів інфраструктури [1]. В подальшому питанням, пов’язаним з безпекою об’єктів критичної інфраструктури, почали приділяти увагу і в інших країнах (Великій Британії, Нідерландах, Німеччині, Польщі, Словаччині, Угорщині, Чеській Республіці та ін). Важливим у цьому відношенні є те, що у деяких національних законодавствах зарубіжних країн при визначенні цього поняття акцентовано на функціях та послугах об’єктів критичної інфраструктури – саме вони є в основі визначення їх критичності, що, відповідно, дає методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту [2, с. 6]. Наприклад, у законодавстві США під терміном «критична інфраструктура» розуміють «системи та ресурси, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що

недієздатність або знищення таких систем або ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого» (Patriot Act, 2001) [3]. У Польщі критична інфраструктура була визначена законом «Ustawa on bezprieczenstwie obywatelskim» як функціонально пов'язані засоби виробництва, установи, послуги, які є ключовими для безпеки країни та її громадян, для забезпечення належного функціонування як державних, так і органів самоврядування та комерційного (приватного) сектору [4].

Терміном «критична інфраструктура» (лат. infra – «нижче», «під» та лат. structura – «будівля», «розташування») зазвичай охоплюють об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної та економічної сфери держави, негативно позначиться на рівні її обороноздатності та національної безпеки. Функціонування критичної інфраструктури в мирний час пов'язують із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки та захищеності [5]. Категорії (ознаки), за якими певні об'єкти відносять до критичної інфраструктури, визначають як: 1) особливо важливі; 2) життєво важливі; 3) важливі; 2) необхідні (ч. 2 ст. 10 Закону України «Про критичну інфраструктуру»).

В Україні критичною інфраструктурою переважно називають енергетичну, газову та транспортну системи. Однак, зміст цього поняття насправді є набагато ширшим.

В Україні основними документами, які регулюють правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури, э: 1) Закон України від 16 листопада 2021 р. «Про критичну інфраструктуру»; 2) Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури»; 3) Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. «Про схвалення Концепції створення державної системи захисту критичної інфраструктури». Поняття критичної інфраструктури ми можемо зустріти і в інших нормативно-правових актах, а саме: Директиві Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту; Постанові від 14.03.2018 р. № 309 «Про затвердження Кодексу системи передачі»; Постанові Кабінету Міністрів України від 23.08.2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Не дивлячись на існування зазначених нормативних актів та зважаючи на нинішню воєнну ситуацію (особливо за наявних реальних загроз державній безпеці в енергетичній сфері), питання захисту критичної інфраструктури та забезпечення безперервності та стійкості її функціонування на сьогодні постає одним із надзавдань державних інституцій. Критична інфраструктура, наголошує О.П. Єрменчук, завжди була і залишається першочерговим об'єктом захисту та джерелом інтересу агресора чи важливим об'єктом, що може бути уражений різного роду факторами, в т.ч. не лише соціального, а і природного характеру [6]. Тому важливість розуміння правової визначеності та змісту указаного поняття, а також його складових поза сумнівом, що підсилюється при створені єдиної системи фізичного захисту енергетичної інфраструктури в Україні та адекватному реагуванні на безпекові виклики.

У Постанові Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23 серпня 2016 р. № 563 зазначений термін визначено як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу чи руйнування яких може мати вплив на національну безпеку й оборону, природне середовище, призвести до значних фінансових збитків і людських жертв [7].

Згідно з Постановою Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 14.03.2018 р. № 309 «Про затвердження Кодексу системи передачі», критична інфраструктура – сукупність об'єктів системи передачі або її частини, що входять до складу ОЕС (об'єднана енергетична система – прим. авт.) України, та є необхідними для забезпечення життєво важливих для суспільства функцій, охорони здоров'я, безпеки та добробуту населення, виведення з ладу або руйнування яких матиме суттєвий вплив на національну безпеку та оборону, навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв [8].

П. 9 ст. 1 Закону України від 16 листопада 2021 р. «Про критичну інфраструктуру» досить лаконічно визначено критичну інфраструктуру – сукупність об'єктів критичної інфраструктури. Об'єктами критичної інфраструктури, відповідно до зазначеного закону (п. 13 ст. 1), є об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [9].

За визначенням, наведеним в Директиві Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту, критична інфраструктура» означає об'єкт, систему, або її частину, розташовану в державах-членах, що є суттєвою для підтримки життєво важливих громадських функцій, здоров'я, безпеки, захищеності, економічного або соціального добробуту населення, пошкодження або знищення якої матиме істотний вплив у державі-члені через неспроможність такої інфраструктури підтримувати згадані функції [10].

Критична інфраструктура – це підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв [11].

І.В. Уряднікова та В.М. Заплатинський поняття критичної інфраструктури тлумачать як фізичні та віртуальні системи, об'єкти і ресурси – руйнування, знищення або зниження дієздатності яких, призведе до суттєвих загроз країні (регіону або міста), її національної безпеки, життєдіяльності та здоров'ю населення [12].

Основною ідеєю формування та функціонування об'єктів критичної інфраструктури в країні В.І. Франчук та П.Я. Пригунов називають необхідність створення таких двох видів умов для реалізації: 1) базових потреб людини; 2) життєво важливих функцій держави в мирний час, в умовах надзвичайного стану, воєнного стану та стану війни. З огляду на зазначене, науковці тлумачать поняття критичної інфраструктури України як сукупність об'єктів незалежно від форми власності, що реалізують функції, виробляють товари (послуги), які є життєво необхідними для людей і діяльності країни та порушення яких призведе до дестабілізації суспільних відносин [1].

Отже, законодавче і наукове розуміння поняття критичної інфраструктури в Україні на сьогодні зведено до таких визначень: 1) сукупність об'єктів; систем та ресурсів; 2) сукупність об'єктів інфраструктури держави; 3) підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології і телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство; 4) сукупність об'єктів,

технологій, державних і наукових структур; 5) об’єкти, системи, мережі або їх частини; системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги [5].

Станом на сьогодні, об’єктами критичної інфраструктури вважаються підприємства та установи в таких сферах, як урядування та надання найважливіших публічних (адміністративних) послуг, енергозабезпечення (у тому числі постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров’я, фармацевтична промисловість, виготовлення вакцин, стале функціонування біолабораторій, інформаційні послуги, електронні комунікації, фінансові послуги, транспортне забезпечення. оборона, державна безпека, правопорядок, здійснення правосуддя, тримання під вартою, цивільний захист населення та територій, служби порятунку, космічна діяльність, космічні технології та послуги, хімічна промисловість, дослідницька діяльність [9].

Вітчизняними нормативно-правовими актами встановлено такі види об’єктів критичної інфраструктури, які потребують захисту: 1) особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення; 2) життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення; 3) важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення; 4) необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Отже, відповідно до чинного законодавства, об’єкти інфраструктури можуть бути віднесені до критично важливих за наявності відповідності не менше одному (законодавче формулювання – «за сукупністю») з критеріїв (ступенів важливості для забезпечення окремих життєво важливих функцій) віднесення об’єктів до критично важливих, зазначених в ч. 3 ст. 8 Закону України «Про критичну інфраструктуру».

Таким чином, на підставі аналізу поняття «критична інфраструктура», підсумуємо: це складна система, яка охоплює стратегічно важливі об’єкти, системи, мережі, послуги, ресурси чи їх частини, для яких характерною загальною властивістю є значущість (соціальна, політична, економічна, екологічна) для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку – відповідно, порушення функціонування чи знищення яких може спричинити істотну шкоду державній безпеці, природному середовищу, національній економіці, завдати суттєвих збитків здоров’ю та благополуччю громадян (чи навіть призвести до втрати життя), суспільству в цілому, підприємствам, установам та системі управління державою.

Література

1. Франчук В.І., Пригунов П.Я., Мельник С.І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Вип. 3 (13). С. 142–148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf.
2. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. К. : НІСД. 2016. 176 с.
3. Кондратов С. Про деякі проблеми правового та організаційного забезпечення протидії тероризму на сучасному етапі. Державна політика протидії тероризму: пріоритети та шляхи реалізації : зб. матеріалів «круглого столу». Київ : НІСД, 2011. С. 18–22.

4. Поняття про критичну інфраструктуру. 2014. URL: http://mailswm.com/ponyattya-pro-kritichnuinfrastrukturu.
5. Теленик С. С. Критична інфраструктура як об’єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). URL: http://elar.naiau.kiev.ua/bitstream/123456789/6663/1/17.pdf.
6. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
7. Постанова Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» від 23 серпня 2016 року № 563. URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text
8. Постанова від 14.03.2018 № 309 «Про затвердження Кодексу системи передачі». URL: https://zakon.rada.gov.ua/laws/show/v0309874-18#Text.
9. Закон України від 16 листопада 2021 року № 1882-IX «Про критичну інфраструктуру». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
10. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту.
URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text.
11. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз.
URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html.
12. Уряднікова І.В., Заплатинський В.М. Наукові підходи до визначення терміну «критична інфраструктура». Вісті Донецького гірничого інституту. 2020. №2 (47), doi: URL: https://doi.org/10.31474/1999-981X-2020-2-184-193
https://jdmi.donntu.edu.ua/wp-content/uploads/2021/02/Uriadnikova-JDMI_2_2020.pdf.

Воропаєв Д. В.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Лучик В. Є.
професор кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, доктор економічних наук, професор,

РОЗРОБКА ТА ОЦІНКА ЕФЕКТИВНОСТІ АНТИВІРУСНИХ ПРОГРАМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

У сучасному світі, де смартфони стали невід'ємною частиною нашого повсякденного життя, питання кібербезпеки стає особливо важливим. Зростає кількість загроз від шкідливих програм, спрямованих на мобільні пристрої, що потребує постійного удосконалення та оцінки антивірусних розв'язків.

Дослідження спрямовані на вивчення та аналіз сучасних методів розробки антивірусного програмного забезпечення для смартфонів, а також на оцінку їх ефективності в умовах актуальних кіберзагроз. Дослідження фокусуються на розробці ефективних методик виявлення та боротьби з вірусами, які можуть погрожувати

доступності та конфіденційності інформації на мобільних пристроях. Антивірусні програми являються важливим засобом захисту від вірусів. При цьому використовуються такі методи, як:

- сигнатурний аналіз – це метод, який порівнює файли або код з базою даних відомих сигнатур шкідливих програм. Якщо файл або код містить сигнатуру шкідливої програми, антивірус її блокує;
- поведінковий аналіз – це метод, який аналізує поведінку програми для виявлення ознак шкідливої діяльності. Наприклад, антивірус може перевіряти, чи намагається програма отримати доступ до конфіденційних даних або чи намагається вона встановити інші програми без відома користувача;
- аналіз машинного навчання – це метод, який використовує алгоритми машинного навчання для виявлення шкідливих програм. Алгоритми машинного навчання навчаються на наборі даних, що містить зразки шкідливих і безпечних програм. Після навчання алгоритми можуть використовуватися для виявлення нових шкідливих програм, які не містяться в базі даних сигнатур.

Аналіз ресурсоємності та впливу на продуктивність, проведений в роботах [4], підкреслює важливість балансу між захистом від кіберзагроз та забезпеченням нешкідливої роботи мобільних пристроїв. Врахування цього балансу в розробці антивірусних програм стає ключовим фактором для задоволення потреб сучасних користувачів.

За роботами [5], оскільки кіберзагрози прогресують, результати аналізу також вказують на важливість урахування тенденцій розвитку рішень антивірусних програм. Оптимальна розробка та оцінка ефективності антивірусних програм для мобільних пристроїв ґрунтуються на поєднанні передових технологій, стратегічного планування та врахування актуальних тенденцій у сфері кібербезпеки. Такий комплексний підхід допомагає забезпечити ефективний захист від загроз та збереження надійності мобільних пристроїв у сучасному цифровому середовищі».

На основі комплексного аналізу сучасних досліджень, проведених у працях [1-5], визначено, що ключовим напрямком в контексті зростаючого обсягу кіберзагроз, є розробка та оцінка ефективності антивірусних програм для мобільних пристроїв. Дослідження вказують на необхідність постійного вдосконалення алгоритмів виявлення та боротьби з шкідливими програмами, зокрема застосування методів машинного навчання, щоб ефективно відповідати на різноманітні типи атак. Важливо враховувати аспекти впливу антивірусних програм на продуктивність, як підкреслено у [4], для забезпечення оптимального функціонування мобільних пристроїв.

Ефективність антивірусної програми оцінюється за такими критеріями, як точність, чутливість, специфічність та вплив на продуктивність. Інтеграція з іншими засобами безпеки дозволяє забезпечити більш повний захист мобільних пристроїв через, те що антивірусні програми все частіше інтегруються з іншими засобами безпеки, такими як брандмауери, фільтри веб-сайтів та менеджери паролів.

Висновки. Розробники антивірусних програм постійно працюють над удосконаленням своїх продуктів, щоб забезпечити максимальний захист користувачів. Вони роблять це, використовуючи передові технології, такі як машинне навчання, інтеграція з іншими засобами безпеки та розробка антивірусних рішень для спеціальних пристроїв. Це допомагає забезпечити безпечне використання мобільних пристроїв. Однак користувачі також можуть вжити заходів для захисту своїх пристроїв, таких як встановлення оновлень безпеки, використання надійних паролів і уникнення невідомих джерел.

Література

1. Г. Стейнер та І. Лю. (2019). «Аналіз сучасних методів виявлення та боротьби з шкідливими програмами на мобільних пристроях». Журнал Інформаційної Безпеки, 23(2), 45-60. URL: https://www.sciencedirect.com
2. К. Міллер та Р. Сміт. (2020). «Огляд розробки антивірусних алгоритмів для платформ Android та iOS». Міжнародна конференція з інформаційної безпеки, 112-125. . URL: http://www.icisc.org
3. Д. Чжао та Л. Ван. (2018). «Ефективність антивірусних заходів на основі машинного навчання для мобільних пристроїв». Журнал Кібербезпеки, 15(4), 321-335. . URL: https://ieeexplore.ieee.org/Xplore/home.jsp
4. М. Джонсон та К. Браун. (2021). «Вплив антивірусних програм на продуктивність мобільних пристроїв: аналіз ресурсоємності». Конференція з комп'ютерних технологій, 201-214. . URL: https://ieeexplore.ieee.org/Xplore/home.jsp
5. С. Лі та В. Кім. (2017). «Тенденції розвитку антивірусних рішень для мобільних пристроїв». Журнал Інформаційної Безпеки та Кібербезпеки, 10(3), 87-102. . URL: https://www.sciencedirect.com

Галайко Н. В.

викладач кафедри інформаційного та аналітичного забезпечення діяльності право–охоронних органів факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

ВПЛИВ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ НА ФОРМУВАННЯ ЦИФРОВОЇ ЕКОНОМІКИ

Останніми роками світ швидкоплинно змінюється. Певною мірою це відбувається завдяки розвитку інформаційного суспільства та сучасних інформаційних технологій, тобто завдяки такому явищу, як цифровізація.

Під цифровізацією слід розуміти складний і комплексний процес, який включає розвиток і впровадження наукомістких цифрових технологій у всіх сферах життя людини. Тобто саме цифровізація допомагає людству вступити у нову еру глобальних змін. Звичайно, світова економіка так само, як і всі інші сфери, піддається впливу цифровізації, що допомагає формувати багато якісних структурних змін. Цифровізація є умовою та одночасно передумовою для формування економіки нового технологічного укладу, що ґрунтується на виробництві та використанні знань, соціально-економічної та технологічної інтеграції економічного суб’єкта в єдиний інформаційний простір.

Розвиток цифрових технологій призвело до появи цифрової економіки. Цифрова економіка – це вся економічна діяльність, яка забезпечується використанням інформаційно-комунікаційних та інших цифрових технологій. Це не лише IT-розробки та наукові цифрові рішення, а й електронна комерція, онлайн-послуги та результати діяльності цифровізованих підприємств [1].

Цифровізацію економіки варто розглядати як інструмент, а не як самоціль. При системному державному підході цифрові технології будуть стимулювати розвиток відкритого інформаційного суспільства як одного з істотних факторів підвищення продуктивності, економічного зростання, створення робочих місць, а також покращення якості життя громадян України [2, с. 5].

За прогнозами, в найближче десятиліття близько 70% створеної вартості буде спиратися на цифрові продукти. Якщо в 2018 сума світового ВВП, яка припадала на цифровізовані підприємства, становила 13,5 трлн доларів США, то уже в 2023 році цей показник прогнозується на рівні 53,3 трлн доларів США (тобто майже вчетверо вище), що становитиме більше половини номінального світового ВВП [1].

Не слід забувати те, що важливу роль при цифровізації економіки відіграють інтернет-технології, які забезпечують комунікації між персоналом та машинами. Підприємства виробляють продукцію відповідно до вимог індивідуального замовника, оптимізуючи собівартість виробництва. Експерти виділяють чотири базових технології, в результаті впровадження яких очікуються революційні зміни (табл. 1).

Таблиця 1. Базові інтернет-технології революційних змін [3].

Технологія	**Зміст технології**
Інтернет речей (Internet of Things, IoT)	Інтернет використовується для обміну інформацією не тільки між людьми, але і між різними «речами», тобто машинами, пристроями, датчиками і т.д. Різновидом IoT є промисловий (індустріальний) інтернет речей (Industrial Internet of Things, IIoT). Саме він відкриває пряму дорогу до створення повністю автоматизованих виробництв.
Цифрові екосистеми.	Системи, що складаються з різних фізичних об'єктів, програмних систем і керуючих контролерів, що дозволяють уявити таке утворення як єдине ціле. Фізичні та обчислювальні ресурси в такий екосистемі тісно пов'язані, моніторинг і управління фізичними процесами здійснюється з використанням технологій IIoT.
Аналітика великих даних (Data Driven Decision) або просто Великі дані (Big data)	Величезні обсяги інформації, що накопичуються в результаті «оцифровування» фізичного світу, можуть бути ефективно оброблені тільки комп'ютерами, із застосуванням хмарних обчислень і технологій штучного інтелекту (Artificial Intelligence). В результаті людина, яка контролює той чи інший процес, ситуацію, обстановку має отримувати оброблені дані, максимально зручні для сприйняття, аналізу і ухвалення рішення.
Складні інформаційні системи (цифрові платформи)	цифрові платформи і системи для управління бізнес-процесами, для інтеграції інтернету речей в фізичні бізнес-процеси, для аналізу і прогнозування стану обладнання.

Процес цифровізації економічних відносин забезпечує динамічне зростання ефективності усіх бізнес-процесів, яких він стосується, а також матиме безпосередній вплив на трансформацію самої організаційної структури економічних відносин шляхом переорієнтації її на побудову принципово нової системи, котра характеризується як Індустрія 4.0 (провідний тренд «Четвертої промислової революції») [4]. Індустрія 4.0 – це цифрова трансформація виробничих процесів (цифровізація на підприємствах). Вперше про програму «Індустрія 4.0» мова зайшла у 2011 році на промисловій виставці в Ганновері, де уряд Німеччини поставив задачу розширити застосування інформаційних технологій у виробництві. При цьому необхідно зазначити, що Індустрія 4.0 орієнтується на широке застосування цифрових технологій та суттєве вдосконалення на їх основі традиційної системи виробничих відносин (рис. 1).

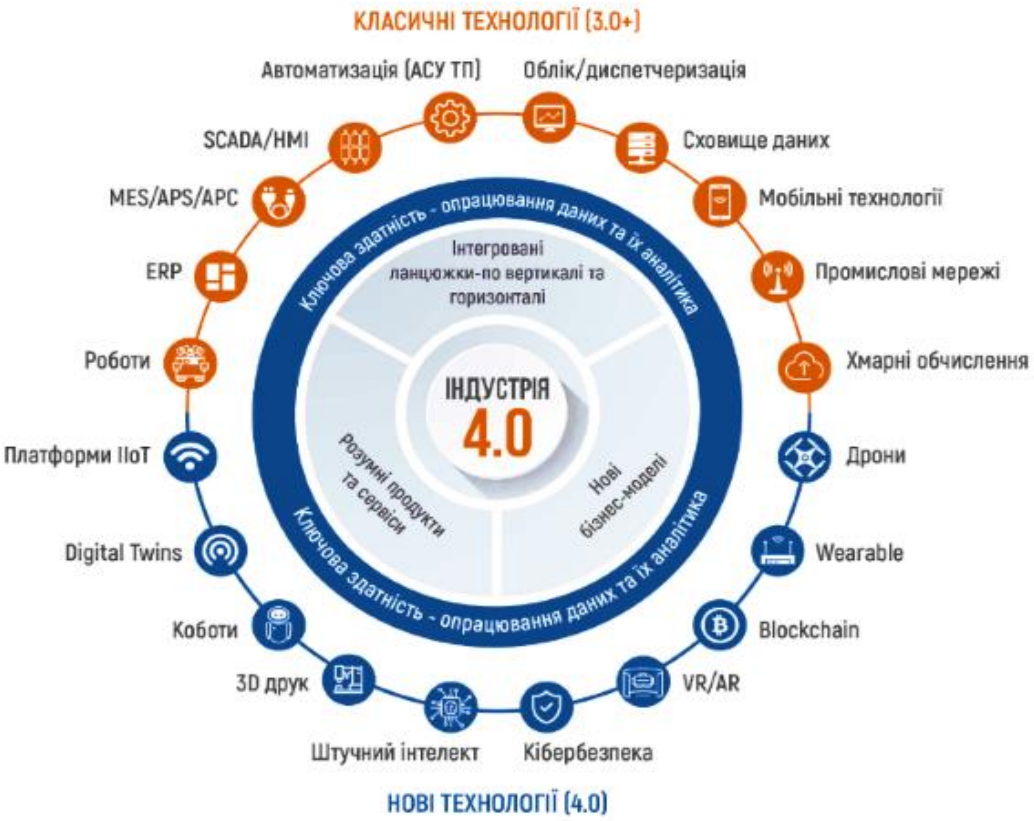

Рис 1. Індустрія 4.0 [5].

Інтегруючись у світовий економічний простір, цифровізація не оминула і економіку України. Звісно, що в існуючих реаліях бізнес на допомогу держави не може розраховувати. Проте щось у напрямку переходу до Індустрії 4.0 все ж робиться. Створено рух «Індустрія 4.0 в Україні», велику увагу цим питанням приділяє АППА (Асоціація підприємств промислової автоматизації України).

Підсумовуючи, можемо стверджувати, що стрімкий розвиток цифрових технологій не оминув економіку, що призвело до появи цифрової економіки. Цифрова трансформація – це не лише про технології, а й про стратегію бізнесу в напрямі становлення Індустрії 4.0, про цифрову освіту, науку та інновації, про цифрове підприємництво. Сектор цифрової економіки в Україні може забезпечити стабільність та зростання фінансових надходжень необхідних, зокрема, для післявоєнної відбудови. Цифрові рішення становлять не лише фінансовий, а й стратегічний інтерес, оскільки здатні посилювати ефективність тих галузей, в які вони інтегруються.

Література

1. Круп'яник Аліна. Цифрова економіка України: основні фактори розвитку. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku
2. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020). Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року.
URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

3. Industry 4.0. URL: https://www.it.ua/knowledge-base/technology-innovation/industry-4
4. Дзямулич Микола, Шматковська Тетяна. Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. Економічний форум. №2. 2022. С. 3-8.
5. Україна 2030е – країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html

Гамулець М. І.
аспірант кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ

РОЛЬ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ У ФОРМУВАННІ ІМІДЖУ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ

Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки передбачає запровадження благодійної діяльності у сферах де вплив держави не відповідає суспільним очікуванням [1]. В умовах європейської інтеграції благодійність починає грати дедалі помітнішу роль життя суспільства. Це пов'язано з тим, що складні процеси, які відбувалися у пострадянський період трансформації, послужили свого роду каталізатором для виникнення багатьох соціальних проблем.

Державні структури не змогли повністю усунути негативні наслідки соціально-економічних потрясінь та забезпечити громадянам гідний рівень життя. У зв'язку з цим зростає роль громадських організацій у соціальній діяльності, спрямованої на допомогу людям, які її потребують. Процеси, що відбуваються, вимагають філософського осмислення благодійності, пов'язаного з виявленням сутнісних засад даного соціального феномену. Дослідження динаміки та статики благодійної діяльності як необхідних факторів сталого розвитку суспільства стало актуальною проблемою соціальної філософії.

У сучасному соціумі поступово першому плані виходять інститути громадянського суспільства, з'являються нові суб'єкти благодійної діяльності, реалізують соціальні ініціативи різної спрямованості.

Сьогодні про творчі можливості таких ініціатив згадується на найвищому рівні. Імідж благодійної організації виступає важливим чинником зростання соціальної стабільності регіонів, від якого залежить приплив зовнішніх та внутрішніх інвестицій. Виконавчі органи місцевої влади наділені повноваженнями щодо формування іміджу благодійної організації.

Сюди входять завдання не лише щодо висвітлення діяльності органів виконавчої влади, преференцій для бізнесу, унікальних характеристик для туристів. Усі ці фактори є імідж-факторами. Міжрегіональна конкуренція спонукає до створення бренду благодійної організації. Для покращення якості життя населення необхідне залучення ресурсів у регіон, це можна зробити, грамотно продемонструвавши переваги благодійної організації.

Ключову функцію у формуванні іміджу благодійної організації несе інформаційна робота, формування новини та висвітлення ключових подій, спрямованих на соціально-економічний розвиток за рахунок діяльності благодійної організації.

Для виконання цих завдань в благодійні організації сформують служби зв'язків із громадськістю, які взаємодіють з органами державної влади. Ці служби забезпечують регулярне надання інформації про результати діяльності благодійних організацій,

плани та прийняті рішення, а також реалізовують виховно-інформаційну функцію, спрямовану на просвітництво громадськості у сфері соціальної відповідальності..

В Україні простежується позитивна тенденція з боку органів державної влади до використання інструментів комунікацій з благодійними організаціями та благодійних організацій громадськістю. Інформаційна робота стала у кілька разів оперативнішою. Причиною цього стало впровадження в систему формування соціальних мереж, а також адаптація матеріалів відповідно до формату соціальних мереж, який передбачає досить високу швидкість підготовки контенту. Тому в даний час інформаційна робота, спрямована в тому числі на формування іміджу, вимагає нового розуміння, нових підходів і заходів щодо вироблення інформаційної стратегії.

Робота у сфері інформаційної політики має важливу роль у процесі формування та закріплення іміджу благодійної організації, який необхідний у сучасних реаліях для залучення інвестицій. Така робота потребує серйозного аналізу, творчого підходу та систематичних дій. Вона складна тим, що, включаючи безліч факторів, вона не може здійснюватися без участі фахівців, експертів та узгодженості всіх ланок, задіяних у процесі такої роботи.

Інформування є невід'ємною ланкою у процесі формування іміджу благодійної організації, закріплення певної громадської думки про благодійну діяльність організації, шляхом створення та розповсюдження контенту.

На сьогоднішній день інформаційний простір не має меж, кількість каналів поширення контенту збільшується, охоплення зростає, конкуренція виробників контенту набирає обертів, зростає кількість фейків і наклеп.

На рівні законодавства виникла потреба регулювати цю сферу, за останні кілька років відбулися зміни у нормативно-правому полі, спрямовані на захист інтересів фізичних осіб, які беруть участь у процесах інформування населення. Щоб донести бажану думку необхідно грамотно та якісно наповнювати цей простір, уважно підбираючи інформаційні приводи, оперативно відпрацьовувати та, що дуже важливо, збирати та залучати свою цільову аудиторію.

Одним із важливих принципів інформаційної політики при впровадженні та популяризації сформованого на галузевому базисі іміджу благодійних організацій, бачимо орієнтацію на вихід інформації щодо благодійної діяльності у переважному позитивному контексті. Важливим і актуальним принципом під час виробництва безпосередньо контенту зокрема на державному рівні бачимо емоційну складову. Згадуючи визначення поняття імідж, повертаємося до дефініцій «образ», «сприйняття». Відношення благодійності є взаємодія соціальних партнерів, яке може протікати у формах, що допускають різну міру суб'єктності у свідомості та діяльності.

Щоб сформувати необхідний образ чи забарвлення сприйняття (позитивний), слід розбиратися в емоційних здібностях і потребах цільової аудиторії. Відповідно до цього розумінням створювати інформаційний продукт.

Література

1. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки: Указ Президента України від 27.09.2021 р. № 487/2021. URL. https://zakon.rada.gov.ua/laws/show/487/2021#Text

Гангола Н. Р.
здобувач вищої освіти факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ;
Магеровська Т. В.
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ РІЗНИХ КРАЇН

Термін «штучний інтелект» вперше було застосовано американським науковцем Дж. Маккарті у 1956 р. для позначення розумового процесу, що реалізовувався комп'ютерною системою на зразок мислення людини. Сьогодні дослідникам вдалося втілити ідею про штучний інтелект в життя.

Інженери та науковці створюють потужні нейрокомп'ютери та програмні нейро-пакети для розпізнавання образів, пошуку зображень, текстового пошуку, перекладу, прогнозування, виявлення шахрайства та вирішення інших завдань, які складно вирішити людині з причин колосального обсягу інформації, що підлягає аналізу.

Але слід зазначити, що нові технології вже досить давно використовуються не тільки на благо суспільства, а й у злочинних цілях. Злочини дедалі частіше відбуваються за допомогою технологій штучного інтелекту. В більшості випадків віртуальний простір практично виводить особистість правопорушника з процесу злочинних взаємодій, що, в свою чергу, породжує відчуття безкарності та підвищує частку нерозкритих злочинів.

Цілком логічною реакцією на перехід правопорушників у режим «онлайн» стало використання інтелектуального інструментарію правоохоронцями.

В рамках цього дослідження буде розглянуто напрямки застосування штучного інтелекту у діяльності правоохоронців різних країн: робота з візуальним контентом (сканування, розпізнавання, аналіз), прогнозування (висування версій) та запобігання правопорушенням.

Застосування нейромереж при розпізнаванні осіб. Технології нейромереж та штучного інтелекту (ШІ) для розпізнавання обличчя для ідентифікації осіб вже досить давно застосовується у правоохоронній діяльності.

Без застосування нейромереж робота з вхідним візуальним контентом є дуже трудомістким процесом. Крім того, обробка графічної інформації вручну неминуче призводить до помилок унаслідок природної втоми та інших психофізичних факторів. Машини, на відміну людей, не втомлюються і оцінюють зображення об'єктивно; вони здатні точніше відрізняти одну людину від іншої на основі аналізу індивідуальних рис обличчя.

Основні аспекти використання нейромереж і ШІ у поліції для розпізнавання обличчя включають:

- розшук злочинців;
- забезпечення громадської безпеки;
- пошук зниклих осіб;
- облік злочинів;
- автоматизована обробка великих обсягів даних.

Технології розпізнавання осіб застосовувалися і до появи нейронних мереж. Традиційні програмні алгоритми функціонували з урахуванням звірення осіб із набором

певних характеристик – розрізу очей, кольору й відстані між ними тощо. Нейтронні мережі ж здатні виробляти власні критерії розпізнавання осіб. Нейронні мережі розпізнають обличчя як на зображеннях анфас, так й зображеннях обличчя людини під різними кутами та на фрагментах зображень.

Крім аналізу осіб, нейронні мережі можуть працювати в областях ідентифікації зброї та інших об'єктів, виявляти аварії та злочини.

Сьогодні у науковій літературі та в реальній практиці все частіше висловлюється думка про можливість замінити людину на машину. Технології ШІ стрімко розвиваються, що ще більше актуалізує питання заміні таким аналізом криміналістичної портретної експертизи, виробленої людиною. Тим не менш у світовій практиці є безліч прикладів помилкового збігу порівнюваних осіб. Нейромережа, що обробляє зображення, може виявляти схожі особи і вводити в оману співробітників поліції. З цієї причини прийнято розмежовувати машинну оперативну ідентифікацію осіб та «повноцінну», яку виконує людина, що доповнюється додатковими методами (дактилоскопія, особиста бесіда тощо).

Тим не менш, не слід ігнорувати дві ключові переваги нейронних мереж: можливість високошвидкісної обробки зображень та здатність відновлювати зображення за фрагментами. Як відомо, найчастіше зображення, отримані з камер відеоспостереження, відрізняються низькою роздільною здатністю, зняті у складних для фіксації умовах (погане освітлення, опади, перешкоди). Більше того, штучний інтелект здатний аналізувати зображення обличь із частково зміненими елементами – у ситуаціях умисної зміни зовнішнього вигляду людини. У криміналістиці дуже часто виникають ситуації, коли необхідно досліджувати зображення осіб, зовнішність яких суттєво змінилася внаслідок травм, при хірургічному втручанні. Таке відновлення машина вміє робити досить якісно.

Як приклад можна навести використання штучного інтелекту в роботі поліції США при пошуку злочинців.

Так, за приблизними підрахунками, в США може бути від 25 до 340 активних маніяків, які вбивають не менше 150 осіб на рік. До того ж поліцейські часом не можуть належним чином класифікувати злочин, вважаючи жертву серійного вбивці нещасним випадком чи вбивством на побутовому ґрунті, тому статистика може бути ще кривавішою.

Штучний інтелект може допомогти правоохоронцям з пошуком злочинців, однак для цього машину потрібно навчити за матеріалами вже розкритих справ.

Томас Хенгроув створив алгоритм для «Проекту боротьби з вбивствами». На його думку, 5000 злочинців щороку уникають покарання. Тому алгоритм працює над створенням «карти нерозкритих вбивств», виявляючи райони, де найчастіше скоюються злочини, винуватців яких так і не вдалося упіймати.

Поліція Чикаго тестує комбінацію з найновіших технологій і підходів, щоб приборкати злочинність. Окремі райони контролює система, що працює на основі потокового відео, Big Date і машинного навчання. Вона передбачає злочини, допомагає поліції встановлювати особу порушників і може автоматично вислати опергрупу. Алгоритм Хенгроува сканує всі дані, які ФБР публікує за результатами розслідувань. Він виділяє випадки, в яких збігаються конкретні деталі, характерні для злочинів, ймовірно здійснених однією і тією ж людиною. Після чого наносить їх на карту. Статистика ведеться не лише у Чикаго, але і по всій країні. На сайті проекту можна переглянути статистику вбивств, здійснених в конкретних містах. Це допомагає слідчим швидко знаходити схожі за почерком злочини, що полегшує розшук серійних вбивць.

Генеральний директор компанії Clearview AI, яка займається розпізнаванням облич за допомогою штучного інтелекту, надавала свої послуги і американській поліції.

Правоохоронці використали її уже мільйон разів, просканувавши відповідну кількість облич, зазначив Хоан Тон-Тат. Йдеться, зокрема, про зображення з таких платформ, як Facebook. При цьому ці зображення були зібрані без дозволу користувачів соцмережі.

Поліції Нью-Йорка вдалося ідентифікувати і затримати торговця наркотиками завдяки моделі ШІ Rekor. Вона проаналізувала дані дорожніх камер і визнала його маршрут підозрілим. Чоловік на ім'я Девід Зайас був зупинений дорожньою поліцією в містечку Скарсдейл. Правоохоронці отримали дані від ШІ, що його маршрут збігався з тими, що зазвичай використовуються наркоторговцями. Обшукавши водія та його авто, копи виявили 34 тис. доларів готівкою, вогнепальну зброю та велику кількість кокаїну. Пізніше затриманий визнав себе винним у незаконному обігу наркотиків.

Поліцейські дрони можуть використовуватися для здійснення спостереження, збору інформації та, в деяких випадках, для здійснення заходів забезпечення безпеки. Це може включати розганяння натовпу, якщо він виявляє агресивну поведінку або становить загрозу громадській безпеці. Використання дронів може залежати від законів та регуляції у конкретній країні або регіоні.

Важливо, щоб в таких ситуаціях вживались заходи, спрямовані на мінімізацію ризиків для всіх сторін і забезпечення дотримання прав людини. Також важливо, щоб влада і поліція діяли відповідно до законів та з урахуванням принципів пропорційності та необхідності.

Так у 2015 році поліція Північної Дакоти запропонувала оснастити дрони сльозогінним газом. Правоохоронці пояснили свою ініціативу тим, що використання дронів зменшує потребу в наземному регулюванні агресивної поведінки натовпу і знижує ризик травмування поліцейських. Безлади простіше відстежувати і контролювати з повітря, до того ж дрони можуть звітувати про ситуацію в режимі реального часу.

У США використання дронів для потреб поліції регулюється на законодавчому рівні окремо у кожному штаті. Основними контраргументами противників є дорожнеча (окрім закупівлі самого апарату, потрібно буде провести курс навчання особового складу з його управління), а також можливість втручання в приватне життя. Але майже в усіх штатах дозволено використовувати дрони під час пошуку зниклих дітей або літніх людей. Для цього, окрім ордера, правоохоронцям необхідно отримати дозвіл від Федерального управління авіації.

У Франції вертоліт Aero Surveillance 150 оснащений денною й нічною камерами, двома сховищами на дев’ять гранат із сльозогінним димом або газом.

Інший китайський гвинтокрил компанії Hubei Handan Mechatronics Ltd презентували на виставці Asia Pacific China Police в 2014 році. Він оснащений не лише сльозогінним газом, але й гранатометом.

Індійська поліція використовує безпілотники, які можуть скидати перцевий порошок на мітингувальників у разі потреби, а також оснащені системою Cyclone для контролю за натовпом.

У Великобританії дронів активно використовують під час завдань Міністерства оборони, а поліція нещодавно почала використовувати їх в аеропортах. Британці схвалюють використання безпілотників для контролю безпеки, і це дозволяє уряду розширювати подібні програми.

У Індонезії в 2015 році в рамках експерименту адміністрація міста Джакарта вирішила застосувати дрони для спостереження за порядком під час свята Ураза-байрам. У місцях масового скупчення людей цей метод виявився ефективним і безпечним, тому тепер дрони використовуються для контролю ситуації в густонаселених районах столиці Індонезії, а також для моніторингу автомобільних доріг.

Правоохоронні органи Китаю використовують як невеликі апарати з відеокамерами, так і шестигвинтовий Tong Fei II, що може переносити будь-яке устаткування, наприклад, декілька бомб або сльозогінний газ.

У Пекіні дорожній патруль протестував першого робота, який стежить за порушеннями водіїв на дорогах. Це маленька поліцейська машина, що їздить зі швидкістю 5 км/год. Випробування пройшли на автостраді до аеропорту Шоуду. Завдання робота-копа – їздити розділовою смугою і робити фото або відео порушень. Також робот відправляє водіям повідомлення про погану погоду, ремонти шляхопроводів або ДТП. При виникненні аварії робот швидко приїжджає на місце, знімає всі необхідні матеріали і відправляє їх у поліцію.

Згідно із статистикою, в країні одна з найбільших систем відеоспостереження в світі, в китайських містах встановлено 170 млн. камер відеоспостереження, кожна з яких підключена до єдиної системи розпізнавання обличь.

Роботизований поліцейський з'явився на залізничному вокзалі Чженчжоу в провінції Хенань. Окрім контролю, він може спілкуватися з пасажирами. Схожі роботи-копи з'явилися в місті ще раніше, в жовтні 2017 року біля Будинку народних зібрань, де проходив XIX з'їзд Комуністичної партії Китаю. Там вони функціонували понад півроку.

На залізничному вокзалі Чженчжоу також працюють патрульні поліцейські, які використовують смарт-окуляри. Ґаджет має функцію розпізнавання облич і допомагає офіцерам впіймати злочинців. Розумні окуляри – це розробка пекінської компанії LIvision Technology. Девайс підключається до невеликого пристрою по дротяному зв'язку. Після сканування обличчя перехожого комп'ютер підключається до єдиної бази даних і за допомогою системи розпізнавання облич починає пошук збігів. Усе це дозволяє виявити злочинця набагато швидше, ніж це зробили б камери.

У 2022 році керівна рада Сан-Франциско проголосувала за те, щоби дозволити міській поліції використовувати роботів, які можуть вбивати. Відтепер поліція може використовувати роботів, оснащених вибухівкою, в екстремальних обставинах. Міська поліція Сан-Франциско повідомила BBC, що наразі не працює з роботами, оснащеними смертоносною силою. Проте вони сказали, що в майбутньому можуть бути сценарії, за яких вогонь на ураження може бути застосований роботом. Представник поліції сказав, що «роботи потенційно можуть бути оснащені вибуховими зарядами, щоб пробивати укріплені споруди, в яких перебувають агресивні, озброєні або небезпечні особи». Вони також сказали, що роботів можна використовувати для «знешкодження чи дезорієнтації жорстоких, озброєних або небезпечних підозрюваних, які загрожують життю людей».

Проте роботів-кілерів вже використовують в інших частинах Сполучених Штатів. У 2016 році поліція в Далласі, штат Техас, застосувала робота, озброєного вибухівкою С-4, щоб знешкодити снайпера, який убив двох офіцерів і поранив ще кількох.

Нейросеть як інструмент прогнозування та попередження злочинності. Як показує світовий досвід, нейромережа може бути застосована з метою ранжування та ідентифікації осіб, найбільш ймовірних як виконавців або жертв насильства. У США, наприклад, нейромережі обчислюють ймовірність скоєння злочинів із застосуванням вогнепальної зброї, керуючись такими критеріями, як попередні арешти, належність до злочинного угруповання та вік на момент останнього арешту. Це дозволяє запобігати злочинам та ідентифікувати осіб, які мають потрапити у фокус уваги профілактичних соціальних служб.

У системі кримінального судочинства США також використовується алгоритм COMPAS компанії Northpointe, який визначає можливість скоєння ще одного злочину правопорушником. Ці та інші прогностичні нейронні мережі працюють на базисі аналогічних алгоритмів: нейромережа акумулює максимальну кількість даних про

особу, що цікавить поліцію (локація, часто відвідувані місця, активність в Мережі, поведінкові патерни та ін.), на основі чого робиться припущення про рецидив.

Здібності до прогнозування нейронних мереж можуть бути використані у визначенні приналежності особи до організованого злочинного угруповання або для пошуку співучасників злочину. Програмний продукт Palantir, наприклад, працює з великою базою даних, що включає архівні документи та судові записи, посвідчення водія, адреси, телефонні номери та відомості з соцмереж. На основі цієї інформації нейронна мережа визначає систему зв'язків між людьми, що, своєю чергою, допомагає поліції ідентифікувати злочинні спільноти.

У росії протидії злочинній діяльності застосовуються, наприклад, такі автоматизовані інтелектуальні інструменти, як система «Блок», що забезпечує інформаційний криміналістичний супровід розслідування злочинів у економічній сфері; «Маньяк», що застосовується при розслідуванні серійних вбивств; «Спрут», що допомагає встановити контактні зв'язки між злочинцями; «Сейф», що систематизує дані про розкрадання коштів зі сховищ; «Дзеркало», що оперує географічними просторовими даними.

Ці можливості використовуються і в Україні.

Розпізнавання обличчя. Так, Київською міською радою на території столиці встановлено вже більше 6200 камер відеоспостереження із системою розпізнавання обличчя. Доступ до користування цією системою має і поліція, що часто відіграє ключову роль у виявленні, відверненні та розслідувані злочинів, встановленні місцезнаходження осіб, оголошених у розшук. Аналогічна система працює і у місті Житомирі, де вона одержала назву «Прозоре місто»

В Департаменті патрульної поліції створено підрозділ аеророзвідки, оснащений останніми зразками дронів. Роботи допомагають не тільки виявляти факти злочинів, наприклад, місця незаконного видобутку бурштину та вугілля, але й затримувати зловмисників. Поліцейські з підрозділу з боротьби з наркозлочинністю за допомогою безпілотників знайшли у 2020 році в Дніпропетровській області 36 ділянок, засіяних коноплями. Також роботи зможуть виявляти браконьєрів, незаконний видобуток корисних копалин, незаконні рубки лісу, осередки лісових пожеж, допоможуть шукати заблукалих в лісі чи горах. Дрони також моніторять дорожню ситуацію на трасах Дніпропетровської та Київської областей і шукають викрадений транспорт. Нацполіція планує створити спецгруп аеророзвідки в кожному регіоні України.

Позитивний досвід використання безпілотників має Держприкордонслужба України. За допомогою дронів прикордонники відслідковують ситуацію в важко-доступних місцях, зокрема для виявлення контрабандистів і нелегальних мігрантів.

Забезпечення безпеки на дорогах. Фіксація даних щодо правопорушень на дорогах реалізується за допомогою комплексів автоматичної фіксації, а саме спеціальних технічних засобів, укомплектованих функціями фото- і відеозапису, що надає можливість в автоматичному режимі здійснювати виявлення та документування в базах даних фактичних подій, які містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху. Установлення стаціонарних технічних засобів здійснюється на аварійно-небезпечних місцях та місцях концентрації дорожньо-транспортних пригод, автомобільних доріг загального користування, державного та місцевого значення, вулиць і доріг у містах та інших населених пунктах за погодженням із відповідним уповноваженим підрозділом Національної поліції.

Отже, технічні досягнення, зокрема штучний інтелект, роботи та дрони, вже тепер допомагають правоохоронцям в усьому світі. Окрім того, що вони спрощують роботу поліцейських, вони також захищають правоохоронців від нещасних випадків чи

надмірної агресії. До того ж штучний інтелект працює над алгоритмами пошуку серійних убивць та кривдників, щоб зробити людське життя безпечнішим.

Гілета І. В.
доцент кафедри САП Національного університету «Львівська політехніка» кандидат технічних наук, доцент

ОСОБЛИВОСТІ ОЦІНКИ ЯКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Інформація та інформаційні технології розглядаються як один із стратегічних ресурсів підприємства. Це характеризує підходи до проектування, експлуатації та модернізації інформаційних систем (ІС) з погляду реалізації інтересів замовників. Процеси розробки та впровадження ІС перебувають під жорстким управлінським контролем.

Наскільки добре ІС відповідає вимогам бізнесу, характеризується споживчою якістю системи. Згідно з міжнародним стандартом ISO 9000:2005 поняття якості продукції визначається як сукупність характеристик об'єкту (діяльності або процесу, продукції, послуги та ін.), що відносяться до його здатності задовольняти встановлені або передбачувані потреби. Це визначення може бути застосовано до ІС. Водночас, слід зазначити, що ІС відносяться до класу складних систем і при формуванні методологічних підходів до оцінки якості ІС необхідно враховувати різні аспекти: якість інфраструктури системи, програмного та апаратного забезпечення, якість даних та інформації, якість адміністративного управління та сервісу. Крім того, сприйняття та інтерпретація поняття якості залежить від точки зору, з якої воно розглядається. Для кінцевого користувача, замовника, менеджера та розробника зміст поняття «якість ІС» має різний зміст.

Оцінка споживчої якості ІС та її програмного забезпечення базується на певній моделі якості. Однією з перших була запропонована модель якості МакКола, визначається трьома групами характеристик: фактори, які формує кінцевий користувач ІС; критерії, що визначаються розробником програмного забезпечення (ПЗ); метрики, які використовуються для кількісного опису та вимірювання якості. Фактори якості згруповані в три групи: функціонування; використання; ревізії. Критерії якості в моделі МакКола є кількісними рівнями факторів, які використовуються як цілі при розробці ІС. Метриками якості в моделі визначено показники: зручність перевірки на відповідність стандартам; точність управління та обчислень; ступінь стандартності інтерфейсів; функціональна повнота; однорідність використовуваних правил проектування та документації; ступінь стандартності форматів даних; стійкість до помилок; ефективність роботи; розширюваність; ширина області потенційного використання; незалежність від апаратної платформи; повнота протоколювання помилок та подій; модульність; зручність роботи; захищеність; само документованість; простота роботи; незалежність від програмної платформи; можливість співвіднесення проекту до вимог; зручність навчання.

Метрики МакКола пропонує оцінювати за 10-ти бальною шкалою. Введені метрики можуть впливати на кілька факторів якості, а фактори оцінюються на основі згортки деяких метрик. У цьому коефіцієнти входження метрик у згортки багато в чому є евристичними і мають конкретизуватися для конкретної організації, видів програмного забезпечення, команд розробки тощо.

Для моделі МакКола одним із суттєвих недоліків є труднощі при оцінюванні метрик за 10-ти бальною шкалою. Для експерта може викликати складність застосування

подібної шкали оцінювання до таких характеристик, як розширюваність, самодокументованість і простота роботи. Крім того, процедури згортки метрик обмежують їхнє застосування для різних об'єктів.

Міжнародною організацією зі стандартизації (International Organization for Standardization, ISO) прийнятий стандарт для моделі якості програмного забезпечення ISO/IEC 25010:2011. У цьому стандарті вводяться поняття внутрішньої та зовнішньої якості, а також якості програмного забезпечення під час використання у різних контекстах. Внутрішня якість визначається характеристиками програмного забезпечення без урахування його поведінки. Зовнішня якість, характеризує ПЗ зі сторони його поведінки. Якість ПЗ при використанні в різних контекстах – це споживча якість. Слід зазначити, що в створенні якісного ПЗ істотна якість технологічних процесів його розробки.

У стандарті для оцінки якості програмного забезпечення інформаційних систем визначають цілі, атрибути та метрики. Як цілі досягнення заданої якості інформаційної системи розглядаються функціональність, надійність, практичність або зручність використання, ефективність, підтримка, переносимість або мобільність. Цілі визначаються атрибутами якості.

Відповідно до стандарту ISO/IEC 25010:2011 у моделі якості програмного забезпечення використовуються такі цілі та атрибути:

- функціональність: придатність до певної роботи, точність, правильність, здатність до взаємодії; відповідність стандартам та правилам, захищеність;
- надійність: зрілість, завершеність (зворотна до частоти відмов), стійкість до відмов; здатність до відновлення працездатності при відмові, відповідність стандартам надійності;
- практичність, зручність використання: зрозумілість, зручність навчання, працездатність, привабливість, відповідність стандартам практичності;
- ефективність: часові характеристики, використання ресурсів, відповідність стандартам ефективності;
- підтримка: аналізованість, змінність, зручність для внесення змін, ризик виникнення несподіваних ефектів при внесенні змін, контрольованість, зручність перевірки, відповідність стандартам підтримки;
- перенесення, мобільність: адаптованість; зручність установки; здатність до співіснування з іншим ПЗ; зручність заміни іншого ПЗ даних; відповідність стандартам переносимості.

Функціональні вимоги формулюються у вигляді тверджень, що описують поведінку системи, які можуть бути формально перевірені. Надійність характеризують поведінку системи при виході межі допустимих значень параметрів функціонування через збій у системі. Оцінюючи атрибутів надійності застосовуються методи теорії ймовірностей і математичної статистики. Зручність використання досить важко оцінюється і, в основному, використовуються експертні методи. Ефективність належать до найважливіших кількісних показників якості програмних систем. Наявні програмно-апаратні засоби та методики дозволяють прогнозувати інтегральні значення показників ефективності системи. Супроводжуваність характеризує необхідні ресурси на супровід та модернізацію системи, що витрачаються експлуатаційним персоналом. У цьому використовуються методики прогнозування витрат за виконання типових процедур супроводу. Перенесення системи характеризує можливість вибору компонентів системного оточення. Оцінка переносимості може залежати від погляду зацікавлених осіб: переносимість різні апаратні платформи, переносимість різні програмні платформи, переносимість різні апаратні і програмні платформи.

Модель якості, яка створюється в рамках стандарту ISO/IEC 25010:2011, визначається загальними характеристиками програмного продукту. Характеристики ставляться у залежність від субхарактеристик якості та атрибутів ПЗ, які повинні піддаватися точному опису та виміру. Вимоги якості видаються як обмеження на модель якості. При оцінці якості продукту спочатку оцінюються атрибути ПЗ за допомогою метрик і формується шкала оцінки в залежності від можливих ступенів відповідності атрибуту обмеженням, що накладаються. Для кожної окремої оцінки атрибута градація зазвичай вибирається заново і залежить від вимог якості, що накладаються на нього. Набір отриманих атрибутів є критерієм для оцінки субхарактеристик і характеристик, і як результат якості продукту в цілому.

Коментуючи стандарт можна наголосити, що характеристики, субхарактеристики та атрибути якості програмних систем можна розділити на три групи: категорійні, кількісні та якісні.

Категорійні показники якості програмного забезпечення інформаційних систем характеризують широкий спектр класів, призначень та функцій інформаційних систем. До цієї групи відносять характеристики, що визначають функціональність, захищеність та важливість.

Кількісні показники якості програмного забезпечення, такі як надійність та ефективність, можуть бути виміряні та представлені чисельними характеристиками.

Якісні характеристики програмного забезпечення мають описовий, якісний вигляд. Такі характеристики оцінюються експертними способами, при цьому застосовують бальну оцінку або використовуються лінгвістичні оцінки рівня якості: відмінний, хороший, задовільний чи незадовільний.

Водночас, концепція планування та управління процесами аналізу якості програмного забезпечення, що розглядається, не вирішує питання спільного використання категоріальних, кількісних і якісних показників і, крім того, проблеми агрегації характеристик якості ПЗ на основі схеми взаємозв'язку залишаються відкритими. Це зумовлює необхідність розвитку методології інтегральної оцінки якості програмного забезпечення інформаційних систем.

Література

1. ISO 9000:2005 Quality management systems – Fundamentals and vocabulary.
2. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models

Глушко П. Л.

курсант факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

Поляк С. П.

викладач кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, доктор філософії

ОКРЕМІ АСПЕКТИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ НА ДЕОКУПОВАНИХ ТЕРИТОРІЯХ

«Будь яка» війна як крайній та найдеструктивніший інструмент вирішення конфліктів призводить до зміни суспільно-ментальної, матеріальної (об’єктової), морально-психологічної та правової обстановки воюючої країни. Якщо розглядати

правоохоронну діяльність в умовах війни, то для неї виникає несприятлива обстановка оперативного, тактичного та процесуального характеру як більш конкретніші види, однак такі, що випливають із перерахованих.

Оперативно-розшукова діяльність покликана виявити ознаки замаскованого кримінального правопорушення, яке готується чи вчиняється в умовах неочевидності та чіткого супротиву правоохоронній системі, використовуючи при цьому напрацьовані десятиліттями методики й тактики такої роботи. Однак, щоденні систематичні акти злочинної поведінки окупаційних військ на території України породжують воєнну ситуативність вчинення таких злочинів. Ці діяння важко передбачати, а тим більше планомірно та системно застосувувати оперативно-розшукові можливості їх документування. Це однозначно створює несприятливу оперативну обстановку зумовлену браком оперативної інформації, недостатністю та непристосованістю інструментів документування, відсутністю кваліфікації оперативних працівників та постійними обстрілами деокупованих територій, що прямо впливають на безпеку учасників документування.

Це спонукає вдосконалювати не тільки оборонний і військовий сектор, а й правоохоронний сектор, який є однією з основних складових національної безпеки України. Перед правоохоронцями постали нові потреби, виклики та нові ризики. Під час військових дій окупантами та колаборціоністами вчиняються низка воєнних злочинів, в тому числі відносно цивільного населення, відповідно крім цих діянь поблизу лінії розмежування і на деокупованих територіях вчиняються багато інших супутніх злочинів.

Залишається відкритим і питання щодо завдань та функціоналу, які повинен виконувати працівник поліції на деокупованих територіях, зокрема оперативний співробітник. Виходячи з актуально визначених завдань, оперативні підрозділи поліції забезпечують пошук та розшук осіб, які безвісті зникли та інших законодавчо визначених категорій осіб, що є надзвичайно актуальним в умовах війни.

Ще одним важливим напрямом діяльності оперативних підрозділів в умовах збройної агресії можна визначити оперативно-розшукову діагностику, ідентифікацію та оперативний пошук. Тому погоджуємося із твердженнями Є. Полякова про те, що надзвичайно актуальною є проблема розпізнання загроз диверсій, саботажу, терористичних загроз в умовах воєнного стану. З огляду на те, що аеропорти, вокзали, станції метрополітену є місцем масового перебування людей, проблеми своєчасної ідентифікації диверсантів, терористів і вибухових пристроїв є дуже важливими в сучасних умовах. На думку науковця, одним з напрямів підвищення безпеки пасажирів є застосування сучасних біометричних систем. Біометрична інформаційно-пошукова система відеоспостереження дозволяє в автоматичному режимі проводити ідентифікацію в потоці людей, здійснюючи перевірку отриманих зображень за базами даних осіб, які перебувають у розшуку. Виділені зображення осіб передаються на сервери розпізнавання (які можуть бути як локальними, так і віддаленими), в яких здійснюється миттєва, за частки секунди, перевірка зображень осіб з фотографіями розшукуваних терористів, злочинців, правопорушників [1, с. 204-205].

Враховуючи наведене, відповідно до ст. 23 Закону України «Про Національну поліцію», правоохоронців наділили зокрема такими повноваженнями як здійснювати збирання біометричних даних осіб [2].

Поряд із тим, слід зауважити, що після відкритої експансії та військового вторгнення на територію України російською федерацією, з метою документування масових фактів воєнних злочинів рашистами на території нашої держави спільно з міжнародними правоохоронними та правозахисними інституціями застосовується спосіб фіксації відкритих цифрових даних відповідно до Протоколу Берклі.

Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних описує професійні стандарти, які слід застосовувати при виявленні, зборі,

збереженні, аналізі та представленні цифрової інформації у відкритому доступі та при використанні у міжнародних кримінальних розслідуваннях та розслідуваннях у сфері прав людини. Крім того, Протокол наголошує на стандартах розслідування порушень міжнародного права, включаючи порушення прав людини та порушення міжнародного кримінального права, включаючи військові злочини, злочини проти людяності та геноцид. Вказівки, передбачені Протоколом, можуть бути застосовані до інших видів розслідувань, у тому числі для національних чи муніципальних судів [3].

Виходячи з наведеного, імпонує й сучасна думка українських науковців, що «електронні докази – це докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки» [4, с. 5].

Як підсумок, всі наведені теоретичні положення та думки наукових шкіл логічно було б висвітлити в національному законодавстві, що стосується виявлення та процесуального закріплення доказової інформації. Це дасть змогу забезпечити невідворотне покарання представників «народу-варварів» з геноциїдальними настроями співіснування на нашій планеті. Цифровий світ та інтелектуальні нейромережі зокрема – це інструмент, який взмозі у недалекому майбутньому відтворити реальну картину окремих подій, виходячи з конкретних даних та інформації, яка буде зібрана про них як вихідні показники відтворення минулої реальності.

Література

1. Поляков Є. Оперативно-розшукова діагностика як засіб протидії кримінальним правопорушенням в умовах воєнного стану. Протидія кримінальним правопорушенням в умовах воєнного стану : збірник матеріалів Всеукраїнської науково-практичної конференції в авторській редакції, (м. Кропивницький, 27 жовтня 2022 року). Кропивницький, 2022. 367 с.
2. Про національну поліцію Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII із змінами і доп. // Відомості Верховної Ради. 2015. № 40-41. – Ст. 379. – Режим доступу: http://zakon.rada.gov.ua/laws/show/580-19.
3. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних: практичний посібник. Режим доступу: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol- Ukrainian.pdf
4. Використання електронних (цифрових) доказів у кримінальному провадженнях : метод. реком. / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

Глущенко І. О.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Світличний В. А.

доцент кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ІНТЕРНЕТ-СВОБОДА ТА ЗАХИСТ ІНФОРМАЦІЇ

Вступ. Інтернет-свобода та право на інформацію є невід'ємною частиною сучасного суспільства, оскільки вони сприяють розширенню прав людини та прозорості

уряду. У сучасному світі, де інформація є ключовим ресурсом, інтернет-свобода та право на інформацію відіграють важливу роль у забезпеченні індивідуальних прав та свобод. Інтернет забезпечує доступ до безлічі джерел інформації, що дозволяє людям бути критичними мислителями та активними учасниками громадського життя [1].

Виклад основного матеріалу. Забезпечення інтернет-свободи має велике значення для розвитку демократії та громадянського суспільства. Це дає людям можливість висловлювати свої думки, обмінюватися ідеями та відстоювати свої права [2]. Наприклад, інтернет-активісти та блогери використовують інтернет для розголошення фактів про порушення прав людини, корупцію та недостатню прозорість урядових структур.

Право на інформацію є необхідною складовою демократичного суспільства. Важливо, щоб громадяни мали доступ до різноманітної та незалежної інформації, яка дозволяє їм приймати обґрунтовані рішення та контролювати дії уряду [3]. Право на інформацію також сприяє боротьбі з корупцією та забезпеченню відповідальності владних структур.

Однак, існує загроза інтернет-свободи та праву на інформацію через практики цензури і контролю соціальних медіа та інших онлайн-платформ. Уряди та недемократичні режими активно блокують доступ до інформації та обмежують свободу висловлювання. Такі дії позбавляють людей можливості отримувати незалежну інформацію та висловлювати свої думки [1].

Для забезпечення інтернет-свободи та права на інформацію необхідно прийняти кроки на рівні національних та міжнародних організацій. Уряди мають розробити та здійснювати законодавчі заходи, які гарантуватимуть свободу доступу до інформації та захищатимуть права користувачів Інтернету. Крім того, потрібно сприяти розвитку технологій, що дозволяють обходити блокування Інтернету та цензуру [2].

Усім зацікавленим сторонам, включаючи уряди, технологічні компанії та громадські організації, слід співпрацювати для забезпечення інтернет-свободи та права на інформацію. Це може включати розробку та впровадження технологій, які будуть захищати приватність користувачів та запобігатимуть цензурі [3].

Висновки: Усім нам, як активним користувачам Інтернету, важливо пам'ятати про значення інтернет-свободи та права на інформацію. Ми повинні бути відповідальними користувачами, пропагувати ці цінності та вимагати їх забезпечення від наших урядів та організацій [1-3]. Тільки тоді ми зможемо сприяти розвитку демократії, захищати права людини та забезпечувати прозорість уряду.

