Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

16 грудня 2022 року

Львів 2023

УДК 004
І 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 7 від 25 січня 2023)

РЕДАКЦІЙНА КОЛЕГІЯ:

І 78 **Інформаційні технології в освіті та практиці** : матеріали Науково-практичної конференції (Львів, 16 грудня 2022) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2023. – 80 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційні технології в освіті та практиці», що проводилася 16 грудня 2022 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

Бойчук А. М.,
доцент кафедри інформаційних технологій ЗВО «Університет Короля Данила», кандидат фізико-математичних наук

Бойчук Т. Я.,
викладач вищої категорії Івано-Франківського фахового коледжу Львівського національного університету природокористування, кандидат фізико-математичних наук

РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ СИСТЕМИ НАВЧАННЯ «ЕЛЕКТРОННА ШКОЛА»

Раніше мережа використовувалася винятково як середовище передачі файлів і повідомлень електронної пошти, то сьогодні вона використовується для більш складних задач розподіленого доступу до ресурсів. Біля трьох років тому були створені оболонки, що підтримують функції мережевого пошуку і доступу до розподілених інформаційних ресурсів, електронним архівам. Саме тому обрана проблематика дослідження є вельми актуальною на даний момент. Високі технології поширюються в усі сфери нашого життя. Українські IT-фахівці не сидять без діла і запускають щупальці прогресу в одну з найболючіших тем – освіту. Крім уже застосованих практик – перенесення навчального процесу в онлайн, електронної системи оцінювання, автоматизації роботи шкіл – є і нові ідеї: психологічний профіль учня, стимуляція персонального підходу до кожного, впровадження медіа-контенту, інтерактивна система навчання.

Сучасна освітня система здатна: створювати сучасні цифрові інформаційні ресурси освіти, формувати концепцію безперервної освіти, робити процес навчання більш ефективним та доступним, покращувати спілкування між учасниками навчального процесу без огляду на час та простір обмеження, щоб дозволити учням отримати доступ до всіх навчальних матеріалів. Система управління та навчання в школі (SMLS) забезпечує вищезазначені вимоги (рис. 1.). В дану систем можна заходити під наступними користувачами:

Батьки – можуть контролювати навчання своєї дитини без огляду на часові та просторові обмеження, і тим самим вони будуть задіяні у навчальному процесі;

Вчитель – за встановленими SMLS параметрами учителю зручно складати навчальний план;

Адміністрація – SMLS надає адміністрації школи можливість керування та контролю;

Учень – весь навчальний матеріал одним натиском кнопки доступний на особистій сторінці SMLS-учня.

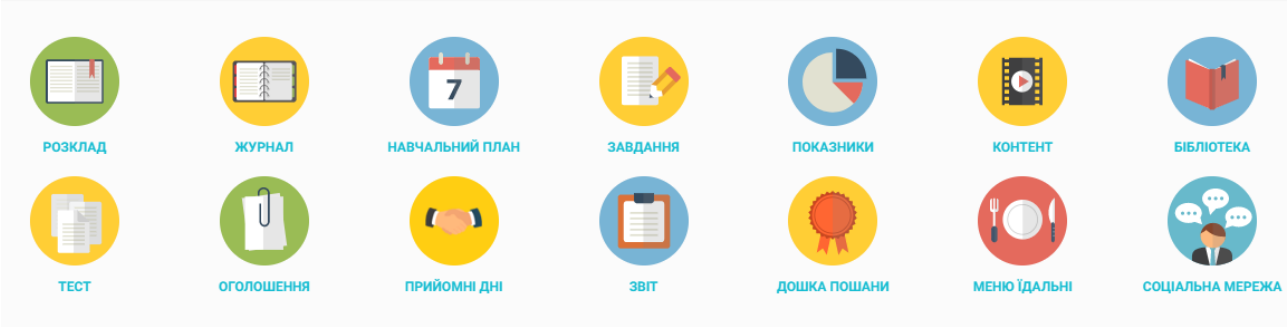


Рис. 1. Вікно основних можливостей системи

SMLS-учитель у будь-який час, в тому числі протягом уроку, може користуватися електронним журналом, що дає можливість керівництву навчального закладу проводити щоденний моніторинг. За своєю структурою програмне забезпечення для ведення успішності школярів складається з шести блоків. Кожен із блоків має своє чітко визначене призначення, яке полягає в реалізації певної функцій системи.

Модуль усіх учнів школи створений для відображення всіх учнів школи з можливістю відбору учнів які навчаються в певному вказаному класі, також для формування вхідних даних модуля успішності який в свою чергу керує формою, яка відображає оцінки певного учня. Модуль усіх вчителів школи створений для відображення всіх вчителів школи з можливістю показу, який предмет веде певний вчитель. Модуль всієї адміністрації має доступ до всіх даних школи.

Модуль, який відповідає за з'єднання даних: клас=вчитель=предмет, повинен з'єднувати таблиці в базі даних так, що відображались дані у вигляді розкладу, без повторень викладачів та накладок їх предметів. Для реалізації програмної складової використано Sublime Text - швидкий кросплатформенний текстовий редактор. Підтри-мує плагіни, розроблені за допомогою мови програмування Python. Користувачі бачать весь свій код в правій частині екрану у вигляді міні-карти, при кліці, на яку можна здійснювати навігацію.

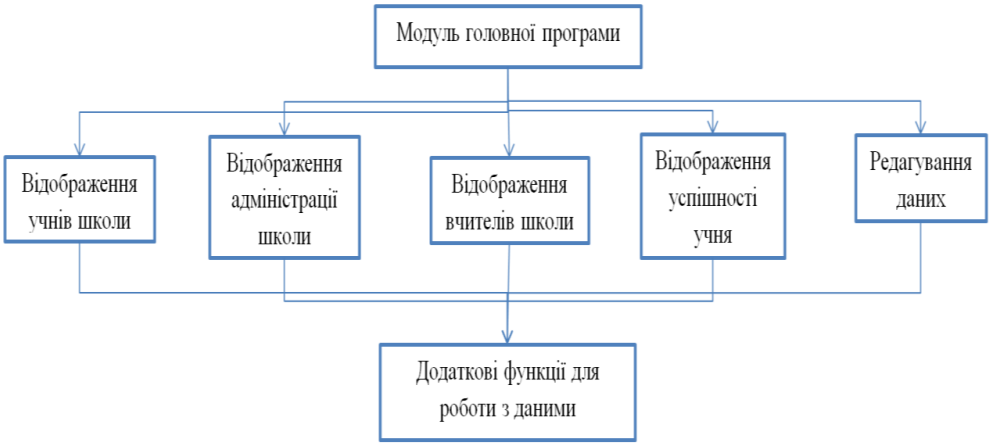


Рис. 2. Модуль журналу

Є кілька режимів екрану. Один з них включає від 1 до 4 панелей, за допомогою яких можна показувати до чотирьох файлів одночасно. Повноцінний (free modes) режим показує тільки один файл без будь-яких додаткових навколо нього меню. Для розроблення бази даних, в якій буде зберігатись інформація про розклад, користувачів, журнали, було вибрано середовище phpMyAdmin – безкоштовне та найчастіше використуване середовище для управління MySQL. База даних програми складається із 7 таблиць: user, settings, journals, pupils, log, schedule та study_plan.

Таблиця «User» містить наступні поля: id (лічильник), login (логін користувача), password (пароль користувача), bio, initials (ініціали), name (ім'я), access (рівень доступу), gender (стать), birthday (дата народження). Таблиця зображена на рис. 3.

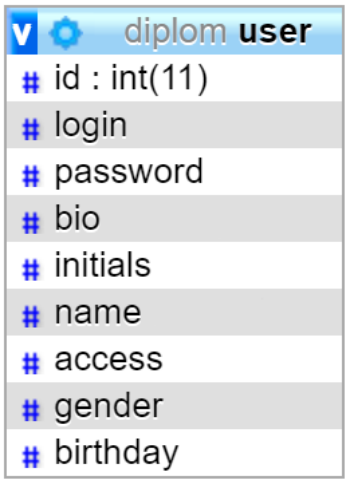


Рис. 3. Таблиця «User»

Таблиця «Settings» містить такі поля: id, status_site, auth, time_session, show_error, debug_mode. Таблиця «Journals» містить такі поля: id (лічильник), id_teacher (id вчителя), name (ім'я), int_class (цифра класу), name_class (символ класу: А, Б або В). Таблиця «Pupils» містить такі поля: id (лічильник), id_user (id користувача), int_class (цифра класу), name_class (символ класу: А, Б або В). Таблиця «Study_plan» містить такі поля: id (лічильник), subject (назва уроку), date (дата), lesson (урок по порядку), thema (тема уроку), homework (домашнє завдання)

Результатом виконання є розроблена система програмного комплексу «Електронна школа». За допомогою цієї системи можна зробити перегляд розкладу та редагування журналу зручнішим

способом. В проекті проведено дослідження щодо корисності електронної школи, розглянуто готові рішення та обґрунтовано вибір технологій для реалізації системи. Під час роботи було проаналізовано принципи побудови систем управління даними та розроблено модульну структуру сайту.

Веселовська Т. С.,
аспірант кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ

ОКРЕМІ ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Технічні засоби є ефективним інструментом для отримання та фіксації злочинної діяльності. Тому питання їх використання для виконання завдань оперативно-розшукової діяльності та кримінального провадження, досліджували як вітчизняні, так і зарубіжні вчені. Зокрема Рогатинська Н. З. зазначає, що існують обставини, які гальмують впровадження науки та техніки у повсякденну роботу практичних підрозділів щодо протидії злочинності. До них можна віднести: різноманітність трактувань суті спеціальних знань та технічних засобів; нечіткість і непослідовність багатьох запропонованих класифікаційних форм використання таких знань та засобів; недостатньо повну, а найчастіше і суперечливу їх правову регламентацію; відсутність єдиного погляду на компетенцію учасників кримінального процесу у використанні цих знань та засобів і на доказове значення отримуваних результатів; не визначено також, що необхідно розуміти під ефективністю застосування спеціальних знань та науково-технічних засобів, які критерії її визначення, як краще всього можливо вплинути на підвищення цієї ефективності; відсутність комплексного дослідження проблем, пов'язаних із застосуванням спеціальних знань та науково-технічних засобів [1, с.134].

Натомість Саприкін Є. І. підкреслив, що відсутність єдиного та чіткого розуміння найважливіших понять і термінів в території та практиці ОРД може призвести до негативного впливу на практику, породити коливання та плутанину до їх застосування [2, с.138].

З даного питання слушно висловились Князєв С. М., Чернявський С. С., Грібов М. Л., що окрім як у визначенні ОРД, терміни «оперативні засоби», «оперативно-технічні засоби», «пошукові заходи», «розвідувальні заходи», «контррозвідувальні заходи», «гласні заходи», «негласні заходи» в тексті Закону не використано. Діяльність з невизначеним змістом не може бути інструментом досягнення певної мети, виконання завдань. З огляду на це, учені, які досліджували аспекти ОРД, змушені були, насамперед, формулювати власне визначення поняття такої діяльності, її змісту й окремих компонентів. Найефективнішими виявилися ті підходи, які ґрунтувалися на глибокому аналізі фундаментальних наукових праць щодо змісту людської діяльності загалом і юридичної діяльності зокрема [3, с.12].

Відтак, Хараберюш І. Ф. розглядаючи використання технічних засобів в правоохоронній діяльності в межах існуючого у той час технічного та правового забезпечення, зробив висновок, що автори по-різному підходили до визначення самого поняття «спеціальна техніка». Окремі науковці звужували його до технічних засобів тільки оперативно-розшукового призначення, інші, визнаючи це поняття родовим, обмежувались тільки технічними засобами не враховуючи методику і тактику їх використання, деякі з них, даючи визначення спеціальній техніці, ураховували її складові, але недостатньо, окреслювали напрямки й форми її використання або не враховували структурних змін, які мали місце в органах внутрішніх справ [4, с. 6]. Стосовно «спеціальної техніки правоохоронних органів» у самому загальному вигляді йдеться про сукупність засобів спеціальної техніки, тактики і методики їх ефективного правомірного використання в правоохоронній діяльності [5, с. 93].

Водночас серед науковців не існує єдиного підходу до їх класифікації. Авторів теоретичних розробок вказаного питання можна умовно поділити на тих, які вивчають теоретичні і практичні аспекти застосування положень статті 273 КПК, а також тих, які під час аналізу зазначеної тематики спираються на теоретичні положення щодо засобів оперативно-розшукової діяльності, оскільки НС(Р)Д засвоїм змістом майже збігаються з відповідними оперативно-розшуковими заходами. Тому Соколов О. В. вважає, що вказане обумовлює необхідність більш детального наукового дослідження питання щодо засобів, які використовуються оперативними підрозділами під час проведенні НСРД, із врахуванням наявної практики правоохоронних органів [6, с.176].

За характером засобів, які використовувались для отримання матеріалів ОРД, останні можна класифікувати на:

- отримані з використання технічних засобів;
- отримані без їх використання.

Такий підхід матеріалів обумовлений необхідністю врахування під час їх використання особливостей технічних засобів, приладів, устаткування, які застосувалися, їх технічних характеристик та властивостей самих матеріалів, що отримані, оскільки залучення таких матеріалів до кримінального провадження потребує їх відповідної перевірки та процесуального оформлення [7, с. 86].

Під час проведення опитуванням 124 слідчих (дізнавачів), у своїй дисертаційній роботі Поляком Ю. П., було задано запитання:

- «Як часто під час досудового розслідування Ви застосовуєте технічні засоби із залученням для цього спеціаліста?»: 54% відповіли, що лише у випадках, коли це прямо передбачено законодавством, 29% – хотілося б частіше, ніж зараз дозволяють обставини, 17% – «по-можливості постійно;
- «Чи проводили Ви негласні слідчі (розшукові) дії особисто?», 100% працівників вказали, що «ні, доручають їх проведення оперативним підрозділам» [8, с. 222–224].

Нами також було проведено анкетування 200 оперативних працівників поліції, які на запитання:

- «Чи виконуєте Ви НСРД/ОТЗ?», 57% відповіли «залучаю оперативно-технічні підрозділи», 43% – «так»;
- «Які потрібно внести зміни до законодавства, для покращення проведення НСРД/ОТЗ?»: 37% відповіли «нічого не потрібно, все врегульовано на законодавчому рівні; 59 % «потрібно створити єдиний уніфікований збірник»; лише 4% надали свій варіант, вирішення даної проблеми.

Також одними із причин недостатнього використання ТЗ у практичній діяльності Н. С. Карпов наводить такі:

- недостатність уваги з боку керівників щодо ефективності використання досягнень науки і техніки;
- проблеми в організаційній, виховній та практичній роботі керівників підрозділів, зокрема відсутність контролю за застосуванням ТЗ;
- громіздкість та ненадійність в експлуатації деяких ТЗ, непристосованість їх до умов проведення процесуальних дій;
- складність процедури підготовки до роботи ТЗ, а також їх технічного обслуговування та інші [8, с. 80–81].

Отже, правильна організація та застосування технічних засобів працівниками Національної поліції під час виконання завдань ОРД та досудового розслідування забезпечує розкриття та фіксацію кримінальних правопорушень. Однак проблеми, які виникають у практичній діяльність (понятійний апарат; фінансове забезпечення; проведення навчання щодо їх використання та ін.) повинні бути врегульовані на законодавчому рівні.

Література

1. Рогатинська Н. З. Використання та фіксування науково-технічними засобів у розшуковій діяльності слідчого. Вісник ХНУ імені В. Н. Каразіна. Серія «Право». 2017. Вип. 24. С. 133-135.
2. Саприкін Є. І. Визначення поняття оперативно-розшукового заходу. Матеріали науково-практичного семінару (ДДУВС, 16.05.2014). Актуальні питання оперативно-розшукової протидії злочинам. 2014. С.138-140.
3. Князєв С. М., Чернявський С. С., Грібов М. Л. Законодавче регулювання оперативно-розшукової діяльності: проблеми та шляхи їх розв'язання. Юридичний часопис Національної академії внутрішніх справ. 2020. №2(20). С.8-20. doi: https://doi.org/10.33270/04202002.8
4. Хараберюш І. Ф. Спеціальна техніка правоохоронних органів як міждисциплінарана категорія юридичної науки. Часопис Національного університету «Острозька академія». 2019. №1(19). С.1-25.
5. Хараберюш І. Ф. Окремі погляди щодо співвідношення спеціальної теніки правоохоронних орнагів та криміналістичної техніки. Теорія та практика судової експертизи і криміналістики. №20. 2020. С.88-102. DOI: https://doi.org/10.32353/khrife.2.2019.06

6. Соколов О. В. Засоби, що використовуються оперативними підрозділами при проведенні негласних слідчих (розшукових) дій. Публічне право. 2018. №1 (29). С.176-186.
7. Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові дії) та використання результатів оперативно-розшукової діяльності у кримінальному провадженні. Навчально-практичний посібник. Харків. 2018. 540с.
8. Поляк Ю. П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його результатів під час досудового розслідування. Дисертаційне дослідження на здобуття ступеня доктора філософії. Львів. 2022. С.230.

Галайко Н. В.,
старший викладач кафедри соціально-поведінкових, гуманітарних наук та економічної безпеки Львівського державного університету внутрішніх справ

Шевченко Н. В.,
доцент кафедри фінансів та обліку Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЧИННИК ІННОВАЦІЙНОГО РОЗВИТКУ ЕКОНОМІКИ

Технологічний прогрес та інновації є довгостроковими рушійними силами економічного зростання. Інформація та знання розуміються як продуктивні сили та стають найважливішим фактором розвитку сучасного суспільства. А галузі, які виробляють знання та інформаційні продукти стають все більш значущими, від них залежить процвітання та конкурентоспроможність країни. Зазначимо, що на сьогодні лідерами стають не ті держави у яких є природні ресурси, військовий потенціал чи значна територія а ті, у яких розвинені наукомісткі галузі та інформаційні технології. Тому стратегічним завданням для реформування економіки України має стати розвиток економіки, яка буде заснована на знаннях і новітніх технологіях.

Системою економічних, соціальних та культурних відносин, які реалізуються з допомогою цифрових інформаційних технологій, є цифрова економіка, яка фокусується не тільки на створенні умов, необхідних для появи революційних та перспективних нових цифрових технологій, а й на застосуванні інноваційних бізнес-моделей.

Розробкою базової системи показників для оцінки цифровізації економіки та соціальних відносин займаються багато впливових міжнародних організацій, інституцій та різних аналітичних агентств. Існує низка загальноприйнятих параметрів, за допомогою яких можна визначити рівень цифровізації економіки.

Для оцінки стану розвитку цифрової економіки найчастіше використовуються наступні рейтингові індекси цифровізації:

- індекс цифрової економіки та суспільства (Digital Economy and Society Index – DESI);
- індекс цифрової еволюції (Digital Evolution Index – DEI);
- індекс прийняття цифровізації (Digital Adoption Index – DAI);
- індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index – IDI);
- глобальний інноваційний індекс (Global Innovation Index – GII);
- індекс мережевої готовності (Networked Readiness Index – NRI);
- індекс цифровізації економіки (Boston Consulting Group – e-Intensity);
- індекс світової цифрової конкурентоспроможності (IMD World Digital Competiveness Index – WDCI) [1].

Так, наприклад за методологією DESI порівнюють середні показники за 5 напрямами:

- піідключення: розгортання широкосмугової інфраструктури та її якість;
- людський капітал: навички, необхідні для використання можливостей, запропонованих цифровим суспільством;
- використання громадянами Інтернету: різноманітність видів діяльності громадян в Інтернеті;
- інтеграція цифрових технологій: оцифрування бізнесу і розвиток каналу онлайн-продажів;
- публічні сервіси: оцифрування державних послуг (електронний уряд) [2].

У звіті 2022 року найбільш інноваційною країною визнано Швейцарію, за нею йдуть США, Швеція, Велика Британія та Нідерланди. Також відзначається, що до ТОП-10 інноваційних економік світу наблизився Китай (11 місце), в той час як Туреччина та Індія вперше увійшли до ТОП-40 [3].

Рейтинг країн у розрізі регіонів за цифровізацією економіки подано на рис. 1.

Україна в Глобальному інноваційному індексі 2022 року займає найгірші позиції за останні сім років і посідає 57 місце, утримуючи 4-ту позицію серед 36 країн економічної групи lower-middle income.

Аналіз даних рис. 2 свідчить, що у рейтингу інноваційних економік, який вже протягом дев'яти років складає агенція Bloomberg, Україна займає також незадовільні позиції. У 2021 році з поміж 60 країн вона займає 58 позицію й слід визнати, що останнім часом ситуація дещо погіршується. Так, за період з 2015 року по 2021 рік наша країна втратила аж 25 сходинок. Зазначимо, що останніми роками зроблено досить багато позитивних кроків з боку держави в напрямку розвитку процесів цифровізації, зокрема створено Міністерство цифрової трансформації. Це в свою чергу має прискорити реалізацію цифрових перетворень в Україні та покращити найближчими роками позиції нашої держави в наведених рейтингах.

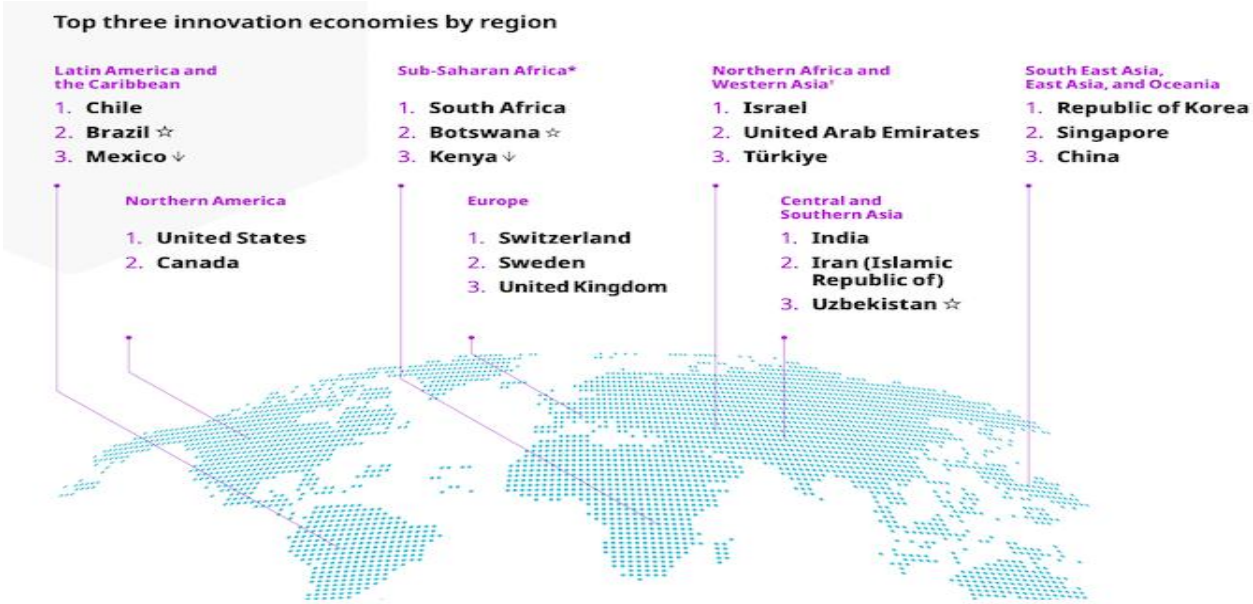


Рис. 1. Топ три інноваційні економіки регіону [3].

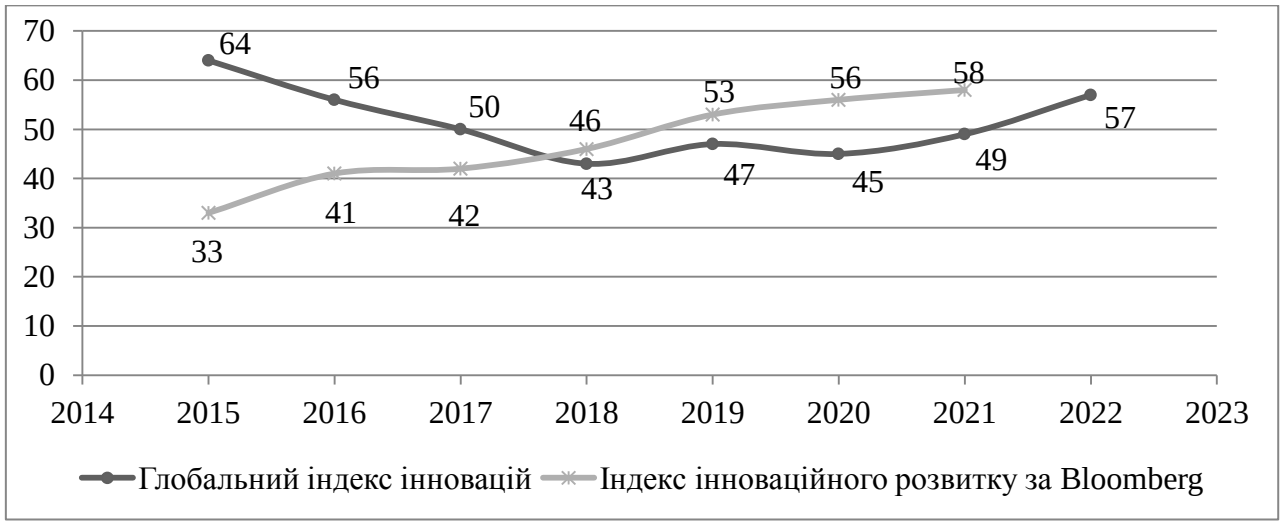


Рис. 2. Україні у міжнародних рейтингах, що відображають інноваційний розвиток [4]

Аналіз даних рис. 2 свідчить, що у рейтингу інноваційних економік, який вже протягом дев'яти років складає агенція Bloomberg, Україна займає також незадовільні позиції. У 2021 році з поміж 60 країн вона займає 58 позицію й слід визнати, що останнім часом ситуація дещо погіршується. Так, за

період з 2015 року по 2021 рік наша країна втратила аж 25 сходинок. Зазначимо, що останніми роками зроблено досить багато позитивних кроків з боку держави в напрямку розвитку процесів цифровізації, зокрема створено Міністерство цифрової трансформації. Це в свою чергу має прискорити реалізацію цифрових перетворень в Україні та покращити найближчими роками позиції нашої держави в наведених рейтингах.

Таким чином, незважаючи на те, що в даний час в Україні спостерігається розвиток галузі інформаційних технологій, наша країна відстає від країн-лідерів інноваційних економік. Серед основних причин можна виділити те, що наше суспільство та влада, ще у повній мірі не усвідомила той факт, що інформація є двигуном та основою нової діяльності. Зростання цифрової економіки сприятиме появі нових можливостей та розвитку інновацій, стимулюватиме подальший ріст ефективності економіки, фінансових установ та бізнес-системи.

Література:

1. Руденко М. В. Аналіз позицій України в глобальних індексах цифрової економіки. *Економіка та держава*. № 2, 2021. С. 11-18.
2. Мазуренко О. К. Оцінювання розвитку цифрової економіки в країнах Балтії та Східної Європи за методологією DESI. InterConf, вип. 52, Травень 2021, с. 74-80, doi:10.51582/interconf.21-22.04.2021.007.
3. Глобальний інноваційний індекс 2022 року. URL: https://ukrpatent.org/uk/news/main/wipo-global-innovation-index-2022-29092022 (дата звернення: 05.12.2022).
4. Крилов Д. В. Аналіз рейтингового оцінювання розвитку інноваційної діяльності в Україні. *Ефективна економіка*. 2022. № 5. – URL: http://www.economy.nayka.com.ua/?op=1&z=10285 (дата звернення: 05.12.2022). DOI: 10.32702/2307-2105-2022.5.8

Глинський Я. М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

Пелех Я. М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

ЕЛЕКТРОННИЙ НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС В LMS MOODLE ЯК ЕКСПЕРТНА НАВЧАЛЬНА СИСТЕМА

Стрімке прискорення науково-технічного прогресу призвело до того, що отримувані в навчальних закладах знання, засновані на фактах, досить швидко потребують удосконалення й оновлення. Неухильне розширення обсягу навчального матеріалу приводить до його «стискання», згортання і алгоритмізованого подання, без розуміння студентом його глибинної сутності. Наслідком цього є низька мотивація до пізнавальної діяльності, формальність отриманих знань, невміння приймати коректні й ефективні управлінські рішення в критичних ситуаціях, поглиблення протиріччя між численною кількістю випускників вищих навчальних закладів та реальним невеликим числом достатньо кваліфікованих фахівців-професіоналів [1]. Типовою стає ситуація, коли студент може знати, але не вміти, або навпаки, вміти, але не в змозі пояснити, як і головно що він робить на практичних чи лабораторних заняттях.

Автоматизація навчального процесу не сприяє вирішенню повсталих проблем, але є конче необхідною в умовах пандемій і воєнного стану, коли заняття відбуваються змішано чи дистанційно. Різновидом засобів автоматизації можуть слугувати експертні навчальні системи, які ми тут розглядаємо з позицій систем підтримки прийняття рішень (СППР).

У цій порівняно новій галузі наукових досліджень немає однозначних трактувань термінів і понять, а також усталених означень.

Експертною системою (ЕС) вважатимемо систему підтримки прийняття рішень, яка містить знання з певної вузької предметної області, а також може пропонувати користувачу розв'язок проблем з

цієї галузі. Експертна система акумулює професійні знання фахівців, використовуючи їх для формування бази знань, яка містить набір взаємопов'язаних правил чи відомостей.

На практиці експертна система являє собою спеціалізовану обчислювальну машину (процесор), що відтворює алгоритм розв'язування людиною певних практичних задач на основі професійно-орієнтованих знань, переданих їй відповідними спеціалістами.

Експертна навчальна система (ЕНС) – це комп'ютерна програма, побудована на основі знань експертів предметної області (кваліфікованих викладачів, методистів, психологів), яка здійснює та контролює процес навчання [2]. Призначення такої системи полягає в том, що вона, з одного боку допомагає викладачу навчати та контролювати студентів, а з іншого – студенту самостійно навчатися.

Розробка експертних систем навчального призначення потребує спеціальних програмних оболонок, які пристосовані для того, щоб їх міг заповнювати викладач, який не є фахівцем в галузі програмування, що робить його автором автоматизованого навчального курсу (ЕНМК – електронного навчально-методичного комплексу) і заохочує до роботи із засобами комп'ютерних технологій навчання.

Такі можливості надають сучасні системи управління навчанням (англ. Learning Management System – LMS). LMS – це комп'ютерний програмний комплекс, який використовується для розробки, управління та поширення навчальних онлайн-матеріалів із забезпеченням спільного доступу до них [3].

Не кожний ЕНМК, розроблений в LMS Moodle, є ЕС.

Створення експертних систем для оцінювання якості засвоєння знань передбачає, насамперед, врахування наступних основних принципів [2]:

- функціонування викладача як фахівця-консультанта у навчальному процесі;
- відмова від поточного методу масового навчання і перехід до індивідуальних траєкторій підготовки студентів;
- перенесення більшої частини навчального процесу на самостійну роботу студентів;
- врахування особливостей використання комп'ютеризованих технологій навчання;
- відмова від традиційних форм контролю і впровадження індивідуального кумулятивного індексу, за допомогою якого різко зростає роль поточного, проміжного та підсумкового контролю знань, умінь і навичок.

За природою знання поділяють на декларативні та процедурні. Декларативні (предметні) знання – це факти і зв'язки між ними. Декларативні знання подаються в ЕНМК через систему взаємопов'язаних фактів з відповідної предметної області.

Перевірка рівня засвоєння декларативних знань відбувається в ЕНМК автоматично за допомогою системи тестування, до якої ставляться вимоги повноти, багатоваріантності і релевантності. Більшість підходів до створення тестів націлені виключно на контроль знань. У нашому підході тести мають слугувати не тільки для контролю знань, але й для генерування нових знань. Студенти часто легко розв'язують тестові задачі і вправи з числовими відповідями, але й так само часто невзмозі підтвердити теоретичні знання. Тому звертаємо увагу на тести, які навчають. Прикладом тесту, який навчає, є тест з таким формулюванням: «Яке з наступних тверджень є хибним: 1) консолідація – це технологія об'єднання даних; 2) кореляція – це залежність між даним; 3) апроксимація – це процес наближення даних; 4) форматування – це процес зміни вигляду даних; 5) Сонце обертається навколо Землі. Після очевидно успішного подолання такого тесту читач буде ознайомлений з поняттями консолідація, кореляція, апроксимація і форматування. Щоб тест не лише навчав, але й виконував контрольну функцію, п'ятий пункт варто сформулювати орієнтовно так: 5) редагування – це процес пересилання даних, що є хибним твердженням.

У свою чергу процедурні знання являють собою набір певних процедур перетворення знань як даних. Процедурні знання виявляються через дію. Процедурні знання генеруються в результаті виконання студентом практичних і головно лабораторних завдань. Перевірити такі знання автоматично вкрай важко, але можна. Якщо зазвичай викладач затрачає значні зусилля і час на перевірку виконання лабораторної роботи студентом у режимі face-to-face, то тепер цей процес рекомендується перекласти на машину. Для цього потрібно створити тести зовсім нового типу. Після виконання лабораторної роботи студент за її результатами виконує тест, що складається з кількох теоретичних запитань і головно запитань, що базуються на отриманих під час роботи індивідуальних результатах. Питання тесту можна формулювати так: Який результат після проведення консолідації даних отримано у клітинці електронної таблиці D8? Або так: За скільки періодів буде погашена надана банком позика? Або ось

приклад невдалого запитання, яке не стимулює аналіз даних: Введіть число, отримане в клітинці електронної таблиці C16. До аналізу даних, що є складовим елементом бізнесаналітики, стимулює запитання задане інакше: Який прибуток (чи дохід) отримала компанія «Метро» у березні 2022 року (саме він є у клітинці C16)? Власне такими тестами можна стимулювати аналітичне мислення і розвивати вміння приймати рішення, тобто зменшити негативні впливи процесів тестування на якість оцінювання знань і вмінь студентів.

Проблему реалізації автоматичної системи захисту лабораторних робіт ми на даний час не розв'язали, а лише сформулювали. Складність лежить у необхідності створення мультиваріантних тестів (в одній лабораторній роботі кожному студенту треба надати інше завдання й інший тест). Результати тестів треба занести в одну графу електронного журналу, що без участі професіоналів-програмістів у LMS Moodle зробити поки що не можемо, хоча вміємо програмувати електронний журнал до інших потреб. Нам невідомі розв'язки цієї проблеми в МВОК (масові відкриті онлайн курси) edX, Coursera чи вітчизняному ресурсі Prometheus. У них реалізовані одноваріантні тести, які контролюють виконання лабораторних завдань, де всі слухачі отримують одне і теж індивідуальне завдання і один тест, що передбачає відсутність контактів між слухачами з метою обміну результатами роботи та відповідями, а також відсутність підходу до навчання за принципом «Дай списати», що у наших реаліях є непродуктивно.

