

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ПРАВООХОРОННИМИ СТРУКТУРАМИ
УКРАЇНИ ТА ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ ЗІ
СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Збірник наукових статей за матеріалами доповідей
учасників Всеукраїнської науково-практичної конференції

21 грудня 2018 р.

Львів 2018

*Рекомендовано до друку Вченою радою Львівського державного
університету внутрішніх справ (протокол № 5 від 26.12.2018)*

РЕДАКЦІЙНА КОЛЕГІЯ

О. М. Балинська – проректор, доктор юридичних наук, професор (голова)
В. В. Сенік – кандидат технічних наук, доцент (заступник голови)
В. Б. Вишня – доктор технічних наук, професор
Ю. І. Грицюк – доктор технічних наук, професор
М. І. Андрійчук – доктор технічних наук, с.н.с.
Я. І. Соколовський – доктор технічних наук, професор
Ю.В. Шабатура – доктор технічних наук, професор
Я. Ф. Кулешник – кандидат технічних наук, доцент
Т. В. Рудий – кандидат технічних наук, доцент
Д. М. Неспляк – кандидат фізико-математичних наук
Т. В. Магеровська – кандидат фізико-математичних наук, доцент
(відповідальний секретар)

П 78 Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 21 грудня 2018 року / упорядник Т. В. Магеровська / – Львів: ЛьвДУВС, 2018. – 281 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції «Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання», що проводилася 21 грудня 2018 року у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

УДК 004 © Львівський державний
університет внутрішніх справ, 2018

Розділ 1.

НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО–
ПРАВОВІ, ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ
ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНО–
ЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ
ПРАВООХОРОННИХ ОРГАНІВ, ЇХ ПРАКТИЧНІЙ
ДІЯЛЬНОСТІ ТА КОМПЛЕКСНОМУ ПІДХОДІ ДО
ПРОБЛЕМ ДЕРЖАВНОЇ БЕЗПЕКИ

ПРАВОВІ ТА ТЕХНІЧНІ ПИТАННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Бортник Надія Петрівна,

*завідувач кафедри адміністративного та інформаційного права
Національного університету «Львівська політехніка»,
доктор юридичних наук, професор*

Якість політичних, соціально-економічних, духовно-культурних та інших державних перетворень сьогодні безпосередньо залежить від стану національної інформаційної безпеки. Формування нових загроз і ризиків забезпечення інформаційної безпеки держави на тлі гібридної війни багато в чому визначає пріоритетні напрямки державної політики в інформаційній сфері як системоутворюючого фактора життя суспільства.

Функціонування ефективної національної системи забезпечення інформаційної безпеки держави вимагає вдосконалення організаційного механізму, а, отже, нормативного регулювання в даній сфері, виходячи з об'єктивної оцінки стану інформаційної безпеки і різних сценаріїв розвитку інформаційного суспільства в національному масштабі з урахуванням реалізації Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [1].

У країнах, де високий рівень комп'ютеризації та інформатизації населення, процесів управління державою, де реалізовано електронне урядування,. Розвиток комп'ютерного парку мимоволі призводить до об'єднання комп'ютерів у мережі, що в свою чергу можуть підключатися до корпоративних, національних, державних і глобальних мереж, де кількість комп'ютерів з різною інформацією, різним рівнем захисту, досягає сотень тисяч. Відповідно проблема боротьби з комп'ютерною злочинністю стає однією з першорядних.

План заходів на 2018 рік з реалізації Стратегії кібербезпеки України передбачає ряд напрямів удосконалення національного законодавства, але не в повній мірі охоплює проблемні питання

[2]. За свідченням експертів привабливим сектором економіки для злочинців є кредитно-фінансова система. Аналіз злочинних діянь, вчинених у кредитно-фінансовій сфері з використанням комп'ютерних технологій, неодноразові опитування представників банківських установ дозволяють стверджувати, що найбільш поширеними є комп'ютерні злочини, що здійснюються шляхом несанкціонованого доступу до банківських баз даних за допомогою телекомунікаційних мереж.

За останній час виявлено деяку кількість правопорушень вчинених злочинними угрупованнями, що наймали бригади з десятків хакерів, надаючи окреме приміщення, що охороняється, обладнане за останнім словом техніки, для скоєння крадіжок грошових коштів за рахунок нелегального проникнення в комп'ютерні мережі великих комерційних банків.