Література

1. Global Internet Freedom: Can Censorship and Freedom Coexist?. Digital Commons@DePaul. URL: https://via.library.depaul.edu/jatip/vol13/iss1/9/
2. The case for unfettered internet freedom. The Daily Star. URL: https://www.thedailystar.net/views/opinion/news/the-case-unfettered-internet-freedom-2137706
3. Policy Recommendations: Internet Freedom. Freedom House. URL: https://freedomhouse.org/policy-recommendations/internet-freedom

Говор Д. С.
курсант Харківського національного університету внутрішніх справ

ПРОБЛЕМАТИКА ОНОВЛЕННЯ ТЕХНІКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Проблема використання застарілої техніки та програмного забезпечення в роботі Національної поліції України може стати перепоною для ефективності та безпеки її роботи.

Застаріла техніка має суттєво обмежені можливості порівняно з більш сучасними зразками. Наприклад, застарілі засоби радіозв'язку можуть мати обмежений радіус дії, що ускладнює комунікацію між поліцейськими одиницями.

Застаріла техніка менш продуктивна та швидкодійна, що ускладнює оперативну реакцію на події та виконання завдань. Наприклад, застарілі автомобілі можуть мати обмежену швидкість та низьку маневреність. Також вона вимагає значних витрат на обслуговування та ремонт. Старі запчастини можуть бути складними для знаходження, а також можуть вимагати спеціалізованого обладнання та кваліфікованого персоналу для ремонту [1].

Застаріла техніка є менш надійною та вразливою до витоків інформації або несправностей. Наприклад, застарілі системи безпеки можуть легше піддатися хакерським атакам або вийти з ладу через несправність, що може загрожувати безпеці та конфіденційності даних. Застаріла техніка може не відповідати сучасним стандартам та вимогам. Наприклад, застарілі камери спостереження можуть мати низьку якість зображення або не мати можливості записувати відео високої роздільної здатності, що ускладнює розслідування злочинів [1].

Відсутність інтеграції є також важливим аспектом оскільки застрілі техніка та технології можуть бути не сумісними з сучасними системами та програмним забезпеченням, що ускладнює їх інтеграцію та обмін даними. Наприклад, застарілі комп'ютери можуть не мати достатньої потужності, що спричине низьку ефективність діяльності підрозділів.

Україна, як й інші країни світу, впроваджує сучасні технології в роботу правоохоронних органів для поліпшення ефективності та результативності їх діяльності. Нижче наведені приклади успішного впровадження сучасних технологій в роботу правоохоронних органів що підвищело загальну ефективність виконання завдань національної полції України.

Електронна система документообігу та електронний архів. Україна впровадила електронну систему документообігу та електронний архів у роботу правоохоронних органів. Це дозволяє зберігати та обробляти документи ефективніше, зменшує ризик втрати або пошкодження документів, а також спрощує доступ до них. Використання відеоспостереження. Багато країн, включаючи Україну, використовують відеоспостереження для забезпечення безпеки та виявлення злочинів. Відеокамери встановлюються на вулицях, в громадських місцях та на об'єктах важливої інфраструктури. Це допомагає правоохоронним органам виявляти та розслідувати злочини, а також забезпечує візуальну документацію подій.

Використання аналітики даних. Сучасні технології аналізу даних дозволяють правоохоронним органам ефективно виявляти та аналізувати злочини. Застосування алгоритмів машинного навчання та штучного інтелекту допомагає виявляти закономірності та залежності у злочинності, що дозволяє забезпечити більш ефективне розслідування та запобігання злочинам. Використання мобільних додатків. Деякі

правоохоронні органи впроваджують мобільні додатки для спрощення комунікації з громадянами та надання публічних послуг. Ці додатки дозволяють громадянам повідомляти про злочини (Чат-бот «Стоп наркотик» допоміг заблокувати понад 300 наркокрамниць), надавати свідчення, отримувати інформацію про розшукові оголошення та інші корисні сервіси [2]. Використання системи розпізнавання обличчя. Деякі країни використовують системи розпізнавання обличчя для ідентифікації підозрюваних та контролю доступу до об'єктів.

У світі існує кілька прикладів країн, де вдалося успішно оновити техніку поліції:

5. Сінгапур: Сінгапур відомий своєю високою якістю поліцейської роботи та сучасними технологіями, що використовуються поліцією. Вони впровадили систему відеоспостереження, яка охоплює майже всю країну, а також використовують безпілотні літальні апарати для патрулювання та нагляду [3].
6. Німеччина: Німеччина також відома своїми сучасними технологіями поліції. Вони використовують високоякісну комунікаційну технологію, яка дозволяє поліцейським швидко обмінюватися інформацією та координувати свої дії. Крім того, вони використовують сучасні автомобілі та спеціальне обладнання для ефективного виконання своїх обов'язків [3].
7. Японія: Японія також відома своїми передовими технологіями поліції. Вони використовують розумні камери відеоспостереження, які можуть розпізнавати обличчя та автоматично виявляти підозрілу діяльність. Крім того, вони використовують роботів-поліцейських для патрулювання та нагляду на громадських місцях [3].
8. США: В США також проводяться оновлення поліцейської техніки. Багато муніципалітетів використовують сучасні системи відеоспостереження, технології розпізнавання номерних знаків та системи передачі даних для поліцейських автомобілів. Крім того, в деяких містах впроваджуються технології штучного інтелекту для аналізу даних та прогнозування злочинності [3].

З метою вирішення задач, які стоять перед Національною поліцією України, необхідно приділити особливу увагу оновленню технічної бази та програмного забезпечення. Це включає заміну застарілої техніки на сучасну, розробку та впровадження нових програмних продуктів, забезпечення належної кібербезпеки та захисту даних, а також підвищення інтеграції та обміну даними між різними системами.

Важливо усвідомити, що оновлення застарілої техніки та програмного забезпечення в Національній поліції України є викликом, успішне подолання якого суттєво підвищить ефективність та результативність поліцейської діяльності.

Література

1. Top 6 Risks of Using Outdated Technology – PAG. PAG. URL: https://profitadvisorygroup.com/blog/top-6-risks-of-using-outdated-technology/
2. Чат-бот «Стоп наркотик» допоміг заблокувати понад 300 наркокрамниць, боротьба з наркочумою триває, – Олександр Гогілашвілі. URL: https://mvs.gov.ua/uk/activity/protidiya-narkozlocinnosti/novini-protidiyi/cat-bot-stop-narkotik-dopomig-zablokuvati-ponad-300-narkokramnic-borotba-z-narkocumoyu-trivaje-oleksandr-gogilasvili
3. What Are Police Like in Other Countries? Council on Foreign Relations. URL: https://www.cfr.org/backgrounder/how-police-compare-different-democracies

Григорович О. Б.
начальник Департаменту інформаційно - аналітичної підтримки Національної поліції України, полковник поліції
Разєнков Є. В.
начальник відділу проєктного та ризикового менеджменту Департаменту інформаційно -аналітичної підтримки Національної поліції України, підполковник поліції

ІНФОРМАЦІЙНО – АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ТА СЛІДЧИХ ОРГАНІВ ПІД ЧАС ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

З першого дня повномасштабного вторгнення російської федерації на територію України, окупаційні війська порушують правила ведення війни і норми міжнародного права та масово чинять воєнні злочини та злочини проти людяності, вбиваючи цивільних, руйнуючи інфраструктуру та депортуючи населення.

Якісний збір доказової бази, документування кожного злочину, накопичення відомостей та даних про воєнні злочини та осіб, які їх скоїли – є запорукою притягнення до відповідальності та невідворотного покарання.

Однак, розслідування багатоепізодних фактів скоєння воєнних злочинів, інформація за якими внесена до Єдиного реєстру досудових розслідувань, великої кількості виявлених в рамках кримінальних проваджень осіб, причетних до скоєння злочинів, документування їх злочинної діяльності декількома структурними та територіальними підрозділами Центрального органу управління поліції та головних управлінь Національної поліції в областях, іншими правоохоронними відомствами, існуючий паперовий облік таких осіб має ряд недоліків: накопичена інформація систематизується недостатньо та не ефективно; відсутня можливість дистанційного вивчення чи аналізу інформації, її миттєвого обміну, та, як наслідок, зменшується якість зібраної інформації в цілому.

Саме тому виникла необхідність у накопиченні в єдиному сегменті всіх відомостей, пов’язаних із збройною військовою агресією російської федерації, яка фактично була розпочата 2014 року в окремих районах Донецької та Луганської областей, а з 24 лютого 2022 року – повномасштабно на всій території країни.

Відповідно до статей 25, 26 Закону України «Про Національну поліцію» поліція в межах інформаційно-аналітичної діяльності формує, наповнює, підтримує в актуальному стані та користується реєстрами і базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС МВС) [1].

Наповнення ЄІС МВС поліцейськими здійснюється за допомогою інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (далі – система ІПНП) відповідно до Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» затвердженого наказом МВС від 03.08.2017 № 676, зареєстрованим у Міністерстві юстиції України 28 серпня 2017 за № 1059/30927 (далі – Положення) [2].

Відповідно до пункту 2 розділу IV Положення адміністратором системи ІПНП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.

Згідно з пунктом 4 Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України (далі – ДІАП), затвердженого наказом Національної поліції України від 31 січня 2020 року № 77 (зі змінами), ДІАП є

відповідальним підрозділом за організацію (здійснення) розроблення, упровадження, супроводження (адміністрування) інформаційних систем [3].

Так, з метою внесення інформації про осіб, які причетні до військової агресії (військовослужбовці збройних сил російської федерації, члени незаконних збройних формувань, приватних військових компаній, колаборантів тощо) та події, пов'язані із вчиненням зазначеною категорією осіб на території України кримінальних правопорушень, ДІАП на центральному серверному програмно-технічному комплексі системи «ІПНП» розроблено та впроваджено в експлуатацію інформаційну підсистему «Воєнний злочинець» (далі – ІП «Воєнний злочинець»).

Функціонал ІП «Воєнний злочинець» передбачає наповнення в режимі реального часу банку даних інформацією про зазначених осіб та події, з можливістю її доповнення та перегляду одночасно всіма користувачами системи «ІПНП», яким наданий відповідний доступ, в тому числі підрозділами кримінальної поліції та слідства як Центрального органу управління поліції, так і територіальних органів; інтеграцію внесеної інформації з наявною в інших підсистемах, зокрема «Єдиний облік», «Кримінальна статистика», «Розшук», «Пізнання» та ін.; наповнення інформаційної картки відомостями про ймовірне місце знаходження, біометричні (в тому числі із можливістю додавання фото, відеозображень) та антропологічні дані, належність до певного військового формування у відповідний проміжок часу, сторінки у соціальних мережах, родинні зв'язки та інші, пов'язані відомості відносно особи з подальшим якісним та миттєвим виводом інформації, систематизацією та графічним відображенням на карті місцевості, в розрізі різних аналітичних рішень [4] [5].

Крім того, Національна поліція України виступила ініціатором об'єднання відомостей, що стосуються збройної військової агресії російської федерації, які маються у Служби безпеки України, Офісу Генерального прокурора, Державного бюро розслідувань, Збройних сил України, Головного управління розвідки Міністерства оборони України, Державної прикордонної служби України, Служби зовнішньої розвідки України в зазначеній інформаційній підсистемі, що надає змогу працівникам підрозділів кримінальної поліції в режимі реального часу при документуванні злочинів отримувати наявні відомості та мати комунікацію із зазначеними правоохоронними відомствами.

Так, Департаментом інформаційно-аналітичної підтримки Національної поліції відповідні доступи на внесення та перегляд інформації в ІП «Воєнний злочинець» системи «ІПНП» надані як співробітникам кримінальної поліції Національної поліції, так і співробітникам зазначених відомств.

Таким чином, завдяки зазначеній інформаційно-аналітичній роботі, яка щоденно та безперервно здійснюється працівниками правоохоронних відомств, встановлюється, фіксується, документується та накопичується інформація про факти переміщення (руху) ворожої техніки, моменти обстрілів та бомбардування, нанесення артилерійських та авіаційних ударів по житлових будинках, школах, дитсадках, електростанціях та інших об'єктах забезпечення життєдіяльності населених пунктів, обстріли колон евакуації цивільних осіб, випадки вчинення мародерства та інших диверсійно-розвідувальних, протиправних і злочинних діянь.

На даний час загальний масив унесеної до підсистеми інформації складає більш ніж 241 тис. інформаційних карток щодо осіб, причетних до військової агресії з боку російської федерації (з них 66 тис. із фотозображенням осіб) та 3125 карток стосовно скоєних кримінальних правопорушень.

Враховуючи вищевикладене, ІП «Воєнний злочинець» системи ІПНП забезпечує процес пошуку та аналізу інформації, швидкої адаптації до виконання різних аналітичних завдань, особливо в умовах дефіциту часу та надає можливість працівникам підрозділів кримінального блоку та слідчих органів, застосовуючи високий

рівень теоретичної підготовки, практичного досвіду та спеціалізованого програмного забезпечення, на високому рівні виконувати функції із розкриття злочинів та притягнення до відповідальності винних осіб.

Література

1. Закон України «Про Національну поліцію». 2015. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
2. Наказ МВС України від 03.08. 2017 № 686 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». 2017. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text
3. Наказ Національної поліції України 31.01.2020 року № 77 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України». 2020. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf
4. Наказ МВС України від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». 2023. URL: https://zakon.rada.gov.ua/laws/show/z0739-19#n14
5. Наказ МВС України від 28.06.2023 № 534 «Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»«. 2023. URL: https://zakon.rada.gov.ua/laws/show/z1486-23#Text

Грищенко О. В.

професор кафедри оперативно-розшукової діяльності та розкриття злочинів, кандидат юридичних наук

Грищенко Д. О.

старший викладач кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ

Чукалов К. Е.

курсант факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

У матеріалі на основі методології системного підходу представлено дослідження теоретико-правових засад правового забезпечення кібербезпеки критичної інформаційної інфраструктури України. Розглянуто чинне законодавство та проаналізовано підзаконні нормативно-правові акти України у галузі кібербезпеки критичної інформаційної інфраструктури. Зазначено, що сьогодні в Україні важливо забезпечити ефективне управління регіональними системами захисту інформації, а також безперебійне і ефективне функціонування об’єктів інформаційної інфраструктури, особливо – критичної інфраструктури. Для того, щоб домогтися цих результатів на практиці, необхідно на перший план поставити реалізацію таких основних завдань, як розвиток кадрового потенціалу в галузі забезпечення кібербезпеки і розвиток національної галузі інформаційних технологій.

Правове регулювання створення і використання інформаційної інфраструктури в Україні безпосередньо пов’язане з правовим забезпеченням безпеки усіх учасників

цього процесу (інформаційних відносин). Організація нових форм взаємодії державних органів влади з фізичними і юридичними особами повинна здійснюватися за певними стандартами електронних форм взаємодії. Використання інформаційної інфраструктури створює суспільні відносини, регулювання яких має здійснюватися за допомогою правових норм, а розробка, прийняття, застосування і виконання обов'язкових вимог до інформаційних технологій має здійснюватися на основі норм технічного регулювання. Інформаційні відносини, які виникають при використанні цифрових технологій, вимагають: визначення державного підходу до правового регулювання поданих відносин; розробки методології забезпечення інформаційної безпеки інформаційної інфраструктури та її користувачів. У цьому випадку формування національного законодавства в галузі створення і використання інформаційної інфраструктури є невідкладним завданням будьякої держави, включаючи Україну.

Так, критична інформаційна інфраструктура відрізняється від інформаційної інфраструктури включенням автоматизованої системи управління суб'єктів критичної інфраструктури та систем електрозв'язку в якості об'єктів критичної інформаційної інфраструктури. Відповідно до чинного Закону України «Про Національну програму інформатизації» під об'єктом інформатизації доцільно розуміти сукупність інформаційних ресурсів, засобів і систем обробки інформації (відомостей та/або даних), які використовуються відповідно до заданої інформаційної технології, засобів забезпечення, приміщень або об'єктів (будівель, споруд, технічних засобів), в яких ці засоби і системи встановлені, або приміщень і об'єктів, призначених для ведення конфіденційних переговорів .

До об'єктів критичної інформаційної інфраструктури доцільно віднести автоматизовані системи управління, що належать державним установам і органам влади, юридичним і фізичним особам-підприємцям, які забезпечують взаємодію зазначених систем або мереж, що функціонують у сфері охорони здоров'я, освіти і науки, транспорту, зв'язку, енергетики, банківській сфері та інших сферах фінансового ринку, паливно-енергетичного комплексу, у галузі атомної енергії, оборонної, ракетнокосмічної, гірничодобувної, металургійної, хімічної промисловості і т. д

Інформаційна інфраструктура – це частина інформаційної сфери, яка є складно організованою системою, створюваною та функціонуючою на засадах принципів і механізмів міжнародного та національного правового регулювання суспільних відносин. Проблема забезпечення кібербезпеки вимагає вдосконалення правових, організаційних і технічних механізмів регулювання суспільних відносин, що виникають в інформаційній сфері. Сьогодні в Україні важливо забезпечити ефективне управління регіональними системами захисту інформації, а також безперебійне і ефективне функціонування об'єктів інформаційної інфраструктури, особливо – критичної інфраструктури. Для того, щоб домогтися цих результатів на практиці, необхідно на перший план поставити реалізацію таких основних завдань, як розвиток кадрового потенціалу в галузі забезпечення кібербезпеки і розвиток національної галузі інформаційних технологій.

Потрібно систематизувати і удосконалити нормативноправові акти Кабінету Міністрів України та органів виконавчої влади на основі виявлення і виокремлення тих положень, які не відповідають вимогам щодо забезпечення кібербезпеки інформаційних технологій у міжвідомчій взаємодії, виходячи із сучасних реалій сьогодення.

Література

1. Про основні засади кібербезпеки України 05.10.2017, № 2163-VIII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Захист критичної інфраструктури : впровадження в Україну [Critical infrastructure protection: problems and prospects of implementation in Ukraine]. Kyiv: NISD (in Ukrainian) [Бірюков, Д. С., & Кондратов, С. І. (2012). Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ: НІСД] https://niss.gov.ua/sites/default/files/2013-02/Sots_zahust-86178.pdf
3. Про національну програму інформатизації [About the National Informatization Program] (Ukraine), 04.02.1998, No 74/98-BP. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (in Ukrainian) [Про Національну програму інформатизації (Україна), 04.02.1998, № 74/98-ВР. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text

Грищук А. Б.

доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Хімко Я. П.

аспірант кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ

КЛАСИФІКАЦІЯ ШІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сучасні електронні носії інформації є складними багатофункціональними пристроями. Будь-який тип фізичних носіїв, здатних зберігати інформацію, може бути підданий аналізу. Сюди входять комп'ютерні жорсткі диски, накопичувачі, зовнішні USB-пристрої, карти SD, що використовуються в камерах, ігрових системах, смартфонах.

Під електронними носіями розуміються пристрої, конструктивно призначені для постійного або тимчасового зберігання інформації у вигляді, придатному для використання в електронно-обчислювальних машинах, для її передачі інформаційно-комунікаційними мережами або обробки в інформаційних системах. Існує широкий діапазон різних електронних носіїв інформації, які мають різне призначення, технічні характеристики, принципи дії. За формою подання більшість інформації на електронних носіях належить до текстової, проте у практиці правоохоронних органів трапляються випадки використання слідів у формі графічної чи звукової інформації.

За формою інформація на електронних носіях може представляти окрему програму, комплекс програм, банки та бази даних, електронні повідомлення, окремі файли, веб-сайти або окремі сторінки.

За цільовим призначенням програми можуть бути орієнтовані на виконання корисних чи шкідливих функцій. Ефективний підхід до виявлення упакованих спеціалізованих шкідливих програм, у яких згодом з'являється кілька версій у скомпрометованих системах, полягає у розробці автоматизованого інструменту, який шукає характеристики, виявлені під час аналізу та реверс-інжинірингу.

Ідеальний інструмент перевірятиме файли та записи реєстру в системі, розпаковувати файли в міру необхідності, декодувати інформацію, яку кодує шкідливе програмне забезпечення, шукати відомі характеристики у шкідливому програмному забезпеченні та реєстрі.

Для правової науки інтерес представляє клас програм – шкідливе програмне забезпечення (Malware). Механізм роботи зводиться або до прямого впливу на програмне середовище, якщо воно технічно здійсненне, або до використання дефектів апаратного та програмного забезпечення.

Класифікація для систематизації видів шкідливих програм, виділяє із класу шкідливих програм (Malware) підкласи: програми-віруси (Virus), програми-черв'яки (Worm) і троянські програми (Trojan) [1].

Для боротьби зі шкідливими програмами важливо правильно класифікувати шкідливі програми. Це різні типи шкідливих програм та пояснення того, як їх розпізнати.

1. **Вірус**. Вчені схильні називати всі шкідливі програми вірусами, але це не так. Вірус змінює інші законні файли хоста таким чином, що коли запускаєте файл у системі жертви, запускаєте вірус. Сьогодні, коли кіберпростір заражають різні шкідливі програми, комп'ютерні віруси стали рідкістю. Вони становлять менше 10 % всіх шкідливих програм. Віруси заражають інші файли. Це єдині шкідливі програми, які дуже важко очистити. У більшості випадків вони або видаляють, або поміщають у карантин заражений файл, але не позбавляються самого вірусу.
2. **Черв'як**. Черв'як відтворюється та поширюється без участі кінцевого користувача, викликаючи руйнування. Якщо вірусам потрібні кінцеві користувачі для запуску, з метою подальшого продовження процесу зараження інших файлів і систем, то черв'як не потребують таких дій. Вони поширюються самі по собі, само відтворюючись у процесі, руйнуючи системи, пристрої, мережі та підключену інфраструктуру. Черв'як розповсюджуються, використовуючи з цією метою інші файли та програми. Коли одна людина в організації відкриває електронний лист, що містить черв'як, вся мережа в організації може бути заражена за кілька хвилин.
3. **Троян**. Трояни маскуються під легітимні програми, але містять шкідливі інструкції. Трояни в основному надходять електронною поштою або поширюються із заражених веб-сайтів, які відвідують користувачі. Вони працюють лише тоді, коли запускають, дають команду на встановлення жертви. Користувач може виявити спливаюче вікно з повідомленням про те, що його система заражена. Вікно наказує запустити програму для очищення системи. Користувач клює на вудку, не знаючи, що то троян. Трояни поширені тому, що їх легко написати. Вони прості, тому що трояни поширюються, обманюючи кінцевих користувачів для їхнього запуску. Це ефективно робить програмне забезпечення безпеки марним.
4. **Програми-вимагачі**. Програма-вимагач вимагає викупу, щоб повернути все в потрібне русло, зробити відкат системи до стану, що передує зараженню. Основна проблема програм-вимагачів, які надзвичайно швидко поширюються по організаціях, мережах та країнах, полягає в тому, що вони шифрують з метою блокування всі файли в системі або мережі, роблячи їх недоступними. З'являється записка з вимогою оплати в валюті або іншому форматі за розшифрування файлів. Якщо викуп не буде заплачено, зашифровані файли можуть бути знищені. Програми-вимагачі розглядають як одну з найбільш руйнівних форм шкідливих програм. Більшість програм-вимагачів є різновидом троянських програм і розповсюджуються за допомогою соціальної інженерії. У деяких випадках хакери відмовляються дешифрувати файли навіть, якщо викуп сплачено.
5. **Рекламне програмне забезпечення**. Рекламне програмне забезпечення – спроба піддати користувачів небажаній, потенційно шкідливій рекламі. Ці оголошення заражають пристрій користувача. Існують рекламні програми, які перенаправляють користувача під час пошуку у браузері на схожі веб-сторінки із рекламою інших продуктів. Видалити рекламне програмне забезпечення простіше. Потрібно знайти

шкідливий файл і видалити його. Не всі методи, які використовуються шкідливими програмами для впровадження на комп'ютер з Windows, будуть виявлені засобами автозапуску або аналогічними інструментами. Наприклад, порядок, у якому операційна система Windows шукає залежності, може використовуватися для запуску шкідливих програм. Тому якщо під час перевірки місць автозапуску не буде виявлено нічого, в системі можуть бути стійкі шкідливі програми.

6. **Шпигунське програмне забезпечення**, як випливає з назви, допомагає хакерам стежити за системами та їх користувачами. Цей тип шкідливого ПЗ може використовуватися для реєстрації ключів та аналогічних дій, допомагаючи хакерам отримати доступ до особистих даних та інтелектуальної власності. Сучасні шкідливі програми призначені для підключення до мережі для виконання різних функцій. Найвідоміший – маяк, коли нещодавно скомпрометована система передає сигнал на сервери зловмисника, щоб підтвердити, що вона є новою жертвою, готова до виконання команд. Шпигунське використовується людьми, які хочуть стежити за діями на комп'ютері людей, особисто відомих їм. Шпигунське програмне забезпечення легко видалити.
7. **Безфайлове шкідливе програмне забезпечення**. Традиційні шкідливі програми переміщуються і заражають за допомогою файлової системи, безфайлові шкідливі програми вирішують завдання без безпосереднього використання файлів або файлових систем. Такі шкідливі програми використовують та поширюються лише в оперативній пам'яті. Вони поширюються за допомогою «нефайлових» об'єктів ОС, API, реєстри. Атаки безфайлових шкідливих програм часто ініціюють з використанням існуючої легітимної програми або з використанням існуючих легітимних інструментів, вбудованих в ОС (наприклад Microsoft Powershell). Стає дуже складно виявити та запобігти таким атакам.
8. **Гібридна атака**. Це досить небезпечний і руйнівний різновид. Є шкідливе ПЗ, яке може бути комбінацією більш ніж одного потоку традиційних шкідливих програм. Наприклад, деякі шкідливі програми є частково вірусами, частково троянськими програмами та частково черв’ями. Таке шкідливе програмне забезпечення може виглядати як троян на початковому етапі, після чого буде поширюватися як черв'як. Існують боти, в яких хакери використовують один вид шкідливого програмного забезпечення для отримання доступу до сотень комп'ютерів. Ці системи використовуються (хакерами, або іншими, які їх купують) щодо інших атак. Наприклад, більшість сучасних троянських програм поєднують не одну поведінку, а набір видів діяльності, що надає злочинцям можливості для маніпулювання інформацією користувача. Для завантаження троянських програм у комп'ютерну систему без відома користувача застосовують різні способи: розсилання електронних листів, які містять шкідливе вкладення; використання зв'язок експлойтів при веб-серфінгу користувачів у мережі Інтернет; впровадження шкідливого коду в легальне програмне забезпечення, що розповсюджується; поширення в локальній мережі за допомогою застосування штатних програмних засобів; фізичний доступ до цільової системи.

Вивчення різних форм існування цифрової доказової інформації на електронних носіях дозволить правоохоронним органам адаптуватися до умов життя в епоху значних технологічних змін. Перелічені носії інформації вивчаються криміналістикою як потенційні слідові носії. Основна проблема прив'язати носій і інформацію до автора або користувача.

Література

1. Журавчак Д. Ю., Дудикевич В.Б., Толкачова А.Ю. Дослідження структури системи виявлення та протидії атакам вірусів-вимагачів на базі Endpoint Detection And Response. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». (2023). № 3 (19), С. 69-82.

Груба В. В.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Світличний В. А.
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

СИСТЕМА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ МВС УКРАЇНИ

В сучасних реаліях терміни «інформація» та «інформаційне забезпечення» відіграють ключову роль у роботі всіх підрозділі Національної поліції України (далі – НПУ), оскільки процеси попередження правопорушень та, насамперед, досудового розслідування повністю залежать від якості та швидкості отримання потрібної інформації.

Система інформаційного забезпечення Міністерства внутрішніх справ України – це сукупність інформаційних підсистем, побудованих з урахуванням дотримання та надання загальновизнаних та обов'язкових вимог: правової бази, організаційної та кадрової підтримки інформаційних департаментів, навчання та перепідготовка кадрів; комп'ютерного програмного забезпечення, телекомунікаційних засобів та технологій; матеріально-технічної та фінансової підтримки [1]. На теперішній час наказом МВС України від 22 квітня 2021 року № 301 затверджено Концепцію програми інформатизації системи МВС України та центральних органів виконавчої влади, діяльність яких спрямовується і координується КМУ через міністра внутрішніх справ України, на 2021-2023 роки.

Насамперед, за інформаційне забезпечення відповідає Департамент інформаційно-аналітичної підтримки (далі ДІАП) НПУ. Підрозділи ДІАП забезпечують функціонування систем оперативно-розшукового, а також довідково-інформаційного призначення. Основні складові цих систем – «Інтегрована інформаційно-пошукова система МВС України» («АРМОР»), «ЄРДР», «НАІС», «АРКАН», «ЦУНАМІ». Ця система облегшує роботу практичних працівників тим, що надає можливість швидкого реагування, звільнення від здійснення однотипних операцій, знаходить оптимальне вирішення складних ситуацій або таких, де людині знадобиться більше часу, ніж електронно-обчислювальній машині, спрощення подальшого розбору певного процесу та, перш за все, можливість одночасного реагування на значну кількість подій [3].

Наразі пріоритетними проєктами інформатизації системи МВС України в сучасних умовах є:

- «Безпечна країна»;
- «Система 112»;
- Модернізація електронних інформаційних ресурсів у сфері безпеки дорожнього руху;
- Єдиний реєстр зброї;
- Реєстр відомостей про статус особи у кримінальному провадженні та судимості;
- Єдиний сервіс ідентифікації фізичних осіб;
- Єдина багатозонова система цифрового радіозв'язку;
- Єдиний державний реєстр територіальних громад;
- Система планування та управління об'єднаними силами із забезпечення громадської безпеки та ліквідації надзвичайних ситуацій.

Отже, питання існування та вдосконалення системи інформаційного забезпечення є актуальним, особливо під час воєнного стану й розслідування кримінальних проваджень пов'язаних з військовими злочинами. Важко отримати інформацію стосовно осіб та їх вчинків, які або не перебувають взагалі не території України, або знаходяться за сотні кілометрів від обслугованої території підрозділу, а також притягнення їх до відповідальності без належного обґрунтування вини обвинуваченого. Вирішення цього питання повністю залежить від системи інформаційного забезпечення. Вона об'єднує увесь інформаційний простір підрозділів НПУ та дозволяє отримати інформацію, що без існування цієї системи отримувалася шляхом використання великих матеріальних та людських ресурсів [2].

Питання вдосконалення та підтримки інформаційного забезпечення є основною функцією ДІАП. Різні за своїм напрямом системи створюють можливості маніпулювання, систематизації та обробки інформації для подальшого використання у досудових розслідуваннях.

У висновку, розвиток систем інформаційного забезпечення забезпечує вдосконалення та облегшення роботи підрозділів НПУ, а саме підвищення рівня якості надання поліцейських послуг та профілактики розкриття кримінальних правопорушень ще на етапі планування.

Література

1. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналіт. доп. Київ : НІСД, 2014. 76 с.
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. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС : постанова Кабінету Міністрів України від 20.10.2017 № 870 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF

Гупалюк Я. Р.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Світличний В. А.

доцент кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ТРЕНУВАННЯ ПОЛІЦЕЙСЬКИХ З ВИКОРИСТАННЯМ СИМУЛЯЦІЙНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сучасні вимоги до поліцейських передбачають не лише фізичну силу, але і високий рівень професійності, комунікативних навичок та здатність швидко реагувати на змінні ситуації. Симуляційні інформаційні технології дозволяють створити віртуальні середовища, в яких поліцейські можуть набути досвіду, аналізувати ситуації та вдосконалювати свої навички.

Одним із найпоширеніших застосувань симуляційних технологій у поліцейській підготовці є віртуальні навчальні площадки. Ці площадки відтворюють реальні ситуації, з якими можуть стикатися поліцейські, і дозволяють їм вправно тренуватися у вирішенні проблемних ситуацій. При цьому відбувається мінімізація ризику для тих, хто

навчається та зменшується потреба в матеріальних ресурсах для організації тренувань на місцях. Прикладом такого може бути автомобільний тренажер, який дозволяє військовим вдосконалювати навички водіння в різних умовах та на будь-який місцевості, зокрема на пересіченій, степовій, горній, пустельній та інших. На ньому встановлені всі прилади як на реальній машині. При цьому дії механіка-водія відпрацьовуються до автоматизму, що в подальшому дає певну перевагу під час керування бойовою технікою. Також значний плюс в такому навчанні – велика економія пального [2].

Симуляційні інформаційні технології також можуть бути використані для тренування поліцейських на реакцію в стресових ситуаціях. Вони дозволяють створити віртуальні ситуації, які можуть бути емоційно навантаженими, і допомагають поліцейським навчитися керувати своїми емоціями та приймати обґрунтовані рішення навіть в умовах стресу.

Симуляційні технології також можуть бути корисним інструментом для тренування поліцейських відповідати на масові події, такі як терористичні акти чи масові заворушення. Віртуальні симуляції дозволяють поліцейським розробляти стратегії, комунікувати та співпрацювати з іншими службами у віртуальних умовах, що може покращити координацію дій під час реальних подій. Наприклад компанія SKIFTECH постачає прокачані до рівня комплексних систем бойової підготовки тренажери розвідникам, спецпризначенцям, нацгвардійцям та іншим підрозділам українського війська. Навчання відбуваються у кількох десятках локацій у польових умовах. Запис бою можна передивитися і провести роботу над помилками [1].

Отже, з використанням симуляційних інформаційних технологій, поліцейські мають можливість ефективно навчатися та тренуватися в умовах, які відтворюють реальні ситуації, але при цьому не створюють реальних загроз для їхнього життя та здоров'я. Ця ініціатива сприяє покращенню рівня професійної підготовки поліцейських та забезпечує їхню готовність до різних викликів, з якими вони можуть стикнутися в сучасному світі. Симуляційні інформаційні технології відкривають нові можливості для підвищення якості навчання поліцейських та розвитку їхніх навичок. Важливо пам'ятати, що вони не замінюють реального досвіду, але допомагають відтворити його в безпечних умовах. Ця інноваційна практика може призвести до покращення роботи правоохоронних органів та забезпечити більш безпечне та ефективне забезпечення громадської безпеки.

Література

1. Стріляй скільки хочеш. Війна дала поштовх розвитку віртуальних тренажерів для військових. Чи можна побудувати на цьому бізнес – Forbes.ua. URL: https://forbes.ua/innovations/strilyay-skilki-khochesh-viyna-dala-poshtovkh-rozvitku-virtualnikh-trenazheriv-dlya-viyskovikh-chi-mozhna-pobuduvati-na-tsomu-biznes-18112022-9834
2. Тренажери майбутнього вже існують для військових URL: https://www.sknews.net/trenazhery-maybutn-oho-vzhe-isnuiut-dlia-viys-kovykh/

Д’яков А. В.
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук

ІНТЕРНЕТ БОЙОВИХ РЕЧЕЙ (IoBT): СУЧАСНА КОНЦЕПЦІЯ РОЗВИТКУ ПРАВООХОРОННИХ ОРГАНІВ

Виникнення поняття Інтернету речей (IoT) обумовлено логікою появи двох потужних технологічних явищ, таких як штучний інтелект та мережеві комунікації. Системи, які відтворюють імітацію розумових функцій стають більш ефективними, коли вони мають можливість комунікувати між собою та поєднуються у єдину систему, що працює за єдиним задумом.

Застосування такої концепції у сфері безпеки і оборони отримала назву Інтернету бойових речей (IoBT), вона характеризується використанням апаратно-програмних приладів і систем спеціального призначення в ході виконання оборонних і правоохоронних заходів. Концептуальні основи Інтернету бойових речей, його теоретична складова на сьогодні стрімко розвиваються та знаходять технічне втілення в окремих середовищах забезпечення безпеки країни, але можна впевнено стверджувати, що у найближчі часи він стане домінуючим фактором в ефективності забезпечення національної безпеки.

З огляду на те, що IoBT має потужні можливості збору, аналізу та передачі інформації та орієнтований на підвищення (бойових) можливостей правоохоронних органів (Національної гвардії, Національної поліції, Державної прикордонної служби, Служби безпеки України та інш.) в сучасних умовах за рахунок досягнення інфокомунікаційної переваги, об'єднання учасників в єдине інформаційне середовище, можна зазначити концептуальні засади його застосування:

Моніторинг та управління озброєнням та технікою: контроль і управління за допомогою IoBT за станом техніки, зброї, обладнання, їх технічними параметрами та здатністю до використання. Це дозволяє оперативно проводити технічне обслуговування та ремонти.

Навчання та моделювання: IoBT може бути використаний для моделювання відповідних умов та кейсів в ході тренувань та навчання правоохоронців. Моделювання різних ситуацій та умов передбачається до застосування оцінки обстановки, розрахунків необхідних сил та засобів, прогнозування розвитку подій та прийняття відповідного рішення.

Системи моніторингу (спостереження) та розвідки: використання дронів, супутникового зв'язку та відповідних сенсорів парціальних каналів приладів та систем спостереження допомагає в отриманні розвідувальної інформації на ворожих територіях, дозволяючи здійснювати нагляд із безпечного віддалення.

Кібербезпека та захист від кібератак: IoBT також включає в себе заходи з кібербезпеки, оскільки важливо захищати спеціальні мережі від кіберзагроз та забезпечувати безпеку обміну даними.

Комунікації та координація: IoBT дозволяє підвищити ефективність комунікацій між підрозділами правоохоронних органів через розроблені системи зв'язку та координації, що сприяє кращій організації запланованих заходів та операцій.

До принципів застосування IoBT можна віднести наступне:

1. Сили та засоби правоохоронних органів, об'єднані надійними мережами, мають змогу покращеного обміну інформацією та досягнення інформаційної переваги супротивником, в ході охорони громадської безпеки і порядку.

2. Обмін інформацією підвищує якість (достовірність, своєчасність, адекватність, об’єктивність та інш.) інформації та загальної ситуаційної поінформованості.

3. Загальна ситуаційна обізнаність дозволяє забезпечувати взаємодіє між силами правоохоронних органів і самосинхронізацію між відповідними засобами, підвищує стійкість і швидкість управління, а це, своєю чергою, різко підвищує ефективність виконання спланованих завдань.

Використання IoBT пов’язано із виникненням ризиків, основним з яких є несанкціонований доступ до важливих систем та безпосередньо даних. Недостатня захищеність може привести до перехоплення інформації, пошкодження та знищення техніки.

Надійність систем є ще одним суттєвим ризиком у застосуванні IoBT. Проблеми з надійністю або непередбачувані відмови можуть призвести до серйозних проблем в ході спланованих заходів та під час проведення операцій. В свою чергу, можна додати, що висока залежність від технологій IoBT може привести до ситуації, коли відсутність або несправність відповідних технічних засобів може привести до зриву виконання відповідних заходів.

Ще одним з перспективних ризиків у застосуванні IoBT є автономність застосування зброї, відповідальність за прийняття рішень системами штучного інтелекту та можливість шкоди для цивільного населення.

Таким чином, управління вказаними ризиками вимагає не лише технічних заходів забезпечення безпеки, але й ретельного регулювання, визначення стандартів та навчання персоналу щодо безпеки та етики використання IoBT.

Донець Я. О.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Світличний В. А.
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

КІБЕРБЕЗПЕКА – ЗБРОЯ У БОРОТЬБІ З ШАХРАЯМИ

Вступ. В наші дні, злодій – це не обов'язково холоднокровна озброєна людина. Інформаційна революція призвела до того, що кожен може виявитися злодієм, навіть звичайний студент із ноутбуком та доступом до інтернету. Процес інформатизації сьогоденного суспільства призвів до того, що інформація перетворюється у так званий стратегічний ресурс, який володіє цінністю, тобто має якості товару. Суспільство вже не може існувати та звичайно функціонувати без інформаційного обміну в інформаційно-телекомунікаційних системах. На даному етапі, внаслідок швидкого розвитку та застосування сучасних технологій, питання захисту людства від їхнього використання в злочинних цілях усе більше загострюється.

Виклад основного матеріалу. З початку війни в Україні, ми стали свідками чисельних кібератак, які охопили державні установи, громадян та приватні організації. Підприємства, які є частиною критичної інфраструктури, зокрема, телекомунікаційні, енергійні, медіа та фінансові компанії, також повинні знаходитися у режимі підвищеної готовності, тому що саме ці галузі часто стають пріоритетними цілями у період війни.

Сьогодні, війна в інформаційному просторі може завдати не меншої шкоди, чим війна на полі бою.

Кіберзлочиність не має державних кордонів, таким чином злочинець може загрожувати інформаційним системам, які знаходяться в будь-якій державі світу. Ці злочини сильно відрізняються від інших, давно визначених злочинів, що обумовлює складність цієї процедури розслідування відповідно до чинних законодавствами держав

Взагалі, комп'ютерна злочинність має наступні характеристики [1]:

- Предметами комп'ютерних злочинів є права на об'єкти нерухомості. Інформаційні атаки працюють відносно інформації пенсійних та інвестиційних фондів, через них відбувається котирування інструментів фондового ринку, обертаються індекси на валютних, торгових та фондових ринках. Фактами таких атак на об'єкти є інформаційна інфраструктура, котрі вона забезпечує функціонуванням сфер, критичних для державного управління та економіки;
- Боротьба з кіберзлочинами для постанов багатьох країн не є пріоритетністю, через що не можна зрозуміти достатній рівень небезпеки від комп'ютерних злочинців у багатьох державах;
- Брак у деяких державах своєрідної взаємодії між правоохоронними відомствами та приватним бізнесом з питань дозволу частини інформації (елементів доказу у електронному вигляді) та її збереження в комп'ютерних системах.

На перший погляд, кожна людина може подумати, що кібератаки не завдають великої шкоди та не забирають людських життів, але це не так. Можна навести декілька прикладів [2].

Збір інформації – злом приватних сторінок або серверів, бази даних для збору цінної інформації. У такому випадку дезінформація та викрадення матеріалів. Можна навести наприклад з відомостей щодо пересування військ у районі ведення бойових дій, призводить до неминучих людських втрат. Це називають – кібершпигунством.

Пропаганда – розсилка повідомлень (спаму), що містять інформацію пропагандистського напрямку, неправдиві новини для просування своєї ідеології та дезорієнтації населення.

Вандалізм – це атаки, які не вбивають людство, але завдає удару по репутації держави у світі та серед населення, простими словами, завдає втрат по авторитету.

Не для кого не секрет, що використовуючи кіберпростір, хакери можуть зламати захищені дані та отримати необхідну інформацію, тому вам варто спрямувати свої сили на захист мереж і забезпечити їх безпеку. Треба дотримуватися таких рівнів захисту інформації:

Запобігання – доступ до інформації має тільки персонал, який отримав спеціальний допуск та вже має необхідні фахові навички.

Виявлення – треба запобігати проявам злочинів і зловживань, навіть коли системи захисту були обійдені.

Обмеження – зменшити обсяг втрат, у випадку, коли злочин все-таки здійснився, незважаючи на спроби щодо його виявлення.

Відновлення – слід забезпечити продуктивне очищення інформації та даних за наявності документованих і перевірених планів з відновлення.

Суспільство вимагає правил, утворення стандартів, норм, положень, інструкцій та безліч інших документів, задля того, щоб почувати себе захищеним у кіберпросторі.

Кожен день з’являються нові галузеві нормативні документи, які відносяться до кіберризиків, підвищується інтерес до певної галузі зі органів.

В Україні створюються норми з безпеки для об’єктів критичної інфраструктури. Все частіше можна почути заклики до більш активної участі у обміні інформацією, а також до надання обов’язкової звітності про кібератаки для нашої протидії виникненню наслідків таких атак. Треба розуміти встановлення обов’язкових вимог у цій сфері. До речі, якщо це і не відбудеться в найближчому часі, загальна думка сьогодні така, що державні органи, структури і навіть клієнти хочуть розширити свої знання про кібербезпеку.

На нашу думку, необхідно надалі розвивати співпрацю у сфері надання інформаційної безпеки використовуючи двосторонні і багатосторонні договори через об'єднання національних законодавств у сфері інформаційної безпеки, організацію спільних виробництв захисту інформації, звісно підготовку професіоналів у сфері інформаційної безпеки інформаційно-телекомунікаційних систем.

Висновки. Успішне вирішення проблем інформаційної безпеки може існувати лише при хорошій взаємодії державних структур усіх держав на основі прийнятих нормативно-правових документів у сфері інформаційної безпеки держав. Державі необхідне збільшення інвестування в кібербезпеку, щоб протидіяти атакам на великі державні й приватні компанії і запобігати спробам дестабілізувати суспільство. Основи законодавчих механізмів для продуктивного кіберзахисту в умовах воєнного стану закладені. Обов'язок для кожного – при виявленні кібератаки швидко запустити цей механізм задля того, щоб у майбутньому таких атак та збитків від них ставало як найменше.

Література

1. Балашов В. Гаджет как опасность. Как украинцам уберечься от кибератак во время войны? – Delo.ua. Останні новини України та світу онлайн -Головний діловий портал Delo.ua. URL: https://delo.ua/ru/technologies/gadzet-kak-opasnost-kak-ukraincam-uberecsya-ot-kiberatak-vo-vremya-voiny-395687/
2. Шахрайство під час війни: схеми, що діють зараз. finance.ua. URL: https://finance.ua/ua/saving/moszenniczestvo-vo-vremia-vojny

Єсімов С. С.

професор кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПОНЯТТЯ, ОЗНАКИ І КЛАСИФІКАЦІЯ ЦИФРОВОЇ ІНФОРМАЦІЇ

Незважаючи на повсюдне активне використання терміна «цифрова інформація», легальне визначення цього поняття відсутнє. Чинне законодавство переважно використовує такі визначення, як «електронне повідомлення – інформація, передана чи отримана користувачем інформаційно-комунікаційної мережі», електронний документ – документована інформація, подана в електронній формі, тобто у вигляді, придатному для сприйняття людиною з використанням електронних обчислювальних машин, для передачі інформаційно-комунікаційних мереж або обробки в інформаційних системах та аналогічні їм.

Незважаючи на використання категорії «цифрова інформація» більшістю галузей права, у тому числі цивільним правом, наукові дослідження щодо визначення даного

поняття здебільшого ведуться в галузі кримінального права. Аналіз наявних на даний момент наукових досліджень, присвячених поняття, що розглядається, дозволяє резюмувати, що цифрова інформація має наступні характеристики: відомості, що надаються в електронній формі (в основному в двійковій системі числення); існує та передається в електронній мережі; для використання потрібна наявність провайдера; передбачено можливість необмеженого копіювання.

Зважаючи на вищевикладене, можна визначити цифрову інформацію як відомості (повідомлення, дані), закодовані в двійковій чи іншій системі числення, які не сприймаються людиною безпосередньо, які утримуються на призначених для цього матеріальних носіях і звертаються або можуть звертатися до інформаційно-комунікаційних пристроях, їх системах та мережах.

Ознаками цифрової інформації: є однією з об'єктивних форм існування інформації – електронною формою; завжди опосередкована через матеріальний носій, поза яким фізично не може існувати; доступ до такої інформації можуть одночасно мати кілька осіб; досить просто та швидко перетворюється з неелектронних форм в електронні і назад; копіюється на будь-які носії та пересилається практично на будь-які відстані; збирається, досліджується та використовується лише за допомогою спеціальних технічних засобів.

Слід зазначити, що, принципова відмінність цифрової інформації від інформації загалом полягає у формі надання внаслідок чого до класифікації можуть бути застосовані загальні підстави з урахуванням зазначеної особливості. Класифікація цифрової інформації може бути визначена у спосіб:

1. За місцем розміщення цифрової інформації: розміщена у мережі Інтернет. Особливістю такої інформації є можливість необмеженого звернення до інформації невизначеного кола осіб, тому при класифікації доцільно говорити про таку інформацію як про загальнодоступну чи обов'язкову для надання інформації; розміщена на електронному матеріальному носії.

Особливістю цього виду є можливість передачі такої інформації шляхом копіювання, та шляхом передачі матеріального носія. Слід зазначити, що дані види інформації можуть взаємно замінюватися – інформація з Інтернету може бути «завантажена» і розміщена на матеріальному носії та навпаки.

2. Доступність для звернення: загальнодоступна інформація – інформація, не обмежена в обігу, яка служить для інформування заінтересованих осіб про товари, роботи, послуги, новини, громадські та інші заходи. Як її особливості варто назвати те, що зацікавлені особи можуть самостійно здійснювати її пошук, обробку та зберігання; інформація, обов'язкова для надання – перелік встановлюється відповідно до нормативно-правових актів

Не розкриваючи перелік вищезгаданої інформації, слід зазначити, що в окремих випадках законом може бути передбачено розміщення інформації на офіційному сайті в Інтернеті; конфіденційна інформація – інформація, поширення якої обмежено чи заборонено володільцем. У співвідношенні з іншими класифікаційними підставами зауважимо, що категорію доцільно співвіднести з інформацією, що не розміщується в мережі Інтернет.

3. За форматом користувача: для використання людиною, надається в електронному форматі у будь-якій формі (аудіо, відео-, текст), що сприймається людиною без додаткової обробки; для використання машиною (машинний код).

4. За змістом: персональні дані – інформація, що відноситься до прямо чи опосередковано визначеної фізичної особи (суб'єкта персональних даних); інсайдерська інформація – точна та конкретна інформація, яка не була поширена та поширення якої може істотно вплинути на ціни фінансових інструментів, іноземної

валюти та товарів; угода в електронній формі – договори різної правової природи, що укладаються за допомогою інформаційних технологій та технічних пристроїв, відмінною особливістю яких є їх можливості щодо створення документів в електронному (цифровому) вигляді за умови, що зазначений електронний документ включає реквізити відповідної угоди; інформація про приватне життя громадянина, зокрема відомостей про походження, про місце його перебування чи проживання, про особисте та сімейне життя; інші види інформації, передбачені законодавством.

Зважаючи на відсутність легального визначення цифрової інформації, в доктрині складається розуміння про неї як відомості, закодовані в двійковій або іншій системі числення, які можуть звертатися виключно в інформаційно-комунікаційних пристроях, системах і мережах.

Цифрова інформація є одним з видів інформації та не є синонімічною комп'ютерної інформації. Вищезгадана характеристика дозволяє класифікувати цифрову інформацію за загальним та за спеціальними підставами.

Желновач Є. Г.
аспірант Одеського державного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СПЕЦІАЛЬНОГО ЗАКОНОДАВСТВО УКРАЇНИ ПРО ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО

Жовтень 2023 року відзначився безпрецедентною подією у сфері формування глобального і національного інформаційного суспільства. Так, в умовах війни загострилося питання боротьби з інформаційно-психологічними нападами агресора, що в свою чергу призвело, що медіарегулятори Латвії, Литви, Польщі, Румунії та України підписали у Варшаві Декларацію про співпрацю і взаємну підтримку в боротьбі з дезінформацією. Тим самим вони скріпили свої наміри разом докладати зусиль, щоби протидіяти впливу пропаганди, найперше російської, у суспільствах цих країн [1].

«Ця подія є чітким виявом спільної відповідальності і рішучості країн Східної Європи боротися з викликами, які ставлять перед нами дезінформація та російська пропаганда», – заявила голова Національної ради О. Герасим'юк. За її словами, історія ще раз доводить, як пропаганда, побудована на викривленні реальності, може впливати на суспільство і бути ключовим інструментом в руках тих, хто прагне контролювати думки громадян [2].

Голова Національної ради з питань мовлення Республіки Польщі Мацей Свірскі назвав підписання декларації історичною подією.

У свою чергу О. Герасим'юк зауважила, що дезінформація постійно пристосовується до нового інструментарію, якщо закривають певний канал її поширення.

Водночас, Єврокомісія оприлюднила звіт з дотримання Кодексу поведінки щодо дезінформації, до якого на добровільній основі приєдналися ключові міжнародні інтернет-платформи, зокрема такі як: Google, Meta, Microsoft, TikTok та інші.

Як зазначила віцепрезидент Єврокомісії Вера Йоурова дезінформація все ще залишається одним із найбільших ризиків для європейської демократії в інформаційному полі, включаючи ті, що пов'язані із російською війною проти України та з виборами» [3].

Єврокомісія оприлюднила приклади окремих розділів звіту з протидії дезінформації, що пов'язана із російською війною проти України. Так, у доповіді Google за період з січня по квітень 2023 року йдеться про те, що мережа YouTube припинила діяльність 411 каналів та 10 окремих блогів, які були долучені до скоординованої

операції впливу через «російське агентство з дослідження інтернету» (IRA), що напряму утримується росією [4].

І вищезгадана Декларація і кодекс не підпадають по багатьох характеристиках під категорію суто міжнародно-правових договорів, хоч і мають значну частку їх рис. Тому на нашу думку, саме це здебільш і є спеціальним законодавством у сфері становлення інформаційного суспільства в умовах війни.

Тому в нашому дослідженні ми поставили за мету проаналізувати чинне законодавство України, що регулює відносини, пов'язані із обігом інформації з урахуванням особливостей забезпечення свободи інформації. Слід сказати, що спеціальне законодавство України в інформаційній сфері налічує дуже велику кількість нормативних актів, але до нашого завдання входить пошук та виявлення лише тих нормативних актів та окремих положень, які безпосередньо відображають проголошення ідей свободи інформації, механізм їх втілення та захисту в інформаційному суспільстві.

Вважаємо доречним розпочати наш аналіз з нормативного акту, що має назву закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V [5].

Вказаний документ є важливим надбанням загальної структури забезпечення свободи інформації в України. Плановий характер нормативного акту відображає заінтересованість української влади у подальшому розвитку інституту свободи інформації. Теза, що міститься в загальних положеннях закону відображає демократичну та направлену на розбудову громадянського суспільства й свободи інформації думку законодавця: «одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя» [5].

Особливу увагу звертає на себе позиція держави щодо економічного стимулювання розвитку інформаційних технологій, так, у п. 3 акту зазначається, що формування сприятливих економічних умов розвитку інформаційного суспільства також виражається у «сприянні підприємницькій діяльності у сфері інформаційно-телекомунікаційних технологій за рахунок формування системи адміністративних, правових і економічних механізмів, які стимулюватимуть попит на інформаційну продукцію [5].

Слід зазначити не зрозумілу ситуацію у зв'язку з тим, що за п'ятнадцять останніх років, з часу прийняття означеного закону, Верховна Рада жодного разу більше не зверталася до його тексту зі змінами, доповненнями, бажанням пролонгації, або якогось іншого удосконалення. Це досить таки дивно, адже інші акти інформаційного законодавства майже щорічно піддавалися значним правкам. Більш того, з моменту набуття чинності закону України «Про медіа» (13.12.2022 р.) [6], що можна назвати актом консолідації інформаційного законодавства, який відмінив велику кількість нормативних актів у березні 2023 року та які будуть нами розглянуті нами нижче. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» не став фрагментально чи категоріально частиною цієї консолідації. Тим самим, законодавець, на наш погляд, зробив значну втрату юридичних інструментальних можливостей в подоланні вищеозначених бар'єрів на шляху формування справжнього інформаційного суспільства в Україні.

На сьогодні, як нами зазначалося консолідованим нормативним актів в сфері інформаційного законодавства є закон України від 13.12.2022 № 2849-IX «Про медіа», який спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на

забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення [6].

Необхідним, у сфері забезпечення свободи інформації був закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР, який втратив чинність 01 березня 2023 року [7]. Відповідно до цього нормативного акту визначались та розподілялись основні завдання та функції органів влади у процесі інформатизації, а також окреслювались головні пріоритети, що існують у вказаній сфері. На сьогодні діє закон України від 01.12.2022 № 2807-IX «Про Національну програму інформатизації» [8], який визнав нечинним закони України від 13.09.2001 № 2684-III Про внесення змін до закону України «Про Національну програму інформатизації» [9] та вище згаданий закон України № 74/98-ВР.

Крім того, закон України від 01.12.2022 № 2807-IX вніс у ряд нормативних актів зміни, перерахуємо саме ті, що мають відношення до нашого дослідження це: закон України від 16.12.2020 № 1089-IX «Про електронні комунікації» [10] та закон України від 13.09.2001 № 2684-III «Про національну інфраструктуру геопросторових даних» [11]. А також на сьогодні регулює правові відносини, що виникають під час формування та виконання Національної програми інформатизації.

Важливим документом, що позитивно впливає на розвиток свободи інформації в Україні, на нашу думку, є закон України «Про науково-технічну інформацію» від 25.061993 р. № 3322-XII [12]. Цей закон забезпечує право фізичних та юридичних осіб на доступ до науково-технічної інформації, що виражається у її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні. Документ проголосив загальне право на відкриту науково-технічну інформацію, яке передбачає можливість вільного її одержання, зберігання, використання і поширення під час здійснення наукової, науково-дослідної, виробничої, громадської та іншої діяльності, що не забороняється чинним законодавством. До плюсів цього документу також слід віднести встановлення механізму підвищення якості, формування, отримання, поширення, розповсюдження науково-технічної інформації. Тобто, він має не лише декларативний характер, але й надає перелік шляхів практичного втілення проголошених прав.

Нормативним актом, що надавав змогу знайомитися із статистичною інформацією, що перебуває у власності держави є закон України «Про державну статистику» від 17.09.1992 р. № 2614-XII, який втратив чинність 01 січня 2023 року. Але згідно з цим документом кожна особа має право на знеособлену статистичну інформацію: «це право гарантує вільний доступ користувачів до такої статистичної інформації, можливість її використання, поширення та зберігання, з метою реалізації ними своїх завдань та функцій, забезпечення прав, свобод і законних інтересів» [13].

Доступ до архівної інформації, що перебуває у державній та приватній власності також регулюється законом України «Про Національний архівний фонд та архівні установи» від 24.12.1993 № 3814-XII [14]. За допомогою цього нормативного акту фізичним особам надається можливість одержувати та знайомитись із інформацією, що перебуває не лише в державних, але й у приватних архівних фондах.

Також, в Україні впроваджено інститут свободи інформації, шляхом надання можливості отримання інформаційних матеріалів за допомогою державних та приватних бібліотек, відповідно до закону України «Про бібліотеки і бібліотечну справу» від 27.01.1995 № 32/95-ВР користувачі бібліотек мають право: безоплатно користуватися інформацією про склад бібліотечних фондів через довідково-пошуковий апарат (крім

комерційних баз даних); безоплатно отримувати консультаційну допомогу в пошуку та виборі джерел інформації; безоплатно отримувати у тимчасове користування документи із фондів бібліотеки, крім документів, придбаних за кошти, одержані від господарської діяльності бібліотеки; одержувати документи або їх копії по міжбібліотечному абонементу; одержувати інформацію з інших бібліотек, користуючись каналами зв'язку [15].

Таким чином, особам, що перебувають на території України проголошується можливість вільного доступу до статистичної, архівної інформації, а також інформації, що міститься у національних та приватних бібліотеках. З метою надання своїм громадянам можливості доступу до загальнолюдських цінностей на території України діє закон України «Про видавничу справу» від 05.06.1997 № 318/97-ВР, оновлена редакція якого, доречі, запланована на 31.12.2023 року [16].

Наступним блоком спеціального законодавства України, що має велике значення для розвитку свободи інформації в Україні є нормативні акти, що присвячуються регулюванню відносин, пов’язаних із діяльністю окремих видів засобів масової інформації. І хоча більшість з 31 березня 2023 року втратили чинність, слід розуміти, що їх нормативні положення не перестали регулювати відносини з приводу окремих видів інформаційної діяльності, а перейшли у структуру консолідованого законодавчого акту «Про медіа» [6], що об’єднав їх положення в єдину конструкцію, яка передує формуванню майбутнього інформаційного кодексу. Серед таких документів, вважаємо доречним визначити закони України:

- Про друковані засоби масової інформації від 16.11.1992 № 2782-XII [17].
- Про телебачення і радіомовлення від 21.12.1993 № 3759-XII [18].
- Про телебачення та радіомовлення від 21.12.1993 № 3759-XII у Розділі VII захищає права осіб, що сприймають інформацію. Зокрема йдеться про вільний доступ осіб до теле- та радіопередач, що транслюються на території України, підіймається питання щодо неможливості надання споживачам перекрученої, недостовірної інформації [20].
- Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» від 23.09.1997 № 539/97-ВР [19].

А також діючі на сьогодні нормативні акти:

- Про державну підтримку засобів масової інформації та соціальний захист журналістів від 23.09.1997 № 540/97-ВР. Відповідно до ст. 2 якого, свобода слова і вільне вираження у друкованій формі своїх поглядів і переконань … означають право кожного громадянина вільно і незалежно шукати, одержувати, фіксувати, зберігати, використовувати та поширювати будь-яку відкриту за режимом доступу інформацію за допомогою друкованих засобів масової інформації. Також вказаним нормативним актом встановлюються недопущення розповсюдження цензури та «диктовки» інформації, що надається громадянам за допомогою ЗМІ [21].
- Про захист інформації в інформаційно-телекомунікаційних системах від 05.07.1994 № 80/94-ВР. Поширення та обіг інформації відбувається надзвичайно швидко через мережу та є досить комфортним для споживачів інформації. Особливий порядок та вимоги до захисту інформації, що міститься у електронних мережах, на нашу думку слід пов’язувати, перш за все, із її важливістю та легкістю її протиправного отримання внаслідок втручання у структуру мережі. Існування такого нормативного акту створює

базис для виникнення відносин пов'язаних із сучасним рухом інформаційних ресурсів, що є безперечним надбанням на шляху до інформаційного суспільства, а також до побудови свободи інформації [22].