Розглянемо прийом стимулювання студентів до навчання через ефективне використання індивідуального кумулятивного індексу навчання і його вплив на об'єктивість оцінювання знань. Навчальний курс розглядається як гра, де встановлюється кумулятивний індекс як сума набраних балів за різні види навчальної діяльності. Протягом семестру реалізуються 100 балів з фіксуванням усіх поточних і підсумкових оцінок в електронному журналі ЕНМК. У нашій дисципліні бали акумулюються щотижнево так: за виконання і захист 13 лабораторних робіт надається 34 бали (по 2-3 бали за роботу), за виконання і захист двох розрахунково-графічних робіт надається 16 балів, за здачу поточних тестів студент може акумулювати до12 балів, а іспитовий тест принесе йому до 38 балів. Один-два рази протягом семестру викладач демонструє на великому екрані журнал як турнірну таблицю змагань з відзнаками лідерів і виявленням аутсайдерів (рис. 1). На проходження кожного поточного тесту надаються 3-4 спроби (життя), де LMS автоматично фіксує у журналі результати останньої спроби. Банк тестів курсу містить більше 50 категорій тем, орієнтовно по 20-30 запитань-завдань у кожній категорії.

Прізвище / Ім'я	Сума	П	Е	Іспит	Л1	Л2	Л3	Л4
Сенів Ліліана	32	24	8	-	2,0	3,0	2,0	3,0
Корінь Софія	32	25	7	-	1,8	3,0	2,0	3,0
Димон Ірина	30	24	6	-	1,0	2,8	1,5	3,0
Педенко Богдан	27	21	6	-	2,0	2,5	1,0	3,0
Красуляк Лілія	26	18	9	-	2,0	2,5	2,0	0,5
Бончик Катерина	26	26	-	-	2,0	3,0	2,0	2,9
Войтович Лілія	22	17	5	-	2,0	2,0	2,0	2,8
Курило Софія	22	13	9	-	2,0	3,0	2,0	2,5
Карачун Ірина	22	18	4	-	1,0	3,0	1,8	2,9
Грицик Олександр	21	19	2	-	2,0	2,5	-	2,9
Папроцька Віта	19	11	8	-	-	3,0	2,0	2,5
Гривняк Марія-Вікторія	17	14	4	-	1,5	2,0	1,8	2,8
Луць Давид	15	9	7	-	-	0,5	0,5	2,0
Соломко Вікторія	15	7	9	-	-	2,0	0,5	-

Рис. 1. Фрагмент електронного журналу з рейтинговими проміжними результатами навчання

Один тест складається з 8-10 запитань на 10-12 хвилин тестування, а іспитовий тест містить 30 запитань різної складності на 40-45 хвилин. Запитання вибираються системою випадково, тому повторення запитань під час тестування у різних студентів чи у різних спробах малоймовірні, але можливі. Тому робота над розширенням категорій, що є запорукою релевантного і об'єктивного

автоматичного оцінювання роботи студента на курсі є актуальною. В цьому і полягає здатність функціонувати цієї системи як експертної оскільки вона повністю замінює викладача на етапі оцінювання знань і звільняє його від рутинної роботи. Якщо іспит розпочався якогось дня о 12 год, то вже о 12.45 результати іспиту і всі підсумкові бали надходять у csv-файлі на вхід електронної системи «Деканат», де автоматично формується електронна відомість без участі викладача.

У цій системі студент має змогу працювати з навчальним матеріалом відповідно до своїх можливостей, використовуючи зручний для себе спосіб отримання навчальних повідомлень: у вигляді текстових файлів, відеолекцій, авторських відеоматеріалів [4]. Завдяки відеоресурсам вдалося вийти на значно вищий рівень навчання, ніж у до відео період, оскільки вдалося ефективно подати складні теми, заохотити студентів до самонавчання, розвинути в них вміння вчитися, застосовуючи можливості LMS Moodle, Google та YouTube [5].

Надання ЕНМК рис ЕС дало змогу максимально автоматизувати процес навчання, вивільнити експерта-викладача від поточної рутинної роботи, зосередити зусилля на поповненні, оновленні бази знань (текстового і відео контенту, банку тестів), аналізі статистичної інформації, яку надає система, простежити успішність кожного студента в динаміці, удосконалити алгоритми навчання, стимулювати у студентів творче мислення, підсилити значимість їхньої самостійної роботи, підтримати постійне зацікавлення до навчальної дисципліни, утвердити впевненість в об'єктивному оцінюванні набутих студентом знань і вмінь.

Література:

1. Соловей Л. Я. Педагогічні аспекти використання експертно-навчальних систем. URL: https://fi.npu.edu.ua/files/Zbirnik_KOSN/17/28.pdf .
2. Донченко Т. В. Експертні навчальні системи в дистанційній освіті. ХНЕУ, Харків. URL: https://core.ac.uk/download/pdf/232882165.pdf .
3. Кухаренко В. М. та ін. Теорія та практика змішаного навчання. Харків, Україна: "Міськдрук", НТУ "ХПІ", 2016.
4. Ярослав Глинський. YouTube-канал. URL: https://www.YouTube.com/ results?search_query= ярославглинський.
5. Глинський Я. М., Пукач П. Я. Досвід змішаного навчання інформатики студентів економічних спеціальностей з використанням засобів LMS Moodle та YouTube: Інформаційні технології і засоби навчання, т. 83, №3, с. 113–119, 2021.

Дегтярьов Д. І.,
здобувач Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ДИСТАНЦІЙНОГО НАВЧАННЯ КУРСАНТІВ У ЗВО ЗІ СПЕЦЕФІЧНИМИ УМОВАМИ НАВЧАННЯ

Потужний розвиток інформаційних технологій зумовлений стрімким впровадженням інноваційних технологій в усі сфери суспільного життя населення. Освітня сфера не є виключенням, адже завдяки новітнім інформаційним нововведенням в навчальний процес вдається не лише покращити рівень знань, а й підвищити якість проведення занять викладачами, зокрема за допомогою сучасних медіа проекторів, звукових установок та ін.

Слід зауважити, що у зв'язку з поширенням епідемічної ситуації в усьому світі особливої актуальності набуло дистанційне навчання. Завдяки запровадженню та розповсюдженню дистанційного навчання можливо в умовах карантину все ж таки надавати можливість не відставати від процесу навчання.

Але, на нашу думку, не для всіх закладів освіти дистанційне навчання є позитивним впровадженням, зокрема для вищих навчальних закладів зі специфічними умовами навчання це є негативним, адже задля підготовки кваліфікованих спеціалістів у галузі правознавства необхідні не лише теоретичні знання, а й практичні.[1, с. 158]. Такі дисципліни як, тактико-спеціальна підготовка, вогнева підготовка та спеціальна фізична підготовка неможливо проводити дистанційно, адже на таких дисциплінах повинні відпрацьовуватися фізичні та тактичні навички, зокрема культура поводження зі зброєю, певні тактичні правила поведінки в ситуаціях, з якими можуть стикатися поліцейські під час проходження служби в правоохоронних органах а також спеціальні прийоми, які допомагають не лише захистити себе від правопорушників, а й захистити інших громадян від злочинних посягань на їх життя чи здоров'я.

Слід зауважити, що освіта правоохоронців повинна бути якісною та з запровадженням якісного закордонного досвіду, адже Україна орієнтована до міжнародних стандартів, а якісна освіта є одним з таких стандартів, тому має досить важливе значення.

На нашу думку, варто розглянути закордонний досвід запровадження дистанційного навчання поліцейських закордоном з метою виявлення позитивних моментів проведення таких спеціальних дисциплін, які потребують не лише теорії а й практики.

Цікавим є досвід Словаччини, в даній країні існує інноваційний підхід до дистанційного навчання поліцейських, який полягає в застосуванні в цій формі навчання найбільш конкурентоспроможних освітніх розробок, сучасного технічного обладнання, впровадження найбільш ефективних інформаційно-комунікаційних технологій (віртуальна реальність, доповнена реальність, 3Dмоделювання тощо).[2, с. 241].

Щодо ситуації з приводу даного питання в Україні, то варто зазначити, що в нас також наявні вищевказані інноваційні технології, але вони запроваджені не у такій кількості як закордоном, що пояснюється у відсутності певного фінансування даного питання, що є негативним аспектом даної проблеми.

У підсумку, варто зазначити, що завдяки впровадженню якісного дистанційного навчання у правоохоронну освіту, яка буде на рівні зі світовими країнами вдасться не лише покращувати знання та навички поліцейських, але й дотримуватися умов карантину, що є досить важливим на сьогоднішній день. А також для курсів які мають добру фізичну підготовку, робити практичні заняття на дистанційному навчанні, а іншим курсам буде до вподоби теоретичні заняття.

Література:

1. Бугайчук К. Л. Застосування технологій дистанційного навчання в післядипломній освіті працівників Національної поліції. Підготовка поліцейських в умовах реформування системи МВС України : зб. матеріалів ІІ міжнар. наук.-практ. конф. Харків : ХНУВС, 2017. С. 157–161.
2. Прібиткова Н. О. Дистанційне навчання як інноваційний підхід у сфері підготовки кадрів для Національної поліції України. Підготовка охоронців правопорядку в Харкові (1917–2017 рр.): зб. наук. ст. і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.). – Харків: ХНУВС, 2017.С. 240–242.

Домчак С. І.,
старший інспектор 1-го відділу (оперативного реагування) Управління протидії кіберзлочинам у Львівській області Департаменту кіберполіції Національної поліції України

МЕТОДИКА ВИКОРИСТАННЯ OSINT В ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ

Перш за все треба зрозуміти, що таке OSINT – це (*Open source intelligence)* в перекладі означає "Розвідка на основі відкритих джерел". Вона складається з концепцій, методологій і технологій добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів.

За наявності публічних даних про конкретну ціль хакер або пентестер може скласти профіль потенційної жертви. Це потрібно для того, щоб краще зрозуміти її характеристики та звузити область

пошуку можливих уразливостей. Зловмисники не обов'язково активно впливають на ціль, але також за допомогою отриманих даних можуть моделювати загрозу і розробляти план атаки.

Кібератака, як і всі атаки починається з розвідувальної операції, для початку відбувається пасивне отримання розвідданих. Збір інформації OSINT про себе або про своє підприємство – це теж добрий спосіб побачити, які дані ви надаєте потенційним зловмисникам. Як тільки ви дізнаєтесь, яку інформацію про вас можна зібрати з відкритих джерел, зможете використовувати її, щоб допомогти собі або вашій команді безпеки розробити ефективні стратегії захисту. OSINT здатний виконати майже всі завдання, що ставляться перед приватними детективами.

Тож чим відрізняється звичайний серфінг у мережі від OSINT'а? Насамперед у глибині підходу. Так, для багатьох користувачів мережі пошук завершується на стадії, де для професіоналів все найцікавіше тільки починається.

OSINT дозволяє виконати близько 90% завдань, що стоять перед приватними детективними агенціями. Так, у мережі представлені найцінніші джерела даних: сайти оголошень, торгові майданчики, блоги, форуми за інтересами, державні проекти, банківські онлайн-системи, соціальні мережі. Важливо лише із загального «сума» зуміти вичленувати справді важливу та корисну інформацію, що іноді може зрівнятися з просіюванням гори землі через сито для фільтру золотих порід. Необхідно розуміти, що іноді інформація є значно ціннішою і суттєвішою, ніж купа дорогоцінного металу. Деякі дані можуть затягнути на мільйони та мільярди.

То чим відрізняється новачок від професійного «серфера»? Перший просто бачить кумедну картинку, репостик з порадами, сторінки та групи для вбивання часу. Професіонал відзначає дати публікації контенту, зацікавленість та активність користувачів, важливі деталі на зображеннях, мітки з геолокацією, оцінює цільову аудиторію – і це лише початок. На наступному етапі може бути надіслано IP-logger, що дозволяє визначити IP-адреси. Потім слід просканувати порти, щоб зрозуміти, яке технологічне оснащення знаходиться поруч із конкретною людиною: камери, принтери, ПК, роутери та інше обладнання, підключене через мережу. Так, якщо у списку буде виявлено 2-3 ксерокси, можемо припустити, що людина знаходиться на робочому місці в офісі. А ось ще один наочний приклад. В адресних рядках соцмережах таких як Facebook, Instagram, Vkontakte до основної адреси профілю після слеша додається персональний ID, що не секрет. Але він може містити не лише цифри, а ще й нікнейм. Останній є найціннішою інформацією, адже більшість користувачів мережі схильні використовувати ті самі псевдоніми на різних ресурсах. Так, по одному нікнейму в адресному рядку можна «пробити» й інші активності конкретного користувача: сторінки в соціальних мережах, повідомлення на тематичних форумах, резюме, замовлення на торгових майданчиках і т. д.

Технологія дозволяє збирати максимум інформації із відкритих джерел для повноцінного професійного аналізу. При цьому дані можуть розміщуватись у різних формах: статті, публікації обговорення на форумах, відео- та аудіофайли, документи, картинки, анімації, гіфки тощо.

Перш ніж знайти відповідь на запитання або задовольнити потребу в знаннях, користувачів здійснює пошук інформації та піддає її якісному аналізу, що забирає часом надто багато часу. Ну а отримання точних результатів для обивателя взагалі стає важко здійсненним завданням. Допомогти в цьому можуть інструменти з відкритим вихідним кодом, які також можна запустити одночасно. Вони зберуть вам дані з доступних джерел, залишаючи за вами лише роботу зі зіставлення та аналітики.

ОСНОВНІ ІНСТРУМЕНТИ І МЕТОДИ

Shodan. Поки все активно використовую гугл для відповідей на найпростіші життєві питання, нереально крута пошукова система Shodan дає можливість хакерам переглядати виставлені активи. Так, сервіс відразу продемонструє вам вибірку результатів, які найповніше в плані сенсу відповідають вашому запиту. Найчастіше користуються системою для пошуку активів, підключених до мережі.

Інструмент має відкритий вихідний код, дозволяє провести якісну аналітику з питань безпеки, перевірити вразливі місця конкретної мети (відкритість особистих даних, доступної паролів та портів, IP-адреси тощо). Також Shodan забезпечує найбільш адаптивний пошук спільнот.

Google Dorks. Сервіс насправді запущений з 2002 року, але зізнайтеся, чи ви чули про нього? Він демонструє чудову продуктивність і є справді інтелектуальним інструментом, що базується на запитах. Сервіс має відкритий вихідний код, допомагаючи користувачам швидко орієнтуватися на результати чи індекс пошуку.

Maltego. Вбудований в Kali Linux ефективний інтелектуальний інструмент від компанії Paterva має відкритий код і призначений для серйозних досліджень цілей за допомогою перетворень. Написаний він мовою програмування Java. Для використання буде потрібна безкоштовна реєстрація на сайті виробника, після чого можна переходити до створення цифрових відбитків вибраної мети в мережі. Чи неправда круто?

ПЕРЕВАГИ РОБОТИ

Незважаючи на те, що існують сотні веб-ресурсів для пошуку даних про конкретних людей або юридичних фірм, користувачі ще не знають, як отримувати ексклюзив.

Так, застосовуючи розширені пошукові запити в системах Googl Doks, Бінг, Яндекс та DuckDuckGo, користувач може отримати дивовижні, а часом і лякаючі результати.

А ще є спеціальні сайти, які призначені для пошуку людей за деякими наданими даними. Тільки уявіть, що існують ресурси, які здійснюють пошук відразу по всьому інтернету та на базі одного критерію! Достатньо ввести адресу електронної пошти або завантажити фотографію, а може вказати IP – і вуаля, ваш об'єкт знайдено всього за один клік. В одному місці ви отримаєте структуровану та впорядковану інформацію з численних ресурсів у мережі. Перевіряйте конкретну особу чи цілу корпорацію всього за годину серфінгу в інтернеті. Це дозволить мінімізувати ризики недобросовісного партнерства чи шахрайства у рази.

Ще однією перевагою є унікальність самої системи OSINT. Тут немає шаблонних алгоритмів щодо вашого розслідування, оскільки всі випадки унікальні, тому вимагають індивідуального підходу. OSINT представлений рядом платформ, які дозволяють проводити комплекс дій за пару кліків: пошук та збирання даних, аналітика, дослідження динаміки змін, порівняння результатів за тимчасовий період тощо. Завдяки технології будь-який користувач може зібрати ексклюзивні дані, які добровільно вам ніхто не надасть: це вивчення сторінок, на які підписана шукана особа, і всі його «лайки», коментарі під публікаціями, коло спілкування та соціальні зв'язки. Ви можете перевірити людину на зв'язок та взаємодію з різними людьми, у тому числі блогерами, політиками, чиновниками, медійними персонами, громадськими організаціями, фондами. Такі можливості дозволяють оцінити рівень ризику взаємодії з тією чи іншою фігурою при особистому спілкуванні чи здійсненні серйозної угоди. Також вони допомагають вибрати оптимальну переговорну стратегію з урахуванням переваг, про які дуже легко дізнатися після моніторингу активності майбутнього партнера на форумах та соціальних мережах.

OSINT просто необхідний для великих фірм та організацій, які хочуть працювати найбільш продуктивно, прибутково та з мінімальними ризиками витоку цінної комерційної інформації.

ЩО ПОТРІБНО ДЛЯ РОБОТИ OSINT У СУЧАСНИХ РЕАЛІЯХ

Алгоритм роботи у системі дуже простий і передбачає дотримання послідовності кроків. Остання була розроблена та протестована на ефективність протягом багатьох років:

- зберіть усю вихідну інформацію про мету, яка є у відкритому доступі (особисті дані, адреси пошти, фотографії, контакти тощо);
- позначте собі завдання: які питання необхідно вирішити, якої інформації не вистачає на формування цілісної картинки;
- визначтеся із інструментами OSINT, які ефективно працюють саме з вашими завданнями;
- налаштуйте пошук, а потім проаналізуйте всі зібрані дані;
- запустіть повторний пошук на основі нової отриманої інформації;
- підтвердіть або спростуйте свої припущення.

Можемо зробити висновок, що OSINT – це технологія нашого сьогодення та майбутнього. Ті, хто розібралися з її інструментами та принципами роботи, завжди будуть на крок попереду в конкурентній боротьбі та питаннях особистої безпеки.

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

ФОРМИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МИТНИХ ОРГАНАХ

Митні органи мають певну специфіку формування інформаційних ресурсів виключно за рахунок документів і відомостей, які з одного боку надаються учасниками зовнішньоекономічної діяльності відповідно до встановлених правил під час здійснення митних операцій, а з іншого боку - за рахунок документів, необхідних для здійснення таких операцій. У силу унікальності та особливої значущості щодо такого роду інформаційних ресурсів, не призначених для широкого розповсюдження та у зв'язку з цим підлягають правової охорони від несанкціонованого доступу, встановлюються специфічні адміністративно-правові режими, зміст яких насамперед зводиться до режиму доступу.

Адміністративно-правовий режим інформаційної безпеки визначається нормами, що встановлюють: право власності на інформаційні ресурси; порядок документування інформації; категорію відомостей щодо права на доступ до них; порядок правової охорони та захисту інформації. Зазначені норми було сформульовано ще у законі «Про захист інформації в інформаційно-комунікаційних системах» [1].

Вибір методів протидії загрозам інформаційної безпеки є проблемою та частиною діяльності, орієнтованої на реалізацію ключових напрямів політики держави у цій галузі. Адміністративно-правові форми публічного адміністрування представляють зовні виражені дії виконавчого органу, здійснені у межах компетенції та викликають певні наслідки юридичного характеру чи мають певне юридичне значення.

Формами публічного адміністрування органу виконавчої влади, уповноваженого в галузі митної справи у сфері інформаційної безпеки будуть аналогічні дії, але спрямовані на досягнення встановлених цілей, вирішення повного спектра поставлених завдань, виконання функцій та реалізацію повноважень, які на законній підставі мають суб'єкти правовідносин у галузі забезпечення інформаційної безпеки митних органів

Важлива особливість митних органів у тому, різні рівні управління у системі Державної митної служби України одночасно виступають як суб'єкти управління, а й як об'єкти. Управління у митних органах носить багаторівневий характер [2]. Кожному рівню управління відповідає суб'єкт та об'єкт управління. Якщо дії суб'єкта, створені задля забезпечення інформаційної безпеки, носять управлінський характер щодо інших суб'єктів правовідносин, вони мають зовнішній прояв. Якщо суб'єкт вживає певні дії, спрямовані на вирішення внутрішніх організаційних завдань, то ці дії становлять внутрішню форму.

Серед форм управлінської діяльності митних органів вирізняються: нормотворчість; правозастосовна та правоохоронна діяльність; діяльність, пов'язана із здійсненням організаційно-штатних заходів; діяльність, спрямована на реалізацію організаційно-технічних заходів; здійснення матеріально-технічного, фінансового, інформаційного забезпечення.

Методи, що використовуються в державних інформаційних системах для забезпечення інформаційної безпеки: запобігання витоку інформації по технічних каналах, що виникає під час експлуатації технічних засобів обробки, зберігання та передачі; забезпечення інформаційної безпеки у разі підключення автоматизованих інформаційних систем митних органів до зовнішніх інформаційних систем і комунікаційних мереж, включаючи інформаційні системи митних адміністрацій іноземних держав; виявлення впроваджених на об'єктах технічні засоби перехоплення інформації; проведення атестації об'єктів інформатизації щодо вимог забезпечення безпеки інформації при роботах, пов'язаних з використанням відомостей, що становлять державну таємницю.

Методи забезпечення інформаційної безпеки митних органів у сфері економіки: заходи щодо організації та здійснення контролю за створенням, розвитком та захистом систем, засобів збору, обробки, зберігання та передачі статистичної інформації, інформації обмеженого доступу, що обробляється в митних органах; використання процедур сертифікації засобів захисту у системах та

засобів збору, обробки, зберігання та передачі статистичної інформації, інформації обмеженого доступу, оброблюваної у митних органах.

Методи забезпечення інформаційної безпеки митних органів у сфері зовнішньої та внутрішньої політики: розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інфраструктури представництв ДМС України при митних службах іноземних держав і міжнародних організаціях; розробка дієвих організаційно-правових механізмів доступу засобів масової інформації та громадян до відкритої інформації про діяльність митних органів.

Методи забезпечення інформаційної безпеки митних органів у правоохоронній та судовій сферах, до яких можна віднести: створення захищеної багаторівневої системи інтегрованих баз даних довідкового, криміналістичного та статистичного характеру на базі спеціалізованих інформаційно-комунікаційних систем; підвищення рівня професійної та спеціальної підготовки користувачів автоматизованих інформаційних систем.

Використані адміністративно-правові методи та процедури забезпечення інформаційної безпеки митних органів, виражені у певні форми, спрямовані на реалізацію заходів з метою вирішення конкретних завдань з нейтралізації загроз інформаційної безпеки, що виникають.

Система забезпечення інформаційної безпеки митних органів – це сукупність сил і засобів забезпечення інформаційної безпеки, яка також включає механізм юридичної відповідальності посадових осіб та працівників митних органів, інших учасників правових відносин. Забезпечення інформаційної безпеки – це одного з актуальних напрямів розвитку митної служби.

Література:

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94. URL: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80
2. Про затвердження положень про Державну податкову службу України та Державну митну службу України: Постанова Кабінету Міністрів України від 06.03.2019 р. № 227. URL: https://zakon.rada.gov.ua/laws/show/227-2019-%D0%BF#Text

Жуковський І. В,
аспірант кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ МІГРАЦІЙНОЇ ПОЛІЦІЇ У ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ З ТОРГІВЛЕЮ ЛЮДЬМИ

Інформаційні технології суттєво змінюють спосіб життя людини та проникають у кожну сферу життя суспільства. Кількість доступних джерел інформації має неабияке значення і важливість мережі інтернет ніхто не в змозі заперечити. Тому в останні десятиліття широкого розповсюдження набула діяльність з добування інформації з відкритих і закритих інформаційних систем, баз і банків даних, контролю за повідомленнями, які передаються в комп'ютерних мережах, отримання персональних даних користувачів автоматизованих інформаційних систем та іншої цінної комп'ютерної інформації.

Відтак була створена організаційна структура управління інформаційно-аналітичною роботою в оперативних підрозділах Національної поліції, яка займається збиранням, оцінкою, аналізом, узагальненням даних, необхідних для протидії злочинам та прийняття оперативних рішень, у тому числі і в протидії торгівлі людьми [1].

Одним із суб'єктів протидії торгівлі людьми є Департамент міграційної поліції, основними завданнями якого, згідно Положення про Департамент міграційної поліції Національної поліції України, затвердженого наказом Національної поліції України від 22.01.2021 № 52, є:

- участь у реалізації державної політики у сфері протидії торгівлі людьми та нелегальній (незаконній) міграції, виявлення осіб, які постраждали від торгівлі людьми, зокрема серед іноземців, та надання в межах, визначених законом, послуг з допомоги та захисту;

- попередження, виявлення та припинення правопорушень у сфері торгівлі людьми, міграції та суспільної моралі, зокрема вчинених учасниками та членами організованих груп і злочинних організацій, розшук осіб, які вчинили такі правопорушення [2].

Департамент міграційної поліції відповідно до покладених на нього завдань здійснює, зокрема: запобігання кримінальним правопорушенням, пов'язаним з торгівлею людьми, зокрема щодо сексуальної експлуатації дітей; запобігання кримінальним правопорушенням, пов'язаним з учиненням незаконних дій щодо усиновлення (удочеріння); запобігання порушенням встановленого законом порядку трансплантації анатомічних матеріалів людини та застосування допоміжних репродуктивних технологій; попередження, виявлення та припинення кримінальних правопорушень у частині насильницького донорства; протидію кримінальним правопорушенням щодо створення та утримання місць розпусти і звідництва, а також у частині сутенерства та втягнення особи в заняття проституцією; запобігання кримінальним правопорушенням, пов'язаним з увезенням, виготовленням, збутом і розповсюдженням порнографічних предметів; попередження, виявлення та припинення кримінальних правопорушень щодо незаконного переправлення осіб через державний кордон України; виявлення кримінальних правопорушень щодо підроблення документів, печаток, штампів та бланків у сфері міграції, а також їх використання для отримання в Україні правового статусу іноземця; протидію кримінальним правопорушенням у частині службової діяльності та професійної діяльності у сфері міграції; попередження, виявлення та припинення кримінальних правопорушень, пов'язаних з порушенням установленого законом порядку працевлаштування за кордоном; оперативно-розшукову діяльність; взаємодію з іншими структурними підрозділами центрального органу управління поліції, територіальними (зокрема міжрегіональними) органами Національної поліції України, органами державної влади, громадськими організаціями, а також з правоохоронними органами зарубіжних країн, міжнародними організаціями і засобами масової інформації у вирішенні питань протидії злочинності; координацію підрозділів міграційної поліції територіальних органів Національної поліції України; виконання в межах компетенції та відповідно до законодавства України письмових доручень слідчого (дізнавача), вказівок прокурора, ухвал слідчого судді, суду, а також запитів уповноважених органів державної влади, установ та організацій, правоохоронних органів іноземних держав або міжнародних організацій, членом яких є Україна, у частині проведення оперативно-розшукових заходів [3];

Важливе значення у діяльності підрозділів міграційної поліції посідає інформаційно-аналітичне забезпечення її діяльності. Зокрема, підрозділи міграційної поліції беруть участь у наповненні автоматизованих інформаційних систем оперативно-розшукового і профілактичного призначення, забезпеченні своєчасного наповнення та належного використання оперативно-розшукових обліків. Надзвичайно важливим є вивчення передового досвіду правоохоронних органів іноземних держав у сфері протидії торгівлі людьми та нелегальній (незаконній) міграції, боротьби зі злочинністю, а також підготовці інформаційно-аналітичних методичних матеріалів щодо стану та підвищення ефективності протидії правопорушенням у відповідних сферах тощо [3].

Одним із прикладів такої співпраці є впровадження системи кримінального аналізу та аналізу ризиків, сумісних з стандартами ЄС, в оперативно-службову діяльність Департаменту міграційної поліції за сприяння Міжнародної організації з міграції та фінансування Державного департаменту США. Також міграційна поліція України, Європол та громадські організації визначили алгоритми протидії торгівлі людьми щодо українців, які виїхали за кордон задля збереження своїх сімей від загарбницької війни, яка розпочалась 24 лютого 2022 року після віроломного вторгнення росії на територію України.

Водночас є ряд проблем у системі інформаційно-аналітичного забезпечення, програмах для доступу до баз даних та можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних, що позначаються на якості управління.

Кінцевою метою інформаційно-аналітичного забезпечення міграційної поліції є підготовка й обґрунтування прийняття рішень на різних рівнях управлінської структури. При цьому управлінські рішення можуть стосуватися будь-яких видів діяльності Департаменту міграційної поліції України та оперативних підрозділів Національної поліції, зокрема корупції, нелегального перетину кордонів та торгівлі людьми. Кожний з них є надзвичайно складним, супроводжується прийняттям відповідальних рішень і проведенням заходів та операцій, що торкаються прав і інтересів громадян. За нашим переконанням, інформаційно-аналітичне забезпечення Департаменту міграційної поліції України у протидії злочинам, пов'язаним з торгівлею людьми, являє собою комплекс заходів, спрямованих на

пошук, збирання, оброблення, класифікацію та аналіз оперативно-розшукової інформації стосовно фактів торгівлі людьми та осіб, що до неї причетні, її фіксацію, накопичення, збереження, опрацювання, аналіз і використання первинних і вихідних даних з метою виконання оперативними підрозділами покладених на них функцій з протидії торгівлі людьми [3].

Література:

1. Про утворення в структурі кримінальної поліції Департаменту міграційної поліції України: наказ Національної поліції України від 07 грудня 2020 року № 946.
2. Про затвердження Положення про Департамент міграційної поліції Національної поліції України: наказ Національної поліції України від 22 січня 2021р. № 52.
3. Мовчан А. В. Міжнародне співробітництво у сфері протидії злочинам, пов'язаним із торгівлею людьми: навч. посіб. Львів : ЛьвДУВС, 2021. 156 с.

Зачек О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Дмитрик Ю. І.,
доцент кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРОБЛЕМА ЗАСТОСУВАННЯ ПРОФАЙЛІНГУ В ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ

З кожним роком все більшої актуальності набуває боротьба з кіберзлочинністю, оскільки спостерігається значне зростання кількості кіберзлочинів. Згідно з повідомленням прес-служби платформи відкритих даних Opendatabot з 2014 по 2019 рік кількість інформаційних злочинів в Україні зросла щонайменше у 2,5 рази [1]. За даними групи аналізу загроз Google у 2021 році зафіксовано на 68% більше викрадень даних ніж у 2020 році (понад 1800 випадків) і це найбільший показник за останні 15 років [2]. Для протидії таким злочинам підрозділи кіберполіції України повинні використовувати найсучасніші методи. Одним з таких методів є профайлінг, який є важливим інструментом розслідування злочинів, у тому числі й інформаційних. Він дозволяє класифікувати кіберзлочинців, зрозуміти їх звички та технічні навички, та має за мету виявлення злочинця.

Профайлінг дозволяє вирішити проблему недостатньої уваги, що приділяється психологічним аспектам діагностики та оцінювання особи злочинця у оперативно-розшуковій діяльності та підвищити ефективність професійної діяльності підрозділів кіберполіції Національної поліції України. Але в даний час профайлінг у діяльності цих підрозділів практично не використовується, хоча у провідних країнах світу використання профайлінгу під час розслідування кіберзлочинів є досить поширеним.

Профайлінг – це сукупність психологічних методів і методик оцінки та прогнозування поведінки особи на основі аналізу найбільш інформативних особистісних ознак, характеристик зовнішності, вербальної та невербальної поведінки [3, с. 132]. Слово «profiling» утворене від англійського «profile» («профіль») та означає «профілювання». Спочатку використовувався «авіаційний профайлінг», який передбачав опитування пасажирів та спостереження за ними для виявлення потенційно небезпечних осіб. Підготовку профайлерів для запобігання терористичним актам започаткували у Ізраїлі у 80-х роках XX століття. Завдяки використанню профайлінгу авіакомпанія Ель-Аль (EL-AL) отримала статус однієї з найбезпечніших у світі [3, с. 133].

В основі профайлінгу є досягнення біології, психології та психолінгвістики, він містить методи для визначення особистісних характеристик людини з метою прогнозування та оцінки її дій.

Профайлінг може використовуватись як для створення психологічного профілю невстановленого злочинця з метою встановлення його особи, так і з метою виявлення осіб, які можуть становити потенційну небезпеку. Основними напрямками застосування профайлінгу під час розкриття і розслідування злочинів є складання психолого-криміналістичного портрета злочинця (дозволяє здійснювати пошук невідомого злочинця і є основою тактики проведення оперативно-розшукових заходів), здійснення географічного профілювання (дозволяє виявити системність у скоєнні злочинів в

певних місцях, що дозволяє виявити місце перебування злочинця), здійснення оцінки правдивості показів особи.

Концепція профайлінгу базується на тому, що протиправна дія і її підготовка можуть бути виявлені шляхом аналізу певного набору фізичних, психологічних, поведінкових ознак, що становлять характеристику підозрюваних осіб, з позицій їх потенційної небезпеки. Існують індикатори, які є критичними для віднесення конкретної особи до групи ризику (демонстрована агресія, прихована агресія, збудженість, відчуженість). Емоційний стан людини, який оцінюється за ознаками тривоги, страху, хвилювання та інше, розглядається як додатковий фактор під час аналізу виявлених домінуючих ознак. Існують ключові ознаки у невербальній і вербальній поведінці людини, які дозволяють профайлерам виявити таку особу у людському середовищі і віднести до категорії потенційно небезпечних.

Значну перспективу застосування має профайлінг у сфері інформаційної безпеки, коли аналізуються загрози інформаційній безпеці та вивчається дотримання працівниками режиму політик інформаційної безпеки. Усунення цих загроз є завданням служб інформаційної безпеки, однією з методик яких є використання технологій аналізу поведінки, які на основі даних журналів інформаційних систем можуть будувати моделі поведінки користувачів і фіксувати відхилення від звичної поведінки, що дозволяє прогнозувати ризики. Автоматизований профайлінг формує профіль особи з повідомленням про ризики, аналізуючи вибірки з текстів робочого листування особи та визначаючи прояви психотипів на основі індивідуальних особливостей мови особи. Точність прогнозу ризиків такої системи значно підвищується, якщо ще враховувати міміку, інтонацію голосу, клавіатурний почерк.