Велика кількість комп'ютерних злочинів вчиняється з використанням інструментів і відомостей, добровільно наданих користувачами Інтернет. Унікальність глобальної системи полягає в тому, що вона не знаходиться у володінні фізичної особи, приватної компанії, державного відомства або окремої країни. Практично у всіх сегментах мережі відсутнє централізоване регулювання, цензура та інші методи контролю інформації. Завдяки цьому відкриваються практично необмежені можливості доступу до інформації, що широко використовуються злочинцями. Мережу Інтернет можна розглядати як інструмент здійснення комп'ютерних злочинів і середовище для ведення різноманітної злочинної діяльності.

Сьогодні державні органи намагаються впорядкувати, а в деяких випадках посилити порядок використання загальнодоступних мереж, тим самим обмежити можливі негативні наслідки використання для розпалювання сепаратизму мережею Інтернет, у зв'язку зі сформованою геополітичною ситуацією та беручи до уваги необхідність України, відстоювати стратегічні інтереси та захищати цілісність держави [3].

Забезпечення надійного рівня захисту інформації можливо тільки при дотриманні політики безпеки. Політика інформаційної безпеки є планом високого рівня, де описуються цілі та завдання заходів в

сфері безпеки. Політика не є ні директива, ні норматив, ні інструкція, ні засоби управління. Політика описує безпеку в узагальнених термінах без специфічних деталей. Вона забезпечує планування всієї програми безпеки так само, як специфікація визначає номенклатуру продукції, що випускається фабрика або завод.

Політика безпеки це комплекс превентивних заходів щодо захисту конфіденційних даних та інформаційних процесів. Політика безпеки описує вимоги до персоналу, технічним службам тощо.

Основні напрями при розробці політики безпеки це математичні обчислення щодо даних і як необхідно захищати, визначення хто і якої шкоди може завдати в інформаційному аспекті, обчислення ризиків і визначення схеми зменшення ризиків до величини прийнятною в даній конкретній ситуації.

25 лютого 2017 року прийнято Доктрину інформаційної безпеки України, що прийшла на зміну Доктрині 2009 року [4]. У Доктрині чітко відзначені завдання та національні інтереси України, позначені загрози в інформаційному просторі. Система стратегічних завдань у галузі інформаційної безпеки має на увазі інтереси громадян, їх інформаційну захищеність.

Особа, суспільство та держава це ступені єдиного механізму, де кожен об'єкт і його інформаційні інтереси є важливими і охороняються державою. У цьому контексті розглянемо, як на сьогоднішній день захищений громадянин і держава від атак на належну їм інформацію: Конституція України; Закони України: від 21 січня 1994 року № 3855-ХІІ «Про державну таємницю»; від 2 жовтня 1992 року № 2657-ХІІ «Про інформацію»; від 5 липня 1994 року «Про захист інформації в інформаційно-телекомунікаційних системах»; від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки»; від 5 жовтня 2017 року № 2155-VIII «Про електронні довірчі послуги»; від 1 червня 2010 року № 2297-VI «Про захист персональних даних»; від 7 грудні 2000 року № 2121-III «Про банки і банківську діяльність» (щодо банківської таємниці); Цивільний кодекс України; Кримінальний кодекс України.

Кожен з наведених законів захищає свою частину інформаційного поля, привносить свої норми в інформаційно-правове поле та

відповідно санкції за порушення особистого, корпоративного або державного інформаційного простору. Але ці закони створювалися в ті часи, коли загрози від хакерів, кібератаки та кіберзлочини не були настільки масштабні. Втрати національних економік, втрати громадян в економічному та моральному плані сьогодні дуже великі.

Необхідно прийняти закон інформаційно-правового характеру, який би мав чіткі формулювання визначень відповідно до теорії інформаційних технологій та систем, програмування, що б відображали актуальний стан речей в сучасному інформаційному світі. Цей закон був би початком для розробки Кодексу в галузі інформаційних телекомунікаційних та транскордонних інформаційних систем.

Закон України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки» розглядає питання кібербезпеки, але, наприклад, не

відображає принцип право на забуття [5]. Право на забуття це спроба захистити громадян і державний апарат від інформації, яка застаріла або є наклепом.

Виявляється цілком слушним наявність у представників законодавчої влади технічної освіти або знання програмування або взагалі знання про будову інформаційного простору ні з юридичної, а з технічної точки зору. Адже автори законів і поправок іноді пишуть досить розпливчасті визначення та поняття, що потім є основоположними для прийняття рішень.