Також, в рамках висвітлення українського законодавства у галузі свободи інформації в інформаційному суспільстві, ми вважаємо доречним звернути увагу на нормативні документи, що певним чином обмежують цей інститут. Серед таких нормативних актів ми виділяємо закони України:

- Про державну таємницю від 21.01.1994 № 3855-XII [23].
- Про захист суспільної моралі від 20.11.2003 № 1296-IV (що хоча і втратив силу 31.03.2023 року, але його положення продовжують свою дію в межах Закону України «Про медіа») [24].
- Про державну таємницю від 21.01.1994 № 3855-XII. За допомогою цього нормативного акту (зокрема у ст. 8) в державі встановлюється чіткий перелік інформаційних ресурсів, що за своїми ознаками слід відносити до державної таємниці, а отже, обмежити чи взагалі заборонити їх вільний обіг [25].
- Про захист суспільної моралі від 20.11.2003 № 1296-IV. Хоча і втратив чинність 31 березня 2023 року містить положення, які необхідні для цивілізованого розвитку свободи інформації, без загального розповсюдження інформаційних матеріалів, що негативно впливають, зокрема, на психіку людини чи її розвиток [26].

На нашу думку, свобода інформації повинна мати певні демократичні стримання, що, з одного боку, запобігають витоку важливої інформації, що має важливе державне значення, а з іншого, запобігають розповсюдженню інформацію, що призводить до руйнації нормальної психіки та свідомості людини.

Таким чином, як можна побачити із вищевказаного, в українському законодавстві існує достатня кількість нормативних актів, які регулюють обіг та використання різноманітних об'єктів інформації, а також суб'єктів, які збирають, отримують, використовують та поширюють їх. Слід вказати, що кожен із переглянутих нормативних актів містить у собі досить чітке визначення об'єкту, що регулюється, а також шляхи та механізми його поширення у загальному суспільному обігу. Позитивним моментом, на нашу думку, слід визнати зазначення мети та завдань окремого закону, що дає змогу споживачам інформації орієнтуватися у великій кількості документів та використовувати саме той, який стосується конкретної ситуації, що склалася.

Література

1. Мультимедійна платформа іномовлення України. Розділ Пропаганда. URL: https://www.ukrinform.ua/tag-propaganda
2. Боротьба з дезінформацією: медіарегулятори України та ще чотирьох країн підписали декларацію. URL: https://www.ukrinform.ua/rubric-society/3769952-borotba-z-dezinformacieu-mediaregulatori-ukraini-ta-se-cotiroh-krain-pidpisali-deklaraciu.html
3. Єврокомісія оприлюднила дані щодо боротьби онлайн-платформ проти дезінформації рф. URL: https://www.ukrinform.ua/rubric-world/3766532-evrokomisia-opriludnila-dani-sodo-borotbi-onlajnplatform-proti-dezinformacii-rf.html
4. Щоденні новини Європейської комісії від 26.09.2023. Брюсель. URL: https://ec.europa.eu/commission/presscorner/detail/en/mex_23_4643

5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 09.01.2007 № 537-V.
URL: https://zakon.rada.gov.ua/laws/show/537-16#Text
6. Про медіа. Закон України від 13.12.2022 № 2849-IX.
URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text
7. Про Національну програму інформатизації. Закон України від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text
8. Про Національну програму інформатизації. Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text
9. Про Національну програму інформатизації. Закон України від 13.09.2001 № 2684-III. URL: https://zakon.rada.gov.ua/laws/show/2684-14#Text
10. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text
11. Про національну інфраструктуру геопросторових даних. Закон України від 13.04.2020 № 554-IX. URL: https://zakon.rada.gov.ua/laws/show/554-20#Text
12. Про науково-технічну інформацію. Закон України від 25.06.1993 № 3322-XII. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
13. Про державну статистику. Закон від 17.09.1992 № 2614-XII. URL: https://zakon.rada.gov.ua/laws/show/2614-12#Text
14. Про Національний архівний фонд та архівні установи». Закон України від 24.12.1993 № 3814-XII. URL: https://zakon.rada.gov.ua/laws/show/3814-12#Text
15. Про бібліотеки і бібліотечну справу. Закон України від 27.01.1995 № 32/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/32/95-%D0%B2%D1%80#Text
16. Про видавничу справу. Закон України від 05.06.1997 № 318/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/318/97-%D0%B2%D1%80#Text
17. Про друковані засоби масової інформації від 16.11.1992 № 2782-XII. URL: https://zakon.rada.gov.ua/laws/show/2782-12#Text
18. Про телебачення і радіомовлення. Закон України від 21.12.1993 № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12#Text
19. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації. Закон України від 23.09.1997 № 539/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80#Text
20. Про телебачення та радіомовлення. Закон України від 21.12.1993 № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12#Text
21. Про державну підтримку засобів масової інформації та соціальний захист журналістів. Закон України 23.09.1997 № 540/97-ВР.
URL: https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text
22. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР.
URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
23. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
24. Про захист суспільної моралі. Закон України від 20.11.2003 № 1296-IV. URL: https://zakon.rada.gov.ua/laws/show/1296-15#Text

25. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
26. Про захист суспільної моралі. Закон України від 20.11.2003 № 1296-IV. URL: https://zakon.rada.gov.ua/laws/show/1296-15#Text

Жмуровська К. Р.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Грищенко Д. О.
старший викладач кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ

РОЛЬ СУЧАСНИХ ТЕХНОЛОГІЙ У РОЗКРИТТІ ТА РОЗСЛІДУВАННІ ЗЛОЧИНІВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ДЛЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У сучасному інформаційному суспільстві, що перебуває під впливом постійних змін та технічного прогресу, роль технологій у галузі правопорядку та правосуддя відіграє важливу та незамінну роль, що особливо актуально для державної поліції України, яка має використовувати сучасні технології для ефективного розкриття та розслідування злочинів.

Зростаюча складність і різноманітність злочинів в сучасному світі створили нагальну необхідність впровадження інноваційних технічних рішень в діяльність правоохоронних органів. Це відкриває нові можливості для Національної поліції використовувати аналітичні інструменти, штучний інтелект та інші передові технології для підвищення ефективності та дієвості у боротьбі зі злочинністю.

Ефективність боротьби зі злочинністю, і перш за все з кримінальними злочинами багато в чому залежить від інформаційного забезпечення правоохоронних органів.[1, с.11]

Інтернет-технології в сучасному світі відіграють важливу роль у розслідуванні злочинів і надають правоохоронним органам важливі інструменти для виявлення, розслідування та припинення злочинної діяльності. Ефективність використання інтернет-технологій в розслідуваннях дозволяє реагувати на сучасні виклики і злочинні схеми, часто з використанням високотехнологічних методів.

Однією з важливих переваг є швидкість отримання та обробки інформації. Інтернет-технології дозволяють отримувати дані в режимі реального часу, аналізувати великі обсяги інформації і швидко реагувати на кримінальні інциденти. Ефективне використання аналітичних інструментів дозволяє виявляти закономірності та зв'язки між різними елементами злочинної діяльності. Декомунізація.

Крім того, інтернет-технології надають можливість проводити відкриті розслідування і взаємодіяти з іншими правоохоронними органами, вітчизняними та зарубіжними партнерами. Це допоможе поліпшити обмін інформацією та координацію заходів по боротьбі з транснаціональною злочинністю.

Але поряд із позитивними аспектами використання інтернет-технологій виникають такі проблеми, як захист від кібератак, конфіденційність громадян та етичні аспекти використання цих технологій. Тому необхідно розробити та вдосконалити правові та технічні механізми для забезпечення ефективного та відповідального використання інтернет-технологій у дослідженнях.

Кібербезпека є важливим аспектом сучасних правоохоронних органів при роботі з електронними доказами, оскільки злочинці здійснюють все більше і більше злочинів і використовують цифрові технології, щоб приховати свої сліди. Забезпечення безпеки електронних доказів вимагає комплексного підходу і постійного вдосконалення технічних і організаційних заходів.

Одним із ключових питань у цьому контексті є захист електронних доказів від несанкціонованого доступу та змін. Використання сучасних засобів кібер-залякування, таких як шифрування та автентифікація, є важливим для забезпечення конфіденційності та цілісності цифрової інформації. Ефективне реагування на кібератаки та виявлення можливих порушень безпеки також є важливими міркуваннями. Розробка та впровадження систем спостереження, аналізу вразливостей та сучасних методів виявлення інцидентів є важливою частиною стратегії кібербезпеки в області обробки електронних доказів.

Паралельно з технічними заходами необхідно приділяти увагу правовим і етичним питанням, зокрема визначенню прав і обов'язків учасників процесу, беручи до уваги конфіденційність громадян і введення стандартів безпеки при обробці електронних доказів. У все більш цифровому суспільстві забезпечення кібербезпеки при роботі з електронними доказами має вирішальне значення для підтримки довіри до правосуддя і верховенства закону в епоху цифрових технологій.

Спрощення роботи поліції за рахунок використання технологій стало важливою передумовою для підвищення ефективності та результативності діяльності правоохоронних органів. Сучасні технології можуть значно спростити роботу поліції, надаючи інноваційні інструменти для виявлення, розслідування та запобігання злочинам.

Ключовим аспектом є використання аналітичних систем, які обробляють великі обсяги даних і допомагають виявляти закономірності злочинної діяльності. Це дозволяє швидко реагувати на правопорушення та ефективно взаємодіяти з іншими правоохоронними органами. Технологія також спрощує спілкування всередині поліції і з іншими службами, що дозволяє швидко обмінюватися інформацією і координувати заходи безпеки. Впровадження цифрових інструментів полегшує швидке розгортання поліцейських ресурсів у відповідь на виклики і забезпечує високий рівень реагування на непередбачені обставини.[2]

Крім того, технологія дозволяє автоматизувати повсякденні процеси, такі як обробка документів і складання звітів, що дозволяє поліції заощадити час для підготовки до більш важливих завдань, пов'язаних з громадською безпекою. Спрощення роботи поліції за рахунок впровадження технологій є ключовим фактором у вдосконаленні правоохоронних систем і створенні більш безпечного суспільства.

Сучасні технології відіграють важливу роль у виявленні та розслідуванні злочинів, створюють нові можливості для Національної поліції України, але в той же час створюють проблеми, що вимагають уважного і компетентного підходу. Спостереження за динамікою технологічного розвитку показує, що впровадження штучного інтелекту, аналітичних систем та інших інноваційних рішень може значно спростити і прискорити процес виявлення злочинів. Але поряд з цим існують проблеми, пов'язані з кібербезпекою, захистом конфіденційності та етичними питаннями.

Таким чином, вивчення і вирішення цих аспектів дозволить Національній поліції України ефективно використовувати можливості сучасних технологій для підтримки правопорядку і забезпечення безпеки громадян в епоху цифрових технологій.

Література

1. Застосування інформаційних технологій у діяльності правоохоронних органів URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/cff3ee6a-12d1-4da1-8ec8-cd1c15f3a36f/content
2. Сучасні технології допомагають правоохоронцям у роботі URL: https://securitypolice.com.ua/novyny2/suchasni-tekhnologiji-dopomagayut-pravookhorontsyam-u-roboti

Зачек О. І.

т.в.о. завідувача кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Йосифович Д. І.

заступник директора ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Зараз спостерігається досить значна інтеграція інформаційних технологій у діяльність правоохоронних органів. Застосування штучного інтелекту (ШІ), як напряму інформаційних технологій, в правоохоронній діяльності є доволі важливим та актуальним аспектом для України. ШІ може бути використаний для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки. Наприклад, використання ШІ може допомогти правоохоронним органам відстежувати правопорушників та злочинні групи, визначати їх місцезнаходження, аналізувати відео- та аудіозаписи, шукати співвідношення між різними злочинами та правопорушниками тощо. ШІ може використовуватись також для аналізу текстової та мовної інформації у процесі профілактичних заходів, проведені гласних чи негласних слідчих дій. Наприклад, за допомогою аналізу мовної інформації ШІ може виявляти ключові слова та зв'язки між повідомленнями, що дає можливість виявити можливі загрози та, безпосередньо, самих правопорушників; за допомогою програм розпізнавання облич можна ідентифікувати осіб, правопорушення яких були зафіксовані засобами фото та відеоспостереження [1].

Інтелектуальні системи безпеки, які використовують системи відеоспостереження на основі відеокамер з ШІ, дозволяють попереджати злочини та терористичні атаки, внаслідок чого рівень злочинності в середньому може значно знижуватись [2, с. 83].

У міжнародній практиці є чимало прикладів успішного використання ШІ в правоохоронній діяльності. Так, наприклад, у США FBI використовує ШІ для розпізнавання правопорушників на відео з камер спостереження в режимі реального часу. За допомогою ШІ агенти FBI можуть аналізувати великі обсяги даних, щоб виявляти правопорушників та спрогнозувати місце та час наступного злочину. У Великобританії поліція використовує ШІ для аналізу соціальних мереж та інших відкритих джерел інформації, щоб виявляти можливі загрози національній безпеці. А у Німеччині поліція використовує ШІ для виявлення злочинів, пов'язаних з фінансовими операціями, оскільки аналітичні системи ШІ спроможні автоматично аналізувати великі обсяги фінансової інформації та виявляти можливі ознаки фінансових злочинів, таких як відмивання грошей, корупція та шахрайство.

ШІ також може використовуватись для автоматизації процесів збору та оброблення доказів у межах кримінальних проваджень. Наприклад, системи ШІ здатні автоматично сканувати та аналізувати великі обсяги текстової інформації, що допомагає розглядати справи швидше та ефективніше.

Одним з найдосконаліших ШІ на сьогоднішній день є ChatGPT (Generative Pre-trained Transformer), який може бути використаний у боротьбі із злочинністю на різних рівнях та у різних контекстах. Ось, наприклад, кілька можливих способів використання ChatGPT для боротьби зі злочинністю:

1. ChatGPT може аналізувати текст, фотографії та відео, що публікуються на сторінках злочинців у соцмережах, та шукати ознаки злочинної діяльності.
2. ШІ може розпізнавати ключові слова та вирази у текстових повідомленнях, що вказують на злочинну діяльність, такі, як наркотики, зброя, планування злочину тощо.
3. Програма здатна розпізнавати обличчя правопорушників, автомобілі, номерні знаки та інші ознаки у відео та фото з камер спостереження, які можуть допомогти в ідентифікації правопорушників.
4. ChatGPT може бути використаний для аналізу даних щодо злочинності та видачі рекомендацій стосовно превентивних заходів.

Разом з тим, ChatGPT приносить як користь, так і шкоду: злочинці легко обходять вбудований розробниками захист – наприклад, заборону на створення шкідливого коду. Для цього вони просто розбивають завдання на кілька частин, щоб запити виглядали нейтральними. А потім за інструкціями від самого ж штучного інтелекту збирають їх в одну програму. Навіть ті, хто нічого не тямлять у програмуванні, створюють віруси під свої потреби, використовуючи ChatGPT як інструктора.

Ще одна популярна ніша незаконного використання нейромережі – соціальна інженерія. ChatGPT здатний без зусиль написати переконливий текст для фішингового сайту або листування, без помилок і з такими деталями, які введуть в оману користувача. Він може вести діалоги та переконувати людей у своїй правоті, створювати привабливі пропозиції для розсилок і наслідувати конкретну манеру спілкування, щоб видати себе за реально існуючу людину.

Наступний спосіб застосування ChatGPT – можливість безпосередньо запитати його, як скоїти злочин з найбільшою вигодою, дізнатися про нові афери, схеми обману, отримати статистику щодо скоєних злочинів, щоб не конкурувати з іншими злочинцями, а також отримати розуміння, які помилки роблять інші шахраї, на чому їх ловить поліція і як цього уникнути. Таким чином, нейромережа перетворилася на інструмент, який приносить як користь, так і шкоду [4].

Велику користь у діяльності правоохоронних органів може принести технологія розпізнавання облич на основі ШІ Clearview AI, яка дозволяє співставляти світлину особи з фотографіями, що розміщені у мережі Інтернет, зокрема в соціальних мережах [3]. Clearview AI має 3100 активних користувачів у щонайменше 600 правоохоронних органах [4]. Після початку повномасштабної війни росії проти України, компанія Clearview AI надала свою технологію Україні вз метою захисту від російського вторгнення. Спочатку ця технологія була надана Міністерству оборони України, а потім багато інших відомств, включаючи Національну поліцію України, приєдналися до проекту [5].

ШІ також може бути корисним для підвищення ефективності збору та якості аналізу інформації з відкритих джерел, оскільки з його допомогою можна швидко зібрати та проаналізувати велику кількість даних з різних джерел в Інтернеті, таких як соціальні мережі, сайти, блоги, форуми та інші. ШІ може також використовуватись для автоматичного визначення ступеня довіри до джерела інформації. Оскільки ШІ може аналізувати великі обсяги інформації за короткий час, це дозволяє забезпечити точніші

та детальніші результати аналізу, що може мати важливе значення в підвищенні ефективності правоохоронної діяльності.

На основі сказаного, можна стверджувати, що ШІ здатен: сприяти підвищенню ефективності розслідувань; знизити кількість помилок та зайвих витрат часу і зусиль; надати допомогу у аналізі великих обсягів інформації і, як наслідок, виявляти можливі зв'язки між різними фактами, що можуть мати ключове значення для розслідування злочинів.

Україна має потенціал для використання ШІ в правоохоронній діяльності, але поки що цей напрямок не повністю реалізований. На даний момент, в Україні застосовуються деякі методи ШІ, але вони не масштабні та не використовуються у повному обсязі.

Проте, в Україні виконується ряд заходів, щоб забезпечити розвиток застосування ШІ в діяльності правоохоронних органів. Зокрема, Національна поліція України вже використовує деякі системи ШІ, наприклад, системи розпізнавання обличчя, які допомагають виявляти правопорушників швидше та ефективніше, попереджувати терористичні акти та інші злочини, а також виявляти злочинців, які перебувають у розшуку. Крім того, діюча система автоматичного розпізнавання номерних знаків автомобілів дозволяє швидко ідентифікувати транспортні засоби, які були задіяні в правопорушеннях.

Україна активно працює над розвитком інноваційного сектора, підтримкою підприємництва та стартапів, впровадженням цифрових технологій у сфери освіти, охорони здоров'я, енергетики та інших галузей діяльності. Метою цих зусиль є створення конкурентоспроможної, інноваційної та цифрової економіки в Україні, яка дозволить підвищити якість життя населення та забезпечити сталий розвиток країни в цілому.

Адвокат Анастасія Клян підкреслює, що правове визначення та регулювання застосування ШІ в українському законодавстві відсутні і відповідальність за неправомірне використання ШІ на даний час нормативно не закріплена [6].

Базовим нормативним документом щодо використання ШІ в Україні є Концепція розвитку штучного інтелекту в Україні, схвалена Розпорядженням Кабінету міністрів України у 2020 р. [7]. Однією із проблем, що потребують розв'язання, згідно цієї Концепції, є відсутність або недосконалість правового регулювання ШІ.

На думку К.С. Токарєвої українські правові акти не регламентують діяльності ШІ, тому планується співпраця з міжнародними організаціями щодо розроблення стандартів та Етичного кодексу використання ШІ в Україні [8, с. 149, 151].

Бортник С.М. вважає, що ШІ у діяльності правоохоронних органів України використовується недостатньо внаслідок складної фінансової ситуації та недостатнього правового регулювання [9].

З метою створення базовоголення законодавства у сфері використання систем ШІ в Україні Національна асоціація адвокатів України створила Робочу групу, яку очолив заступник Голови Ради адвокатів України Валентин Гвоздій [10].

Законодавство, що регулює використання ШІ, у інших країнах світу також не прийняте. Європейська Комісія запропонувала регламент щодо регулювання використання ШІ Artificial Intelligence Act, і 6 грудня 2022 року Рада ЄС ухвалила спільну позицію щодо цього регламенту. Але законом він стане лише після узгодження спільної версії тексту закону Радою ЄС та Європарламентом. У Канаді розробляється Закон про штучний інтелект і дані – Artificial Intelligence and Data Act (AIDA). Також на стадії розроблення подібні законодавчі акти є у США, Бразилії та інших країнах [11].

Найбільш значною проблемою є відсутність нормативно-правового регулювання застосування ШІ в Україні, і зокрема, у правоохоронній діяльності. Тому, важливе значення має прийняття нормативно-правових актів, які регламентують використання

ШІ в правоохоронній діяльності. Це є непростим завданням, зважаючи на відсутність прийнятих законів в цій галузі навіть у інших країнах.

Пропонуємо ввести зміни до Статті 25 «Повноваження поліції у сфері інформаційно-аналітичного забезпечення» Закону України «Про Національну поліцію» [12], а саме, додати пункт 6 частини 2 «Поліція в рамках інформаційно-аналітичної діяльності:» у редакції: «Для збору, обробки та аналізу інформації може застосовувати засоби штучного інтелекту».

Також вважаємо за необхідне додати до переліку прав підрозділів, які здійснюють оперативно-розшукову діяльність, право на використання ШІ та інших сучасних технологій в процесі здійснення оперативно-розшукових заходів. Для цього пропонуємо ввести зміни до Статті 8 «Права підрозділів, які здійснюють оперативно-розшукову діяльність» Закону України «Про оперативно-розшукову діяльність» [13], а саме, додати пункт 22 частини першої у редакції: «Застосовувати засоби штучного інтелекту для отримання, обробки, перевірки та аналізу оперативної інформації» [1].

Література

1. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. № 3 (2023). Львів: ЛьвДУВС, 2023. С. 148-156.
2. Бугера О.І. Використання штучного інтелекту для запобігання злочинності // Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 32 (71). № 6. 2021. С. 82-86.
   URL: https://www.juris.vernadskyjournals.in.ua/journals/2021/6_2021/15.pdf
3. 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
4. Kashmir Hill. What We Learned About Clearview AI and Its Secret ‘Co-Founder’ // NY Times. March 18, 2021. URL: https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html
5. Війна в Україні. URL: https://www.clearview.ai/ukraine
6. Клян Анастасія. Правове регулювання штучного інтелекту в Україні та світі // GOLAW. 03.02.2022. URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/
7. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
8. Токарєва К.С., Савліва Н.О. Особливості правового регулювання штучного інтелекту в Україні // Юридичний вісник. 2021. № 3 (60). С. 148-153. URL: https://jrnl.nau.edu.ua/index.php/UV/article/view/15967/23255&ved=2ahUKEwigrav1n7j-AhXthv0HHTTeDv84ChAWegQIBBAC&usg=AOvVaw28DCqkdlvGIOj_-Ug9thXv
9. Бортник С.М. Особливості регулювання використання штучного інтелекту у правоохоронної системі // Застосування інформаційних технологій у діяльності правоохоронних органів: матеріали круглого столу (м. Харків, 14 грудня 2021 р.) / МВС України, Харк. нац. ун-т внутр. справ., Каф. кібербезпеки та DATA-технологій. Харків: ХНУВС, 2021. С. 28-31.

10. Гришанова Надія. Правове регулювання штучного інтелекту: у НААУ створено Робочу групу // ЛІГА:ЗАКОН. 09.03.2023. URL: https://jurliga.ligazakon.net/news/218005_pravove-regulyuvannya-shtuchnogo-ntelektu-u-naau-stvoreno-robochu-grupu
11. Котков Ігор. AI Act: що ЄС думає про штучний інтелект // Legal IT Group. 31.01.2023. URL: https://legalitgroup.com/ai-act-shho-yes-dumaye-pro-shtuchnij-intelekt/
12. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
13. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. URL:https://zakon.rada.gov.ua/laws/show/2135-12#Text

Здебський Д. В.
аспірант Одеського державного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ВІЙСЬКОВОСЛУЖБОВЦІВ СУБ'ЄКТІВ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ

Практика проведення поліграфологічних досліджень в Україні набула особливу актуальність під час військової агресії росії проти України, метою проведення яких є виявлення зрадників, шпигунів і диверсантів серед військовослужбовців. А отже питання збереження та захисту персональних даних суб'єктів опитування із застосуванням поліграфа, що мають статус військовослужбовців, в умовах сьогодення, є на часі, підлягає обговоренню, додатковому дослідження та чіткого нормативного врегулюванню.

Ратифікована Україною у 2010 році Конвенція Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї [9], є основним міжнародним документом у сфері обігу особистої інформації для забезпечення дотримання прав і свобод людини, які визначили необхідність дотримання прав і свобод кожної особи, незалежно від її громадянства чи місця проживання, у зв’язку з автоматизованою обробкою персональних даних. Стаття 5 Конвенції передбачає, що персональні дані, які підлягають автоматизованій обробці, повинні зберігатися у формі, яка дозволяє ідентифікувати суб’єктів даних не довше, ніж це потрібно для цілей, для яких вони потрібні. З метою імплементації Конвенції Верховною Радою України було прийнято Закон України «Про захист персональних даних» [8], який закріпив основні принципи та положення обробки персональних даних, права суб’єктів персональних даних та підстави обробки персональних даних.

Аналізуючи нормативні акти про захист персональних даних та накази з організації і проведення поліграфологічних перевірок, можна виділити наступні документи в питаннях захисту персональних даних військовослужбовців:

1. Інструкція з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України (МОУ) та Збройних Силах України (ЗСУ) [2];
2. Інструкція про порядок організації та проведення опитування особового складу Національної гвардії України (НГУ) з використанням поліграфа [5];
3. Інструкція з організації та проведення опитування із застосуванням поліграфа в Державній прикордонній службі України (ДПСУ) [1];
4. Порядок проведення психофізіологічного дослідження із застосуванням поліграфа в Управлінні державної охорони України (УДО) [7];

5. Служба безпеки України (СБУ) та Служба зовнішньої розвідки України (СЗР) керівні документи, що визначають порядок організації та проведення опитування із застосуванням поліграфа у відомствах не мають. Проте Інструкція про порядок проведення службових розслідувань та службових перевірок стосовно військово-службовців СБУ зазначає, що опитування особи, за її згодою, може проводитись з використанням поліграфа відповідно до законодавства [4]. Відповідно до Положення про проходження військової служби військовослужбовцями СЗР зазначено, що: ...на військову службу за контрактом до Служби зовнішньої розвідки України приймаються та призначаються на посади громадяни України, які пройшли також психофізіологічне дослідження із застосуванням технічних засобів фіксації реакцій людини [6].

Власником персональних даних є фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [8]. Під дану категорію підпадають ініціатори поліграфологічної перевірки. Розпорядником персональних даних до Закону є фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця [8]. В дану категорію входять спеціалісти поліграфа та підрозділи де вони проходять службу.

До матеріалів поліграфологічного дослідження відносять: завдання де зазначено ПІБ суб'єкта, заява про надання добровільної згоди на проведення психофізіологічної перевірки, а також письмова довідка за отриманими результатами. Відповідно, у даних матеріалах вже містяться персональні дані суб'єктів опитування (дослідження) із застосуванням поліграфа [1; 2; 5; 7]. У СЗР такими матеріалами є письмові висновки з питань службового розслідування, які долучаються до матеріалів службового розслідування [3]. За результатами поліграфологічної перевірки готується довідка, де зазначаються як персональні дані загального характеру, так і чутливі дані, наприклад про стан здоров'я.

За інструкціями МОУ ЗСУ, НГУ й ДПСУ інформація, що викладена у довідках і матеріалах дослідження не має перевищувати грифа обмеження доступу «Для службового користування». Матеріали дослідження зберігаються у визначених структурних підрозділах протягом трьох років, після чого знищуються в установленому порядку. Відпрацьовані довідки, за результатами поліграфологічного дослідження, реєструються у журналах обліку проведення психофізіологічних досліджень із застосуванням поліграфа, які ведуться у структурних підрозділах [1; 2; 5]. Дана вимога інструкцій дотична до визначення Закону щодо бази персональних даних, котра є іменованою сукупністю упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних. Зауважимо, що довідки складаються в письмовій формі, й відповідно зберігаються у картотеках.

Інструкції МОУ ЗСУ, НГУ й ДПСУ не визначають порядок ведення електронних баз даних результатів поліграфологічних досліджень, відсутність прямої вказівки на ведення електронних баз зазначених даних унеможливлює законну обробку отриманих результатів у електронному вигляді. Однак, дану прогалину було враховано в Порядку УДО [7]. Відповідно до Порядку, матеріали дослідження, що утворилися в результаті дослідження в електронному вигляді, зберігаються на електронних носіях інформації. В залежності від виду інформації з обмеженим доступом електронні носії інформації реєструються в журналі обліку електронних носіїв інформації, на які планується записувати службову інформацію за встановленою формою [7].

В переважній більшості керівних документів, що визначають процедуру поліграфологічної перевірки в військових формуваннях України відсутня норма, яка регламентує порядок ведення та обробки персональних даних в електронному вигляді. В умовах цифровізації відомств ведення електронних баз поліграфологічних перевірок

розпорядники та власники даної інформації в свою чергу можуть порушуватись права на захист персональних даних суб'єктів поліграфологічних досліджень. Крім того, відсутність даної норми унеможливлює використання електронних бази даних поліграфологічних перевірок у законний спосіб підрозділами внутрішньої та власної безпеки в ході проведення кримінального аналізу.

Таким чином, за результатом аналізу нормативних актів у сфері захисту персональних даних та організації і проведення поліграфологічних перевірок у військових формуваннях України ми прийшли до висновку, що:

1. В Інструкціях МОУ ЗСУ, НГУ й ДПСУ, що визначають порядок організації та проведення поліграфологічних досліджень, обробка інформації в електронному вигляді, що утворилися в результаті поліграфологічної перевірки, не передбачена. Дана прогалина, в разі здійснення такої обробки, по-перше порушує права на захист персональних даних суб'єктів перевірки із застосуванням поліграфа. По-друге, стримує процес цифровізації відомств. По-третє, унеможливлює в законний спосіб обробляти матеріали поліграфологічних перевірок підрозділами внутрішньої та власної безпеки зазначених військових формувань в ході проведення кримінального аналізу;
2. В СБУ та СЗР відсутні керівні документи які визначають порядок організації та проведення поліграфологічних досліджень, що може порушувати права на обробку та захист персональних даних персоналу, які надали згоду на опитування із застосуванням поліграфа.

Враховуючи викладене рекомендуємо:

1. Внести зміни до діючих відомчих наказів МОУ ЗСУ, НГУ й ДПСУ, що визначають порядок та організацію поліграфологічних перевірок, щодо допустимості обробки отриманих матеріалів для забезпечення дотримання прав і свобод персоналу та розвитку цифровізації відомств;
2. В СБУ та СЗР України врегулювати порядок та організацію проведення поліграфологічних перевірок, з врахуванням захисту персональних даних військовослужбовців, що отримано за результатами проведення поліграфологічних перевірок та підлягають обробці в електронному вигляді.

Література

1. Інструкція з організації та проведення опитування із застосуванням поліграфа в Державній прикордонній службі України Затв. Нак. МВС України 19 квіт. 2022 року № 221 Зареєстровано в Міністерстві юстиції України 21 квітня 2022 р. за № 440/37776. URL: https://zakon.rada.gov.ua/laws/show/z0440-22#TextText
2. Інструкція з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України та Збройних Силах України : затв. Нак. м-ва об. України від 14.04.2015 № 164 (у редакції від 22 лип. 2019 ро. № 394). URL: https://zakon.rada.gov.ua/laws/show/z0477-15#Text
3. Інструкція про порядок проведення службового розслідування у Службі зовнішньої розвідки України : затв. Нак. СЗР України від 26 лют. 2013 р. № 326/22858. веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/z0326-13#Text
4. Інструкція про порядок проведення службових розслідувань та службових перевірок стосовно військовослужбовців Служби безпеки України затв. Нак. СБУ від 04 лют. 2016 р. № 45. URL: https://zakon.rada.gov.ua/laws/show/z0328-16#Text

5. Інструкція про порядок організації та проведення опитування особового складу Національної гвардії України з використанням поліграфа. Затв. Нак. 01 вер. 2017 р. № 749. URL: https://zakon.rada.gov.ua/laws/show/z1169-17#Text
6. Положення про проходження військової служби військовослужбовцями Служби зовнішньої розвідки України: затв. Ук. През. України від 30 гр. 2021 р. № 690/2021. URL: https://zakon.rada.gov.ua/laws/show/690/2021#Text
7. Порядок проведення психофізіологічного дослідження із застосуванням поліграфа в Управлінні державної охорони України: затв. Нак УДО від 09 лют. 2021 р. № 95. URL: https://zakon.rada.gov.ua/laws/show/z0335-21#Text
8. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
9. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 лип. 2010 р. № 2438-VI. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
10. Ismailov, K. To the issue of personal information circulation in the national police databases. Fundamental and applied researches in practice of leading scientific schools, 38 (2). Canada, 2020. P. 41-45.

Кащевський В. О.
аспірант Львівського університету бізнесу та права
Гранківська С. Р.
здобувач вищої освіти Львівського державного університету внутрішніх справ
Огірко О. І.
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ В ПРАВООХОРОННИХ ОРГАНАХ: ПРОБЛЕМИ ВПРОВАДЖЕННЯ, ПЕРЕВАГИ ТА ПЕРСПЕКТИВИ

Сьогодні в Україні стрімко впроваджуються інформаційні технології у всі сфери державного управління та правоохоронну діяльність. Розроблені різноманітні інформаційні системи: прийняття рішень, інформаційно-пошукові, електронного документообігу, які забезпечують швидкий доступ до інформації, та багато в чому полегшують і підвищують ефективність роботи, оптимізують діяльність організацій та державних установ.

Використання системи електронного документообігу в сферах державного управління, правотворчої, правозахисної та правоохоронної діяльності забезпечує швидкий доступ до інформації, а відтак оптимізує діяльність тієї чи іншої інституції сприяє зміцненню правової системи держави, захисту прав і основних свобод людини.

За даними ООН Україна щороку підіймається у загальносвітовому рейтингу, щодо впровадження електронного документообігу на підприємствах та органах державної влади. Таку у 2014 році вона посідала 87 місце, у 2020 році — 69 місце, а у 2022 році — 46 місце в світі за розвиток електронного документообігу в органах державної влади за індексом EGDI (рис.1).

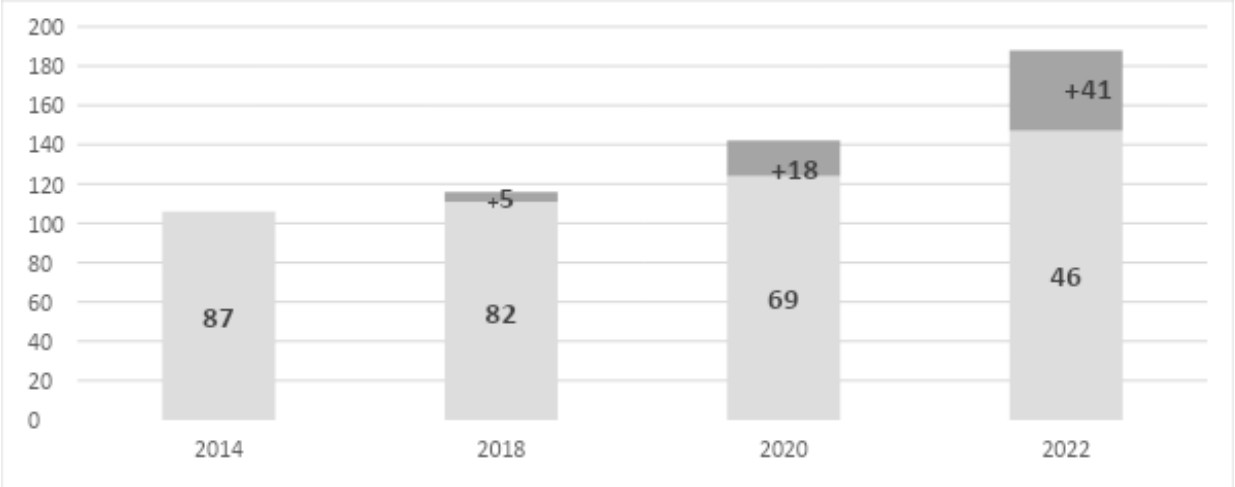

Рис. 1. Місце України у світовому рейтингу щодо впровадження електронного документообігу в органах державної влади (серед 193 країн) складено за даними [1]

Електронний документообіг в правоохоронних органах це автоматизована система, яка призначена для документального забезпечення процесів управління та автоматизації діловодства та документообігу.

У підпорядкуванні Міністерства внутрішніх справ користувачами СЕД є (рис 2.)

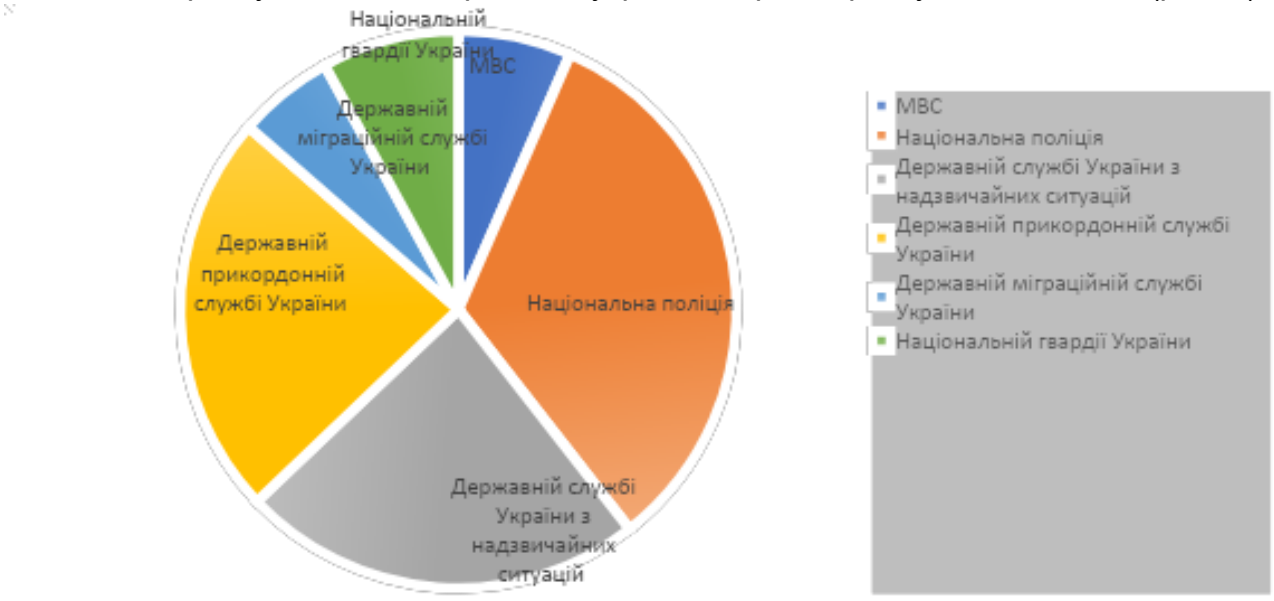

Рис. 2. Користувачі системи електронного документообігу в системі МВС складено за даними [5]

- Національна поліція України
- Державна служба України з надзвичайних ситуацій
- Державна прикордонна служба України
- Державна міграційна служба України;
- Національна гвардія України

В правоохоронних органах електронній документообіг впроваджується для вирішення та покращення комплексу завдань, зокрема [1, 4, 5]:

- Документообігу, основні функції, якого полягають у реєстрації вхідної/ вихідної документації, введення шаблонів резолюцій, обмін відповідними

документами в системі МВС та з органами виконавчої влади, складанні інформаційних документів для висвітлення на WEB-сайтах.

- Опрацюванні запитів і звернень громадян, народних депутатів України, а також реєстрації та опрацювання адвокатських запитів та запитів на публічну інформацію.
- Підготовки документів (положень, наказів, аналітичних довідок).
- Формуванні резолюцій, накладанні шаблонів резолюцій;
- Маршрутизації, тобто шляху проходження документу згідно схеми. Обов'язково повинно бути встановлено блок для підтримки паралельних та послідовних маршрутів, запису історії маршруту документів, переадресації ділової інформації на різні етапи опрацювання.
- Системи оповіщення, яка повинна передбачати автоматичне розсилання повідомлень через електронну почту або системне вікно у відповідність до термінів передбачених в документах, формувати реєстри оповіщення, відображати перелік завдань виконавця.
- Створення та робота електронного архіву передбачає автоматизація процесів архівного зберігання паперових та електронних документів, заборону, захист внесення змін у архівних електронних документах, здійснення пошуку документів за реквізитами, змістом тексту та іншими критеріями.
- Роботи зі звітністю, а саме ведення шаблонів звітів, формування звітів по шаблонах.
- Створення довідників, класифікаторів та безпосередня робота з ними.
- Адміністрування та безпеки.

Для впровадження електронного документообігу в правоохоронні органи система повинна відповідати вимогам: надавати технічні та ліцензійні умови для одночасної кількості користувачів системи більше 110000 осіб; проводити автентифікацію користувачів системи; містити можливість підписання документів із використанням електронного цифрового підпису; працювати на мобільних пристроях під операційними системами Android, iOS або Windows в режимах інформування та перегляду інформації; проводити автоматичне архівування баз даних, електронних документів; забезпечувати завантаження інформації до бази даних як з паперових (сканування та друк штрих-коду), так і з електронних носіїв інформації чи з використанням каналів електронної пошти; мати високу надійність роботи центрального серверу, захист електроживлення та підтримки роботи в мережі [5].

Таким чином, використання систем електронного документообігу у правоохоронних органах сприяє взаємодії з громадянами, підприємствами, державними органами управління, дозволяє значно скоротити час і ресурси, поліпшити процес пошуку та отримання інформації від державних установ, розширити канали взаємодії між державними органами влади.

Сучасні системи документообігу функціонують на використанні новітніх інформаційних технологій створення, поширення, використання і архівування документів. Електронний документообіг, який є основою електронного управління та адміністрування має великі переваги і можливості у порівнянні з паперовим документообігом. Але на відміну від паперових документів, електронний документ більш вразливий до зовнішніх атак спрямованих на конфіденційність, цілісність і зміну інформації, яка знаходиться в ньому. Тому в процесі запровадження електронного документообігу в системи управління необхідно розробляти і системи захисту електронних документів.

Література

1. Закон України «Про електронні документи та електронний документообіг», від 22.05.2003 № 851-IV. Відомості Верховної Ради України. 2003. № 36. С. 275 URL: https://https://zakon.rada.gov.ua/laws/show/851-15#Text
2. Електронний документообіг, тенденції та перспективи [Електронний ресурс] / М. Б. Величкевич, Н. В. Мітрофан, Н. Е. Кунанець // Вісник Національного університету «Львівська політехніка». № 689. Інформаційні системи та мережі : Збірник наукових праць / відповід. ред. В. В. Пасічник. – Львів : НУ «Львівська політехніка», 2010. – С. 44-53
3. UN E-Government Knowledgebase. Country Data. URL: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine/dataYear/2022
4. Вдовіна О. О. Використання електронного документообігу в системі судочинства України. Вісник ХДАК. 2015. Вип. 46. С. 82-91.
5. Вимоги до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України (Шифр – СЕД системи МВС). URL: https://mvs.gov.ua/upload/file/vimogi_do_sed_sistemi_mvs_363.pdf.

Ковалів М. В.

завідувач кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

Партика А. Ю.

здобувач вищої освіти Інституту права Львівського державного університету внутрішніх справ

ІНТЕРНЕТ-ПРАВОВІДНОСИНИ: ВИНИКНЕННЯ, ЗМІНИ ТА ПРИПИНЕННЯ

Поняття правові відносини виступає одним з найбільш затребуваних в юридичній науці, є вихідним пунктом і об’єднуючими засади характеристики права у процесі реалізації його потенціалу. Розвиток суспільства ініціював появу нового виду правових відносин – відносин у мережі Інтернет.

Правовідносини можна визначити, як суспільні відносини, врегульовані правом, учасники якого виступають носіями прав і обов’язків. Взявши за основу загально-теоретичних дефініцію правовідносин, розглянемо категорію Інтернет-правовідносин. Інтернет-правовідносини виникають, змінюються та припиняються при наявності певних передумов, серед яких можна виділити загальні та спеціальні. Спільними передумовами виникнення Інтернет-правовідносин є: наявність інтересу у користувачів Інтернету, під впливом яких вони вступають у відповідні правовідносини у віртуальному просторі і обумовлюють об’єктивну необхідність правового регулювання Інтернет-відносин; наявність суб’єктів Інтернет-правовідносин; наявність об’єкта правовідносин, з приводу якого особи вступають в Інтернет-правовідносини.

До спеціальних передумов виникнення Інтернет-правовідносин можна віднести: наявність норм кримінального, цивільного, адміністративного і іншого права, які поширюють дію на суб’єктів правовідносин в Інтернеті; суб’єкти Інтернет-правовідносин

мають правоздатність і дієздатність; наявність певних обставин, тобто юридичного факту, у межах якого між суб'єктами виникають, змінюються або припиняються Інтернет-відносини [1, с. 1002].

У реальному світі люди вступають у правовідносини у результаті виникнення певного інтересу, дії в Інтернеті залежать від бажань користувачів. Інтерес виступає як первинний елемент будь-яких правовідносин, від якого в подальшому буде залежати об'єкт і суб'єкт правовідносин.

Суб'єктами правовідносин у загальній теорії права виступають окремі фізичні і юридичні особи, які на підставі юридичних норм можуть бути учасниками правовідносин, носіями суб'єктивних прав і обов'язків. Що стосується Інтернет-правовідносин, то в науковій літературі немає єдиної думки щодо їх складу. У науковій літературі виділяють три групи суб'єктів: творці програмно-технічної частини інформаційної структури мережі Інтернет – розробники мереж, засобів зв'язку, телекомунікацій, програмних засобів; суб'єкти, які виробляють і поширюють інформацію у мережі Інтернет, власники інформаційних ресурсів, інформаційних продуктів, власники інформаційних систем і засобів забезпечення, які надають послуги з доступу до мережевих ресурсів; споживачі інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг: фізичні і юридичні особи, які підключаються до мережі для отримання інформації та використання у власній діяльності.

Крім наведеної класифікації, виділяють провайдера, юридичну особу, у якої є ліцензія на надання послуг в Інтернеті та користувача віртуального простору, який звертається до Інтернету у власних інтересах.

Є. Харитонов і О. Харитонова виділяє наступних суб'єктів Інтернет-відносин: оператори зв'язку, постачальники послуг доступу до Інтернету, постачальники інформації, користувачі [2, с. 35].

На наш погляд, наведені класифікації охоплюють повною мірою всіх суб'єктів Інтернет-правовідносин. Водночас оскільки управління ними включає участь різних сторін, які мають експертні знання з наукової та технічної сторін, у тому числі міжнародні організації.

Загальносвітова громадська організація Internet Society ввела термін «екосистема Інтернету», під яким розуміють організації та спільноти, які допомагають Інтернету працювати та розвиватися, серед яких: технологи, архітектори, інженери, винахідники, організації, які здійснюють загальну координацію і допомагають впроваджувати відкриті стандарти; глобальні та місцеві організації, які управляють ресурсами, що забезпечують можливості глобальної адресації, наприклад, (ICANN), реєстри та реєстратори доменних імен; оператори, інженери та постачальники, які забезпечують послуги мережевої інфраструктури, такі як служба іменування доменів, мережеві оператори та точки обміну трафіком; користувачі Інтернету, які використовують Інтернет для обміну інформацією один з одним, а також для надання послуг; освітні заклади, які навчають і створюють ресурси для розробки та використання Інтернет-технологій. Кожен з перелічених учасників Інтернет-відносин займає певну нішу, є володарем або носієм певних прав і обов'язків в Інтернеті.

Подібний перелік учасників Інтернет-правовідносин, що враховує інтереси, пріоритети та можливості зацікавлених сторін у галузі вирішення питань управління Інтернетом, знайшов відображення в статті 49 Декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті», визначальну роль для основних сторін: держави – політичні повноваження по зв'язаних з Інтернетом і питань державної політики (включаючи міжнародні аспекти); приватний сектор – розвиток Інтернету в технічній і в економічній сфері; громадянське суспільство – важлива роль в відносяться до Інтернету питаннях, особливо на рівні населення;

міжурядові організації – координація пов’язаних з Інтернетом питань державної політики; міжнародні організації – розробка відносяться до Інтернету технічних стандартів і відповідної політики [3].

Таке різноманіття суб’єктів Інтернет-правовідносин можна об’єднати у групи: технічні, індивідуальні, колективні, міжнародні.

Технічні суб’єкти, відповідають за роботу Інтернету, інфраструктури та компонентів. До них відносяться: технологи, архітектори, інженери, організації, які здійснюють загальну координацію і допомагають впроваджувати відкриті стандарти тощо.

Специфікою цієї групи суб’єктів виступає те, що вони не можуть здійснювати роботу без відповідного дозволу органів державної влади. До індивідуальних суб’єктів відносяться фізичні особи, користувачі Інтернету.

Колективні суб’єкти Інтернет-правовідносин представлені юридичними особами. Як суб’єкти правовідносин юридичні особи можуть бути державними та недержавними. До державних відноситься Міністерство цифрової трансформації зв’язку України, основним завданням якого є вироблення і реалізація державної політики та нормативно-правове регулювання у сфері інформаційних технологій, електрозв’язку, масових комунікацій і засобів масової інформації, а також Інтернету.

Важливу роль у розвитку Інтернету займають громадянське суспільство, у тому числі науковці, а також бізнес-співтовариство, зусиллями яких створюється технологічна інфраструктура, комп’ютери, мережі, програмне забезпечення.

Особливе місце в Інтернет-правовідносинах займають міжнародні організації, найбільш значущим є Міжнародний союз електрозв’язку. Його діяльність спрямована на надання допомоги у розвитку інформаційно-комунікаційної інфраструктури та послуг, розвитку людського потенціалу та новітніх технологій.

Формування правовідносин важливий етап правового регулювання Інтернет-відносин, необхідний елемент досягнення юридичних цілей.

Література

1. Ковалів М., Єсімов С., Скриньковський Р., Красницький І., Мазур Ю., Гарасим П., Князь С. Особливості правових відносин, які виникають в мережі Інтернет. Traektoriâ Nauki = Path of Science. 2021. Vol. 7. № 3. S. 1001-1007.
2. Харитонов Є. О., Харитонова О. І. «Інтернет-відносини» та «інтернет-правовідносини»: до визначення поняття і сутності. Університетські наукові записки. 2017. № 3. С. 27-38.
3. Declaration of Principles «Building an Information Society - a Global Challenge in the New Millennium». URL. https://zakon.rada.gov.ua/laws/show/995_c 57#Text

Коваль І. І.

курсант факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ НА ДЕОКУПОВАНИХ ТЕРИТОРІЯХ

Оперативно-розшукова діяльність на деокупованих територіях має свої особливості через специфіку ситуації. Наприклад, необхідно враховувати розподіл компетенції між органами влади на звільнених територіях, що, зазвичай, передбачає

взаємодію військових, цивільних та правоохоронних органів. Військові органи відповідають за забезпечення безпеки та управління військовою складовою операції, тоді як цивільні органи мають на меті відновлення нормального функціонування громадського життя, управління соціальними питаннями та інфраструктурою. Правоохоронці відповідають за здійснення оперативно-розшукової та правоохоронної діяльності для забезпечення громадської безпеки. Цей розподіл може варіюватися залежно від конкретної ситуації та стратегії влади. Також на деокупованій території може існувати загроза дії нелегальних структур, які можуть намагатися встановити свій контроль або втручатися у суспільні відносини. Це може виражатися у організації злочинних угруповань, терористичних елементів або інших формувань, що використовують вакуум влади для своїх протиправних цілей. Забезпечення безпеки та здійснення ефективної правоохоронної та військової діяльності важливі для запобігання та протидії таким нелегальним злочинним структурам. Забезпечення безпеки на деокупованих територіях вимагає тісної співпраці між військовими та правоохоронними органами. Військові можуть брати на себе відповідальність за загальний контроль та безпеку, забезпечуючи стабільність, тимчасовий порядок і захист населення [1].

Співпраця з правоохоронцями важлива для здійснення оперативно-розшукової діяльності та забезпечення правопорядку. Обмін інформацією, координація заходів та спільне планування допомагають ефективно вирішувати завдання забезпечення безпеки на території. Така взаємодія сприяє впевненості громадян в стабільності та захищеності регіону.

Оперативно-розшукова діяльність на деокупованій території має свої особливості: специфіка ситуації, взаємодія з військовими, контроль над контрабандою та тероризмом, охорона громадянського населення, міжнародна співпраця [2]. Розглянемо кожний аспект детальніше.

Специфіка ситуації при здійсненні оперативно-розшукової діяльності на деокупованих територіях включає такі аспекти:

1. Нестабільність та ризики: наявність конфлікту може створювати непередбачувані обставини, що вимагають від оперативників готовності до реагування на різні сценарії та управління ризиками.

2. Наявність різних впливових груп: присутність різних політичних та збройних формувань може ускладнювати співпрацю між органами та вимагати виваженої стратегії співробітництва.

3. Операції в умовах відсутності сталої влади: відсутність стабільного уряду може вимагати від правоохоронних органів більш широкого спектру відповідальностей, включаючи адміністративні та гуманітарні функції.

4. Небезпека терористичних та злочинних актів: деокуповані території часто стають об'єктом інтересу терористичних та злочинних груп, що підсилює необхідність ефективного реагування та протидії.

5. Гуманітарний вимір: оперативно-розшукова діяльність повинна враховувати гуманітарні аспекти, включаючи захист цивільного населення, надання гуманітарної допомоги та відновлення інфраструктури.

Ці фактори створюють складну та динамічну ситуацію, де оперативці повинні виявити високий рівень гнучкості та адаптивності для досягнення ефективних результатів [3].

Взаємодія з військовими при здійсненні оперативно-розшукової діяльності на деокупованих територіях є важливим елементом для забезпечення загальної безпеки та ефективного управління ситуацією.

Деякі ключові аспекти цієї взаємодії включають:

- Координацію заходів: спільне планування та координація заходів між військовими та правоохоронними органами допомагають уникнути конфліктів і забезпечити оптимальне використання ресурсів;
- Обмін інформацією: ефективний обмін розвідувальною інформацією між військовими та оперативними підрозділами сприяє більш швидкому та точному розгортанню сил та засобів правопорядку та військових.
- Забезпечення безпеки під час спільних операцій: врахування особливостей військових операцій та взаємна допомога в забезпеченні безпеки під час проведення спільних операцій [4].
- Спільні навчання та тренування: проведення спільних навчань дозволяє військовим та правоохоронцям навчитися спільній діяльності та розвивати взаєморозуміння.
- Гуманітарні аспекти: спільна робота у гуманітарних питаннях, таких як надання допомоги цивільному населенню, є також важливою складовою взаємодії. Ця взаємодія вимагає ефективного комунікаційного процесу, взаємного поваги та здатності адаптуватися до змін в обстановці на деокупованій території.
- Контроль над контрабандою та тероризмом на деокупованих територіях є важливим завданням для забезпечення стабільності та безпеки. Декілька ключових аспектів цього контролю включають:
  - Моніторинг кордонів: ефективний контроль кордонів є важливим для запобігання контрабанді та незаконному переміщенню терористичних елементів.
  - Розвідка та розвідувальна діяльність: активна розвідка є важливою для виявлення та слідкування за діяльністю контрабандистів та терористичних груп.
  - Міжнародна співпраця: співпраця з іншими країнами та міжнародними організаціями важлива для обміну інформацією та спільних заходів по боротьбі з контрабандою та тероризмом.
  - Спільні операції: здійснення спільних оперативних заходів між військовими та правоохоронними органами для придушення контрабанди та нейтралізації терористичних загроз.
  - Використання технологій: впровадження сучасних технологій для виявлення та відстеження незаконної діяльності, таких як надзвичайні засоби спостереження, дрони та інші технічні рішення.

Ці заходи спрямовані на забезпечення ефективного контролю та відповіді на потенційні загрози, які можуть виникнути на деокупованих територіях [5].

Охорона громадянського населення є однією з ключових місій оперативно-розшукової діяльності на деокупованих територіях. Деякі аспекти цього завдання включають:

- Безпеку населення: забезпечення основної безпеки громадян, включаючи захист від злочинності та негайну реакцію на можливі загрози.
- Гуманітарну допомогу: надання допомоги цивільному населенню в умовах конфлікту, включаючи медичну допомогу, харчування та притулок.
- Евакуацію та захист цивільних об'єктів: організація ефективної евакуації та захист важливих об'єктів, таких як школи, лікарні та інфраструктура.

- Інформаційна безпека: забезпечення правдивої та своєчасної інформації громадянам щодо безпекової ситуації та рекомендацій з попередження небезпек.
- Співпрацю з громадськістю: залучення громадськості до спільних заходів з безпеки, створення механізмів зворотного зв'язку та врахування побажань та потреб громадян.

Охорона цивільного населення вимагає виваженості, чутливості до гуманітарних аспектів та глибокого розуміння конкретних викликів, які виникають на деокупованих територіях [6].

Міжнародна співпраця в оперативно-розшуковій діяльності на деокупованих територіях включає такі важливі аспекти:

- Обмін інформацією: активний обмін розвідувальною та оперативною інформацією між країнами сприяє ефективній боротьбі з транскордонними злочинними групами та терористичними загрозами.
- Спільні оперативні заходи: організація спільних спеціальних операцій між країнами для придушення транскордонної злочинності та забезпечення безпеки регіону.
- Інтернаціональні домовленості: укладання та дотримання міжнародних договорів та конвенцій, спрямованих на спільну боротьбу з тероризмом, контрабандою та іншими злочинами.
- Організація спільних навчань та тренувань: проведення спільних навчань для підвищення ефективності взаємодії та розвитку спільних стратегій.
- Співпраця з міжнародними організаціями: співпраця з міжнародними організаціями, такими як Інтерпол чи Європол, для координації міжнародних зусиль та обміну ресурсами.

Міжнародна співпраця є ключовою для успішного протидії транскордонним загрозам та забезпечення безпеки на деокупованих територіях [7].

Ці риси визначаються конкретним контекстом конфлікту та потребами безпеки на деокупованій території.

Література

1. Документування злочинів на деокупованих територіях: факультативні бінарні заняття з оперативно-розшукової діяльності. Сайт ОДУВС. URL: https://oduvs.edu.ua/news.
2. Стабілізаційні заходи на деокупованих територіях: сайт ДДУВС. URL: https://dduvs.in.ua/2022/12/01/stabilizatsijni-zahody-na-deokupovanyh-terytoriyah-kursanty-dduvs-opanovuyut-aksiomy-roboty-politsejskogo-v-umovah-vijny/.
3. Чорна А. Принципи запобігання поліцією кримінальних правопорушень на деокупованих територіях. Науковий вісник Дніпропетровського державного університету внутрішніх справ. № 2. 2023. С. 43-47. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/08/2/NV_2-2023-43-47.pdf.
4. Білецький В. Взаємодія оперативних підрозділів Державної прикордонної служби України з оперативними підрозділами інших органів на деокупованих територіях. Підприємництво, Господарство і Право. № 10. 2018. С. С.122−126. URL: http://pgp-journal.kiev.ua/archive/2018/10/25.pdf.
5. Протидія кримінальним правопорушенням в умовах воєнного стану : збірник матеріалів Всеукраїнської науково-практичної конференції в авторській редакції, (м.

Кропивницький, 27 жовтня 2022 року). 367 с. URL: https://dnuvs.in.ua/wpcontent/uploads/2022/12/zbirnyk_konferencziya_27_10_onovlenyj.pdf.
6. Про забезпечення прав і свобод громадян та правових режим на тимчасово окуповані території України: Закон України від 15.04.2014 № 1207-VII. URL: https://zakon.rada.gov.ua/laws/show/1207-18#Text
7. Єфімов. В. Міжнародне співробітництво в оперативно-розшуковій діяльності. Право і суспільство. № 1. 2012. URL: http://pravoisuspilstvo.org.ua/archive/2012/1_2012/57.pdf.

Кондратюк Н. С.
здобувач вищої освіти Державного податкового університету
Котух Є. В.
професор кафедри кримінальних розслідувань Державного податкового університету, доктор наук з державного управління, кандидат технічних наук, доцент

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИФРОВІЙ КРИМІНАЛІСТИЦІ

У сучасних умовах війни та глобальних загроз головним завданням криміналістики є розроблення та застосування інноваційних засобів, прийомів та методів, що дозволяють ефективно збирати, досліджувати, використовувати у досудовому розслідуванні та судовому розгляді різноманітну доказову інформацію [1, с. 73-77], у тому числі й цифрову. Сьогодні цифрова реальність пов'язана із появою нових форм злочинності – кіберзлочинів, інформаційно го шахрайства, великою кількістю кібернетичних атак на різні підприємства та установи, що зумовлює необхідність грунтовних наукових досліджень цих проблем, їх спеціального вивчення та дослідження.

Дійсно, за таких умов цифрова інформація, як невід'ємний атрибут сучасної злочинної й діяльності органів кримінальної юстиції, визначає нині перспективи розвитку криміналістики [2, с. 149-160], яка знаходиться на передньому краю боротьби зі злочинністю в сучасних реаліях воєнного стану, цифровізації суспільства та активного застосування цифрових технологій у різних сферах діяльності людини. Саме тому зараз в реаліях воєнного часу проблеми застосування штучного інтелекту в діяльності органів правопорядку та юстиції набувають актуальності та потребують спеціальних дослідженнь з врахуванням європейського досвіду та сучасної практики [3, с. 89-93].

В. М. Шевчук доречно відзначає, що «застосування штучного інтелекту у судочинстві та правоохороній діяльності є можливим із обов'язковим врахуванням принципів верховенства права, дотримання основних прав людини, поваги до честі і гідності, рівності перед законом і судом, пропорційності, змагальності сторін, прозорості, неупередженості та справедливості тощо. Водночас, неможливо на сьогодні повністю замінити суддю при здійсненні судочинства на штучний інтелект, однак, ніщо не забороняє оптимізувати роботу судді та суду шляхом залучення таких технологій. Головна роль штучного інтелекту має бути визначена не як заміна судді при здійсненні судочинства, а як своєрідна допомога для здійснення правосуддя суддею» [4, с. 174].