Також важливу роль відіграє профайлінг під час розслідування кіберзлочинів. Профайлінг допомагає слідчому робити висновки щодо злочинця чи місця злочину. Звичайно, не всі методики класичного профайлінгу можна застосувати до кіберзлочинів, але на думку американського слідчого та фахівця з кібербезпеки Рея Йепеса, основна методологія «чому+як=хто» може бути використана під час профілювання кіберзлочинів [4]. Визначення причини та способу скоєння злочину сприяє викриттю особи злочинця. Слідчі та оперативні працівники можуть розробляти профілі підозрюваних на основі аналізу деталей кіберзлочинів. Для цього вони повинні бути не лише фахівцями з профайлінгу, але і фахівцями з інформаційних технологій, кібербезпеки та цифрової криміналістики. Завдання працівника кіберполіції полягають у виявленні списку підозрюваних, у вивченні атаки з технологічної сторони, виявленні рівня майстерності хакера, у дослідженні жертви та мети нападу. Вивчення цих питань дозволяє звузити список підозрюваних [4].

Як вважає Деб Шіндер, у процесі профайлінгу більшість кіберзлочинців можуть бути описані наступними характеристиками:

- певний рівень технічних знань;
- нехтування законом;
- потреба у ризику;
- насолода від маніпулювання іншими;
- мотив злочину – гроші, емоції, політичні чи релігійні переконання, сексуальне задоволення та бажання розважитися [5].

На думку Наташі Гарсіа з Utica College в Utica, New York, розуміючи профіль кіберзлочинців, слідчі можуть розвивати свої стратегії боротьби з кіберзлочинністю та зменшувати кількість кіберзлочинів [6].

Зокрема, профайлінг може допомогти у прив'язці кіберзлочинів на різних об'єктах до однієї хакерської групи, оскільки злочинці під час скоєння злочину залишають кіберслід, характерний саме для них. Один злочинець може використовувати вірус, який розповсюджується через електронну пошту і знищує дані, а інший здійснює злам через комп'ютерну мережу. Шляхом аналізу кіберслідів можна визначити технічні навички злочинця, що допоможе визначити усталений спосіб вчинення злочинів злочинцем. Також профайлінг дозволяє визначити мотив злочину (наприклад, гроші, емоції, сексуальні мотиви, бажання розважитись, релігія, політика).

Під час розслідування комп'ютерних злочинів здійснюється системний аналіз та мережевий аналіз. Системний аналіз – це аналіз файлової системи комп'ютера злочинця чи жертви, який дозволяє виявити змінені файли та їх вміст, а також це перевірка записів у файлах журналу. Мережевий аналіз включає дослідження файлів журналів, що містять вхідний та вихідний

мережевий трафік. Під час тривалої мережевої атаки можна за допомогою маршрутизатора чи шлюзу здійснити реєстрацію мережевого трафіку, необхідного для аналізу. Результати аналізу можуть бути використані для створення профілю злочинця. Експерти досліджують підписи, файли журналів, Інтернет-кеш, файли зображень, метадані файлів, сайти соціальних мереж, бо як і звичайні злочинці, кіберзлочинці залишають сліди, які можуть бути використані для їх профілювання та викриття. Особливо важливими є файли системних журналів, бо вони показують, що сталося та коли, і можуть бути використані як докази, а також допомагають зібрати інформацію для початку створення профілю. Метою профілювання є виявлення та спроба зрозуміти злочинця, який причетний до злочину [6].

Дуже важливим є правове регулювання використання профайлінгу у діяльності підрозділів кіберполіції Національної поліції України.

Діяльність Департаменту кіберполіції Національної поліції України регулюється Положенням про Департамент кіберполіції Національної поліції України [7]. Також Департамент кіберполіції Національної поліції України керується нормами Закону України «Про Національну поліцію» [8], нормами Закону України «Про ратифікацію Конвенції про кіберзлочинність» [9] та нормами Закону України «Про основні засади забезпечення кібербезпеки України» [10]. Згідно з визначенням, яке дається на офіційному сайті кіберполіції України: «Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність» [11]. Тому він також керується Законом України «Про оперативно-розшукову діяльність» [12].

У жодному з цих нормативно-правових документів не передбачено використання профайлінгу в діяльності кіберполіції. Тому подальші розробки в галузі правового регулювання застосування профайлінгу підрозділами кіберполіції Національної поліції України є дуже важливими.

Висновки. Відсутність досвіду використання профайлінгу в діяльності оперативних підрозділів Національної поліції України, зокрема підрозділів кіберполіції, недооцінка його можливостей вимагає в даний час переосмислення. Технології профайлінгу можуть бути успішно впроваджені у діяльність оперативних підрозділів Національної поліції, в тому числі підрозділів кіберполіції, що дасть можливість більш ефективно протидіяти злочинності. З цією метою, доцільно до існуючих пошукових заходів додати на законодавчому рівні такий захід як «оперативний профайлінг», що дасть змогу широко застосовувати його можливості. Також важливо здійснювати навчання працівників кіберполіції основам профайлінгу, для чого необхідно запровадити відповідну навчальну дисципліну в освітній процес закладів вищої освіти.

Література:

1. Кількість кіберзлочинів в Україні зросла вдвічі за останні п’ять років – Opendatabot. [Електронний ресурс]. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення: 30.11.2022).
2. Данило Бєлов. Цілі хакерів: топ-5 вразливостей бізнесу // Українська правда від 03.11.2022. [Електронний ресурс]. URL: https://www.epravda.com.ua/columns/2022/11/3/693426/ (дата звернення: 30.11.2022).
3. Дручек О.В. Профайлінг як метод забезпечення державної безпеки і громадського порядку: проблеми застосування. Наук. вісн. публічного та приватного права. Київ, 2018.С.132-136.
4. Ray Yepes, “The Art of Profiling in a Digital World,” // The Police Chief 83 (February 2016). [Електронний ресурс]. URL: https://www.policechiefmagazine.org/the-art-of-profiling-in-a-digital-world/ (дата звернення: 30.11.2022).
5. Deb Shinder, Profiling and categorizing cybercriminals // Tech & Work on July 19, 2010 [Електронний ресурс]. URL: https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/ (дата звернення: 30.11.2022).
6. Natasha Garcia, The use of criminal profiling in cybercrime investigations. / Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity. [Електронний ресурс].

URL:https://www.researchgate.net/publication/327187114_The_use_of_criminal_profiling_in_cybercrime_investigations (дата звернення: 30.11.2022).
7. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85// Єдиний загальнодержавний публічний ресурс законодавчих та нормативно-правових актів, які стосуються діяльності поліцейських [Електронний ресурс]. URL: http://tranzit.ltd.ua/nakaz/ (дата звернення: 30.11.2022).
8. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.
9. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. 2006 р., № 5, / 5-6 /, с. 128, Ст. 71.
10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017 р., № 45, с. 42, Ст. 403.
11. Офіційний сайт кіберполіції України. [Електронний ресурс]. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 30.11.2022).
12. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII // Відомості Верховної Ради України. 1992. №22. Ст. 303.

Івкова В. С.,
старший інспектор 1-го сектору (рекрутингу та оперативного пошуку) Управління протидії кіберзлочинам у Львівській області Департаменту кіберполіції Національної поліції України

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ АТАКИ ЯК ЗАГРОЗА ДЕРЖАВНІЙ БЕЗПЕЦІ

В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Як зазначено у Законі України "Про основи національної безпеки" однією з основних загроз інформаційній безпеці є "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації".

У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками.

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави.

Проблема гарантування інформаційної безпеки України актуалізується в умовах війни, коли з боку російської федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість.

Вказані діяння зі сторони країни-агресора можна трактувати, як прояв кібертериторизма.

Законом України «Про основні засади забезпечення кібербезпеки України» № 2163-19 від 05.10.2017 року було закріплено поняття кібертероризму в національному законодавстві України.

Таким чином, відповідно до даного закону під дефініцією «кібертероризм» необхідно розуміти наступне: терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Чинним національним законодавством деяких європейських країн вже досить давно передбачено кримінальну відповідальність за вчинення актів кібертероризму або інформаційного тероризму [1].

Зокрема, Закон про тероризм 2000 р. (Terrorism Act 2000) Великої Британії вперше розширив визначення тероризму на діяння, вчинені у кіберпросторі, а стаття 324-1 КК Грузії також передбачає відповідальність за кібертероризм, який визначено як протиправне заволодіння охоронюваної законом комп'ютерною інформацією, її використання або загроза використанням, що створює небезпеку настання тяжких наслідків, вчинене з метою залякування населення або (і) впливу на орган влади.

Відповідно до чинного КК України, знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації з метою ослаблення держави шляхом несанкціонованого втручання, яке спричинило істотну шкоду, є диверсією, повністю охоплюється складом, передбаченим ст. 113 КК України «Диверсія». Додаткова кваліфікація за ч. 2 ст. 361 КК не потрібна, оскільки втручання в електронну систему є складовою частиною об'єктивної сторони іншого, більш тяжкого злочину (диверсії), в той час як кримінальної відповідальності, за вчинення інформаційно-психологічних атак на населення не передбачено.

Такий же підхід до кваліфікації можливий і щодо актів кібертероризму, однак, на нашу думку, теперішнє визначення тероризму не повною мірою враховує специфіку та суспільну небезпечність вчинення кібертероризму, тому слід замислитися щодо передбачення окремої відповідальності за цей злочин.

Можна виділити такі основні ознаки вищевказаної протиправної діяльності:

- реалізується через загальнодоступні ресурси масової інформації та за допомогою глобальної мережі Інтернет (насамперед, профільних спільнот в соціальних мережах);
- є однією з форм проявів терору або організованого насильства;
- є особливим різновидом психологічного терору;
- має публічний і демонстративний характер дій тощо.

Масове та досить швидке поширення кібертероризму обумовлене широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства.

Об'єкти кібертероризму аналогічні об'єктам кіберзлочинності. Серед них можна виділити: устаткування; програмне забезпечення; мережеві стандарти і коди передачі даних; інформацію, яка може бути представлена у вигляді баз даних, аудіо-, відеозаписів, архівів тощо; фізичні особи.

З метою протидії інформаційно-психологічним атакам, які реалізується через загальнодоступні ресурси масової інформації та за допомогою глобальної мережі Інтернет (насамперед, профільних спільнот в соціальних мережах) працівниками Департаменту кіберполіції було реалізовано проект «MRIYA», який налічує в собі три окремі проекти - **Бот «StopRussia | MRIYA»** https://t.me/stopdrugsbot, **канал «StopRussia | MRIYA»** https://t.me/stoprussiachannel та **Сервіс «MRIYA Automatic».**

Зокрема, Бот «StopRussia | MRIYA» https://t.me/stopdrugsbot – приймає інформацію про фейкові ресурси, котрі перевіряються нашими модераторами та відправляються на блокування в Телеграм-канал. У розділі «Надіслати скаргу на ресурс» – кожен може долучитися до блокування ресурсів окупанта. Вам буде надано випадкове посилання, а також текст скарги, які постійно змінюються.

Канал «StopRussia | MRIYA» https://t.me/stoprussiachannel – це спільнота небайдужих українців, котрі блокують та протидіють російській агресії в Інтернеті. Канал – це головна інструкція та засіб комунікації з підписниками щодо блокування, а також платформа, де щоденно та систематично надаються онлайн-завдання для підписників, актуальні новини та свіжа інформація, у тому числі навчальні матеріали по кібергігієні.

Сервіс «MRIYA Automatic» – безкоштовний автоматизований сервіс для боротьби з російською пропагандою, який працює в хмарі, не використовує ваш браузер, і не вимагає від вас включеного та активного браузера комп'ютера чи смартфону.

Так наприклад станом на 09.12.2022 року на каналі https://t.me/stoprussiachannel приймає участь майже 305 тис. людей, які надіслали з початку війни більше 6,3 млн скарг та заблокували (обмежили доступ) до більше 20 тисяч ворожих ресурсів, загальна аудиторія яких була близько 230 млн підписників. Крім цього, було отримано інформацію (виявлено) більше 77 тисяч ворожих ресурсів, з них перевірено та відправлено на блокування 38 тисяч.

Аналізуючи стан забезпечення інформаційної безпеки, вбачаємо необхідність удосконалення системи законодавчого регулювання інформаційної безпеки. Одночасно з цим, постає потреба у кримінально-правовому закріпленні такого діяння як кібертероризм, виробленні нових засобів забезпечення інформаційної безпеки державного управління та введення постійного моніторингу інформаційного середовища на предмет наявності нових загроз та небезпек.

Підсумовуючи вищевикладене, необхідно зазначити, що в умовах глибокого латентного проникнення злочинності до глобальної мережі Інтернет, яка в свою чергу посідає провідне місце в регулюванні суспільного та державного життя, подолання такої злочинної активності стає нагальною потребою на шляху розбудови інформаційного суспільства і входження України у світовий інформаційний простір.

Калітовський Н. О.,
здобувач вищої освіти факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

Огірко О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЦИФРОВІ ТЕХНОЛОГІЙ ПІД ПРОВЕДЕННЯ ОНЛАЙН НАВЧАННЯ ДЛЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Реалії сьогодення вимагають змін у системі навчання здобувачів закладів вищої освіти, оскільки якісне і доступне викладання матеріалу неможливе без застосування можливостей, які надають цифрові технології. Сучасні комп'ютерні та інформаційні технології дають альтернативний спосіб навчання, додаткову можливість використання чогось нового в навчанні, підвищення інтересу до навчання у молоді.

До основних цифрових технологій, які використовують в освітньому процесі для проведення онлайн занять можна віднести:

Платформа для навчання Moodle, яка надає розвинутий набір інструментів для комп'ютеризованого навчання, зокрема й дистанційного. Велику популярність має в Європі та США □1, 2□. В Україні використовується переважно в закладах вищої освіти. На платформі кожен викладач розробляє електронний курс під особливості свого предмету, додає текстові фрагменти з можливістю тестування після прочитання, наповнює відеофайлами, гіперпосиланнями на додаткові джерела інформації, презентаціями. Є можливість створювати тести різних видів і форматів.

Відеоплатформи для проведення конференцій та вебінарів. За допомогою них можна проводити навчання, демонструючи при цьому зображення екрану доповідача, передавати відео і звук, бачити список присутніх.

Найпопулярнішою платформою для проведення онлайн занять в Україні є Zoom. Платформа розроблена компанією Zoom Video Communications, підходить як для індивідуальних так і групових занять, дозволяє підключатися одночасно до 100 слухачів курсу, причому, підключатися можна з комп'ютера, телефона, планшета. Під час демонстрації екрану, в даній платформі Zoom, можна ввімкнути інструмент коментувати, що дає змогу малювати, коментувати демонстрований матеріал. До переваг можна віднести і розподіл слухачів на окремі зали - міні конференції, де вони спілкуються один з одним, а організатор має можливість переходити в різні зали, тим самим перевіряючи роботу слухачів □5□.

Також популярною і зручною в користуванні, особливо в Польщі, вважають Google Meet, сервіс відео телефонного зв'язку, розроблений компанією Google. Щоб користуватися платформою потрібно мати обліковий запис Google, а Zoom дозволяє підєднатися кожному, хто має посилання.

Хмарні технології. Концепція хмарних технологій в освіті полягає в розподіленій обробці даних, де додатки, комп'ютерні технології та потужності надаються користувачеві, як Інтернет-сервіс. Головною перевагою використання таких технологій є доступність інформації та засобів для її опрацювання за допомогою програмного забезпечення □3, 6□. Всіма налаштуваннями, розширенням інфраструктури, захистом від несанкціонованого доступу займається сервіс-провайдер.

Технологій віртуальної та доповненої реальності. Технологій доповненої реальності та віртуальної реальності здатні проектувати цифрову інформацію (зображення, відео, текст, графіку) поза

екранами пристроїв та об'єднувати віртуальні об'єкти з реальним середовищем. За допомогою таких технологій можна створити точну 3D-модель простору навколо певного об'єкта, оновлювати її в реальному часі, вимірювати відстані, вставляти інші об'єкти і взаємодіяти з ними □7□. До таких технологій доцільно віднести Go-Lab (Global Online Science Labs) – це система дослідницького навчання, яка складається з двох основних компонентів: колекції віртуальних лабораторій, застосунків на порталі Go-Lab та платформи для створення дослідницьких навчальних середовищ Graasp. Graasp.

Ці ресурси дозволяють робити експерименти, перевіряти гіпотези, робити дослідження з астрономії, біології, хімії, математики, фізики, електроніки, наприклад: «Побудувати атом», «Лабораторія сили тяжіння», «Графіки», «Закон Фарадея», «Побудувати дроби» та багато іншого. Застосування застосунків не тільки цікаве, а й підвищує інтерес до навчання, сприяє запам'ятовуванню інформації та отриманню нових знань.

Інтерактивне програмне забезпечення Mozaik education, яке складається з набору застосунків □4, 7□:

- mozaBook – електронні підручники, які, крім матеріалу друкованих видань, містять ігри, тематичні інструменти та інтерактивне наповнення. Вбудовані анімації, презентації та ілюстрації допомагають вчителю в роботі;
- mozaWeb – бібліотека тривимірних сцен, кілька сотень освітніх відео, картинок, аудіо, що дотичні до навчальних предметів, застосунків та ігор, доступні в режимі online у будь-якому місці. Дозволяють здійснити віртуальні прогулянки з динозаврами, побачити системи органів людського тіла, відвідати стародавні місця на нашій планеті й ще понад 1200 різноманітних 3D-сцен;
- mozaMap – цифрові інтерактивні атласи: різні типи мап, елементи яких можуть вільно замінюватися та складатися;
- mozaLog – цифровий журнал, інформаційна система, яка робить можливим виконання щоденних шкільних адміністративних та організаційних завдань на єдиному інтерфейсі;
- LabCamera – це програмне забезпечення, що призначене для вивчення природних наук і реєстрації даних. Дозволяє проводити наукові спостереження й вимірювання за допомогою комп'ютера та вебкамери.

Цифрові технологій Kahoot, LearningApps, GoogleClassroom, Google Earth, SolarSystem, Gios, The Brain AR App, Code.org, LegoEducation, Zoom, Skype та багато-багато інших програм, що урізноманітнюють навчальний процес, роблять його цікавим, насиченим, корисним, а головне – ефективним.

Переваги від впровадження сучасних цифрових технологій в освітній процес для проведення навчальних заходів в онлайн форматі показано на рис.1.

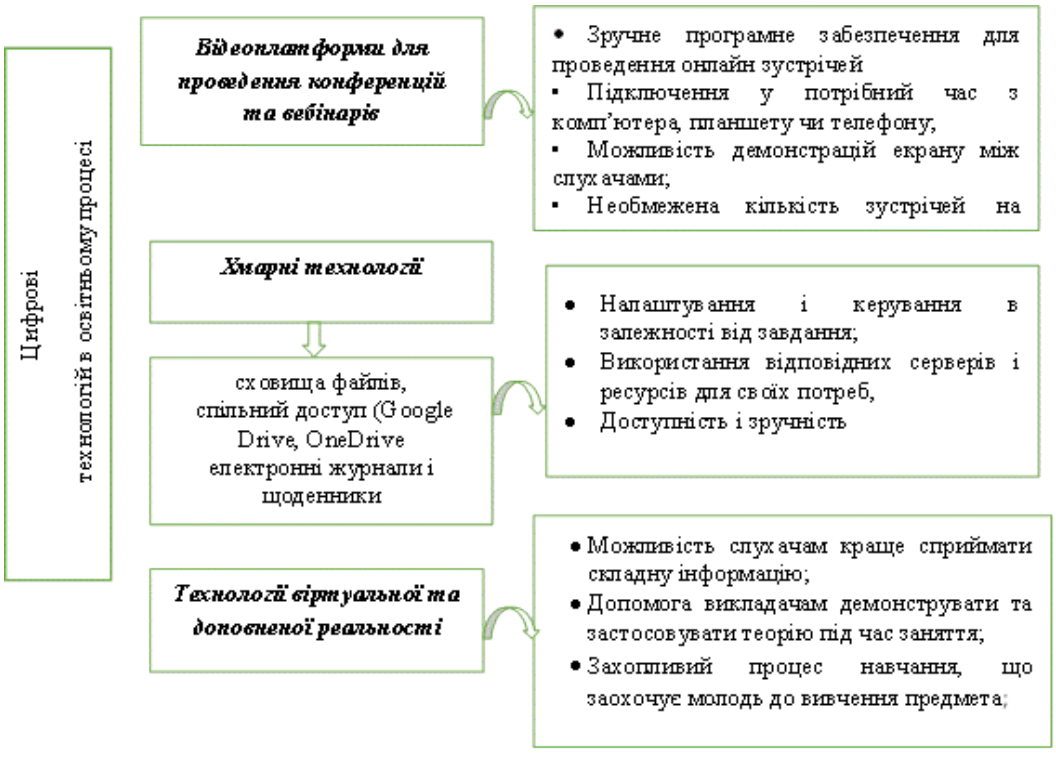


Рис.1. Цифрові технології в освітньому процесі

Завдяки цифровим технологіям освітній процес трансформується і набуває нових можливостей. Проведення навчальних занять в онлайн форматі стає новим способом отримання освіти з допомогою комп'ютерних та сучасних інформаційних технологій та надає можливість навчатися на відстані, що є дуже важливим у теперішній час.

Впроваджувати цифрових технологій, які використовуються для проведення онлайн занять, доцільно і при очному навчанні, це вдосконалить підготовку здобувачів вищої освіти України та дозволить покращити якість освіти. Проведений аналіз дозволяє стверджувати, що активне використання цифрових технологій у навчальний процес посилює взаємодію між викладачем і студентом та робить процес навчання більш цікавим і захоплюючим, тим саме заохочує студента до вивчення предмету.

Література:

1. Долинський Є. В. Дистанційне навчання- одна з прогресивних форм підготовки фахфвців. *Теоретичні питання культури, освіти та виховання:* збірник наукових праць. Вип.42. Київ. КНЛУ. 2020. С-202-207.
2. Сидорчук Л. А. Впровадження інформаційних технологій в навчальний процес вищих шкіл. *Проблеми педагогічних технологій*: Збірник наукових праць Луцьк: 2010. С.280-286.
3. Биков В. Ю. & Жалдак М. І. (2018). Хмарні технології в освіті. Матеріали Всеукраїнського науково-методичного Інтернет-семінару. Вилучено із https://www.twirpx.com/file/1909983.
4. 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.*
5. Магеровський Д. М. Особливості деяких платформ для проведення відеоконференцій та вебінарів *Інформаційні технології в освіті та практиці*: матеріали Всеукраїнської науково-практичної конференції. Львів: ЛьвДУВС, 2020. С.113–116.
6. Кулешник Я. Ф. Порівняльна характеристика хмарних сховищ. *Інформаційні технології в освіті та практиці*: матеріали Всеукраїнської науково-практичної конференції. Львів: ЛьвДУВС, 2020. С.116–118.
7. Огірко О. І. Використання вітруальних технології та технології доповненої реальності в освітньому процесі. *Інформаційні технології в освіті та практиці*: матеріали Всеукраїнської науково-практичної конференції. Львів: ЛьвДУВС, 2020. С. 36–38.

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

Шукалович Б. В,
здобувач вищої освіти Інституту права Львівського державного університету внутрішніх справ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Поява нових інформаційно-комунікаційних технологій набуває ряд специфічних характеристик, які важливо враховувати не тільки в загальнотеоретичному, але й у практичному плані, зокрема при виробленні та реалізації відповідної правової політики держави.

Хід правового розвитку регулювання та використання інформаційних технологій характеризується тим, що спочатку законодавець намагається усунути протиріччя, що випливають з безпосереднього переведення інформаційних відносин в юридичні принципи, і встановити гармонійну правову систему, а потім вплив і примусова сила подальшого розвитку інформаційних технологій деформують систему і втягують в нові протиріччя.

Досягнутий у визначений час баланс в системі правових норм, які регулюють інформаційні відносини, у тому числі у сфері інформаційної безпеки, не є абсолютними. Правові засоби завжди обмежені рівнем суспільного розвитку. Цілі, які визначаються законодавцем є ідеальними за суттю і не завжди узгоджуються з рівнем розвитку, впровадження та використання інформаційних технологій. Це призводить до невідповідності у відносинах поставлених цілей та обраних для їх досягнення засобів.

Активізація процесу законотворчості з питань регулювання правовідносин в інформаційній сфері значно ускладнена відсутністю стрункої системи регламентації правових відносин і стрімким розвитком цього сегмента законодавства. На думку О. Баранова, це можна спостерігати при прийнятті кожного нового законопроекту з окремим понятійним апаратом і використанням різноманіття існуючих дефініцій [1, с. 29-30].

Питанню розвитку інформаційного законодавства тільки за 2021 рік присвятили наукові дослідження І. Арістова, О. Баранов, В. Бєлєвцева, Д. Біленська, Н. Бортник, В. Брижко, С. Єсімов, В. Ліпкан та інші науковці. З огляду на те, як зазначає О. Баранов, інформаційні відносини є як самостійними і автономними, так і супутніми для переважної більшості інших суспільних відносин в різних сферах людської діяльності, широта інформаційних відносин у законодавстві призвела до пропозиції поділити їх на два блоки:

- питання, що регулюються безпосередньо сферою інформації, інформаційно-комунікаційних технологій і систем;
- питання, що в значній мірі становлять предмет регулювання інших сфер, але які мають значення для розвитку правового забезпечення сфери інформації, інформаційних технологій і інформаційної безпеки [2].

Дійсно, Закон України від 02 жовтня 1992 року № 2657-XII «Про інформацію», Закон України від 21 січня 1994 № 3855-XII «Про державну таємницю», Закон України від 22 травня 2005 року № 851-IV «Про електронні документи та електронний документообіг», Закон України від 01 червня 2010 року № 2297-VI «Про захист персональних даних», Закон України від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації», Закон України від 17 квітня 2014 року № 1227-VII «Про Суспільне телебачення і радіомовлення», Закон України від 17 лютого 2022 року № 2075-IX «Про хмарні послуги», Цивільний кодекс України і інші створюють різноманітні інформаційно-правові режими, які охоплюють правове регулювання інформаційної безпеки.

В одних випадках набір можливих засобів за своїм розвитком випереджає визначення орієнтирів, як це було при прийняття Закону України від 22 травня 2005 року № 852-IV «Про електронний цифровий підпис», тобто постановку цілей (втратив чинність). Це призводить до неповного або неоптимального використання наявного інструментального потенціалу, що потягнуло внесення змін і доповнень до вказаного нормативного акту.

В інших випадках, навпаки, визначення цілі не ґрунтується на обліку засобів, які є у наявності, що характерно для Закону України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах». Цей варіант є набагато більш поширеним, ніж перший, і проявляється в тих ситуаціях, коли законодавець ставить кілька, або навіть одну мету, яка не має реального механізму реалізації [3].

Інформаційне законодавство часто змінюється шляхом внесення у діючі нормативно-правові акти «інформаційно-комунікаційних або електронних» змін, наприклад, Закон України від 6 жовтня 2016 року № 1666-VIII «Про внесення змін до деяких законодавчих актів України щодо вдосконалення державної реєстрації прав на нерухоме майно та захисту прав власності» [4].

Все це не сприяє оформленню галузі інформаційного законодавства за типом, наприклад, цивільного. Існує та навіть зростає кількість чинників, що свідчать про необхідність регулювання, наприклад, Інтернету, розглядаючи питання інформаційної безпеки, доступу до інформації та її збереження і інші проблеми. Вирішення даної проблеми видається, зокрема, шляхом послідовного впровадження таких принципів, як правова визначеність, пропорційність на основі оптимального балансу нормативно-правового регулювання соціально-правових конфліктів між учасниками публічно-правових і приватноправових відносин у сфері використання інформаційних технологій, у тому числі щодо забезпечення інформаційної безпеки.

Як будь-яке негативне явище, недоліки у нормативно-правовому регулюванні інформаційної безпеки, породжує прагнення до усунення або хоча б мінімізації масштабів. Проте зробити це в силу об'єктивних причин складно. Справа в тому, що домінуючою причиною законодавчого дисбалансу в інформаційній безпеці у самому загальному плані можна назвати невідповідність в цілому системи нормативно-правових актів і норм які містяться в них, що склалася на певному історичному етапі, відповідному рівню та стану розвитку суспільних відносин.

З цієї точки зору недосконалість інформаційного законодавства явище багато в чому неминуче, оскільки суспільне життя, яке лежить в основі права і системи законодавства, несе цілий ряд суперечностей, а нормативно-правова матерія, що відображає її, намагається постати у вигляді несуперечливої системи. Не сприяють досягненню балансу інформаційного законодавства у сфері інформаційної безпеки процеси безперервної зміни суспільних відносин, що відбуваються у науково-технічній і соціально-економічній системі в процесі формування інформаційного суспільства.

У цьому контексті адаптація права до нових умов суспільних відносин має відбуватися комплексно, усіма галузями права на основі досліджень загальної теорії держави та права.

Удосконалення законодавства у сфері інформаційної безпеки може вестись на двох принципово різних рівнях: або шляхом переважання підзаконних нормативних актів над законами в конкретній сфері правового регулювання громадських відносин, що виступає важливим, водночас негативним у плані реалізації регулятивного потенціалу права, проявом, або в процесі законодавчої нормотворчості з адаптації національного законодавства до вимог Європейського Союзу.

Співвідношення законів і підзаконних нормативно-правових актів в інформаційному законодавстві не слід трактувати односторонньо – тільки і виключно як абсолютний пріоритет перших по відношенню до других. Це ґрунтується на визнанні безумовної значущості як законів, так і підзаконної нормотворчості, яка спрямована на вирішення більш приватних, але не менш насущних завдань. Підзаконні нормативно-правові акти в системі інформаційного права можуть і повинні доповнювати, конкретизувати, «наповнювати життям» закони.

Література:

1. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права. Інформація і право. 2016. № 2 (17). С. 15-31.
2. Єсімов С. С., Малашко О. Є. Нормативно-правове забезпечення інформаційної безпеки в Україні // Міжнародний науковий журнал "Інтернаука". 2020. №14. https://doi.org/10.25313/2520-2057-2020-14-6295
3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР / Відомості Верховної Ради України. 1994. № 31. Ст. 286.
4. Про внесення змін до деяких законодавчих актів України щодо вдосконалення державної реєстрації прав на нерухоме майно та захисту прав власності» Закон України від 06.10.2016 р. № 1666-VIII / Відомості Верховної Ради України. 2016. № 47. Ст. 800.

Ковбасюк О. М.,
здобувач вищої освіти кафедри програмного забезпечення Національного університету «Львівська політехніка»

Грицюк Ю. І.,
професор кафедри програмного забезпечення Національного університету «Львівська політехніка»

ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН МЕТОДАМИ МАШИННОГО НАВЧАННЯ

З розвитком Інтернет-технологій та мобільного зв'язку соціальні медіа-ресурси стають все більш масштабними та глибоко інтегрованими в наше повсякденне життя. Завдяки легкому доступу до них користувачі мають можливість отримувати найновішу інформацію та обмінюватися нею, а також висловлювати й поширювати свої думки. Шкода, але через відкритість соціальних мереж, через велику кількість користувачів і, як наслідок, джерел надходження інформації часто з'являються різні фейкові новини.

Під фейковими новинами розуміють інформацію, яка є неправдивою або такою, що вводить в оману людей, однак її подають як достовірну. Термін "фейкові новини" став часто траплятися в різних мережах під час президентських виборів у США 2016 року, після яких компанії Google, Twitter і Facebook вжили нагальних заходів для боротьби з ними. Однак, через експоненціальне зростання обсягу інформації на новинних онлайн-порталах і на сайтах соціальних мереж навіть непересічному користувачу розрізняти справжні та фейкові новини стало значно важче [7].

На сьогодні методи виявлення фейкових новин в основному поділяють на два типи – ручна перевірка фактів і автоматичні методи їх виявлення, які є альтернативою ручним методам, широко розповсюджених на практиці [21].

Після аналізу наявних досліджень [3, 8, 13, 18, 20] стосовно методів автоматичного виявлення фейкових новин не можливо однозначно стверджувати, що існує певний набір методів і алгоритмів, які найкраще підходять для вирішення розглянутої проблеми. Навпаки, більшість дослідників намагаються виробити свій підхід із застосуванням унікальної комбінації уже відомих практик, щоб якомога достовірніше вирішити дану проблему. Розглянемо їх дещо грунтовніше.

Shaina Raza і Chen Ding [17] розробили інноваційний фреймворк, у якому використали найсучасніші підходи з області машинного навчання. Цей фреймворк використовує вміст новин і соціальні контенти для вивчення корисного подання інформації, отриманої з різних медіа-ресурсів, а також для прогнозування ймовірності появи фейкових новин. Їхня модель побудована на архітектурі Transformer, яка значно полегшує процес машинного навчання на етапі репрезентації коефіцієнтів з даних фейкових новин і допомагає завчасно їх виявляти. У цій роботі автори також використовували додаткову інформацію (метадані) із вмісту новин і соціальних контекстів для підтримки адекватності розробленої моделі з метою дещо достовірнішої класифікації правдивої інформації.

L. Ying та інші [20, 21] розробили багаторівневу мультимодальну мережу перехресної уваги MMCN (англ. *Multi-level Multi-modal Cross-attention Network*), у якій намагалися проаналізувати якомога більше ознак, що можуть впливати на визначення правдивості публікацій. Запропонована ними нова мережа спільно перетворює багатомодальну інформацію та багаторівневу семантику дописів у єдину наскрізну структуру, щоб виявляти фейкові новини. Мультимодальна мережа розроблена для внесення відповідної інформації для кожної публікації, яка може використовувати зв'язки між словами речення та областями зображення для доповнення та просування одне одного з метою високоякісного мультимодального її подання. Окрім цього, багаторівнева семантика текстової інформації інтегрована з візуальним вмістом для генерування багаторівневих семантичних характеристик за допомогою багаторівневої мережі кодування, об'єднаних у одне ціле для формування всебічного її подання.

Гібридну модель для визначення фейкових новин було досліджено Indhumathi Gurunathan [3], в якій використано методи машинного навчання. З усіх відомих частин новин, що можуть слугувати для їхнього аналізу, було використано всі доступні, в т.ч. заголовки, основний вміст, пов'язані зображення, соціальні мережі користувачів, які поширюють фейкові новини, і упередженість джерел, щоб виявити оманливі публікації.