Наприклад, поняття месенджер потрапляє під визначення «організатор поширення інформації, сповісник», але з цим можна не погодитися. Виходячи з визначень форум (веб-форум), блог (англ. blog, від web log – мережевий журнал чи щоденник подій), соціальна мережа та месенджер – це взаємозамінні, еквівалентні поняття, що явно не є істинною. Ці організатори поширення повинні надавати ключі до дешифрування інформації своїх клієнтів. Ключі, якщо вони є унікальними для кожного контенту, також повинні зберігатися, що збільшує масив інформації. Багато месенджерів не реєструються в якості «організаторів поширення

інформації». Законодавець хоче позначити або визначити дії месенджерів. Можливо, що такий підхід буде продуктивним і знайде позитивний відгук у користувачів та операторів.

Не кожна людина хоче, щоб його слухали та читали повідомлення, переглядали фото. Наприклад, зараз популярний месенджер Threema – ним користуються просунуті студенти, чиновники, бізнесмени. Кількість його завантажень зростає, але ще не досягло рівня Telegram.

У висновку хотілося б відзначити, що остаточно та масштабно вирішити питання про баланс інтересів особи, її безпеки і інтересів держави та її безпеки, з урахуванням інтересів соціуму, неможливо. Але рішення цих питань має бути першочерговим завданням науки. Юридична наука та практика повинні йти в ногу з мінливими реаліями технологічного та інформаційного прогресу суспільства. Випереджати не можливо, але йти в ногу з часом це реально. Актуальність і пріоритетність напрямів вдосконалення нормативно-правової бази в галузі забезпечення інформаційної безпеки, з урахуванням відповідних пропозицій і рекомендацій Ради Національної безпеки і оборони України, підтверджуються необхідністю створення структурно єдиної та функціонально взаємозалежної системи забезпечення інформаційної безпеки на центральному, регіональному та місцевому рівнях, що, в свою чергу, підкреслює важливість стратегічного планування та правового забезпечення у даній галузі.

-
1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII. Відомості Верховної Ради України. 2014. № 40. Ст. 2021.
 2. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 11.07.2018 р. № 481-р. URL. <http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80> (дата звернення 06.12.2018).
 3. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» :

Указ Президента України від 15.05.2017 р. № 133/2017. URL. <https://www.president.gov.ua/documents/1332017-21850> (дата звернення 06.12.2018).

4. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 27.02.2017 р. № 47/2017. URL. <http://zakon.rada.gov.ua/laws/show/47/2017> (дата зв-ня 06.12.2018).
5. Про основні засади забезпечення кібербезпеки : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

ОСНОВНІ ЦІЛІ, ЗАВДАННЯ ТА ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СЬОГОДЕННЯ

Власюк Олександр Михайлович,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Копанецька Наталія Василівна,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Сеник Володимир Васильович,

*завідувач кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Сьогодні, в умовах гібридної війни на перший план виходять питання забезпечення інформаційної безпеки державних установ, організацій чи окремих підприємств.

Загалом, проведення будь-яких заходів стосовно забезпечення інформаційної безпеки мають відповідати забезпеченню потреб суспільства, пройти обґрунтування з фінансової, правової, організаційно-технічної точок зору. З огляду на це, основними цілями інформаційної безпеки є забезпечення:

1. Визначеного режиму доступу до інформації (таємності, конфіденційності);
2. Цілісності інформації, даних та процесів їх опрацювання;
3. Доступності інформаційних ресурсів, систем та процесів;
4. Підтримки реалізації стратегічних основ структур, установ, підприємств тощо, щодо окремих питань інформаційної безпеки;
5. Захисту інформаційних ресурсів структур, установ, підприємств тощо від будь-яких, навмисних та випадкових загроз інформаційній безпеці;
6. Захисту законних інтересів власників інформаційних ресурсів від протиправних дій, втрати, витоку, модифікації,

розголошення чи знищення даних, порушення роботи інформаційно-телекомунікаційних систем, засобів захисту інформації та процесів її опрацювання.

Відштовхуючись від викладених цілей інформаційної безпеки, можемо визначити і основні її принципи. Це, насамперед:

- обґрунтований, комплексний, та системний підхід до забезпечення інформаційної безпеки;
- постійний процес розвитку та удосконалення питань інформаційної безпеки, її інтеграція з новими підходами до безпеки інформації, інформаційними технологіями і рішеннями;
- уведення планів та реалізація окремих рішень з безпеки інформації як елемента побудови інформаційно-телекомунікаційних систем, комп'ютерних мереж, систем захисту;
- розроблення та впровадження як запобіжних заходів швидкого реагування на непередбачені події;
- підтримка інформаційної культури обслуговуючого персоналу.