У свою чергу, слід погодитись, що «в сьогоднішніх реаліях штучний інтелект використовується щоденно у повсякденній діяльності людини, наприклад, для перекладу текстів, створення субтитрів для відео або блокування електронних листів (спаму). При цьому штучний інтелект розглядається як сукупність методів, способів, технологій і засобів (зокрема, апаратних), комп'ютерних програм, які реалізують одну,

кілька або всі когнітивні функції, еквівалентні когнітивним функціям людини; це сконструйований людиною пристрій або комп'ютерна програма зі здобування, оброблення й застосування інформації та формування вмінь, подібних до дій, свідомо виконуваних людиною» [5, с. 9].

Таким чином, дослідження ролі та використання методів штучного інтелекту в цифровій криміналістиці вказує на важливий етап еволюції сучасних кримінальних розслідувань. Застосування штучного інтелекту в цифровій сфері надає правоохоронним органам потужний інструментарій для виявлення, аналізу та боротьби з кіберзлочинністю. Можна стверджувати, що застосування штучного інтелекту є закономірним етапом розвитку й формування сучасних криміналістичних знань, який передбачає впровадження цифрових технологій у різні галузі криміналістичної науки, судової експертології та юридичної практики.

Література

1. Konovalova V.O., Shevchuk V.M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. Advanced discoveries of modern science: experience, approaches and innovations: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific Conference, January 20, 2023. Pp. 73-77.
2. Tymoshenko, Y.P., Kozachenko, O.I., Kyslenko, D.P., Horodetska, M.S., Chubata, M.V., & Barhan, S.S. Latest technologies in criminal investigation (testing of 176 foreign practices in Ukraine). Amazonia Investiga, 2022, 11(51). С. 149-160.
3. Malevski H. Textbook of criminalistics. Vol. 1: General theory. Kharkiv: Apostille Publishing House, 2016. 488 p. P. 89-93.
4. Шевчук В.М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. Актуальні проблеми протидії злочинності та корупції. Харків. 2023. С. 171-176.
5. Баранов О. Ідентифікація робота зі штучним інтелектом як суб'єкта права. Інтернет речей: проблеми правового регулювання та впровадження. Київ, 2018. С. 9–14.

Кондратюк О. В.

професор кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Лепеха О. М.

заступник директора з питань цифровізації Державної установи «Центр інфраструктури та технологій Міністерства внутрішніх справ України», кандидат юридичних наук

ПРО НЕОБХІДНІСТЬ ПЕРЕОСМИСЛЕННЯ ЮРИДИЧНОЇ ОЦІНКИ ПРАВОВОЇ ПОВЕДІНКИ НЕГЛАСНОГО ПРАЦІВНИКА

Важко переоцінити роль негласних працівників у повному, а саме головне об'єктивному (якісному) інформаційно-аналітичному забезпеченні діяльності правоохоронних органів, зокрема і в сфері національної безпеки.

Якщо без зайвої деталізації, то на сьогодні напрями використання негласних працівників підрозділами Національної поліції України виглядають наступним чином: а) для проведення негласної роботи (до прикладу – агентурно-оперативної) з метою

пошуку будь-якої оперативної інформації, яка становить фактичний інтерес для оперативного підрозділу в залежності від його функціонального призначення та визначених оперативно-службових завдань. В цьому випадку негласними працівниками здійснюється загальна пошукова діяльність будь-яких фактичних даних, які можуть містити ознаки вчиненого кримінального правопорушення або такого, яке готується, встановлюється коло потенційних зловмисників, які, теоретично, можуть становити інтерес для правоохоронних органів; б) для проведення оперативної розробки в межах оперативно-розшукової справи. В цьому випадку здійснюється вже цілеспрямована робота негласного працівника в умовах повної очевидності (відомі фігуранти) чи неповної очевидності (невідомі фігуранти, проте є фактичні дані щодо злочинної діяльності), тобто, в загальному, негласний працівник зорієнтований де, що і кого шукати; в) для проведення негласних слідчих розшукових дій за участю осіб, з якими встановлено конфіденційно співробітництво, або із використанням негласних працівників оперативного підрозділу. Процес доказування відбувається за участі негласного працівника, перед яким слідчим (прокурором) визначені конкретні завдання.

Якщо в першому (а) із перерахованих випадків негласний працівник пасивною поведінкою (користуючись своїми діловим якостями та розвідувальними можливостями) ще може виконувати завдання оперативного підрозділу, то в наступних двох випадках (б; в) лише пасивна його діяльність є малоефективною. Крім того найбільш законодавчо врегульованим в Україні є використання негласного працівника для виконання спеціального завдання з викриття злочинної діяльності організованої групи чи злочинної організації, яке може застосовуватися як оперативно-розшуковий захід або ж як негласна слідча розшукова дія. Менш урегульованою є можливість використання негласного працівника для проведення одноразових оперативно-розшукових заходів (оперативно-технічних заходів, оперативної закупки) або контролю за вчиненням кримінального правопорушення у кримінальному провадженні.

Законодавство України у сфері боротьби із злочинністю урегульовує діяльність правоохоронних органів у протидії неочевидній (латентній) злочинності та її суб'єктам (відомим та невідомим особам), зокрема положеннями статті 6 Закону України «Про оперативно-розшукову діяльність» уповноважено спеціально визначених цим же Законом суб'єктів проводити оперативно-розшукову діяльність щодо кримінальних правопорушень, які готуються. Це означає, що правоохоронному органу відомо про ознаки кримінального правопорушення, яке готується або ж вчинене, проте невідомими залишаються його співучасники та інші деталі. На цьому етапі протидії злочинності основним завданням правоохоронного органу є встановлення причетності конкретної особи до злочинного діяння, що, зазвичай, вирішується за допомогою негласних працівників. Останні, незалежно від того, чи це агенти або ж поліцейські, які діють конспіративно під прикриттям правоохоронного органу, попередньо надавши добровільну згоду та усвідомлюючи небезпеку своєї професії та обумовлені з цим ризики, впроваджуються в кримінальне середовище з метою його нейтралізації – притягненням співучасників до відповідальності, конфіскацією активів та майна, здобутого злочинним шляхом. На противагу цьому представники криміналітету вживають різноманітних заходів щодо протидії власному викриттю і у виборі засобів вони не обмежуються ані мораллю, ані законом, в той час коли правоохоронці зобов'язані діяти суворо в рамках як національного, так і міжнародного законодавства. По суті це війна, де сторона агресора діє як їй заманеться на чужій території, а сторона, яка вимушена захищатися, повинна зважати у виборі засобів того ж захисту, щоб не нашкодити своїм громадянам, в той же час і не перевищити меж так званої необхідної оборони. Ця ж сторона, по суті, позбавлена засобів нападу. А це вже не рівнозначна позиція протиборчих сторін. Прийнято вважати, що ресурси, які виділяються та забезпечуються державою для

боротьби із злочинністю, є суттєво більшими, ніж ті, які є у розпорядженні криміналітету для вчинення кримінальних правопорушень та протидії правоохоронним органам. Проте, насправді, ефективність їх використання злочинним середовищем є значно більшою, що підтверджується суттєвою кількістю виявлених кримінальних правопорушень та причетних осіб та зовсім незначною кількістю обвинувальних вироків суду та реально конфіскованого в дохід держави майна (цінностей).

В судовій практиці України трапляються випадки визнання негласної роботи правоохоронних органів щодо суб'єкта кримінального правопорушення провокацією. Не можна вважати некваліфіковану роботу агентів чи поліцейських під прикриттям основною причиною такого стану речей, оскільки сьогодні негласний працівник, по суті, залишився один на один із злочинним середовищем, куди він впроваджений для виконання спеціального завдання, і вимушений розраховувати на власний професіоналізм, досвід та навики виживання в ворожому середовищі, а ще паралельно необхідно виконувати оперативно-розшукові, розвідувальні або ж контррозвідувальні завдання, суворо дотримуючись закону. Кожний день негласний працівник проживає відповідно до легенди-прикриття, грає роль відповідно до заздалегідь визначеної правоохоронним органом лінії поведінки, і у разі навіть неумисного відступу від описаного виникає безпосередня загроза його життю. Відомо, що ділові якості та пошукові можливості особи формують можливість формального допуску агента або ж поліцейського під прикриттям до оперативної інформації кримінального характеру, якою безпосередньо володіє кримінальне середовище, але ж власне доступ до конкретних фактичних даних надається самим кримінальним суб'єктом, який усвідомлює всю небезпеку для кримінального співтовариства від поширення цієї інформації для «новоприбулих зловмисників». І далеко не завжди пасивна поведінка негласного працівника чи імітація злочинної діяльності, яка все ж таки містить формальні ознаки кримінального правопорушення, відкриває доступ до законспірованої злочинної діяльності та раніше невідомих співучасників вищого рівня ніж підбурювач, пособник чи виконавець.

Легенда, лінія поведінки, імітація протиправної діяльності мають спільну мету – викликати довіру у суб'єкта злочинного середовища, який вже за своєю природою теоретично припускає настання небезпеки у зв'язку із опосередкованою чи безпосередньою обізнаністю «новоприбулого» про кримінальне співтовариство. А завданням негласного працівника, яке від нього вимагає закон, є створення умов, щоб саме ініціатива та умисел протиправної діяльності активно проявлялися саме суб'єктом кримінального середовища.

Оперативна комбінація, як і імітація злочинної діяльності негласним працівником, за своїм змістом можуть та повинні хоча б формально містити елементи вищенаведених способів підбурювання та пособництва, щоб забезпечити високу ступінь вірогідності легенди та лінії поведінки агента чи поліцейського під прикриттям та створити ілюзію у суб'єкта кримінального середовища щодо уявних кримінальних можливостей негласного працівника, впровадженого в небезпечне для його життя злочинне середовище для виконання завдань держави в особі правоохоронного органу щодо боротьби із злочинністю. Погодьтесь, що пасивна діяльність правоохоронного органу щодо формальної реалізації способів підбурювання та пособництва з метою виявлення злочинних намірів та діянь суб'єктів кримінального середовища взагалі невиправдана тими ризиками, в яких постійно перебуває негласний працівник заради інтересів держави (суспільства). Та й існує лише невисокий відсоток того, що таке пасивне очікування досягне бажаних результатів для правоохоронного органу і абсолютно не гарантує, що паралельно не буде вчинено іншого кримінального правопорушення, яке протягом тривалого часу залишиться невідомим. Тому, ми переконані, що держава, враховуючи міжнародну судову практику, побудовану в більшості на прецедентах,

зобов'язана брати на себе відповідальність за негласну роботу правоохоронних органів, негласні працівники яких ризикують власним життям не задля задоволення особистих інтересів, а заради суспільства, держави, кожної законослухняної людини, якій немає чого боятися, бо навіть у випадку порушення (обмеження) її прав і свобод, держава їй гарантовано компенсує матеріальну та моральну шкоду в повному обсязі, офіційно спростує свої підозри, вибачиться тощо.

Підбір, навчання, а тим більше впровадження негласного працівника в злочинне середовище супроводжуються не лише ризиками, небезпечними як для його життя, так і життя близьких, але й суттєвими фінансовими затратами з боку держави в особі правоохоронного органу на матеріальне підкріплення легенди та визначеної лінії поведінки, імітацію протиправної діяльності, зашифровані компенсаційні витрати або ж відшкодування заподіяної шкоди правоохоронюваним інтересам, нанесеної в умовах виправданого ризику для досягнення суспільно корисної мети – викриття злочинної діяльності. Впровадження негласного працівника в злочинне середовище, як правило, відбувається при сукупності двох умов, по перше, коли правоохоронний орган, як суб'єкт оперативно-розшукової, розвідувальної або контррозвідувальної діяльності обґрунтовано зорієнтований та достовірно обізнаний про наявність протиправної діяльності, яка безпосередньо або ж опосередковано стосується готування чи вчинення тяжких, особливо тяжких злочинів, як правило, організованою групою (злочинною організацією), рідше окремим суб'єктом, по-друге, якщо іншими силами, засобами, заходами та методами виявити і припинити таку діяльність не представляється можливим. Відповідно до положень національного законодавства негласне співробітництво можливе в рамках оперативно-розшукової, розвідувальної або контррозвідувальної діяльності, а конфіденційне співробітництво допускається в межах негласної діяльності органу досудового розслідування у конкретному кримінальному провадженні. Такий стан речей збігається із правовою позицією Європейського суду з прав людини, який неодноразово відзначав, що держава зобов'язана мати у розпорядженні конкретні та об'єктивні свідчення, що підтверджують вчинення обвинуваченим конкретних кроків на вчинення діяння, за яке він у подальшому переслідується, в той же час будь-яка інформація, що стосується існуючого наміру вчинити злочин або вчинюваного злочину, має бути такою, що може бути перевіреною, та публічне обвинувачення повинно мати змогу продемонструвати на будь-якій стадії, що в його розпорядженні наявні достатні підстави для проведення оперативного заходу.

Відтак в практиці правоохоронних органів, зокрема поліції, згадані впровадження відбуваються при наявності вагомих приводів, які свідчать про ознаки організованої злочинної діяльності та підстав, які нормативно це дозволяють зробити та в яких документально зафіксовано причетність відомих або невідомих осіб до злочинного діяння. Також оцінюється рівень суспільної небезпеки та наслідків від раніше невідомої правоохоронному органу злочинної діяльності. Іншими словами негласна робота правоохоронного органу розпочинається не безпідставно, а тим більше не переслідує оперативно-профілактичну мету, оскільки, як вже згадувалося, увесь процес супроводжується найвищими ризиками та значними матеріальними витратами. В процесі оперативного відпрацювання суб'єктів, які мають пряме чи непряме відношення до злочинного середовища, увага негласного працівника зосереджується на конкретній відомій або ж раніше невідомій особі (групі), яка себе компрометує, відповідно до аналітики правоохоронного органу, вміннями, навиками, поведінкою, статусом, а інколи і конкретними діяннями, які не завжди на перший погляд носять кримінальний характер. Але останнє трапляється все рідше через обізнаність кримінального світу із методами негласної роботи правоохоронних органів. Відтак пасивне очікування негласним працівником як новим потенційним формальним співучасником протиправної

діяльності активних дій, які повинні містити ознаки кримінального правопорушення, навіть без виконання перевірочних злочинних завдань, компрометує його статус, ставить його під сумнів, чим викликає недовіру. Навіть виникнення недовіри до впровадженого в злочинне середовище негласного працівника може загрожувати його життю і усунення такої небезпеки, в залежності від спеціалізації кримінальної структури, може відбутися миттєво або в короткий час, не достатній для виведення особи з оперативної розробки із подальшим забезпеченням заходів безпеки. Залишаємо риторичним запитання, чи буде злочинне середовище картати себе за нейтралізацію або знищення не агента. Через загрозливі масштаби як світової та і національної організованої злочинності, небезпечні міжнародні кримінальні тенденції, а також в силу існування найвищого ризику для негласного працівника – небезпеки для його життя – сам зміст меж негласної роботи агента чи поліцейського під прикриттям щодо можливості провокації злочину необхідно переглянути, ввівши поняття активної провокації до вчинення злочину. Слід визнати, що імітація злочинної діяльності чи протиправної поведінки негласним працівником, цілеспрямоване доведення до свідомості людини своїх протиправних можливостей, демонстрація вмінь та навиків, які можна використати для досягнення злочинної мети − це все, якщо розглядати кожне окремо, є формальною провокацією, а в сукупності є однією цілеспрямованою провокацією, яка в залежності від оперативно-розшукової, розвідувальної чи контррозвідувальної ситуації в комплексі із збігом життєвих негараздів може спровокувати абсолютну більшість людей до протиправного вчинку, якщо не злочину.

Упродовж 2017-2019 років на базі закладу вищої освіти із специфічними умовами навчання із підготовки поліцейських (Львівський державний університет внутрішніх справ, Україна) підвищення професійної кваліфікації проходили працівники оперативних підрозділів Національної поліції. В результаті проведеного соціологічного дослідження методом анкетування, організованого науково-педагогічними працівниками кафедри Оперативно-розшукової діяльності, було встановлено, що 78 % опитаних, а це 209 практичних працівників оперативних підрозділів із допуском до агентурно-оперативної роботи, підтвердили неефективність пасивної поведінки негласного працівника в злочинному середовищі з метою виявлення злочинних намірів суб’єктів неочевидної протиправної діяльності; з них 72 % опитаних були послідовними у своїй позиції і погодилися із пропозицією щодо необхідності переходу негласними працівниками від пасивного очікування до активних дій із виявлення злочинних намірів особи, внесенням відповідних змін в національне законодавство, яке б гарантувало не притягнення до кримінальної відповідальності за активну правомірну поведінку негласного працівника в злочинному середовищі, якщо формально вона містить ознаки складу кримінального правопорушення.

Ми підтримуємо позицію науковців, які наполягають, що професійна діяльність осіб, укорінених у злочинне середовище, регламентована чинним законодавством, потребує оптимізації щодо складових елементів ефективного правового, соціального, фізичного та психологічного захисту негласних працівників, котрі виконують спеціальне завдання із розкриття злочинної діяльності.

Підсумовуємо, що Україні необхідно кардинально змінити державну політику з напряму протидії на напрям боротьби із злочинністю, що продемонструє, що влада і народ єдині в нетерпимості до злочинності у всіх її проявах та формах, тим більше, що це не лише вітається, але й всіляко підтримується міжнародними партнерами, зокрема Сполученими Штатами Америки у сфері протидії корупції, та заохочується на прикладі співпраці із Міжнародним валютним фондом. Некодифікованість національного законодавства, яке урегульовує правоохоронну діяльність, здебільшого його внутрішня суперечливість, нагромадження правових норм, необізнаність правоохоронних органів,

а подекуди і нехтування рішеннями Європейського суду з прав людини (у кримінальних провадженнях за матеріалами агентурно-оперативної та негласної поліцейської роботи) при організації оперативно-розшукової діяльності призводять до системного правового нігілізму, що врешті нівелює очікувані суспільством результати боротьби із злочинністю. На державному (законодавчому) рівні необхідно урегулювати загальні засади та принципи негласної роботи правоохоронних органів, зокрема шляхом розширення меж пасивної поведінки негласних працівників під час пошукової діяльності у злочинному середовищі, для забезпечення наступальності правоохоронних органів у боротьбі із злочинністю. Це прогнозовано призведе до формування істинної правової держави та правового суспільства, здатного на паритетних умовах приєднатися до Європейського Союзу і разом захищати європейські цінності.

Корляков Б. О.
курсант факультету № 4 Харківського національного університету внутрішніх справ

ІННОВАЦІЙНІ ФОРМИ РЕАБІЛІТАЦІЇ У ВОЄННИХ ТА ПІСЛЯВОЄННИХ УМОВАХ

Війна – це трагічна подія, яка може призвести до значних фізичних та психологічних травм. Люди, які пережили війну, часто потребують реабілітації, щоб відновити своє здоров’я та благополуччя.Традиційні форми реабілітації, такі як фізична терапія, психологічне консультування та професійне навчання, є важливими для людей, які пережили війну. Однак інноваційні форми реабілітації також можуть бути корисними.Інноваційні форми реабілітації використовують передові технології та методи лікування для надання допомоги людям, які пережили війну. Вони можуть бути більш ефективними та доступними, ніж традиційні форми реабілітації і ось деякі приклади інноваційних форм реабілітації:

Телемедицина та телетерапія, використовуються для надання реабілітаційних послуг людям, які живуть у віддалених районах або регіонах, де недостатньо забезпечених медичних послуг. Наприклад, у 2016 році Міжнародний Комітет Червоного Хреста запустив телемедичну програму для допомоги жертвам війни в Сирії. Це дозволило МКЧХ надавати медичну та психологічну допомогу людям, які живуть у районах бойових дій, доступ яких до звичайних медичних закладів ускладнений через військові дії.

Протези та ортопедичні досягнення, вони зробили життя кращим для людей з ампутованими кінцівками або людей, поранених під час війни. Наприклад, у 2018 році компанія Oculus VR розробила прототип протеза руки на основі штучного інтелекту. Це дозволяє людям, які втратили кінцівки, виконувати складні завдання, наприклад тримати або підбирати речі.

Мистецька та музична терапія використовувалася, щоб дати людям можливість відновитися після психологічної травми, спричиненої конфліктом під час або після нього. Наприклад, у 2022 році організація Save Children запровадила музикотерапію для дітей, які постраждали від війни в Україні. Це допомагає дітям зрозуміти, що вони відчувають, і впоратися зі стресом, пов’язаним з війною.

Реабілітація віртуальної реальності (VR) – це вид терапії, який використовується для лікування посттравматичного стресового розладу (ПТСР). Наприклад, у 2021 році видання The Lancet Psychiatry опублікувало статтю, в якій виявилося, що VR-терапія ефективна для зменшення симптомів посттравматичного стресового розладу у солдатів, які брали участь у бойових діях. Реабілітація в громаді – це підхід,

спрямований на сприяння соціальному залученню та інтеграції людей з обмеженими можливостями. Наприклад, у 2020 році Програма розвитку ООН ініціювала проект реабілітації людей з обмеженими можливостями на рівні громади в Сирії. Ця програма допомагає їм отримати нові навички та реінтегруватися в суспільство.

Але не слід ігнорувати той факт, що інноваційні форми реабілітації можуть бути недоступні через економічні фактори. У цьому випадку, наприклад, країнам, що розвиваються, може не вистачити коштів, необхідних для придбання обладнання або навчання персоналу, відповідального за надання цих послуг. Політичні чинники також можуть впливати на те, чи є інноваційні форми реабілітації доступними чи ефективними. Наприклад, може бути важко забезпечити заходи безпеки, пропонуючи таке лікування під час, коли в межах країни точиться війна. Етичні питання, пов'язані з інноваційними формами реабілітації. Однією з помітних етичних проблем є те, що деякі люди не можуть дозволити собі дорогі номінали, пов'язані з новими методологіями, оскільки вони ще не широко поширені або існують у невеликій кількості для всіх, хто їх потребує. Інший етичний виклик полягає в тому, що ці форми реабілітації можуть не підходити для всіх людей. Наприклад, деякі люди можуть не відчувати себе комфортно, використовуючи такі технології, як віртуальна реальність.

Висновок. Люди, які пережили війну, можуть знайти багато переваг у нових формах реабілітації. Однак при створенні та впровадженні цих форм не можна ігнорувати економічні, політичні та етичні обмеження. Тому важливо враховувати ці фактори при розробці інноваційних форм реабілітації.

Література

1. Relief and Rehabilitation for a Post-war World. Bloomsbury. URL: https://www.bloomsbury.com/us/relief-and-rehabilitation-for-a-postwar-world-9781350179110/
2. Post-conflict rehabilitation: the humanitarian dimension. URL: https://www.files.ethz.ch/isn/102390/1998_10_Post-Conflict_Rehabilitation.pdf
3. CORE – Aggregating the world's open access research papers. URL: https://core.ac.uk/download/pdf/29179645.pdf

Кочин В. Д.

курсант факультету №4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, доктор економічних наук

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогоднішній день, щоб забезпечити національну безпеку України, правоохоронні органи збирають все більше інформації про своїх громадян. Аби уникнути обурення народу, був прийнятий Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [1], в якому зазначено наступне: «Державі дозволяється зберігати дані про громадян України, якщо це необхідно для:

- забезпечення національної безпеки, оборони, охорони громадського порядку, боротьби з правопорушеннями;
- надання громадянам державних послуг;

- забезпечення виконання законів та інших нормативно-правових актів;
- виконання міжнародних зобов'язань України.»

Також держава може зберігати дані і про юридичні особи, якщо це необхідно для:

- забезпечення національної безпеки, оборони, охорони громадського порядку, боротьби з правопорушеннями
- забезпечення виконання законів та інших нормативно-правових актів
- виконання міжнародних зобов'язань України.

Згідно [2], у системи баз даних є свої недоліки. Досвід практичної експлуатації та створених на їх основі облікових баз свідчить про такі основні проблеми:

- розбіжність між іншими базами;
- несвоєчасне надходження інформації до підрозділів оперативного реагування;
- недосконаліть або дефіцит кадрового забезпечення;
- недосконаліть та неврегульованість правової бази інформаційних баз.

Нормативно-правова база діяльності поліції є недосконалою стосовно використання інформаційних баз. Також можна виділити, що підрозділи національної поліції стосовно вміння використовувати інформаційні бази не зовсім професійно підготовлені для повсякденного їх використання. У зв’язку із специфікою роботи поліцейських, інформаційна база має оновлюватись майже кожну хвилину, але через застарілість технічного обладнання, самої системи баз даних, можуть виникати технічні проблеми, які також уповільнюють оперативну діяльність поліції.

Розвиток інформаційно-аналітичних систем сприяв створенню інформаційно-аналітичних підрозділів майже за всіма напрямами діяльності НПУ, тому їх можна називати молодими підрозділами НПУ, які і по сьогоднішній день розвиваються. До прикладу, у Харківському національному університету внутрішніх справ постійно ведеться робота по підвищенню кваліфікації фахівців із протидії кіберзлочинам, із 2024 навчального року розпочинає своє існування спеціальність номер 126 «Інформаційні системи та технології». Все це свідчить про актуальність проблеми підготовки фахівців з інформаційних технологій для національної поліції і подальший розвиток інформаційних технологій у підрозділах НПУ.

Висновки. Хоча і система інформаційних баз в Україні є не досконалою і має певні недоліки, інформаційні технології в національній поліції України та країні в цілому розвиваються дуже швидко. Підрозділи НПУ розширюють працевлаштування молодих фахівців, які в подальшому будуть сприяти вдосконаленню інформаційних баз, систем та способів комунікації. Парламент приймає нові закони для розширення нормативно-правової бази щодо інформаційних та комунікаційних систем. Тому, очевидно, проблеми застарілості систем баз даних в Україні є тимчасовими і будуть вирішені у найближчий час.

Література

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
2. С. Пеньков. Проблеми та перспективи інформаційного забезпечення оперативних підрозділів національної поліції України. [Електронний ресурс]. URL: https://univd.edu.ua/general/publishing/konf/01_12_2017/pdf/85.pdf.

Кулешник Я. Ф.
доцент кафедри систем автоматизованого проектування НУ «Львівська політехніка», доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент
Дробіняк Х. Т.
здобувач вищої освіти Львівського державного університету внутрішніх справ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ВОЄННИЙ ЧАС. ДЕЯКІ СКЛАДОВІ КОМУНІКАЦІЇ ТА ЗВ'ЯЗКУ

Інформаційні технології відіграють важливу роль у воєнній сфері, сприяючи покращенню комунікацій, визначенню стратегій, розвідці, керуванню зброєю та забезпеченню кібербезпеки.

В сучасній військовій сфері ефективний зв'язок між військовими частинами та командуванням є критично важливим для успішного ведення операцій. Використання сучасних комунікаційних технологій грає ключову роль у забезпеченні надійного та швидкого зв'язку під час військових операцій.

Розглянемо деякі аспекти застосування інформаційних технологій у воєнний час.

Сучасні комунікаційні системи військових сил. Забезпечення надійного та швидкого зв'язку. Важливим аспектом застосування інформаційних технологій у воєнний час є комунікації та зв'язок. В сучасній військовій сфері ефективний зв'язок між військовими частинами та командуванням є критично важливим для успішного ведення операцій. Використання сучасних комунікаційних технологій грає ключову роль у забезпеченні надійного та швидкого зв'язку під час військових операцій.

Розглянемо деякі з основних технологій, які застосовуються у цьому контексті:

1. **Супутникові комунікації:**
   - **Призначення**: Супутникові системи дозволяють встановлювати комунікацію в будь-якому місці, навіть в областях, де немає традиційної інфраструктури.
   - **Переваги**: Висока мобільність, глобальне охоплення, висока стійкість до перешкод.
   - **Застосування**: Забезпечення зв'язку в труднодоступних чи віддалених районах, глобальне ведення операцій, передача великих обсягів даних.

Супутникові комунікації відіграють ключову роль в забезпеченні глобального та надійного зв'язку у різних галузях, включаючи військову, цивільну та комерційну сфери. Цей вид комунікацій використовує штучні супутники для передачі сигналів між різними точками на Землі. Основні аспекти супутникових комунікацій:

1.1. Геостаціонарні та низькі орбіти:

- **Геостаціонарні супутники**: Розташовані на великій відстані від Землі та обертаються з тією самою швидкістю, що і Земля. Забезпечують постійний зв'язок з конкретною областю, але можуть мати затримку у сигналі.
- **Супутники низької орбіти (LEO)**: Знаходяться на низьких відстанях від Землі, що забезпечує меншу затримку у сигналі. Використовуються для глобального Інтернет-зв'язку та спостережень.

1.1.1. Геостаціонарні орбіти:

- Особливості:

- Знаходяться на великій відстані від Землі, на висоті приблизно 35 786 км.
- Обертаються навколо Землі з тією самою швидкістю, що і планета, тому здається, що стоять на одному місці над екватором.
- Забезпечують постійний зв'язок з конкретною точкою на Землі.

– Застосування:
- Використовуються для супутникових телекомунікацій, де важливий постійний доступ до сигналу (наприклад, супутникове телебачення або Інтернет).
- Геостаціонарні супутники також застосовуються у військових цілях для надання стійкого зв'язку та спостережень.

1.1.2. Низькі орбіти (LEO):

– Особливості:
- Знаходяться на низькій відстані від Землі, зазвичай від 160 до 2,000 км.
- Обертаються навколо Землі з високою швидкістю, що дозволяє їм перетинати різні області Землі протягом короткого часу.
- Забезпечують меншу затримку сигналу порівняно з геостаціонарними супутниками.

– Застосування:
- Використовуються для глобального Інтернет-зв'язку, забезпечуючи більшу пропускну здатність та меншу затримку.
- Застосовуються в місіях спостереження за Землею та космічних дослідженнях.
- Військове використання для надання географічного огляду та передачі даних.

1.1.3. Порівняння та вибір:

– **Геостаціонарні орбіти**: Забезпечують постійний зв'язок над конкретною областю, але можуть мати велику затримку у сигналі. Відмінно підходять для послуг, які вимагають сталого покриття.

– **Низькі орбіти**: Забезпечують меншу затримку та використовуються для глобального Інтернет-зв'язку та вимірювань.

Обидва типи орбіт грають важливу роль в сучасних супутникових комунікаціях, доповнюючи одна одну в різних застосуваннях та викликах, таких як надання послуг і ведення військових операцій.

1.2. Військове використання.

Головне військове використання це забезпечення зв'язку між військовими частинами та командуванням у будь-якій точці світу з застосування шифрування для захисту від перехоплення та несанкціонованого доступу.

Розглянемо деякі з основних технологій, які застосовуються у цьому контексті:

1.2.1. Глобальне ведення операцій:

– **Необхідність глобального зв'язку**: Військові операції можуть відбуватися в різних частинах світу, від великих міст до віддалених та важкодоступних регіонів.

- **Супутниковий зв'язок**: Використання супутникових комунікацій для забезпечення постійного та надійного зв'язку між різними військовими частинами, літаками, кораблями та командуванням.

1.2.2. Шифрована Комунікація:

- **Захист інформації**: В умовах військових конфліктів забезпечення конфіденційності та цілісності інформації стає критично важливим.
- **Шифрування даних**: Застосування сучасних шифрувальних алгоритмів для захисту від перехоплення та розшифрування ворожих сил.

1.2.3. Використання технологій шифрування:

- **Сучасні криптографічні протоколи**: Використання TLS/SSL для безпечного зв'язку через Інтернет, VPN (віртуальні приватні мережі) для захищеного обміну даними.
- **Алгоритми ключового обміну**: Використання алгоритмів, таких як Diffie-Hellman, для безпечного обміну ключами без взаємного обміну секретами.

1.2.4. Безпека мережевих з'єднань:

- **Захист від атак**: Використання брандмауерів, інтрузійних систем виявлення (IDS) та інших засобів для захисту від мережевих атак.
- **Сегментація мережі**: Розділення мережі на сегменти для обмеження розповсюдження можливих загроз.

1.2.5. Мобільна безпека:

- **Шифровані мобільні зв'язки**: Застосування шифрування для захисту мобільних комунікацій в театрах операцій.
- **Безпека з'єднань з бортовими системами**: Захист зв'язку між військовими транспортними засобами та командними пунктами.

1.2.6. Шифрування військової інфраструктури:

- **Захист систем**: Застосування шифрування для захисту важливих систем, таких як військові бази даних, пункти керування та комунікаційні вузли.

1.2.7. Тренування та профілактика:

- **Кібербезпека**: Тренування військових кадрів з питань кібербезпеки та регулярна оцінка вразливостей.

Військове використання криптографії та захищеного зв'язку є стратегічно важливим для забезпечення успішності та безпеки військових операцій у сучасному інформаційному середовищі.

1.3. Шифрування і безпека.

Шифрування та забезпечення безпеки інформації є важливим аспектом в будь-якій області, включаючи військову сферу. Сучасні технології дозволяють захищати конфіденційні дані від несанкціонованого доступу шляхом використання різних методів шифрування та криптографії.

Ось деякі ключові аспекти захисту конфіденційної інформації:

1.3.1. Криптографічні протоколи:

- **TLS/SSL**: Використовується для захищеного обміну даними через Інтернет. Забезпечує конфіденційність та цілісність інформації.

1.3.2. Симетричне та асиметричне шифрування:

- **Симетричне**: Використовує один ключ для шифрування та дешифрування. Швидший, але потребує безпечного обміну ключами.
- **Асиметричне**: Використовує пару ключів (приватний та публічний). Більш безпечний, але менш ефективний для великих обсягів даних.

1.3.3. Шифрування на рівні файлів та дискового простору:

- **BitLocker, FileVault**: Забезпечують шифрування на рівні диска або файлової системи для захисту всього вмісту.

1.3.4. Використання блокчейн-технологій:

- **Децентралізовані бази даних**: Забезпечують високий рівень безпеки інформації, оскільки дані зберігаються у вигляді блоків, які важко змінити або видалити.

1.3.5. Мережева безпека:

- **Firewalls, Intrusion Detection Systems (IDS)**: Використовуються для виявлення та блокування несанкціонованого доступу до мережі.
- Використання відомих протоколів для безпечного обміну даними, таких як SSH (Secure Shell) для віддаленого доступу.

1.3.6. Багатофакторна аутентифікація:

- **Використання паролів, біометричних даних, токенів**: Забезпечує додатковий шар безпеки, вимагаючи кілька методів аутентифікації.

1.3.7. Захист від атак типу «людина посередника» (Man-in-the-Middle):

- **Використання криптографічних ключів**: Забезпечує надійний обмін ключами та захист від перехоплення атаками.

1.3.8. Регулярні оновлення безпеки:

- **Оновлення програмного забезпечення**: Забезпечує виправлення вразливостей та збереження високого рівня безпеки.

1.3.9. Цифровий Підпис:

- Застосовується для підтвердження автентичності та цілісності даних.
- Алгоритми, такі як RSA, використовуються для створення цифрових підписів.

Шифрування та методи криптографії важливі для забезпечення високого рівня безпеки інформації в сучасному цифровому середовищі, особливо у військових, фінансових та інших критичних секторах.

Супутникові комунікації грають критичну роль у забезпеченні надійного та глобального зв'язку, зокрема в військових операціях, де доступність інформації та зв'язку є важливою для успішного ведення операцій.

Висновки. Застосування інформаційних технологій у військовій сфері сприяє покращенню ефективності, точності та безпеки військових операцій. Однак, разом із цим, це також вносить нові виклики, пов'язані з кібербезпекою та етичними питаннями, які потребують уважного розгляду.

Література

1. «Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners» by Jason Andress, Steve Winterfeld.
2. «Information Warfare: Chaos on the Electronic Superhighway» by Winn Schwartau.
3. «Satellite Communications Systems: Systems, Techniques and Technology» by Gerard Maral, Michel Bousquet.
4. «War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century» by David Patrikarakos.

Лазуренко С. О.

здобувач вищої освіти факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

Федчак І. А.

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЗАСТОСУВАННЯ МЕТОДУ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ (OSINT) У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Як відомо, усі сфери суспільних відносин уражені проявами злочинності, і такий стан справ спостерігається в усіх країнах світу. І хоча практика діяльності правоохоронних органів нараховує багато століть напрацьованого досвіду протидії поширенню злочинності, проте учені та практичні співробітники правоохоронних органів перебувають у стані постійного пошуку новітніх підходів до виявлення злочинної діяльності, застосування яких дозволить досягати максимальних результатів при виконанні своїх службових обов'язків [1, с. 82]. Одним з таких підходів є метод розвідки з відкритих джерел (OSINT), який надає правоохоронним органам засоби для більш швидкого та точного реагування на існуючі загрози, що дозволяє не лише більш ефективно виконувати поточні завдання – реагування на інциденти, а що особливо важливо – дозволяє розвивати проактивність (діяти на упередження).

Різні аспекти використання розвідки з відкритих джерел (OSINT) досліджено у працях Н. В. Жмура та М. П. Землянікіна, О.В. Минько, О. Ю. Іохова, В. Т. Оленченко, К. В. Власова, О. О. Кожушко, Я. М. Жаркова, А. О. Васильєва, К. Ю. Ісмайлова та інших вітчизняних та зарубіжних учених.

В Україні, як і в інших країнах, OSINT використовується в різних сферах для збору інформації, аналізу та прийняття управлінських рішень про застосування ресурсів з метою досягнення максимальних результатів.

Так учений К. Ю. Ісмайлов констатує, що пошук та збір інформації з відкритих та загальнодоступних джерелах в інтересах викриття і розслідування злочинів є актуальним напрямком вдосконалення діяльності правоохоронних органів [2]. Метод розвідки з відкритих джерел (OSINT) в правоохоронній діяльності має широкий спектр напрямків використання, які допомагають правоохоронцям забезпечувати безпеку та здійснювати ефективну протидію злочинності.

Найважливішими напрямками в діяльності правоохоронних органів є пошук підозрюваних, установлення їх зв'язків та місцезнаходження за допомогою соціальних мереж, відкритих баз даних та інших відкритих джерел. Також до напрямів застосування

OSINT у правоохоронній роботі є здійснення моніторингу оперативної обстановки або стану криміногенної ситуації. Застосування OSINT дозволяє здійснювати і упереджувальні (превентивні дії) – спостереження за соціальними мережами та іншими платформами для виявлення можливих злочинних замахів, або загроз громадській безпеці.

У правоохоронній діяльності OSINT відіграє важливу роль і у здійсненні підтримки оперативно-розшукової та кримінальної процесуальної діяльності, зокрема, збір інформації про можливих злочинців, їхні зв'язки та місцезнаходження тощо. Вивчення даних із соціальних мереж дозволяє здійснювати визначення тенденцій, які можуть вказувати на зростання або зміну закономірностей у кримінальному світі.

Використання методу розвідки з відкритих джерел (OSINT) має важливе значення у оперативно-службовій діяльності підрозділів правоохоронних органів. OSINT дозволяє оперативникам отримувати значущу інформацію для встановлення осіб, виявлення, викриття та запобігання злочинній діяльності та більш ефективно реалізовувати управлінську функцію керівниками оперативних підрозділів та органів досудового розслідування щодо використання наявних ресурсів (сили, засоби, технічні можливості, особовий склад, негласне, конфіденційне співробітництво тощо). Нижче наведено деякі аспекти використання OSINT у цій сфері:

- отримання інформації про вчинені злочини або злочини, які плануються;
- отримання відомостей про осіб, які становлять оперативний інтерес, їх зв'язків, способу життя, місць перебування тощо;
- виявлення загроз та ризиків у стані криміногенної ситуації з метою своєчасного застосування превентивних правоохоронних заходів;
- здійснення інформаційно-аналітичної підтримки під час проведення оперативних розробок в межах оперативно-розшукових справ;
- ідентифікація закономірностей, тенденцій, патернів та особливостей в серійній повторюваний злочинності;
- вирішення більш масштабних довгострокових проблем і цілей, для виявлення крупних фігур злочинного світу або синдикатів, прогнозування зростання видів злочинної діяльності і встановлення пріоритетів діяльності правоохоронних органів.

Застосування методу розвідки з відкритих джерел (OSINT) у правоохоронній діяльності є корисним інструментом для правоохоронних органів для моніторингу стану криміногенної ситуації через дослідження відомостей із соціальних мереж. Так, у соціальних мережах часто циркулює інформація, яка становить інтерес для правоохоронних органів, яку можна використовувати для пошуку розшукуваних осіб та осіб, які ухиляються від слідства, суду, відбування кримінального покарання, установлення зв'язків кримінально-активних осіб, пошуку повідомлень про кримінальну активність тощо.

Отже, основна ідея застосування розвідки з відкритих джерел (OSINT) полягає в тому, щоб використовувати інформацію, яка вже існує у загальному доступі, для створення розуміння подій, явищ чи поведінки осіб, або для прогнозування з метою вирішення різноманітних правоохоронних завдань. Метод розвідки з відкритих джерел (OSINT) в правоохоронній діяльності має широкий спектр напрямків використання, які допомагають правоохоронцям забезпечувати безпеку та здійснювати ефективну протидію злочинності.

Важливою частиною OSINT є аналіз отриманих даних. Важливо, щоб зібрані дані були перевірені перед їх використанням в інтересах правоохоронних органів.

Література

1. Федчак І. А. Практичні аспекти вирішення проблем злочинності під час реалізації моделі діяльності поліції, орієнтованої на певну проблематику (Problem-Oriented Policing). Науковий журнал «Juris Europensis Scientia». 2023. № 3. С. 82–85. URL: DOI https://doi.org/10.32782/chern.v3.2023.17
2. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирания оперативної інформації. Південноукраїнський правничий часопис. 2016. № 2. С. 110-113.

Латишев С. О.
курсант факультету № 4 Харківського національного університету внутрішніх справ

НАЛАШТУВАННЯ VPN НА БАЗІ ВІРТУАЛЬНОЇ МАШИНИ GOOGLE

На даний момент Google надає сервіс для створення віртуальних машин, що дозволяє звичайним користувачам скористатися віртуальними середовищами, побудованими на різних операційних системах, та створювати нові проекти без ризику завдати шкоду своєму комп'ютеру або особистим даним.

Google Cloud Platform є комплексом хмарних послуг, які надаються Google на тій самій інфраструктурі, що використовується для їхніх продуктів для кінцевих користувачів, таких як Google Search і YouTube. Ця платформа забезпечує інструменти для управління та різноманітні хмарні послуги, такі як хмарні обчислення, зберігання даних, аналітика і машинне навчання. Для реєстрації користувачам потрібно мати банківську картку або банківський рахунок.

Для того щоб скористатися можливостями сервісів Google, спочатку потрібно увійти в свій обліковий запис Google або створити новий, якщо він відсутній. Після цього потрібно перейти до сервісу Google Cloud, де можна активувати віртуальну машину. Після переходу на відповідну сторінку Google Cloud слід натиснути на кнопку «Get started for free» для безкоштовного використання віртуальної машини на обмежений період часу, оскільки платформа є платною.

Після натискання кнопки відбувається перенаправлення на сторінку для заповнення інформації про обліковий запис. На цій сторінці потрібно обрати країну «Україна» у спадаючому меню «інше». Після ознайомлення з умовами використання продукту Google, потрібно підтвердити свою згоду і перейти до наступної сторінки.

Наступним кроком буде заповнення особистих даних і введення банківської картки, після чого необхідно підтвердити всі дії.

Далі потрібно натиснути на три горизонтальні лінії у верхньому лівому кутку, щоб відкрити список опцій, де обрати «Обчислювальні машини». У цьому розділі слід натиснути «Екземпляри ВМ», після чого розпочнеться процес створення віртуальної машини.

У вікні створення потрібно вказати ім'я машини, регіон і зону, з якої буде братися IP-адреса. У налаштуваннях машини обирається тип і серія інстансу, кількість процесорів та об'єм пам'яті, а також налаштовуються додаткові опції або параметри відповідно до визначених потреб.

Після завершення налаштувань можна перейти до використання віртуальної машини. Щоб створити на її базі VPN потрібно:

1. Налаштувати API, це робиться за допомогою спадаючого списку, та налаштувань Firewall.

2. Після всіх налаштувань потрібно відкрити порти, повернувшись до кроку з трьома горизонтальними лініями, в опціях обрати розділ «Мережа VPC», а в ньому «Брандмауер».

3. На сторінці, що відкрилась, обираємо вкладку «Створення правила брандмауера». В поля вводимо: logs = off, Network = default, Prioriti = 1000, direction = Ingress, Action on match = Allow, Source filters = IP ranges 0.0.0.0/0, Protocols and ports = udp:1194, Endorcement = enabeled.

4. Наступним кроком буде відкриття статичної IP-адреси, після цього треба буде назвати VPN, обрати версію та тип, а зі спадаючого списку регіон.

5. Далі переходимо в SSH, переключимся на root командою «sudo su», наступним кроком вводимо команду «yum install -y wget», завантажуємо VPN на машину ось такою командою: wget https://skiddow.github.io/OpenVPN/openvpn-install.sh.

Тепер виконуємо такі дії:

- командою ls перевіряємо чи завантажився файл;
- вводимо команду bash openvpn-install.sh;
- вводимо нашу статичну IP-адресу;
- вводимо відповідний порт, після чогосервіс дає вибір, який DNS обрати (наприклад, DNS GOOGLE);
- вводимо команду cd та шлях VPN;
- завантажуємо файл з налаштуваннями VPN до віртуальної машини;
- завантажуємо OpenVpn або TunnelBlick, і запускаємо з використанням файлу налаштувань, який був завантажений до віртуальної машини;

Література

1. Платформа віртуалізації Google Cloud Platform. URL: https://cutt.ly/0wANkn0n

Левчук Р. П.
курсант Харківського національного університету внутрішніх справ

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В НАВЧАЛЬНИХ ПРОГРАМАХ В ОСВІТНЬОМУ ПРОЦЕСІ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ СИСТЕМИ МВС УКРАЇНИ

Інноваційні технології у викладанні професій з високим рівнем ризику в системі МВС України є важливим аспектом підготовки працівників Національної поліції. Для забезпечення ефективної підготовки поліцейських до роботи в умовах високого ризику використовуються різноманітні інноваційні підходи та технології.

Одним з таких підходів є використання симуляційних тренажерів. Ці тренажери дозволяють поліцейським набувати практичні навички у віртуальному середовищі, що допомагає зменшити ризик для навчального персоналу та забезпечує можливість відтворення реальних ситуацій. Такі тренажери можуть бути використані для навчання таких професій, як переговори з заручниками, реагування на терористичні акти, розслідування злочинів тощо [1].

Крім того, використання відео- та аудіоматеріалів є ще одним інноваційним підходом у викладанні професій з високим рівнем ризику. Ці матеріали можуть включати записи реальних подій, інтерв'ю з досвідченими поліцейськими, аналіз

ситуацій тощо. Вони допомагають студентам отримати більш глибоке розуміння професії та набути необхідних навичок [2].

Також, використання інтерактивних методів навчання, таких як групові дискусії, рольові ігри, кейс-стаді, сприяє активному залученню студентів до навчального процесу та сприяє розвитку їхніх аналітичних та прийняття рішень навичок [1].

Інноваційні технології у викладанні професій з високим рівнем ризику в системі МВС України є важливим кроком у покращенні підготовки поліцейських. Вони допомагають студентам набути необхідні знання, навички та вміння для ефективного функціонування в умовах високого ризику. Переваги симуляційних тренажерів у навчанні поліцейських з високим рівнем ризику можуть бути наступними: Симуляційні тренажери дозволяють поліцейським відпрацьовувати складні ситуації з високим рівнем ризику без реальної загрози для їх життя та здоров'я. Це дозволяє їм набути необхідного досвіду та навичок без реальних наслідків [1].

Симуляційні тренажери можуть точно відтворювати різні ситуації, з якими поліцейські можуть зіткнутися у реальному житті. Це дозволяє їм набути практичний досвід та виробити правильні реакції на різні сценарії.

Симуляційні тренажери дозволяють поліцейським відпрацьовувати одну й ту саму ситуацію кілька разів, що дозволяє їм вдосконалювати свої навички та стратегії дій. Вони можуть аналізувати свої помилки та вдосконалювати свої навички для досягнення кращих результатів.

Симуляційні тренажери дозволяють поліцейським ефективно використовувати свій час та ресурси. Вони можуть відпрацьовувати різні сценарії та ситуації без необхідності організації реальних тренувань або використання додаткових ресурсів. Також важливим аспектом є оцінка та зворотний зв'язок симуляційні тренажери дозволяють поліцейським отримувати об'єктивну оцінку своїх дій та реакцій. Вони можуть аналізувати свої помилки та вдосконалювати свої навички на основі зворотного зв'язку, що дозволяє їм стати більш ефективними та компетентними [1]. У зв'язку з специфікаю професії важливим є розвиток стресостійкості симуляційні тренажери дозволяють поліцейським відпрацьовувати дії та приймати рішення в умовах стресу. Це допомагає їм розвивати стресостійкість та здатність до ефективного функціонування в складних ситуаціях.

Інноваційні технології виконують важливу роль у викладанні професій з високим рівнем ризику, особливо в контексті системи МВС України. Впровадження передових методів та технічних рішень в освітній процес дозволяє не лише підвищити якість навчання, але й забезпечити максимальний рівень безпеки та ефективності в підготовці військовослужбовців.Застосування інноваційних технологій, таких як віртуальна та розширена реальність, електронні тренажери, системи симуляції та автоматизації, дозволяє створювати навчальні сценарії, які максимально наближені до реальних умов високоризикових ситуацій. Це надає студентам можливість отримати практичні навички та досвід, не виходячи за межі безпечного навчального середовища.

Література

1. Науковий вісник – Дніпропетровського державного університету внутрішніх справ. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/10/3/nv_3-2023-276-283.pdf
2. KhNUIAIR Home. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/e1f94901-17f7-4a5b-ab25-eff53a74df5e/content

Лозинський Ю. Р.
доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук

ІНФОРМАЦІЙНА СКЛАДНА ЕКОНОМІЧНОЇ БЕЗПЕКИ

Важливою якісною відмінністю сучасного етапу соціально-економічного розвитку України можна назвати загальну інформатизацію, що визначено у Національній програмі інформатизації [1]. Оскільки накопичення, обробка та використання інформації відіграє важливу роль у нормальній роботі та розвитку підприємства, установи і організації, вона стала одним із основних ресурсів управління. Необхідно захищати джерела інформації, методи обробки, інформаційні ресурси від несанкціонованого доступу та модифікації.

Захищена інформація створює умови для більш вигідних контрактів із субпідрядниками, дає компаніям значно вищий рівень конкурентоспроможності та збільшення доходів. Цим встановлюється та підтверджується роль ефективної системи захисту інформації у створенні умов економічної безпеки.

На даний момент немає загальноприйнятого визначення понять «економічна безпека» та «інформаційна безпека». Критерії визначення залежать від середовища, в якому проводиться аналіз використанням. Однак зазначені терміни розкриваються в Стратегіях інформаційної і економічної безпеки України [2; 3].

При виділенні загальних рис різних визначень понять можна уявити їх так:

- захист суб'єктів інформаційних відносин (інтереси яких зачіпаються при створенні та функціонуванні інформаційної системи) від можливого завдання відчутного матеріального, фізичного, морального або іншого збитку за допомогою випадкового або навмисного несанкціонованого втручання в процес функціонування об'єктів інформатизації або несанкціонованого використання;
- забезпечення дотримання вимог законодавства, керівних і нормативних документів та загальної безпекової політики;
- забезпечення працездатності підсистеми інформаційної безпеки. Економічна безпека – стан середовища діяльності підприємства, в якому інформація захищена від негативних дестабілізуючих факторів зовнішнього та внутрішнього середовища, здатних вплинути на здійснення соціально-економічних функцій та інтересів. Інформаційна безпека – стан інформаційного середовища підприємства, в якому інформація захищена від негативних дестабілізуючих факторів зовнішнього та внутрішнього середовища, здатних вплинути на збереження основних властивостей наявної інформації;
- забезпечення вимог і умов цілісності та конфіденційності інформації, що циркулює в системі.

Об'єктивна необхідність створення системи інформаційної безпеки пов'язані з багатьма чинниками. Першим чинником є зростання інформації в бізнес-діяльності.

В умовах інформаційного суспільства інформаційні технології широко використовуються у виробництві, наприклад, при поступовому переході від паперових до цифрових робочих процесів. Швидкий розвиток інформаційних технологій призводить до того, що комплексні інструменти та інтеграція комп'ютерів у мережу значно полегшують обробку завдань, обмін інформацією та доступ до неї.

Простота доступу поширюється на конкурентів на ринку та інших людей, які можуть використовувати інформацію компанії з незаконною метою. Інформація завоювала економічну роль – стала джерелом, товаром та послугою. У секторі генерації інформації завдання інформаційної безпеки стають ще важливішими. Ці чинники призвели до значного зростання інтересу підприємств, установ і організацій щодо створення інтегрованих систем інформаційної безпеки.

На підприємстві, в установі і організації, які не використовує хоча б один із методів захисту інформації, створюється сприятлива обстановка для виникнення загроз – подій, дій, процесів, явищ, результатом яких може стати втрата конфіденційності, цілісності або доступності інформації.

Загрози інформаційної безпеки можна класифікувати відповідно до залученого аспекту інформаційної безпеки, задіяної частиною інформаційної системи, наміром, з яким виникає загроза та іншими характеристиками, що не часто використовуються.

Засоби захисту від загроз – розкриття конфіденційної інформації включають несанкціонований доступ до баз даних, прослуховування та інші технологічні процеси. Реалізація цих загроз дозволяє зловмисникам реалізувати: розголошення – навмисні чи необережні дії працівників, які призвели до ознайомлення з конфіденційною інформацією не допущених осіб; витік – безконтрольний вихід конфіденційної інформації за межі установи або кола осіб, яким вона була довірена; несанкціонований доступ – протиправне навмисне ознайомлення з конфіденційною інформацією недопущених осіб.

Порушення цілісності та доступу до інформації, що захищається. Несанкціонований доступ є найбільш поширеним типом комп'ютерної загрози полягає в отриманні користувачем доступу до об'єктів, які він не авторизував відповідно до політик безпеки, прийнятих в установі.

Залежно від характеру впливу несанкціонований доступ є активним впливом використання системної помилки. Будь-який об'єкт у системі може бути несанкціонованим доступом. Несанкціонований доступ може бути реалізований стандартними та спеціально розробленими програмними засобами.

Розголошення конфіденційної інформації може завдати значної матеріальної та моральної шкоди установі, в якій функціонує інформаційна система та користувачам. Багато чинників і умови, створюють передумову та можливість неправомірного заволодіння конфіденційною інформацією, випливають із недоліків керівників та працівників установи.

Заходи захисту інформації є багатогранними і зачіпають відразу кілька типів загроз інформаційній безпеці. До таких заходів належать: шифрування інформації; використання антивірусного програмного забезпечення; використання систем багатофакторної автентифікації, що мінімізують ймовірність несанкціонованого доступу до акаунтів; використання послуг «білих хакерів»; проведення перевірок і стрес-тестів різних компонентів інформаційних систем; навчання персоналу основним методам інформаційної безпеки та роботи з інформаційними системами, що дозволяє запобігти можливим людським помилкам та атакам комуніканта-реципієнта.

Що стосується великих компаній, постійне підвищення рівня загроз створює необхідність захищатися за всіма напрямами. В останні роки стало популярним використання в інформаційних атаках об'єктів Інтернету речей, коли кожна підключена до мережі кавоварка або холодильник стають потенційним джерелом DDoS-атак.

DDoS-атака – хакерська атака на обчислювальну систему з метою довести до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів (серверів), що надаються, або цей доступ буде утруднений.

Способи захисту від DDoS-атак: зменшення зон доступних для атаки. Одним із методів нейтралізації DDoS-атак є: зведення до мінімуму розміру зони, яку можна атакувати; план масштабування; відомості про типовий та нетиповий трафік; розгортання брандмауерів для відображення складних атак на рівні додатків.

Для забезпечення інформаційного захисту даних, що зберігаються та передаються технічними засобами, використовують: автентифікацію; регламентування доступу до об'єктів; систему шифрування файлів; ключі; безпечні з'єднання.

Інформаційна безпека є складовою системи економічної безпеки реальної економіки. Забезпечення надійної економічної безпеки є необхідною умовою переходу до моделі сталого розвитку не лише окремих підприємств, установ і організацій, а й усієї національної економіки, що відображено у Національній економічній стратегії на період до 2030 року [4].

Література

1. Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text
2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
3. Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки»: Указ Президента України від 11.08.2021 р. № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text
4. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.3021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text

Магеровська Т. В.

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

Селеші А. Й.

курсант факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

АНАЛІЗ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ ФОТОРОБОТУ

Фоторобот – це графічне зображення спогадів одного чи кількох очевидців про обличчя людини. Такі композиції обличчя широко використовуються поліцією під час розслідування злочинів. Ці зображення застосовуються для реконструкції обличчя підозрюваного із надією впізнати їх.

Створення фотороботів для поліції зазвичай включає в себе використання спеціалізованих програм та технологій, які можуть допомогти відтворити обличчя потенційного злочинця на основі описів свідків. Розглянемо найбільш поширені із них.

Найбільш давній метод – це ручний малюнок, який досі застосовується у певних ситуаціях. Для побудови фоторобота зазначеним способом необхідна наявність спеціально навченого художника, який співпрацює із слідством і можливість свідка детально описувати підозрюваного.

Користуються популярністю системи, які покладаються на вибір окремих рис обличчя людини. Ці риси вибираються по черзі з великої бази даних, а потім «накладаються», щоб створити цілісне зображення. Такі системи спочатку були механічними, використовували креслення або фотографії, надруковані на прозорих аркушах, які можна було накладати один на одного для отримання комбінованого зображення. Першою такою системою був «Identikit» на основі малюнків, який був представлений у США в 1959 році. Система, заснована на фотографіях, «Photofit», була представлена у Великобританії в 1970 році [1]. Механічні варіанти даного підходу втратили актуальність і більше не застосовуються. Наразі найбільш поширений підхід, який полягає в тому, щоб покладатися у питанні вибору рис на програмні інструменти, які дозволяють точно контролювати створені зображення [2]. Такі системи включають SketchCop FACETTE Face Design System Software, Identi-Kit 2000, FACES, E-FIT і PortraitPad.

Негативною стороною наведених програм є те, що вони вимагають багато втомливої і трудомісткої ручної роботи. З іншого боку, вони можуть бути застосовні без наявності значних спеціальних знань чи вмінь.

Багатообіцяючою альтернативою є програмні методи, які безпосередньо реконструюють зображення, базуючись на активності мозку, що записується, коли користувачі дивляться на ретельно продумані візуальні стимули [3] [4]. Однак вимірювання активності мозку є непрактичним для більшості систем реального світу, враховуючи те, що потребує дорогого та спеціального обладнання, а також операторів, навчених за визначеними складними програмами. Цей метод є детальним і результативним, але важкодоступним у реальних умовах на теперішній стадії розвитку інформаційних технологій і бюджетів, що можуть витрачатись на розслідування злочинів. Тому наразі є експериментальним.

З іншого боку, частину мозкової діяльності організму людини, а саме погляд, можна зафіксувати, виміряти і оцінити за певними критеріями із використанням візуальних стимулів достатньо легко. Для цього використовуються готове обладнання, яке нещодавно стало значно доступнішим і може бути використаним також неспеціалістами. Для користування ним потрібно лише ознайомлення, без детального і довгого навчання. Було розпочато дослідження пошуку уявних образів на основі погляду людини [5], а також візуальної реконструкції [6]. Крім того, було продемонстровано перший метод реконструкції уявного зображення, базуючись виключно на фіксації погляду [7].

Можна здійснити порівняльний аналіз основних методів створення фотороботів для роботи поліції, які існують у наш час і користуються певною популярністю.

Метод / Критерій	**Ручний малюнок**	**Програмний вибір рис обличчя**	**Реконструкція, базуючись на активності мозку**	**Реконструкція на основі погляду людини**
Точність	Висока	Середня	Висока	Висока
Тривалість	Кілька годин, деколи кілька днів	Кілька годин	Кілька годин	Кілька годин
Потребує програмного забезпечення	Ні	Так	Так	Так

Потребує додаткового обладнання	Ні	Ні	Так	Так
Доступність додаткового обладнання	-	-	Невисока	Середня
Потребує навчених спеціалістів	Так	Ні (короткотривале ознайомлення)	Так	Ні (короткотривале ознайомлення)

Можемо бачити, що методи ручного малюнку та програмного вибору рис обличчя мають багато негативних рис, що ускладнюють їх використання у сучасних поліцейських розслідуваннях. Тим не менш, ці методи все ще можуть бути застосовні у випадку дуже обмежених бюджетів, відсутності стиснутих термінів.

Метод реконструкції, що базується на активності мозку, є перспективним, але поки що складним для інтегрування у реальні розслідування. Потрібні додаткові дослідження для зниження вартості цього процесу та його уніфікації, щоб надати можливість користуватись ним неспеціалістам.

Метод реконструкції, що базується на основі погляду людини, стає все більш доступним за рахунок зниження вартості додаткового обладнання і відсутності необхідності тривалого навчання. Наразі він активно досліджується і здійснюються спроби його застосування у більшій кількості поліцейських розслідувань. Він є перспективним способом відтворення рис підозрюваного для розкриття злочинів.