Окрім наведених вище складних комплексних підходів, для вирішення поставленого завдання застосовують звичайні алгоритми без додаткових надбудов чи змін [1]. Розглянемо деякі з цих популярних алгоритмів дещо детальніше, а саме:

- **Support Vector Machine** – алгоритм машинного навчання з вчителем [1, 18], який використовують для класифікації інформації, тренують на маркованих наборах даних. Дослідники використовували різні класифікатори машинного навчання, тому алгоритм дав їм найкращі результати у виявленні фейкових новин.
- **Naive Bayes** – алгоритм машинного навчання [1, 16], який використовують для встановлення класифікаційних завдань, щоб перевірити, чи є новина достовірною чи фейковою. Це ймовірнісний класифікатор, що використовує теорему Баєса для визначення ймовірності приналежності спостереження (елемента вибірки) до одного з класів при припущенні (наївному) незалежності змінних. Тобто, якщо на підставі значень змінних можна однозначно визначити, до якого класу належить спостереження, класифікатор Баєса повідомить ймовірність приналежності до цього класу.
- **Logistic Regression** – популярний алгоритм машинного навчання з вчителем [1, 13], який використовують для прогнозування категоріальної залежної змінної з набору незалежних

змінних. Очікуваний результат прогнозують за допомогою логістичної регресії, тобто він повинен мати категоріальне або дискретне значення. Це може бути "Так" або "Ні", 0 або 1, "True" або "False" тощо, але замість відображення точних значень, як-от 0 і 1, він пропонує значення ймовірностей надходження неправдивої інформації, що знаходяться між 0 і 1.

- **Random Forest** (випадковий ліс) – ансамблевий метод машинного навчання [1, 4] для класифікації, регресії та виконання інших завдань, який працює на підставі побудови численних дерев прийняття рішень під час тренування моделі й продукує моду для класів (класифікацій) або усереднений прогноз (регресію) побудованих дерев. Недоліком є схильність до перенавчання. Метод містить велику кількість окремих дерев рішень, які взаємодіють як ансамбль, тобто генерує прогноз класу для кожного дерева, і клас з найбільшою кількістю голосів стає прогнозом абстрактної моделі. Основним принципом алгоритму є спільні знання, які є простими та потужними. Модель випадкового лісу є особливо успішною, оскільки вона містить велику кількість некорельованих моделей (дерев), які взаємодіють між собою, щоб перевершити кожну з окремих складових моделей.
- **Convolutional Neural Network** – згорткові нейронні мережі (ЗНМ, CNN, ConvNet) в машинному навчанні [1, 6] – це клас глибинних штучних нейронних мереж прямого поширення, який успішно застосовують для аналізу візуальних зображень, є корисним для виявлення фейкових новин. Дослідники використовували рекурентну нейронну мережу, щоб класифікувати новини як правдиві чи фальшиві.
- **Neural Network** – один із видів алгоритмів машинного навчання [1, 8], який використовують для вирішення проблем класифікації новин. Сьогодні нейронні мережі використовують як альтернативу всім наявним алгоритмам для машинного перекладу, розпізнавання мови та музики, оброблення зображень, визначення об'єктів на фото та відео. Глибинне навчання (англ. Deep Learning) – метод машинного навчання, заснований, передусім, на нейронних мережах, хоча можна застосовувати й інші методи. У сучасній реальності практично в усьому, що стосується Deep Learning, використовують нейронні мережі.
- **K-Nearest Neighbor** – контрольований алгоритм машинного навчання [1, 10], який використовують для вирішення проблем класифікації фейкових новин. Він зберігає дані про всі випадки, щоб класифікувати новий випадок на підставі подібності. Дослідники використовували цей класифікатор для виявлення фейкових новин у соціальних мережах.
- **Decision Tree** (дерево рішень) – контрольований алгоритм машинного навчання [1, 12], який допомагає виявляти фейкові новини. Він високоефективний і має певну точність класифікації, практично однакову з іншими методами машинного навчання. Він поділяє набір даних на різні менші підмножини, оцінює всі можливі спліт-тести даних і вибирає той, який має найбільший приріст інформації. Дослідники використовували різні класифікатори машинного навчання, а одним із них є дерево рішень. Дерево прийняття рішень (також називають деревом класифікації або регресійним деревом) – засіб підтримки прийняття рішень, який використовують в машинному навчанні, аналізі даних і статистиці. Структура дерева є "листя" і "гілки". На ребрах ("гілках") дерева рішення записані ознаки, від яких залежить цільова функція, в "листках" записані значення цільової функції, а інших вузлах – ознаки, якими відрізняються випадки. Щоб класифікувати новий випадок, треба спуститись деревом до аркуша і видати відповідне значення.
- **XGBoost** [12] (англ. eXtreme Gradient Boosting, екстремальне градієнтне підсилювання) – програмна бібліотека з відкритим кодом, яка пропонує систему градієнтного підсилювання для таких мов, як C++, Java, Python, R, Julia, Perl та Scala. Вона працює під Linux, Windows та macOS. Згідно з опису її проекту, вона має на меті забезпечити "Масштабовану Портативну та Розподілену Бібліотеку Градієнтного Підсилювання (GBM, GBRT, GBDT)". Вона працює як на одній машині, так і підтримує системи розподіленого оброблення Apache Hadoop, Apache Spark та Apache Flink. Бібліотека нещодавно набула великої популярності та уваги як вибір алгоритму багатьох команд-переможниць змагань з машинного навчання.
- **SVM** (англ. *Support Vector Machine* – метод опорних векторів) – один із найбільш популярних методів машинного навчання, який застосовують для вирішення завдань класифікації та регресії. Основна ідея методу полягає у побудові гіперплощини, що оптимально розділяє

об'єкти вибірки. Алгоритм працює в припущенні, що чим більша відстань (зазор) між роздільною гіперплощиною і об'єктами розділених класів, тим менше буде середня помилка їх класифікації.

Z. Khanam et al. [11] виконав практичне дослідження, у якому порівняв ефективність роботи деяких алгоритмів на одному наборі даних (рис. 1). Схоже дослідження було опубліковано Dharmaraj R. Patil у роботі [15]. Результати аналізу алгоритмів з цієї роботи наведені у таблиці.

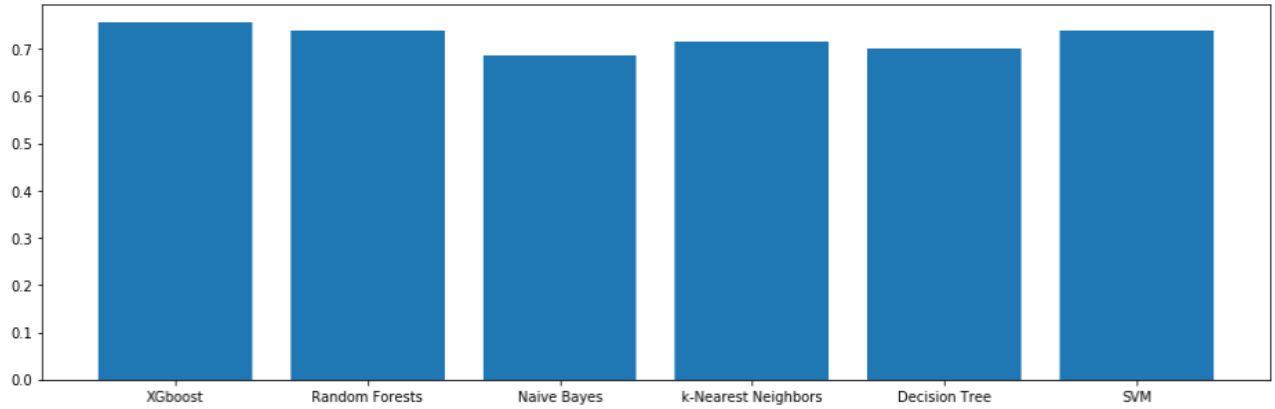


Рис. 1. Точність результатів усіх алгоритмів [11]

Таблиця. Оцінка ефективності методів на наборі даних Fake News [15]

Classifier	Accuracy, %	Precision, %	Recall, %	F1-score, %
Logistic Regression	94.89	95	95	95
Random Forest	91.60	92	92	92
SVM	96.49	97	96	96
Naive Bayes	84.62	88	85	84
Decision Tree	88.51	89	89	89

З наведених даних можна побачити, що найкращі результати класифікації новин на правдиві та фейкові дали XGboost та SVM класифікатори. З інших методів, що показали високу точність виявлення фейків, можна виділити алгоритми Random Forest та Logistics Regression. Усі решта алгоритми машинного навчання також дають можливість вирішувати дану проблему на відповідних наборах даних, але їх результати є дещо гіршими і самі методи потребують кращого підбору параметрів їхньої роботи й налаштування.

Незважаючи на прийнятні результати роботи стандартних алгоритмів, Sudhakar Murugesan [19], Rohit Kumar Kaliyar [9], Nishant Rai [14] у своїх дослідженнях довели, що одними з найкращих методів визначення фейкових новин є рішення, побудовані на BERT моделі для класифікації текстів. У роботах вони показали, що підхід із застосуванням BERT моделі дає кращі результати, ніж розглянуті Dharmaraj R. Patil [15] і Z Khanam et al. [11], стандартні алгоритми.

Нагадаємо, що BERT (англ. *Bidirectional Encoder Representations from Transformers*, двоспрямовані кодувальні подання з трансформерів) – методика машинного навчання, що ґрунтується на трансформері, призначена для попереднього тренування процедури оброблення природної мови (ОПМ), розроблена компанією Google. BERT було створено й опубліковано 2018 року Джейкобом Девліним та його колегами з компанією Google. Станом на 2019 рік Google застосовувала BERT, щоби краще розуміти пошуки користувачів.

Оригінальну англомовну модель BERT постачають у двох наперед натренованих варіантах: модель BERTBASE, нейромережна архітектура з 12 шарами, 768 прихованими, 12 головами, 110 мільйонами параметрів; модель BERTLARGE, нейромережна архітектура з 24 шарами, 1024 прихованими, 16 головами, 340 мільйонами параметрів; обидві треновано на BooksCorpus з 800 мільйонами слів, та одній з версій англійської Вікіпедії з 2 500 мільйонами слів.

Отже, BERT-модель є новою розробкою, яка і зараз перебуває у процесі розвитку та вдосконалення. У 2018 році компанія Google представила BERT з відкритим кодом. На етапах свого дослідження структура досягла революційних результатів у 11 завданнях на розуміння природної мови, в т.ч. аналіз настрою, маркування семантичних ролей, класифікацію речень та усунення неоднозначності багатозначних слів або слів з кількома значеннями [2].

Виконання цих завдань відрізняє BERT-модель від попередніх мовних моделей, таких як word2vec і GloVe, які обмежені в інтерпретації контексту та багатозначних слів. BERT ефективно усуває неоднозначність, яка є найбільшою проблемою для розуміння природної мови, про що стверджують дослідники в роботі [2].

Мета будь-якого методу оброблення природної мови – зрозуміти людську мову так, як вона зазвичай вимовляється. У випадку BERT, це означає передбачення слова в пустому місці. Для цього моделі, як правило, повинні навчатися, використовуючи велике сховище спеціально позначених навчальних даних [2, 5].

Однак, BERT-модель пройшла попередню підготовку, використовуючи тільки корпус звичайного тексту без міток (а саме, всю англійську Вікіпедію та Корпус Брауна). Вона продовжує навчатися без вчителя з тексту без міток і вдосконалюватися, навіть якщо її використовують у практичних програмах (наприклад, пошук Google). Її попередня підготовка слугує базовим рівнем "знань", яку можна пристосовувати під свої завдання. З цього моменту BERT-модель може адаптуватися до постійно зростаючої маси пошукового вмісту та запитів і бути налаштованою відповідно до специфікацій користувача. Цей процес відомий як трансферне навчання [2, 5].

Створення BERT-модель стало можливим завдяки дослідженням Google алгоритмів Transformers, позаяк є частиною моделі, яка надає BERT підвищену здатність розуміти контекст і неоднозначність мови. Transformer робить це, обробляючи будь-яке задане слово за відношенням до всіх інших слів у реченні, а не обробляючи їх по одному. Переглядаючи всі навколишні слова, Transformer дає змогу BERT- моделі зрозуміти повний контекст слова, а отже, краще зрозуміти наміри шукача [5]. Це контрастує з традиційним методом оброблення мови, відомим як вбудовування слів, у якому попередні моделі, такі як GloVe та word2vec, відображали кожне окреме слово у вектор, який представляє тільки один вимір, фрагмент, значення цього слова.

BERT також є початковою технікою оброблення природної мови, яка покладається виключно на механізм самоуважності (self-attention), що стало можливим завдяки двонаправленим Transformers у центрі дизайну BERT. Це вельми важливо, оскільки часто слово може змінювати значення в міру розвитку речення. Кожне додане слово доповнює загальне значення слова, на якому фокусується алгоритм NLP. Що більше слів у кожному реченні чи фразі, то більш двозначним стає слово у фокусі. BERT враховує розширене значення, читаючи в обох напрямках, враховуючи вплив усіх інших слів у реченні на фокусне слово та усуваючи імпульс зліва направо, який зміщує слова до певного значення в міру просування речення.

Нагадаємо, що NLP (англ. Neuro-linguistic Programming) – нейролінгвістичне програмування (НЛП), кодування психіки – псевдонауковий напрям у психотерапії та практичній психології, що вивчає закономірності суб'єктивного досвіду людей через розкриття механізмів і способів моделювання поведінки і передачі виявлених моделей іншим людям. Ефективність цього методу спростована.

Отже, після аналізу проблеми автоматичного виявлення фейкових новин за допомогою методів машинного навчання можна зробити такі висновки. Дана проблема є актуальною на сьогодні й навіть пріоритетною для визначеної цільової аудиторії. Багато дослідників уже спробували вирішити її за допомогою певного підходу, використовуючи уже відомі алгоритми чи створюючи власні інноваційні моделі. Деякі праці показують прийнятні результати точності виявлення фейків на певних наборах даних, але все одно мають деякі проблеми, щоб набути масового використання. Здебільшого, це складність реалізації, підготовка і маркування тренувальних наборів даних, погіршення показників точності зі зміною контексту даних та ін. Окремо варто виділити BERT-модель для аналізу природної мови, яка набуває все більшої популярності у вирішенні таких завдань. Її перевагами є достатньо високі та стабільні протягом певного часу показники точності виявлення фейкових новин, можливість конфігурації моделі і використання різних параметрів роботи для підбору найбільш ефективних для вирішення певного типу проблем. Також варто виділити кращі показники виявлення фейкових новин, ніж у стандартних алгоритмів, рекомендації інших дослідників щодо використання та постійне вдосконалення підходів, що базуються на BERT-модель.

Література:

1. Ahmed, A. A. A., Aljarbouh, A., Donepudi, P. K., & Choi, M. S. (2021). Detecting Fake News Using Machine Learning: A Systematic Literature Review. Journal of Educational Psychology, vol. 58, no. 1, pp. 1932–1939. https://doi.org/10.48550/arXiv.2102.04458
2. Ben Lutkevich. (2020). BERT language model. Retrieved from: https://www.techtarget.com/searchenterpriseai/definition/BERT-language-model
3. Gurunathan, Indhumathi. (2019). A Hybrid Model to Detect Fake News. Computer Science Graduate Projects and Theses. 17. Retrieved from: https://scholarworks.boisestate.edu/cs_gradproj/17
4. Houtao Deng, An Introduction to Random Forest, https://towardsdatascience.com/random-forest-3a55c3aca46d (accessed 15 December 2021).
5. Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers), pp. 4171–4186, Minneapolis, Minnesota. Association for Computational Linguistics.
6. Jadhav, S. S., & Thepade, S. D. (2019). Fake News Identification and Classification Using DSSM and Improved Recurrent Neural Network Classifier, Applied Artificial Intelligence, 33(12), 1058-1068. https://doi.org/10.1080/08839514.2019.1661579
7. Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, & Huan Liu. (2017). Fake News Detection on Social Media: A Data Mining Perspective. ACM SIGKDD Explorations Newsletter. Vol. 19, Issue 1, pp. 22–36. https://doi.org/10.1145/3137597.3137600
8. Kaliyar, R. K., Goswami, A., Narang, P., & Sinha, S. (2020). FNDNet–A deep convolutional neural network for fake news detection. Cognitive Systems Research, 61, 32-44. https://doi.org/10.1016/j.cogsys.2019.12.005
9. Kaliyar, R. K., Goswami, A. & Narang, P. FakeBERT: Fake news detection in social media with a BERT-based deep learning approach. Multimed Tools Appl 80, 11765–11788 (2021). https://doi.org/10.1007/s11042-020-10183-2
10. Kesarwani, A., Chauhan, S. S., & Nair, A. R. (2020). Fake News Detection on Social Media using K-Nearest Neighbor Classifier. 2020 International Conference on Advances in Computing and Communication Engineering (ICACCE), Las Vegas, NV, USA, pp. 1-4. https://doi.org/10.1109/ICACCE49060.2020.9154997
11. Khanam, Z., et al. (2021). IOP Conference Series: Materials Science and Engineering. 1099 012040
12. Kotteti, C. M. M., Dong, X., Li, N., & Qian, L. (2018). Fake news detection enhancement with data imputation. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). Athens, 2018, pp. 187-192. https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00042
13. Logistic Regression in Machine Learning, available online, https://www.javatpoint.com/logistic-regression-in-machine-learning, (accessed 15 December 2021).
14. Nishant R., Deepika K., Naman K., Chandan R., Ahad A. (2022) Fake News Classification using transformer based enhanced LSTM and BERT. International Journal of Cognitive Computing in Engineering, Volume 3, 2022, Pages 98-105, https://doi.org/10.1016/j.ijcce.2022.03.003
15. Patil, D.R. (2022). Fake News Detection Using Majority Voting Technique. *ArXiv, abs/2203.09936*.
16. Pratiwi, I. Y. R., Asmara, R. A., & Rahutomo, F. (2017). Study of hoax news detection using naïve bayes classifier in Indonesian language. 2017 11th International Conference on Information & Communication Technology and System (ICTS), Surabaya, pp. 73-78. https://doi.org/10.1109/ICTS.2017.8265649
17. Shaina Raza & Chen Ding. (2022). Fake news detection based on news content and social contexts: a transformer-based approach. International Journal of Data Science and Analytics, 13, 335–362. https://doi.org/10.1007/s41060-021-00302-z
18. Singh, V., Dasgupta, R., Sonagra, D., Raman, K., & Ghosh, I. (2017). Automated Fake News Detection Using Linguistic Analysis and Machine Learning. International Conference on Social Computing,

Behavioral-Cultural Modeling, & Prediction and Behavior Representation in Modeling and Simulation (SBP-BRiMS). https://doi.org/10.13140/RG.2.2.16825.67687
19. Sudhakar Murugesan, Kaliyamurthie K. P. (2022). Estimation of precision in fake news detection using novel bert algorithm and comparison with random forest. Authorea. May 12, 2022.
20. Ying, L., Yu, H., Wang, J., Ji, Y., & Qian, S. (2021). Multi-Level Multi-Modal Cross-Attention Network for Fake News Detection," in IEEE Access, vol. 9, pp. 132363-132373. https://doi.org/10.1109/ACCESS.2021.3114093
21. Ying, L., Yu, H., Wang, J., Ji, Y., & Qian, S. (2021). Fake News Detection via Multi-Modal Topic Memory Network. In IEEE Access, vol. 9, pp. 132818-132829. https://doi.org/10.1109/ACCESS.2021.3113981

Кулешник Я. Ф.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент;

Д'яков А. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук

ЄВРОПЕЙСЬКИЙ ПІДХІД ЩОДО СТВОРЕННЯ ЄДИНОГО ЦИФОРОВОГО РИНКУ

Успішне та ефективне прийняття технологій і створення Єдиного Європейського цифрового ринку вимагає партнерських відносин та спільної праці між усіма членами цієї спільноти. Для цього потрібно гармонізувати усі нормативно-правові, технічні та бізнесові аспекти у даній сфері. У реальному житті реалізація та супровід такої ідеї може зайняти багато років чи навіть десятиліть, тому що для досягнення належного рівня довіри між усіма сторонами потрібно прийняти цілу низку загально визнаних та широко використовуваних правил співжиття. Значення подібних правил та роль електронних підписів (на яких базується уся довіра між партнерами) в успішності реалізації таких ідей в ЄС усвідомили ще в 1999 році, коли Європейський Парламент видав Директиву №1999/93/ЄС. Ця Директива повинна була стати гарною основою для спільної інфраструктури електронних підписів та заохоченням для використання та впровадження усіма Європейськими державами. Однак, Директива своєчасно не спрацювала, тому, що вона чітко не вимагала від країн-членів ЄС використання спільних технічних стандартів для забезпечення використання транскоридорних електронних операцій. В цей же час досвід прийняття платіжних карток на чіпах показав, як технологічна сумісність рішень, що використовуються під час надання електронних послуг, та їхня здатність взаємодіяти між собою, може привести до успіху. Чому не спрацювала Директива №1999/93/ЄС? Споживчі настрої та використання електронних послуг (будь-які послуги, що надаються через інформаційно-телекомунікаційну систему) ще два десятиліття тому були на стадії становлення а запуск Facebook відбувся лише через три роки.

Тому на заміну Директиви №1999/93/ЄС було прийнято Регламент № 910/2014 де електронні підписи було трансформовано на **eIDAS,** що містить три складові:

- електронну ідентифікацію (electronic identification, eID);
- автентифікацію (authentification);
- довірчі послуги (trust services).

Регламент **eIDAS** був опублікований у липні 2014 року і за перші два роки став чинним для усього внутрішнього ринку ЄС.

eIDAS сприяє технологічній сумісності технічних рішень в усіх 28 країнах-членах ЄС, котрі використовуються під час надання електронних послуг та забезпечує здатність їх взаємодіяти між собою шляхом взаємного визнання в них схем електронної ідентифікації, та спрощення надання послуг по всьому Європейському Союзі. Він також гарантує, що довірчі послуги, надані кваліфікованими постачальниками послуг, можуть прийматися в якості доказів в судовому провадженні.

Завдяки **eIDAS** громадяни, підприємства та органи державної влади можуть використовувати засоби електронної ідентифікації та довірчі послуги (тобто електронні підписи, електронні печатки, штемпелі часу, реєстрову електронну доставку та автентифікацію веб-сайту) для доступу до електронних послуг або управління електронними операціями як у себе в країні, так і поза її межами. Він також створює європейський внутрішній ринок електронних довірчих послуг. Це дозволяє:

- підвищити прозорість та підзвітність – чітко визначено мінімальні зобов'яз'ння та відповідальність для постачальників довірчих послуг (trust service providers, TSP);

- гарантувати надійність послуг разом з підвищенням вимог безпеки для їх провайдерів;
- забезпечити технологічну нейтральність – уникнути вимог, які можна задовольнити лише при виконанні певної технології;
- визначити ринкові правила та забезпечити стандартизацію.

Як державні послуги, так і послуги у приватному секторі ставатимуть більш гнучкими і зручними у використанні та запропонують багато інших переваг, включаючи:

- зменшення адміністравтивного тиску на електронні операції з іншими підприємствами, клієнтами та державними адміністраціями;
- організація більш ефективних бізнес-процесів;
- досягнення економії за рахунок значного скорочення накладних витрат;
- здійснення безпечних електронних транзакцій, що приведе до збільшення довіри споживачів та потенційної споживчої бази – громадяни можуть укладати безпечні транскордонні електронні угоди та повною мірою скористатися своїми правами в ЄС, від зарахування до іноземного університету до доступу до електронних медичних записів;
- зменшення проблем, пов'язаних з безпекою та конфіденційністю, оскільки громадяни та підприємства можуть використовувати свої власні національні електронні ідентифікаційні номери для доступу до електронних послуг;
- збільшення та урізноманітнення державних електронних послуг, що призведе до зменшення обігу паперових документів – громадяни, які переїжджають до іншої держави-члена ЄС, можуть реєструватися та користуватися іншими послугами онлайн.

Такий підхід створює основу для гарантування безпечної, швидкої та більш ефективної електронної взаємодії між підприємствами, незалежно від того, в якій країні Європи вони відбуваються.

Для побудови єдиного цифрового ринку CEF та реалізації норм **eIDAS** Європейським Союзом було започатковано фонд під назвою Програма інтеграції Європи (Connecting Europe Facility, CEF). Він пропонує гранти та іншу фінансову допомогу для підтримки проектів, які працюють над створенням взаємопов'язаної європейської інфраструктури в енергетиці, транспортній сфері, та сфері цифрових послуг. Ця ключова цифрова інфраструктура широко відома під назвою «будівельні блоки CEF». Вона пропонує основні можливості, які можна використовувати в будь-якому європейському проекті для полегшення створення міждержавних електронних публічних послуг та розвитку цілих секторів бізнесу.

За своєю суттю будівельний блок CEF – це сукупність технічних специфікацій, програмного забезпечення та послуг, які можна повторно використовувати в проектах будь-якої сфери діяльності, причому:

- технічні специфікації будівельного блоку максимально відкриті та орієнтовані на ринок;
- послуги будівельного блоку чітко визначені, тобто задукоментовані, з угодами про рівень послуг, навчання, забезпечення службою підтримки тощо;
- програмне забезпечення будівельного блоку достатньо зріле, тобто пройшло успішен використання в пілотних проектах для реалізації транскордонних транзакцій.

До переліку основних будівельних блоків цифрової інфраструктури зокрема входять:

- Елктронна інфраструктура eID – надає набір стандартів та послуг для електронної ідентифікації в ЄС. За наявності та правильного функціонування цієї системи громадяни ЄС можуть використовувати свої національні електронні посвідчення особи, щоб скористатися послугами по всьому ЄС, не потребуючи нового електронного посвідчення, якщо вони переміщуються з однієї до іншої країн ЄС. Основна ідея полягає в тому, щоб об'єднати існуючі системи електронної ідентифікації між країнами-членами ЄС та змусити їх працювати без перешкод з дотриманням Регламенту ЄС, котрий забезпечує виконання технічних стандартів.
- Електронні підписи eSignature – це цифрова версія звичайних рукописних підписів. У такий спосіб підписант приймає юридичну прив'язку до умов, зазначених у документі. Електронні підписи надають користувачам можливості укладати господарські договори, здійснювати фінансові операції та користуватися державними послугами. Отже, електронні підписи повинні гарантувати безпечний, надійний, а також простий у використанні для всіх механізм.
- Електронний eInvoicing – виставлення рахунків та управління платежами і дебіторською заборгованістю, яке все ще є процесом, що виконується вручну на багатьох підприємствах. Причиною цього є використання нестандартних форматів організації даних, що ускладнює

автоматизацію, навіть якщо використовується спеціальне програмне забезпечення. У цей блок також входять електронні рахунки, що використовують стандартні формати для збору всієї необхідної інформації, яку легко читати за допомогою програмного забезпечення AP/AR (кредиторська/дебіторська заборгованість). Відповідно до Європейської директиви та стандарту електронних рахунків eInvoicing підтримує безперебійну генерацію, надсилання, отримання та обробку електронних рахунків, в тому числі міжнародних. Це робить процес виставлення рахунків та платежів набагато простішим, швидшим, дешевшим та без помилок.

- Електронна реєстрована доставка eDelivery – це сукупність розподілених вузлів, призначених для обміну відповідною інформацією між зацікавленими сторонами в цифровій транзакції. Специфікації eDelivery стандартизовані, що дозволяє використовувати їх різними організаціями, які в іншому випадку могли б використовувати широкий спектр різних IT-систем. Ці вузли можуть використовуватися по всій Європі національними чи регіональними організаціями, громадянами, державними адміністраціями та бізнесом.
- eArchiving – заснований на проектах Європейського архіву та збереження знань (E-ARK). Технічні характеристики та відповідне програмне забезпечення сервісної платформи eArchiving розроблені та пілотовані в рамках проекту E-ARK за часткового фінансування Комісією, що, допоможе досягти значного зниження витрат на впровадження та підтримку рішень електронного.

Головна мета Програми інтеграції Європи – це підтримка проектів з використанням заснованих на стандартах базових компонентів (будівельних блоків), що забезпечуватимуть взаємодію систем між собою.

Література:

1. Освітній курс «Вступ до електронного документообігу» – https://u-learn.org.ua/p/e Міністерство цифрової трансформації України - https://www.facebook.com/eGovernanceUkraine/photos /a.740436362676302/2798632726856645/?type=3&eid=ARA1ghg5jjIXrYEseqTmv4w4eHRQ4BRGGp3D5 bsfDADbmvnqix- JY6UzUpPQDGhYHan8lJWOHkqOWJua&__tn__=EEHH-R.
2. Закон України «Про електронні довірчі послуги» – https://zakon.rada.gov.ua/laws/show/2155-19 16 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» – https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF?Kclid=I-wAR0ionHGuRIWGNJNY14osHWsFIZz0KJRJgH8DZdaTLzsPNI_aotaip6CdYs .
3. Кваліфікований надавач електронних довірчих послуг Інформаційно-довідковий департамент ДПС – https://acskidd. gov.ua/partnershipdoc

Кулинич М.-М. А.
аспірантка кафедри кримінального процесу та криміналістики Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ ЗАХИСНИКОМ ПІДСИСТЕМИ «ЕЛЕКТРОННИЙ СУД» ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

05.10.2021 офіційно почали функціонувати такі підсистеми (модулі) Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС), як «Електронний кабінет» та «Електронний суд» [1].

Стаття 35 КПК України зобов'язує адвокатів реєструвати офіційні електронні адреси в ЄСІТС в обов'язковому порядку, а відтак пройти процедуру реєстрації користувача в ЄСІТС (реєстрація Електронного кабінету з використанням кваліфікованого електронного підпису, далі – КЕП) [2]. На відміну від інших процесуальних кодексів (ЦПК, КАС та ГПК) Кримінальний процесуальний кодекс України не містить норми про те, що особи, котрі зареєстрували свої офіційні електронні адреси в ЄСІТС можуть подати процесуальні документи, вчинити інші процесуальні дії в електронній формі

виключно за допомогою ЄСІТС, з використанням власного електронного підпису, прирівняного до власноручного підпису.

Втім, як визначено Положенням про порядок функціонування окремих підсистем ЄСІТС, затвердженим рішенням ВРП від 17.08.2021 №1845/0/15-21, процесуальні документи та докази можуть подаватися до суду в електронній формі, а процесуальні дії – вчинятися в електронній формі виключно за допомогою ЄСІТС з використанням власного КЕП, за винятком випадків, передбачених процесуальним законом [3].

Безперечно, впровадження означених модулів ЄСІТС є вагомим досягненням в напрямку цифровізації судочинства та кримінального провадження. Підсистема «Електронний суд» надає технічну можливість адвокату в електронний формі, незалежно від місця його знаходження оскаржувати під час досудового розслідування процесуальні рішення, дії чи бездіяльність слідчого, дізнавача або прокурора в порядку статті 303 КПК України, подавати клопотання, а також ознайомлюватись з матеріалами «справи» (термін вжито і далі по тексту буде вживатися у розумінні Положення про порядок функціонування окремих підсистем ЄСІТС, затвердженого рішенням ВРП від 17.08.2021 №1845/0/15-21 відповідно до правил цитування) за тими чи іншими скаргами, клопотаннями, запитами тощо. Використання цього модулю зменшує як часові, так і фінансові затрати захисника, адже виключає потребу в копіюванні додатків до скарги чи клопотання, поданні процесуальних документів у приміщенні суду чи їх скеровуванні поштовим відправленням. Більше того, суттєвою перевагою використання Електронного суду є оперативна та своєчасна поінформованість щодо ходу розгляду того чи іншого клопотання, скарги тощо. Підсистема надає змогу увімкнути сповіщення про усі нові надходження процесуальних документів у «справі», про що адвокат отримує відповідне повідомлення на електронну пошту. Це дозволяє завчасно бути повідомленим про час та місце розгляду скарги чи клопотання, швидше отримувати копії ухвалених судових рішень в Електронному кабінеті. Паралельно, вже понад рік успішно функціонує офіційний мобільний застосунок Електронного суду «єСуд», котрий забезпечує швидкий та комфортний доступ до сервісів Електронного Суду безпосередньо з мобільних пристроїв (за винятком можливості формування проєктів процесуальних документів та їх подання) [4].

Поряд з вказаними перевагами підсистеми «Електронний суд», практика її використання у перебігу досудового розслідування дозволяє окреслити ряд проблемних аспектів, що зумовлені як об’єктивними, так і суб’єктивними факторами.

Насамперед, мова йде про неналежне забезпечення судів технічними пристроями, як-то швидкісними сканерами, для сканування та переведення в електронну форму тих документів, що надходять до суду у паперовому вигляді. Відтак, доволі часто матеріали «справи» в Електронному суді містять лише процесуальні документи, складені судом (повістки, ухвали, протоколи автоматизованого розподілу судових справ між суддями), проте не включають процесуальних документів, поданих учасниками кримінального провадження.

Крім цього, приєднання учасника до матеріалів «справи» в електронному вигляді здійснюється секретарем судового засідання, котрий в силу зайнятості в судових засіданнях, незначний досвід користування сервісом чи з інших причин не завжди своєчасно надає доступ адвокату до матеріалів конкретної «справи» в Електронному суді.

Не можна не згадати технічні збої та несправності, що інколи трапляються в роботі модулів (скажімо, подана адвокатом скарга в підсистемі «Електронний суд» зареєстрована в підсистемі, проте картку справи за скаргою не створено, автоматизований розподіл справи між суддями не проведено, а отже й розгляд скарги не відбувається). Особливо гостро цю проблематику сторона захисту відчула після початку повномасштабного вторгнення рф в Україну 24.02.2022, коли доступ до Електронного суду було обмежено повністю, з неможливістю подати будь-який процесуальний документ, зберегти раніше завантажені файли чи отримати електронну копію судового рішення. Такі прецеденти є своєрідним застереженням для адвоката регулярно зберігати наявні в електронній «справі» процесуальні документи на матеріальні носії інформації чи у хмарних сховищах даних з тим, щоб не втрачати доступу до документів, котрі складені виключно в електронній формі.

Між тим, механізм реєстрації Електронних кабінетів слідчими, дізнавачами та прокурорами залишається не врегульованим, попри наявність зареєстрованих Електронних кабінетів ЄСІТС в органів прокуратури, органів Національної поліції, органів безпеки, органів Державного бюро розслідувань та Національного антикорупційного бюро України. Як наслідок, вказані суб’єкти кримінального провадження

не є активними користувачами Електронного суду, а отже не можуть подати за його допомогою процесуальні документи чи отримати в Електронних кабінетах ті процесуальні документи, що складені слідчими суддями чи стороною захисту. В той же час, оскільки поки що відсутня інтеграція між ЄСІТС та інформаційно-телекомунікаційною системою досудового розслідування (котра ще не функціонує), слідчий, дізнавач, прокурор в силу п.20-6 Перехідних положень КПК України зобов'язаний подавати до суду матеріали як в паперовій формі, так і в електронній формі з використанням КЕП. Вочевидь, наявність зареєстрованого Електронного кабінету у слідчого та прокурора дозволила б останнім надсилати засвідчені КЕП матеріали в електронній формі не лише на електронну адресу суду, але й шляхом завантаження таких в підсистемі Електронного суду. При цьому, функціонал Електронного суду містить опцію надсилання документів до Електронних кабінетів інших учасників перед відправкою до суду, а отже сторона обвинувачення зможе попередньо надіслати підозрюваному, обвинуваченому та захиснику в їх Електронні кабінети (за умови реєстрації таких в ЄСІТС) в електронному вигляді ті клопотання та додані до них матеріали, обов'язок надання яких прямо визначений у КПК України (клопотання про застосування, зміну, продовження та скасування запобіжних заходів).

Таким чином, використання захисником під час досудового розслідування підсистеми «Електронний суд» є невід'ємною частиною імплементації електронного кримінального провадження та суттєво спрощує організацію робочого процесу. В той же час, окреслені недоліки в роботі модуля потребують якнайшвидшого комплексного організаційного, нормативного та фінансового вирішення. Також, оскільки реалізація стороною захисту своїх прав, пов'язаних з використанням Електронного суду, частково пов'язана із наявністю зареєстрованих Електронних кабінетів у слідчого, дізнавача та прокурора, окрім правової регламентації такої реєстрації доцільно популяризувати використання цієї підсистеми поміж означених правоохоронних органів, а також, очевидно на часі, вирішити питання із запуском інформаційно-телекомунікаційної системи досудового розслідування (котра ще, на жаль, фактично не функціонує).

Література:

1. Електронне судочинство в дії: в Україні офіційно починають функціонувати три підсистеми (модулі) ЄСІТС. URL: https://court.gov.ua/press/news/1188723.
2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 №4651-VI у редакції від 06.11.2022. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 05.12.2022) .
3. Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи : рішення Вищої ради правосуддя від 17.08.2021 №1845/0/15-21. URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text (дата звернення: 05.12.2022) .
4. «Суд у смартфоні»: в Україні запрацює новий застосунок. URL: https://www.ukrinform.ua/rubric-society/3323469-sud-u-smartfoni-v-ukraini-zapracue-novij-zastosunok.html.

Лепісевич П. М.,
доцент кафедри загально-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат історичних наук, доцент

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ ВОЄННОЇ АГРЕСІЇ

Відповідно до Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 року, інформаційна безпека є складовою національної безпеки України. Своєю чергою інформаційна безпека – стан захищеності інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими

організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України□1□.

В умовах війни проблема поширення інформації стає питанням національної безпеки. Сьогодні ми спостерігаємо як деструктивна російська пропаганда як ззовні, так і всередині України, використовуючи різноманітні суспільні настрої, розпалює міжнаціональну ворожнечу, підриває основні засади державного суверенітету України. Поширення деструктивної інформації відбувається в різний спосіб: у формі публічних закликів, через мережу Інтернет, з використанням засобів масової інформації тощо. Тому перед державою стоїть нагальна необхідність швидко реагувати та запобігати відповідним злочинним проявам.

Чинний Кримінальний кодекс України містить заборони порушення режиму державної та службової інформації, серед яких основними вважаються «Державна зрада» (ст.111), «Шпигунство» (ст.114), «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни» (ст.330). Водночас, повномасштабне вторгнення російської федерації на територію України 24 лютого 2022 року зумовило значне реформування кримінального законодавства України у частині охорони інформаційної безпеки України від негативного інформаційного впливу держави-агресора.

Зокрема йдеться про криміналізацію наступних протиправних діянь:

1. **«Колабораційна діяльність»** (ст.111-1) у таких формах:

- публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України (ч.1 ст.111-1);
- публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора (ч.1 ст. 111-1);
- публічні заклики громадянином України до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора (ч.1 ст.111-1);
- публічні заклики громадянином України до невизнання поширення державного суверенітету України на тимчасово окуповані території України (ч.1 ст.111-1);
- здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, активна участь у таких заходах (ч.6 ст. 111-1).

2. **«Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану» (ст. 114-2)**, а саме:

- поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, у тому числі про їх переміщення територією України, якщо така інформація не розміщувалася (не поширювалася) у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України, Головним управлінням розвідки Міністерства оборони України чи Службою безпеки України або в офіційних джерелах країн-партнерів, вчинене в умовах воєнного або надзвичайного стану (ч.1);
- поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, вчинене в умовах воєнного або надзвичайного стану (ч.2).

3. **«Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників» (ст.436-2)**:

- виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії Російської Федерації проти України як внутрішнього громадянського конфлікту (ч.1);
- виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України(ч.1);

- глорифікація осіб, які здійснювали збройну агресію Російської Федерації проти України, розпочату у 2014 році, представників збройних формувань Російської Федерації, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих Російською Федерацією, а також представників окупаційної адміністрації Російської Федерації, яку складають її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних Російській Федерації самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України (ч.1);
- виготовлення, поширення матеріалів, у яких міститься виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії Російської Федерації проти України як внутрішнього громадянського конфлікту (ч.2);
- виготовлення, поширення матеріалів, у яких міститься виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України (ч.2);
- виготовлення, поширення матеріалів, у яких міститься глорифікація осіб, які здійснювали збройну агресію Російської Федерації проти України, розпочату у 2014 році, представників збройних формувань Російської Федерації, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих Російською Федерацією, а також представників окупаційної адміністрації Російської Федерації, яку складають її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних Російській Федерації самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України (ч.2).

Названі законодавчі новели не позбавлені певних недоліків, які пов'язані як і з порушенням правил законодавчої техніки, так і проблемами застосування норм у судовій практиці. Першочергово постало актуальне питання про розмежування нових складів кримінальних правопорушень з «Державною зрадою» (ст.111), адже як виявилось вказані форми колаборaційної діяльності можна трактувати як державну зраду у такій її формі як перехід на бік ворога в період збройного конфлікту. Виникло чимало питань, пов'язаних з співвідношенням норм про нові склади кримінальних правопорушень між собою, а саме ч.1 ст.111-1 КК України та ч.1 ст.436-2 КК України, основною відмінністю яких слід визнавати те, що саме для колаборaційної дяльності обов'язкове встановлення наявності співпраці з державою-агресором, що часто ігнорується під час правозастосування. Незважаючи на певні труднощі під час тлумачення та застосування нових кримінально-правових заборон, все-таки відповідні зміни слід вважати доречними та своєчасними, здатними ефективно реагувати на загрози інформаційній безпеці України. Заслуговують на увагу також пропозиції правників щодо криміналізації у КК України відповідальності за кібертероризм □2, С.70-81□. Також зважаючи на те, що інформаційна безпека охоплює, з-поміж іншого, захист від невірогідної інформації, перспективними видаються питання встановлення кримінальної відповідальності за випуск новин, допуск до ефіру, тираж або допис редакції в соціальній мережі завідомо неправдивої суспільно необхідної інформації, як це визначено в Проєкті КК України (ст.7.7.10) □3□.

Література:

1. Стратегія забезпечення державної безпеки: Указ Президента України від 16 лютого 2022 року №56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text(Дата звернення: 01.12.2022).
2. Кучерина Сергій, Олєйніков Денис. Проблемні аспекти впровадження кримінальної відповідальності за кібертероризм. Збірник наукових праць. *Геополітичні пріоритети України.* 2021. Випуск 1 (26). С.70 – 81.
3. Проєкт КК України (станом на 29.09.2022). https://newcriminalcode.org.ua/upload/media/2022/09/29/1-kontrolnyj-tekst-proektu-kk-29-09-2022.pdf(Дата звернення: 01.12.2022).

Магеровська Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

Магеровський Д. В.,
викладач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ

Романюк Д. І.,
здобувач вищої освіти факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

ТЕХНОЛОГІЇ BIG DATA В ЮРИСПРУДЕНЦІЇ

Щодня користувачі інтернету створюють близько трьох квінтильйонів байт даних. Щоразу, коли вони заходить на сайт або пишуть повідомлення електронною поштою, десь у світі стоїть комп'ютер, який відстежує ці дії та реєструє їх в онлайн-профілі кожного користувача. Можливості аналізу великих масивів даних за допомогою складних математичних алгоритмів тепер використовуються в низці сфер для покращення клієнтського сервісу, аналізу ситуації на ринку або реклами. Впровадження технологій Big Data, які дозволяють аналізувати дані в їхньому початковому стані, без додаткового структурування, вже відбулася і юриспруденція – не виняток.

Юридичні фірми, не надто сприйнятливі до технологій і які не використовують у роботі аналіз великих масивів даних можуть залишитися на периферії ринку.

Перший напрям, в рамках якого юристи працюють з аналізом Big Data, – використання масивів даних для автоматизації роботи з метою пошуку різноманітних невідповідностей або навпаки, можливостей у законах. Так, наприклад, успішно працює система прогнозування ймовірності проходження законів через Конгрес США.

Аналіз даних суттєво допомагає у судовій практиці. Наприклад, отримати короткий та змістовний висновок на підставі аналізу сотень судових актів. Економить час та гроші. Створює перевагу перед опонентами. На жаль, зараз автоматизувати цю роботу в Україні складно через обмеження в системі електронного правосуддя.

За кордоном юридичні фірми, особливо великі, вже почали використовувати великі дані в щоденній роботі. Наочний приклад – електронний асистент ROSS, програма, створена в компанії ROSS Intelligence і працююча на когнітивному комп'ютері IBM Watson, що оснащений запитально-відповідною системою штучного інтелекту. Вона використовує природну мову для того, щоб зрозуміти питання юристів і повідомити їм інформацію щодо судових справ і законодавства з необхідними посиланнями, що їх цікавлять, і застосовується тими, хто аналізує контракти. Інший каліфорнійський стартап, Lex-Machina, серед клієнтів якого Google і Nike, аналізує суперечки у сфері інтелектуальної власності та створює структуровані бази з відкритих даних – наприклад, із використанням судових документів. Він допомагає юристам уявити результат справи або вибрати правильну стратегію дій у суді. Аналогічні системи допоможуть підібрати зручну юрисдикцію для спору.

Прогнози, які складають машини, згодом стають дедалі точнішими. Так, сьогодні команді дослідника Даніеля Каца з Університету Мічигана вдається вгадати рішення ЗС США з точністю до 70%. Можна прорахувати, які аргументи працюють для більшості, а що має значення для конкретного судді. Також завдяки аналізу масивів даних юридичної фірми простіше зрозуміти, чи взагалі варто братися за справу: якщо раніше подібне дослідження питання забирало до 20 днів, то сьогодні завдяки технологіям воно займе 20 хвилин.

Вигідно це не лише юристам, а й суспільству загалом. Скорочення тимчасових витрат юристів на підготовку до справи теоретично дозволить зменшити рахунок за юридичні послуги і зробити правосуддя доступнішим. Такі аналітичні системами як LexisNexis, Westlaw, Judges Analytics дозволяють, наприклад, досліджувати та візуалізувати, хто із суддів буде більш прихильний до тих чи інших аргументів.

У правосуддя аналіз даних принесе як доступність, так і якісно новий рівень розгляду питань. Так у США вже є приклади, коли результати аналізу великих даних із відкритих джерел було представлено як доказів у суді.

Інший напрямок застосування аналізу великих даних – їх використання для позбавлення людства від юристів. Наочний приклад – історія з автоматизацією пошуку незаконних штрафів за паркування у Нью-Йорку. Тоді лише один аналітик, який сидить за комп'ютером, знайшов тисячі нелегально виписаних штрафів за допомогою міських відкритих даних.

Поки футурологи від права прогнозують заміну значної кількості юристів машинами, згідно з більш виваженим поглядом на проблему, при найгіршому для юристів сценарії скорочення штату може становити не більше 13%. Причому скоротять лише тих, хто зайнятий рутинною роботою: згідно з дослідженням, проведеним McKinsey & Co., 23% роботи, що виконується юристами, та 69% роботи паралігалів можуть бути автоматизовані за допомогою сучасних технологій.

Ще одна область, де юристи зіштовхуються з новою технологією аналізу інформації – використання великих даних для розробки алгоритмів, які починають приймати рішення за людину. Тут і починається найбільш проблемна зона, а саме виникає питання до юристів про правозастосування у разі помилок.

Відповідно до рекомендацій Американської асоціації юристів ABA від 2012 року, юрист має бути у курсі змін у професії, зокрема пов'язаних із ризиками від використання технологій. Тобто, якщо ви недостатньо поінформовані про ризики, пов'язані з, наприклад, великими даними, це цілком можна розцінювати як несумлінність – з усіма наслідками, що випливають. Для корпоративних клієнтів питання полягає в тому, чи можуть предиктивні можливості аналізу спричинити велику відповідальність щодо ідентифікації ризиків. Іншими словами, чи зросте відповідальність юридичних фірм за проблеми бізнесу з урахуванням того, що вони мали більше можливостей передбачати ситуацію. А якщо додатки, які використовуються для аналізу великих масивів даних, проаналізують інформацію неправильно – чи спричинить це відповідальність для юридичної фірми? Поки що ці питання залишаються відкритими.

Інша складність для юридичних фірм, які використовують великі дані, полягає в тому, що законодавство у цій галузі змінюється щодня, як і самі технології. Законодавці намагаються встигнути за прогресом, щоб задовольнити вимоги захисту персональної інформації, зазначає американський дослідник Коузен О'Коннор, і юридичним фірмам доводиться стежити за новинками в законодавстві з подвійною увагою. Крім того, закони в цій галузі постійно змінюються, тому ризик порушити ті чи інші законодавчі норми великий.

В американському дослідженні 45 компаній, що використовують Big Data, не виявилося жодної юридичної фірми – і це не дивно з урахуванням того, що юридичний бізнес не завжди швидко реагує на інновації. Але експерти все ж таки сходяться на думці: аналіз великих даних неминуче вплине не тільки на роботу юристів, а й на сам бізнес. Згідно з результатами опитування, більш ніж 1000 компаній із 19 країн світу 85% респондентів упевнені, що зміни будуть значними. Британська Law Gazette зазначає, що для великих світових компаній наявність стратегії використання Big Data стане необхідністю для збереження клієнтів і підтримки конкурентоспроможності.

Поки що аналіз даних успішно використовується для розвитку бізнесу. Аналіз інформації про клієнтів, включаючи компанії, які перестали звертатися за послугами, їх арбітражне навантаження, інформаційний контекст та актуальні проекти допомагає знайти правильний підхід у побудові відносин. Використовують нововведення і при рекрутингу. Так, актуальні дані про випускників юридичних факультетів, співробітників інших юридичних фірм та корпоративних юристів, включаючи інформацію про їх нагороди, проекти, кар'єру, дозволяє завжди тримати машину відбору кращих кадрів запущеною.

Ще один із напрямків, де вже використовують великі дані, – аналіз ціноутворення на юридичному ринку. Big Data використовують і юристи, і їх клієнти. Перші – щоб проаналізувати власні рахунки, витрати та те, як вони виглядають на тлі конкурентів, інші – для оптимального вибору консультанта. Особливий інтерес в останньому випадку виявляють страхові компанії та банки, які розробляють інструменти для аналізу та оптимізації витрат та обчислення найуспішніших фахівців.

У результаті юридичні фірми, які використовують нові технології аналізу даних, готові запропонувати клієнтам кращий сервіс за менші гроші – адже вони, ймовірно, вже проаналізували цінову політику конкурентів. А ті, хто повільніше пристосовується до нових реалій, у цьому випадку залишаються у програші, програючи більш технологічним та клієнтоорієнтованим компаніям.

Література:

1. https://www.techtarget.com/searchdatamanagement/definition/big-data
2. https://forbes.kz/process/technologies/bolshie_dannyie_prishli_v_yurisprudentsiyu_i_ona_uje_ne_budet_prejney/
3. https://legalhub.online/sudova-praktyka/big-data-yak-peredbachyty-rishennya-sudu/

Мельник А. М.,
здобувач навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ДИСКУСІЙНІ АСПЕКТИ НА ШЛЯХУ ЛЕГАЛІЗАЦІЇ КРИПТОВАЛЮТ

На сьогоднішній день цифрові та інформаційні технології неймовірно сильно проникли у наше життя і ми вже не уявляємо своє існування без них. Так, виходячи з дому, ми завжди беремо з собою смартфон, який містить у собі інформацію усього відкритого інтернету, картографічні дані, пам'ять для збереження необхідної інформації, засоби для проведення безконтактних операцій (оплата через технологію NFC) та багато чого іншого. Важко б було усвідомити що все це може зникнути в один день, як і швидко появилось. Так і швидко з'явились криптовалюти у нашому повсякденні.

Криптовалюта – різновид цифрової валюти, емісія та облік якої виконується децентралізованою платіжною системою повністю в автоматичному режимі без можливості внутрішнього або зовнішнього адміністрування. Основною принциповою особливістю роботи криптовалют є збереження інформації у блокчейні, де асиметричне шифрування перевіряє повноваження, а інші криптографічні методи – як proof-of-work та/або Proof-of-stake.

На сьогоднішній день статус криптовалют в Україні не визначений, оскільки законопроект "Про віртуальні активи" №3637 є, але постійно доопрацьовується [1]. Віртуальні активи занадто вільна система, яку не взмозі контролювати одна держава і повною мірою законодавець не забезпечить регулювання цього питання, оскільки існують кілька фундаментальних проблем які неможливо вирішити.

Однією з проблем є те, легалізація криптовалют та її масове впровадження призведе до активізації роботи шахраїв, які матимуть змогу ефективніше поширювати шкідливе програмне забезпечення, яке буде здатне використовувати ресурси персонального комп'ютера, ноутбуку чи інших пристроїв для майнінгу (видобування криптовалют) на системних потужностях користувачів. Це в свою чергу може завдати серйозної шкоди апаратним елементам пристроїв громадян. Таких злочинців важко відстежити, через те що "намайнені" засоби відправляються анонімно на анонімний гаманець. Фактично це буде нелегальним заробітком за рахунок чужих ресурсів.

Здійснювати контроль криптовалютних операцій це ідея яку важко реалізувати на практиці, оскільки порушується основний принцип роботи блокчейн систем, а саме анонімність та самостійність проведення усіх операцій [2]. А з теперішнім розвитком технологій органи виконавчої влади не зможуть контролювати цей складний процес. Логічно припускати, що частина громадян буде дотримуватись визначених норм, але більшість власників цифрових валют зможуть і надалі користуватись усіма "забороненими" можливостями цих систем, оскільки для звичайного переказу коштів потрібно лише дві сторони, а в варіанті держави ще буде залучатись посередник у лиці банку, який зніматиме додаткову комісію. Виникає логічне запитання, а для чого платити, коли є можливість цього не робити, та й ніхто про це не дізнається? Не відомо як саме закон повинен здійснювати свою реалізацію, проте на таку основоположну проблемо не можна закривати очі.

Якщо держава не зможе контролювати криптовалюту, і вирішить її заборонити, забезпечити повну заборону вона не зможе, оскільки криптовалюти функціонують за децентралізованим принципом, тому що немає єдиного сервера чи комп'ютера, який обробляє усі або частину операцій, а сервером

виступають тисячі пристроїв користувачів, які самостійно обробляють усі транзакції. У влади просто не буде засобів для здійснення такої заборони, та припинення існування криптовалют.

Також виникає проблема з тим, що фактично власники криптовалют не захищені з боку закону, адже сучасний кримінальний кодекс України не визначає криптовалюту предметом злочину, що призводить до того що справи з не повним складом кримінального правопорушення не можуть бути кримінальним правопорушенням. Тому законодавцеві слід звернути увагу у сторону цього питання, та діяти відповідно тенденцій розвитку сучасних технологій [3].

Підсумовуючи вище сказане, ми дійшли висновку, що контроль за обігом криптовалют це ідея, яку важко буде контролювати, оскільки контролювати те, що будувалось на принципах конфіденційності, децентралізованості та самостійності неможливо на даний момент.

Література:

1. Пропозиції Президента до Закону "Про віртуальні активи" URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110
2. Галушка Є.О., Пакон О.Д. Сутність криптовалют та перспективи їх розвитку, журнал «Молодий вчений» №4, 2017. с. 634. URL: http://molodyvcheny.in.ua/files/journal/2017/4/147.pdf
3. Кримінальний кодекс України URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (Дата звернення: 09.11.2022)

Миронов Ю. О.,
т. в.о. завідувача кафедри спеціальної фізичної та домедичної підготовки факультету № 3 Донецького державного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розглядаючи питання використання інформаційно-аналітичного забезпечення в діяльності підрозділів Національної поліції України в умовах воєнного стану необхідно зазначити, що з точки зору ефективної протидії злочинності заслуговує на увагу і інформація що характеризує:

- оперативну обстановку;
- психологічні риси осіб, підозрюваних у підготовці й вчиненні кримінальних правопорушень, або осіб, які сприяють укриттю інформації про кримінальну подію та про осіб, які до неї причетні;
- поточні профілактичні, слідчо (розшукові) дії та оперативно-розшукові заходи;
- види й способи вчинення кримінальних правопорушень;
- прикмети злочинців – організаторів, підбурювачів, посередників, пособників, виконавців;
- прикмети викрадених речей, здобутих злочинним шляхом, а також речей, матеріалів заборонених або обмежених до обігу в Україні;
- дані про задумані й підготовлювані кримінальні правопорушення і інші відомості.

Дефініцією є те, що інформаційне забезпечення діяльності підрозділів Національної поліції України має законодавче та нормативно-правове забезпечення. Так Законом України «Про Національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР (редакція від 01.01.2022) [1] визначені загальні терміни, які вживаються у такому значенні:

- база даних – іменована сукупність даних, що відображає стан об’єктів та їх відношень у визначеній предметній області;
- база знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами;
- засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв’язку, що використовуються для реалізації інформаційних технологій;
- інформаційна послуга – дії суб’єктів щодо забезпечення споживачів інформаційними продуктами;
- інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки

даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

- інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;
- інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо), тощо [1].

У статті 25 Закону України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII (редакція від 15.06.2022) зазначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень [2]. Окрім того, поліція уповноважена наповнювати та підтримувати в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (стаття 26 Закону України «Про Національну поліцію») [2].

Підрозділи Національної поліції України здійснюють інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень визначених законодавством України.

В рамках інформаційно-аналітичної діяльності поліція (стаття 25 Закону України «Про Національну поліцію»):

1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями;

5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів в електронній формі та в обсягах даних, зазначених у статтях 7, 14 Закону України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів», відомості, необхідні для забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів [2].

Також поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Стаття 27 Закону України «Про Національну поліцію» регламентує є безпосередній оперативний доступ поліції до інформації та інформаційних ресурсів інших органів державної влади. При цьому передбачено обов'язок дотриманням Закону України «Про захист персональних даних» [2]. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. Зазначаємо, що кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 Закону України «Про Національну поліцію», фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України [2].

Отже нами визначені деякі питання використання інформаційно-аналітичного забезпечення в діяльності підрозділів Національної поліції України. І тому, завершуючи аналіз означеної тематики зазначаємо, що діяльність підрозділів Національної поліції, безпосередньо пов'язана із захистом і обробкою персональних даних осіб. І тому дана діяльність повинна здійснюватися на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

Література:

1. Про Національну програму інформатизації: Законом України» від 4 лютого 1998 року № 74/98-ВР (редакція від 01.01.2022). Відомості Верховної ради України. URL:https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 #Text.
2. Про Національну поліцію: Закону України від 2 липня 2015 року № 580-VIII (редакція від 15.06.2022). Відомості Верховної ради України. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

Мойсієнко Р. С.,
здобувач вищої освіти факультету №2 Львівського державного Університету внутрішніх справ;

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного Університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка» кандидат технічних наук, доцент

РОЛЬ БІОМЕТРИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМИ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Аналіз сучасних публікацій, виступів у засобах масової інформації, документів, наукових статей показує, що інформаційні системи відіграють одну із провідних ролей у сучасних технологіях протидії злочинності. Нині можна впевнено стверджувати, що ефективність діяльності правоохоронних органів у сфері протидії злочинності головно залежить від стану інформаційно-аналітичного забезпечення, наявності відповідних інформаційно-комунікаційних систем, баз даних, розроблення та впровадження новітніх підходів у розслідувані злочинів з використанням сучасних досягнень у галузі інформаційних технологій. Тобто, розвиваючи та впроваджуючи новітні досягнення в галузі інформаційних технологій та інформаційно-телекомунікаційних систем дасть змогу значно підвищити ефективність діяльності правоохоронним органам сфері розкриття, розслідування та запобігання злочинам.

Не дивлячись на те, що поняття інформаційних технологій та інформаційно-телекомунікаційних систем носить досить широке поняття, охоплює широку сферу діяльності, ми б хотіли акцентувати увагу, в першу чергу, на використанні біометричних інформаційних систем. Враховуючи те, що злочинність як явище носить часто транснаціональний характер, то такі системи мають створюватися, впроваджуватися та використовуватися спільно різними структурами МВС України, наприклад, Національною поліції України, Державною міграційною службою, Державної прикордонною службою України тощо [1].

Уже сьогодні для удосконалення системи реєстрації біометричної інформації у різних структурах розробляються та впроваджуються відповідні інформаційні підсистеми. Так, наприклад, у Державній міграційній службі запроваджено Центр оброблення даних Єдиної інформаційно-аналітичної системи управління міграційними процесами, який забезпечує функціонування підсистем «Оформлення документів, що підтверджують громадянство України» та «Облік біженців та іноземців»; розгорнуто захищену телекомунікаційну мережу Державної міграційної служби з комплектом обладнання для оформлення документів та взяття біометричних даних (параметрів). У Державній прикордонній службі України уведено до експлуатації систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, за допомогою якої забезпечується встановлення особи іноземця та особи без громадянства, які в'їжджають до України, виїжджають з неї, здійснюється контроль за додержанням ними правил перебування на території України та виконання суб'єктами національної системи повноважень та завдань, визначених Законом України «Про правовий статус іноземців та осіб без громадянства» [2].

У нормативних документах МВС України передбачено створення Інтегрованої системи біометричної інформації про особу, її ідентифікації та верифікації, яка забезпечуватиме використання інтегрованих програмних продуктів та на базі інформаційної взаємодії з національною системою біометричної верифікації та ідентифікації, Єдиною інформаційною системою управління міграційними процесами, Єдиним державним демографічним реєстром, інформаційними системи дактилоскопічного обліку та іншими інформаційними, інформаційно-телекомунікаційними системами з метою удосконалення процесів ідентифікації та верифікації особи.

Разом з цим, під час розроблення та запровадження систем біометричної ідентифікації осіб є ряд питань, на які потрібно дати відповіді уже сьогодні. Це:

- удосконалення нормативно-правової бази, яка регламентує доступ до інформаційних ресурсів користувачами різних структур;
- організація міжвідомчої взаємодії у протидії злочинності;
- удосконалення діючих біометричних інформаційних систем (у відповідності до стану розвитку інформаційних технологій);
- забезпечення дотримання законності щодо отримання біометричних даних тощо.

Література:

1. Сеник В. В., Кулешник Я. Ф. Вдосконалення біометричних інформаційних систем ідентифікації осіб як чинник у протидії торгівлі людьми / Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. – Одеса : ОДУВС, 2018. с. 83–84.
2. Сеник В. В., Сеник С. В., Кулешник Я. Ф. Стан і напрями вдосконалення нормативно-правового й інформаційно-технічного забезпечення діяльності підрозділів Національної поліції України у сфері протидії торгівлі людьми / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2021. Вип. 1 (11). С. 46-52.

Мосюрчак В. М.,
викладач Фахового коледжу ЗВО «Університет Короля Данила» м. Івано-Франківськ, спеціаліст вищої категорії, викладач-методист

Морушко О. В.,
доцент кафедри інформаційних технологій ЗВО «Університет Короля Данила» м. Івано-Франківськ, кандидат фізико-математичних наук

ВИКОРИСТАННЯ СКРІНКАСТІВ ПРИ ВИКЛАДАННІ ФІЗИКО- МАТЕМАТИЧНИХ ДИСЦИПЛІН

В умовах воєнного стану в Україні найбільш безпечною і обґрунтованою є дистанційна форма освітнього процесу, що поєднує синхронний та асинхронний режими навчання з використанням інформаційно-комунікаційних технологій. Тому для кожного закладу вищої освіти пошук оптимальних форм організації навчального процесу з урахуванням воєнної ситуації у регіоні, наявних матеріально-технічних ресурсів і можливостей науково-педагогічних працівників є актуальним питанням.

На сьогоднішній день українські ЗВО створили власні дистанційні навчальні середовища в мережі Інтернет за допомогою сучасних інноваційних навчальних платформ Google Classroom, Moodle, Padlet та інших онлайн- сервісів. Науково-педагогічними працівниками створено велику кількість різноманітних навчальних матеріалів для синхронного та асинхронного режимів проведення навчальних занять, зокрема, і для навчання математичним і фізичним дисциплінам: конспекти лекцій та практичних занять, відеолекції, рекомендації до самостійної роботи та виконання лабораторних робіт, мультимедійні завдання та тести для контролю знань тощо. Безперечно, перевагу слід надавати синхронному режиму проведення занять, але в умовах воєнного стану це не завжди можливо, тому викладач має забезпечити здобувачів освіти повним комплексом навчально-методичних матеріалів для опанування певної теми у безпечний та зручний для них час. При вивченні математичних та фізичних дисциплін до переліку таких матеріалів можна включити конспекти лекцій та практичних занять, презентації, відеолекції, контрольні тести тощо.

У роботах [1, 2] розглянуто різні типи відео, які можна використовувати у освітньому процесі: навчальні фільми, студійні та натурні відеолекції, відеоскрайбінг, скрінкасти, інтерактивні відеоролики тощо. Зокрема, вказується, що навчальні матеріали у форматі відео є для студентів ефективними і приємними, стимулюють їх працювати над завданнями, дають змогу розвивати навички до самонавчання та дають їм відчуття контролю над процесом навчання. Підтверджується пряма позитивна кореляція між результатами, які демонструють здобувачі освіти під час проходження курсів, і вміннями, яких вони набувають. На думку спеціалістів з дистанційного навчання, ефективним є таке відео, в якому глядачі можуть спостерігати за появою певних візуальних елементів у кадрі та чути коментарі, які синхронно накладаються на появу слів, цифр, зображень чи анімацій [2]. Досить часто викладачами використовуються так звані скрінкасти – цифрові відеозаписи відомостей, що виводяться на екран комп'ютера та можуть супроводжуватися голосовими коментарями [1, с. 25]. Англомовний термін «screencast» з'явився 2004 року за участі колумніста Jon Udell, який шукав назву для нового жанру контенту. Одним із найпопулярніших професійних сервісів для запису скрінкастів є Camtasia – програмний продукт компанії TechSmith. Це програмне забезпечення можна встановити для Windows та MacOS 10.10 і воно дає змогу захоплювати відео з екрану, записувати відео та звук із вебкамери (або окремо), редагувати відео та аудіо, додавати візуальні ефекти тощо. Більш простішим способом

створення скрінкасту є онлайновий сервіс Screencast-O'Matic або ж використання базової функції «Вставити – Запис з екрану», інтегрованої у звичайний PowerPoint. Також можна створювати записи трансляцій у Zoom та Google Meet. На сьогоднішній день скрінкаст можна вважати оптимальним форматом навчального відео [2]. При викладанні математичних та фізичних дисциплін скрінкасти є досить зручним інструментом, оскільки дозволяють не лише демонструвати послідовне викладення навчального матеріалу на віртуальній дошці та озвучувати пояснення до нього, але також паралельно використовувати за необхідності стандартні пакети прикладних математичних програм (Derive, Eureka, Matlab, MathCad, Mathematica), що дають можливість виконувати типові математичні операції у числовому та символьному виді.

Зважаючи на невисокий рівень математичної підготовки здобувачів освіти, що спостерігається останнім часом, а також на особливості сприйняття даних сучасним поколінням, найбільш доцільно надавати перевагу мультимедійним матеріалам з використанням віртуальної дошки та графічного планшету. У цьому випадку викладення матеріалу найбільш наближене до звичної роботи викладача в аудиторії біля дошки, коли матеріал викладається поступово, створюючи для студентів з високим рівнем знань можливість «передбачити» наступний крок, а також з детальними поясненнями усіх математичних перетворень для кращого сприйняття матеріалу студентами, які мають значні прогалини у знаннях з математики та фізики. У роботі [3] розглянуто використання різноманітних сервісів, що спираються на візуалізацію даних, а також переваги використання функції дошки, що реалізується у багатьох програмних засобах для проведення відеоконференцій. Підкреслено, що для повноцінної роботи необхідно використовувати графічний планшет, який підключається до комп'ютера і сумісний з такими застосунками як Word, Paint та PowerPoint. Це дозволяє створювати якісні наочні матеріали, зберігати їх та, за потреби, надсилати студентам. Практика показує, що за умови використання згаданих програмних та технічних засобів, а також високої мотивації до навчання і достатнього рівня шкільної математичної підготовки здобувачі освіти непогано справляються з опануванням фізико-математичних дисциплін, що викладаються дистанційно [3, с. 60].

Отже, для забезпечення якості освітнього процесу при навчанні фізико- математичних дисциплін доцільно застосовувати сучасні програмні та технічні засоби, зокрема, скрінкасти, як один з найбільш зручних та ефективних форматів навчального відео.

Література:

1. Вембер В.П., Бучинська Д.Л. Сучасні типи навчального відео та особливості їх використання у навчальному процесі // Освітологічний дискурс, 2016, № 1 (13). С. 19-29.
2. Литвин Ольга Як зробити навчальне відео ефективним? // Центр навчальних та інноваційних технологій УКУ [Електронний ресурс] / Режим доступу: http://ceit-blog.ucu.edu.ua/ed-tech/yak-zrobyty-navchalne-video- efektyvnym/
3. Кудзіновська І., Трофименко В. Використання візуальних технічних засобів для дистанційного навчання математичних дисциплін // Розвиток сучасної освіти і науки: результати, проблеми, перспективи. Том XII: Якісні дослідження для покращення життя людини: XII Міжнар. наук.-практ. конф.,22 квітня 2022 р.: тези доп. – Конін – Ужгород – Перемишль: Посвіт, 2022. –С. 59-61.

Мовчан А. В.,
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ІНТЕРПОЛУ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Важливе значення для підвищення ефективності діяльності правоохоронних органів України у протидії злочинності має взаємодія з міжнародними правоохоронними організаціями, зокрема Інтерполом та Європолом. В інформаційній системі Інтерполу використовується 19 банків даних з інформацією про злочини та злочинців, які доступні в реальному часі країнам-членам Інтерполу. Формування цих банків даних здійснюється за рахунок інформації, яку надають правоохоронні органи

держав-членів Інтерполу на добровільних засадах. Право власності на цю інформацію належить виключно тим державам, які її надали.

У Генеральному секретаріаті Інтерполу створені та функціонують наступні банки даних:

1. *Особи:*

1) банк даних «Особи» (ASF Nominal database) – містить інформацію про відомих міжнародних злочинців, зниклих осіб та невпізнані трупи з історією їх злочинів, фотографіями, відбитками пальців тощо.