Література

1. Davies, Graham M.; Valentine, Tim «Facial Composites: Forensic Utility and Psychological Research». In Rod C. L. Lindsay; et al. (eds.). Handbook of Eyewitness Psychology. Vol. 2 Memory for People. Mahwah, NJ: Lawrence Erlbaum Associates. Section, «Mechanical Systems». doi:10.4324/9781315805535. ISBN 9780805851526 – via Routledge Handbooks Online (2014).
2. Valentin Schwind, Katrin Wolf, and Niels Henze. FaceMaker - A Procedural Face Generator to Foster Character Design Research, volume Game Dynamics: Best Practices in Procedural and Dynamic Game Content Generation, pages 95–113. Springer International Publishing, Cham, 2017. ISBN 978-3-319-53088-8. doi: 10.1007/978-3-319-53088-8 6. URL http://dx.doi.org/10.1007/978-3-319-53088-8_6.
3. Roman Beliy, Guy Gaziv, Assaf Hoogi, Francesca Strappini, Tal Golan, and Michal Irani. From voxels to pixels and back: Self-supervision in natural-image reconstruction from fmri. In Advances in Neural Information Processing Systems, pages 6517–6527, 2019.
4. Guohua Shen, Tomoyasu Horikawa, Kei Majima, and Yukiyasu Kamitani. Deep image reconstruction from human brain activity. PLoS computational biology, 15(1):1–23, 2019. doi: https://doi.org/10.1371/journal.pcbi.1006633.
5. Xi Wang, Andreas Ley, Sebastian Koch, David Lindlbauer, James Hays, Kenneth Holmqvist, and Marc Alexa. The mental image revealed by gaze tracking. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pages 1–12, 2019. doi: https://doi.org/10.1145/3290605.3300839.

6. Hosnieh Sattar, Mario Fritz, and Andreas Bulling. Deep gaze pooling: Inferring and visually decoding search intents from human gaze fixations. Neurocomputing, 387:369–382, 2020. doi: https://doi.org/10.1016/j.neucom.2020.01.028.
7. Florian Strohm, Ekta Sood, Sven Mayer, Philipp M¨uller, Mihai Bˆace, and Andreas Bulling. Neural photofit: Gaze-based mental image reconstruction. In Proc. IEEE International Conference on Computer Vision (ICCV), pages 1–10, 2021.

Маляренко Д. С.
курсант факультету № 4 Харківського національного університету внутрішніх справ
Рвачов О. М.
старший викладач кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ

СИНТЕЗ МОВЛЕННЯ: ВІД ІННОВАЦІЙ ДО КІБЕРЗЛОЧИННОСТІ

Си́нтез мо́влення (СМ) – це перетворення друкованого тексту на мовний сигнал. Система, яка може виконувати конвертування нормального друкованого тексту на аудіо в реальному часі називається text-to-speech (TTS) [1].

Основним завданням СМ є перетворення будь-якої текстової інформації в акустичний сигнал. З розвитком технологій цифрової обробки сигналів мета дослідження синтезу мовлення еволюціонувала від зрозумілості та чіткості до природності та виразності [2].

Розвиток синтезу голосу – це динамічний процес, що відзначився важливими науковими та технологічними досягненнями протягом останніх десятиліть. Історія цієї галузі охоплює ряд ключових подій і кроків, які допомогли сформувати сучасний синтез голосу [3]. Рішення для синтезу мовлення пропонують полегшений спосіб читання текстових документів зі смартфонів та комп'ютерів.

Технологія СМ допомагає в автоматизації різних процесів, таких як:

- увімкнення мовлення під час передпродажної та післяпродажної роботи, що мінімізує робоче навантаження на людей, скорочує операційні витрати та прискорює пропускну здатність;
- допомога людям, які мають обмежені можливості (особливо людям із вадами зору) та проблеми в навчанні, читанні, включно з порушенням навчання мови.

Прослуховування інформації з використанням функції СМ дає можливість:

- одночасно виконувати різні фізичні завдання, як-от приготування їжі, прибирання, фізичні вправи тощо;
- слухати матеріали під час подорожі та здійснювати переміщення за допомогою голосових підказок від навігатору [4].

Попри чималу користь технології TTS, є негативний аспект – стрімке зростання шахрайських схем зі застосуванням нейромережевого синтезу мови. Зловмисники здійснюють фішингові дзвінки під час яких, наприклад, імітують розмову з родичем, який, нібито, попав у надзвичайну ситуацію та негайно потребує фінансової допомоги.

Шахраї можуть використовувати синтезовані записи голоів керівників та працівників компаній, щоб отримати корпоративну інформацію, яку можна продати конкурентам чи отримати фінансову винагороду за її нерозповсюдження [5; 6].

На теперішній час технології синтезу голосу можуть імітувати тембр та інтонації голосу політиків та інших знаменитостей. Сторонні особи можуть озвучити чужим

голосом що завгодно, будь-який текст, у тому числі те, що власники голосів ні за яких обставин вимовляти не хотіли б – це може спричинити масове невдоволення, конфлікти, тощо [7].

Також зловмисники можуть синтезувати голоси співробітників банків або служб підтримки, щоб обманним шляхом примусити клієнтів таких установ надати доступ до своїх рахунків або іншої конфіденційної інформації [8]. Під час розмови для більшої переконливості шахраї можуть підмінити свій номер телефону на телефонні номери банків, різних державних організацій та великих відомих компаній, використавши можливості сучасної технології телефонії – Session Initiation Protocol (SIP) і Primary Rate Interface (PRI) [9].

Крім того, чимало кіберзлочинців продають послуги віртуальних дикторів. «Комп'ютерні крадії» пропонують потенційним покупцям несанкціоновано, оминаючи норми законодавства про авторські права, скористатись згенерованими за допомогою штучного інтелекту голосами відомих артистів для озвучування текстів.

Висновок: синтез мовлення є важливим для сьогодення, який постійно розвивається і з часом ставатиме лише кращим. Технологія TTS відкриває широкі можливості для доступу до інформації, покращення комунікації, допомозі людям з обмеженими можливостями та в багатьох інших сферах.

Проте на фоні позитивних аспектів використання СМ необхідно враховувати ризики та використання цієї технології для злочинних цілей. Зловмисники активно використовують синтетичні голоси для отримання конфіденційної інформації та неправомірного збагачення.

У майбутньому використання нейромережевого СМ без створення нормативної бази щодо їх використанням назавжди може позбавити роботи дикторів та ставить під загрозу безпеку користувачів інтернет-сервісів.

Безсумнівно, сама технологія синтезу голосу важлива і корисна, але її використання необхідно врегулювати на державному рівні.

З огляду на ці виклики, важливо розробляти та впроваджувати ефективні методи захисту від синтетичних голосових атак, регулювати використання технології для запобігання її незаконному використанню та забезпечити дотримання авторських прав та етичних стандартів. Таким чином, розвиток синтезу мовлення повинен іти пліч-о-пліч із заходами щодо забезпечення безпеки, щоб забезпечити користь використання цієї інновації для суспільства.

Література

1. Учасники проектів Вікімедіа. Синтез мовлення // Вікіпедія : вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Синтез_мовлення
2. Deep Learning Based Speech Synthesis / Y. Ning et al. // Encyclopedia MDPI | Scholarly Community. URL: https://encyclopedia.pub/2975
3. How speech synthesis works // Explain that Stuff : вебсайт. URL: https://www.explainthatstuff.com/how-speech-synthesis-works.html
4. 11 найкращих рішень синтезу мовлення для бізнесу та особистого використання // techukraine.net : вебсайт. URL: https://techukraine.net/11-найкращих-рішень-синтезу-мовлення-дл/
5. Українцям розповіли чому шахраї записують їх голос по телефону // GSMinfo : вебсайт. URL: https://gsminfo.com.ua/32512-ukrayinczyam-rozpovily-chomu-shahrayi-zapysuyut-yih-golos-po-telefonu.html

6. Кушнерик Т. Курйозний злочин. В ОАЕ шахраї пограбували банк, клонувавши голос директора // Главком | Glavcom: вебсайт URL: https://glavcom.ua/economics/finances/kuryozniy-zlochin-v-oae-shahraji-pograbuvali-bank-klonuvavshi-golos-direktora-791319.html
7. Нейромережу навчили говорити голосом Путіна, Познера і Собчак. Відео // Волинські новини : вебсайт. URL: https://www.volynnews.com/news/all/neyromerezhu-navchyly-hovoryty-holosom-putina-poznera-i-sobchak-video-/
8. Шахраї актуалізували схему «дзвінок із банку». Як вберегти свої кошти? // Hromadske | Громадське : вебсайт URL: https://hromadske.ua/posts/nova-shema-obmanu-vid-shahrayiv-u-policiyi-rozpovili-detali
9. Стало відомо, як шахраї роблять підміну телефонного номера // GSMinfo: вебсайт. URL: https://gsminfo.com.ua/31827-stalo-vidomo-yak-shahrayi-roblyat-pidminu-telefonnogo-nomera.html

Мейдич Р. О.
курсант факультету №4 Харківського національного університету внутрішніх справ
Лучик В. Є.
професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, доктор економічних наук

КІБЕРБЕЗПЕКА В СФЕРІ ІНТЕРНЕТ-ОСВІТИ

Через широкомасштабне вторгнення російської федерації на територію суверенної України, заклади до шкільної та середньої освіти були вимушені перейти на дистанційне навчання. Як показує статистика, близько 800 тисяч учнів перейшли з очної форми навчання на дистанційну[1]. Найбільше всього, це торкнулося південних та східних регіонів таких як: Харків, Луганськ, Запорізька та інші прифронтові регіони України [2]. Інші освітні заклади, перейшли або на змішану форму або на очну (звичайну) форму навчання. Але дистанційне навчання може бути і небезпечним. Наприклад, під час дистанційних занять, здобувач освіти, може зайти не на той сайт, або випадково вибрати не справжній сайт (наприклад систему Moodle чи Google Classroom або систему Google meet) та зайти на фішинговий сайт, що може призвести до того, що введені учнем його конфіденційні дані можуть потрапити у мережу або до зловмисників.

Фішинг – це вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані – наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [3].

Крім ризику потрапити на фішинговий сайт, під час дистанційного навчання були виявлені такі проблеми як:

1. Обмежений доступ учнів до інтернету. У деяких регіонах України, особливо в прифронтових, доступ до інтернету є обмеженим або відсутнім. Це може ускладнювати участь учнів у дистанційних заняттях.

2. Відсутність у них цифрових пристроїв. У деяких сім'ях не вистачає коштів на придбання цифрових пристроїв, необхідних для дистанційного навчання. Це може ускладнювати або унеможливлювати участь таких учнів у дистанційних заняттях.

3. Низька мотивація учнів. Дистанційне навчання вимагає від учнів більшої самостійності та самодисципліни. У деяких учнів може виникати труднощі з адаптацією до такої форми навчання, що може призвести до зниження їхньої мотивації до навчання.

Для зменшення ризиків та проблем дистанційного навчання в умовах війни необхідно вжити таких заходів:

1. Просвітницька робота серед батьків та учнів щодо кібербезпеки. Батьки та учні повинні бути поінформовані про ризики фішингу та інших кіберзагроз, а також про способи захисту від них.

2. Забезпечення учнів доступом до інтернету та цифровими пристроями. Уряд та благодійні організації повинні надавати допомогу сім'ям, які не мають доступу до інтернету або цифрових пристроїв.

3. Розробка ефективних методів мотивації учнів до дистанційного навчання. Вчителі повинні використовувати різноманітні методи навчання та мотивації, щоб зацікавити учнів у дистанційному навчанні.

Виконання цих заходів допоможе зробити дистанційне навчання в Україні в умовах війни більш ефективним та безпечним.

Висновки. Для забезпечення якісного дистанційного освітнього процесу слід глибше дослідити цю проблему. По-перше законотворцям прийняти нормативні документи, які будуть регулювати дистанційне навчання. По-друге, для порушників навчального процесу має бути можливість завершення їх участі у конференції з автоматичним повідомленням їх батьків. Бажано також розробити спеціальну програму, яка через блокування чи спеціальний батьківський контроль буде захищати учнів від фішингових сайтів.

Література

1. Самостійне навчання та неадаптовані до онлайну методи викладання: головні проблеми українських шкіл. Освіторія Медіа. URL: https://osvitoria.media/experience/samostijne-navchannya-ta-neadaptovani-do-onlajnu-metody-vykladannya-golovni-problemy-ukrayinskyh-shkil/
2. Яким буде навчання з 1 вересня 2023 в областях України. ФАКТИ ICTV. URL: https://fakty.com.ua/ua/ukraine/20230829-yakym-bude-navchannya-z-1-veresnya-2023-v-oblastyah-ukrayiny/
3. Учасники проектів Вікімедіа. Фішинг – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Фішинг
4. Навчальний проєкт: «Словник неологізмів». Освітній проект «На Урок» для вчителів. URL: https://naurok.com.ua/navchalniy-proekt-slovnik-neologizmiv-277436.html
5. Ketlandia. Маніпуляція. Розсилка від «Ukraine» – це фішинг. 0412.ua - Сайт міста Житомира. URL: https://www.0412.ua/news/3364770/manipulacia-rozsilka-vid-ukraine-ce-fising

Мельник Р. О.
курсант факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

Правові засади застосування оперативно-розшукових заходів регулюються законодавством кожної конкретної країни. Зазвичай, це включає в себе ряд законів і нормативних актів, що визначають, які оперативну діяльність можуть виконувати правоохоронні органи в рамках оперативного роботи та які обмеження і гарантії встановлені для захисту прав та свобод громадян.

Зазвичай, такі правові засади включають в себе наступні аспекти:

1. Законність: Оперативні заходи повинні здійснюватися на підставі чітко визначених законів та з урахуванням конституційних прав громадян.
2. Обґрунтованість: Правоохоронні органи повинні мати підстави для проведення оперативних заходів, такі як наявність підозри або обґрунтованих підстав для втручання в права громадян.
3. Пропорційність: Заходи повинні бути пропорційними меті, яку слід досягти, і не можуть бути занадто інтенсивними або обмежувальними.
4. Конфіденційність: Зазвичай інформація, зібрана під час оперативних заходів, повинна бути конфіденційною та захищеною від несанкціонованого доступу.
5. Судовий контроль: Деякі країни передбачають судовий контроль над оперативними заходами для забезпечення їх законності та обґрунтованості.

Зазначені принципи можуть відрізнятися в різних юрисдикціях, але завжди важливо дотримуватися правових норм та гарантувати захист прав і свобод громадян.

Підстави проведення оперативно-розшукових заходів містяться в Законі України «Про оперативно-розшукову діяльність», а саме тут зазначається, що наявність достовірної інформації, отриманої в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про злочини, що готуються; осіб, які готують вчинення злочину; осіб, які переховуються від органів досудового розслідування, суду або ухиляються від відбування кримінального покарання; осіб безвісно відсутніх; розвідувально-підривну діяльність спеціальних служб іноземних держав, організацій та окремих осіб проти України; реальну загрозу життю, здоров'ю, житлу, майну працівників суду і правоохоронних органів у зв'язку з їх службовою діяльністю, а також осіб, які беруть участь у кримінальному судочинстві, членів їх сімей та близьких родичів, з метою створення необхідних умов для належного відправлення правосуддя; співробітників розвідувальних органів України у зв'язку із службовою діяльністю цих осіб, їх близьких родичів, а також осіб, які конфіденційно співробітничають або співробітничали з розвідувальними органами України, та членів їх сімей з метою належного здійснення розвідувальної діяльності.

Також зазначено, що застосування оперативно-розшукових заходів необхідне коли є: необхідність проведення оперативно-розшукових заходів для виконання доручення, наданого відповідно до КПК України; запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках; потреба в отриманні розвідувальної інформації в інтересах безпеки суспільства і держави; наявність узагальнених матеріалів центрального органу виконавчої влади із

спеціальним статусом з питань фінансового моніторингу, отриманих в установленому законом порядку.

Підстави застосування оперативно-розшукових заходів можуть міститись в заявах, повідомленнях посадових осіб, матеріалах органів дізнання, ухвалах суду в кримінальних провадженнях, що перебувають у його провадженні, у письмових дорученнях і постановах слідчого, запитах повноважних державних органів, установ та організацій, про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках, повідомленнях громадян, вказівках прокурора, повідомленнях громадських організацій, повідомленнях засобів масової інформації, матеріалах інших правоохоронних органів, у запитах і повідомленнях правоохоронних органів інших держав та міжнародних правоохоронних організацій, ухвалах слідчого судді.

З вище викладеного висновуємо, що забороняється приймати рішення про проведення оперативно-розшукових заходів при відсутності підстав, передбачених у ст. 6 Закону України «Про оперативно-розшукову діяльність» [1].

Крім того, працівники оперативних підрозділів виконують вимоги Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному проваджені, в якій зазначається що негласні слідчі розшукові дії проводять тільки уповноважений оперативний підрозділ або уповноважена особа.

Уповноважений оперативний підрозділ − оперативний підрозділ, який входить до складу державного органу, визначеного у статті 246 КПК України [2], залучений за рішенням керівництва органу до здійснення або участі у проведенні негласної слідчої (розшукової) дії.

Уповноважена особа − співробітник (працівник) уповноваженого оперативного підрозділу, залучений за рішенням керівника до проведення або участі у проведенні негласної слідчої (розшукової) дії, інші особи, залучені за рішенням слідчого, прокурора, оперативного підрозділу.

Здійснення оперативно-розшукової діяльності регулюють, крім законів України, підзаконні нормативно-правові акти, серед яких чималу частину складають ті, що мають гриф обмеження доступу або секретності, які із зрозумілих причин у відкритому контексті ми аналізувати не вправі.

Отже, правових засад застосування оперативно-розшукових заходів є багато, та кожна з них необхідна для якісного та законного застосування цих заходів.

Література

1. Про оперативну діяльність: Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
2. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13. URL: http://zakon.rada.gov.ua/laws/show/4651-17

Мельникова Н. І.
професор кафедри систем штучного інтелекту Національного університету «Львівська політехніка», професор кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, доктор технічних наук, доцент
Патерега Ю. І.
аспірант кафедри систем автоматизованого проектування Національного університету «Львівська політехніка»
Басистюк О. А.
асистент кафедри систем штучного інтелекту Національного університету «Львівська політехніка», викладач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

ДОСЛІДЖЕННЯ ВПЛИВУ СОЦІАЛЬНИХ ЧИННИКІВ НА РІВЕНЬ ЗЛОЧИННОСТІ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність проблеми та існуючі рішення

Поняття соціальних чинників несе дуже широкий діапазон факторів, що їх спричиняють. За останні роки світова спільнота пережила катастрофічний вплив на суспільство через агресію пандемії COVID-19, що стала однією з наймасштабніших суспільних подій в останньому десятилітті. Для зупинки поширення даного вірусу органи влади багатьох країн світу вдалися до радикальних заходів, таких як скасування всіх масових заходів, обмеження пересування людей, закриття робочих місць або перенесення їх в мережу, що в свою чергу спричинило нестабільність в економіці та збільшення рівня безробіття, що впливає на інші аспекти життя людей. Зважаючи на ці події рівень злочинності може дуже стрімко змінюватися, як через обмеження пересування людей на вулицях, так і через втрату роботи та неможливість змінити своє оточення бодай на якийсь час. Це частково підтверджується в дослідженні[1], де автори знайшли зв'язок між твітами з агресивним змістом та злочинністю, проаналізувавши існуючі дослідження, зроблено висновок що штучний інтелект широко використовується для роботи із злочинністю у різних сферах: від прогнозування рівня злочинності, як такої залежно від впливу соціальних чинників [2] та прогнозів ризиків скоєння злочинів узагалі або певного виду, що спрямовані проти людей, до економічних [3].

Було розглянуто набори даних та реалізовано їхню обробку перед створенням моделей на дослідженні уже існуючих рішень, що дозволило визначити категорізовану статистику щодо злочинів, у датасетах, як у дослідженні [6], де дані просто структуровані за типом злочину, кількістю випадків злочину, які сталися в певний проміжок часу, так і додаткові дані, наприклад статистика по вихідних. Якщо дані містять просторовий вимір, то автори обов'язково розбивають весь регіон на сітки із певним кроком для структуризації даних за ним. Задля створення більш точної моделі автори дослідження можуть додавати такі дані як інформацію про погоду, дзвінки у міську службу сервісу, або, наприклад, інформацію із соцмереж про спортивні події, як, наприклад, у дослідженні [4], що, в свою чергу, підвищило точність прогнозування.

Методи та засоби дослідження

Розглянуто методи LSTM та її варіації та статистичні моделі як ARIMA/SARIMA/SARIMAX, оскільки вони придатні до використання у задачах по типу Time Series. Брався до уваги перший набір даних для дослідження містить поліцейські звіти за злочини, що відбулися у Лос-Анджелесі за 2020-2022 роки та 608 тис. елементів [5].

date	county	state	fips	cases	deaths
specific date	name of county	specific state	a specific code for counties, this may vary for metro areas	number of cases	total deaths due to COVID-19
21Jan20 – 13May22	1932 unique values	Texas 8% Georgia 5% Other (2184424) 87%	1001 – 78.0k	0 – 2.91m	0 – 40.3k
2020-01-21	Snohomish	Washington	53061	1	0
2020-01-22	Snohomish	Washington	53061	1	0

Рис. 1 Приклад набору даних із статистикою Covid-19

Дані, які одержуємо після роботи моделей, будуть аналогічні - у вигляді масиву послідовних чисел, що означають кількість захворюваності кожного потрібного періоду (щоденні або щотижневі) за часовий проміжок, визначений раніше. Дані візуалізовано на графіку та для них буде обчислена похибка за метрикою MAPE.

Як метрику точності, яку я використовую у своєму дослідженні, я обрав ті, які є пропорційними до даних, наприклад MAPE – (Mean Absolute Percentage Error). Формула даної метрики є наступною –

$$M = = 1\ nt = 1nAt\text{-}FtAt \qquad (1)$$

де A – актуальні дані та F – спрогнозовані. Ця метрика показує результати точності спрогнозованих даних відсотках порівняно з початковими. Найкращий результат похибки – 0. Чим більший результат даної похибки - тим гірше [4].

Результат даної метрики представлений в діапазоні від – 1(негативна кореляція) до 1(позитивна кореляція). Якщо значення є 0 – кореляція відсутня [6].

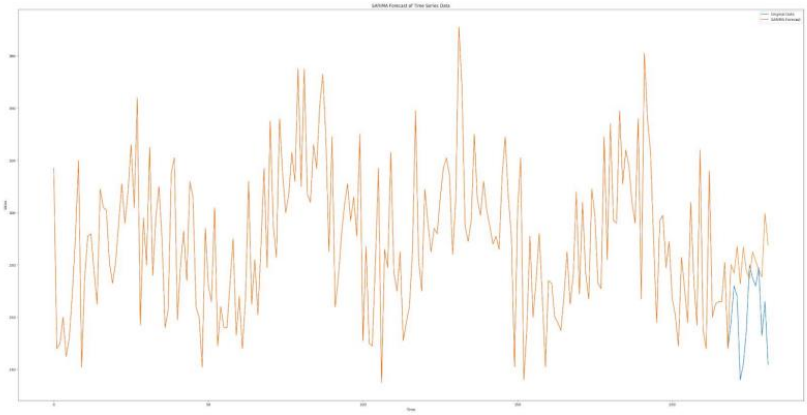

Рис. 2. Графік прогнозу для тижневих даних моделлю SARIMA

Похибка даної моделі – 9%. Застосуємо до тижневих даних модель LSTM. Як довжину послідовності для входу обрано ACF та PACF діаграму. Результат був наступним – похибка моделі – 6%.

Моделі, використані в цій роботі, були запущені з коефіцієнтами, отриманими на попередньому етапі(якщо це статистичні моделі як ARIMA та SARIMA), або без них (LSTM). Дані, які були отримані в результаті їх роботи були візуалізовані та збережені в файл. Також одночасно із вказаними процесами була обчислена похибка за метрикою MAPE. Для обчислення похибки було використано коефіцієнт кореляції Пірсона між різницею спрогнозованих та минулорічних даних за аналогічний часовий проміжок та спрогнозованими даними по Covid-19 використовуючи відповідний засіб бібліотеки numpy.

Рис. 3. Передбачення рівня злочинності із використанням звичайної LSTM моделі на тестових даних.

Таблиця 1. Підсумки отриманих результатів за метрикою MAPE

Модель\Період	Щоденний	Щотижневий
ARIMA	16%	12%
SARIMA	17%	9%
LSTM	18%	6%

Висновки. В результаті дослідження було проведено аналіз взаємозв'язку між рівнем захворюваності на Covid-19 та рівнем злочинності шляхом дослідження кореляції між моделями, що прогнозують рівні злочинності та захворюваності даними просумованими в тижневому проміжку на однаковому часовому проміжку було встановлено, що кількість злочинів, а саме домашнього насильства, зворотньо пропорційна захворюваності на Covid-19.

Література

1. Ashby M. P. J. Initial evidence on the relationship between the coronavirus pandemic and crime in the united states / M. P. J. Ashby // Crime Science. – 2020. – Vol. 9, No. 1. – P. 6.een the coronavirus pandemic and crime in the united states / M. P. J. Ashby // Crime Science. – 2020. – Vol. 9, No. 1. – P. 6.
2. Hou M. Investigating the impact of the covid-19 pandemic on crime incidents number in different cities / M. Hou, Z. Zeng, X. Hu, J. Hu // Journal of Safety Science and Resilience. – 2022. – Vol. 3, No. 4. – P. 340–352.
3. Rosés R. A data-driven agent-based simulation to predict crime patterns in an urban environment / R. Rosés, C. Kadar, N. Malleson // Computers, Environment and Urban Systems. – 2021. – Vol. 89. – P. 101660.
4. Tasnim N. A novel multi-module approach to predict crime based on multivariate spatio-temporal data using attention and sequential fusion model / N. Tasnim, I. T. Imam, M. M. A. Hashem // IEEE Access. – 2022. – Vol. 10. – P. 48009–48030.
5. Esquivel N. Spatio-temporal prediction of baltimore crime events using clstm neural networks / N. Esquivel, O. Nicolis, B. Peralta, J. Mateu // IEEE Access. – 2020. – Vol. 8. – P. 209101–209112.
6. Matijosaitiene I. Predicting safe parking spaces: a machine learning approach to geospatial urban and crime data / I. Matijosaitiene, A. McDowald, V. Juneja // Sustainability. – 2019. – Vol. 11, No. 10. – P. 2848.

Мовчан А. В.
професор кафедри оперативно-розшукової діяльності факультету № 2 ІНФПНП Львівського державного університету внутрішніх справ, доктор юридичних наук, професор
Горошко О. В.
здобувач ступеня доктора філософії з галузі 08 «Право» кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ БАЗИ ДАНИХ ПРОЄКТУ «МІЛЕНІУМ» ІНТЕРПОЛУ У ПРОТИДІЇ ДІЯЛЬНОСТІ ЗЛОЧИННИХ СПІЛЬНОТ

У червні 2020 року набрав чинності Закон України «Про внесення змін до Кримінального кодексу України щодо відповідальності за злочини, вчинені злочинною спільнотою», завдяки якому поліцейські отримали додаткові інструменти для припинення діяльності злочинних спільнот та притягнення до кримінальної відповідальності «злодіїв у законі» [1]. Своєю чергою, Рада національної безпеки й оборони України 14 травня 2021 року запровадила санкції до представників кримінальних угруповань, зокрема до 557 так званих «злодіїв у законі», 542 з яких – іноземці, 15 – громадяни України, а також щодо 111 громадян іноземних держав, які перебували на території України та вважалися кримінальними авторитетами [2].

В умовах військової агресії російської федерації проти України особливої актуальності у протидії діяльності злочинних спільнот та притягнення до кримінальної відповідальності «злодіїв у законі» набуває співробітництво оперативних підрозділів Національної поліції з іншими правоохоронними органами України і міжнародними правоохоронними організаціями, а також організації обміну оперативно-розшуковою інформацією. Зокрема, у рамках проєкту «Міленіум» Національна поліція України співпрацює із 42 державами-членами Інтерполу у боротьбі з транснаціональною євразійською організованою злочинністю з метою попередження поширення та нейтралізації впливових євразійських злочинних угруповань країн Східної Європи та кавказського регіону на території Євросоюзу, які займаються торгівлею наркотиками, людьми, автотранспортом та вогнепальною зброєю, злочинністю у сфері фінансів та легалізацією (відмиванням) злочинних доходів [3].

Адже, як свідчать результати проведеного Європолом опитування SOCTA-2021, мільярди євро незаконних прибутків, отриманих організованою злочинністю в Європейському Союзі, було інвестовано в легальну економіку, всі форми організованої злочинності глибоко впливають на суспільство і мають прямий негативний вплив на повсякденне життя громадян, економіку, державні інституції і верховенство права [4].

Відтак ще у 1999 році Інтерпол розпочав проєкт «Міленіум» для подолання нової загрози транснаціональної євразійської організованої злочинності. З 2015 року команда проєкту «Міленіум» брала активну участь у 13 операціях національних поліцій проти євразійських ОЗГ у Франції, Італії, Португалії та Іспанії. Зазначимо, що проєкт «Міленіум» сприяє країнам-членам Інтерполу обмінюватися процесуальною інформацією, яка допомагає ідентифікувати людей і компанії, що стоять за транснаціональною євразійською організованою злочинністю, на європейському континенті, у Північній Америці та Близькому Сході [3].

Команда проєкту «Міленіум» регулярно проводить оцінку євразійської організованої злочинності на основі інформації, яку надають їй НЦБ Інтерполу. Зокрема,

спеціальна база даних проєкту – Criminal Analysis File (CAF) містить інформацію про персональні та біометричні дані, спільників, належність до злочинних організацій, місця злочинної діяльності та впливу, персональні ідентифікаційні ознаки її членів (татуювання, фізіологічні особливості тощо), так само як і відомості про «злодіїв у законі» (Thieves in Law). CAF надає країнамучасницям зібрані дані про високопоставлених членів російськомовних ОЗГ, якими правоохоронні органи можуть користуватись у своїй службовій діяльності [3].

Ще у травні 2018 року на міжнародній зустрічі учасників проєкту «Міленіум», яка відбулась у Львові, пріоритетними напрямами своєї діяльності Україна визначила посилення взаємодії з державами – учасницями проєкту в протидії організованій злочинності. Зокрема, у рамках зустрічі розглядалися питання обміну інформацією про осіб із статусом, який ще не було криміналізовано в українському законодавстві – «злодіїв у законі», лідерів та членів злочинних угруповань, об'єднання зусиль країн щодо протидії організованій злочинності. На практиці правоохоронці не розкривають інформацію про внесення особи у базу проєкту «Міленіум», у зв'язку з чим адвокати стикаються з проблемами в отриманні інформації про наявність даних щодо свого клієнта в базі проєкту. Зазначену інформацію можна отримати лише шляхом звернення до Комісії з контролю за файлами Інтерполу із запитом на розкриття інформації (Request for access) про особу [3].

На початку 2021 року команда проєкту «Міленіум» почала тісно співпрацювати з Центральним офісом боротьби зі злочинністю (OCLDI) жандармерії Франції над операцією, спрямованою проти «злодіїв в законі», обмінюючись інформацією та досвідом. «Злодії в законі» часто знаходяться на вершині кримінальної ієрархії, мають значний вплив і контроль над злочинними групами, що здійснюють торгівлю наркотиками, вимагання, вбивства на замовлення та відмивання грошей. Російськомовні ОЗГ походять з різних країн, зокрема з Вірменії, Грузії, росії та України. Як і інші організації в стилі мафії, «злодії в законі» підривають економіку по всьому світу, інвестуючи злочинні доходи в легальні фонди та бізнес, розширюючи свої важелі впливу в певному секторі економіки. Здійснюючи внески до спільного багатомільярдного кримінального фонду, відомого як «общак», яким керують найвпливовіші та високопоставлені члени злочинного співтовариства, вони інвестують злочинні кошти в акції, нерухомість та компанії [5].

Врешті співпраця досягла кульмінації у квітні 2021 року, коли правоохоронні органи в ході одночасних поліцейських операцій в Ліоні, Нансі та Парижі заарештували 25 підозрюваних, вилучили транспортні засоби класу люкс, понад 300 тисяч євро готівкою та банківські рахунки, а також документи, що свідчать про злочинний фонд. Інтерпол надавав оперативну підтримку протягом всієї операції у формі Групи підтримки Інтерполу (IST), до якої на запит країни-члена входить спеціалізований персонал із Генерального секретаріату Інтерполу. 21 червня 2021 року понад 100 французьких офіцерів за підтримки проєкту «Міленіум» IRT розпочали серію скоординованих рейдів у Страсбурзі та Нансі. Ватажки двох різних кланів «злодіїв у законі», грузинського та вірменського, були заарештовані разом із 10 іншими особами. Під час рейдів поліція вилучила транспортні засоби, зброю, запаси нелегальних сигарет, алкоголю та парфумів, а також понад 17 тисяч євро готівкою [5].

Найчастіше українські правоохоронці використовують відомості з бази даних проєкту «Міленіум» для проведення оперативно-розшукових або контррозвідувальних заходів, у ході яких можуть обмінюватись оперативною інформацією з правоохоронними органами іноземних країн. Наслідком таких заходів, наприклад, може стати заборона іноземцю в'їзду в Україну або ж, навпаки, заборона громадянину України в'їзду на територію інших країн.

Література

1. Про внесення змін до Кримінального кодексу України щодо відповідальності за злочини, вчинені злочинною спільнотою: Закон України № 671-IX від 04.06.2020 URL: https://zakon.rada.gov.ua/laws/show/671-20#Text
2. Монастирський назвав три країни, звідки найчастіше приїжджали в Україну «злодії у законі». URL: https://www.ukrinform.ua/rubric-society/3348564-monastirskij-nazvav-tri-kraini-zvidki-najcastise-priizdzali-v-ukrainu-zlodii-u-zakoni.html
3. Project Millennium helps countries identify the people and companies behind transnational Eurasian organized crime URL: https://www.interpol.int/Crimes/Organized-crime/Project-Millennium
4. EUROPOL. EU Serious and Organised Crime Threat Assessment 2021. A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime URL: https://www.europol.europa.eu/
5. 28 арештів у Франції та Іспанії проти головного «злодія в законі» URL: https://www.europol.europa.eu/media-press/newsroom/news/28-arrests-france-and-spain-hit-chief-%E2%80%98thief-in-law%E2%80%99

Мовчан А. В.

професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

Рішко В. В.

здобувач ступеня доктора філософії з галузі 08 «Право» кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ З ТОРГІВЛЕЮ ЛЮДЬМИ, В УМОВАХ ВОЄННОГО СТАНУ

На сьогодні, в умовах воєнного стану, ризик потрапляння в ситуацію торгівлі людьми як всередині України, так і за її межами став ще більшим. Якщо раніше поняття «торгівля людьми» охоплювало здебільшого сексуальне рабство, то сьогодні воно увібрало широкий спектр форм: від трудової експлуатації до нелегальної трансплантації органів. Крім того, у ході російсько-української війни з'явилась нова група ризику – вимушені переселенці або внутрішньо переміщені особи із зони бойових дій. Усього з початку війни з України за кордон переміщено понад 11,5 млн українських громадян. Водночас в Україні офіційно зареєстровано 4 867 106 внутрішньо переміщених осіб, а за міжнародними оцінками кількість внутрішніх переселенців перевищує 7 млн громадян. Крім того, станом на 21.11.2023 р. депортовано до рф 19 546 дітей, повернуто всього 387 дітей [1].

За цих умов працівники Національної поліції України протидіють непоодиноким спробам шахраїв обдурити людей, які евакуюються з прифронтових районів і є особливо вразливими, оскільки прагнуть знайти нове житло і роботу. Адже з початку війни продовжує залишатись досить високим ризик потрапляння в ситуацію торгівлі людьми, тому що значна кількість громадян України залишилась без житла, без грошей, без роботи. Відтак існують певні групи ризику, які об'єднують особливо вразливих людей, стосовно яких є висока ймовірність, що вони можуть стати об'єктами цього злочину. Насамперед до цієї категорії слід віднести представників соціально

незахищених і неблагополучних верств населення, які знаходяться у складних життєвих обставинах, зокрема: членів багатодітних родин та малозабезпечених сімей; одиноких матерів; самотніх людей похилого віку; людей з особливими потребами; сиріт, дітей, що позбавлені опіки та піклування, «дітей вулиці»; жертв насильства в сім'ї; безробітних працездатного віку; безпритульних [2].

Зважаючи на існуючі загрози торгівлі людьми, підрозділи Департаменту міграційної поліції Національної поліції України налагодили співпрацю з європейськими партнерами, зокрема під егідою Європолу спільно з правоохоронними органами країн Євросоюзу створено міжнародну інформаційну платформу в режимі 24/7, призначену для проведення спільних перевірок за ознаками можливих фактів торгівлі людьми. Основною метою створення зазначеної платформи є запобігання трафікингу українських біженців, спільне оперативне реагування на повідомлення щодо можливих фактів торгівлі людьми та взаємодія під час ідентифікації жертв торгівлі людьми [3].

Працівники міграційної поліції спільно з координатором протидії торгівлі людьми ОБСЄ та Міжнародною організацією «A21 Україна» проводять роз'яснювальну кампанію серед громадян, які виїжджають за кордон. За допомогою чат-боту «Залишайся в безпеці» @stay_in_safe_ua у месенджері «Telegram» громадяни України можуть дізнатися про ризики торгівлі людьми, правила безпечного працевлаштування, контакти установ, що надають допомогу в Україні та за кордоном, форми торгівлі людьми та законодавство.

Крім того, Україна плідно співпрацює з Міжнародною організацією міграції та іншими партнерами, аби вживати превентивні заходи для протидії торгівлі людьми. Йдеться про інформаційні кампанії на пунктах пропуску на кордоні, розсилку смс українцям на території Європи, створення чат-ботів тощо.

За даними різних міжнародних організацій, кількість переміщених дітей складає понад половину дитячого населення країни. Більше ніж 2 млн дітей переїхали в сусідні країни як біженці та близько 3 млн дітей є внутрішньо переміщеними особами. Розроблений у партнерстві з американською компанією «Find My Parent» мобільний застосунок «Reunite Ukraine» сприятиме пошуку дітей, з якими втрачено зв'язок, за допомогою технологій штучного інтелекту, а також возз'єднанню членів сімей, які були внутрішньо переміщені, змушені виїхати за межі України або незаконно депортовані до рф, білорусі чи тимчасово окупованих територій України [4].

З 18 по 22 вересня 2023 року в Нідерландах за підтримки Європолу було проведено загальноєвропейський онлайн-хакатон проти торгівлі людьми EMPACT, в якому брали участь 85 експертів з різних правоохоронних органів ЄС з 26 країн. Організації, що займаються торгівлею людьми, стають все більш цифровими, а Інтернет стає важливим джерелом злочинної діяльності в цій сфері. Торговці людьми використовують різні методи, щоб заманити вразливих людей і використовувати їх для отримання прибутку. Наприклад, вони все частіше використовують соціальні медіа та онлайн-платформи для вербування жертв для сексуальної та трудової експлуатації, а також для інших форм рабства. Вони використовують кілька підходів для вербування своїх жертв. Одна з них – обман: торговці людьми обманюють жертв брехливими обіцянками кращого життя, освіти, роботи чи шлюбу. Іншим є фальшива пропозиція високооплачуваної роботи за кордоном, яка виявляється високоексплуатаційною роботою з дуже низькою оплатою або взагалі без неї. Торговці людьми також можуть пропонувати імміграційні послуги людям, які хочуть мігрувати, а потім скористатися їхньою вразливістю та експлуатувати їх, коли вони опиняться в чужій країні. Під час хакатону 2023 року учасники досліджували, як збирати оперативні розвіддані на рівні ЄС про веб-сайти та платформи соціальних мереж, де, ймовірно, відбувається вербування українських біженців. Дослідження відкритих джерел показало, що торговці

людьми справді використовують найпопулярніші соціальні медіа-платформи, а також додатки для знайомств і форуми для відгуків. Спроби вербування також часто відбуваються в групах спільнот у соціальних мережах, які створюються на основі географічного походження тих, хто шукає послуги та країни призначення [5].

Отже, зважаючи на потребу в удосконаленні правоохоронної діяльності щодо протидії торгівлі людьми в умовах воєнного стану, Національна поліція України запроваджує передовий досвід діяльності правоохоронних органів зарубіжних країн та міжнародних поліцейських організацій Інтерполу й Європолу стосовно використання новітніх технологій у боротьбі зі злочинами, пов'язаними з торгівлею людьми, у практичну діяльність підрозділів міграційної поліції та навчальний процес закладів вищої освіти МВС.

Література

1. Злочини, вчинені військовими рф під час повномасштабного вторгнення в Україну (станом на 21.11.2023). URL: https://www.npu.gov.ua/news/zlochyny-vchyneni-viiskovymy-rf-pid-chas-povnomasshtabnoho-vtorhnennia-v-ukrainu-stanom-na-21112023
2. «Від початку війни рівень злочинності в Україні знизився», – Ігор Клименко в інтерв'ю Reuters. URL: https://www.npu.gov.ua/news/vid-pochatku-viiny-riven-zlochynnosti-v-ukraini-znyzyvsia-ihor-klymenko-v-interviu-reuters
3. Міграційна поліція під егідою ЄВРОПОЛ створює міжнародну інформаційну платформу для запобігання торгівлі людьми серед українських біженців. URL: https://www.npu.gov.ua/news/torgivlya-lyudmi/migraczijnapolicziya-pid-egidoyu-Jevropol-stvoryuje-mizhnarodnu-informaczijnuplatformu-dlya-zapobigannya-torgivli-lyudmi-sered-ukrajinskix-bizhencziv/
4. «Возз'єднати Україну»: Нацполіція запустила новий мобільний додаток із пошуку зниклих дітей. URL: https://www.npu.gov.ua/news/vozziednaty-ukrainu-natspolitsiia-zapustyla-novyi-mobilnyi-dodatok-iz-poshuku-znyklykh-ditei
5. Цільовий: торговці людьми, які заманюють жертв в Інтернеті. URL: https://www.europol.europa.eu/media-press/newsroom/news/targeted-human-traffickers-luring-victims-online

Мороз А. О.

курсант факультету №4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, доктор економічних наук

СТРАТЕГІЇ ЗАХИСТУ ОСОБИСТОЇ КОНФІДЕНЦІЙНОСТІ ТА ДАНИХ КОРИСТУВАЧІВ В ОНЛАЙН СЕРЕДОВИЩІ

В онлайн-середовищі користувачі стикаються з постійними загрозами для їхньої особистої приватності та даних. Ці загрози можуть надходити від хакерів, державних органів і навіть від самих компаній, які збирають дані користувачів.

Щоб захистити себе в онлайн-середовищі, користувачі можуть використовувати різні стратегії. Деякі з них використовують надійні паролі та двофакторну автентифікацію. Паролі повинні бути складною комбінацією букв, цифр і символів. Двофакторна

автентифікація додатково захищає обліковий запис, надсилаючи код на мобільний телефон користувача.

Особливо потрібно бути обережним з інформацією, яка розміщується в Інтернеті. Ні в якому випадку не можна розголошувати конфіденційну інформацію, а, саме: імена, адреси, номери телефонів, кредитних карток тощо. Анонімні сервіси не вимагають від користувачів реєстрації та не зберігають дані.

Слід також оновлювати програмне забезпечення. Виробники програмного забезпечення регулярно випускають оновлення безпеки, які виправляють вразливості, що можуть бути використані хакерами. Не завадить встановлювати антивірусне програмне забезпечення. Антивірусне програмне забезпечення допомагає захистити комп'ютери від шкідливого програмного забезпечення, яке краде дані користувачів.

Збереження особистої інформації в інтернеті є складним завданням у світі постійних кіберзагроз. Використання унікальних паролів для кожного облікового запису є першим кроком до ефективного захисту, оскільки це ускладнює доступ до всіх аккаунтів при можливому зламі лише одного паролю. Важливо не зберігати паролі у браузері, оскільки отримання доступу до комп'ютера може привести до несанкціонованого входу у всі облікові записи.

Використання VPN на публічних Wi-Fi мережах забезпечує шифрування трафіку, запобігаючи можливе перехоплення даних хакерами. Обережність при встановленні додатків на мобільні пристрої та відмова від програм від невідомих розробників є важливими кроками для запобігання потенційним загрозам.

Ознайомлення з політикою конфіденційності веб-сайтів та додатків перед їх використанням дозволяє розуміти, яким чином дані будуть використовуватися. Необхідно мати на увазі, що жоден метод захисту не є абсолютно надійним, проте дотримання вищезазначених порад може значно знизити ризики витоку особистої інформації та даних в онлайн-середовищі.

Дослідження доводять, що більшість користувачів Інтернету усвідомлюють загрози для своєї приватності, проте не всі вживають належних заходів безпеки. Лише 30% використовують надійні паролі та двофакторну автентифікацію, 50% не приділяють уваги своїм особистим даним в мережі, а 20% не користуються анонімними сервісами, що може привести до загроз для їхньої приватності та безпеки.

Висновки. З метою підвищення рівня захисту особистої приватності та даних користувачів в онлайн-середовищі рекомендується розробити та впровадити ефективні закони та підзаконні акти щодо захисту особистого життя та даних користувачів, підвищувати рівень обізнаності користувачів про існуючі загрози, впроваджувати технічні заходи захисту, які ускладнюють доступ хакерів до особистої інформації та даних користувачів. Окремі стратегії захисту, такі як використання складних паролів, двофакторної автентифікації, уважність при обміні особистою інформацією, оновлення програмного забезпечення та використання антивірусних програм можуть значно зменшити ризики витоку даних та загрози для приватності.

Література

1. Впроваджуємо цифрові інструменти для фіксації воєнних злочинів росії. URL: https://shtab.net/news/view/vprovadzhuemo-cifrovi-instrumenti-dlya-fiksaciji-v/.
2. Дія. Доказ. Як повідомити про воєнний злочин проти українців? URL: https://www.facebook.com/diia.gov.ua/photos/a.196543131750045/767598614644491/?type=3.
3. Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних». URL: https://zakon.rada.gov.ua/go/2297-17.

4. Звіт Європейського агентства з питань мереж та інформаційного суспільства (ENISA) про кібербезпеку в Європі (2023). URL: http://zpd.inf.ua/page12.html.
5. Опитування інтернет-користувачів, проведене Інститутом кібербезпеки України, 2023рік. URL: https://ela.kpi.ua/bitstream/123456789/59588/1/Shpotia_bakalavr.docx.

Мрачковський О. М.
курсант Львівського державного університету внутрішніх справ

КВАНТОВА ТЕХНОЛОГІЯ: ПЕРСПЕКТИВИ РОЗВИТКУ

Квантова технологія - це галузь науки та техніки, яка використовує властивості квантової механіки для створення нових продуктів та послуг. Квантові технології мають потенціал кардинально змінити наш світ, у тому числі в таких сферах, як комп'ютерні науки, хімія, матеріалознавство, медицина та телекомунікації.

Основи квантової технології

Квантова механіка - це теорія, яка описує поведінку матерії та енергії на атомному та субатомному рівнях. Квантові технології використовують такі квантові властивості, як суперпозиція, заплутаність та квантова телепортація.

Суперпозиція – це властивість квантових об'єктів перебувати в двох або більше станах одночасно. Наприклад, електрон може перебувати одночасно у двох різних точках простору або мати два різних значення спіну.

Заплутаність – це властивість квантових об'єктів, за якої їхні стани тісно пов'язані один з одним. Зміна стану одного об'єкта миттєво впливає на стан іншого, навіть якщо вони знаходяться на значній відстані один від одного.

Квантова телепортація – це процес передачі інформації з одного місця в інше без використання фізичного переносу інформації. Квантова телепортація використовує заплутаність для передачі квантового стану одного об'єкта в інший.

Застосування квантових технологій

Квантова технологія має потенціал змінити наш світ у багатьох сферах. Ось деякі приклади можливих застосувань квантових технологій:

- Квантові комп'ютери – це комп'ютери, які використовують квантові принципи для обробки інформації. Квантові комп'ютери можуть вирішувати деякі завдання набагато швидше, ніж традиційні комп'ютери. Наприклад, квантові комп'ютери можуть бути використані для розробки нових ліків, моделювання клімату та створення нових матеріалів.
- Квантові сенсори – це сенсори, які використовують квантові принципи для вимірювання фізичних величин. Квантові сенсори можуть бути набагато точнішими та чутливішими, ніж традиційні сенсори. Наприклад, квантові сенсори можуть бути використані для виявлення хімічних речовин, виявлення витоків і моніторингу стану навколишнього середовища.
- Квантова криптографія – це метод шифрування даних, який використовує квантові принципи для забезпечення безпеки. Квантова криптографія є набагато безпечнішою, ніж традиційна криптографія, оскільки вона не може бути зламана навіть найпотужнішими комп'ютерами.

Перспективи розвитку квантових технологій.

Квантова технологія все ще знаходиться на ранніх стадіях розвитку, але вона швидко розвивається. У міру розвитку квантових технологій ми побачимо все більше застосувань квантових технологій у нашому житті.

Ось деякі перспективи розвитку квантових технологій:

- **Квантові комп'ютери** мають потенціал вирішувати деякі завдання набагато швидше, ніж традиційні комп'ютери. Наприклад, квантові комп'ютери можуть бути використані для розробки нових ліків, моделювання клімату та створення нових матеріалів.

  У міру розвитку квантових комп'ютерів вони стануть все більш потужними та доступними. Це призведе до революції в багатьох галузях, включаючи фармацевтику, виробництво, фінанси та штучний інтелект.
- **Квантові сенсори** можуть бути набагато точнішими та чутливішими, ніж традиційні сенсори. Наприклад, квантові сенсори можуть бути використані для виявлення хімічних речовин, виявлення витоків і моніторингу стану навколишнього середовища.

  У міру розвитку квантових сенсорів вони стануть все більш поширеними. Це призведе до покращення безпеки, охорони здоров'я та навколишнього середовища.
- **Квантова криптографія** є набагато безпечнішою, ніж традиційна криптографія, оскільки вона не може бути зламана навіть найпотужнішими комп'ютерами. Це пов'язано з тим, що квантова криптографія використовує властивості квантової механіки, які не можна змоделювати на традиційних комп'ютерах.

  Квантова криптографія є набагато безпечнішою, ніж традиційна криптографія, оскільки вона не може бути зламана навіть найпотужнішими комп'ютерами. Це призведе до підвищення безпеки в Інтернеті та інших сферах.

  Квантову криптографію можна використовувати для створення безпечних каналів зв'язку, які неможливо перехопити або підслухати. Це може бути використано для захисту конфіденційних даних, таких як банківські рахунки, медичні записи та державні секрети.
- **Квантові мережі** – це мережі, які використовують квантові технології для передачі інформації. Квантові мережі можуть бути використані для створення високошвидкісних та надійних каналів зв'язку.

  Квантові мережі можуть бути використані для створення глобальних мереж, які об'єднують квантові комп'ютери у всьому світі. Це може призвести до створення нових можливостей для співпраці та обміну інформацією.
- **Квантова медицина** – це галузь медицини, яка використовує квантові технології для лікування хвороб. Квантова медицина може бути використана для розробки нових методів лікування раку, хвороб серця та інших захворювань.

Квантова медицина може бути використана для створення нових діагностичних методів, які дозволяють більш точно визначати захворювання. Це може призвести до більш раннього виявлення захворювань та кращого лікування.

Висновок. Квантова технологія – це динамічно розвиваюча галузь науки та техніки, яка має потенціал кардинально змінити наш світ. У міру розвитку квантових технологій ми побачимо все більше застосувань квантових технологій у нашому житті.

Квантова технологія має потенціал вирішити деякі з найскладніших проблем нашого часу, таких як кліматичні зміни, хвороби та безпека. Однак, щоб квантові технології досягли свого повного потенціалу, необхідно подолати ряд викликів, таких як технологічні проблеми, фінансові проблеми та нормативно-правові проблеми.

Література

1. Стаття «The Future of Quantum Computing» в журналі Nature
2. Книга «Quantum Computing for Beginners» від John Preskill
3. Доповідь «Quantum Computing: A Strategic Plan for the United States» від Національної ради з питань науки і техніки

Мусійовська М. М.

старший викладач кафедри комп'ютерних наук та інформаційних технологій Української академії друкарства, доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук

ОРГАНІЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У сфері вищої освіти для формування професійних і загальнокультурних компетенцій майбутніх бакалаврів і магістрів потрібні нові умови навчання. Освіта наразі дещо відстає від загальної діджиталізації, і необхідно докласти більше зусиль, щоб скористатися інструментами та сильними сторонами нових інформаційних технологій, одночасно вирішуючи проблеми щодо можливих зловживань, таких як кібервторгнення та проблеми конфіденційності.

Завдання розвитку законодавства у сфері освіти окреслюються Національною доктриною розвитку освіти, яка визначає систему концептуальних ідей та поглядів на стратегію і основні напрямки роз витку освіти до 2025 р. [2, 3].

Згідно зі Стратегією розвитку вищої освіти в Україні на 2021-2031 роки, в основу концептуальної моделі вищої освіти України має бути покладений кібернетичний принцип необхідного розмаїття [1].

Істотний вплив на впровадження нових інформаційних технологій здійснюють сучасні інформаційні технологічні тенденції, основні з яких такі:

- віртуалізація та «хмарні» технології;
- розширення використання сервісорієнтованих архітектур;
- впровадження мобільних пристроїв та рішень на корпоративному рівні для доступу до ресурсів та виконання корпоративних до атків;
- посилення диференціації користувацьких переваг;
- візуалізація, вебінари та відеоконференцзв'язок [6].

Одним із важливих шляхів забезпечення ефективного функціонування освітньої системи при впровадженні інформаційних технологій у навчальний процес у закладах вищої освіти є створення та використання електронних навчально-методичних комплексів. Усі документи у складі цього інформаційного комп'ютерного продукту – мультимедійні, у них завжди присутні елементи інтерактивності, вони можуть бути оформлені в вигляді набору веб-сторінок. Електронні навчальні комплекси можуть бути використані на лекційних заняттях (проказ відеозаписів, інтерактивних моделей та

анімації), під час проведення лабораторних робіт, атестації та самостійної роботи здобувачів вищої освіти. Таким чином, електронний навчально-методичний комплекс це програмний мультимедіапродукт навчального призначення, що забезпечує безперервність та повноту дидактичного циклу процесу навчання та містить організаційні систематизовані теоретичні, практичні, контролюючі матеріали побудовані на принципах системного підходу, інтерактивності інформаційної відкритості [4].

Щоб підвищити ефективність роботи закладу вищої освіти, потрібно комплексно впливати на систему в цілому стратегію, мережеву інфраструктуру, організаційну структуру, систему управління, систему мотивації до праці, корпоративну культуру. Для вирішення завдання інформатизації закладу вищої освіти необхідно створити його єдину електронну систему, яка б дозволила управляти знаннями, що забезпечило б розвиток інновацій, збільшення продуктивності праці шляхом скорочення часу пошуку потрібного рішення в управлінні та обсягу виконаних робіт, підвищення компетентності персоналу. В результаті користувачі отримають доступ до високоякісної інформації, а самі рішення в галузі інформаційних технологій будуть так задіяні в основні ділові процеси закладу вищої освіти, що персонал і здобувачі вищої освіти вже не зможуть обходитися без сервісів, що надаються інформаційним середовищем. При цьому підвищується ефективність виконання персоналом його посадових обов'язків, підвищується якість навчання здобувачів вищої освіти, що робить інвестиції в інформаційні технології економічно виправданими [4].

Можна виділити такі основні завдання, виконання яких спрямовані на формування єдиної інформаційної системи закладу вищої освіти:

- формування організаційної структури інформатизації;
- створення інформаційної інфраструктури закладу вищої освіти та автоматизація її управління;
- інформатизація процесів управління закладом вищої освіти, зокрема фінансами;
- інформатизація навчального процесу,
- інформатизація наукових досліджень та проектів;
- підвищення рівня компетентності персоналу у сфері інформаційних технологій [5].

При створенні інформаційної системи закладу вищої освіти слід забезпечувати розумний обсяг інновацій як у навчальній, так і в управлінській діяльності. Створення та організація єдиної інформаційної системи закладу вищої освіти – складне організаційне та технологічне завдання, що обумовлює доцільність поетапної розробки системи: розв'язання задачі отримання на кожному етапі закінченого продукту, який послідовно модифікуватиметься та нарощуватиметься від етапу до етапу. Тільки на такій основі може бути забезпечене стійке функціонування інформаційної системи вищої освіти.

Інформатизація вищої освіти в Україні є одним із пріоритетних напрямків реформування вищої школи. На шляху інформатизації навчального процесу важливим є створення, впровадження та розвиток комп'ютерно орієнтованого освітнього середовища на основі інформаційних технологій, систем, мереж та ресурсів.

Це – комплекс перетворень, пов'язаних із насиченням освітньої системи інформаційною продукцією, інформаційними засобами, що грунтуються на мікропроцесорній техніці, та інформаційними технологіями при всебічному використанні можливостей системного підходу як методологічної бази.

Ресурс системного підходу, інтегрованого застосуванням інформаційних технологій у процесі професійної підготовки, позволяє організаторам та учасникам навчального

процесу чітко усвідомлювати взаємозв'язок усіх компонентів освітньої системи та більш ефективно реалізовувати основні її функції: організацію, керівництво, контроль.

Література

1. Міністерство освіти і науки України Стратегія розвитку Вищої освіти в Україні на 2021-2031 роки [Електронний ресурс]. Режим доступу: https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf
2. Президент України Указ № 347/2002. Про Національну доктрину розвитку освіти [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/347/2002#Text
3. Президент України Указ № 344/2013. Про Націонаь стратегію розвитку освіти в Україні на період до 2021 року [Електронний ресурс]. Режим доступу: https://mon.gov.ua/storage/app/media/news/2022/04/15/VO.plan.2022-2032/Stratehiya.rozv.VO-23.02.22.pdf
4. Ватковська М. Г. Формування інформаційної системи управління освітою як етап модернізації інформаційного забезпечення державного управління у галузі освіти України. Актуальні проблеми державного управління. 2015. № 1. С. 124–131.
5. Польгун К. В. Організаційні засади створення електронного освітнього середовища закладу вищої освіти на базі платформи MOODLE. Фізико- математична освіта. 2020. Ч. 1. № 3(25). С. 68-73 [Електронний ресурс]. Режим доступу: https://fmo-journal.fizmatsspu.sumy.ua/journals/2020-325-1/20203-25-Polhun FMO.pdf
6. Cloud Computing: Concepts, Technology & Architecture. by Thomas Erl, Ricardo Puttini, Zaigham Mahmood. [Електронний ресурс]. Режим доступу: https://ptgmedia.pearson cmg.com/images/9780133387520/samplepages/0133387526.pdf

Овдійчук Д.

здобувач вищої освіти факультету №1 ІПФПНП Львівського державного університету внутрішніх справ

Д'яков А. В.

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

ПРОЯВИ КІБЕРЗЛОЧИННОСТІ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Кіберзлочинність є однією з найактуальніших проблем сучасного світу і представляє собою злочинну діяльність, пов'язану з використанням інформаційних технологій та комп'ютерних систем. Це явище є сучасним, оскільки воно почало набирати обертів і ставати серйозною загрозою для суспільства внаслідок розвитку і поширення інтернету, комп'ютерів, мобільних пристроїв та інших технологічних засобів.

Основні аспекти кіберзлочинності включають: хакерство (отримання несанкціонованого доступу до комп'ютерних систем або мереж), фішинг (обман людей та намаганні зламати їхні паролі або викрасти особисту інформацію, шляхом відправки подібних до легітимних повідомлень або веб-сайтів), віруси і малвара (Це шкідливі програми, які можуть встановлюватися на комп'ютери або мобільні пристрої без згоди власника),

кібертероризм (використання кіберзасобів для проведення терористичних атак або ведення інформаційної війни), кіберкрадіжки (використання кіберзасобів для викрадення грошей або цінних ресурсів), спам і шахрайство (надсилання небажаних комерційних повідомлень або спроби обдурити людей для отримання їхніх коштів чи особистої інформації), кібершпигунство (використання кіберзасобів для викрадення конфіденційної інформації від інших країн або організацій).

Кіберзлочинність може призвести до серйозних наслідків, таких як фінансові втрати, порушення конфіденційності, пошкодження репутації та загрози для національної безпеки. Однією з причин її поширення є те, що кіберзлочинці можуть діяти анонімно і використовувати складні технічні методи для ухилення від виявлення та покарання.

Для боротьби з цим явищем влади, компанії та індивіди повинні вдосконалювати свої кіберзаходи безпеки, а також співпрацювати на міжнародному рівні, оскільки кіберзлочинність має міжнародний характер і вимагає спільних зусиль для її запобігання та припинення.

Вирішення проблеми кіберзлочинності вимагає комплексного підходу та спільних зусиль влад, організацій та індивідів. Шляхами вирішення проблеми кіберзлочинності можна визначити наступні заходи:

Заходи по запобіганню: Проактивна політика безпеки є одним з найважливіших аспектів боротьби з кіберзлочинністю. Організації та індивіди повинні приділяти увагу заходам безпеки, встановлювати оновлення програмного забезпечення, використовувати сильні паролі та багатошарову аутентифікацію, а також навчати співробітників та користувачів правилам кібербезпеки.

Нормативно-правові заходи: уряд має розробляти та удосконалювати законодавство, що стосуються кіберзлочинності, і накладати суворі покарання на кіберзлочинців. Законодавство також повинно сприяти співпраці між країнами у справах кіберзлочинності та обміну інформацією.

Міжнародна співпраця: кіберзлочинність має міжнародний характер, і для її боротьби необхідна міжнародна співпраця. Країни повинні спільно працювати над ідентифікацією та припиненням кіберзлочинців і обмінюватися інформацією про загрози.

Кіберзаходи безпеки: організації повинні розробляти та впроваджувати ефективні кіберзаходи безпеки, включаючи моніторинг, виявлення і реагування на інциденти. Технологічні рішення, такі як мережеві брандмауери, антивірусне програмне забезпечення і системи контролю доступу, можуть допомогти захистити комп'ютерні системи.