Крім того, Генеральний секретаріат за допомогою системи I-24/7 надає доступ до банку даних циркулярних повідомлень Інтерполу. Департамент міжнародного поліцейського співробітництва Національної поліції на підставі отриманого від правоохоронного органу України запиту чи звернення забезпечує використання інформаційної системи Інтерполу шляхом надсилання запиту про публікацію Генеральним секретаріатом Інтерполу оповіщень: червоне оповіщення (RED NOTICE) – «розшукується»; синє оповіщення (BLUE NOTICE) – «встановлення місцезнаходження»; зелене оповіщення (GREEN NOTICE) – «попередження»; чорне оповіщення (BLACK NOTICE) – «невпізнаний труп»; жовте оповіщення (YELLOW NOTICE) – «зниклий безвісти»; пурпурне оповіщення (PURPLE NOTICE) – «спосіб злочину»; помаранчеве оповіщення (ORANGE NOTICE) – «безпосередня загроза»; оповіщення про викрадені культурні цінності – «культурні цінності».

Повідомлення публікується лише у тому випадку, якщо воно відповідає Статуту Інтерполу та умовам для обробки інформації, визначеним Правилами обробки даних;

2) банк даних порнографічних зображень, створених із залученням неповнолітніх (INTERPOL Child Abuse Image database), дозволяє ідентифікувати зображення порнографічного характеру за «авторством» та місцем розміщення в мережі Інтернет. Міжнародний банк даних зображень та відео щодо сексуальної експлуатації дітей (ICSE) – це інструмент розвідки та розслідування, який дозволяє спеціалізованим слідчим ділитися даними про випадки сексуального насильства над дітьми. Використовуючи програмне забезпечення для порівняння зображень та відео, слідчі можуть миттєво встановити зв'язок між жертвами, зловмисниками та їх місцезнаходженням.

2. *Криміналістика*. Відбитки пальців, профілі ДНК та розпізнавання осіб можуть зіграти вирішальну роль у розкритті злочинів, оскільки вони можуть встановити зв'язок між особами та/або місцями вчинення злочинів. Не менш важливо, що вони можуть допомогти довести невинуватість підозрюваного, зокрема:

1) банк даних відбитків пальців рук (Fingerprints database) – містить набори відбитків пальців рук, вилучені з місць вчинення злочинів на території держав-членів Інтерполу та від злочинців і сліди злочинів з місця подій, що подаються державами-членами в електронному вигляді або поштою. Уповноважені користувачі в країнах-членах Інтерполу можуть переглядати, подавати та перехресно перевіряти записи в банку даних відбитків пальців за допомогою автоматизованої системи ідентифікації відбитків пальців (AFIS);

2) банк даних ДНК-профілів (DNA Profiles database) – створений в 2002 році банк даних містить інформацію про профілі ДНК, вилучені з місць вчинення злочинів на території держав-членів Інтерполу та від злочинців. До профілю, який подається у вигляді буквено-цифрового коду, не додаються персональні дані;

3) I-Familia. Метою I-Familia є виявлення зниклих безвісти осіб у всьому світі за допомогою відповідності сімейної ДНК. Його рушійний принцип – гуманітарний: возз'єднати близьких або закрити справу;

4) система розпізнавання обличчя забезпечує спеціальну платформу для зберігання та перехресної перевірки зображень з метою ідентифікації втікачів, зниклих безвісти осіб та осіб, що представляють оперативний інтерес. Система розпізнавання осіб Interpol Facial Recognition System (IFRS) містить зображення обличчя, отримані з більш ніж 179 країн, що робить її унікальною глобальною базою даних про злочини. У поєднанні з автоматизованим програмним забезпеченням для біометричного використання ця система здатна ідентифікувати або перевірити людину шляхом порівняння та аналізу візерунків, форм та пропорцій рис та контурів обличчя.

3. *Банк даних викрадених/втрачених документів* (ASF Stolen/Lost Travel Documents and Stolen Administrative Blank Documents database) – містить інформацію про викрадені/втрачені ідентифікаційні документи, а також викрадені/втрачені бланки адміністративних документів, які використовуються для ідентифікації об'єктів, а саме:

1) викрадені та загублені проїзні документи (SLTD) – зберігаються дані про втрачені, викрадені та анульовані проїзні документи – такі як паспорти, посвідчення особи, пропуски ООН або візові штампи, включаючи викрадені бланки проїзних документів;

2) викрадені адміністративні документи (SAD) – містить дані про викрадені офіційні документи, які служать для ідентифікації об'єктів, наприклад, документи про реєстрацію транспортних засобів та сертифікати оформлення для імпорту/експорту;

3) підроблені документи – цифрова бібліотека сповіщень Interpol - Document (Dial-Doc) – дозволяє країнам ділитися на світовому рівні попередженнями, що готуються на національному рівні, щодо нових виявлених форм підробки документів;

4) порівняння справжніх та фальшивих документів – електронна система документації та інформації про мережі розслідувань (Едісон) надає приклади справжніх проїзних документів, щоб допомогти виявити підробку.

4. *Викрадене майно*. Викрадені транспортні засоби, плавзасоби та твори мистецтва можуть бути переправлені через кордони. Глобальні банки даних Інтерполу допомагають правоохоронним спільнотам у виявленні викрадених речей та збільшують шанс на їх повернення, зокрема:

1) банк даних викрадених транспортних засобів (ASF Stolen Vehicles database) – містить інформацію про транспортні засоби, викрадені на території держав-членів Інтерполу;

2) банк даних викрадених плавзасобів (ASF Stolen Vessels database) – банк даних викрадених плавзасобів служить централізованим інструментом для відстеження та встановлення викрадених плавзасобів та двигунів до них;

3) банк даних викрадених творів мистецтва (ASF Stolen Works of Art) – містить інформацію щодо творів мистецтва, предметів антикваріату, інших культурних цінностей, викрадених на території держав-членів Інтерполу.

5. *Торгівля вогнепальною зброєю*. Три потужні інструменти допомагають країнам-членам Інтерполу збирати й аналізувати інформацію, яка може бути отримана як всередині, так і ззовні країни, з метою запобігання та розкриття злочинів, пов'язаних із вогнепальною зброєю, а саме:

1) довідкова таблиця вогнепальної зброї Інтерполу «Ідентифікація вогнепальної зброї» являє собою інтерактивний онлайн-інструмент, який забезпечує стандартну методику для виявлення і опису вогнепальної зброї більш точно, таким чином вони можуть бути простежені в транскордонних дослідженнях;

2) автоматизована система «Розшук вогнепальної зброї» – система управління документацією Інтерполу про незаконне озброєння та управління відстеженням зброї (iARMS), яка забезпечує централізовану платформу для звітності, запитів та трасування втраченої, викраденої зброї, незаконної торгівлі або контрабанди вогнепальної зброї правоохоронними органами у всьому світі;

3) балістична інформаційна мережа Інтерполу (IBIN) «Порівняння балістичних даних» – це єдина масштабна платформа для міжнародного обміну та порівняння балістичних даних, яка дозволяє здійснювати пошук зв'язків між злочинами в різних країнах.

6. *Мережі організованої злочинності*. Метою банку даних «Мережі організованої злочинності» є покращення збору та обміну розвідувальними даними, підтримка розслідувань та кращий аналіз злочинних мереж, що може призвести до ідентифікації та арешту їх керівників та фінансистів.

7. *Морське піратство*. Банк даних «Морське піратство» зберігає інформацію, пов'язану з випадками піратства та збройного пограбування на морі, включаючи дані про фізичних осіб, номери телефонів, адреси електронної пошти, випадки піратства, місцезнаходження, підприємства та фінансову інформацію [1].

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу здійснюється: безпосередньо, в режимі on-line – через телекомунікаційну систему Інтерполу I-24/7 або шляхом надсилання запиту до Генерального секретаріату Інтерполу.

Отже, використання інформаційних систем Інтерполу має важливе значення для підвищення ефективності діяльності оперативних підрозділів Національної поліції у сфері протидії злочинності.

Література:

1. Офіційний веб-сайт Інтерполу URL: https://www.interpol.int/

Огірко І. В.,
професор кафедри інформаційних та мультимедійних технологій Української академії друкарства
доктор фізико-математичних наук, професор

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА

Рівень сучасних технологій та виробництв сприяє стрімкій глобалізації та розвитку інформаційних та комунікаційних технологій, що у свою чергу налагоджує процес міжнародної співпраці у різних сферах. Проте виникає велика кількість загроз та зростає потреба забезпечення інформаційної безпеки. Актуальність цієї теми обумовлена тим, що в сучасних умовах саме розвиток інформаційних технологій та рівень інформаційної кібербезпеки будуть визначати місце держави на міжнародномій арені. Найближчим часом залежність всіх сфер діяльності суспільства та держави від інформаційних систем буде тільки зростати і вимагати підвищення якості новітніх технологій.

Раціональне управління інформаційною безпекою сприяє зростанню рівня конкурентоспроможності країни на світовому ринку, а також зростанню економічного потенціалу держави. Питання забезпечення інформаційної безпеки як складової національної безпеки та безпеки підприємства розглядають зарубіжні та вітчизняні вчені. У своїх роботах вони здебільшого приділяють увагу таким питанням як: безпека комп'ютерних та інформаційних систем; забезпечення міжнародної інформаційної безпеки; забезпечення інформаційної безпеки держави та підприємств; ефективність інформаційної безпеки. Проте невирішеними залишаються питання зв'язку інформаційної кібербезпеки, а саме: вплив інформаційних факторів.

Стрімка глобалізація суспільства сприяє зростанню значення інформаційної безпеки як для міжнародної спільноти, держави в цілому, так і окремо для секторів економіки, для підприємств та особистості. Впровадження та позповсюдження новітніх технологій посприяло тому, що інформація перетворилася на економічну категорію, стала одним з найважливіших елементів ринку та фактором. Інформаційні впливи можуть спричиняти результат не відразу, а через тривалий час. Визначальним фактором життєдіяльності сучасного суспільства стає глобалізація інформаційних ресурсів.Тому важливими на цей час є питання, що належать до інформаційної сфери. А отже виникає необхідність забезпечення та регулювання інформаційної безпеки різних сфер дільності.

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство. Міжнародна інформаційна безпека - характеризується, як взаємодія учасників міжнародних відносин для підтримання тривалого миру на основі захисту світового кіберпростору разом із засобами масової інформації, глобальної інфраструктури та суспільної свідомості від реальних інформаційних загроз.

Інформаційна безпека, як складова національної безпеки – стан захищеності життєво важливих інтересів людини, суспільства і держави, коли запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека, як складова безпеки підприємства – діяльність керівництва підприємства з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує нормальне функціонування розвиток підприємства. Але інформаційна безпека на сьогодні це не лише забезпечення безпеки інформації, яка зберігається на електронних носіях, серверах чи персональних пристроях.

Також інформаційна безпека регулюється рядом наступних міжнародних стандартів та норм: CoBiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IES 15408. Варто зазначити, що механізми управління інформаційною безпекою суттєво відстають у розвитку від сучасного рівня інформатизації, що сприяє зростанню рівня кіберзлочинності, яка у свою чергу спричиняє важкі, а іноді й незворотні наслідки для держави, підприємства, суспільства, особи. У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов'язані з використанням інформації, яка міститься в

комп'ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем.

Література:

1. M. E. Whitman, H. J. Mattord, Principles of Information Security, Cengage Learning, Boston, USA, 2021. URL: https://inlnk.ru/XO3VB0
2. D. Pereira, J. F. Ferreira, A. Mendes, Evaluating the Accuracy of Password Strength Meters using Off-The-Shelf Guessing Attacks, in: Proceeding of 2020 IEEE International Symposium on Software Reliability Engineering Workshops(ISSREW), Coimbra, Portugal, 2020, pp. 237-242. doi: 10.1109/ISSREW51248.2020.00079.

Пекарський С. П.,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ПРОГРАМНО-ЦІЛЬОВОГО МЕТОДУ В ІНФОРМАЦІЙНОМУ ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ КРИМІНАЛЬНОЇ ПОЛІЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Розвиток інформаційно-комунікативних технологій надав можливість оперативним підрозділам, в тому числі підрозділам кримінальної поліції Національної поліції України використовувати сучасні програмно-апаратні засоби отримання, обробки та використання інформації з метою виконання завдань визначених Законами України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про національну безпеку», «Про національний спротив» тощо.

В попередні року, в умовах протидії незаконним збройним формуванням проросійських терористів, відбулися заходи щодо впровадження Концепції Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року (далі Концепція – прим. автора), яка була схвалена розпорядженням Кабінету Міністрів України від 6 лютого 2013 р. № 51-р. В різних містах запрацювали сучасні системи безпеки, під якими розуміємо сукупність високотехнологічних програмно-апаратних засобів з можливістю підвищення їх функціонального потенціалу та збільшення потужності [1]. Означені програмно-апаратні засоби призначені для моніторингу, фіксації зображення, передавання інформації про стан громадського порядку і публічної безпеки, що забезпечує невідкладне оповіщення та швидке реагування на ситуації, пов'язані з вчиненням правопорушення або виникненням надзвичайної події. В Концепції надано визначення засобам зовнішнього контролю (спостереження), під якими розуміємо технічне обладнання (відеокамери, відеореєстратори), включаючи пристрої екстреного виклику, за допомогою яких здійснюється відеоспостереження у місцях, що потребують постійного нагляду, або передається інформація відповідним підрозділам правоохоронних органів з метою швидкого реагування [1].

Отже, в Концепції зазначено, що розроблення і запровадження ефективних сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та організація швидкого реагування є нагальним питанням державної політики у сфері забезпечення охорони громадського порядку та громадської безпеки, у тому числі запобігання проявам тероризму.

Ефективність застосування таких систем підтверджується зарубіжним досвідом правоохоронної діяльності. Зокрема, використання систем відеоспостереження в країнах Європейського Союзу та США значно сприяє оперативності реагування на правопорушення, швидкому встановленню осіб, які їх вчиняють. Застосування зазначених систем стримує потенційного правопорушника від вчинення протиправних дій навіть за відсутності поліцейського.

На тепер, у різних областях та територіальних громадах йде процес впровадження сучасних систем безпеки, під якими розуміємо сукупність високотехнологічних програмно-апаратних засобів з можливістю підвищення їх функціонального потенціалу та збільшення потужності, які призначені для моніторингу, фіксації зображення, передавання інформації про стан публічного порядку і громадської безпеки. В подальшому це забезпечує невідкладне оповіщення та швидке реагування на ситуації,

пов'язані з вчиненням правопорушення або виникненням надзвичайної події (приклад – рух військової колони агресора, прим. автора).

В умовах воєнного стану на території Донецької області свою ефективність показала система «Безпечне місто», яка передбачає використання засобів зовнішнього контролю (спостереження), тобто технічного обладнання (відеокамер, відеореєстраторів). В громадах області також впроваджені пристрої екстреного виклику, за допомогою яких здійснюється відеоспостереження у місцях, що потребують постійного нагляду, або передається інформація територіальним підрозділам поліції з метою оперативного реагування. Під оперативним реагуванням розуміємо скоординовані дії чергової служби, нарядів патрульної поліції, ГРПП та інших нарядів, спрямовані на організацію невідкладного прибуття працівників поліції до заявника або на вказане місце події з метою припинення правопорушення, установлення особи та затримання ймовірного правопорушника, збереження слідів правопорушення, а також надання допомоги потерпілим особам у межах повноважень поліції [2].

Тому, в умовах воєнного стану, на нашу думку одним із пріоритетних завдань є застосування програмно-цільового методу та концентрації зусиль підрозділів кримінальної поліції під час проведення стабілізаційних заходів на деокупованих територіях. Зокрема, нагальною є робота з програмними комплексами з метою покращення якості відео- та фото-зображень під час фіксації руху транспорту, громадян, або під час перевірки транспортних засобів та громадян на блокпостах [3; 4; 5], за місцем мешкання чи перебування тощо.

Отже, діяльність підрозділів кримінальної поліції в умовах воєнного стану з використання інформаційно-аналітичного забезпечення та програмно-цільового методу дозволяє своєчасно виконувати загальні завдання, які стоять перед силами оборони та безпеки, а також силами національного спротиву.

Література:

1. Концепція Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року: схвалена розпорядженням Кабінету Міністрів України від 6 лютого 2013 р. № 51-р.
2. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: затв. наказом МВС України від 27 квітня 2020 року № 357.
3. Методичні рекомендації «Дії на блокпосту (контрольно-перепускному пункті)» (за досвідом проведення ООС(раніше АТО). Центр оперативних стандартів і методики підготовки Збройних сил України спільно з Головним управлінням підготовки Збройних сил України. 2019 р. 76 с.
4. Організація і тактика несення служби на блокпостах в умовах антитерористичної операції : метод. рек. / С. В. Албул, О. Т. Ніколаєв, А. О. Шелехов. Одеса : ОДУВС, 2014. 34 с. - з іл.
5. Методичні рекомендації «Дії на блокпосту (контрольно-перепускному пункті)» (за досвідом проведення ООС (раніше АТО). – Київ: «Центр учбової літератури», 2022. 72 с.

Питель М. В.,
здобувач вищої освіти факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

Рудий Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технычних наук, доцент

ПАРАДИГМИ ПРОГРАМУВАННЯ

Американський вчений Роберт Флойд під час вручення йому Тьюрінгової медалі ACM 1978 року виступив з лекцією "Парадигми програмування", термін "парадигми" став часто вживаним у програмуванні, а тому варто зупинитися на ньому окремо.

В імперативному програмуванні виокремлюють парадигми програмування, які можуть підтримуватися або не підтримуватися мовами програмування. Парадигми програмування – це моделі, які відтворюють спосіб мислення розробника програми [1].

Розглянемо три основних наказових парадигми – процедурне, об'єктне (модульне) і об'єктно-орієнтоване (ієрархічне) програмування (рис. 1).

На рис. 2 подано мови програмування, які зробили суттєвий внесок у розбудову сучасних парадигм. Так, мова програмування ФОРТРАН (*FORmule TRANslator* – перекладач формул) уперше розв'язала проблему автоматизації програмування математичних формул, а її компілятори уперше впоралися із задачею роздільного компілювання.

Мова програмування АЛГОЛ (*ALGOrithmic Language* – алгоритмічна мова), у якій було запроваджено блокову структуру програми, стала першою мовою структурного програмування із сучасними розгалуженнями і циклами. Майже одночасно з'явилися дві інші знакові мови програмування – Паскаль і С, які дотримувалися майже діаметрально протилежних підходів. Мова програмування С не передбачала стандарту обчислювача, а навпаки, містила засоби налаштовування програми на конкретне обчислювальне середовище.

Проблема складності програмування на основі процедурної парадигми стимулювала пошук нових підходів. Так з'явилася концепція абстрактних типів даних як способу об'єднання даних і засобів їхнього оброблення та одночасно, як методу відокремлення специфікацій (інтерфейсів) від їх реалізування. Типи даних Паскалю були розвинуті в абстрактні типи даних у вигляді модулів мови МОДУЛА-2.

Особливо важливий крок було зроблено внаслідок залучення до мови С засобів мови моделювання СІМУЛА (*SIMUlation Language* – мова моделювання), в якій вперше з'явилися класи і об'єкти. З цього союзу виникла мова програмування С++, яка сама пройшла еволюційний шлях вдосконалень і розвитку. Цій темі присвячена одна з книг автора С++ Б'єрна Страуструпа.

Рис. 1. Парадигми імперативного програмування

Відзначимо, що хоча мова МОДУЛА-2 не набула широкого розповсюдження, закладені в ній ідеї призвели до розширення мови Паскаль класами та об'єктами. Так під назвою Object Pascal виникла об'єктна версія мови Паскаль, реалізована в системі програмування Delphi. Зрештою, назву Delphi одержала й сама мова програмування, яка продовжила давню традицію конкуренції між Паскалем і С.

Головне досягнення С++ полягає у зміні парадигми програмування (*paradigm shift*) з процедурної на об'єктно-орієнтовану, яка визначає стандарт розроблення програмного забезпечення. Головним доробком об'єктно-орієнтованої парадигми стала ієрархічність програмних структур, яка відтворюється в агрегації об'єктів та успадкуванні класів.

Водночас властивість ієрархічності дала змогу об’єднувати програмні структури у складні архітектурні конструкції, максимально використовуючи наявний код, налагодження якого тепер не потребує перепрограмування.

Основу структурного програмування складає поєднання теорії програмування та особистого досвіду висококваліфікованих програмістів з урахуванням сучасних вимог до програм та промислового характеру їх створення. Головною вимогою, якій повинна відповідати програма – працювати у повній відповідності до специфікації та адекватно реагувати на довільні дії користувача. Окрім того, розроблення програми повинно завершитися у встановлені терміни і надавати можливість внесення необхідних змін і доповнень.

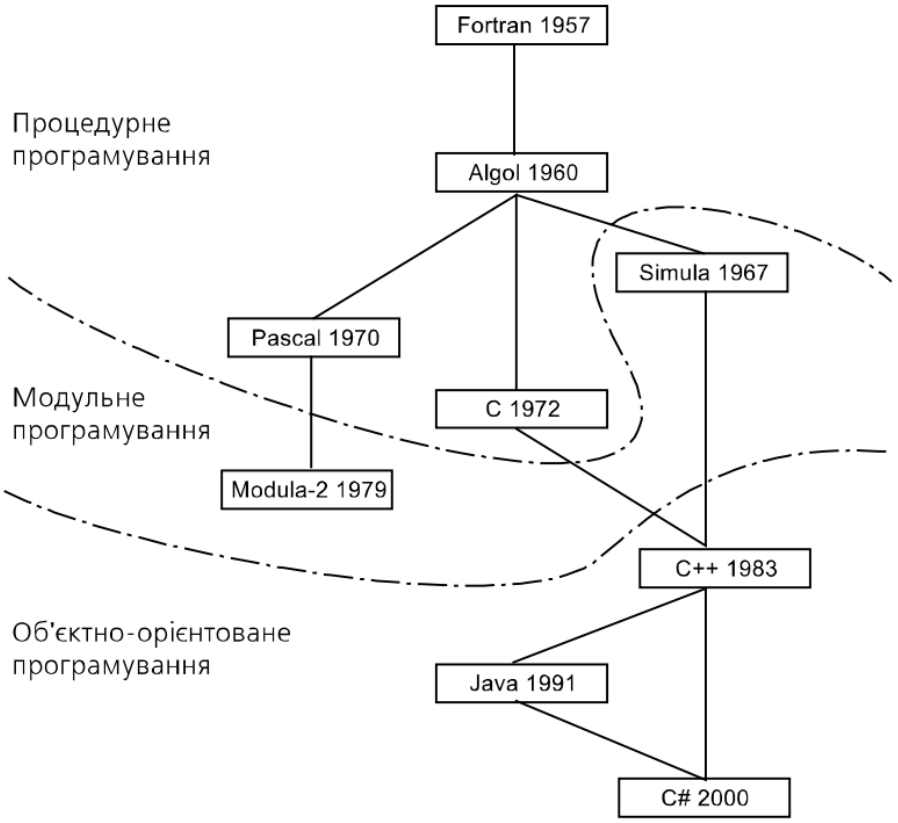


Рис. 2. Хронологія мов і парадигм програмування

Структурне програмування – це технологія створення програм, яка охоплює усі етапи проєкту – специфікацію, проєктування, тестування.

Отож, структурне програмування – методологія й технологія розроблення поважних програмних проєктів, яка об'єднує способи розроблення структури програми, зручної для читання та розуміння людиною, стеження за логікою її роботи, внесення до неї виправлень та інших змін. Згідно з думкою Н. Вірта, "структуризація є принциповим інструментом, яка допомагає програмісту систематично аналізувати і синтезувати складні програми, зберігаючи про них повне уявлення". Ідеї структурного програмування з'явилися на початку 1970-х роках у компанії IBM, у її розробленні брали участь відомі вчені Е. Дейкстра, Х. Милі, Є. Батіг, С. Хоор.

Структурне програмування базується на таких основних принципах: тпрограмування має здійснюватися зверху-униз; вся програма розв'язання складної задачі має бути поділена на модулі з одним входом і одним виходом (оптимальний розмір модуля – кількість рядків, які поміщається на екрані дисплея); логіка алгоритму й програми має допускати тільки три основні структури: послідовне виконання, розгалуження й повторення (недопустиме передавання керування в довільну точку програми); при розробленні коду програми супровідна документація має створюватися одночасно із програмуванням, у вигляді коментарів до неї.

Процедурне програмування. Процедурне програмування зображає програму у вигляді набору алгоритмів, для оформлення яких можуть бути застосовані іменовані програмні блоки – процедури та функції. В останньому випадку передбачено наявність механізмів передавання параметрів і повернення результату.

Структурне програмування (не зовсім вдалий переклад англійського *structured programming* – структуроване програмування) – це варіант процедурного, що використовує лише три типи структур керування: послідовне виконання дій, розгалуження і цикл. Не дивно, що Фортран не підтримував цю парадигму: в наборі його засобів не було циклів за умовами.

Професор Ніклаус Вірт, автор мови програмування Паскаль, відібрав до неї лише прості в поясненні й легкі в реалізуванні конструкції. Внаслідок сильної типізації програми на Паскалі відзначаються високою надійністю, закладена в них концепція Паскаль-машини робить їх мобільними, їх легко читати і розуміти завдяки дисципліні програмування, яка продиктована вжитою парадигмою.

Головним критерієм, застосованим Д. Річі до створеної ним мови С, стала саме гнучкість використання особливостей конкретної апаратури та ефективність виконання програм.

Об’єктне (модульне) програмування. Процедурна парадигма віддала належне алгоритмічній компоненті програмування. Але зі зростанням обсягу програм і складності даних з’явилася нова проблема, а саме проблема структурної організації даних, найбільш влучно висловлена Віртівською формулою: "алгоритми + структури даних = програми" [2].

Поняття модуля як абстракції даних було вперше запропоноване Девідом Парнасом у 1972 році [3].

Головна ідея модульності даних полягає в забезпеченні доступу до них і оперування ними незалежно від способу їхнього конкретного кодування у пам’яті комп’ютера. Самі дані разом із процедурами їх оброблення вбудовують (інкапсулюють) в окрему одиницю програми. Ось простий приклад, який демонструє, як складність обчислень може перетікати у складність даних.

Модулі мають дві головні риси. По-перше, вони об’єднують структури даних з алгоритмами їхньої оброблення. По-друге, у них відокремлено специфікацію від реалізації інкапсульованих у модулі конструкцій, і це перетворює модуль на так званий абстрактний тип даних (abstract data type), на що свого часу звернув увагу Джон Гуттаг [1].

Об'єктно - орієнтоване програмування (ООП) – це модель програмування яка базується на стверджені того, що програма це сукупність об’єктів які взаємодіють між собою. Кожен об’єкт в цій моделі є незалежним, і він здатний отримувати, обробляти дані та відправляти ці дані іншим об’єктам. В ООП використано моделі успадкування, модульності, поліморфізму та інкапсуляції [1].

Основним поняттям ООП є об'єкт. Об'єкт можна визначити як певну сукупність даних (характеристик об'єкта) та методів роботи з ними. Для класифікації об'єктів у ООП використовують класи. Клас служить зразком для створення об’єкту, тобто об'єкт є нічим іншим, ніж копією класу.

Кожен об'єкт має процедури і функції, які служать для роботи з даними об'єкта. Ці процедури і функції називаються методами.

Існування ООП можливе завдяки трьом основним парадигмам на яких базується саме ООП.

Інкапсуляція. Також відома як приховування даних. Зміст інкапсуляції полягає у приховуванні від зовнішнього користувача деталей реалізації об'єкта, замість цього надаючи інтерфейс взаємодії з ним.

Успадкування. Це означає, що об'єкти (класи) можуть переймати деякі властивості у своїх прабатьків. Як? Це залежить від тієї мови, на якому пишеться програма. Однак у будь-якому випадку картина та ж: це призводить до повторного використання вже написаного одного разу коду. Підкласи успадковують атрибути та поведінку своїх батьківських класів, і можуть мати нові власні атрибути. Тобто утворюється ієрархія з класів, де від основного класу (так званого, предка) походять усі інші класи.

Поліморфізм означає залежність поведінки від класу, в якому ця поведінка викликається, тобто, два або більше класів можуть реагувати по різному на однакові повідомлення. Це спричинене зміною в одного з класів якогось методу (процедури, функції), шляхом запису іншого алгоритму. Як приклад, деяка комп'ютерна програма при натисканні клавіші Esc завершить роботу, інша ж програма після натискання кнопки Esc тільки відкриє меню даної програми.

Література:

1. Бублик В.В. Об’єктно-орієнтоване програмування: Підручник / В.В. Бублик. – К.: ІТ книга, 2015. – 624 с.
2. Н. Вирт, Алгоритмы + структуры данных = программы. Москва, Мир, 1985, 198 с.
3. D. Parnas, On the Criteria To Be Used in Decomposing Systems intoModules, Communications of the ACM, 1972, vol. 15, № 12, 1972, pp.1053–1058.

Підхомний О. М.,
професор кафедри фінансів, грошового обігу і кредиту Львівського національного університету імені Івана Франка, доктор економічних наук, професор

Ревак І. О.,
професор кафедри соціально-гуманітарної підготовки Львівського державного університету внутрішніх справ, доктор економічних наук, професор

ФОРМУВАННЯ МОДЕЛІ БАЗИ ДАНИХ ДЛЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗШУКУ АКТИВІВ

Розшук активів часто стає актуальним напрямом інформаційно-аналітичної роботи при розгляді багатьох кримінальних і цивільних справ. Відповідні розслідування можуть бути у провадженні як державних органів, так і суб'єктів підприємництва, що займаються інформаційно-аналітичною діяльністю. Дуже часто розшук активів виходить за межі однієї юрисдикції. У подібних розслідуваннях необхідно брати до уваги широке коло джерел інформації та юридичних особливостей їхнього використання у різних країнах.

Належна організація роботи з великими обсягами даних у процесі розшуку активів має вирішальне значення. Це стосується налагодження документообігу і фіксації результатів розслідування у відповідних базах даних. Складність побудови баз даних, що слугують для інформаційного забезпечення процесу розшуку активів, зумовлена багатоаспектністю даної проблематики [2]. Адже потрібно фіксувати дані про самі активи, які є предметом розшуку, факти переміщення, обміну та зміни форми цих активів, інформацію про фізичних і юридичних осіб, які пов'язані з такими активами, а також злочини, що стосуються таких активів. Окремим об'єктом уваги є самі носії інформації про відповідні процеси та явища. Серед таких носіїв інформації можна виділити документи, виявлені учасниками інформаційно-аналітичної роботи та документи, створені самими учасниками пошукового процесу для фіксування проміжних і кінцевих результатів.

Не завжди відомо, які саме активи є предметом пошуку. Активи можуть змінювати свою форму в процесі відмивання, нелегальні доходи можуть перемішуватись із легальними, буває важко заздалегідь оцінити способи та засоби фінансування тероризму, масштаби та сфери обходу санкцій.

Розшукувані активи можуть мати різний ступінь вираження унікальних ознак. Приміром, викрадені твори мистецтва та інші культурні цінності досить чітко ідентифікуються, тоді як безготівкові гроші при переказах між різними рахунками з подрібненням та перемішуванням сум не мають попредметної ідентичності. Не можна однозначно обґрунтувати, що конкретна безготівкова гривня має легальне або нелегальне походження. У таких ситуаціях аналіз можливо проводити лише за узагальненими сумами зі встановленням відповідності між певною сумою нелегальних доходів та вартістю тих чи інших активів на кінцевих або призупинених правоохоронними органами етапах відмивання.

Потрібно здійснити непростий вибір пріоритетного типу об'єктів дослідження в процесі розшуку активів, навколо яких має певними чином упорядковуватись інформація про інші аспекти розслідування. На роль центральних інформаційних елементів можуть претендувати відомості про: 1) власне активи; 2) осіб, які пов'язані з цими активами; 3) сукупність дій щодо відповідних активів; 4) документи, в яких відображена інформація про відповідні активи, дії щодо них, осіб, які ці дії вчиняють.

На перший погляд найбільш актуальною є дилема, пов'язана з активоцентричним та суб'єктоцентричним підходами. Однак активоцентричний підхід передбачає наявність повної інформації про певний актив, його переміщення та правовий статус у різних ситуаціях його існування. Такий рівень інформованості є певним ідеалом, який не завжди досяжний навіть на кінцевих етапах розслідування. Подібно до цього окрема фізична чи юридична особа може бути пов'язана з широким колом інших осіб та активів із різним правовим статусом. Дослідження всіх цих зв'язків і характеристик є надто трудомістким і далеко не завжди виправданим у процесі розслідування окремого злочину чи пошуку конкретного активу або сукупності взаємопов'язаних активів, наприклад, колекції культурних цінностей. Окремий документ, які б не були його обсяги, зазвичай, не містить повного та всебічного відображення досліджуваної проблеми. Тому документоцентричний підхід також не є ефективним.

Відповідно роль базового поняття у процесі розшуку активів має належати «епізоду». Окреме розслідування можна розглядати як дослідження одного епізоду або низки взаємопов'язаних епізодів. Зміст окремого епізоду може полягати у привласненні, переміщенні, зберіганні, даруванні, знищенні тощо окремого активу або їх колекції. Навколо окремого епізоду можна формувати відомості про активи, осіб, документи та інші епізоди. Така комплексна інформація дає підстави для правової кваліфікації відповідного епізоду та визначає орієнтири щодо можливостей розслідування наступних або попередніх епізодів (наприклад, перехід від розслідування відмивання до розслідування злочину, що став джерелом доходів). Адже не можна виключати ситуації, що в конкретному епізоді сліди, які необхідні для подальшого пошуку активів, перериваються. У такому разі доцільно прийняти такий невтішний висновок, щоб не витрачати ресурси на розслідування, яке немає перспектив. Інші підходи, а саме активо-, суб'єкто-, документоцентричний, не забезпечують такого рівня чіткості оцінок щодо перспективності тих чи інших напрямів розслідування.

Якщо активи, особи, документи, які пов'язані з актуальним епізодом, мають належні ідентифікатори та відображені у базі даних, якою володіють учасники розслідування або інших доступних їм базах даних, то інформацію про відповідні елементи можна використовувати для доповнення знань про даний епізод та його зв'язки з іншими епізодами. Враховуючи складність зв'язків між зазначеними сутностями, можна зробити висновок про незручність використання табличної форми, а отже, й баз даних реляційного (SQL) типу, для зберігання інформації, що стосується розшуку активів та пов'язаних із ним розслідувань. Серед типів нереляційних (NoSQL) баз даних найзручнішим для вирішення відповідних проблем видається графовий тип. Вершинами графу будуть виступати епізоди, активи, особи, документи та різноманітні їх характеристики. Наприклад, фізична особа може мати податковий код, номер соціального страхування, номери телефонів, адреси проживання та електронної пошти, номер криптогаманця тощо. Такі характеристики можуть бути проміжними ланками, які виводять на інші епізоди, що вже розслідувані, чи потребують розслідування. Концепція графу тісно пов'язана з можливостями візуалізації зв'язків між сутностями, що стосуються проблематики дослідження. Відомо чимало універсальних та спеціалізованих програмних засобів візуалізації зв'язків між різними елементами та їх характеристиками, які актуальні в процесі розслідування [1].