Вдосконалення освіти: освіта щодо кібербезпеки є важливою для всіх. Організації повинні навчати своїх співробітників, а користувачі повинні бути усвідомлені щодо ризиків та навичок безпеки в онлайн-середовищі.

Кіберполіція: створення спеціальних підрозділів поліції, які займаються кіберзлочинністю і проводять розслідування, може бути ефективним заходом.

Розвиток нових технологій: захист від кіберзлочинності також вимагає розвитку нових технологій, таких як шифрування, інтелектуальний аналіз інцидентів та інші інноваційні підходи до кібербезпеки.

Етичне використання: організації та індивіди повинні дотримуватися етичних стандартів у використанні інформаційних технологій і уникати використання їх для злочинних цілей.

Зрозуміння та своєчасна реакція на загрози кіберзлочинності є надзвичайно важливими для забезпечення безпеки в онлайн-середовищі. Це завдання вимагає постійного оновлення та адаптації до змінюючихся загроз і технологічних розвитків.

Огірко О. І.
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП, кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ВИКЛАДЕННІ ЗАГАЛЬНОГО КУРСУ ВИЩА МАТЕМАТИКА

Сучасна система навчання в закладах вищої освіти трансформується та адаптується до моделі освітнього процесу з використанням сучасних технологій, які дають додаткову можливість використання чогось нового у вивченні курсу, підвищують інтересу до навчання у молоді.

Традиційні методи проведення аудиторних занять з загального курсу «Вища математика» носять досить пасивний характер. Використання інформаційних технологій при проведенні занять, особливо для студентів технічних спеціальностей, активізує процес, привертаючи увагу і сприяючи кращому розумінню матеріалу.

Серед безлічі комп'ютерних систем є багато універсальних математичних пакетів за допомогою яких можна автоматизувати виконання як чисельних так і аналітичних (символьних) обчислень і розрахунків. До комп'ютерних систем, які використовують при викладанні курсу «Вища математика» відносяться:

MathCAD – інтегрована система, яка орієнтована на проведення математичних та інженерно-технічних розрахунків. До переваг пакета відносяться: можливості збереження документів в форматі Webсторінок та Microsoft Word; швидкі і точні чисельні розрахунки у різних предметних галузях; відкритість і розширюваність; підтримку 3D-графіки, що важливо при вивченні розділу «Аналітична геометрія»; сумісність з різними операційними платформами; підтримку роботи з базами даних. Документ MathCAD одночасно є лістингом програми, результатом виконання цієї програми та звітом, який може бути роздрукований на принтері чи опублікований в Web.

Mathematica – система комп'ютерної алгебри компанії Wolfram Research. Містить багато функцій як для аналітичних перетворень, так і для чисельних розрахунків. Крім того, програма підтримує роботу з графікою і звуком, містить розділи для побудови дво- і тривимірних графіків функцій, малювання довільних геометричних фігур, імпорт та експорт зображень і звуку, має вбудовану підтримка паралельних обчислень.

Maple – програмний пакет, система комп'ютерної алгебри (точніше, система комп'ютерної математики). Є продуктом компанії Watcom Products Inc (англ.) рос., яка з 1982 року випускає програмні продукти, орієнтовані на складні математичні обчислення, візуалізацію процесів та моделювання систем. Система Maple призначена для символьних обчислень, хоча має низку засобів і для чисельного вирішення диференціальних рівнянь та знаходження інтегралів. Взаємодіє з CAD-системами, що надає можливість візуалізувати складні об'єкти, створювати креслення на підставі отриманих результатів обчислень та інше. Має власну інтерпретовану мову програмування.

Впровадження інформаційних систем та технологій до організації освітнього процесу буде сприяти здобувачам освіти поглибленню та закріпленню знань, умінь і навичок, формуванню навичок роботи з технологічним інструментарієм, розвитку технологічного мислення, умінь самостійно планувати, алгоритмізувати, стандартизувати своє учіння, формуванню спрямованості та навичок раціонально організовувати самонавчання [1-5].

До основних переваг використання інформаційних технологій при вивчені вищої математики можна віднести:

- скорочення часу на розв'язання задач;

- ознайомлення студентів з роллю та місцем вищої математики в наукових та прикладних дослідженнях, використовуючи доступні комп'ютерні програми;
- отримання навичок математичного дослідження, спрощення процес моделювання;
- вміння оцінювати отримані результати, розвивати математичне мислення та підвищувати загальний рівень математичної культури студентів за допомогою програмних засобів;
- розуміння отриманих знань та навичок для подальшого їх використання у навчанні та в майбутній професійній діяльності.

Література

1. Сидорчук Л.А. Впровадження інформаційних технологій в навчальний процес вищих шкіл. Проблеми педагогічних технологій: Збірник наукових праць Луцьк: 2010. С.280-286.
2. Min-Jeong Choa , Joon Pio Hongb The emergence of virtual education during the COVID-19 pandemic: The past, present, and future of the plastic surgery education. Journal of Plastic, Reconstructive & Aesthetic Surgery 74 (2021) 1413–1421 URL: https://e-tarjome.com/storage/panel/fileuploads/2021-06-26/1624681200_E15479.pdf
3. Огірко О. І. Використання вітруальних технології та технології доповненої реальності в освітньому процесі. Інформаційні технології в освіті та практиці: матеріали Всеукраїнської науковопрактичної конференції. Львів: ЛьвДУВС, 2020. С. 36-38.
4. Хохлова, Лариса Григорівна, and Надія Григорівна Хома. «Використання сучасних інформаційних технологій для викладання вищої математики в умовах заочної форми навчання». РЕДАКЦІНИЙ КОМІТЕТ (2021): 234
5. Інформаційні технології: Системи комп'ютерної математики [Електронний ресурс] : навч. посіб. для студ. спеціальності «Автоматизація та комп'ютерно-інтегровані технології» / І. В. Кравченко, В. І. Микитенко; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 243с.

Оксанишина В. В.

курсант факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

РОЛЬ НЕГЛАСНИХ СПІВРОБІТНИКІВ (АГЕНТІВ) В ПРОВЕДЕННІ ОПЕРАТИВНОЇ РОЗРОБКИ (НА ОСНОВІ ОПРИЛЮДНЕНИХ (ВІДКРИТИХ) МАТЕРІАЛІВ)

Для отримання інформації в ході оперативної розробки необхідно насамперед використати всі резерви оперативної обізнаності, які вже накопичені, особливо матеріали за результатами профілактичної діяльності. Така обізнаність під час оперативної розробки використовується для наступних цілей: а) ідентифікація джерел інформації; забезпечення оперативних розробок агентами шляхом вивчення особливостей зв'язків, що склалися в певних мікрогрупах, і через знання психологічних особливостей і настроїв людей, які потрапляють у поле зору оперативників під час ОРД; здійснення операційних злиттів для досягнення цілей операційних розробок.

При організації таких комбінацій важливу роль відіграє детальне знання відповідного мікросередовища, створених у ньому стосунків, знання ключових людей і вразливих зв'язків у системі зв'язків, яку необхідно розвинути [1, с. 37].

Таке різнобічне використання матеріалів оперативної профілактики для розробки зумовлене тим, що розробляються, і агенти, і особи, які становлять оперативний інтерес, які так чи інакше пов’язані з криміналітетом, тобто з контингентом, щодо яких поширюється вплив оперативної профілактики.

В оперативно-розшуковій практиці ця система взаємовідносин, як правило, засвоюється в процесі контакту агентів з об'єктами розслідування (провадження). У той же час можлива тактика безконтактного збору інформації. Це поняття дуже умовне. Воно було введене як альтернатива існуванню довірчих відносин між агентами та розроблюваними. Якщо такого зв'язку немає, а відтак немає контакту між агентом і розроблюваним. Тільки в цьому сенсі умовне отримання інформації (тільки щодо зв'язку між агентом і розроблюваним) можна назвати безконтактним. Однак це не виключає, а навпаки, передбачає різноманітні контакти агента з людьми з найближчого оточення розроблюваних, які в певній ситуації можуть вільно відвідувати їх житло, спостерігати за їх діями і бути присутніми під час розмов.

Особливу увагу слід приділяти особам, які перебувають у конфліктних стосунках з індивідами, що розвиваються, і які змушені продовжувати підтримувати з ними близькі стосунки, фактично відчуваючи ворожнечу, образу та ненависть. Від таких людей агенти часто отримують надзвичайно цінну інформацію. Однак слід брати до уваги емоційний стан осіб, які передають таку інформацію агентам. Складні емоції (образа, ненависть тощо) впливають на інтерпретацію фактів. У такій ситуації не можна виключати перебільшень, непорозумінь, а часом і свідомих компромісів з боку кривдників та інших осіб, з якими склалися неприязні, ворожі стосунки [2, с. 99].

Працюючи з такими особами, агент дотримується певної дистанції між собою і розробляється особою; у багатьох випадках він може навіть не знати його. Не встановивши довірливих стосунків з об’єктом, агент може під тим чи іншим приводом відвідувати їх вдома і спостерігати за їхніми діями; спілкування з родичами може забезпечити доступ до одягу, предметів, на яких зберігаються сліди злочину, до приміщень, де можуть проводитися обшуки, тощо.

Агенти можуть успішно отримувати інформацію від колег, сусідів, послугами яких користуються розроблювані, і яким вони довіряють у повсякденному житті, оскільки останні часто мають доступ до особистого життя об’єктів оперативної розробки, відвідують їх житло, можуть оглядати цікаві об'єкти, документи, ідентифікувати інші можливі джерела оперативно значущої інформації, не докладаючи для цього додаткових зусиль, а лише використовуючи природно сформовані відносини між ними; можуть розроблятися члени сім'ї, коханці, знайомі. Завданням агента, є крім першочергових завдань, є, також, отримання інформації з других рук.

Відсутність довіри можна і потрібно компенсувати короткими контактами, індивідуальними спостереженнями, «випадковим» прослуховуванням розмов підслідних чи інших осіб, які тією чи іншою мірою знають або здогадуються про злочинну діяльність підслідних. У цьому випадку нерідко велике значення має встановлення факту обізнаності особи про вчинений злочин, обізнаності певних осіб, щодо яких проводиться розслідування, та її реакції на ту чи іншу інформацію [3, с. 111].

Важливо в кожному конкретному випадку визначити роль агента: чи необхідно безпосередньо отримати інформацію, що цікавить, чи лише здійснити певні дії (таємне фотографування, позначення певних об'єктів тощо). Залежно від цього вибирається агент і розробляється програма його поведінки.

Виведення агентів із ризикованих ситуацій або відсутність агентурних можливостей має бути компенсовано залученням до оперативної розробки інших сил, а також додатковими засобами та методами: можливістю особистого розшуку, оперативних установок, негласного спостереження.

Як джерела інформації доцільно використовувати тих осіб із оточення тих, хто розробляється, які в силу налагоджених стосунків або з інших причин можуть, не викликаючи підозр, спостерігати за їхніми діями, бути присутніми під час розмов, фіксувати факти та обставини оперативний інтерес.

Оперативна розробка є основним етапом оперативно-розшукового процесу. Змістом є здійснення оперативно-процесуальних заходів щодо отримання фактичних даних про вчинення (невчинення) злочину особою, яка перевіряється, а мета – підготовка до реалізації в кримінальному провадженні (легалізація).

Підсумовуючи викладене, доводиться констатувати, що проведена нещодавно реформа кримінального процесуального законодавства України визначила суттєві труднощі практичного втілення відповідних правових норм під час здійснення протидії злочинності оперативними підрозділами. Важливою проблемою, що потребує сьогодні вирішення, є повноцінне нормативно-правове забезпечення можливості використання оперативної розробки як важливого інституту оперативно-розшукової діяльності.

Вирішення потребує додаткових нормотворчих заходів із застосуванням комплексного підходу, в основу якого мають бути покладені сучасні досягнення оперативно-розшукової науки та враховані недоліки процесу впровадження нового законодавства у практичну діяльність правоохоронних органів.

Література

1. Притула А. М., Халимон С. І., Митрофанов І. І. Закон України «Про оперативно-розшукову діяльність»: науково-практичний коментар. Хмельницький. Видавництво НАДПСУ. 2021. 236 с.
2. Шинкаренко І.Р. Правові та організаційні основи здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій (структурно-логічні схеми) підрозділами кримінальної поліції: навчальний посібник / І.Р. Шинкаренко, І.О. Шинкаренко, О.В. Кириченко. Дніпропетровськ. ДДУВС. 2016. 224 с.
3. Кримінальний процес: підручник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін. Львів. ЛьвДУВС. 2019. Ч. 1. 532 с.

Оніщенко Є.П.

курсант факультету №4 Харківського національного університету внутрішніх справ

Калякін С.В.

викладач кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ

ЗАХИСТ ІНФОРМАЦІЇ: РОЛЬ КРИПТОГРАФІЇ У СУЧАСНОМУ СВІТІ

Шифрування, що визначає сучасну інформаційну безпеку, стає ключовою галуззю в епоху цифрових технологій, де швидкі темпи технологічного розвитку вимагають надійних засобів забезпечення конфіденційності, цілісності та доступності даних. Шифрування не тільки забезпечує захист електронних комунікацій та інформаційних систем, але і відіграє важливу роль у зміцненні довіри між учасниками цифрового середовища.

У сучасному світі, де обсяг електронного обміну інформацією стрімко зростає, криптографічні протоколи гарантують конфіденційність персональних даних, фінансову безпеку і захист комерційної таємниці.

За допомогою систем шифрування ви можете прогнозувати можливі загрози і уникати ризиків, пов'язаних з несанкціонованим доступом до інформації.

Завдяки розвитку квантових обчислень, важливою стає постійна модернізація криптографічних алгоритмів для забезпечення стійкості перед новітніми технологічними викликами. Такий постійний розвиток дозволяє криптографії залишатися невід'ємною складовою сучасної безпеки, працюючи на благо індивідів, корпорацій та суспільства в цілому.

З розвитком квантових обчислень стає все більш важливим постійно модернізувати криптографічні алгоритми для забезпечення стабільності перед лицем новітніх технологічних викликів.

Цей постійний розвиток дозволяє шифруванню залишатися невід'ємною частиною сучасної безпеки та працювати на благо окремих осіб,підприємств та суспільства в цілому.

Як результат, роль криптографії полягає у створенні надійних механізмів захисту та сприянні сталому розвитку цифрового світу.

Крім того, шифрування відіграє важливу роль у забезпеченні кібербезпеки та захисті від кібератак. Шифрування і цифрові підписи дозволяють перевіряти достовірність інформації, що передається по мережі , і запобігати її модифікацію або підробку .Захищені канали зв'язку та протоколи аутентифікації забезпечують безпеку у віртуальному просторі, де зловмисники постійно шукають уразливості.

Зі збільшенням кількості підключень між пристроями в Інтернеті речей (припинення зв'язку в Інтернеті речей) шифрування використовується для шифрування кількості підключених пристроїв та кількості пристроїв ,якими вони обмінюються.

Наприклад, в області електронної пошти ми використовуємо шифрування для шифрування електронної пошти, щоб забезпечити конфіденційність приватних повідомлень. Популярні протоколи, такі як Pretty Good Privacy (PGP)S/MIME, дозволяють користувачам шифрувати електронні повідомлення та підписувати їх цифровим підписом, захищаючи їх від несанкціонованого доступу та модифікації.

У галузі інтернет-банк декомунізації та електронних фінансових операцій шифрування використовується для створення безпечних каналів зв'язку між користувачами та банками. Протоколи шифрування, такі як SSL (Secure Sockets Layer) і його еквівалент, новітня технологія безпеки транспортного рівня (TLS), дозволяють проводити безпечні фінансові транзакції через Інтернет, зберігаючи при цьому конфіденційність банків.

Наприклад, у галузі технології блокчейн, що використовується в криптовалютах, шифрування використовується для забезпечення безпеки та цілісності транзакцій. Це передбачає використання хеш-функцій для створення унікального підпису в блоці даних у блокчейні Це стійко до змін і гарантує надійність процесу.

З іншого боку, в області Інтернету речей шифрування використовується для переривання зв'язку між підключеними пристроями і захисту їх від несанкціонованого доступу і дезінформації декомунізації.

Шифрування і передача даних по захищених протоколах забезпечує конфіденційність і цілісність інформації, що передається між декомунізованими пристроями Інтернету речей.

У галузі мережевої безпеки шифрування використовується для створення віртуальних тунелів для захисту передачі даних через відкриті мережі, такі як Інтернет. Віртуальна приватна мережа(VPN) використовує шифрування для шифрування з'єднань і забезпечує безпеку під час передачі даних через непатентовану або не надійну мережу.

Роль шифрування також набула важливого значення в області захисту персональних даних. Шифрування файлів на вашому комп'ютері або зберігання паролів у захищеному хеш-форматі є одним із прикладів використання шифрування для захисту особистої інформації.

Крім того, шифрування використовується для забезпечення конфіденційності та інтеграції голосування в системи електронного голосування.

Шифрування гарантує відсутність можливості втручання у виборчий процес і забезпечує надійність результатів. Загалом шифрування відіграє важливу роль у багатьох аспектах сучасного світу, від захисту персональних даних та фінансових операцій до забезпечення безпеки великих мереж та інтернет-платформ. Його реалізація стає важливим фактором забезпечення цифрової безпеки і довіри в сучасному інформаційному суспільстві.

У сучасному світі, де обмін інформацією є неодмінною частиною нашого щоденного життя, захист інформації стає надзвичайно важливим завданням.

Криптографія відіграє визначальну роль у забезпеченні безпеки, конфіденційності та цілісності даних, що циркулюють в цифровому просторі. Її застосування розповсюджується від електронної пошти та онлайн-фінансів до блокчейн-технологій та Інтернету речей, надійно захищаючи інформацію від несанкціонованого доступу та забезпечуючи високий ступінь довіри в цифровому середовищі.

У цілому, криптографія залишається основоположною технологією для збереження довіри та забезпечення приватності в інформаційному суспільстві, і подальший розвиток цієї галузі визначатиме успішну та безпечну інтеракцію в цифровому віці.

Література

1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
2. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC, 2008.
3. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

Питель М. В.

курсант Львівського державного університету внутрішніх справ

ОПТИМІЗАЦІЯ ДАННИХ

Вступ. Оптимізація – це наука про знаходження найкращих рішень для певних задач. Вона використовується в різних сферах діяльності людини, таких як економіка, виробництво, логістика, транспорт, наука, інженерія тощо.

У сучасному світі оптимізація є все більш важливим інструментом. Вона дозволяє підвищити ефективність та продуктивность, а також знайти нові можливості для розвитку.

У цій статті ми розглянемо сучасні методи оптимізації та їхні перспективи розвитку.

Методи оптимізації. Існує безліч методів оптимізації, які можна класифікувати за різними ознаками. Залежно від типу задачі, яку вирішують, методи оптимізації можна розділити на такі групи:

- Методи математичного програмування – це класичні методи оптимізації, які ґрунтуються на використанні рівнянь і нерівностей.
- Методи штучного інтелекту – це методи, які використовують різні алгоритми, засновані на принципах штучного інтелекту.
- Методи комбінаторної оптимізації – це методи, які застосовуються для вирішення задач з великою кількістю варіантів рішень.

Методи математичного програмування. Методи математичного програмування є найпоширенішими методами оптимізації. Вони ґрунтуються на використанні рівнянь і нерівностей, які описують задачу оптимізації.

До методів математичного програмування відносяться такі методи, як:

- Линейне програмування – це метод оптимізації задач, які описуються системою лінійних рівнянь і нерівностей.
- Нелінійне програмування – це метод оптимізації задач, які описуються системою нелінійних рівнянь і нерівностей.
- Дискретно-нелінійне програмування – це метод оптимізації задач, які описуються системою рівнянь і нерівностей, деякі з яких є дискретними.

Методи штучного інтелекту. Методи штучного інтелекту є потужним інструментом для вирішення складних задач оптимізації. Вони використовують різні алгоритми, засновані на принципах штучного інтелекту, таких як навчання машин, генетичні алгоритми, алгоритми мурах тощо.

До методів штучного інтелекту відносяться такі методи, як:

- Нейронні мережі – це методи, які навчаються на наборі даних прикладів і потім можуть використовуватися для вирішення задач оптимізації.
- Генетичний алгоритми – це методи, які використовують принципи природного відбору для пошуку оптимального рішення.
- Алгоритми мурах – це методи, які використовують поведінку мурах для пошуку оптимального маршруту.

Методи комбінаторної оптимізації. Методи комбінаторної оптимізації застосовуються для вирішення задач з великою кількістю варіантів рішень. Вони ґрунтуються на використанні різних алгоритмів, які дозволяють швидко перебрати всі можливі варіанти рішень.

До методів комбінаторної оптимізації відносяться такі методи, як:

- Бінарний пошук – це метод, який використовується для пошуку елемента в масиві.
- Бінарне дерево пошуку – це структура даних, яка дозволяє швидко шукати елементи в масиві.
- Алгоритм Дейкстри – це метод, який використовується для знаходження найкоротшого шляху між двома вершинами в графі.

Перспективи розвитку оптимізації

Оптимізація є активною галуззю досліджень. Вчені постійно розробляють нові методи оптимізації, які дозволяють вирішувати більш складні задачі.

Ось деякі перспективні напрямки розвитку оптимізації:

- Розробка нових методів оптимізації для вирішення задач із невизначеністю.
- Розробка методів оптимізації для вирішення задач з паралельним виконанням.
- Розробка методів оптимізації для вирішення задач із обмеженими ресурсами.

Висновок. Оптимізація є важливим інструментом, який використовується в різних сферах діяльності людини. Вона дозволяє підвищити ефективність та продуктивность, а також знайти нові можливості для розвитку. Сучасні методи оптимізації дозволяють вирішувати все більш складні задачі.

Плевак К. О.
здобувач вищої освіти факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ
Галайко Н. В.
викладач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

ШТУЧНИЙ ІНТЕЛЕКТ В СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

На сьогодні рівень технічного прогресу досяг неймовірних висот, помітно збільшилася його роль у багатьох сферах повсякденного життя. Сучасна людина не уявляє себе без речей наукового прогресу. Штучний інтелект (ШІ) – це одна із галузей, що розвиваються найстрімкіше. Головним напрямком цієї сфери є розробка технологічних рішень, які працюють за принципом людського інтелекту або близько до нього. Штучний інтелект – це область, яка займається розробкою інтелектуальних комп'ютерних систем, тобто систем, що володіють можливостями, які ми традиційно пов'язуємо з людським розумом – це розуміння мови, навчання, здатність міркувати, вирішувати проблеми [1].

Отже, під штучним інтелектом розуміється комплекс технологічних рішень, що дозволяє імітувати когнітивні функції людини та отримувати при виконанні конкретних завдань результати, що дорівнюють результатам інтелектуальної діяльності людини [2].

Однією з найзначущіших тенденцій є впровадження ШІ в бізнес-процеси. Корпорації використовують алгоритми машинного навчання для аналізу даних, прогнозування ринкових тенденцій та підтримки прийняття рішень. Автоматизація завдяки ШІ забезпечує більш ефективне використання ресурсів, оптимізацію ланцюга постачання та підвищення конкурентоспроможності. Компанії використовують алгоритми машинного навчання для зменшення витрат та уникнення зайвого запасу товарів. Tesla, наприклад, використовує системи штучного інтелекту для управління виробничим процесом та планування виробництва автомобілів. За даними Forbes, застосування ШІ в бізнесі може пришвидшити виробничі процеси на 50%, зменшити витрати на 20% та покращити якість продукту на 60%.

Зараз ШІ використовують в маркетингу та рекламі, у кадровому менеджменті, логістиці, виробництві. Наприклад, компанія Amazon інтегрувала ШІ для прогнозування попиту та оптимізації запасів на складах. Це дозволило зменшити час доставки товарів до клієнтів та мінімізувати витрати на зберігання [3]. Фінансові установи використовують ШІ для автоматизації управління портфелем та прийняття інвестиційних рішень. Наприклад, робо-консультанти, як Betterment чи Wealthfront, використовують алгоритми машинного навчання для рекомендацій щодо розподілу активів та оптимізації інвестиційних стратегій. Це дозволяє зменшити витрати та надає індивідуально адаптовані рішення для кожного клієнта.

Багато компаній використовують ШІ для аналізу великих обсягів даних з метою визначення ринкових тенденцій та прогнозування попиту. Наприклад, компанія Netflix використовує алгоритми машинного навчання для рекомендацій фільмів, що дозволяє

персоналізувати вміст для кожного користувача. Такі підходи допомагають підприємствам адаптуватися до змін ринкового середовища та удосконалювати свої стратегії залучення клієнтів.

Для поліпшення клієнтського сервісу набуло значного попиту впровадження інтелектуальних чат-роботів та віртуальних асистентів. Наприклад, компанія Amtrak використовує віртуального асистента для відповіді на питання пасажирів та надання інформації про рейси. Це не лише спрощує обслуговування клієнтів, але й дозволяє компаніям ефективно взаємодіяти з великим потоком запитань та комунікувати індивідуалізовано.

У сфері охорони здоров'я ШІ використовується для посилення точності діагностики, розробки персоналізованих підходів до лікування та виявлення нових методів боротьби з хворобами. Застосування нейромереж і аналізу великих обсягів даних дозволяє точніше передбачати розвиток захворювань та вдосконалює медичні дослідження.

Одним з вражаючих прикладів впливу ШІ в медицині є система IBM Watson for Oncology. Цей інтелектуальний аналітичний інструмент використовується для аналізу великої кількості медичної літератури, клінічних протоколів та пацієнтських записів для надання індивідуалізованих порад щодо лікування онкологічних захворювань. Такий підхід дозволяє лікарям швидше та ефективніше розробляти плани лікування, а пацієнтам отримувати персоналізовані та оптимальні методи терапії.

Ще одним прикладом є використання ШІ в нейрореабілітації, де розробляються ігрові платформи, що використовують техніки машинного навчання для індивідуалізованої реабілітації пацієнтів з різними порушеннями рухової активності. Ці технології полегшують процес відновлення та сприяють розвитку фізичних навичок.

Отже, на сучасному етапі розвитку штучного інтелекту спостерігається його впровадження у різні сфери діяльності людини. Застосування ШІ у бізнесі, медицині та дослідженнях вимагає збалансованого підходу до використання технологій. Розвиток ШІ має великий потенціал, але його вплив має бути здійснений з урахуванням цінностей та інтересів суспільства.

Література

1. Технології штучного інтелекту. URL: https://cit-program.com/artificial-intelligence-technologies/
2. Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України. Державне управління: удосконалення та розвиток. 2022. № 1. – URL: http://www.dy.nayka.com.ua/?op=1&z=2601
3. Штучний інтелект для бізнесу: сфери застосування, ризики та перспективи. URL: https://strategi.com.ua/shtuchnyy-intelekt-dlia-biznesu/

Подубінський І. Б.

аспірант кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

АНАЛІТИЧНА РОБОТА ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ, ЯК СКЛАДОВА ОПЕРАТИВНОГО ПОШУКУ У БЮДЖЕТНІЙ СФЕРІ

Аналітичний пошук може здійснюватися як щодо проблеми в цілому (проблемний пошук), так і щодо конкретної кримінальної ситуації (ситуативний пошук). Перший з них

припускає максимально широке охоплення джерел даних, що стосуються мети пошуку. Ситуативний пошук максимально орієнтований на предмет, збір фактичної інформації для наступної її реалізації у кримінальному процесі.

Оперативний пошук спрямований на виявлення серед значної кількості однорідних об'єктів, саме того, який має ознаки злочинного. Процес виявлення полягає у пошуку ознак злочинної поведінки. Виявлення – це основна пізнавальна діяльність, яка складається із знайдення і розпізнавання певних об'єктів. Виявлення полягає в отриманні, аналізі і перевірці інформації про факти та ознаки злочинної поведінки [1, с.13].

Важливою складовою оперативного пошуку є розпізнання криміногенних процесів та явищ, які виявляються при проведенні оперативно-розшукових заходів. У свою чергу, відмінність аналітичного пошуку від інформаційно-аналітичної роботи оперативного підрозділу в цілому полягає у тому, що остання має на меті збір, збереження, аналіз, оцінку і реалізацію не тільки оперативної, а й іншої корисної інформації, що стосується діяльності оперативного підрозділу. Тому аналітичний пошук є одним із специфічних елементів інформаційно-аналітичної роботи оперативного апарату в цілому.

Інформаційно-аналітична функція передбачає збір, обробку, аналіз і оцінку інформації з метою підвищення ефективності діяльності, вона містить усі дії щодо оперування інформацією. Усі ці дії спрямовані на досягнення однієї мети - створення умов для реалізації інших функцій управління. Розглянута функція відображає природу управління, тому що цілеспрямований організуючий вплив ґрунтується на інформації та її оцінці.

Стратегічні й тактичні цілі втілюються у цільових функціях - прогнозуванні й плануванні.

Під прогнозуванням розуміється наукове визначення ймовірних шляхів і результатів майбутнього розвитку явищ, процесів і подій (формування злочинних організацій, готування та вчинення злочинів тощо), оцінки показників, що характеризують ці явища та процеси для порівняно віддаленого майбутнього. Прогнозування в ОРД є невід'ємною складовою загального передбачення, що поєднує всі різновиди способів отримання інформації про майбутній розвиток подій.

Планування - це обрання цілей і рішень, необхідних для їх досягнення, заздалегідь ухвалене рішення про те, хто, що, коли і як буде робити, процес підготовки на перспективу рішення про те, що, ким, як і коли має бути виконано.

Для виконання заходів, передбачених плануванням, і досягнення бажаного стану об'єкта управління необхідно здійснити низку організаційних функцій: загальноорганізаційну, координаційну, матеріально-технічного забезпечення, фінансово-економічну, обліку й контролю, кадрового забезпечення, політико-правового забезпечення, соціального забезпечення та соціального захисту, мотивації тощо[2, с.160].

Одним з головних місць під час здійснення оперативного пошуку є аналітична робота, тобто дослідження змісту здобутих під час пошуку відомостей шляхом розгляду окремих їх аспектів на предмет наявності в них ознак кримінально значимої події. Для цього вдаються до декодування економічної інформації. Це досягається шляхом застосування спеціальних методик аналізу, зокрема оперативно-економічного та економіко-правового. Зміни в господарській діяльності, як правило, досить повно трансформуються в матеріали обліку, в звітні показники [3].

Працівники обліку, реєструючи господарські операції, відображають хід економічних процесів і матеріалізують це відображення (представляють, кодують його) за допомогою знаків у формі економічних даних (показників). Іншими словами, економічні дані – це кодове, знакове представлення різних відомостей, з яких відображаються економічні процеси. В ході аналізу ці дані співставляються з інформацією, отриманою

з інших джерел, визначається їх відповідність вимогам нормативних актів, що регламентують бюджетний процес тощо.

Наприклад, при отриманні інформації про видання розпорядчого акту, що змінив видатки бюджету, оперативні працівники повинні вивчити документи: бюджет області, міста або району та рішення обласної або районної (в місті) державної адміністрації, які стосуються змін до бюджету. При аналізі таких документів оперативні працівники шукають відповідь на такі запитання:

- яким розпорядникам, в яких розмірах та з якою метою передбачені видатки бюджету?
- за якими статтями та в якому розмірі планувалися надходження до бюджету?
- чи було дотримано виконання бюджету в розрізі кожного розпорядника бюджетних коштів (якщо ні, то через що)?
- який суб'єкт бюджетних правовідносин ініціював внесення змін до відповідного бюджету?
- яким чином була вмотивована пропозиція щодо внесення змін до бюджету?
- чи була дотримана процедура внесення змін до бюджету, яка визначена у законодавстві?

Далі зміст письмових розпоряджень зіставляється з вимогами чинного бюджетного законодавства і у випадку виявлення протиріч між змістом розпорядження та законодавством проводиться ретельна перевірка всіх попередніх розпоряджень цієї службової особи. Підтвердження інформації свідчить про навмисні порушення запланованих видатків з боку конкретної службової особи - розпорядника бюджетних коштів. Тобто пошукова діяльність може включати як епізодичне використання окремих елементів оперативно-економічного аналізу (наприклад, застосування деяких його прийомів), так і проведення такого аналізу для цілеспрямованого дослідження значних обсягів економічної інформації.

Отримання під час оперативного пошуку первинної інформації про факти, наприклад, нецільового використання бюджетних коштів саме по собі не є самоціллю, оскільки значущість інформації визначається можливістю і результатами її використання. Якщо під час її аналізу встановлено оперативно-значимі відомості, що відповідають вимозі достатності і потребують проведення документування, оперативний працівник приймає рішення про заведення ОРС.

Таким чином, проведення оперативного пошуку дозволяє: визначити ознаки латентних злочинів, пов'язаних з порушенням бюджетного законодавства, встановити осіб, які готують, вчиняють або вчинили такі злочини; провести оперативну перевірку отриманої первинної інформації та її аналіз як із застосуванням суто оперативних методів, так і шляхом використання економічного аналізу та аналізу нормативно-правових актів, що регламентують бюджетний процес, отримати підстави для документування фактів протиправної діяльності в межах оперативно-розшукової справи або для оперативно-профілактичного впливу на причетних до цього осіб.

Література

1. Аналітична робота в оперативно-розшуковій діяльності: навчально-практичний посібник / Никифорчук Д.Й., Бусол О.Ю. Бірюков Г.М. – К., 2012. – 152 с.
2. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А.В. Мовчан – Львів. ЛьвДУВС, 2017. – 244 с.

3. Ортинський В.Л., Захаров В.П., Некрасов В.А. Баб'як А.В. Попередження та розкриття злочинів, пов'язаних з порушенням бюджетного законодавства: навч. посібник. – Львів:, ВАТ Львівська книжкова фабрика «Атлас» , 2009. – 198 с.

Поляк С. П.

викладач кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: АСПЕКТИ

Спроба автоматизація усіх форм людської діяльності поклала початок реалізації бурхливих та подекуди ефемерних ідей кібернетиків, математиків, намагаючись об'єктувати їх у конкретних продуктах. Перша та друга промислові революції показали надзвичайну продуктивність виробничих процесів, внаслідок втілення в життя інтелектуальних ідей їх автоматизації за допомогою станків, маниш, замінивши інтенсивні методи промисловості на екстенсивні. Однак, ці процеси все таки ще потребували достатньої фізичної участі людини в управління машинами, що неможливо було без застосування інтелектуальних математичних алгоритмів науковців та спеціалістів. Адже самостійно мислити та приймати рішення на основі аналізу певних даних машини були не в змозі.

Людство переживає чергову промислову революцію: стрибком долаючи 4-й та 5-й технологічний уклади, воно вже вступає до 6-го технологічного укладу, головними рисами якого є революційне удосконалення матеріалів (які служитимуть набагато довше за звичні), скорочення потреб у енергії (завдяки підвищенню енергоефективності), проникнення інформаційних технологій та штучного інтелекту до усіх сфер діяльності, але головне – це стирання границь між галузями знань, галузями виробництва. Відбуватиметься конвергенція нано-, біо-, інфо- та когнітивних технологій. Це вимагає революційних змін на усіх рівнях людської діяльності, зокрема й у вищій освіті: хто зміниться швидше за інших – стане переможцем; хто не зможе переналаштуватися – зникне немов динозаври [1, с. 5].

Існує декілька передумов, що зумовлюють появу Індустрії 4.0. Перша з них це поява у світі величезної кількості доступної інформації і техніки, яка може працювати з цією інформацією. Іншою передумовою можна вважати майже безмежні комунікаційні та інтеграційні можливості. Тобто будь-яка інформація може бути інтегрована з одного пристрою на інший. Поява та розвиток штучного інтелекту є однією з головних причин промислової революції 4.0, а в особливості інтегрування робототехніки у виробничий процес. Ну і останнє це вихід нової технології на комерційний рівень. Наприклад віртуальна реальність, «смарт-одяг» і т.д. [2, с. 184].

Такий розвиток подій однозначно сприятиме і виникненню нових видів правопорушень із використанням штучного інтелекту як кримінального характеру так і тих, що стануть предметом спорів у приватно-правових відносинах, у тому числі щодо порушення чи визнання авторських прав. І найголовніше, що штучний інтелект перебуваючи у протиправних руках перетвориться на інструмент порушення прав людини як природніх так і визначених національними конституціями держав.

Однак погоджуємося з думкою дослідників, що заборона досліджень в сфері штучного інтелекту принципово не може стати дієвою. На відміну від досліджень в сфері ядерної зброї, розробка систем автономного озброєння в рази дешевше, отже є

більш доступною. З розвитком інформаційних технологій дана діяльність ставатиме ще доступнішою, а отримані зразки зброї – ще більш небезпечними. В таких умовах законодавча заборона розробки автономної зброї приведе до ситуації, коли органи безпеки та правопорядку будуть оснащені на порядок гірше ніж злочинці, терористичні організації тощо [3, с. 90-91].

Тому, як і у всьому цивілізованому світі, в Україні також замислюються над регулюванням технології штучного інтелекту. Глобальних досягнень в нормативно-правовій базі поки що немає, однак така перспектива промальовується. До прикладу розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р схвалено Концепцію розвитку штучного інтелекту в Україні, яка визначає пріоритетні сфери, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту. До них зокрема належать: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя. Реалізація Концепції передбачена на період до 2030 року. Враховуючи воєнний стан, ці строки можуть бути скореговані [4].

В цьому самому контексті 7 жовтня 2023 року Міністерство цифрової трансформації України представило дорожню карту з регулювання штучного інтелекту в Україні, що передбачає два етапи:

- на першому, який, як очікується, триватиме 2-3 роки (2023-2025 рр.), бізнесу буде надано можливість для підготовки до регулювання;
- на другому – почнеться регуляторний процес, який передбачає імплементацію закону ЄС про штучний інтелект (AI Act) та розробку національного закону із врахуванням напрацьованого на першому етапі досвіду.

Впровадження Україною регуляторних моделей, запропонованих законом ЄС про штучний інтелект, сприятиме гармонізації національного законодавства у цій сфері. Таке вирівнювання стандартів не лише відповідатиме вимогам ЄС, але й забезпечуватиме вищий рівень безпеки та етичності у розробці систем штучного інтелекту в Україні [5].

Поряд із тим дедалі більше науковців вже розглядають майбутню систему юстиції і правоохоронної діяльності крізь призму нейромереж. Як зазначається, створення даної системи стане необхідною умовою для того, щоб забезпечити людству можливість контролювати розвиток суспільних процесів. Скоріше за все, юстиція штучного інтелекту буде створена на основі роботів. Фізичних та інтелектуальних даних людини, очевидно, стане недостатньо для ефективного функціонування даної системи юстиції. Створення такої системи буде потребувати узагальнення в чіткі алгоритми досвіду, отриманого за час існування традиційної юстиції. Таке узагальнення, можливо, стане одним із основних напрямків майбутньої юридичної науки [6, с. 32].

Також з’явилося поняття «машини Тюрінга», що уточнює загальне поняття алгоритму. Машина Тюрінга – абстрактний пристрій, що має стрічку із символами, а також голівку для зчитування та запису інформації. Після зчитування, машина, на основі отриманої інформації та власного внутрішнього стану, робить наступний крок. А. Тюрінг вважається засновником теорії штучного інтелекту. Він створив тест, який визначає, чи може машина мислити як людина. Класично тест інтерпретується так: «Суддя взаємодіє з комп’ютером та людиною, усі троє не бачать один одного. На підставі відповідей, суддя має сказати, хто з двох є людиною. Завдання комп’ютерної програми – увести суддю в оману, змусивши зробити неправильний вибір» [7, с. 22].

Так, до прикладу правоохоронними органами та спецслужбами Ізраїлю широко використовуються програми, що аналізують і детектують брехню чи правдивість інформації при допиті підозрюваних та інших учасників правових процедур. Такою програмою є зокрема LVA 6.50, яка активно впроваджується і у діяльність

правоохоронних органів України. LVA 6.50 – це професійний інструмент для розслідування на базі технології багаторівневого голосового аналізу Nemesysco. LVA 6.50 вимірює психофізіологічні реакції, когнітивні процеси та рівні стресу. На основі цих даних програма визначає емоційний стан людини та вказує на проблемні для неї теми [8].

Проте тут постає питання: «Тоді що ж є мислення?». За яким принципом працює людський розум, та чи можливо, взагалі, визначити це аналогічно опису алгоритму комп'ютера? Якщо математичні розрахунки чи просту пам'ять можна якось пояснити послідовністю дій та провести аналогії з алгоритмом програми, то більш складні дії людини, наприклад, у творчості, мистецтві чи комунікації пояснити даним принципом важко [9, с. 34].

Загальний аналіз стратегій розвитку штучний інтелект різних держав свідчить про те, що суспільство і уряди країн розуміють важливість застосування сучасних інформаційно-комунікаційних технологій, в тому числі і технологій ШІ. Розвиток цифрових технологій є невід'ємним аспектом розвитку суспільства і часто сприяє прискоренню його позитивного розвитку. Разом з тим, людство цілком реально усвідомлює ризики безконтрольного застосування штучний інтелект і розуміє необхідність застосування правового регулювання його використання через стандарти та нормативно-правові акти. Стратегії розвитку ШІ водночас є індикаторами стану загальної цифровізації тієї чи іншої держави та готовності перенацілити ресурси на сферу застосування штучний інтелект.

Література

1. Вища освіта назустріч четвертій промисловій революції: кейси з європейського та українського досвіду. Монографія. За заг. редак. В. Шатоха. Дніпро. «Поліграфічна акцидентна фірма», 2021. – 68 с.
2. Бізнес, інновації, менеджмент: проблеми та перспективи: зб. тез доп. II Міжнар. наук.-практ. конф., 22 квіт. 2021 р. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 288 с.
3. Економічна та інформаційна безека: проблеми та перспективи : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 27 квіт. 2018 р.).Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. – 276 с.
4. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text
5. Дорожня карта з регулювання штучного інтелекту в Україні. Режим доступу: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf
6. Марценко Н. Застосування технологій штучного інтелекту при здійсненні митного контролю зарубіжний досвід. Редакційна колегія. 2022. С.237.
7. Демура М. Міжнародний досвід використання алгоритмів штучного інтелекту у кримінальному провадженні. Використання технологій штучного інтелекту у протидії злочинності. 2020. С.24-28.
8. Аналіз голосового сигналу. Електронний ресурс. Режим доступу: https://vas-ua.com/lva65/
9. Карчевський М. Штучний інтелект та протидія злочинності. Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару Харків. 2020. С.32-43.

Проць І. М.
доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ДЕРЖАВНОМУ УПРАВЛІННІ

Одним із питань правового регулювання інформаційної безпеки є питання захисту інформації та інформаційних ресурсів. Механізм правового регулювання інформаційної безпеки можна розглядати як засіб захисту. Інформаційна безпека відноситься до захисту інформаційних систем і даних, що містяться в них, захищає від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення інформації.

Правові норми відіграють вирішальну роль у встановленні меж та вимог для захисту інформації забезпечення цілісності, конфіденційності та доступності. Як зазначається у Декларації принципів побудови інформаційного суспільства, цифрові технології відкривають нові перспективи досягнення вищих рівнів розвитку [1].

Закони та нормативні акти, що стосуються у сфері інформаційної безпеки, визначають права, обов'язки окремих фізичних і юридичних осіб, Кабінету Міністрів України щодо поводження з інформацією та її захисту. Правові норми визначають юридичні кордони, у яких інформація може бути доступна, зберігатися, передаватися і оброблятися.

Ці правила встановлюють стандарти безпечного зберігання та передачі конфіденційної інформації, визначають порядок накладання штрафів за несанкціонований доступ або розкриття інформації, надають засоби правового захисту у разі порушень інформаційної безпеки. Встановлюючи юридичні вимоги в законах «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», правилах конфіденційності та стандартах кібербезпеки, встановлюється механізм правового регулювання спрямований на захист інформації фізичних і юридичних осіб від різних загроз, включаючи злом, витік даних, крадіжку персональних даних та інші форми кіберзлочинності [2].

Механізм правового регулювання встановлює структуру для запобігання, виявлення, реагування на інциденти безпеки та відновлення після них, гарантує вжиття відповідних заходів для захисту конфіденційної інформації. Правові норми сприяють підвищенню підзвітності, встановлюють керівні принципи для звітності про інциденти та розкриття інформації, полегшують співпрацю між різними установами та заохочують впровадження передової практики у сфері інформаційної безпеки.

Правова база діє як захисний механізм, створюючи правову основу для забезпечення безпеки інформації та надаючи засоби правового захисту окремим особам чи організаціям, які постраждали від порушень безпеки.

Інформаційна безпека – це багатогранне питання, що включає не лише правові норми, а й технологічні заходи, організаційні політики безпеки та обізнаність користувачів. Хоча правове регулювання відіграє важливу роль у захисті інформації, його слід доповнювати іншими заходами безпеки для створення всеосяжної та ефективної стратегії інформаційної безпеки.

Основним нормативно-правовим актом, який регулює питання інформаційної безпеки у сфері державного управління, є закон «Про захист інформації в інформаційно-комунікаційних системах» [3].

У цьому законі визначено основні поняття у сфері інформаційної безпеки, встановлено вимоги до захисту інформації, визначено відповідальність та заходи захисту при порушенні правил обробки та захисту інформації. Існує низка нормативно-

правових актів, що регулюють питання інформаційної безпеки у конкретних сферах державного управління. До таких актів для органів виконавчої відносяться закон «Про державну таємницю», який встановлює вимоги до організації роботи з державною таємницею та її захисту [4].

Стратегія інформаційної безпеки України охоплює різні аспекти, пов'язані із захистом інформації та інформаційних систем. Стратегія інформаційної безпеки включає:

- конфіденційність: інформаційна безпека гарантує, що конфіденційна інформація захищена від несанкціонованого доступу, розкриття фізичними та юридичними особам, які не уповноважені на доступ до інформації.
- цілісність: цілісність інформації передбачає підтримку точності, несуперечності та надійності інформації. Це гарантує, що дані не підробляють, не змінюються та не модифікують несанкціонованим чином.
- доступність: інформаційна безпека гарантує, що авторизовані користувачі мають доступ до інформації та інформаційних систем, коли це необхідно. Доступність включає реалізацію заходів запобігання збоям, простоям або відмови у доступі до критично важливих інформаційних ресурсів.
- захист даних: інформаційна безпека включає захист даних від втрати, крадіжки чи ушкодження. Це включає впровадження відповідних процедур резервного копіювання та відновлення, методів шифрування та методів безпечного зберігання даних.
- виявлення та запобігання загрозам: інформаційна безпека спрямована на виявлення та запобігання потенційним загрозам і вразливості, які можуть поставити під загрозу конфіденційність, цілісність або доступність інформації. Заходи включають розгортання технологій безпеки, таких як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення, впровадження процедур запобіжного моніторингу та реагування на інциденти.

Це деякі з ключових елементів, які зазвичай включаються до Стратегії інформаційної безпеки. Однак важливо зазначити, що інформаційна безпека – динамічна галузь, яка постійно розвивається через загрози, технологічні досягнення та мінливі умови регулювання.

Сьогодні не склалося одноманітного підходу до розуміння змісту термінів «інформаційна безпека» та «захист інформації». Інформаційна безпека та захист інформації є не тотожними поняттями, а радше взаємодіючими процесами. Захист інформації є складовою інформаційної безпеки.

Визначення «інформаційна безпека» має включати не тільки технічні заходи захисту інформації та інфраструктури, а й організаційні та правові заходи забезпечення безпеки інформації в державному управлінні.

Література

1. Declaration of Principles Building the Information Society: a global challenge in the new Millennium. URL. https://old.apitu.org.ua/wsis/dp
2. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL. https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL. https://zakon.rada.gov.ua/laws/card/2163-19
4. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. URL. https://zakon.rada.gov.ua/laws/card/3855-12

Рижков Е. В.
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Законодавче забезпечення інформаційної безпеки в Україні в умовах воєнного стану є надзвичайно важливим аспектом забезпечення національної безпеки та обороноздатності країни. У воєнний час, інформаційна безпека стає критичною, оскільки ворожі російські сили можуть використовувати різноманітні методи інформаційної війни для дестабілізації суспільства, дезінформації та маніпуляції громадською думкою. Ця діяльність включає в себе прийняття спеціальних законів, що регулюють доступ до інформації, захист особистих даних, боротьбу з кіберзлочинністю, контроль за мас-медіа та соціальними мережами, та інші аспекти, спрямовані на запобігання втручання агресора у внутрішні справи країни.

Умови воєнного стану на ряду із посилення ролі збройних сил також вимагає вжиття спеціальних заходів щодо обмеження доступу до деякої інформації, контролю за медіа та інтернет-платформами, та забезпечення безпеки критичних інформаційних інфраструктур. Тому, вказане законодавче забезпечення також може включати в себе розвиток та впровадження нових технологій, таких як кіберзахист, штучний інтелект для виявлення та запобігання кібератак, та інші інноваційні підходи до захисту інформаційних ресурсів країни.

Разом з тим, в рамках законодавчої ініціативи суспільству пропонується прийняти зміни та доповнення до існуючих нормативних положень новацію, яка фактично надає додаткові повноваження одному з державних суб'єктів кіберзахисту – Держспецзвязку [1]. Ці новації серед іншого передбачають глобальний контроль з боку офіцерів служби за усіма підрозділами із кіберзахисту, які повинні бути створені в органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом. Як потенційним керівникам цих підрозділів таким офіцерам пропонується надати право визначати функції, повноваження, загальні вимоги до підрозділів із кіберзахисту та їх співробітників, а також особливості правового статусу.

За логікою воєнного часу якщо і розглядати збільшення контролю за ситуацією в країні то він повинен бути зосереджений у військових. Прикладом доцільності такого підходу є функціонування військових адміністрацій з початку військової агресії.

Державні структури щодо яких є претензії правого характеру навпаки повинні бути обмежені у своїх повноваженнях. Принаймні до проведення у них процедур санації/реструктуризації чи взагалі їх повного перезавантаження.

Корупційна ситуація з Держспецзв'язком свідчить про підвищені ризики держбезпеці та про доцільність саме такого підходу [2, 3].

З огляду на зазначене, пропозиція реалізувати зазначені законодавчі ініціативи не прибирає, а збільшує вірогідність кіберзагроз для України в період воєнного стану та повинна розглядатись як хибна. Тому, будь-які спроби подальшого просування законопроекту № 8087 від 29.09.2022 повинні бути припинені, а сам він знятий з розгляду.

Більш того, за твердженням екс-заступника Міністра оборони України, засновника фонду «Повернись живим» В. Дейнеги Міністерство оборони та ЗСУ мають максимально швидко вийти з-під впливу та регулювання Держспецзв'язку. Бо не

цифровізована армія — це не тільки про крипту на гаманці (Р.Е. у екс-керівництва Держспецзв'язку). Це про щось значно більше зараз. Про виживання (не подумайте що тільки солдат) [4].

Зі слів автора ми бачимо, що мова йде вже саме про виживання країни.

Разом з тим, ситуація ускладняється зволіканням законотворців та інших суб'єктів, які так і не реалізували до поточного моменту положення Стратегії кіберзахисту України в частині прийняття закону «Про кібервійська України», що у свою чергу є неприпустимим з огляду на сучасні загрози нашій державності. Збройні сили України, їх кіберпідрозділи, а у найближчий час і кібервіська повинні бути основним пріоритетом державницької політики щодо розвитку суб'єктів кіберзахисту в період воєнного протистояння з російським ворогом [5].

Припускаємо можливі причини, чому закон про кібервійська України дотепер не був прийнятий. Серед них можуть бути наступні:

- складність визначення та регулювання: Кібервійська має складну та швидкозмінну природу, що робить важкою розробку ефективного та повноцінного законодавства в цій сфері;
- відсутність консенсусу: Різні політичні сили та соціальні групи можуть мати різні погляди на те, як повинен бути сформульований закон про кібервійська. Це може призвести до затримок у прийнятті відповідного законодавства;
- технічні та технологічні виклики: Швидкий розвиток технологій у кіберпросторі може ускладнювати розробку законодавства, яке було б актуальним на довготривалий період;
- відсутність світового досвіду: Кібервійська - це нова сфера, і багато країн ще тільки розробляють свої власні закони щодо цього. Відсутність чіткого світового досвіду може ускладнювати розробку відповідного законодавства.

Проте, Україна стала першою жертвою першої у світі кібервійни. Тому і заходи повинні бути адекватні, і законотворчі пріоритети повинні бути відповідні.

Створення нашими партнерами ІТ-коаліції тому приклад [6]. Запуск ІТ-коаліції безумовно буде сприяти розвитку інформаційних технологій у ЗСУ, що позитивно позначиться на перспективах обороноздатності країни. ІТ-коаліція може впроваджувати технологічні рішення для боротьби з корупцією в оборонній сфері України, зокрема за допомогою електронного урядування та цифрових інструментів для забезпечення прозорості та відкритості у державних процесах. Також ІТ-коаліція може також сприяти підвищенню рівня кібербезпеки в Україні, захищаючи країну від кібератак та інших кіберзагроз. Саме цей напрямок, на наше переконання, є одним із перспективних та повинен розвиватись з боку уповноважених суб'єктів держави.

Україна як один з основних суб'єктів сучасної кібервійни моє шанси не тільки сформувати свої кібервійська, але й стати трендом прогресивних змін при формуванні нових міжнародних структур колективної безпеки, в тому числі у кіберпросторі [7, с. 60].

Законодавче забезпечення інформаційної безпеки в умовах воєнного стану потребує комплексного підходу, який враховує потреби безпеки, посилення ролі збройних сил, прозорості та міжнародного співробітництва. Саме тому, негайне прийняття закону «Про кібервійська України» та їх створення повинно розглядатись як один із законотворчих пріоритетів держави наприкінці 10 років військового протистояння з російським агресором.

Кібервійська України повинна стати одним із провідних суб'єктів кіберзахисту країни. У сучасних умовах, коли інформаційні загрози дедалі посилюються та стають

все більш складними та небезпечними, держава повинна мати сучасну ефективну некорумповану систему інформаційного захисту.

Література

1. Проект Закону про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40553
2. Заволодіння 62 млн грн при закупівлі програмного забезпечення: підозрюється керівництво Держспецзв'язку. URL: https://nabu.gov.ua/news/zavolod-nnia-62-mln-grn-pri-zakup-vl-programnogo-zabezpechennia-p-dozriu-t-sia-ker-vnitctvo-derzhspetczviazku/?fbclid=IwAR3WRTcvHq7Mo-nPSbgX6gPOxFUmUnszhPALLdL8oDqzhI3K-tRx1YULHWw
3. Катерина Жирій Уряд звільнив голову Держспецзв'язку та його заступника через корупцію. URL: https://www.unian.ua/society/uryad-zvilniv-golovu-derzhspeczv-yazku-ta-yogo-zastupnika-cherez-korupciyu-12461352.html
4. Віталій Дейнега Корупція в держспецзв'язку. URL: https://bastion.tv/korupciya-v-derzhspeczvyazku_n59118
5. Рижков Е.В. Формування стратегії кіберзахисту в умовах воєнного стану / Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 10 жовтня 2023 року). – Дніпро: ДДУВС, 2023. – С. 41-46
6. Учасники »Рамштайну» запустили IT-коаліцію для України. URL: https://www.ukrinform.ua/rubric-ato/3763413-ucasniki-ramstajnu-zapustili-itkoaliciu-dla-ukraini.html
7. Ryzhkov Eduard Problematic issues of staffing cyber troops of Ukraine under martial law / E. Ryzhkov // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. 2022. Special Issue. – № 1 (120). – p. 55-60 URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/04/S1/NV_DDUVS_spec_1_2022-55-60.pdf

Сапрун А. М.

здобувач вищої освіти Львівського державного університету внутрішніх справ

Зачек О. І.

т.в.о. завідувача кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІНФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ, КЕРОВАНІЙ АНАЛІТИКОЮ

Правоохоронна діяльність, керована аналітикою, використовує аналітичні методи та інструменти для збору, обробки та аналізу інформації з метою покращення ефективності діяльності правоохоронних органів. Цей підхід дозволяє збирати та використовувати дані для прийняття обґрунтованих рішень, прогнозування злочинності, виявлення та запобігання правопорушенням. У Євросоюзі стратегія діяльності поліції заснована на концепції «правоохоронна діяльність, керована аналітикою» і значна кількість злочинів розкриваються саме завдяки використанню цього підходу [1].

Поліцейська діяльність, керована аналітикою (Intelligence-led Policing, ILP) – це сучасна модель поліцейської діяльності, яка передбачає вбудовування розвідувальної аналітичної функції в діяльність правоохоронної системи. Комплексним завданням такої діяльності є прогнозування ризиків та вплив на дії правоохоронних органів шляхом поєднання аналізу та прийняття рішень [2, с. 25]

Основні аспекти правоохоронної діяльності, керованої аналітикою, включають:

1. **Збір інформації:** Використання різноманітних джерел для збору даних, таких як бази даних, відкриті джерела, соціальні мережі та інше.
2. **Аналіз інформації:** Використання аналітичних інструментів для обробки та аналізу великого обсягу даних з метою виявлення закономірностей, тенденцій та небезпечних ситуацій.
3. **Прогнозування:** Використання аналітичних моделей для прогнозування можливих подій, в тому числі злочинів, що можуть трапитися в майбутньому.
4. **Стратегічне планування:** Використання аналітики для розробки стратегій боротьби з злочинністю та підвищення ефективності правоохоронних заходів.
5. **Оптимізація ресурсів:** Визначення найбільш ефективного використання ресурсів на основі аналізу даних та пріоритетів.
6. **Запобігання злочинам:** Використання аналітичних результатів для розробки та впровадження програм та заходів з запобігання злочинам.
7. **Система відслідковування:** Створення систем відслідковування та моніторингу для оперативного реагування на потенційно небезпечні ситуації.

Застосування аналітики у правоохоронній діяльності дозволяє зробити процес прийняття рішень більш обґрунтованим, забезпечуючи ефективнішу реакцію на виклики та загрози в галузі правопорядку.

Інформація, яку в процесі своєї діяльності отримує поліція, сама по собі не має особливої цінності, поки її не проаналізувати. Лише проаналізована та оброблена інформація дозволяє здійснювати реагування на події та формувати політику дій поліції, а також здійснювати перерозподіл ресурсів. Також важливу роль відіграє аналіз ризиків на основі проаналізованої інформації. Розвиток інформаційних технологій полегшує та робить більш швидкими збір та опрацювання інформації [1].

У процесі здійснення аналізу інформації використовують відповідне програмне забезпечення та інформаційні ресурси. Правоохоронні органи різних країн використовують різні методики аналізу інформації, але найчастіше використовуються такі програми, як i2 й ANACAPA. Вони призначені для підрозділів поліції, які мають необхідність аналізу даних та інформаційних потоків [3, с. 20].

Інформаційні технології (ІТ) грають важливу роль у правоохоронній діяльності, керованій аналітикою. Використання сучасних технологій та аналітичних підходів дозволяє правоохоронним органам ефективно збирати, обробляти та використовувати інформацію для прогнозування, запобігання та боротьби зі злочинністю. Ось кілька аспектів використання ІТ в правоохоронній діяльності, керованій аналітикою:

1. Біг-дата та аналітика:
   - Збір та обробка великих обсягів даних для виявлення тенденцій, злочинних мереж та інших закономірностей.
   - Використання аналітичних інструментів для швидкого аналізу біг-даних та отримання цінної інформації для прийняття рішень.
2. Штучний інтелект (ШІ) та машинне навчання:

- Впровадження алгоритмів машинного навчання для прогнозування можливих злочинів та оптимізації стратегій боротьби з ними.
- Використання ШІ для автоматизації деяких процесів, таких як розпізнавання обличь, аналіз аудіо- та відеоматеріалів.

3. Системи відеоспостереження та розпізнавання обличь:
   - Використання великомасштабних систем відеоспостереження для виявлення та відстеження злочинців.
   - Впровадження технологій розпізнавання обличь для ідентифікації осіб на відеозаписах.
4. Кібербезпека:
   - Захист інформаційних систем від кібератак та зловживань, зокрема за допомогою систем виявлення вторгнень та аналізу кіберзагроз.
5. Електронна обробка доказів:
   - Використання електронних систем для збору, збереження та обробки цифрових доказів в справах.
6. Системи GPS та геопросторовий аналіз:
   - Використання технологій GPS для відстеження руху осіб, транспортних засобів та визначення місць подій.
   - Геопросторовий аналіз для визначення взаємозв'язків між подіями та географічними областями.
7. Електронні системи звітності та моніторингу:
   - Впровадження систем для ефективного моніторингу та звітності щодо правопорушень та результатів правоохоронних заходів.

Ці технологічні інновації допомагають правоохоронним органам створювати ефективніші та швидкі механізми реакції на злочини та підвищувати загальну безпеку в суспільстві.

Найчастіше Національна поліція у своїй роботі застосовує як аналітичний інструмент програмний пакет Microsoft Office, а саме Word та Excel, хоча в деяких підрозділах використовується спеціалізоване програмне забезпечення для аналізу даних, таке як, i2 Analyst’s Notebook, ArcGIS, E-Gismaps тощо [4].

Концепція правоохоронної діяльності, керованої аналітикою, в повній мірі використовується в країнах Європейського союзу, а в Україні застосовується лише частково. Лише деякі принципи цієї концепції використовуються деякими підрозділами Національної поліції України, але про широке застосування, як частину інституційної культури, говорити ще не можна [1]. Тому, з метою більш ефективної правоохоронної діяльності, необхідно більш широко застосовувати такий підхід у всіх підрозділах Національної поліції України.

Література

1. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності. URL: https://www.euam-ukraine.eu/ua/news/opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/
2. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою. INTELLIGENCE-LED POLICING (ILP) : навч. посіб. / О.Є. Користін , Д.О. Пефтієв , С.В. Пеньков , В.А. Некрасов ; ред. М.Г. Вербенський. – Київ :

Видавництво Людмила, 2019. – 120 с. URL: https://er.dduvs.in.ua/handle/123456789/10630
3. Мовчан А.В. Актуальні проблеми впровадження в органах національної поліції України моделі поліцейської діяльності, керованої аналітикою / Мовчан Анатолій Васильович // Соціально-правові студії. 2018. Випуск 1. С. 17-22. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/1613
4. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності. URL: http://euam.php7.postbox.kiev.ua/ua/news/opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/

Сидор М. Я.
доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук

РОЗВИТОК ЦИФРОВИХ КОМПЕТЕНЦІЙ ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ФОРМУВАННЯ ЛЮДСЬКОГО КАПІТАЛУ

Людський капітал стає ключовим фактором забезпечення ефективного розвитку окремих суб'єктів господарювання і економічних систем різного рівня. Для людського капіталу характерний дуалізм сутнісного змісту, в рамках якого він проявляється у формі економічного ресурсу, та комплексу специфічних знань, умінь і навичок, якими володіють працівники на певному рівні підприємства, регіону, держави.

Набір компетенцій, що дозволяє говорити про можливість капіталізації здібностей людини, багато в чому визначається умовами та факторами соціально-економічного розвитку, до важливих з яких на є становлення цифрової економіки як форми виробничих відносин, в рамках якої домінують цифрові технології, а інформаційні потоки функціонально залежить від використання інформаційно-комунікаційних технологій.

На відміну від попередніх етапів науково-технічної революції, цифровізація характеризується всеосяжним характером, що стосується всіх сфер економічної діяльності та суспільного життя, відбувається у стислий термін. Стрімке поширення процесів цифровізації висуває такий вид компетенцій, як цифрові в розряд ключових. Подібна ситуація визначається тим фактом, що вміння працювати з цифровими технологіями є необхідним практично для будь-якого носія людського капіталу.

Під цифровими компетенціями розуміється сукупність знань і здібностей, які необхідні для того, щоб людина могла використовувати цифрові технології в процесі досягнення цілей, що стоять перед нею, в особистій або професійній діяльності. Цифрові компетенції повинні сприйматися не лише як певні технічні навички, а як знання, що стосуються когнітивних, соціальних та емоційних аспектів життєдіяльності в цифровому середовищі.

Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації вказує, що формування та реалізація цифрових компетенцій – багатогранний процес, що еволюціонує, постійно змінюється в міру появи нових цифрових технологій [1].

Цифрова грамотність віднесена Європейським Союзом до ключових компетенцій, володіння якими є необхідною умовою забезпечення ефективної життєдіяльності індивіда [2; 3]. У платформі Digital Competence 2.0 виділено понад два десятки цифрових компетенцій, особливу увагу серед яких привертає вказівка на володіння

«цифровим інтелектом», яке передбачає наявність у працівника вміння оцінити наявність необхідності отримання нових навичок у цифровій сфері [4].

Як наголошується у звіті Human Capital Trends 2017, питання цифрової адаптації працівників та підприємств мають винятково важливе значення. Це підтверджується тим фактом, що 90% керівників компаній із 140 країн, які були опитані під час його підготовки, вказали на наявність кардинальних трансформацій, зумовлених впровадженням цифрових технологій, а 70% відзначили відсутність організаційних навичок, які б дозволили успішно адаптуватися до наслідків цих трансформацій [5].

Подібний розвиток подій зумовлює важливе значення розвитку цифрових компетенцій як елементів людського капіталу конкретного індивіда та організації. Зміст процесу формування цифрових компетенцій не можна зводити до форми спеціалізованого навчання або ототожнювати із отриманням певної професії. У даному контексті можна виділити рівні формування цифрових компетенцій як складової підвищення кваліфікації та підвищення ступеня конкурентоспроможності працівника на ринку праці та як елементу процесу соціалізації особистості, інтеграції у цифрове суспільство.

У першому випадку потреба у придбанні цифрових компетенцій є очевидною – остійна поява нового обладнання та нових виробничих процесів вимагає від працівників самовдосконалення.

Цифрові технології протягом останніх двох десятиліть докорінно змінили основи організації виробничих процесів у багатьох галузях економічної діяльності. Людина, яка не вдосконалює власні професійні навички та не освоює цифрові технології, ризикує втратити конкурентоспроможність на ринку праці в досить короткостроковій перспективі.

У другому випадку йдеться про необхідність володіння цифровими компетенціями через наявність загрози втрати доступу до значної кількості суспільних благ, що надаються в цифровій формі, позбавлення можливості повноцінної участі в громадському житті, втрати соціального статусу.

Відмінності в рівні реалізації можливостей між індивідами, які мають необхідні для повноцінної участі в трудовому та суспільному житті цифрові компетенції, і позбавлені подібної можливості настільки разючі, що більша кількість фахівців відзначають розвиток такого явища як цифрова нерівність, яка може знаходити прояв на рівнях особи та держав.

Однією з проблем, що зумовлюють наявність подібної нерівності, є необхідність постійного оновлення цифрових компетенцій, які повинні мати всі члени суспільства. Проблема формування цифрових компетенцій має яскраво виражене суспільне значення.

Останніми роками у багатьох державах здійснюється розробка ключових документів, визначальних рамки цифрових компетенцій, необхідні людині забезпечення нормального життя умовах цифровизации. Зокрема, у підготовленому в рамках Європейського Союзу на основі узагальнення досвіду різних держав, документі під назвою Digital Competence Framework for Citizens 2.0 представлено опис основних позицій у сфері цифрової компетентності, які має мати особа [4].

Цифрової компетентності виділені в підгрупах: інформація та цифрова грамотність, комунікація та співпраця, створення цифрового контенту, безпека вирішення проблем у цифровій сфері. Окремо виділено цифрові компетентності для освітян (DigCompEdu), освітніх організацій (DigCompOrg), споживачів (DigCompConsumers), підприємців (EntreComp).

Інструментарій системи Europass дозволяє оцінювати рівень цифрових компетенцій індивідів у процесі навчання під час працевлаштування [6]. Одним із параметрів

оцінки є вміння аналізувати, порівнювати та критично оцінювати достовірність та надійність цифрового контенту.

Важливою умовою успішності взаємодії людини та цифрових технологій є необхідність для носія цифрових компетенцій певної особистісної та професійної трансформації, орієнтованої на адаптацію до нових реалій часу та набуття здатності до ефективної діяльності, що дозволяє використовувати надані цифровими технологіями переваги.

Література

1. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: Розпорядження Кабінету Міністрів України від 03.03.2021 р. № 167-р. URL. https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text
2. Commission Staff Working Document Accompanying the Document Proposal for a Council Recommendation on Key Competences for LifeLong Learning SWD/2018/014 final – 2018/08 (NLE). URL. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:0014:FIN
3. Про основні компетенції для навчання протягом усього життя: Рекомендація 2006/962/ЄС Європейського Парламенту та Ради (ЄС) від 18.12.2006 р. URL. https://zakon.rada.gov.ua/laws/show/994_975.
4. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. URL. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254
5. The 2017 Global Human Capital Trends. URL. https://www.trginternational.com/white-paper/2017-global-human-capital-trends-2/
6. Europass. URL. https://europa.eu/europass/uk

Скриньковський Р. М.

професор кафедри економіки підприємств та інформаційних технологій Львівського університету бізнесу та права, кандидат економічних наук, професор

ДЕЯКІ ПРОБЛЕМИ ПРОТИДІЇ КРИМІНАЛЬНІМ ПРАВОПОРУШЕННЯМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Комп'ютерні технології настільки глибоко інтегровані у життєдіяльність суспільства, що уникнути потреби в користуванні такими технологіями неможливо. Люди різного віку змушені вдаватися до користування різними апаратними та програмними засобами для вирішення професійних та побутових питань. З огляду на затребуваність та поширеність інформаційні технології стрімко розвиваються. Фахівцями розробляються нові системні та програмні рішення. Це призводить до необхідності актуалізації знань і вмінь користувачами інформаційних систем, постійним переходом на нові технології.

Зважаючи на багатофункціональність та практичність інформаційних технологій вони використовуються учасниками суспільних відносин не тільки на благо, а й у корисливих цілях. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку тобто інформаційних технологій є феноменом не менш важливим та

поширеним, ніж класичні форми та способи скоєння кримінальних правопорушень. Доступність, поширеність та відносна анонімність комп'ютерних технологій відіграє роль у скоєнні таких правопорушень.

Нові технології використовуються зловмисниками у різних формах і способах для скоєння різних злочинів. Число вчинених кримінальних правопорушень різного виду за допомогою інформаційних технологій останніми роками стабільно зростає. З числа кримінальних правопорушень майже половину становлять шахрайства.

Злочини у сфері інформаційних технологій є одними з найбільш латентних. Деякі автори вказують високий рівень латентності досліджуваного виду кримінальних правопорушень – до 90 %.

Однією з основних причин зростання кримінальних правопорушень, які скоєні за допомогою інформаційних технологій, є складність у розкритті. Різні дослідники проблематики кіберзлочинності підтримують цю тезу. Розкриття та розслідування кримінальних правопорушень, що скоєні у сфері інформаційно-комунікаційних технологій, є складним завданням.

Проблеми, які є у розслідуванні, наприклад, шахрайства в мережі Інтернет, багато в чому пов'язані з технічним аспектом. Виникають обставини, коли підозрюваний невідомий, інформація про нього відсутня, а її встановлення є надмірно довгим, трудомістким та дорогим процесом.

У зв'язку зі зростанням кількості кримінальних правопорушень останніми роками Генеральна прокуратура України приділяє особливу увагу підвищенню ефективності протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (інформаційних технологій). При координуючій ролі прокуратури вживаються заходи щодо створення умов для запобігання, виявлення та припинення кримінальних правопорушень, що скоєні з використанням інформаційних технологій.

Крім посилення нагляду за роботою правоохоронних органів на регулярній основі, проводяться заходи, спрямовані на підвищення правової та фінансової грамотності громадян. У Генеральній прокуратурі наголосили, що метою вжитих заходів є формування системи забезпечення інформаційної безпеки, включаючи організацію ефективної міжвідомчої взаємодії у цьому напрямі.

Незважаючи на заходи зменшення кількості вчинення кримінальних правопорушень та підвищення відсотка розкриття такого підходу до вирішення проблеми зростання кіберзлочинності може бути недостатньо. Необхідним є опрацювання можливості вирішення базових, фундаментальних недоліків законодавства, що регулює сферу дослідження.

Проблеми кримінальних правопорушень, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, розглядаються з різних позицій та мають різнобічний понятійний апарат. У наукових працях злочину у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку називаються по-різному: як кіберзлочини, інтернет-злочини, злочини, вчинені з використанням інформаційно-комунікаційних технологій, що не призводить до формування науково обґрунтованого поняття досліджуваної групи кримінальних правопорушень.

При виробленні такого поняття необхідно використовувати законодавство, що регламентує питання використання інформаційних технологій та кримінальний закон. Наприклад, згідно із законом «Про Національну програму інформатизації» під терміном «інформаційно-комунікаційні технології» законодавець розуміє процеси, методи пошуку, збирання, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів та методів [1]. Слід зазначити, що Кримінальний кодекс

України термін «інформаційні технології» не містить. Деякі склади кримінальних правопорушень, які у Кодексі, містять суміжні і непрямі поняття.

Злочини досліджуваної сфери у Кримінальному кодексі України виділено в окремий розділ: «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [2]. Назва вважається чинною і застосовується до існуючих кримінально-правових відносин, проте вимагає модернізації.

Понятійний апарат кримінального законодавства потребує актуалізації відповідно до розвитку інформаційних технологій. Така актуалізація має сприяти сучасній кваліфікації кримінальних правопорушень, що у результаті має сприяти виробленню ефективної політики та стратегії протидії досліджуваним правопорушенням.

Інформаційні технології дозволяють навіть користувачам забезпечувати деяку анонімність у мережі. У досвідчених користувачів такі можливості може бути розширено. Злочинці, які мають необхідні знання, можуть забезпечувати часткову чи повну анонімність. Зважаючи на це, при розслідуванні правопорушень у сфері інформаційних технологій покладатися виключно на трекінг IP-адрес недоцільно.

Дослідження свідчать, що злочинці залишають цифровий слід. Йдеться про сліди технічного характеру: реєстраційні дані доменного імені, сліди налаштування з хостинг-провайдером, листування з постраждалими від кримінальних правопорушень, реквізити платіжних систем, сліди міграції коштів та інші значимі для слідства сліди.

У випадках, коли кримінальне правопорушення скоєно з використанням незахищеної мережі передачі даних, у локальні мережі за відсутності захищеного за допомогою спеціалізованих програмних засобів сегменту мережі та недотримання вимог інформаційної безпеки, розкриття таких кримінальних правопорушень практично неможливе.

Виникають проблеми при отриманні екстериторіальних даних, що зберігаються на серверах іноземних держав. Інтернет-провайдери при отриманні запитів від правоохоронних органів посилаються на норми права, що обмежують передачу конфіденційних даних.

Зазначені проблеми можуть бути вирішені не тільки через розвиток криміналістичної техніки, але й приведення в актуальний стан нормативно-правової бази, що регулює протидію злочинам у сфері дослідження. Наприклад, для вирішення проблеми анонімності злочинців необхідне формування нормативної бази, що регулює деанонімізацію інформаційно-комунікаційного простору, блокування дзвінків із заміною номерів та протиправного контенту в мережі Інтернет, несанкціонованим діям та неправомірному використанню послуг мереж зв'язку.

Перелічені проблеми та передбачувані рішення не є вичерпними. Подальші дослідження на тему кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку мають бути спрямовані на виявлення конкретних проблем та рішень щодо вдосконалення нормативно-правової бази у сфері протидії таким злочинам.

Підсумовуючи, слід зазначити, що активний розвиток інформаційних технологій несе побічні ефекти у вигляді прогресування кримінальних правопорушень у цій сфері. Цей факт диктує гостру необхідність своєчасної актуалізації законодавчого регулювання протидії таким злочинам. Законодавство містить умови боротьби з досліджуваним типом кримінальних правопорушень. Окремі напрями правового регулювання протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку потребують розвитку та розробки програм з їхньої актуалізації.

Література

1. Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-IX. URL. https://zakon.rada.gov.ua/laws/show/2807-20#Text
2. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL. https://zakon.rada.gov.ua/laws/card/2341-14/conv

Скрябіна М. О.
курсант факультету №4 Харківського національного університету внутрішніх справ
Калякін С. В.
викладач кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ЕЛЕКТРОННОЇ ТА АКУСТИЧНОЇ СЛІДКОВОЇ СИСТЕМИ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З ростом обізнаності людей у технологіях, зростає кількість злочинів пов’язаних саме за цим напрямом. Відповідно і методи розслідування правопорушень мають розвиватися та вдосконалюватися. Поліцейським у цьому допомагають сучасні розробки, такі як електронні та акустичні слідкові пристрої.

Як приклад акустичної слідкової системи ми розглянемо радіостанції:

Радіостанції (рації) – є універсальним пристроєм, який може застосовуватись у різних ситуаціях. При спеціальних заходах чи операціях може слугувати для підтримки ефективного двостороннього зв’язку та секретного збору інформації. У повсякденному житті поліцейських рація може застосовуватись під час тренувань та відпрацювання певних навичок для комунікації у реальному часі, а також корективів дій задля ефективного проходження навчання. Радіостанція не є новою у діяльності поліції, але все одно поширено використовується.

За рахунок радіохвиль вона передає інформацію навіть у місцях з обмеженим зв’язком. Ще однією перевагою радіостанції є змога шифрувати дані задля перешкоджання незаконному прослуховуванню та захисту конфіденційної інформації. Детальніше роздивимось конкретні види радіостанцій:

1. **Стаціонарні радіостанції без дистанційного управління** (ДУ), які призначені для встановлення в чергових частинах та на стаціонарних постах за умов можливості розміщення антенного пристрою на відстані, обмеженій довжиною антенного ВЧ кабелю (не більше 30 м).

2. **Стаціонарні радіостанції з ДУ**, які призначені для встановлення в чергових частинах та на стаціонарних постах підрозділів внутрішніх справ, де немає можливості встановити стаціонарні радіостанції без дистанційного управління.

3. **Базові радіостанції**, які призначені для організації багаточастотних радіомереж.

4. **Центральні радіостанції**, які призначені для організації радіомереж великих чергових частин з дальністю зв'язку до 60 км, мають підвищену вихідну потужність передавача. Надають можливість з'єднання з абонентами телефонної мережі.

Пересувні засоби радіозв'язку органів внутрішніх справ поділяються на наступні види:

1. **Радіостанції переносні** – станції, які мають автономне джерело живлення та призначені для роботи під час пересування абонента чи при його зупинці;

2. **Радіостанції портативні** (в тому числі і таємно-переносні) – аналогічні до переносних, крім того, їхня маса не перевищує 1 кг, а потужність передавача обмежена 0,5 Вт;

3. **Радіостанції мобільні** – пересувні станції, призначені для встановлення на сухопутних пересувних об'єктах (автомобілях, мотоциклах, пересувних 12 залізничних об'єктах), кораблях внутрішнього плавання;

4. **Радіостанції універсальні** – станції, призначені для експлуатації і як стаціонарні, і як мобільні, і як переносні, і як портативні чи в будь-якій комбінації (для досягнення універсальності радіостанцій використовуються спеціальні адаптери).

Ми розглянули декілька прикладів пристроїв обробки аудіоданих, додамо також кілька недоліків їх застосування.

Основними недоліками радіозв'язку є:

- залежність якості та стійкості прийому: від рівня радіоперешкод у пункті прийому, від умов проходження іоносферних радіохвиль (на великих відстанях);
- мала пропускна спроможність;
- можливість перехвату переговорів та передач;
- створення навмисних перешкод.

Радіостанції вже давно використовуються в діяльності поліції, але зараз вони все більш викорінюються через деякі причини. Розвиток нових технологій: з винаходом інших технологій, таких як мобільні телефони, радіостанції стають менш популярні. Вартість: якісні рації є дорогими, що є проблемою у їх використанні у невеликих містах, де менше фінансування. Навчання: нові моделі рацій можуть бути досить важкими у застосуванні, адже невелика кількість поліцейських вміють з ними поводитись та застосовувати.

З боку електронної слідкової системи роздивимось GPS навігацію:

GPS навігація – це навігаційна система, яка працює за рахунок супутників, що знаходяться на орбіті Землі. Як саме використовується GPS навігація у діяльності Національної поліції України?

1. **Автомобільні патрулі**. Поліцейські машини зараз обладнані GPS трекерами задля оперативного відстеження їх на карті. При надзвичайних подіях можна швидко координувати рух автомобіля та направляти його на місце події.

2. **GPS у поліцейських**. Трекер можуть використовувати також і поліцейські офіцери, з такою ж метою, що й автомобілі, для відстеження найближчого офіцера, якого можна направити на місце події для швидкого вирішення проблеми.

3. **Використання під час військових дій**. Під час виконання спеціальних завдань у місцях небезпечних для життя поліцейського, використання GPS є важливим елементом. Адже можна у несподіваних ситуаціях визначити місцеположення поліцейського офіцера та швидко прийти на допомогу.

Наскільки б ефективною в застосуванні не була GPS навігація, але у неї також є свої недоліки. Якість отримання сигналу може залежати абсолютно від різних факторів: погодні умови, кількість та види будівель навколо. Але найголовнішою проблемою можна виділити здатність сторонніми особами перехоплювати сигнал, та можливість видати своє місце розташування.

Роздивимось декілька відмінностей між використанням GPS навігації в діяльності поліції України та європейських державах.

Якість обладнання. В інших країнах Європи GPS навігація почала використовуватися раніше, тому вони закуповують для поліції більш якісні та надійні трекери.

Поширеність у використанні. В Україні менш поширеною є використання навігації, у порівнянні з європейськими країнами. Як прикладом, можна зазначити контроль дорожнього руху, а саме відслідковування автомобілів порушників.

Як висновок, скажемо, що в України є усі можливості досягти рівня поширеності застосування навігації, як в державах Європи. Для цього потрібно збільшити фінансування поліції (але в теперішніх умовах це зробити важко) та підвищити рівень обізнаності та практичних навичок у самих поліцейських.

Нами було розглянуто два види слідкової системи: електронну та акустичну, їх переваги та недоліки. У підсумку можна сказати, що явними перевагами є поширеність застосування розглянутих систем та зручність використання у різних ситуація. Спільним недоліком для радіостанцій та GPS можемо виокремити здатність третім особам вкрасти конфіденційну інформацію через не якісне шифрування даних. Важливо правильно обирати пристрої, якими в подальшому ви будете користуватись та поважати конфіденційну інформацію оточуючих.

Література

1. Балтовський О.А. «Засоби та системи радіозв'язку та технічні засоби охорони» URL: https://oduvs.edu.ua/wp-content/uploads/2016/09/Lektsiya-3-9.pdf
2. І.В. Іванова, А.І. Іванов. Використання GPS-навігації в діяльності поліції України: сучасний стан та перспективи розвитку.: Правоохоронна діяльність 2021 р.
3. В. В. Діденко, С. О. Шевчук. GPS-навігація в діяльності поліції: досвід європейських країн. Право та суспільство. 2022 р.

Смик Д. Д.

аспірант Львівського державного університету безпеки життєдіяльності;

Бурак Н. Є.

заступник начальника кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

ХМАРНІ ТЕХНОЛОГІЇ: ПРИНЦИПИ РОБОТИ ТА РЕАЛІЗАЦІЇ

Хмарні технології вражають ефективністю завдяки масштабованості та гнучкості, що дозволяють швидко адаптуватися до змін у роботі та до сучасних користувацьких потреб. Вони забезпечують високий рівень доступності, базуючись на розгалужених серверних інфраструктурах. Автоматизація процесів у хмарному середовищі сприяє ефективній оптимізації ресурсів, зменшенню трудовитрат і зниженню витрат на обладнання та обслуговування, а застосування моделі оплати за фактичне використання ресурсів підтверджує економічну перевагу в застосуванні технологій такого типу. Важливими аспектами є також забезпечення безпеки та спрощення співпраці, що робить хмарні технології невід'ємною частиною ефективного функціонування бізнес-середовища.

У сучасному світі необхідність збільшення фізичних ресурсів для обробки даних з кожним роком стає зростає. Такі темпи прогнозують динамічний ріст кількості інформації, яка створюватиметься різними розумними пристроями та інформаційними системами. В таких умовах використання відокремлених фізичних засобів для забезпечення інформаційних потреб суспільства стає проблемою, оскільки це потреб є

значних фінансових затрат. З метою вирішення таких проблем, зокрема для досягнення високої продуктивності та швидкості обробки застосовують хмарні технології. Такий підхід передбачає реалізацію моделі надання комп'ютерних ресурсів, таких як обчислювальна потужність, засоби для зберігання даних та мережеві послуги із використання сучасних технологій електронних комунікацій, зокрема через глобальну мережу Інтернет. Хмарні обчислення дозволяють організаціям і приватним особам отримувати доступ до цих ресурсів, не купуючи та не підтримуючи власну інфраструктуру. Важливою особливістю застосування таких технологій є «розподіленість», тобто дані опрацьовуються з використанням не лише одного комп'ютера, а розподіляється по декількох комп'ютерах, які підключені до мережі та формують віртуальних єдиний обчислювальний ресурс.

Розподілені обчислювальні системи – це системи, які використовують декілька комп'ютерів для виконання одного завдання та контролюються єдиною програмною системою для балансування навантаження між окремими її компонентами. Такі системи можуть використовуватися для вирішення складних завдань, які були б неможливими для виконання на одному мікропроцесорі чи пристрої.

Для зберігання інформації у хмарних технологіях використовуються розподілені бази даних – бази, які фізично розміщені на декількох пристроях, одна для користувача відображаються як єдиний ресурс. Такі бази даних дозволяють організаціям зберігати великі обсяги даних у централізованому місці, а також забезпечують доступ до цих даних з будь-якого місця, де є Інтернет-з'єднання(див. Рис. 1).

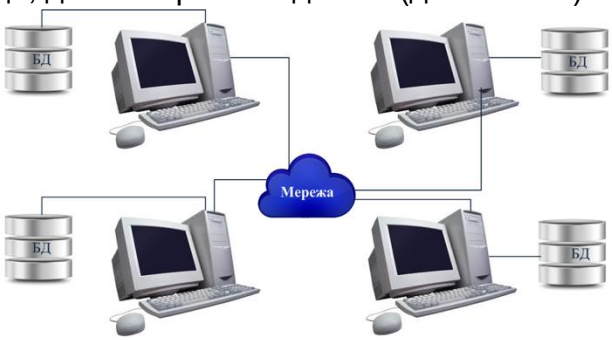

Рис. 1. Принцип роботи архітектури розподілених баз даних

Сучасні розподілені технології мають ряд переваг, основними з них є:

- Ефективність – використовуватися для підвищення ефективності обробки даних і виконання завдань;
- Доступність – забезпечують доступ до даних і ресурсів з будь-якого місця, де є Інтернет-з'єднання;
- Масштабування – можуть динамічно змінювати кількість компонентів та їх потужності в залежності від потреб.

Архітектура реалізації розподілених технологій визначається тим, як комп'ютери, які складають розподілену систему, взаємодіють один з одним. Існує кілька різних підходів до проєктування розподілених технологій, кожен з яких має свої переваги та недоліки.

Одна з найпоширеніших архітектурних реалізацій розподілених технологій – це клієнт-серверна архітектура. При такій реалізації один комп'ютер (сервер) відповідає за обслуговування запитів від інших комп'ютерів (клієнтів). Клієнти відправляють запити серверу, а сервер обробляє ці запити та повертає відповіді клієнтам. Клієнт-серверна архітектура є ефективною для завдань, які вимагають централізованого управління.

Інша поширена архітектура реалізації розподілених технологій – це розподілена обчислювальна архітектура. У такій архітектурі декілька комп'ютерів об'єднуються для

виконання одного завдання. Кожен комп'ютер виконує певну частину завдання, а результати роботи всіх пристроїв об'єднуються для отримання кінцевого результату. Розподілена обчислювальна архітектура є ефективною для завдань, які вимагають великої обчислювальної потужності.

Ще одна архітектура реалізації розподілених технологій – це розподілена база даних. У такій реалізації дані зберігаються на декількох комп'ютерах. Окремі компоненти загальної мережі віртуально об'єднані в єдину базу даних і при використанні даних з неї усі користувачі сприймають її як єдиний цілісний об'єкт. Розподілена база даних є ефективною для завдань, які вимагають зберігання великих обсягів даних.

Вибір архітектури реалізації розподілених технологій залежить від конкретних вимог до системи. Якщо система вимагає централізованого управління, то найкращим вибором буде клієнт-серверна архітектура. Якщо система вимагає великої обчислювальної потужності, то найкращим вибором буде розподілена обчислювальна архітектура. Якщо система вимагає зберігання великих обсягів даних, то найкращим вибором буде розподілена база даних.

Література

1. Grid Systems [Електронний ресурс]. – Доступний з https://www.interaction-design.org/literature/topics/grid-systems
2. Blockchain based decentralized [Електронний ресурс]. – Доступний з https://www.sciencedirect.com/science/article/pii/S2352484721007204
3. Samoylenko, H.T. & Selivanova, A.V.. (2023). Distributed information systems in e-commerce. Mathematical machines and systems. 2. 69-74. DOI:10.34121/1028-9763-2023-2-69-74.
4. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система «UniBell» як складова частина проєкту «Smart-університет». Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 105–113

Стахура В. І.

аспірант кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ

НЕДОСТОВІРНА ІНФОРМАЦІЯ ЯК ЗАГРОЗА ДІЛОВОЇ РЕПУТАЦІЇ ЮРИДИЧНОГО ОСОБИ

Цивільний кодекс України як один з виду об'єктів цивільних прав визначає нематеріальні блага. Більш детально зміст поняття «нематеріальні блага» розкрито у ст. 201 Цивільного кодексу України (далі – ЦК України) [1]. У цій статті у переліку нематеріальних благ вказано, зокрема, ділова репутація. У даний час розвиток соціально-правових та економічних відносин викликають необхідність підтримки ділової репутації на певному рівні.

Виходячи з норм Національного положення (стандарт) бухгалтерського обліку 8 «Нематеріальні активи», ділова репутація як символ професійної діяльності організації є складовою нематеріальних активів цієї організації чи підприємства. Відповідно вона буде відображена у фінансовій звітності у вигляді або позитивної або негативної ділової репутації [2].

У суспільному житті під діловою репутацією прийнято розуміти певні ділові та професійні характеристики, які особа набуває у процесі здійснення певного виду

діяльності. Зовні щодо особистісного сприйняття ділова репутація проявляється у формуванні громадської думки про особу, її ділові якості. Категорія «ділова репутація» властива фізичним та юридичним особам. Певною мірою юридичним особам «позитивна характеристика» ділової репутації важливіша, ніж фізичним.

Складним і спірним є питання про наявність ділової репутації у неприбуткових організацій. Ця категорія не оспорюється щодо прибуткових юридичних осіб. Проте щодо неприбуткових організацій у науковій літературі досить тривалий час висловлювалися протилежні погляду.

Важливе значення у цій галузі має Постанова Пленуму Верховного Суду України «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» [3].

У Постанові питання, що стосуються категорії осіб, які мають право пред'явити позови у справах про захист ділової репутації, роз'яснені в такий спосіб. Фізичні та юридичні особи, які вважають, що про них поширені невідповідні дійсності ганебні відомості, мають право пред'явити позови про захист честі, гідності та ділової репутації.

Жодних додаткових вимог щодо обов'язкової приналежності юридичної особи до прибуткової організації або підприємницької діяльності у Постанові Пленуму Верховного Суду України не міститься.

Нині можна стверджувати, що ділова репутація одна із нематеріальних благ прибуткових і неприбуткових юридичних осіб. Українське законодавство не дає тлумачень поняття «ділова репутація», проте постанова Пленуму Верховного Суду від 27 лютого 2009 року № 1 визначає ділову репутацію юридичної особи, у тому числі підприємницьких товариств, фізичних осіб – підприємців, адвокатів, нотаріусів та інших осіб як оцінку їх підприємницької, громадської, професійної чи іншої діяльності, яку здійснює така особа як учасник суспільних відносин [4].

Механізм їхнього захисту нині є єдиним. З положень ст. 299 ЦК України можна дійти висновку у тому, що законодавцем закріплено єдиний спосіб порушення прав на ділову репутацію – поширення відомостей, які не відповідають дійсності. У разі права на захист одним із головних критеріїв оцінки поширеної інформації буде невідповідність дійсності.

У Постанові Пленуму Верховного Суду України «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» надано поняття відомостей невідповідних дійсності – твердження про факти чи події, які не мали місця насправді щодо часу, до якого належать оспорювані відомості.

Поширення правдивих відомостей не є порушенням прав особи на ділову репутацію. Відповідно претендувати на захист особа за подібних ситуацій може лише тоді, коли поширення такої інформації порушує інші нематеріальні блага (зокрема, право на недоторканність приватного життя).

У законодавстві передбачено спеціальний порядок захисту прав і законних інтересів при поширенні правдивих відомостей негативного характеру у засобах масової інформації. Особа може опублікувати відповідь у цьому засобі масової інформації, а у разі незаконної відмови в опублікуванні відповіді у зазначеної особи виникає право вимагати компенсації нематеріальної шкоди.

Незважаючи на вищезазначені положення про захист прав особи у разі достовірної дифамації, деякі автори вважають, що відсутність у цивільному праві підстав для захисту ділової репутації особи у разі її порушення поширенням достовірних відомостей, що ганьблять, обмежує можливість реалізації права на захист даних благ. Висловлюється думка про необхідність розробки поняття достовірної інформації, при поширенні якої також може мати місце порушення прав юридичної

особи на ділову репутацію. Необхідно звертати увагу на спосіб та специфіку викладу такої інформації.

Якщо достовірна інформація викладена у образливій формі або з використанням неналежних виразів, особі може бути надано право вимагати вибачення або офіційної заяви з цього приводу. Спростування є спеціальним способом захисту немайнових прав під час поширення недостовірної інформації про особу. У загальному вигляді положення про спосіб захисту прав зафіксовані в ЦК України, згідно з яким відомості, що ганьблять ділову репутацію громадянина і набули поширення в засобах масової інформації, у цих же засобах масової інформації повинні бути спростовані.

Фізичним особам доступний ще один спосіб захисту прав у разі порушення нематеріальних благ – відшкодування моральної шкоди. Однак стосовно юридичних осіб дана категорія не застосовна. Нині у судовій практиці та у науковій літературі склалася аналогічна категорія щодо юридичних осіб – репутаційна шкода.

Ні законодавцем, ні судовими органами не заперечується наявність у юридичної особи права на захист ділової репутації. Це право однаково притаманне прибутковим і неприбутковим організаціям. У судовій практиці склався механізм захисту нематеріальних благ юридичної особи через застосування категорії репутаційної шкоди.

Література

1. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV/ URL. https://zakon.rada.gov.ua/laws/card/435-15
2. Про затвердження Національного положення (стандарту) бухгалтерського обліку: Наказ Міністерства фінансів України ввід 18.10.1999 рр. № 242. URL. https://zakon.rada.gov.ua/laws/show/z0750-99#Text
3. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленума Верховного Суду України від 27.02.2009 р. № 1. URL. https://zakon.rada.gov.ua/laws/show/v_001700-09#Text
4. Ділова репутація: судова практика захисту. ТОВ «ЛІГА ЗАКОН», 2023. URL. https://uz.ligazakon.ua/ua/magazine_article/EA016396

Терещенко О. О.

курсант Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ;

Прокопов С. О.

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

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ДРОНІВ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Застосування сучасних технологій у поліцейській діяльності має значний потенціал для покращення ефективності і безпеки правоохоронних органів. Одним із найважливіших досягнень в цій сфері є використання дронів, або безпілотних літальних апаратів. Дрони, завдяки своїм унікальним можливостям, здатні змінити підхід до забезпечення громадського порядку та здійснення поліцейських операцій. Ціллю даного дослідження є вивчення використання дронів у діяльності Національної поліції України та розкриття їх потенціалу для забезпечення безпеки громадян, виявлення

злочинів та підвищення ефективності поліцейських операцій. У рамках дослідження будуть розглянуті наявні системи дронів, їх переваги, технологічні та правові аспекти використання, а також виклики та перешкоди, з якими стикається поліція при впровадженні дронів у свою роботу.

Використання дронів у поліцейській діяльності вже довело свою ефективність у багатьох країнах світу, де вони успішно використовуються для надання допомоги під час пошуково-рятувальних операцій, контролю над територією, виявлення злочинів та спостереження за масовими заходами. Впровадження дронів у діяльність Національної поліції України має потенціал покращити оперативну реакцію, збільшити рівень безпеки громадян та сприяти більш ефективному використанню людських ресурсів. Застосування дронів у діяльності Національної поліції України може стати вагомим кроком у напрямку модернізації поліцейського апарату та покращення якості надання правоохоронних послуг. Впровадження новітніх технологій, таких як дрони, покаже високий рівень професійності та готовності Національної поліції до викликів сучасного світу.

Поточний стан використання дронів у поліції України свідчить про поступове впровадження цієї сучасної технології в поліцейську діяльність. Національна поліція України розуміє потенціал, який надають дрони, тому здійснює кроки щодо впровадження їх у свою роботу. На сьогоднішній день Національна поліція України вже має на озброєнні деякі системи дронів, які використовуються для різних цілей. Одним із прикладів використання дронів є їх застосування під час пошуково-рятувальних операцій. Дрони дозволяють здійснювати повітряну розвідку території, знаходити важкодоступні місця, де можуть перебувати постраждалі або зниклі особи, та надавати важливі візуальні дані для координації дій рятувальних служб. Крім того, дрони використовуються для підвищення безпеки під час масових заходів та патрулювання над великими територіями. Вони забезпечують можливість здійснювати нагляд та спостереження з повітря, що дозволяє оперативно виявляти можливі порушення громадського порядку, заборонених предметів чи небезпеки для громадян. Завдяки високоякісній камері та маневреності, дрони можуть бути використані для запису порушень, які здійснюються з використанням автомобілів, що не відповідають правилам дорожнього руху.

Варто відзначити, що впровадження дронів у поліцейську роботу також супроводжується навчанням та підготовкою персоналу. Поліцейські отримують спеціальні навички та знання з керування дронами, технічного обслуговування та аналізу отриманих візуальних даних. Незважаючи на певний прогрес у використанні дронів, існують певні виклики та перешкоди, з якими стикається поліція. Це включає такі аспекти, як забезпечення безпеки та конфіденційності зібраних даних, розробка відповідних правових рамок, а також фінансування та підтримка технічного оснащення. Загалом, поточний стан використання дронів у поліції України свідчить про поступовий розвиток та використання цих технологій для поліцейських потреб. [1]

Використання дронів у діяльності поліції супроводжується рядом технологічних та правових аспектів, які потребують уваги та розробки відповідних регулятивних механізмів. Одним з технологічних аспектів є розвиток та вдосконалення самого дронового обладнання. Технології дронів швидко розвиваються, і важливо впевнитися, що поліцейські дрони відповідають сучасним вимогам і можуть ефективно виконувати свої завдання. Це включає вдосконалення систем навігації та автономності, які дозволяють дронам працювати у різних умовах і покращують точність їх руху та маневреність. Також важливим аспектом є якість камер та обладнання для збору візуальної інформації, що забезпечує якісне зображення та передачу даних. У сфері правових аспектів використання дронів в поліції важливо забезпечити дотримання приватності та безпеки громадян. Збір, обробка та зберігання даних, отриманих від дронів, повинні

підпадати під відповідні правові норми та обмеження. Важливо розробити відповідні протоколи та процедури щодо обробки та зберігання таких даних з метою захисту особистої інформації та запобігання її зловживанню. Також потрібно розробити чіткі правила щодо використання дронів у поліцейських операціях. Це включає визначення меж використання, заборону незаконного перехоплення комунікацій, регулювання збору даних та обмежень у зоні приватних просторів. Правила повинні унеможливлювати дії, такі як шпигунство або порушення приватності, і забезпечувати справедливе та етичне використання дронів поліцією. Загалом, технологічні та правові аспекти використання дронів у діяльності поліції потребують системного підходу та узгодження. Необхідно забезпечити розвиток та вдосконалення дронової технології, одночасно дотримуючись етичних принципів, захищаючи приватність та безпеку громадян, та створити відповідну правові рамки, які регулюють використання дронів поліцією.

Загалом, використання дронів у діяльності поліції дозволяє підвищити оперативність, ефективність та безпеку поліцейських операцій. Вони забезпечують широкий огляд з повітря, швидкий доступ до складних та важкодоступних місць і надають важливі візуальні дані для прийняття обґрунтованих рішень. [2]

У висновку можна констатувати, що використання дронів у діяльності Національної поліції України має значний потенціал для покращення ефективності та результативності поліцейських операцій. Переваги використання дронів включають можливість повітряного нагляду та розвідки, пошуково-рятувальних операції, контролю дорожнього руху та забезпечення безпеки громадян, а також нагляд під час масових заходів. Використання дронів у діяльності поліції може відкрити нові можливості для забезпечення громадської безпеки, покращення відповіді на надзвичайні ситуації та розвитку поліцейської роботи в Україні. Зробивши це, Національна поліція України зможе максимально використовувати переваги дронових технології для забезпечення безпеки та порядку в країні.

Література

1. Гребенюк А.М. Використання безпілотників для потреб поліції / А.М. Гребенюк, Л.В. Рибальченко // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 28 листоп. 2019 р.). – Дніпро: ДДУВС, 2019. URL: https://er.dduvs.in.ua/bitstream/123456789/5024/1/3.pdf
2. Ігор Сєров. Українська поліція почала ловити злочинців з повітря. URL: https://ukraine.segodnya.ua/ua/ukraine/policiya-nachala-lovit-prestupnikov-s-vozduha-1053821.html

Титаренко А. В.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Клімушин П. С.

доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ТЕХНОЛОГІЧНІ ІННОВАЦІЇ ЯКІ ДОПОМОЖУТЬ ПОЛІЦІЇ ДЛЯ ВИЯВЛЕННЯ ЗЛОЧИНІВ

Технології змінюють роботу поліції у 21 столітті, пропонуючи нові інструменти для боротьби зі злочинністю та нові категорії злочинів. Одна з найбільш суперечливих

поліцейських технологій пов'язана з використанням програмного забезпечення для розпізнавання осіб, яке виявилося ефективним інструментом розслідування. Щороку виникають нові технологічні інновації, які через певний час стають буденною реальністю, а саме [1]:

- Розумні окуляри компанії Google (2019 р.) – це окуляри доповненої реальності, які забезпечують поєднання реальних і згенерованих комп'ютером зображень, які накладаються одне на одне, у результаті чого користувач на базі доступу до баз даних осіб та об'єктів, що розшукується, має можливість ідентифікувати їх в реальному часі.
- Розумні дані – це автоматизація процесу побудови оперативно-пошукового списку контактів, поштових скриньок, повідомлень осіб, що підозрюються тощо.
- Дисплеї без екранів – це контактні лінзи для очей, що проектують віртуальне зображення на сітківку ока, в процесі проведення розвідувальної та спостережної діяльності поліцейських.
- Нейрокомп'ютерні інтерфейси, які організують відповідно до думки користувача дії на комп'ютері, тобто управляють комп'ютерної системою без допомоги мишки для забезпечення ефективної роботи фахівців поліції.
- Цифрові завантаження медіафайлів, документів для зменшення розповсюдження фізичних копій продуктів в діяльності підрозділів поліції.
- Робототехніка для заміщення безпечних операцій в діяльності поліцейських.
- Бездротова передача енергії для зарядки без кабелю поліцейських смартфонів, планшетів, електромобілів.
- Графен для забезпечення особистої безпеки поліцейських як надміцний матеріал, а також для виготовлення нової елементної бази комп'ютерів.
- Біометричні системи безпеки компанії Apple, яка змогла впровадити технологію сканування відбитків пальців у смартфоні. Біометрія допомогла розвинути системи мобільних платежів NFC, які використовують додаткову безпеку для автентифікації платежів. Технологія розпізнавання осіб (відбитків пальці з допомогою датчиків під сам екран смартфону) Face ID є подальшим розвитком NFC.
- Бездротові навушники, які рахують частоту серцевих скорочень, контактні лінзи, які вимірюють рівень цукру в крові, тощо для визначання стану здоров'я поліцейських.
- DATA-технології для забезпечення прогнозної політики у кримінальної сфері.
- Криптографічні методи захисту інформації в сфері безпеки баз даних з обмеженим доступом інформаційного порталу національної поліції.

Висновки. Завдяки дослідженням можна зробити висновок, що за останній час з'явилось багато технологій у західних країнах, які допомагають і покращують службу поліції [2]. Тому Україні треба оновлювати свої передові технології, щоб понизити рівень злочинності.

Література

1. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
2. New Technology in Law Enforcement. URL: https://www.powerdms.com/policy-learning-center/new-technology-in-law-enforcement

Федчак І. А.
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРАКТИЧНІ АСПЕКТИ ВИРІШЕННЯ ПРОБЛЕМ ЗА МЕТОДОЛОГІЄЮ SARA ПІД ЧАС РЕАЛІЗАЦІЇ МОДЕЛІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ, ОРІЄНТОВАНОЇ НА ПЕВНУ ПРОБЛЕМАТИКУ (Problem-Oriented Policing)

Як відомо, усі сфери суспільних відносин уражені проявами злочинності, і такий стан справ спостерігається в усіх країнах світу. І хоча практика діяльності правоохоронних органів нараховує багато століть напрацьованого досвіду протидії поширенню злочинності, проте універсальних заходів щодо обмеження кримінальних активності сформовано бути не може у силу різноманітних змінних об'єктивних та суб'єктивних причин. Разом з тим учені та практичні співробітники правоохоронних органів перебувають у стані постійного пошуку новітніх підходів до організації діяльності, застосування яких дозволить досягати максимальних результатів при виконанні своїх службових обов'язків з огляду на обмежені ресурси (матеріальні, технічні, людські, фінансові тощо) [1, с. 82].

Позитивним прикладом сформованої зарубіжної правоохоронної практики упереджувального впливу на злочинність є реалізації проактивної моделі діяльності поліції, орієнтованої на вирішення проблем (Problem-Oriented Policing), яка спрямована на подолання першопричин злочинності та порушення громадського порядку. Методологія проблемно-орієнтованої поліцейської діяльності полягає в пошуку цих основних причин (проблем), їх детальному аналізі, пропозиції оптимальних рішень (контрзаходів), а також оцінці ефективності цих рішень щодо нейтралізації проблеми [2, с. 91-92].

Концептуально модель діяльності поліції, орієнтованої на вирішення проблем (Problem-Oriented Policing) впливає на зміну результатів проблеми завдяки підвищенню знань про механізми, за допомогою яких діє конкретна проблема, і реагування на них, використовуючи методологію SARA. З наукової та практичної сторони запровадження методології вирішення проблем SARA (сканування (Scanning), аналіз (Analysis), реагування (Response), аналітична оцінка (Assessment)), у моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), набула ще більшого практичного значення, оскільки допомогла фахівцям-практикам упровадити у роботу при вирішення складних проблем процес розв'язання їх на фаховому і методичному рівні з відповідним науковим рівнем.

Реалізація такої методології формує стійкі передумови для розкриття складних механізмів, що діють у проблемах злочинності, і для розробки спеціально розроблених персоніфікованих заходів для вирішення основних умов, які викликають такі проблеми.

Для того, щоб сформувати вичерпне та відповідне дійсності розуміння криміногенної ситуації співробітникам поліції слід здійснити сканування операційного середовища (S). Цей крок вимагає від співробітників поліції здійснити виявлення потенційних проблем та провести їх пріоритизацію.

На другому етапі застосування методології SARA (абревіатура «А» означає аналіз), проводиться ґрунтовне аналітичне дослідження отриманих даних, їх характеристик з метою визначення першопричин виникнення кримінальних та

адміністративних проблем та умов, за яких вони діють. Аналіз дозволяє ідентифіковувати конкретні географічні місця, які найбільш сприятливі для прояву протиправної діяльності. Крім того, оцінюють характеристики такого місця, з метою визначити чинники, які сприяють поширенню протиправної поведінки. Аналіз тенденцій також проводиться з метою пошуку належної реакції з боку поліції. Аналіз відомостей про проблеми дозволяє приймати рішення про те, як їм протидіяти – підготувати відповіді.

На третьому етапі – реагуванні (R) – співробітники поліції розробляють та впроваджують заходи, спрямовані на усунення причин виникнення та умов існування проблем. Здійснюючи діяльність щодо діагностики проблем та розробки рішень слід дотримуватись поетапного процесу. Цей процес акцентує увагу на розумінні сутності різноманітних кримінальних проблем та їх причин, розробці та перевірці рішень щодо їх нейтралізації, і здійснюється на основі напрацьованого досвіду поліції.

Останнім кроком застосування методології SARA є аналітична оцінка (A), яка включає оцінку впливу відповіді та того, яких результатів вдалось досягти.

У розгорнутому вигляді процес діагностики проблем та розробки рішень у моделі Problem-Oriented Policing складається з таких етапів: 1. ретельне дослідження ситуації; 2. чітке формулювання проблеми; 3. вибір конкретної проблеми для реагування (реакції); 4. збір та обробка даних про проблему; 5. аналіз причин виникнення проблеми; 6. розробка плану вирішення проблеми; 7. перевірка (тестування) плану вирішення проблеми; 8. оцінка результату перевірки (тестування) способу вирішення проблеми; 9. впровадження рішення у реалізацію; 10. оцінка якості процесу реалізації рішення проблеми, а згодом – перехід до наступної проблеми [3].

Прикладом застосування методології вирішення проблем SARA під час реалізації моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing)Problem-Oriented Policing) може бут наступна ситуація. Так, до прикладу, відділ поліції може визначити, що злочинність, пов’язана з обігом наркотичних речовин зростає, що становить проблему, яка потребує вирішення (фаза сканування). Подальше вивчення природи злочинів, пов’язаних з поширенням незаконного обігу наркотичних речовин, може виявити проблемні ділянки місцевості та окремі часові періоди кримінальної активності (фаза аналізу). На основі отриманої аналітичної інформації співробітники поліції можуть прийняти рішення про застосування посиленого патрулювання у визначений час та визначену місцевість, які вважаються проблемними, а також посилити співпрацю з громадськими організаціями для реалізації програм лікування від наркотичної залежності (фаза реагування). Через певний період часу відділ поліції може порівняти показники про стан поширення незаконного обігу наркотичних речовин, в цілому на території обслуговування, а також у цільових областях, до та після впровадження відповіді (фаза оцінки), за потреби до заходів реагування вносяться корективи.

Цей процес загалом, а не конкретна проблема чи обрана відповідь, представляє основну концепцію моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing). Таким чином, різноманітний набір варіацій проблем, відповідей та видів і тривалості втручань можливий для низки цілей (тобто в центрі уваги можуть бути як проблемні місця різного розміру так і проблемні люди), і практично для будь-якої одиниці аналізу.

Як висновок слід зазначити, що застосування методології вирішення проблем SARA під час реалізації моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing) дозволяє напрацювати позитивний досвід вирішення різноманітних проблем злочинності, застосування якого може сприяти більш ефективному застосуванню ресурсів правоохоронних органів до повторюваних проблем.

Література

1. Федчак І. А. Практичні аспекти вирішення проблем злочинності під час реалізації моделі діяльності поліції, орієнтованої на певну проблематику (Problem-Oriented Policing). Науковий журнал «Juris Europensis Scientia» № 3, 2023. С. 82-85. URL: DOI https://doi.org/10.32782/chern.v3.2023.17
2. Федчак І. А. Концептуальні основи сутності та змісту моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing). «Ампаро» 2023. № 2. Запорізький національний університет. С. 90–96. URL: DOI https://doi.org/10.26661/2786-5649-2023-2-12
3. Problem-Oriented Policing. Better Policing Toolkit. RAND. URL: https://www.rand.org/pubs/tools/TL261/better-policing-toolkit/all-strategies/problem-oriented-policing.html

Хаджийський М. О.

курсант ННІ ППФПНП Дніпропетровського державного університету внутрішніх справ.

Рибальченко Л. В.

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

ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

У наш час інформаційна безпека є досить важливою складовою для усієї держави. Україні важливо забезпечити власний суверенітет в усіх сферах діяльності. На теперішній час, під час повномасштабного вторгнення інформаційна безпека набула особливого значення.

Інформаційна безпека – це захист від дезінформації та кібератак, які зможуть порушити стійкість країни, стан захищеності інформаційного середовища суспільства, особи, організації. Інформаційна безпека країни в основному характеризується ступенем захищеності і стійкістю основних сфер життєдіяльності: науки, економіки, техносфери, військової сфери, сфери управління. Зараз особливо важливо зосередити увагу на функціонуванні системи забезпечення інформаційної безпеки України. Для громадян це не тільки зовнішньополітична інформація, а й усі сфери, до забезпечують повне функціонування держави.

Інформаційне суспільство – це відносно глобальне поняття, яке описує рівень всього людства на даному етапі розвитку. Ми можемо сказати, що різні суспільства перебувають на різних етапах інформаційного та технологічного розвитку. На теперішній момент ми можемо спостерігати те, що людина постійно у пошуку інформації. Або, ще більше стосується сучасної людини – це пошук інформації через мережу Інтернет. Упевнившись в цьому, ми можемо сказати, що безпека не вийшла на новий рівень розуміння і відношення до її забезпечення. Таким чином, виникла актуальність розглянути інформаційну безпеку як окрему наукову категорію і як суспільне явище, яке створює нові світові умови і формування нових норм і правил суспільних відносин.

На жаль, українці стали свідками того який вплив має інформація на сьогоднішній день. Для повного розуміння цих процесів ми повинні розуміти природу і контекст інформаційного протиборства. Поняття інформаційної безпеки можна розглядати і тлумачити різними спробами, наприклад : доктринальні, енциклопедичні, нормативно-

правові рішення. Усі методологічні підходи та сфери застосування можуть відрізнятись. Розглянувши нормативно-правові акти України інформаційної безпеки з легальної сторони, у статті 17 Конституції України свідчить про «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» .

Усі основні нормативні акти для забезпечення міжнародної інформаційної безпеки закріплені у Статуті ООН і в ряді інших нормативно-правових актах. Серед основних правових принципів щодо забезпечення інформаційної безпеки виділяють суверенну рівність держав в інформаційній сфері, щодо використання ресурсів, забезпечення інформаційного суверенітету, а також рівна участь в процесах розробки міжнародних правових документів в інформаційній сфері.

Інформація для України є зброєю, бронею та інструментом впливу. Найбільш потужним методом боротьби став інформаційний фронт, як зі сторони суспільства так і державних органів влади. За останні роки усі процеси в державі розвивались досить динамічно, та інформаційна безпека не є виключенням. Тому сьогодні це є процесом який здійснює важливий інформаційний вплив.

Роль інформації під час війни - критична, і зазвичай розглядається в контексті інформаційної війни або протиборства. Інформація є предметом дослідження багатьох сфер, однак розглядаючи саме історію розвитку інформаційних конфліктів роль перетворюється на системне використання інформаційно-комунікативних технологій при веденні війни.

Однією із складових інформаційної безпеки є комплексний захист прав і інтересів від непередбачуваного й шкідливого впливу. Іншими словами, головною ознакою стану захищеност в інформаці ній сфері є оптимальне співвідношення інтересів людини, суспільства й держави. Високими показниками забезпечення воєнно-інформаційної безпеки держави є гарантування доступу до інформації, безпеки інформації, мереж зв'язку, інформаційно-телекомунікаційних систем.

В ці роки війни Україна як ніколи постраждала саме в сферах критичної інфраструктури, і держава, працюючи на останній засобах успішно вистояла випробування на темряву, відсутність зв’язку та інше. Однак, якщо дивитись на подібну ситуації через перспективу, то слід сказати про стан мереж зв’язку та інформаційно-телекомунікаційні системи, адже при черговому вимкненні світла людина втрачає можливість робити базову для нашого суспільства річ – дзвонити, може втратитися її конфіденційність інформації, захищеність та інше [3].

За останні роки Україна зробила ряд важливих рішень щодо врегулювання інформаційної безпеки на нормативно-правовому рівні. Загальному мова йдеться про Стратегію інформаційної безпеки, основною метою якої є посилення забезпечення інформаційної безпеки держави, її простору, підтримка охорони і захисту державного суверенітету. Сучасною зброєю є не обов’язково вогнева потужність, а ефективність сучасної зброї все більше визначається ступенем інформаційної забезпеченості. На полі бою все більше використовують інформаційний фронт, тобто сьогодні це потужний засіб війни, оскільки її технічна інноваційність, спроможність наприклад залишити місто без світла чи тепла.

З інформаційною безпекою під час війни варто зробити наступні висновки:

- важливість інформаційної безпеки полягає у військових конфліктах інформаційна безпека стає критично важливою, оскільки дезінформація та кібератаки можуть суттєво підірвати обороноздатність та довіру населення;
- захист від дезінформації виступає через владу та громадян, які повинні бути освіченими та здатними розрізняти правдиву інформацію від фейкових новин та пропаганди;

- кіберзахист полягає через захист від кіберзагроз і включає в себе заходи для захисту критичних інфраструктур, мереж та даних від атак та порушень безпеки;
- співпраця та обмін інформацією має відбуватися через співпрацю між країнами та обміном інформацією з метою попередження кібератак та інших загроз;
- планування кризових ситуацій відбувається через розробку та впровадження планів кризового управління, що є ключовими для ефективного відгуку на інформаційні загрози під час війни.

Таким чином, інформаційна безпека є необхідною для забезпечення національної безпеки під час війни і вимагає створення відповідних ефективних та дієвих умов для забезпечення захисту від можливих загроз та небезпек для кожного її громадянина та усієї України.

Література

1. Інформайційно-воєнна безпека як елемент національної безпеки України / Володимир Юрійович Артемов, Володимир Олексійович Хорошко, Юлія Євгеніївна Хохлачова, Володимир Володимирович Погорелов // Захист інформації. – 2022.– Т. 24, № 1. – С. 21-29
2. Перше правило інформаційної безпеки під час війни – не вір джерелам інформації ворога. Київська обласна військова адміністрація. Режим доступу : https://koda.gov.ua/pershe-pravylo-informaczijnoyi-bezpeky-pid-chas-vijny-ne-vir-dzherelam-informacziyi-voroga/
3. Іванова Є.І. Воєнно-інформаційна безпека України за умов ескалації конфлікту на сході України. Режим доступу : https://jarch.donnu.edu.ua/article/download/13389/13296

Хімко Я. П.

аспірант кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ

ПЕРСПЕКТИВИ ДОСЛІДЖЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ХМАРНИХ ПОСЛУГ В УКРАЇНІ

Глобальний прискорений розвиток науки і техніки дозволив суспільству використовувати різні інформаційні технології у повсякденній та професійній діяльності. Серед таких технологій важливе місце посідають хмарні інформаційні технології. Закон України від 17.02.2022 р. № 2075-IX «Про хмарні послуги» [1] передбачає збереження інформації у хмарних сховищах. Хмарне сховище інформації є модель онлайн-сховища, в яке завантажуються дані користувача і зберігаються в центрі обробки даних. Хмарне сховище інформації – це особлива високотехнологічна цифрова послуга. Специфіка використання викликала необхідність проведення аналізу правового регулювання зберігання інформації, як послуги, за допомогою цієї технології. Хмарні сховища інформації використовуються повсюдно. Технологічна основа та техніка, що використовується, є подібними, однак правове регулювання даних відносин відрізняється в різних країнах.

На основі вивчення досвіду України та держав Європейського Союзу виявляються особливості, послідовності та напрями розвитку правового регулювання надання хмарних послуг. Порівняльно-правовий аналіз дозволяє виділити загальні риси,

вивчити можливість використання методів регулювання, що застосовуються в Європейському Союзі.

Для створення ефективного правового регулювання хмарних послуг можуть запозичуватися окремі законодавчі моделі та рішення, які застосовуються у країнах Європейського Союза, а також моделі та стандарти, що пропонуються міжнародними інститутами, що діють у даній сфері. На рівні Європейського Союзу розробляються уніфіковані підходи та принципи в цій галузі, що надасть більшої чіткості та універсальності правовим механізмам, що використовуються у регулюванні відносин із зберігання інформації у хмарному сховищі та при надання інших послуг у зазначеній сфері. Перспектива розширення використання технології вимагає більш поглибленого аналізу її правового режиму, що сформувався в Україні та найбільш розвинених із правової та технологічної точки зору країнах Європейського Союзу.

Особливе значення має дослідження правового регулювання надання хмарних послуг відповідно до Порядку передачі, збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) та їх резервних копій, розміщених на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, затвердженого постановою Кабінету Міністрів України від 30 грудня 2022 року № 1500 [2].

Поширення розглянутої технології пояснюється природним технологічним розвитком суспільства, та тим, що використовувати хмарні послуги економічно вигідно. Вивчення правового режиму зберігання інформації з погляду наукових підходів, позицій законодавця, правознавців є важливим, оскільки результати дослідження можуть бути використані стосовно інших технологій.

Необхідно дослідити правове регулювання надання хмарних послуг щодо зберігання інформації в хмарному сховищі, який включає: режим програми для електронних обчислювальних машин віртуальне майно; режим центру обробки даних – матеріального майна, що є системоутворюючим для функціонування програми хмарного сховища у контексті хмарних послуг; режим інформації користувача, яку користувач завантажує у сховище хмар.

Правовідносини щодо використання хмарних послуг, у контексті хмарних сховищ інформації розглядаються з позиції інформаційного права та з погляду адміністративного права, оскільки розвиток цієї технології та використання мережі Інтернет визначають наявність іноземного елемента. Правове регулювання надання хмарних послуг, у тому числі зберігання інформації в хмарному сховищі торкається питань авторського права – авторські права користувача на інформацію, що завантажується ним, на базу даних, яку він створив при використанні хмарного сховища; авторські права на програму хмарного сховища інформації та інтелектуальну власність; конфіденційність інформації – захист відомостей користувача від розповсюдження з хмарного сховища; захист персональних даних.

Складність правового регулювання відносин, пов'язаних із наданням хмарних послуг, у тому числі зберіганням інформації в хмарному сховищі, полягає в тому, що не всі аспекти цих правовідносин врегульовані правовими нормами, що властиво багатьом інформаційних технологій. Створення нових законів для кожної нової інформаційної технології не завжди є продуктивним, оскільки невідомо, чи використовуватиметься технологія тривалий час.

У юридичній науці в державах Європейського Союзу йде процес формування правових підходів до регулювання різних аспектів правовідносин, які складаються завдяки використанню мережі Інтернет та інформаційних технологій. Значний вклад внесли вчені: Дж. Катаге, Ф. Кох, Д. Крегер, Ф. Ниманн, Й.-А. Пауль, Ю. Тегер, Х. Ханкен, Т. Херен, Э. Вінфилд, Р. Вебер, М. Гейтс, Т. Гренс, Д. Джонсон, Д. Менте, Д. Морріс, М.

Моуслі, С. Муругезан, П. Мелл, Дж. Неклеріо, Р. Ньюфельд, Д. Пост, С. Уилскі, Л. Едвардс та інші.

Необхідно провести комплексний аналіз правового регулювання хмарних послуг, виявлення аспектів, які потребують регулювання та наукового осмислення, пропозиція та обґрунтування напрямів розвитку правового регулювання хмарних послуг в Україні, адаптації нормативної бази Європейського Союзу до національного законодавства.