Практика розшуку активів певного виду з часом дає змогу виділити сукупність досить обмеженого кола характеристик та їх варіантів, в тому числі критеріїв ризику, для окремих видів досліджуваних елементів: епізодів, активів, фізичних та юридичних осіб, офіційних і неофіційних документів. Графовий тип відповідних баз даних можна вважати основним, що зовсім не виключає його поєднання з іншими типами нереляційних баз даних за результатами дослідження та фахового обговорення специфічних проблемних ситуацій у сфері розшуку активів.

Література:

1. 6 Asset Tracing Tools For Financial Fraud Investigators In 2023. URL: https://personable.com/6-asset-tracing-tools-for-financial-fraud-investigators/
2. Maclay A., Rees M., Pan M. Data analytics and data visualisation in asset tracing: Evolving approaches to transaction analysis and communication. URL: https://www.forensicrisk.com/wp-content/uploads/2020/03/CDR_Fraud-Asset-Tracing-Recovery_Data-analytics-and-data-vis-in-asset-tracing_2020_AM-MR-MP.pdf

Рижков Е. В.,
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВСТАНОВЛЕННЯ КОЛАБОРАНТІВ

Перед початком повномасштабного вторгнення росії в Україну в державі спостерігались досить двозначні тенденції у питані ефективної оборони держави та захисту її населення від проявів тероризму

з боку агресора. Заводи з виготовлення снарядів та патронів не будувались, кримінальні провадження щодо державних зрадників та проявів сепаратизму належним чином не розслідувались, на керівні посади у правоохоронній сфері призначались особи із проросійськими поглядами та зв'язками тощо.

У законотворчий політиці мали місце факти нівелювання потенційних загроз державності та приниження вагомості патріотизму через намагання декриміналізації колаборантських намірів, проявів та конкретних вчинків. За сім років від початку військового протистояння було написано два проекти закону з цього питання: перший, «Про заборону колабораціонізму (№ 6170)» подала до Верховної Ради група депутатів («Народний фронт») у 2017 році. У 2019 році проект був відкликаний; другий, «Про захист української державності від проявів колабораціонізму (№ 7425)» подала група розробників також у 2017, і його було відкликано 2019-го [1].

Реальні зміни у політиці державних та правоохоронних структур почалися після констатації світовою спільнотою, що по відношенню до українського народу в процесі ведення війни ворог припускається відвертих проявів геноциду. І тільки навесні 2022 року колаборантські прояви були остаточно криміналізовані у вітчизняному кримінальному законі [2].

Встановлення колаборантів та фактів їх діяльності необхідно проводити в рамках документування складу злочину, що передбачено статтею 111-1. Колабораційна діяльність Кримінального кодексу України.

Задля забезпечення збирання доказової бази необхідно здійснити відпрацювання інформаційного контенту у глобальних та соціальних мережах у відношенні до конкретних осіб та за конкретними фактами.

У період війни така діяльність буде найбільш ефективною за умов здійснення вдалої співпраці представників Національної поліції зі Службою безпеки України та військовими. У кожного з зазначених суб'єктів є своє розуміння щодо проведення оперативних комбінацій, в т.ч. пов'язаних із оглядом змісту гаджетів та доступу до акаунтів. Такі заходи у період воєнного стану можуть проводитись з максимальною ефективністю на випередження до знищення даних та контенту потенційними колаборантами після нашої перемоги.

На сьогодні крім спеціалізованих відомчих підсистем, призначених для службового користування у загальному доступі маємо інформаційну базу «Миротворець» та цілу череду чат-ботів, розроблених за ініціативою не тільки правоохоронних органів але й Міністерства цифрової трансформації України та НАЗК [3].

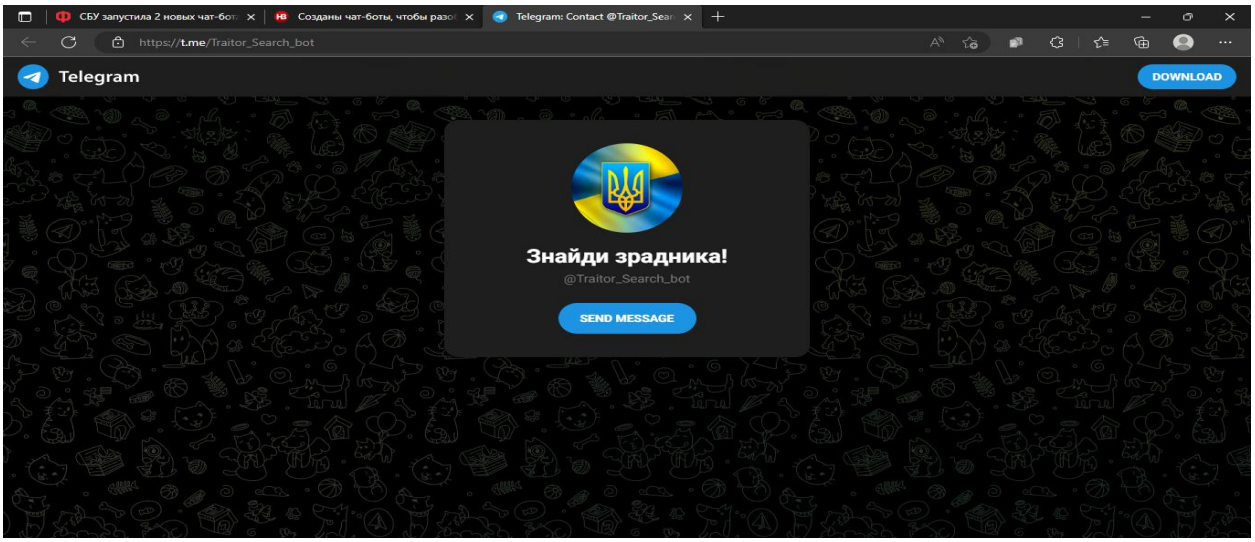
Статистика, яка подається для суспільного загалу за останні місяці, свідчить про позитивну тенденцію щодо виявлення таких осіб та фактів їх діяльності [4]. Проте, кількість їх відносно мала у співвідношенні до кількості громадян України, які перебували чи перебувають на тимчасово окупованих територіях з 2014 року. З огляду на обсяги підривної діяльності з боку росії аксіоматичним є те, що робота з такого виявлення повинна проводитись на всій території України не тільки зараз, але й протягом наступних років.

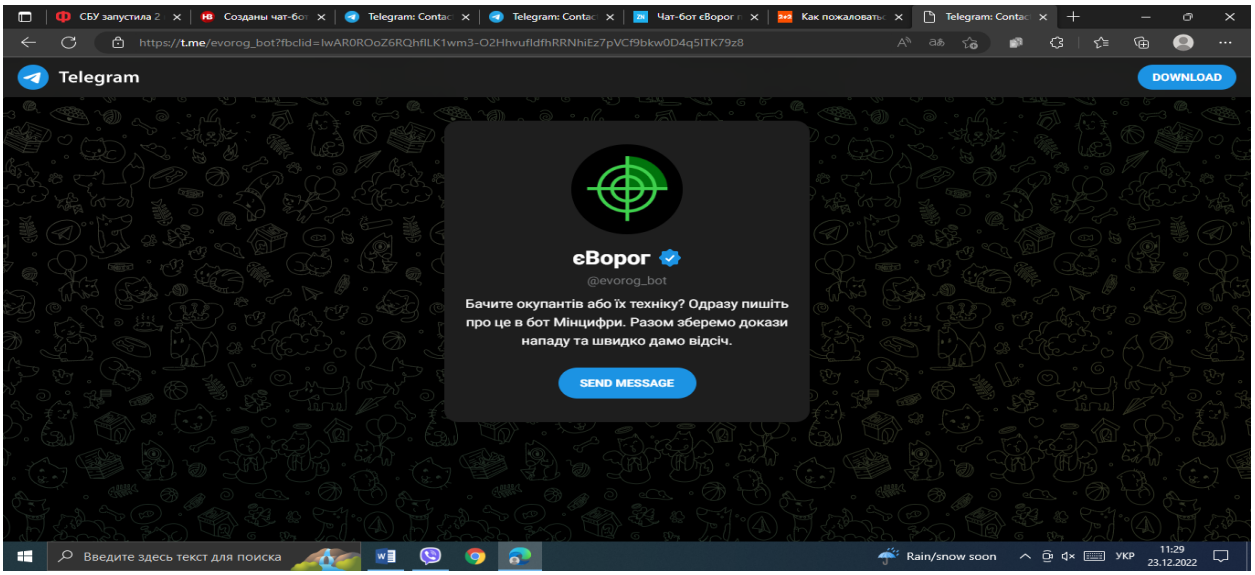
Представники громадськості також створюють спеціалізовані інформаційні площадки задля формування бази даних відносно потенційних колаборантів [5].

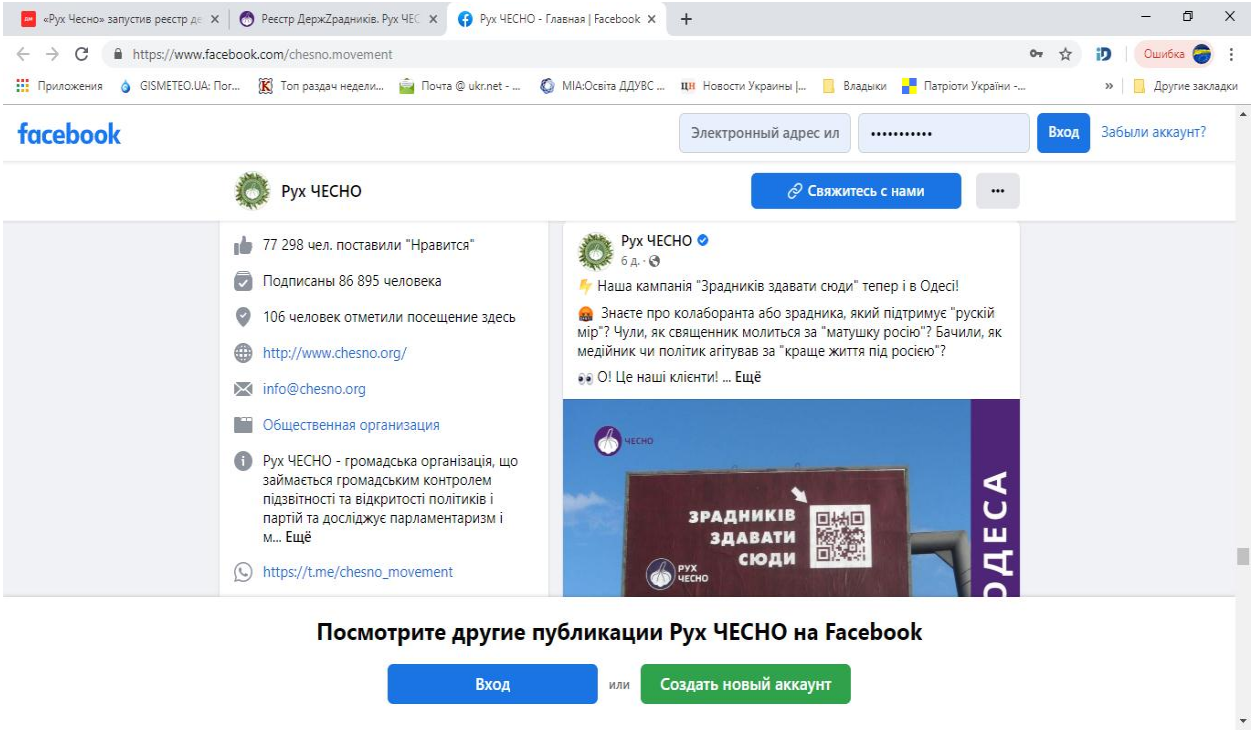
Доцільно звернути увагу на те, що громадські активісти розпочали цю роботу за середини березня 2022 року. Тоді як підрозділи Національної поліції спроміглися на таку ініціативу лише у листопаді 2022 року [6].

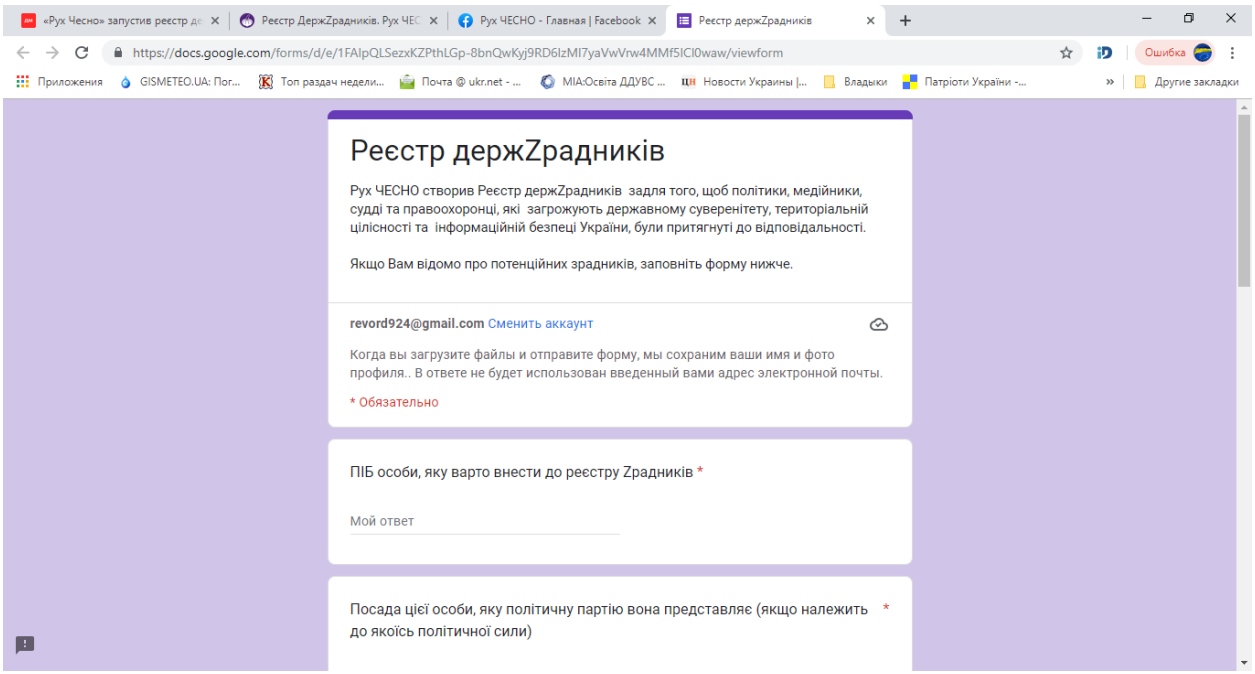
Можливо, саме тому, відпрацьовуючи інформаційний контент фігурантів, доцільно починати з самих працівників правоохоронних органів [7]. Бо наслідки діяльності саме цих осіб створюють підвищену суспільну небезпеку [8].

Таким чином, слід констатувати, що з 2014 року робота щодо притягнення до відповідальності осіб, які в той чи інший спосіб перейшли на бік країни-агресора мала формальний характер і не може, на наш погляд, бути визнана задовільною, бо у свою чергу створила більш сприятливі умови для повномастабного вторгнення в Україну у 2022 році.


Telegram
DOWNLOAD
Знайди зрадника!
@Traitor_Search_bot
SEND MESSAGE


Telegram
DOWNLOAD
єВорог
@evorog_bot
Бачите окупантів або їх техніку? Одразу пишіть про це в бот Мінцифри. Разом зберемо докази нападу та швидко дамо відсіч.
SEND MESSAGE


facebook
Рух ЧЕСНО
Свяжитесь с нами
77 298 чел. поставили "Нравится"
Подписаны 86 895 человека
106 человек отметили посещение здесь
http://www.chesno.org/
info@chesno.org
Общественная организация
Рух ЧЕСНО - громадська організація, що займається громадським контролем підзвітності та відкритості політиків і партій та досліджує парламентаризм і м... Ещё
https://t.me/chesno_movement
Рух ЧЕСНО
Наша кампанія "Зрадників здавати сюди" тепер і в Одесі!
Знаєте про колаборанта або зрадника, який підтримує "рускій мір"? Чули, як священник молиться за "матушку росію"? Бачили, як медійник чи політик агітував за "краще життя під росією"?
О! Це наші клієнти! ... Ещё
ЗРАДНИКІВ ЗДАВАТИ СЮДИ
Посмотрите другие публикации Рух ЧЕСНО на Facebook
Вход
или
Создать новый аккаунт



Разом з тим, безумовним позитивом є те, що за 9 місяців активної фази війни у інформаційному полі держави створені зручні та доступні для небайдужих громадян інструменти фіксації відповідної інформації та закладено фундамент задля проведення ефективної роботи щодо формування баз даних потенційних колаборантів і зрадників. Ця робота потребує активного інформаційного супроводу, роз'яснення та популяризації серед всіх верств населення з метою нейтралізації за допомогою інформаційних технологій представників п'ятої колони в середині країни.

Література:

1. Почему Украина отказывается от слова «коллаборанты»? URL: https://www.radiosvoboda.org/a/kolaboratsiya-pokarannya-mizhnarodne-pravo/31076292.html
2. Закон України Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колаборaційну діяльність. URL: https://zakon.rada.gov.ua/laws/show/2108-20
3. Чужие среди своих: как сообщить про коллаборанта за несколько кликов в чат-боте. URL: https://2plus2.ua/ru/novyny/chuzhi-sered-svoih-yak-povidomiti-pro-kolaboranta-u-dekilka-klikiv-u-chatboti; СБУ запустила 2 новых чат-бота для выявления коллаборантов и мародеров. URL: https://focus.ua/digital/514350-sbu-zapustila-2-novyh-chat-bota-dlya-vyyavleniya-kollaborantov-i-maroderov; НАЗК створило реєстр ймовірних зрадників України. URL: https://detector.media/infospace/article/197674/2022-03-19-nazk-stvorylo-reiestr-ymovirnykh-zradnykiv-ukrainy/;
4. В Минцифры рассказали о количестве заявок на коллаборантов, поданных через бот «єВорог». URL:https://zn.ua/TECHNOLOGIES/v-mintsifry-rasskazali-o-kolichestve-zajavok-na-kollaborantov-podannykh- cherez-bot-jevoroh.html
5. «Рух Чесно» запустив реєстр держзрадників. URL: https://detector.media/infospace/article/197490/2022-03-14-rukh-chesno-zapustyv-reiestr-derzhzradnykiv/ Реєстр держЗрадників. URL: https://docs.google.com/forms/d/e/1FAIpQLSezxKZPthLGp8bnQwKyj9RD6lzMl7yaVwVrw4MMf5ICl0waw/viewform
6. Нацполиция запускает чат-бот для сообщений о коллаборантах. URL: https://ukranews.com/news/898014-natspolitsiya-zapuskaet-chat-bot-dlya-soobshhenij-o-kollaborantah
7. У Куп'янську затримано колаборанта-поліцейського. URL: https://ua.korrespondent.net/city/kharkov/4546543-u-kupiansku-zatrymano-kolaboranta-politseiskoho; Колишнього та діючого працівників СБУ спіймали на держзраді — Офіс генпрокурора. URL: https://www.ukrinform.ua/rubric-regions/3284950-kolisnogo-ta-diucogo-pracivnikiv-sbu-spijmali-na-derzzradi-ofis-genprokurora.html; Президент позбавив звань генералів двох зрадників із Служби безпеки. URL: https://lb.ua/society/2022/04/01/511827_prezident_pozbaviv_zvan_generaliv.html

8. Рижков Е. В., Манченко Є. А. Протидія корупції в органах внутрішніх справ //Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2015. – №. 3. – С. 19-24.

Селецька Л. Є.,
здобувач вищої освіти факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДОПОВІДЕЙ, ПІДГОТОВЛЕНИХ З ВИКОРИСТАННЯМ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ

На сьогоднішньому етапі розвитку інформаційного суспільства роль мультимедіа технологій з кожним днем зростає. Мультимедійний комп'ютер, проникаючи у всі галузі життєдіяльності людини, стає універсальним інструментом. Спостерігається це у всіх сферах діяльності, де необхідно якісно та ефективно передавати за одиницю часу більші обсяги інформації.

Мультимедіа технології – один з перспективних напрямів інформаційних технологій, що найбільш активно розвиваються. На етапі інформатизації суспільства впровадження мультимедіа технологій та їх використання в освітньому процесі є одним із основних факторів інформатизації освіти.

Розглянемо поняття "мультимедіа", що характеризують особливості, визначимо роль мультимедіа технологій в освітньому процесі.

У літературі поняття «мультимедіа» визначається як комп'ютерна інформаційна технологія, яка дозволяє в комп'ютерній системі об'єднати різні види інформації як текст, звук, музику, відео, графіку та анімацію, так і зв'язати їх у єдиному цифровому поданні [1].

Також зустрічаються підходи до розуміння «мультимедіа» як «мультимедіапродукту» (програми) і як обладнання, що працює з різною інформацією (мультимедіа комплекси та центри).

Засоби мультимедійних технологій прийнято ділити на два класи: засновані на взаємодії та їх застосуванні. Перша категорія включає засоби синхронного, асинхронного взаємодії, онлайн режим. До другої категорії належать різні віртуальні об'єкти, відео та аудіо фрагменти, анімаційна графіка тощо.

У мультимедійних ресурсах інформація:

- представлена в єдиній цифровій формі, де міститься у різних поєднаннях різні її види (текст, звук, графіка, відео тощо);
- організована з використанням гіпертексту та гіпермедіа;
- відрізняється інтерактивністю, що дозволяє взаємодіяти користувачеві з цим об'єктом, ресурсом чи програмою [2].

Внаслідок одночасного впливу на користувача різного виду інформації (графічної, звукової та візуальної) мультимедійні ресурси мають великий емоційний заряд.

Найважливішими цілями застосування мультимедіа в освітньому процесі є перехід від знаної педагогіки до компетентнісної, розвиток та формування творчих здібностей студентів через інтерактивність, яка відкриває нові пізнавальні можливості.

Використання мультимедіа реалізує на більш ефективному та якісному рівні один із принципів дидактики – принцип наочності. Метод мультимедійної візуалізації навчального матеріалу можна як новий, якісніший наочний метод навчання. Надані наочні образи об'єктів, процесів або явищ, що вивчаються, у поєднанні з інтерактивністю, є основним джерелом знань і головним засобом пізнання даного методу навчання. А емоційне і чуттєве сприйняття мультимедійних образів, що надаються, та інтерактивні дії над ними ведуть до більш міцного засвоєння досліджуваного матеріалу [1].

Модернізація та генерування нових форм та методів навчання вимагають розширення застосування мультимедіа технологій в освіті. Подібний підхід дозволяє, індивідуалізуючи процес здобуття знань, підвищити ефективність занять та побудувати абсолютно нову систему.

Психологами встановлено, що у методу сприйняття інформації люди діляться на кілька типів. Одні краще сприймають інформацію візуально, інші – за допомогою слуху, а третій – при практичному

застосуванні. Схильності, можливості та швидкість обробки інформації, що надходить із зовнішнього середовища, у всіх різні.

Створення необхідного середовища, де навчальний матеріал сприймається на слух і водночас візуально, значно підвищує ефективність розуміння дисципліни. Неоціненним також є і впровадження віртуальних лабораторій, які дозволяють студентам взяти участь безпосередньо в різних експериментах.

Зазначається у літературі й існування можливих негативних аспектів застосування мультимедійних засобів навчання, які необхідно врахувати студентам. До них можна віднести недостатню доступність матеріалу, розсіювання уваги, можливу відсутність зворотного зв'язку та ряд інших аспектів [3].

Таким чином, використання засобів мультимедіа в навчальному процесі дозволяє значно підвищити ефективність та результативність процесу навчання за рахунок візуалізації тих моментів, які інакше педагогу довелося б описувати вербально, інтерес здобувачів освіти до дисципліни, що вивчається, досягти більшої глибини розуміння та розширення меж сприйняття ними навчального матеріалу, розвитку пізнавальних здібностей та мислення.

Література:

1. Ларіонов Володимир, "Мультимедійні технології як засіб підвищення якості освіти." Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: педагогічні науки 26. 2021. с. 82-96.
2. Моца А. А. Інноваційні технології навчання у вищій військовій освіті України: практичне застосування. Воєнні науки. Міжнародний науковий журнал “Інтернаука”. 2017. № 5(27). С. 26–34.
3. Полюга Галина. "Використання мультимедійних технологій у навчальному процесі ВНЗ". Наукові записки Тернопільського національного педагогічного університету. Серія: педагогіка 8. 2015. с. 59–63.

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету №2 Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету "Львівська політехніка" , кандидат технічних наук, доцент

АНАЛІЗ ЗАСТОСУВАННЯ ДИСТАНЦІЙНОЇ ФОРМИ НАВЧАННЯ ПІД ЧАС ЇЇ ЗАСТОСУВАННЯ У 2021-2022, 2022-2023 НАВЧАЛЬНИХ РОКАХ У ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

Вимушений перехід на дистанційну форму навчання у Львівському державному університеті внутрішніх справ, як і у інших закладах вищої освіти, обумовлювався у 2021–2022, 2022–2023 навчальних роках двома факторами: по-перше, зростанням захворюваності серед населення у Львівському регіоні на Covid-19; по-друге, початком повномасштабного російського вторгнення наприкінці лютого 2022 року.

Які загальні висновки можна висловити за результатами аналізу вимушено проведеного навчання у дистанційній формі? У загальному випадку, усі проблеми, переваги та недоліки такого навчання можна поділити на три категорії: 1) зі сторони здобувача вищої освіти; 2) зі сторони виконання науково-педагогічним працівником своїх обов’язків; 3) спільні переваги та недоліки.

Проведені дослідження дозволяють стверджувати, що зі сторони здобувача вищої освіти основна зручність дистанційного навчання полягає у тому, що він особисто визначає для себе час та його тривалість на виконання завдань. При цьому тривалість цього часу легко збільшується за рахунок часу, який затрачається для того, щоб добратися до та із закладу вищої освіти. Особливо, якщо цей час займає понад одну годину в одну сторону. Можемо констатувати, що така перевага забезпечує можливість для здобувачів вищої освіти навчатися індивідуально, у власному темпі.

Здобувач вищої освіти завжди може повернутися до вивчення складніших питань, а відомий матеріал може пропускати. Окрім цього дистанційне навчання дозволяє здобувачу вищої освіти економити накладні витрати пов'язані із транспортом та проживанням. Важливою перевагою для здобувача вищої освіти також є можливість створення власної, зручної, спокійної побутової обстановки для навчання.

Зі сторони науково-педагогічного працівника безумовною перевагою є індивідуальний підхід. Під час традиційного навчання науково-педагогічному працівнику досить важко приділити необхідну кількість часу усім здобувачам вищої освіти у групі, підлаштуватися під темп роботи кожного. Тому, використання дистанційних технологій є зручним інструментом для організації індивідуального підходу. Далі, науково-педагогічний працівник може урізноманітнити форми подання матеріалу, проявити гнучкість у його підготовці, проводити заняття із зручної локації, що також сприяє підвищенню якості викладання навчальної дисципліни.

Спільними перевагами дистанційного навчання є: а) постійна доступність до усієї необхідної, і що важливо, актуальної літератури, яку здобувач вищої освіти отримує через систему дистанційного навчання, електронну бібліотеку, інформаційні ресурси мережі Інтернет (зникає проблема нестачі чи відсутності підручників, навчальних посібників, інших навчально-методичних матеріалів; б) мобільність – зв'язок із науково-педагогічним працівником може здійснюватися як on-line, так і off-line (проконсультуватися з викладачем за допомогою електронної пошти іноді ефективніше та швидше, ніж очікувати зустріч під час його графіка чергувань чи консультацій).

Поряд з переліченими перевагами дистанційного навчання у процесі його проведення у 20021–2022, 2022–2023 навчальних роках виявлено і ряд недоліків.

Зі сторони здобувача – дистанційне навчання позбавляє здобувачів вищої освіти навчатися командної роботи, комунікабельності, можливості працювати над спільними проєктами. Підготовка до командної роботи є одним із важливих аспектів підготовки фахівців.

Зі сторони науково-педагогічного працівника встановлено, що під час проведення семінарських, практичних чи лабораторних занять є проблема ідентифікації здобувача вищої освіти. Нині найефективніший спосіб простежити за тим, чи здобувач вищої освіти самостійно здає матеріал – це застосування відеоспостереження, що, як показує практика, не завжди є можливим. Сюди ж можна віднести ідентифікацію здобувача вищої освіти під час виконанням ним індивідуальних завдань, математичних задач, тестів тощо. Дана проблема стосується без виключення усіх навчальних дисциплін.

Спільними ж недоліками дистанційної форми навчання є підтримання науково-педагогічним працівником та здобувачем вищої освіти власної мотивації до навчання. Це пов'язано із тим, що значний обсяг навчального матеріалу здобувач вищої освіти має засвоювати самостійно. Така ситуація потребує відповідної сили волі, відповідальності і самоконтролю.

І, зрештою, ефективність дистанційної форми навчання багато у чому залежить від якості роботи інформаційно-телекомунікаційних систем, в першу чергу мережі Інтернет, що, як показує практика, не завжди є належному рівні. А також забезпеченістю здобувачів вищої освіти відповідною власною комп'ютерною технікою з необхідними технічними характеристиками та програмним забезпеченням. Також слід зауважити, що під час дистанційної форми навчання у 2021–2022, 2022–2023 навчальних роках відбувалися зриви занять через оголошення повітряних тривог.

Підсумовуючи, слід зазначити наступне, аналіз навчального процесу у 2021–2022, 2022–2023 навчальних роках у Львівському державному університеті внутрішніх справ показав – дистанційна форма навчання в окремих випадках є доволі ефективним інструментом, яка має право на існування та застосування. Насамперед це стосується проведення лекційних занять, консультацій, семінарських та практичних занять за окремими темами. Поряд з цим, вважаємо, що слід провести додаткові дослідження результатів використання дистанційного навчання за окремими освітньо-професійними програмами.

Сеник С. В.,
доцент кафедри європейського права факультету міжнародних відносин Львівського національного університету імені Івана Франка, доктор філософії у галузі права

Микієвич Л. М.,
здобувачка освітнього ступення магістр юридичного факультету Львівського національного університету імені Івана Франка

ОСНОВНІ ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ В УКРАЇНІ

Інформаційні права людини – це гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації. Гарантоване Конституцією України право на інформацію стає все більш важливим для існування демократичного суспільства. Та не варто ототожнювати право на інформацію й інформаційні права людини. Інформаційні права і свободи людини та громадянина становлять цілісний екзистенціальний феномен, який можна пізнати виключно крізь призму їхніх системних властивостей, що проявляється у наявності прав і свобод інформаційного характеру у різних сферах життєдіяльності суспільства. Тому доцільно говорити про інформаційні права і свободи людини та громадянина в екологічній сфері, економічній сфері, політичній сфері, управлінській сфері тощо, які корелятивно поєднані і в своїй інтегративній сукупності становлять систему інформаційних прав і свобод. Адже поява інших сфер життєдіяльності суспільства не змінює сутності цього феномена. Нині будь-які суспільні відносини проявляються через інформацію, інформаційну сферу. Можна стверджувати, що інформаційні права і свободи є в будь-якій сфері життєдіяльності суспільства. «Право на інформацію» та «інформаційні права» – поняття нетотожні.

Поняття «інформаційні права і свободи людини та громадянина» є ширшим поняттям, оскільки охоплює не лише можливість «вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, на свій вибір» або навіть «можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів», а це усі права і свободи людини і громадянина, що мають інформаційний характер [1].

Основним нормативно-правовим актом у сфері є Конституція в нормах якої закріплено, що:

1) цензура заборонена (ст.15);

2) кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції винятки можуть бути встановлені лише судом (ст. 31);

3) не допускається збирання, зберігання, використання та поширення конфіденціальної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ст. 32);

4) кожен громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе, які не є державною або іншою захищеною законом таємницею (ст. 32);

5) кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів та переконань (ст. 34);

6) кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ст. 34);

7) усі мають право направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);

8) кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (ст. 50);

9) кожному гарантується свобода творчості(ст. 54) та ін.

Деякі конституційні положення також мають відношення до інформаційних прав і свобод (наприклад, статті 21, 24, 23, 35, 53). Зрозуміло, що Конституція України [2] закріплює основний зміст прав і свобод в інформаційній сфері, але їх конкретизація відображається в низці інших нормативно-правових актів.

Література:

1. Собків Я. М. Класифікація інформаційних прав і свобод людини та громадянина. URL: http:// goal-int.org/klasifikaciya-informacijnixprav-i-svobodlyudini-ta-gromadyanina.
2. Конституція України від 28 червня 1996 року. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

Сибірна Р. І.,
професор кафедри теоретичної психології Львівського державного університету внутрішніх справ;
професор кафедри кримінального права і процесу Національного університету «Львівська політехніка», доктор біологічних наук, професор

Сибірний А. В.,
доцент кафедри загальної гігієни з екологією Львівського національного медичного університету імені Данила Галицького, кандидат біологічних наук, доцент

СУЧАСНЕ ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРАВОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сьогодні завдяки новим інформаційним технологіям щодо передачі, отримання, зберігання та переробки інформації, юридична діяльність значно раціоналізувалася. Юридичні питання електронного документообігу, користування мережею Internet, застосування криптографічних засобів і цифрової готівки, забезпечення таємниці та захисту даних стало повсякденною діяльністю сучасних юристів, готових до перспективи розвитку та впровадження інформаційних технологій у всі сфери своєї діяльності.

Як відомо, правові системи належать до класу інтелектуальних систем, які виконують операції, імітуючи інтелектуальну діяльність людини - дії та розумові висновки людей у нестандартних ситуаціях, коли схема, алгоритм розв'язування задачі, що постала перед фахівцем, апріорі невідомі. Інтелектуальні системи забезпечують розв'язування неформалізованих задач користувача в певній предметній галузі та організовують його взаємодію з комп'ютером у звичних поняттях, термінах, образах. Отже, правові системи призначені для розв'язування задач на основі наданих знань, що містять інформаційну базу і підтримують функції обґрунтування, пояснення та виправдання [1, с. 82–85].