Для досягнення зазначеної мети потрібно виконати такі завдання:

- провести аналіз правового регулювання надання хмарних послуг;
- охарактеризувати з позиції інформаційного права програму для електронно-обчислювальної машини, що використовується для зберігання інформації;
- дослідити правовий режим роботи центру обробки даних, що забезпечує роботу інформаційної технології;
- вивчити правову природу хмарних послуг щодо використання хмарного сховища інформації;
- розглянути правові проблеми, пов'язані із укладанням договору на використання хмарних послуг;
- проаналізувати застосовного права щодо використання хмарних сховищ інформації у разі наявності іноземного елемента.

Основні перспективи дослідження правового регулювання хмарних послуг в Україні полягають в розробці заснованих на результатах наукового аналізу практичних пропозицій щодо вдосконалення використання хмарних послуг, внаслідок чого буде сформовано системне уявлення про правове регулювання хмарних послуг, на підставі досвіду регулювання використання технології в державах Європейського Союзу.

Література

1. Закон України від 17.02.2022 р. № 2075-IX «Про хмарні послуги». URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text
2. Постанова Кабінету Міністрів України від 30 грудня 2022 року № 1500 «Деякі питання забезпечення функціонування державних інформаційних ресурсів». URL: https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#Text

Царук Ю. Ю.

ад'юнкт кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ ЯК ДІЄВИЙ ЗАХІД ПРИЙНЯТТЯ «ВИКЛИКУ» СУЧАСНОСТІ В ІНФОРМАЦІЙНО – АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ПРОТИДІЇ ШАХРАЙСТВУ. ВИРІШЕННЯ ОКРЕМИХ ПРОБЛЕМНИХ АСПЕКТІВ В ПРОВЕДЕННІ ТИМЧАСОВОГО ДОСТУПУ ДО РЕЧЕЙ І ДОКУМЕНТІВ

На сьогоднішній день, особливої актуальності та гостроти набувають проблеми виявлення, припинення та документування підрозділами Національної поліції фактів шахрайства, учинених шляхом незаконних операцій з використанням електронно – обчислювальної техніки. На жаль, в умовах воєнного стану такий вид кримінального

правопорушення не лише не зник, а й має можливість до створення нових умов для сприяння його вчиненню.

Протидію шахрайству в мережі Інтернет слід розглядати як комплекс організаційно – тактичних дій, що здійснюється відповідними суб'єктами з метою захисту і охорони прав користувачів Інтернету.

В інформаційному просторі існує чимало способів вчинення шахрайства. Ситуація з протидією вчинення шахрайства, шляхом незаконних операцій з використанням електронно – обчислювальної техніки, надалі залишається складною, так як жертвами Інтернет – шахрайства можуть стати не тільки громадяни, але й юридичні особи, органи державної влади, місцевого самоврядування, підприємства, установи та організації різних форм власності.

Значний внесок у формування теоретичного підґрунтя розслідування шахрайства в Інтернеті зробили дослідники, серед яких: Д. Ричка, Т. Коршикова, А. Рейнгольд, С. Чучко, В. Берназ, В. Лисенко, Ю. Орлов, С. Чернявський, В. Шевчук, О. Шляхов, та інші.

Водночас, для успішної протидії злочинам вказаної категорії, вважаю необхідне належне інформаційно – аналітичне забезпечення оперативно – розшукової діяльності (далі ОРД) підрозділів Національної поліції України (далі НПУ), яке полягає в збиранні, опрацюванні, узагальненні та аналізу оперативної, оперативно – розшукової, оперативно – довідкової, аналітичної, статистичної і контрольної інформації для оцінки ситуації і прийняття обґрунтованих оптимальних рішень на всіх рівнях управління НПУ [1, с.83].

Ст.5 Закону України «Про оперативно-розшукову діяльність», передбачає суб'єктів здійснення ОРД та визначає, що ОРД здійснюється оперативними підрозділами, в тому числі НПУ, зокрема підрозділами кримінальної поліції. Оперативним підрозділам створюються в складі правоохоронних органів, виконують завдання, визначені оперативно – розшуковим законодавством, відповідно до своєї компетенції, використовують гласні та негласні, розвідувальні та контррозвідувальні заходи. Відповідно до п.18 ст.8 вказаного закону підрозділи, що здійснюють ОРД, мають право створювати і застосовувати автоматизовані інформаційні системи [2].

Ст.25 Закону України «Про Національну поліцію» визначено, що НПУ здійснює інформаційно – аналітичну діяльність виключно для реалізації своїх повноважень. Кримінальна поліція забезпечує протидію злочинності, захист прав та свобод, інтересів суспільства і держави від протиправних посягань [3].

Для ефективної боротьби із фактами шахрайства, оперативним підрозділам НПУ, необхідно мати відповідну інформацію відносно ідентифікаційної належності особи злочинця до терміналу мобільного зв'язку.

Фактично така ідентифікація користувачів електронних комунікаційних мереж, можлива за рахунок їх особистої ідентифікації згідно паспортних даних у постачальника комунікаційних послуг, доступ до баз даних яких підрозділам НПУ надано в межах визначених ст.ст. 159 – 166 глави 15 Кримінально – процесуального кодексу України (далі КПК України), якими передбачено загальні положення, підготовка та розгляд клопотань, порядок виконання ухвали слідчого судді суду про тимчасовий доступ до речей і документів, а також наслідки невиконання такої ухвали [4].

На мою думку, найбільш дієвим способом в забезпеченні діяльності підрозділів НПУ та ключовим заходом забезпечення кримінального провадження в розслідуванні та протидії вчинення шахрайства, в умовах сучасності, є швидке виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів, з метою отримання інформація та фактичних даних, про наявність чи відсутність обставин, що мають значення для кримінального провадження та підлягають доказуванню, виконання якого можливе шляхом накладення електронного підпису особи, якій надано таке право

тимчасового доступу, без її особистої участі за місцем знаходження юридичної адреси особи, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець таких речей або документів, що значно пришвидшить темп організації досудового розслідування матеріалів кримінального провадження та зменшить бюрократичні чинники в даному питанні.

Не менш важливим є особливості обов'язкової реєстрації користувачів мобільного зв'язку за паспортами, визначені Законом України «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку», яким усіх абонентів мобільного зв'язку ідентифікують до 01.01.2025 року, а до цього часу не заборонено отримання комунікаційних послуг не ідентифікованим абонентам [5].

В НПУ функціонує Інформаційно – телекомунікаційна система «Інформаційний портал Національної поліції України» (далі система ІПНП), яка призначена для інформаційно – аналітичного забезпечення діяльності Національної поліції, наповнення та підтримки в актуальному стані інформаційних ресурсів, що входять до Єдиної інформаційної системи МВС України (ЄІС МВС). Інструкція з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно – комунікаційної системи «ІПНП», затверджена наказом МВС №508 від 14.06.2019 із змінами та доповненнями [6].

Враховуючи те, що основним завданням системи ІПНП є інформаційно – аналітичне забезпечення діяльності НПУ, особисто вважаю, що з метою більш ефективного функціонування засад, спрямованих на протидію механізмам та способам вчинення шахрайства, швидкого, повного та всебічного розслідування матеріалів кримінальних проваджень, необхідно забезпечити належну, швидку, електронну взаємодію підрозділів НПУ з центральним органом виконавчої влади із спеціальним статусом – регуляторним органом (Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку), який утворюється Кабінетом Міністрів України, в частині ідентифікації користувачів електронних комунікаційних мереж, шляхом пошуку та аналізу інформації в інформаційних ресурсах регуляторного органу.

Національна поліція вживає всіх заходів, спрямованих на недопущення будь – яких порушень прав і свобод людини, пов'язаних з обробкою інформації. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації. Чинними нормативними актами визначено, що інформаційно – аналітичне забезпечення ОРД це передбачена законодавством України система запроваджених заходів, спрямованих на збір, узагальнення, аналіз, зберігання та використання інформації, у тому числі обмеженого доступу, що має значення для вирішення завдань цієї діяльності в інтересах досудового слідства, безпеки громадян, суспільства і держави. Основною метою інформаційно – аналітичного забезпечення ОРД є підвищення ефективності протидії злочинності, профілактична робота з криміногенною категорією громадян та особам, які перебувають на обліках НПУ. Аналітична робота не може здійснюватися окремо від інформаційної. В процесі аналізу інформації постійно виникають нові обставини та необхідність додаткового отримання інформації. Інформація є основою, фундаментом для аналітики та подальшого прогнозування. Інформаційно – аналітичного забезпечення ОРД НПУ починається з вивчення, аналізу та оцінки оперативної обстановки, яка склалася [1, с.87-100].

Висновки. Для ефективної боротьби із фактами шахрайства, оперативним підрозділам НПУ, необхідно мати відповідну інформацію відносно ідентифікаційної належності особи злочинця до терміналів мобільного зв'язку, що можна досягти шляхом обов'язкової реєстрації користувачів мобільного зв'язку за паспортами.

Належна, швидка, електронна взаємодія підрозділів НПУ під час використання системи ІПНП з центральним органом виконавчої влади із спеціальним статусом - регуляторним органом (Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку).

Найбільш дієвий спосіб в забезпеченні заходу кримінального провадження в розслідуванні та протидії вчинення шахрайства, в умовах сучасності, є швидке виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів, яке можливе шляхом накладення електронного підпису особи, якій надано право тимчасового доступу, без її особистої участі за місцем знаходження юридичної адреси особи, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець таких речей або документів, що значно пришвидшить темп організації досудового розслідування матеріалів кримінального провадження та зменшить бюрократичні чинники в даному питанні.

Література

1. Оперативно – розшукова діяльність. Навчальний посібник для підготовки до іспитів /2-ге вид. перероблене та доповнене/ - К.: «Центр учбової літератури», 2022. – 228 с.
2. Закон України «Про оперативно – розшукову діяльність» від 18.02. 1992 р. (із змінами та доповненнями). Електронний ресурс. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
3. Закон України «Про Національну поліцію» від 23.12.2015 р. (із змінами та доповненнями). Електронний ресурс. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
4. Кримінально – процесуальний кодекс України від 05.07.2012 р. (із змінами та доповненнями). Електронний ресурс. Режим доступу URL: https://zakon.rada.gov.ua.
5. Закон України «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку». Електронний ресурс. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/1971-IX#Text.
6. Наказ МВС №508 від 14.06.2019 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно – комунікаційної системи «ІПНП» (із змінами та доповненнями). Електронний ресурс. Режим доступу URL: https://ips.ligazakon.net/document/RE33710?an=1.

Чемерис А. О.

здобувач вищої освіти Національної академії внутрішніх справ.

Свобода Є. Ю.

професор кафедри криміналістичного забезпечення та судових експертиз Національної академії внутрішніх справ, кандидат юридичних наук, доцент

СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ЕКСПЕРТНОЇ СЛУЖБИ МВС УКРАЇНИ

Інформаційно-довідкове забезпечення судово-експертної діяльності виступає видом практичної діяльності, яка пов'язана з отриманням та використанням інформації

з інформаційно-пошукових систем. Конкретно для суб'єктів розслідування основним завданням забезпечення інформаційної бази є не лише пошук та одержання, а також оновлення та коригування вже наявних даних з метою використання їх в процесі виявлення, розкриття, розслідування та попередження кримінальних правопорушень.

Перш за все слід зазначити, що функціонування інформаційного забезпечення передбачене двома видами діяльності: безпосередньо отримання необхідної інформації з доступних й законних джерел, і саме накопичення та систематизація виокремленої потрібної інформації. Причому, на відміну від слідчої діяльності, експерти збирають дані лише з наявних об'єктів матеріального світу, якими в кримінальному провадженні виступають сліди.

Самі сліди розглядаються наукою в двох значеннях: в широкому – вони є результатом будь-якої зміни первинної обстановки внаслідок вчинення злочину, у вузькому розумінні – це матеріально-фіксовані відображення зовнішньої будови одного об'єкта на іншому. Їх класифікують на сліди-предмети, сліди-відображення та сліди-речовини.

Вилучені сліди-предмети складають зміст криміналістичних обліків, які є основою для інформаційно-довідкового забезпечення експертної діяльності. Сліди-відображення також використовуються для створення обліків, і є достатньо інформативними з боку пояснення механізму та особливостей утворення. Для вилучення таких слідів необхідно докласти більших зусиль, тому зазвичай їх вилучають або разом з предметом-слідоносієм, або за допомогою виготовлення копій з використанням техніко-криміналістичних засобів. Сліди-речовини переважно слугують джерелом інформації на місці події, і допомагають слідчому та спеціалісту зрозуміти та відтворити ймовірний алгоритм вчинення злочину.

Крім зазначених слідів для створення інформаційної бази важливу роль відіграє також обстановка на місці події, до якої також можуть бути залучені експерти в якості спеціалістів, тому важливо знати особливості їхньої участі. Для сприйняття обстановки не лише в комплексі, а й в конкретних елементах, експерту необхідно усвідомлювати важливість розуміння обстановки місця події як системи взаємопов'язаних частин, кожна з яких має значення при виокремленні певних слідів, об'єктів, ознак. Вона дозволяє отримати інформацію про факти, які через деякий час можуть бути зіставлені у їх взаємозв'язку.

Другим видом діяльності, як вже було згадано, є саме накопичення та систематизація отриманої інформації судовими експертами, тобто створення та забезпечення криміналістичних обліків в експертній діяльності. Обліки за призначенням поділяють на оперативно-розшукові та інформаційно-довідкові.

Оперативно-розшукові обліки на базі Експертної служби включають обліки слідів рук, взуття, рукавичок, знарядь злому, транспортних засобів, генетичних ознак людини тощо. Зосередження обліків оперативно-розшукового призначення у підрозділах Експертної служби МВС України обумовлено тим, що при їх використанні необхідно залучати спеціалістів із дослідження тієї категорії властивостей об'єктів, які подані в певному обліку.

Інформаційно-довідкові обліки призначені для проведення експертиз, вони містять в собі зразки для порівняльного дослідження. Ці обліки існують у вигляді колекцій, каталогів, картотек різного спрямування: зброї та вибухових пристроїв, документів, грошей, наркотичних речовин, паливно-мастильних матеріалів тощо. Функціонування обліків відбувається за допомогою сучасного обладнання, яке знаходиться на базі Експертної служби.

Дактилоскопічний облік забезпечується автоматизованими дактилоскопічними ідентифікаційними системами, які реалізують велику кількість функцій: введення в базу

даних дактилокарт, демографічних даних, зберігання та керування базою даних, в тому числі це стосується і слідів рук, вилучених з місць нерозкритих злочинів для майбутніх процесуальних дій. Важливим призначенням є проведення та аналіз пошуків категорій «дактилокарта – база даних дактилокарт», «дактилокарта – база даних неідентифікованих слідів пальців рук», «слід – база даних дактилокарт», «слід – база даних неідентифікованих слідів пальців рук», а також пошук за демографічними даними особи (прізвище, ім'я, по-батькові, дата народження тощо). Дактилоскопічна система дозволяє швидко здійснювати обробку наданої дактилоскопічної інформації та пошук даних про конкретні об'єкти та людей серед наявної інформаційної бази.

На даний момент в Україні існує проблема використання російського та білоруського обладнання в експертній діяльності («Дакто-2000», «Сонда», «DEX» і т. д.), тому актуальним постає питання заміни цих систем на оснащення українського виробництва, або закупівля зарубіжного. Наприклад, варта уваги американська система Automated Fingerprint Identification Systems (AFIS), вона містить високоякісні пристрої для введення відбитків пальців рук та фотографічних матеріалів. Також достатньо новим, але ефективним можна вважати пристрій введення відбитків, що передбачає безконтактний спосіб зняття відбитків пальців рук від японської компанії «Mitsubishi Electric». Також перспективним є виготовлення власної української системи, яка може функціонувати на базі зарубіжного досвіду.

Балістичний облік функціонує на базі автоматизованої балістичної інформаційної системи «BalScan» виробництва Transfarm, автоматизованих балістичних ідентифі–каційних комплексів «IBIS» канадського, «Рикошет» та «Баліст» українського вироб–ництва тощо. Завданнями балістичного обліку є встановлення факту використання однієї зброї при вчиненні декількох кримінальних правопорушень; пошук потрібної зброї серед вилученої, зданої добровільно або знайденої; пошук зброї, що була на озброєнні поліції, серед використаних правопорушниками тощо.

Варто зазначити особливості формування кулегільзотеки, по-перше, це об'єкти, що мають безпосереднє відношення до події правопорушення, тобто вилучені під час проведення слідчих (розшукових) дій, по-друге, джерелами обліків є об'єкти, що використовуються для порівняльного дослідження. На практиці здійснюється плановий відстріл зброї, але малоефективне використання обліків для співробітництва Національної поліції при пошуку конкретної зброї, тому невирішеним є питання надання більшого фінансування на розвиток балістичної галузі та на закупівлю обладнання, щоб безперешкодно отримувати інформацію на запити до бази від підрозділів поліції.

Трасологічний облік, до якого входить облік слідів знарядь злому, слідів взуття, транспортних засобів (протекторів шин). В Експертній службі є автоматизовані комплекси «ToolScan», які розроблені для забезпечення зображення в режимі реального часу та зручного прямого сканування 2D- та 3D-зображень високої роздільної здатності; «TrasoScan», які дозволяють досліджувати відбитки взуття, пальців, документів, пласких об'єктів та поверхонь. В Україні також є автоматизовані системи «SoleMate FRX», завдяки роботі яких є можливість кодування, розміщення в базі даних, та перевірка за обліками слідів взуття.

Для ведення обліку підроблених грошових знаків, цінних паперів та бланків документів експертами використовується автоматизована інформаційно-пошукова система «Технічне дослідження та облік документів», а також системи «Девіза-М» та «Абрис», що містять облік грошових знаків.

Облік генетичних ознак людини (ДНК профілі осіб) встановлює осіб, які залишили біологічні сліди, що вилучені за фактами нерозкритих злочинів, в разі вчинення декількох злочинів, безвісти зниклих осіб, а також трупів. Для цього запроваджені автоматизовані інформаційно-пошукові системи EMGILAB, яка містить проведені

експертизи разом з результатами, і призначена для пошуку збігів за профілем ДНК; а також комбіновані системи індексації ДНК KODIS американського виробництва.

На даний момент у зв'язку з воєнними злочинами Росії проти українського народу є потреба в збільшенні фінансування на забезпечення наявних та закупівлю нових систем ідентифікації осіб, та розширення колекцій ДНК-профілів для якомога ефективнішого знаходження та ідентифікації загиблих та вбитих громадян України. Тому зарубіжні компанії-меценати передають нові ДНК-лабораторії, які дуже ефективні в отриманні результатів за короткий проміжок часу.

Проаналізувавши вище викладену інформацію, можна зробити висновок, що на сучасному етапі інформаційне забезпечення судово-експертної діяльності має досить потужний потенціал для розвитку. Експертною службою активно розробляються та забезпечуються обліки за різними напрямами судової експертизи та досліджень, використовується досвід розвинутих країн задля впровадження в українську сферу знань та навичок щодо функціонування автоматизованих інформаційно-пошукових систем та комплексів (Сполучені Штати Америки, Чехія, Канада, Польща тощо). Тому для здійснення судово-експертної діяльності існують всі перспективи успішного розвитку, включаючи можливість розробки власних продуктів для ведення обліків. В Україні є всі ресурси для комплексного вирішення питання систематизації інформації, необхідної для найбільш швидкого розкриття, розслідування та попередження кримінальних правопорушень.

Література

1. Криміналістика: Криміналістична техніка : навч. посіб. / [Степанюк Р. Л., Гусєва В. О., Кікінчук В. В. та ін.]. Харківський національний університет внутрішніх справ. 2023. С. 354-361.
2. Бондар В. С. Підвищення ефективності інформаційно-аналітичного забезпечення розслідування злочинів, учинених із застосуванням вогнепальної зброї: питання запровадження балістичного стандарту. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2018. Вип. 2 (82). С. 206-221.
3. Пиріг І. В. Інформаційне забезпечення експертної діяльності. Теорія та практика судової експертизи і криміналістики: зб. наук. пр./редкол.: О. М. Клюєв, В. Ю. Шепітько та ін. Харків: Право, 2020. Вип. 21. С. 179—193.
4. Хахановський В. Г. Можливості і перспективи використання інформаційних технологій в експертній практиці. Криміналістика і судова експертиза. 2017. Вип. 62. С. 330-344.
5. Кажанов С. П. Використання автоматизованої інформаційної системи ідентифікації пальцевих відбитків в організації розкриття та розслідування злочинів. Київ. 2016. 104 с.
6. Темник, І. М., Колісник, Н. І. Взаємодія дактилоскопічного обліку експертної служби МВС України з правоохоронною системою зарубіжних країн. Актуальні проблеми криміналістичного та експертного забезпечення діяльності правоохоронних органів та суду в Україні : тези доп. учасників наук.-практ. конф. (Харків, 28 трав. 2021 р.)

Чмир С.-І. М.
інспектор відділу аналітичної роботи управління кримінального аналізу ГУНП у Львівській області

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ПРОГРАМНИХ ПРОДУКТІВ І МЕТОДИК КРИМІНАЛЬНОГО АНАЛІЗУ У ВИЯВЛЕННІ ТА ДОКУМЕНТУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

В умовах сьогодення запорукою ефективної роботи та функціонування будь-якої державної установи, чи системи державних органів влади є, насамперед, збір, класифікація, аналіз великого обсягу інформації та швидке прийняття рішень за результатами її обробки. Саме це в умовах сучасного, динамічного, високоінформативного світу є одним з найважливіших чинників успіху.

Національна поліція України, як центральний орган виконавчої влади, що служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, як ніхто інший потребує постійного впровадження сучасних інформаційних технологій, для забезпечення високої ефективності роботи кожного поліцейського, надання швидкого доступу до інформаційних банків даних Національної поліції, сприяння повному збору інформації безпосередньо на місці події, здійснення аналітичної і превентивної діяльність, що має на меті зменшення кількості скоєних кримінальних та адміністративних правопорушень.

Проблемам розробки та впровадження інноваційних технологій у практичну діяльність правоохоронних органів приділяли увагу у своїх працях вітчизняні та зарубіжні науковці: В. В. Бірюков, В. Ю. Шепітько, Р. С. Бєлкін, В. О. Коновалова, І. Ф. Крилов, М. В. Салтєвський, О. Р. Россинська, М. Л. Цимбал, М. Я. Сегай та ін.

Під час здійснення кримінального аналізу кримінальними аналітиками забезпеч-у-ється цілеспрямований пошук, виявлення, фіксація, вилучення, упорядкування, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація.

Зокрема, в аналітичній роботі використовується:

- оперативний аналіз (аналіз даних телефонних дзвінків, аналіз злочинних угруповань, аналіз справ, порівняльний аналіз);
- тактичний аналіз (кримінальний аналіз, аналіз кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, кримінальні моделі, профілі підозрюваних/жертв);
- стратегічний аналіз (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз із використанням географічного профілювання).

В цей нелегкий час як ніколи гостро постало питання практичного використання інформаційних ресурсів та спеціалізованого програмного забезпечення (ботів, додатків тощо), особливо під час виявлення та документування кримінальних правопорушень.

З перших днів війни кримінальні аналітики збирають, узагальнюють, систематизують, проводять аналіз інформації, спрямованої на забезпечення якісного документування злочинів агресора на території України, викриття винних у цих злочинах та встановлення потерпілих, а також викриття осіб, причетних до колабораціонізму та диверсійної діяльності. Окрім цього наявні у кримінальних аналітиків інформаційні ресурси та програмне забезпечення сприяють пошуку та встановленню за «відкритими даними» активів осіб, причетних до збройної агресії в Україні та вчинення воєнних злочинів, а також встановлення інформації про членів їх сімей, бізнесу, близького оточення, з метою притягнення їх до відповідальності за вчиненні злочини.

Інформаційні ресурси науково-технічної інформації – рушійна сила прогресу – законом визначено як «систематизоване зібрання науковотехнічної літератури і документації (книги, брошури, періодичні видання, патентна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях» [1, с.34].

У зв'язку із чим працівники кримінального аналізу постійно поповнюють списки ресурсів та інструментів, які необхідні для виявлення та документування кримінальних правопорушень. Слід зауважити, що інформацію в мережі Інтернет на юридичних та фізичних осіб можливо отримати в доволі великих обсягах. Отримання цієї інформації здійснюється за допомогою різноманітних методик [2, с. 111-115] здійснення пошуку, а також засобів [2, с. 110, 111, 114-122], що дозволяє здійснювати пошук в напів-автоматичному, чи навіть в автоматичному режимі. Як приклад програмних засобів для автоматизації пошуку інформації можемо навести такий програмний комплекс як IBM i2 analyst's notebook [3] з підключеними програмними модулями SocialGrabber4i2 2.0 [4].

Для прикладу, основним призначенням SocialGrabber4i2 2.0 є отримання даних із соціальних мереж для аналізу явних і прихованих зв'язків між різними об'єктами дослідження, що дозволяє визначити приховані спільноти, організовані злочинні групи і виявити ключові об'єкти і лідерів груп.

Що ж до програмного модулю IBM i2 iBase [5], то наявні у ньому можливості дозволяють вилучати інформацію з різних баз даних, а також імпортувати ці бази даних гуртом. Інші джерела, які можливо використовувати для пошуку більш-менш достовірної інформації.

Окрім цього, аналітиками в умовах сьогодення використовуються різновекторні (у т.ч. нетрадиційні, оригінальні, подекуди творчі) способи пошуку інформації та введення пошукових запитів.

На озброєнні в працівників кримінального аналізу є понад 50 інформаційно-пошукових ресурсів, які знаходяться у відкритому доступі та сприяють ідентифікації та пошуку осіб, котрі причетні до збройної агресії в Україні та вчинення воєнних злочинів, в тому числі пошуку наявного у них майна, зокрема:

- Locatefamily (https://www.locatefamily.com/) – пошук адрес;
- Infobel (https://www.infobel.com/fr/world) – пошук номеру телефона, адреси та ПІБ;
- Rocketreach (http://rocketreach.co/) – пошук людей в linkedIn, Facebook та на інших сайтах і в соц мережах, пошук email;
- @egrul_bot (https://t.me/@egrul_bot) – пошук компаній та інші.

Реєстрам, які зазначені вище віддається найбільша перевага, у зв'язку з тим, що за допомогою пошуку необхідного реєстру можливо встановити юридичну особу, судові справи, тендери, торгівельні марки та патенти, рухоме/нерухоме майно, донати на компанії, фінансову звітність особи. Також у своїй діяльності кримінальні аналітики користуються Єдиними та Державними реєстрами, відомчими базами даних та програмним забезпеченням, а саме: ІТС «ІПНП», інтегрованою міжвідомчою автоматизованою системою «Аркан», Єдиним державним реєстром судових рішень, Єдиним державним реєстром юридичних осіб, фізичних осіб підприємців та громадських формувань, Державним реєстром речових прав на нерухоме майно, Державним реєстром актів цивільного стану, ЄІАС УМП, загальнообласною системою відеоспостереження «Безпечна Львівщина», геопорталом «Ліси України», Єдиним державним реєстром транспортних засобів та їх власників, реєстр посвідчень водія національної

автоматизованої інформаційної системи, Єдиним державним реєстром довіреностей, банком даних Інтерполу по технології «Find» підсистеми: особи, транспортні засоби, втрачені (загублені) проїздні документи, ЄРДР аналітикою.

Під час проведення аналітичної та інформаційно-пошукової роботи, на постійній основі використовуються наявні у підрозділі програмно-пошукові продукти, аналітичні онлайн-системи, сервери керованих даних, платформи та інше спеціалізоване програмне забезпечення, зокрема YouControl, Clearview AI, Big Data People (Artellence), та спеціалізований інформаційний сервіс програмно-пошуковий модуль «Face-check»

Важливою умовою пошуку є постійне документування процесу. Це сприятиме прозорості розслідувань.

Враховуючи вищенаведене, за роки діяльності кримінального аналізу вдалось максимально акумулювати інформаційні ресурси в одній службі, завдяки чому підрозділи кримінального аналізу мають ексклюзивну серед інших підрозділів поліції можливість використовувати в реальному часі автоматизовані інформаційні і довідкові системи, реєстри та банки даних, необхідні для успішного проведення аналітично-розвідувальної та інформаційно-пошукової роботи під час виявлення та документування кримінальних правопорушень.

Література

1. Партико З.В. Теорія масової інформації та комунікації/ З. В. Партико.– Львів: Афіша, 2008.– 290с.
2. Застосування комп'ютерних технологій в Національній поліції : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2017. – 161 с.
3. https://www.ibm.com/us-en/marketplace/analysts-notebook
4. http://www304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=51450&expand=true&lc=ru
5. https://www.ibm.com/us-en/marketplace/data-management

Шведа Б. В.

аспірант кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ

РОЗВИТОК НАВИКУ ПЕРЕОСМИСЛЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ПРАВОСУДДЯ У КОНТЕКСТІ ЕЛЕКТРОННОГО ПРАВОСУДДЯ

Концепцію Програми інформатизації місцевих та апеляційних судів і проекту побудови Єдиної судової інформаційно-телекомунікаційної системи розроблено на виконання Закону України «Про Національну програму інформатизації», з урахуванням норм законів України «Про судоустрій і статус суддів» та Положення про порядок функціонування окремих підсистем (модулів) ЄСІТС, затвердженого рішенням Вищої ради правосуддя [1].

Реалізація Програми сприятиме покращенню організаційного забезпечення та підвищенню рівня інформатизації діяльності судів, органів та установ системи правосуддя, сформує передумови для функціонування і подальшого розвитку ЄСІТС, сприятиме відкритості і покращенню взаємодії судів та органів судової влади з іншими державними інституціями, забезпеченню доступності правосуддя для фізичних та юридичних осіб.

Електронне судочинство передбачає подальший розвиток суддівського розсуду. Щоб останні відбулися, необхідно важливі питання, що регулюються інститутом судочинства, періодично оцінювати на спроможність перебування у ланцюжку сучасних процесів. Багато суддів пишаються наявними знаннями, досвідом та відданістю правосуддю. Названа частина характеристик приносить свої плоди у кон'юнктурі стабільного світу.

На даний момент людство живе у світі з високим ступенем нестійкості. У умовах переосмислювати існуючу позицію щонайменше важливо, ніж її формувати. В епоху глобалізації, цифровізації реконструкція системи безперервного виконання основних напрямів державної діяльності потребує радикального оновлення з погляду інноваційних ідей, теоретичних, практичних та методологічних розробок.

Для створення культури накопичення знань потрібна відповідальність, яка змусить переосмислювати звичні методи робіт. На увазі – актуальність застосування ризик-орієнтованого підходу. Різноманітні ситуації у контексті діяльності судді вимагають постійного перегляду.

Якість наявних навичок – один із основних показників компетентності (тобто єдності практичних і теоретичних умінь) людини будь-якої сфери, оскільки результат повноцінного навчання має відбивати готовність застосування навички у житті. Накопичення знань в інституті вчинення правосуддя також не має закінчуватись.

Освіта – це непросто накопичення інформації. Це звички, які виробляються під час виправлення допущених помилок, і навички, що дозволяють навчатися на протязі всього життя. Тобто, отримані нові знання допоможуть суддям вирішувати повсякденні завдання, а нове мислення полегшить розуміння життєвих труднощів населення: рівень матеріального, соціального, культурного стану. Для ефективного вирішення суспільно значущих завдань судочинства судді повинні мати склад розуму вченого, який постійно оновлює точку зору відповідно до отриманої інформації.

У культурі продуктивності люди схильні прив'язуватись до звичних методів. Небезпека виникає, якщо методи досягли меж, їх час удосконалити, але ніхто не бачить недоліків через нахвалювання визнаних, але вже неактуальних переваг.

Розглянемо приклад найкращої профілактики виникнення правопорушень – діалог. Вміння пояснювати правові процедури, дії та рішення суду необхідні для винесення якісного рішення.

Комунікація держави та суспільства – виключно важлива частина роботи судової влади. Здорове та розумне суспільство конструктивно спілкується з судовою владою. Активний громадянин, у свою чергу, пише скарги та пропозиції, адресуючи їх відповідним державним органам; бере участь у обговоренні законопроектів; дає суддям конструктивний зворотний зв'язок щодо реалізації повноважень у сфері правосуддя.

Одночасно реалізується принцип клієнто-орієнтованості, спростовуючи помилкові міркування про те, що використовується тільки у сфері правового конфлікту. Інформаційно-комунікативна функція суду полягає у передачі правової інформації з метою не тільки повідомити населення про діючі правові норми, а й сформувати шанобливе ставлення до них. Тривогу викликає неконтрольоване зростання інформації, що провокує насильство, цинізм, неповага до законності, споживче ставлення до держави.

Сенсації, скандали успішно маніпулятивні привертають увагу фізичних осіб призводять до спотворення морально-правових норм. У культурі продуктивності з її акцентом на результати психологічної безпеки часто недооцінюють відсутність правових знань та вплив на стан особистої психологічної безпеки. Судді розуміють, що це важливо, але не знають, що це конкретно і як забезпечити. Необхідно підкреслити, що такий вид безпеки не передбачає зниження стандартів зручності спілкування з учасниками судового процесу. Практика показує, що ступінь довіри до судової влади зростає, якщо помітні старання зробити більше, ніж потрібно за судовою процедурою з

позиції розсуду судді. Ці дії характеризуються як вище за очікувані, ширші за передбачені. Громадяни України не повинні перебувати у болісно суперечливих психологічних відносинах із судовою владою.

Україна потребує відповідальних осіб, які мають соціально-правову активність, розуміння громадянського обов'язку. Гнучкий розум, певні практичні навички, вміння підлаштовуватися під життєві обставини, що змінюються, готовність працювати на результат на своєму полі відповідальності призводять до дійсного поступового поліпшення добробуту країни.

Для помітного зростання потенціалу країни потрібно докласти чимало зусиль. Слід створювати та зберігати такі соціальні інститути, які генеруватимуть корисні професійні та моральні знання, пов'язуватимуть теоретичні та практичні дослідження, маючи єдину мету – покращити якість життя населення, подолавши значні перешкоди на шляху ефективної реалізації повноважень суддів.

Література

1. Концепція програми інформатизації місцевих та апеляційних судів і проекту побудови Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС) на 2022-2024 роки. URL. https://zakononline.com.ua/documents/show/ 503687___687052

Шийович Р. Я.

аспірант кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ

КРИТЕРІЇ СТАДІЙНОЇ СТРУКТУРИЗАЦІЇ АДМІНІСТРАТИВНОГО ПРОЦЕСУ ЯК ПРОЦЕСУ РОЗПОДІЛУ ІНФОРМАЦІЇ

Розвиток інформаційних технологій створює умови для виникнення нових видів інформації та способів їх використання, у тому числі в юриспруденції. Розподіл інформації в юридичному процесі виглядає як розподіл по певних стадіях. Однією з основних ознак правозастосовного процесу в науковій літературі називають стадійність, яка означає розвиток такого процесу через одиниці, що змінюють одна одну щодо самостійні частини – стадії.

Кожна стадія характеризується властивими тільки їй особливостями та спрямована на досягнення загальних цілей юридичного процесу. У правовій літературі зазначається, що зміст стадій як етапів проходження юридичної справи залежить від виду правозастосовного процесу.

Для адміністративного процесу як різновиду правозастосовного процесу також характерна ознака стадійності. Можливість поділу адміністративного процесу на ряд самостійних фаз розвитку, які змінюють одна одну, зумовлена циклічним характером – діяльність учасників адміністративного процесу здійснюється у вигляді повторення низки процесуальних дій, передбачених адміністративно-процесуальним законодавством, наступних по черзі.

Одні учасники вчиняють процесуальні дії щодо виявлення адміністративного правопорушення та його фіксації, інші – розглядають справи про адміністративні правопорушення, треті – здійснюють перегляд постанови у справі про адміністративне правопорушення, четверті – виконують постанову. Сам термін «стадія» у своєму лексичному значенні визначається як період чи ступінь у розвитку чогось.

Ковалів М. В. відзначаючи органічний взаємозв'язок стадій між собою, вказує, що кожна наступна стадія зазвичай починається тільки після того, як закінчена попередня, при цьому на новій стадії перевіряється те, що було зроблено раніше [1].

Стадії вирішення судової адміністративної справи в ході їх реалізації поєднуються в єдину динамічну систему, в якій вони не можуть виникнути та функціонувати одна без одної. Завдяки такій специфічній правовій конструкції стадії, крім володіння характерними відмінностями, взаємопов'язані та поступово змінюють один одного в ході адміністративного судочинства за заздалегідь заданим маршрутом руху судової адміністративної справи, що розглядається та вирішується.

Диференціація стадій адміністративного процесу має практичне значення – вони розкривають внутрішню структуру процесу, дозволяють розмежувати компетенцію суб'єктів адміністративної юрисдикції та визначити найближче процесуальне завдання. На логічну необхідність угруповання всієї сукупності правозастосовних операцій вказує порядок судочинства – розгляд, дебати, прийняття рішення, який склався історично. Деталізація юридичного процесу за часовими параметрами і характером скоєних дій не потрібна для самоцілі – процесуальні норми призначені отримання такого матеріально-правового результату, який може бути отримано одномоментно.

Виділення стадій адміністративного процесу дозволяє правильно визначити завдання суб'єктів адміністративно-правових відносин, що діють на відповідній стадії, конкретизувати їх правовий статус, деталізувати особливості та часові межі процесуальних дій на кожній стадії. Поділу адміністративного процесу на стадії сприяють певні критерії – відмінні риси, що характеризують стадію як відносно самостійну [2, с. 107].

У юридичній літературі єдиної думки щодо критеріїв розмежування стадій адміністративного процесу не склалося. Більшість правознавців сходиться на думці, що основним критерієм є безпосереднє завдання (мета), яке покликане досягти відповідна стадія.

Відмінна риса стадії це специфічні, тільки властиві конкретній стадії завдання. Багато вчених наводять додаткові критерії, що дозволяють відокремити стадії. Це наявність у кожної стадії властивих лише цій стадії цілей та особливостей, що стосуються учасників процесу, прав та обов'язків учасників, термінів здійснення процесуальних дій та характеру оформлення процесуальних документів.

Кожна стадія має свої тимчасові рамки, коло учасників, специфічні завдання, порядок та термін проведення, процесуальні документи, прийняті процесуальні рішення. На кожній стадії специфічна безпосередня мета, склад суб'єктів правовідносин, збирана та використовувана інформація, вчинені дії, складені документи, проміжні та остаточні рішення, що приймають.

Як критерії, що відрізняють стадії виділяють: наявність у кожної стадії властивих тільки їй завдань, свого кола учасників, здійснення на кожній стадії різних дій, оформлення вирішених на кожній стадії завдань спеціальним процесуальним документом, яким підбивається підсумок діяльності, із прийняттям якого починається наступна стадія.

З урахуванням вищенаведених обґрунтованих суджень, можна визначити, що основним критерієм виділення стадії адміністративного процесу виступають властиві їй безпосередні завдання, створені задля досягнення загальних цілей адміністративного процесу. Цим критерієм обумовлено наявність у кожної стадії додаткових критеріїв – особливостей, властивих даної стадії. Для цілей виділення стадій визначимо такі критерії, наявність яких характеризує частину адміністративного процесу відносно самостійну стадію.

Кожна стадія:

- є відносно самостійною частиною адміністративного процесу, що логічно взаємопов'язана з іншими стадіями та підпорядкована загальним принципам адміністративного процесу, за своїм змістом не може збігатися з адміністративним процесом, а істотно вже за обсягом;
- спрямовано на досягнення властивих специфічних завдань, реалізація яких сприяє досягненню загальних завдань адміністративного процесу та дозволяє закінчити процес чи перейти у наступну стадію;
- підпорядкована певним просторово-часовим межам, які сформовані нормативно закріпленими термінами провадження процесуальних дій, накладення адміністративного стягнення та іншими процесуальними термінами, які можуть починатися та закінчуватися не лише певною датою, а й подією;
- має специфічне коло учасників, права та обов'язки яких можуть мати особливості;
- включає сукупність юридичних дій, вкладених у досягнення безпосередніх завдань стадії;
- закінчується прийняттям специфічних рішень, зокрема оформлюваних у вигляді прийняття процесуальних документів.

З урахуванням наведених критеріїв, стадією адміністративного процесу є відносно самостійна частина, логічно взаємопов'язана з іншими стадіями і спрямована на досягнення загальних цілей адміністративного процесу, має свої специфічні завдання, просторово-часові межі, коло учасників, які виконують юридичні дії та приймають рішення.

Література

1. Адміністративне право України (загальна частина): навчальний посібник / Остапенко О. І. Ковалів М. В., Єсімов С. С. та ін. Вид. 2-е, доп.] Львів: СПОЛОМ, 2021. 616 с.
2. Адміністративний процес України: підручник / за заг. ред. Д. І. Йосифовича. Львів: Львівський державний університет внутрішніх справ, 2021. 500 с.

Шийович С. Я.

аспірант кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ

ЦИФРОВІ ТЕХНОЛОГІЧНІ КАРТИ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ НАДАННЯ ПУБЛІЧНИХ ПОСЛУГ

Цифрові технології вже давно проникли у кожну сферу нашого життя, і вирішення державних питань не стало винятком. Поняття «цифрова економіка», «цифрове державне управління», «цифрова трансформація» використовуються в офіційних нормативно-правових документах.

Розвиток «цифрова економіка» в Україні розпочала 6 років тому, коли було визначено Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації [1].

У 2021 році було прийнято Національну економічну стратегію на період до 2023 року, яка закріпив впровадження цифрових технологій у соціальній сфері та економіці, наданні публічних послуг [2].

Надання публічних послуг займає важливе місце у системі управління, а цифровізація цього процесу останнім часом один із значних напрямів. Надання послуги

здійснюється відповідно до технологічної карти, а основним законом, що регулює цю сферу, є закон України «Про адміністративні послуги» [3].

У зв'язку з виникненням цифровізації державного сектору та економіки змінюється законодавча база – законом України «Про особливості надання публічних (електронних публічних) послуг» в контексті якого потрібно збільшити частку масових соціально значущих послуг, що надаються у цифровому вигляді [4].

Відображення цієї норми в Законі України говорить про важливість розвитку цифровізації у сфері надання послуг і її оптимізації. Ще однією важливою зміною у нормативно-правовому забезпеченні державного управління є поява закону України «Про цифровий контент та цифрові послуги» [5]. Цей нормативно-правовий акт закріплює нові принципи надання послуг: проактивний режим, модель фіксації результатів наданих послуг, екстериторіальність.

Закон України «Про адміністративні послуги» встановлює обов'язок розробки, погодження, а також з експертизи та реєстрації інформаційних і технологічних карт. Порядок розробки технологічних карт визначається постановою Кабінету Міністрів України «Про затвердження вимог до підготовки технологічної картки адміністративної послуги» [6]. Вимоги встановлені для суб'єктів надання публічних послуг, останні можуть розробляти, погоджувати та затверджувати інформаційні та технологічні карти у власних інформаційних системах, що забезпечують встановлені вимоги. Закон України «Про адміністративні послуги» не називає адміністративні регламенти цифровими, але закон України «Про особливості надання публічних (електронних публічних) послуг» уточнює поняття електронних публічних послуг.

Згідно закону України «Про особливості надання публічних (електронних публічних) послуг» біло внесено коригування до порядку підготовки інформаційних та технологічних карт надання послуг.

Технологічна картка повинна передбачати максимально можливе з урахуванням ресурсного забезпечення суб’єкта надання адміністративної послуги використання інформаційно-комунікаційних технологій, зокрема під час взаємодії структурних підрозділів суб’єкта надання адміністративної послуги і здійснення процедур (етапів) надання адміністративної послуги.

Розробка та затвердження технологічної карти відбуватиметься в інформаційній системі у процесі розробки вводяться відомості про послугу, які повинні перетворюватися на машино-читаний вид з автоматичним формуванням технологічної карти як нормативного документа.

Правила передбачають необхідність підвищення якості надання послуг під час розробки технологічної карти: проактивність, впровадження реєстрової моделі надання послуги, екстериторіальність, багатоканальність, скорочення термінів надання необхідних документів, детальний опис усіх варіантів надання послуги.

Органи місцевої влади та місцевого самоврядування розробляються місцеві порядки щодо приведення інформаційної та технологічної карти в електронний вигляд.

Оцифрування технологічної карти є обов'язковою умовою дотримання вимог закону та підзаконних актів. Переведення інформаційної та технологічної карти у цифру, окрім необхідності дотримання вимог нормативно-правових актів, обумовлено тим, що цифрові технологічні карти можуть стати важливим інструментом удосконалення сфери державного управління з надання послуг.

У правовстановлюючій практиці цифровий технологічні карти є нововведенням, оскільки технологічна карта формується у машино-читаному вигляді та виконання його положень мається на увазі безпосередньо «навченою» інформаційною системою, без участі фахівця, який раніше надає послугу.

Створення технологічної карти більше не передбачає роботи з паперовим документом, в інформаційній системі необхідно заповнювати відповідні поля шляхом вибору значень із довідника, а форматно-логічний контроль, вбудований у реєстр, допоможе уникнути помилок.

Узгодження, затвердження та реєстрація технологічної карти проходитиме у цифровому середовищі, що дозволить значно знизити трудовитрати фахівців та посадових осіб органів влади, зменшити термін розробки та затвердження технологічної карти. Плюсом цифрової технологічної карти є спрощення розроблення та надання фізичній та юридичній особі послуги відповідно до певного варіанту надання.

Цифрові технологічні карти надання послуг – це один з прикладів використання цифрових технологій у державному управлінні. Цифрові технологічні карти дозволяють значно скоротити час та спростити процес надання публічних послуг, підвищують прозорість та доступність публічних послуг для фізичних і юридичних осіб. Цифровий регламент може сприяти зниженню корупції та збільшенню якості надання публічних послуг.

Література

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL. https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text
2. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text
3. Про адміністративні послуги: Закон України від 06.09.2021 р. № 5203-VI. URL. https://zakon.rada.gov.ua/laws/card/5203-17/conv
4. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15.07.2021 р. № 1689-IX. URL. https://zakon.rada.gov.ua/ laws/card/1689-20
5. Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 р. № 3321-IX. URL.https://zakon.rada.gov.ua/laws/show/3321-20#Text
6. Про затвердження вимог до підготовки технологічної картки адміністративної послуги: Постанова Кабінету Міністрів України від 30.01.2013 р. № 44. URL. https://zakon.rada.gov.ua/laws/show/44-2013-%D0%BF#n7

Широкий Б. В.

здобувач вищої освіти факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ;

Прокопов С. О.

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

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНОЇ РОЗВІДКИ В ПРОЦЕСІ СЛІДЧИХ РОЗШУКОВИХ ДІЙ ТА НЕГЛАСНИХ СЛІДЧИХ РОЗШКУКОВИХ ДІЙ

Засоби інформаційного забезпечення в процесі проведення слідчих та негласних слідчих розшукових дій є важливим і необхідним елементом досудового розслідування.

Вони допомагають збирати, зберігати та аналізувати інформацію про підозрюваних, свідків та обставини кримінальних правопорушень, що в свою чергу допомагає розкривати кримінальні правопорушення та притягати винних до відповідальності.

Проте, використання засобів інформаційного забезпечення в процесі проведення слідчих дій має свої особливості, що відрізняють їх від оперативно-технічних засобів, що використовуються в межах оперативно-розшукової діяльності. Зокрема, відбувається регулювання застосування засобів інформаційного забезпечення за допомогою кримінально-процесуального законодавства, зокрема, щодо вимог до їх використання, оформлення та збереження [1, с. 15].

Особливістю засобів інформаційного забезпечення є їх повна відкритість, окрім інформаційних ресурсів: Інформаційний портал Національної поліції, Цунамі, Єдиний реєстр досудових розслідувань, систем Державної міграційної служби та інших систем. Інформація, зібрана за допомогою відкритих джерел, повинна бути достовірною та перевіреною на засадах наукової обґрунтованості. Також, використання засобів інформаційного забезпечення має бути обмеженим лише необхідними заходами, що не порушують конституційних прав та свобод громадян [2, с. 34].

Відповідно до чинного КПК можна виділити пред’явлення особи для впізнання у натуральному вигляді та за його зображеннями (фотознімки, матеріали відеозапису). Пред’явлення особи для впізнання може проводитись за анатомічними (зовнішній вигляд і прикмети особи) та функціональними (голос, хода) ознаками (ч. 1, 9 ст. 228 КПК). Оскільки в ст. 174 КПК України 1960 р. мова йшла тільки про зовнішній вигляд і прикмети особи, можливість пред’явлення її для впізнання за функціональними ознаками ставилась під сумнів, незважаючи на те, що на практиці проводилось [3, с. 5].

У сфері діяльності поліції інформаційна комп'ютерна розвідка є важливою складовою в здійсненні цілеспрямованого збору, аналізу та обробки інформації, що стосується злочинів, злочинців, потенційних загроз безпеці та кримінальної активності. Вона включає в себе розробку та застосування спеціалізованих програмних засобів, технологій і методик для пошуку електронних слідів, аналізу цифрових доказів, розкриття злочинів в онлайн-середовищі, ідентифікації зловмисників та забезпечення безпеки інформаційних систем. Ця розвідка вимагає спеціалізованих знань та навичок з області кібербезпеки, кримінального аналізу для ефективного використання комп'ютерних ресурсів у боротьбі зі злочинністю. розшуку та збору інформації про злочини та злочинців. Інформаційна комп'ютерна розвідка зазвичай складається з чотирьох головних елементів, які слід класифікувати.

Першим елементом є фактичний пошук інформації. Цей елемент передбачає використання обчислювальної техніки, програмного забезпечення та систем дій, які спрямовані на встановлення або підтвердження місця розташування фізичного джерела інформації та виявлення інформації, що представляє доказове значення. Завдяки цьому елементу, поліція може знайти джерела інформації та отримати підтвердження її достовірності [3, с. 19].

Другим елементом є фіксація інформації. Цей елемент включає систему дій, спрямованих на збереження отриманої інформації на матеріальних носіях з метою подальшого використання. Інформація може бути збережена на комп'ютерах, флеш-накопичувачах або інших матеріальних носіях.

Третім елементом є аналітична обробка (аналіз інформації) отриманої та збереженої на матеріальних носіях інформації. Для реалізації цього елементу необхідно використовувати логічні прийоми та методи, обчислювальну техніку та програмне забезпечення на основі мети збирання цієї інформації. При цьому інформація може бути аналізована з різних точок зору для більшої достовірності даних залежно від потреб поліції.

Четвертим елементом є документальне оформлення результатів обробки [3, с.24].

Найбільше уваги хотілось приділити першому елементу, так як він має важливе значення як початковий етап, бо поліцейські при здійснені слідчих розшукових дій та негласних слідчих розшукових дій рідко посилаються на збирання інформації з засобів OSINT, таких як Google, Facebook, Vkontakte, Twitter, Instagram, що в свою чергу пришвидшує збір необхідної інформації.

Оскільки пошукова система компанії Google користується найвищою популярністю серед користувачів мережі інтернет вона накопичує величезну кількість інформації, про організації, користувачів які навіть не здогадуються що своїм серфінгом в інтернет мережі залишають велику кількість слідів. Головною задачею правоохоронця вміти своєчасно, знаходити ці сліди аналізувати їх, та вживати заходів превенції та розкриття злочинів [4, с. 361].

Користувачі Facebook мають можливість створювати профілі з фотографіями, списками інтересів, контактними даними та іншою особистою інформацією яка досить корисна для правоохоронних органів наприклад тим що непотрібно звертатись з офіційними запитами до інших інстанцій. Це значно пришвидшує роботу правоохоронних органів та потребує менших зусиль [4, с. 386].

Отже, доцільне використання сучасних інформаційних технологій, відкритих мережевих ресурсів, державних чи комерційних баз даних, а також сучасних підходів до виконання доручення слідчого та дізнавача істотно прискорює хід досудового розслідування. Оперативні підрозділи мають можливість отримати низку інформації за короткий проміжок часу, використавши можливості інноваційних сучасних технологій, що також сприяє швидкому і повному попередженню, своєчасному виявленню і припиненню кримінальних правопорушень.

Література

1. Абламський С. Є., Юхно О. О., Лук’яненко Ю. В. Взаємодія1 слідчого2 з іншими органами і підрозділами при розкритті та розслідуванні кримінальних правопорушень : навч. посіб. / за заг. ред. О. О. Юхно. Харків : ХНУВС, 2017. 152 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/4517
2. Бойко О. П., Рогальська В. В. Взаємодія слідчих Національної поліції України з підрозділами карного розшуку на досудовому провадженні : монографія. Дніпро : Вид. Біла К. О., 2018. 180 с. URL: https://er.dduvs.in.ua/handle/123456789/2036
3. Васильковський І. І. Взаємодія правоохоронних органів при розслідуванні кіберзлочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2019. 19 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/12895
4. В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Підручник «Інформаційні технології» Дніпро, ДДУВС, 2021 492с. URL: http://er.dduvs.in.ua/handle/123456789/6820

Ярема О. Г.

доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ОСНОВНІ ТИПИ ШТУЧНОГО ІНТЕЛЕКТУ

Перехід світової економіки до інформаційного типу, пов'язаний з перетворенням індустріального суспільства на постіндустріальне, яке засноване на новому

технологічному способі виробництва та споживання, спричинило і зміни вимог організації самого виробництва. досягнень. Безсумнівно, розвиток інформаційних технологій дуже впливає на багато сфер життя людини.

Стратегічний курс на цифрову трансформацію включає комплекс заходів, основа яких ґрунтується на застосуванні штучного інтелекту. Від рівня розвитку інформаційних технологій та насамперед штучного інтелекту залежать процеси управління діяльністю людини практично у всіх сферах. Важливу роль цьому процесі має зіграти штучний інтелект.

Штучний інтелект відповідно до Концепції розвитку штучного інтелекту в Україні – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [1].

Мета штучного інтелекту (далі – ШІ) – створити видимість наявності у машини людського інтелекту. Якщо комп'ютер демонструє когнітивні здібності, властиві людям, ми називаємо це штучний інтелект.

Інтелект – здатність сприймати інформацію та зберігати її як знання для побудови адаптивної поведінки у середовищі чи контексті. Це визначення інтелекту може бути застосоване як органічного мозку, так і до машини. Проте наявність інтелекту ще передбачає наявність самого свідомості.

Обробка природної мови та розпізнавання мови стали першими прикладами комерційного використання машинного навчання. Після ними з'явилися інші завдання автоматизації розпізнавання (текст, аудіо, зображення, відео, особи). З погляду права, розглядаємо штучний інтелект – як комплекс технологічних рішень, що дозволяє імітувати когнітивні функції людини та отримувати при виконанні конкретних завдань результати, які можна порівняти з результатами інтелектуальної діяльності людини. Комплекс технологічних рішень включає інформаційно-комунікаційну інфраструктуру, програмне забезпечення, процеси та сервіси з обробки даних і пошуку рішень.

Штучний інтелект у науковій літературі зазвичай класифікують на два види або два типи. Перший тип – Вузький штучний інтелект [Weak AI]: цей вид штучного інтелекту, який іноді називають «слабкий ШІ», працює в обмеженому контексті і є імітацією людського інтелекту. Слабкий ШІ орієнтований на дуже гарне виконання лише одного завдання. Незважаючи на те, що ці машини можуть здатися розумними, вони працюють із великими обмеженнями.

Другий тип – Загальний штучний інтелект (AGI): цей вид іноді називають «сильний ШІ» – вид штучного інтелекту, який ми бачимо у фільмах, це машина із загальним інтелектом, яка, як і людина, може застосовувати для вирішення будь-якого завдання.

Слабкий штучний інтелект оточує нас усюди, це успішна реалізація штучного інтелекту. Орієнтуючись виконання конкретних завдань, протягом останнього десятиліття зробив безліч проривів у суспільстві, і зробив помітний внесок у економічне життя суспільства.

У системі розвитку штучного інтелекту виділяють три типи: штучний інтелект вузького призначення (слабкий), штучний інтелект загального призначення (сильний) та супер штучний інтелект. Незважаючи на те, що в основі лежить загальний принцип, вони відрізняються один від одного.

Штучний інтелект – це здатність цифрового комп'ютера або керованого комп'ютером робота виконувати завдання, які зазвичай пов'язані з розумними істотами. Питання, чим штучний інтелект відрізняється від природного інтелекту, лежить скоріше

у філософській площині, ніж у строго науковій. Жоден штучний інтелект, який існує на сьогоднішній день, не досягнув достатньо високого рівня розвитку, щоб змагатися з людиною на рівних.

Перший висновок, який необхідно зробити, це те, що всі типи штучного інтелекту залежать від рівня інтелекту і їх можна чітко класифікувати на три типи: вузький Штучний Інтелект (ANI), загальний Штучний Інтелект (AGI) та Штучний Супер інтелект (ASI).

Вузький штучний інтелект (слабкий штучний інтелект) спрямований на вирішення одного завдання, будь то моніторинг погоди, гра в шахи або аналіз даних. Він має вузький діапазон здібностей. Вузький ШІ це той самий штучний інтелект, з яким ми пов'язані щодня в житті. Машинним інтелектом, наприклад, є Google Assistant, Google Translate, Siri, Cortana або Alexa, які використовують у практиці обробку природної мови. Розуміючи мову й текст, можуть взаємодіяти з людьми індивідуальним, природним образом. Як видно, дана система здатна справлятися з однією конкретною проблемою, вирішення якої вона навчена.

Людський мозок є моделлю до створення загального інтелекту. На відміну від ШІ загального призначення, відомого як сильний, ШІ вузького призначення не має людських почуттів і свідомості, а працює лише в заздалегідь заданому людиною діапазоні. Всі ШІ-рішення – це приклади слабкого штучного інтелекту, в тому числі Google Assistant, Google Translate, Siri та інші інструменти обробки природної мови. Їхня особливість полягає в тому, що вони не можуть думати, як людина самостійно. Наприклад, Siri не має свідомості, вона тільки виконує ряд завдань: обробляє людську мову, вводить отримане питання в пошукову систему і видає відповідь.

Штучний інтелект вузького призначення – це такі системи здатні обробляти дані та виконувати завдання значно швидше, ніж людина, що дозволило підвищити загальну продуктивність, а також якість життя. Ця технологія значно покращила наше життя, тому ми не повинні її недооцінювати.

Сильний ШІ (General AI) або штучний інтелект загального призначення схожий на людський інтелект. Він може успішно виконувати розумові завдання, які під силу людям. Сьогодні комп'ютери можуть обробляти дані швидше, ніж людина, але вони не здатні мислити абстрактно, продумувати стратегію чи використовувати спогади, щоб приймати обґрунтовані рішення. Завдяки цьому типу інтелекту людина перевершує штучний інтелект.

Очікується, що сильний ШІ в перспективі зможе долати проблеми, інтегрувати попередні знання у процес прийняття рішень, та пропонувати новаторські ідеї. Але для досягнення цих цілей дослідники повинні вигадати, як наділити машини свідомістю.

На зміну простому комп'ютеру приходить квантовий комп'ютер, який має протилежні властивості: по-перше, він враховує безліч змінних, а, по-друге, квантові обчислення не є послідовними відбувається оцінка всіх можливих рішень одночасно. Як відомо, звичайний комп'ютер зберігає інформацію в бітах, а квантові обчислення це кубити. Вони мають певні властивості, що дозволяє забезпечити набагато більшу обчислювальну потужність, ніж двійкові біти з класичних обчислень.

Можна припустити, що наступний крок у розвитку штучного інтелекту буде пов'язаний із квантовими обчисленнями, які, як очікується, зможуть вирішувати складніші завдання, які стоять перед суспільством.

Аналіз показав, що фінансові установи здатні додатково залучити понад 5 млрд доларів при використанні суперкомп'ютерів. Використовуючи квантовий комп'ютер, наприклад, ЕВМ бачать можливість вирішення складних і масштабних завдань комбінованої оптимізації. Щоправда, справжні квантові обчислювальні рішення цих проблем залишаються на експериментальному рівні, окремі банки почали

впроваджувати квантовий комп'ютер у діяльність. Доцільно зауважити, що План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки передбачає розвиток квантових обчислень [2].

Слабкий штучний інтелект може виконувати такі функції як інтелектуальний аналіз даних для вибору оптимального варіанта рішення, але не має людських почуттів та свідомості, функціонуючи тільки в заздалегідь заданому діапазоні.

Реактивна система - найпростіший тип штучного інтелекту сприймає обстановку і пропонує реакцію у відповідь, не виходячи за рамки цієї ситуації, не формуючи пам'ять, тобто не спираючись на минулий досвід, щоб видати рішення. Прикладом такого штучного інтелекту є комп'ютер для гри в шахи (Deep Blue), який не може оцінювати можливі майбутні ходи.

Наступним щаблем еволюції є штучний інтелект з обмеженою пам'яттю, який враховує накопичену інформацію та доповнює нею запрограмоване раніше бачення світу. Створені безпілотні автомобілі та чат-боти можна віднести до цього підвиду.

Перспективні методи штучного інтелекту – методи, створені задля створення принципово нової науково-технічної продукції, зокрема з метою розробки універсального (сильного) штучного інтелекту (автономне розв'язання різноманітних завдань, автоматичний дизайн фізичних об'єктів, автоматичне машинне навчання, алгоритми вирішення завдань з урахуванням даних з частковою розміткою та незначних обсягів даних, обробка інформації на основі нових типів обчислювальних систем, обробка даних, та інші методи.

Література

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: : Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. URL. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
2. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки: Розпорядження Кабінету Міністрів України від 12.05.2021 р. № 438-р. URL. https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text

Зміст

Наукове видання

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

22 грудня 2023 року

Опубліковано в авторській редакції

Формат 60×84/8. Умовн. друк арк. 9,3.

Львівський державний університет внутрішніх справ Україна, 79007, м. Львів, вул. Городоцька, 26.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ДК № 2541 від 26 червня 2006 р.

І 78 **ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ**: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2024. – 192 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 22 грудня 2023 року у Львівському державному університеті внутрішніх справ.

УДК 004