Основною відмінністю інтелектуальних систем від інших є те, що в них об'єктом нагромадження, зберігання, оброблення, передавання та використання є не дані, а знання як сукупність фактів, закономірностей, відношень та евристичних правил, що відображає рівень обізнаності з проблемами деяких предметних галузей [2, с.112-127].

Можна визначити такі напрями застосування інтелектуальних систем і технологій у галузі права:

- інтелектуалізація автоматизованих інформаційно-пошукових систем із законодавства;
- створення автоматизованих систем аналізу нормативних правових текстів;
- побудова консультативних систем із правотворення;
- створення експертних систем у сфері правозастосовної діяльності;
- розробка алгоритмів і програм ідентифікації за допомогою ЕОМ об'єктів при розслідуванні та розгляді судових справ (сфера криміналістики й судової експертизи).

Окремою сферою застосування експертних систем є прийняття рішення про напрямок розслідування і виконання слідчих дій. Вирішення великої кількості правових завдань залежить від якості результатів інформаційного пошуку – вибору з усієї відомої сукупності документів, текстів, відомостей, фактів і даних тих елементів, які відповідають інформаційним потребам. За умов великих обсягів інформації, серед якої здійснюється пошук, стає доцільним і, навіть, необхідним використання інформаційно-пошукових систем.

Серед наявних комп'ютерних правових систем України слід виділити:

1. Спеціалізована інформаційно-пошукова система «ЛІГА:ЗАКОН» (розробка інформаційно-аналітичного центру «Ліга»). Система складається з програмної оболонки, яка забезпечує пошук документів, та інформаційного ядра – текстових баз даних нормативних документів.

2. Правова інформаційно-пошукова система «Нормативні акти України», реалізація якої здійснюється трьома мовами.

3. Мережа Інтернет – найбільший світовий інформаційний ресурс, що містить практично всю інформацію, якою може зацікавитись людина. Використовуючи пошукові системи Інтернет, потрібно враховувати наступні фактори, що впливають на результативність пошуку:

- кожна пошукова система Мережі має свою спеціалізацію;
- пошук здійснюється не за повними текстами документів, а за їх пошуковими образами, причому кожна система має оригінальний механізм роботи з ключовими словами. Зокрема, якщо база даних системи невелика, то до неї записується більше термінів, в іншому разі у пошуковий образ документа відбираються «найвагоміші» ключові слова [1; 4, с. 278].

За останні роки технології пошуку інформації в Інтернет змінились завдяки пошуковим агентам, що являють собою програми, розміщені у певному середовищі і здатні до гнучкої автономної поведінки для досягнення визначеної мети. Агент не тільки сприймає імпульси від середовища, в якому він функціонує, а й може змінювати його. У користувача не має необхідності втручатись у роботу агента, контролювати його дії або внутрішній стан. Гнучкість агента виявляться у його проактивності, здатності до змін і взаємодії з користувачами та іншими агентами.

Агенти, що їх позначають як інтелектуальні, можуть вести спостереження і здійснювати вимірювання, керувати комп'ютерними мережами, передавати повідомлення, сортувати електронну пошту. Програмні агенти змінюють людино-машинний інтерфейс та на їх основі розробляються інтерактивні персонажі, з якими можна спілкуватись і радитись.

Пошукові агенти мають такі переваги порівняно зі звичайним зверненням до пошукових систем:

- пошуковий агент передає користувачеві не просто результати роботи пошукової машини, а й попередньо переглядає документи і вибирає з-поміж них найбільш релевантні з його погляду;
- агент може налаштовуватись на переваги користувача, враховувати обмеження на пошук;
- деякі агенти можуть працювати в off-line режимі – користувач дає завдання агенту і відключається від мережі, а агент виконує завдання на сервері та передає результати користувачеві, як тільки він знову підключиться. Агенти можуть бути настроєні на пошук за розкладом – шукати інформацію щогодини, щодня, щотижня, щомісяця і т. д. Ця можливість корисна, наприклад, при пошуку новин, інформації, яка постійно оновлюється або постійно потрібна в роботі;
- агенти можуть навчатись – користувач оцінює роботу агента, а той може скоректувати свої критерії відбору інформації, враховуючи ці оцінки [5, с.90].

Таким чином, пошукові агенти можуть розглядатись як інтелектуальна надбудова над пошуковими машинами.

На даний час на Web-сервері Верховної Ради України функціонує система «Закони та підзаконні акти України в Інтернет». Сайт має такі розділи: Конституція України, законодавство України, законопроекти, пленарні засідання, депутатський корпус, інформаційний сервер Верховної Ради, бібліотека Верховної Ради, уповноважений Верховної Ради з прав людини, міжнародні парламентські інститути, сайти парламентів зарубіжних країн, сторінки депутатських фракцій і груп.

Таким чином, інформаційні технології на сучасному етапі розвитку суспільства є невід'ємною часткою діяльності юриста. Володіння спеціалізованими інформаційними системами для обробки інформації, робота з базами даних, застосування локальних та глобальних мереж, робота з графічними об'єктами та системами є необхідними у професійній юридичній діяльності.

Створення єдиного інформаційного суспільства та ефективне проведення процесів, пов'язаних з інформатизацією, потребують удосконалення правового регулювання інформаційних відносин та принципів формування інформаційного права, які визначають систему соціальних норм і відносин та охороняються державою у сфері виробництва, перетворення та споживання інформації. [3, с. 56].

Ефективність інформатизації суспільства залежить від рівня вирішення проблем правового, наукового, методологічного та організаційного їх забезпечення. Важливим і актуальним напрямом законодавчої роботи у сфері інформатизації є об'єднання державних і недержавних інформаційних

ресурсів, мереж і систем в єдину загальнодержавну систему національних інформаційних ресурсів та формування державної системи правової інформації.

Отже, глобальним завданням сучасної юриспруденції є створення ефективної системи національного законодавства у сфері інформаційних відносин та проведення правової інформатизації із застосуванням інформаційно-телекомунікаційних систем для формування, накопичення, обробки, організації і надання користувачеві масивів соціально-правових інформаційних ресурсів з метою сприяння вдосконалюванню правової системи держави і світового правопорядку.

Література

1. Денісова О. О. Інформаційні системи і технології в юридичній діяльності: навч. посіб., Київ: КНЕУ, 2004. С. 78-95.
2. Береза А. М. Основи створення інформаційних систем: навч. посібник. Київ: КНЕУ, 2004. С. 112-127.
3. Кісельов М. Про створення єдиної інформаційної системи органів юстиції України. Право України. 1997. № 3. С. 53-57.
4. Ситник В. Ф. та ін. Основи інформаційних систем: навч. посіб. Київ: КНЕУ. 2001. 420 с.
5. Трінтіна Н. А., Котелевець С. Є. Інформаційні технології в юридичній діяльності. *Фізико-математична освіта*. 2021. Випуск 1(27). С. 89-93.

Хром'як І. В.,
здобувач вищої освіти факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

Зачек О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНИХ ПІДСИСТЕМАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Згідно з ст. 25 Закону України «Про Національну поліцію» поліція може створювати власні реєстри та бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень [1]. Під час формування та використання таких реєстрів та баз даних, а особливо таких, що формуються під час здійснення оперативно-розшукової діяльності, важливу роль відіграє система захисту інформації. Адже злочинці дуже прагнуть отримати інформацію про діяльність поліції, а особливо про оперативно-розшукову діяльність.

Під системою захисту інформації в інформаційних системах розуміють єдиний комплекс правових норм, організаційних заходів, технічних, програмних і криптографічних засобів, які забезпечують захищеність інформації у інформаційних системах у відповідності до прийнятої політики інформаційної безпеки [2, с. 4]. Одним з важливих елементів системи захисту інформації є саме криптографічний захист.

Криптографічний захист – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Засіб криптографічного захисту інформації – програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації. Криптографічна система (криптосистема) – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається [3].

За призначенням засоби криптографічного захисту інформації поділяються на наступні категорії:

- призначені для шифрування інформації;

- призначені для виготовлення ключових даних або ключових документів та управління ключовими даними;
- призначені для забезпечення захисту цілісності чи неспростовності інформації;
- призначені для надання електронних довірчих послуг та виконання функцій засобу кваліфікованого електронного підпису чи печатки;
- призначені для захисту від несанкціонованого доступу, у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки;
- спеціально призначені для розроблення, дослідження, виробництва та випробувань засобів криптографічного захисту інформації та криптографічних модулів [4].

Система криптографічного захисту інформації – сукупність органів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми і засоби криптографічного захисту інформації. Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації. Для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають сертифікат відповідності [3].

За дією на вихідну інформацію методи криптографічного захисту інформації поділяють на 4 групи: шифрування, стеганографія, кодування та стиснення. Процес шифрування полягає у проведенні зворотних математичних, логічних, комбінаторних та інших перетворень вихідної інформації, в результаті яких зашифрована інформація являє собою хаотичний набір букв, цифр, інших символів і двійкових кодів [2, с. 19].

Сучасні методи шифрування повинні відповідати наступним вимогам:

- стійкість шифру протистояти крипто аналізу (криптостійкість) повинна бути такою, щоб розшифрування могло бути здійснене шляхом вирішення завдання повного перебору ключів;
- криптостійкість повинна забезпечуватися не секретністю алгоритму шифрування, а секретністю ключа;
- шифротекст не повинен суттєво перевищувати за обсягом вихідну інформацію;
- помилки, що виникли під час шифрування, не повинні призводити до спотворення і втрати інформації;
- час шифрування не повинен бути довгим;
- вартість шифрування повинна бути співставлень з вартістю інформації, яка зашифровується.

Основним показником ефективності є криптостійкість, яка визначається часом чи вартістю засобів, які необхідні криптоаналітику для розшифрування інформації [2, с. 20].

Згідно Положення про Національну поліцію України Національна поліція відповідно до покладених на неї завдань забезпечує в межах повноважень, передбачених законом, криптографічний захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої визначена законом [5].

Тому, розробка методів та засобів криптографічного захисту інформації, які задовільняють всім вимогам, і спроможні надійно захистити інформацію, яка міститься у інформаційних підсистемах Національної поліції України, є важливою задачею державної ваги.

Література:

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.
2. Сеник В.В. Технології захисту інформації : методичні рекомендації для здобувачів вищої освіти юридичних та економічних спеціальностей / В. В. Сеник, Т. В. Рудий, Т. В. Магеровська. – Львів, ЛьвДУВС. – 2018. – 92 с.
3. Указ Президента України від 22 травня 1998 року № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні». [Електронний ресурс]. URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=505%2F98#Text (дата звернення: 11.12.2022).

4. Технічний регламент засобів криптографічного захисту інформації. [Електронний ресурс]. URL: https://www.kmu.gov.ua/storage/app/uploads/public/601/286/214/60128621415cd223194591.pdf (дата звернення: 11.12.2022).
5. Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877 «Про затвердження Положення про Національну поліцію України». [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text (дата звернення: 11.12.2022).

Чернобров В. В.,
здобувач вищої освіти факультету №3 Донецького державного університету внутрішніх справ

Пекарський С. П.,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЗАБЕЗПЕЧЕННЯ ВИМОГ РЕЖИМУ СЕКРЕТНОСТІ ПІД ЧАС РОБОТИ З АВТОМАТИЗОВАНОЮ ІНФОРМАЦІЙНОЮ СИСТЕМОЮ ОПЕРАТИВНОГО ПРИЗНАЧЕННЯ

Наказом МВС України від 20.10.2017 № 870 (редакція від 12.08.2022) затверджено «Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС». Автоматизована інформаційна система оперативного призначення (далі – АІС ОП) є сукупністю програмно-технічних та технічних засобів електронних комунікацій і призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності та діяльності з проведення кримінального аналізу Національної поліції України [1]. АІС ОП утворена для наповнення та підтримки в актуальному стані бази даних єдиної інформаційної системи МВС та є її складовою частиною.

Відповідно до вимог даного положення основними завданнями АІС ОП є:

- підвищення рівня інформаційно-аналітичного забезпечення оперативно-розшукової діяльності Національної поліції України;
- забезпечення процесу підтримки управлінських рішень керівництвом Національної поліції України;
- об’єднання отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного та електронного комунікаційного обладнання;
- створення умов для електронної взаємодії суб’єктів АІС ОП, центрального та регіонального вузлів АІС ОП, зменшення часових та фінансових витрат на управлінські, інформаційно-пошукові та аналітичні роботи, формування звітності;
- протидія злочинності та проведення профілактичної роботи, спрямованої на запобігання вчиненню правопорушень [1].

Відповідно до вимог зазначеного Положення обліку в АІС ОП підлягають відомості про осіб, відносно яких заведено оперативно-розшукові справи, отримані:

- від осіб, які конфіденційно співробітничають з оперативними підрозділами Національної поліції України;
- в ході проведення оперативно-розшукових заходів у рамках оперативно-розшукових справ [1].

Найвищим ступенем обмеження доступу до інформації, що обробляється в АІС ОП, є ступінь секретності «таємно», тобто категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою [2, ст. 1].

Зазначені відомості підпадають під відомості, які відносяться до державної таємниці [2]. Так, відповідно до положень статті 8 Закону України «Про державну таємницю» від 21 січня 1994 року № 3855-XII (редакція від 15.03.2022) відомості про форми, методи і результати оперативно-розшукової діяльності, а також про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність відносяться до державної таємниці [2, ст. 8].

Інформація щодо осіб, стосовно яких проводилися оперативно-розшукові заходи та за результатами ухвали або вироку суду доведено їх причетність до злочинної діяльності, перебуває на обліку АІС ОП п'ять років з дня закриття оперативно-розшукової справи, після чого знищується в установленому законодавством України порядку [1].

У разі якщо причетність до правопорушення особи, щодо якої здійснювались оперативно-розшукові заходи, не підтвердилась, така інформація зберіганню не підлягає та знищується в установленому законодавством України порядку.

Розпорядником інформації, яка обробляється в АІС ОП, є Національна поліція України. Національна поліція України вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи [1]. Серед підрозділів Національної поліції України розпорядником АІС ОП є Департамент кримінального аналізу, який є структурним підрозділом кримінальної поліції.

Користувачами АІС ОП є посадові особи Національної поліції України, яким в установленому порядку надано право наповнювати, підтримувати в актуальному стані та використовувати інформаційні ресурси АІС ОП, які відповідають за достовірність інформації, що вводиться ними до АІС ОП, та зобов'язуються не розголошувати у будь-який спосіб інформацію, що міститься у системі, крім випадків, передбачених законодавством України [1].

Безпосередньо АІС ОП побудована за такими рівнями:

- перший рівень – центральний вузол АІС ОП, розташовується в службових приміщеннях ДКА, де накопичується та систематизується узагальнена інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України;
- другий рівень – регіональні (обласні) вузли АІС ОП – розташовуються в службових приміщеннях УКА (ВКА, СКА), де накопичується та систематизується інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України, за територіальним принципом [1].

Отже, на підставі викладеного висновуємо, що відповідно до статті 18 Закону України «Про державну таємницю», з метою охорони державної таємниці під час роботи з АІС ОП впроваджуються єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації та режим секретності, тобто – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці. Саме тому в АІС ОП впроваджені програмні та технічні засоби комплексної системи захисту інформації, основним завданням якої є забезпечення достатнього рівня доступності, цілісності й конфіденційності інформації шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованого доступу та витоку технічними каналами [1].

Література:

1. Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: затв. наказом МВС України від 20.10.2017 № 870 (редакція від 12.08.2022). URL: https://zakon.rada.gov.ua/ laws/show/z1433-17#Text.
2. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII (редакція від 15.03.2022). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

Шабатура Ю. В.,
завідувач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор

Смичок В. Д.,
доцент кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Лунькова Г. В.,
професор кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент;

Квасньовський В. В.,
здобувач вищої освіти Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

КОМП'ЮТЕРНИЙ ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ПРИХОВАНИХ ЗВ'ЯЗКІВ РАКЕТНИХ АТАК З ПОЛОЖЕННЯМИ СУПУТНИКОВИХ УГРУПУВАНЬ В ХОДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Інтенсивний розвиток комп'ютерних технологій вже з першої половини 90-х років минулого століття спричинив стрімке зростання масивів даних пов'язаних з дослідницькою, виробничою, навчальною, та іншими видами діяльності людей. Закономірно, що лавиноподібне накопичення об'ємів даних спричинило до необхідності пошуків певних неочевидних і в більшості випадків прихованих закономірностей і зв'язків, які можуть мати суттєве практичне значення. Саме для вирішення даного класу задач виникла і почала інтенсивно розвиватися інформаційна технологія інтелектуального аналізу даних (Data Mining). В першу чергу дана інформаційна технологія призначалася для використання при прийнятті обгрунтованих управлінських рішень із врахуванням виявлення таких закономірностей, про існування яких користувачі, як правило, не мали жодних уявлень. Однак базові підходи цієї технології цілком можуть бути використані і для аналізу великих масивів даних накопичених і в інших галузях діяльності людей.

Повномасштабна війна Росії проти України стала ще одним, вкрай негативним фактором, який призводить до накопичення особливих масивів даних. Одним з таких масивів, який привернув нашу увагу став масив даних про оголошення повітряних тривог і відповідних їм ракетних атак. На жаль війна продовжується і даний масив невпинно продовжує зростати, тому в проведених дослідженнях ми вибрали статистику повітряних тривог за обмежений часовий проміжок і лише для західного регіону України, зокрема для Львівської області. Завдяки суттєвій віддаленості від зон бойових дій, західні регіони України принаймні до даного часу зазнавали виключно ракетних ударів, це дозволяє зосередитися на пошуках відповідним чином диференційованих зв'язків і закономірностей пов'язаних з ракетними атаками.

Для виконання комп'ютерного аналізу в ході проведених досліджень були сформовані часові ряди в яких фіксувалися моменти оголошення повітряних тривог, причому параметрами тривалості і завершення тривог на цій стадії дослідження автори консенсуально вирішили нехтувати. Отримані дані зведені в електронні таблиці, що дозволило проводити їх математичну обробку і візуалізацію. Вже поверхневий аналіз призвів до виявлення певної періодичності в зафіксованих даних, це одразу наштовхнуло авторів на гіпотезу про можливий зв'язок ракетних атак з періодичністю входження військових космічних супутників ворога в зону радіовидимості, яка покриває на період атак західні регіони України і тим самим вони можуть забезпечувати стійкий канал зв'язку центрів управління для передачі і прийому інформації з ракетами, які були запущені для виконання бойових завдань. Тому автори зосередилися на пошуках саме причин, які зумовлюють такий характер поведінки ворога при нанесенні ракетних ударів по західному регіону нашої держави.

Метою проведеного дослідження став пошук закономірностей в здійснених і очевидно ще можливих в майбутньому ракетних атаках ворога на об'єкти в західних регіонах України, а також встановлення можливих зв'язків запусків ракет ворога з перебуванням в зоні радіовидимості об'єктів військових космічних угрупувань над західними регіонами України.

Аналіз зібраних даних був виконаний за період з 24.02.2022 р. по 11.09.2022 р. Дані спостережень були взяті з відкритих джерел і представлені у вигляді трьох узгоджених послідовностей: дати дати (день і місяць оголошення тривоги), часу доби (момент оголошення тривоги, представлений з точністю до хвилини) та оперативного часу – безперервного часу, відлік якого ведеться з моменту початку нападу ворога на Україну (у ньому теж відзначаються моменти оголошення тривоги, представлені з точністю до хвилини).

Графічна візуалізація отриманих даних за принципом «дата – час», тобто в координатній системі час доби – дата оголошення тривоги, з усередненням по трьом точкам і побудовою поліноміальної апроксимації наведена на рис. 1.

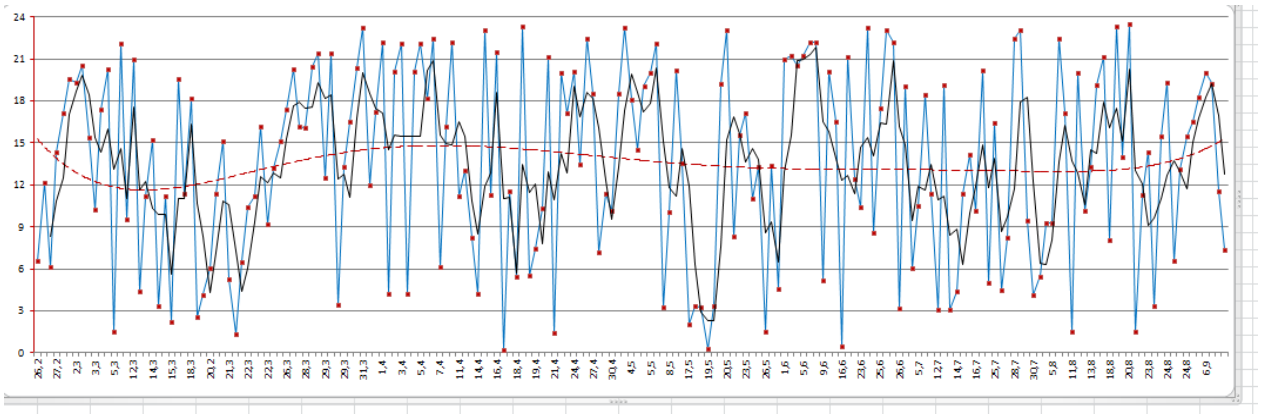


Рис. 1. Візуалізація спостережень за принципом «дата – час»

Усереднення по 3 точках не дає чіткої вираженої картини достатньої для висновків адже це може бути пов'язане з людським фактором перестрахування під час бойових дій, коли тривоги оголошувалися коли булла лише загроза але самиі ракетні атаки не відбувалися, тому послідовно були виконані усереднення по 5 і 7 точках. Графік з усередненням по 7 точках наведений на рис. 2.

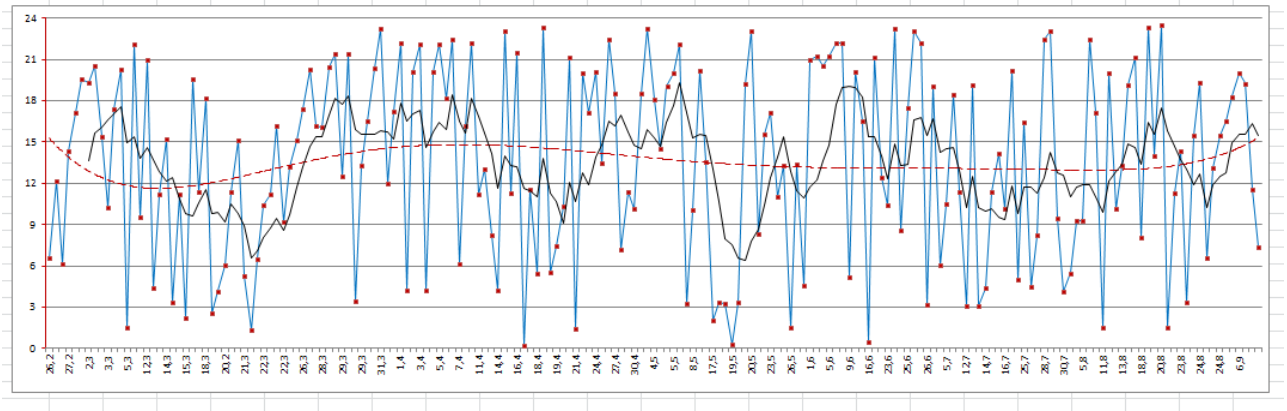


Рис. 2. Візуалізація спостережень з усередненням по 7 точках

Усереднена лінія тренду по 7 точках чітко показує періодичний характер повітряних тривог, що співпадають з пусками ракет по території західної України. Тепер залишається лише з'ясувати причини такої «періодичності».

Відомо, що в збройних силах Російської Федерації вагоме значення для вирішення задач спостережень, зв□язку і навігації відіграють повітряно-космічні сили, які головним чином представлені військовими супутниками. Завдяки використанню відкритої інформації представленої командуванням повітряно-космічної оборони Північної Америки (NORAD) нам вдалося співставити виявлену періодичність ракетних атак з циклічним характером і часом прольоту цілого ряду військових супутників Росії над територією України. Серед таких супутників нами виявлені наступні: COSMOS 2506; COSMOS 2502; COSMOS 2503; COSMOS 2222 COSMOS 2429. На наведеному нижче рис. 3 в якості прикладу представлена основна траєкторна та навігаційна інформація по супутнику COSMOS 2506, яка отримана за допомогою системи NORAD.

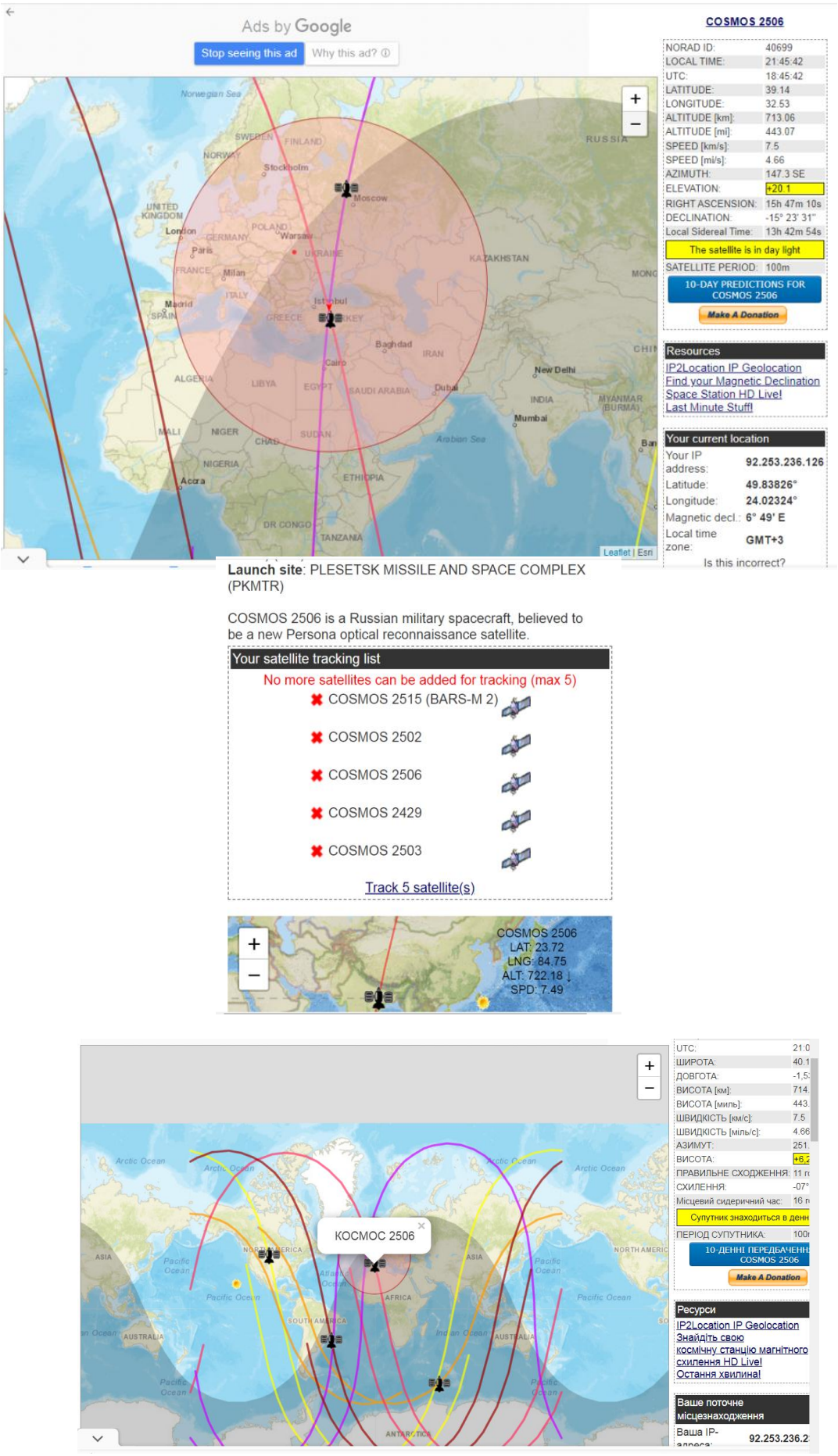


Рис. 3. Основна інформація, проекції траєкторій польоту та еферемиди супутника COSMOS 2506

Таким чином, на підставі зібраних даних і виконаних досліджень та аналізу їх результатів встановлено існування періодичного характеру ракетних атак на територію західних регіонів України, та виявлено потенційну можливість використання ряду військових супутників повітряно-космічних сил Російської Федерації для прямого контролю і управління їхніми ракетами під час виконання ними бойових завдань принаймні на території західних регіонів України. Крім того, цілком очевидно, що дані супутники можуть виконувати функцію безпосереднього фіксування місць попадань запущених ракет.

Шабатура Ю. В.,
завідувач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор

Рибак В. Р.,
аспірант Національного лісотехнічного університету України

ДОРАДЧА КОМП'ЮТЕРНА СИСТЕМА ЛІКАРЯ-СТОМАТОЛОГА

Професійна діяльність сучасного лікаря-стоматолога навіть у порівнянні з іншими лікарськими спеціальностями відрізняється високою складністю і вимагає від нього великої уважності, зосередженості, швидкості і точності рухів інструментами та професійного досвіду. Саме тому важливою в науковому відношенні і цінною для практики є задача створення дорадчих комп'ютерних систем, які дозволятимуть як покращувати процес підготовки лікарів-стоматологів так і допомагати їм у професійній діяльності [1, 3].

Основою розроблюваної дорадчої системи є програмний модуль штучного інтелекту, який має обширну базу професійних знань і отримує об'єктивну інформацію як від технічних засобів візуального спостереження, так і від рентгенівського обстеження та різноманітних аналізів і проб від конкретного пацієнта. У відповідь на запит лікаря система формує рекомендаційний висновок та надає його обґрунтування.

Як показали попередні дослідження і результати моделювання, застосування такої системи дозволить підвищити якість лікування і суттєво зменшить ризик прийняття неправильних лікарських рішень або упущень важливих деталей як в процесі діагностики так і під час лікування [1].

У процесі підготовки майбутні кваліфіковані фахівці у сфері стоматології традиційно витрачають велику кількість навчальних годин на теоретичну та достатньо важку навіть у фізичному відношенні практичну підготовку, з опрацюванням виняткових випадків та ексцесів, що безсумнівно дає свої результати. Проте, яким би кваліфікованим не був фахівець, можливості людського інтелекту та особливості фізіології не дають підстав вважати його професійну діяльність бути цілком позбавленою помилок. Навіть найкращі стоматологи під впливом втоми, психофізичного стану чи простої неуважності можуть допустити помилку при лікуванні чи діагностиці, що в свою чергу може мати значні наслідки в майбутній перспективі для конкретної людини-пацієнта.

Добре навчена система, на базі нейронних мереж, що постійно «вчаться», завжди помітить допущену помилку чи не враховані дрібниці і надасть свою допомогу лікарю-стоматологу [2, 3]. Однак, перш ніж використовувати моделі штучного інтелекту в звичайних клінічних операціях, все ще важливо додатково підтвердити їх ефективність, надійність і достовірність.

Після здійсненого аналізу вищеописаної задачі, було здійснено висновок, що для даного завдання доцільним буде застосування алгоритмів штучного інтелекту, зокрема алгоритмів комп'ютерного зору, серед яких найпопулярнішими на даний момент є алгоритми, що базуються на використанні капсульних нейронних мереж (CapsNet).

При аналізі алгоритмів комп'ютерного зору, було здійснено порівняння алгоритму CapsNet з більш популярним на даний момент алгоритмом згорткових нейронних мереж (ConvNet)[5]. Після порівняння було зроблено висновок, що незважаючи на високу популярність згорткові нейронні мережі мають багато проблем і для деяких задач стали малоефективними, в свою чергу капсульні нейронні мережі, як є відносно новою технологією, в більшості випадків, можуть усунути недоліки ConvNet [4, 5].

Одне з найбільш значущих нововведень CapsNet є виділення не лиш окремих деталей зображення, але і побудова зв'язків між їх місцезнаходженням одне відносно одного, що, також надає можливість здійснювати відтворення оригінального вхідного зображення [5].

Для оцінки алгоритмів CapsNet та ConvNet, було здійснено навчання з однаковими вхідними наборами з MNIST та CIFAR-10, а після навчання здійснено перевірку моделей на вхідних наборах. Отримані результати показали, що CapsNet може здійснювати кращі прогнозування навіть з меншою вибіркою вхідного набору. Вагомою перевагою також є здатність CapsNet розпізнавати обернені зображення, з чим не може настільки успішно впоратись ConvNet. Виходячи з проведеного аналізу для вирішення даної задачі було обрано модель CapsNet [5].

Першою задачею яку поставлено систему було виявлення потенційних патологій поверхонь. Для побудови системи використовувалась платформа з вбудованими інструментами для побудови різних моделей нейронних мереж TensorFlow. Навчання моделі було проведено за допомогою навчальної вибірки з більш ніж 5000 рентгенівських зображень ротової порожнини. Вибравши оптимальну кількість ядер та їх розмірність при заданій розмірності навчальної вибірки вдалося досягти точності виявлення патологій у 89,41%.

Як показали проведені нами дослідження, використання моделей штучного інтелекту, таких як штучні нейронні мережі, можуть мати великі перспективи застосування у найрізноманітніших задачах. Серед перспективних напрямків використання можна виділити наступні: виявлення патологій, виявлення карієсних уражень, переломів коренів, визначення робочої довжини з рентгенограм, прогнозування повторного лікування, прогнозування та моделювання для щелепно-лицьової хірургії [1].

Література:

1. A. Aminoshariae, J. Kulild, and V. Nagendrababu, “Artificial Intelligence in endodontics: Current applications and Future Directions,” Journal of Endodontics, vol. 47, no. 9, pp. 1352–1357, 2021.
2. S. V. Deshmukh, “Artificial Intelligence in Dentistry”, Journal of the International Clinical Dental Research Organization, vol. 10, no. 2, p. 47, 2018.
3. D. Tandon, J. Rajawat, and M. Banerjee, “Present and future of Artificial Intelligence in Dentistry”, Journal of Oral Biology and Craniofacial Research, vol. 10, no. 4, pp. 391–396, 2020.
4. X. Wang, R. Girshick, A. Gupta, “Non-local Neural Networks”, Conference on Computer Vision and Pattern Recognition, pp. 18–22, 2018.
5. S. Woo, J. Park, J. Lee, I.S. Kweon, CBAM: “Convolutional Block Attention Module”, European Conference on Computer Vision, pp. 3–19, 2018

Зміст

Наукове видання

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

16 грудня 2022 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 **Інформаційні технології в освіті та практиці** : матеріали Науково-практичної конференції (Львів, 16 грудня 2022) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2023. – 80 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційні технології в освіті та практиці», що проводилася 16 грудня 2022 року у Львівському державному університеті внутрішніх справ.

УДК 004