У зв'язку із цим в усіх структурах, установах, підприємствах тощо, де проводяться заходи із забезпечення безпеки інформації має бути уведений постійний контроль щодо ефективності встановлених заходів інформаційної безпеки та механізмів їх реалізації в інформаційно-телекомунікаційних системах, вивчений перелік інформаційних процесів та ресурсів, які підлягають захисту. В процесі цього слід досягнути безпеки чи встановити певний рівень захисту для таких властивостей інформації як доступність, конфіденційність цілісність тощо. Насамперед це відноситься до державної таємниці, службової та конфіденційної інформації.

Доступ користувачів та обслуговуючого персоналу до інформаційних систем (підсистем) має бути заснований на моделі доступу з урахуванням принципу надання мінімальних повноважень, які необхідні для виконання посадових обов'язків та завдань.

Розроблення, уведення до експлуатації та виведення з експлуатації інформаційних систем чи окремого обладнання має здійснюватися за певною встановленою процедурою.

Хмарні технології для зберігання та опрацювання даних, а також забезпечення роботи певних сервісів можуть використовуватися відповідно до нормативно-правового законодавства та з реалізацією відповідного рівня захисту інформації. Окрім цього кожна структура, установа чи підприємство має неухильно дотримуватися вимог законодавства України, нормативно-правових актів та регулятивних документів Верховної Ради України, Кабінету Міністрів України, Служби безпеки України та інших нормативно-правових актів (наприклад, [1-5]).

Для контролю інформаційної безпеки у будь якій структурі, установі чи підприємстві створюється підрозділ з інформаційної безпеки, який визначає, впроваджує та контролює дотримання вимог з інформаційної безпеки, забезпечує належне функціонування та використання засобів забезпечення інформаційної безпеки, організовує належне навчання обслуговуючого персоналу та користувачів з питань інформаційної безпеки, контролює виконання, вдосконалення та підтримку політики інформаційної безпеки в актуальному стані, а також проводить аналіз та готує різного характеру звітність щодо стану інформаційної безпеки.

Дані підрозділи у своїй діяльності мають керуватися основними вимогами до інформаційної безпеки та забезпечити відповідність процесів налаштування, розробки, підтримки інформаційних-телекомунікаційних систем у відповідності до вимог нормативно-правових документів України з питань інформаційної безпеки.

Усі співробітники структур, установ чи підприємств мають нести персональну відповідальність за виконання вимог нормативних документів та законодавства України з питань інформаційної безпеки. Це стосується, зокрема збереження державної таємниці, персональних даних та іншої конфіденційної інформації, дотримання відповідного рівня інформаційної безпеки під час виконання власних посадових обов'язків.

-
1. Про інформацію : Закон України 02 жовтня 1992 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2657-12/>

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/>
3. Про захист персональних даних : Закон України від 01 червня 2010 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2297-17/>
4. Положення про державну експертизу в сфері технічного захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93 [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon.rada.gov.ua/laws/show/z0820-07>
5. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації / Затверджено наказом ДСТСЗІ СБ України від 10.03.2004 № 04. – Київ, 2004.

ДЕРЖАВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Гаврильців Марія Теодорівна,

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

Забезпечення інформаційної безпеки України як найважливішої функції держави реалізується за допомогою відповідного державно-правового механізму забезпечення інформаційної безпеки, що втілюється в життя через діяльність як органів державної влади, так і ряду недержавних інституцій.

Досліджуючи проблематику інформаційної безпеки Б. Кормич оперує декількома поняттями: «державно-правовий механізм інформаційної безпеки» й «інституційний механізм інформаційної безпеки». При цьому, якщо державно-правовий механізм інформаційної безпеки автор визначає як сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки, їх ролей і відносин, що підпорядковані чіткій ієрархії правових норм та принципів [2, с. 148–149], то інституційний механізм інформаційної безпеки, що є складовим елементом державно-правового механізму, має декілька визначень. Відповідно до першого, інституційний механізм інформаційної безпеки України – це сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки [2, с. 149]. Згідно з другим, інституційний механізм інформаційної безпеки представляє собою сукупність інститутів публічної влади й інститутів громадянського суспільства, до компетенції яких входить вирішення питань щодо забезпечення умов функціонування та розвитку інформаційної сфери [2, с. 175].

Таким чином, поняття «інституційний механізм інформаційної безпеки» має широке та вузьке розуміння. У вузькому значенні інституційний механізм інформаційної безпеки охоплює виключно державні інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки. У широкому значенні,

крім інститутів публічної влади, до його складу входять також інститути громадянського суспільства.

Перелік інституцій, які можуть брати участь у проведенні політики або виробленні конкретних політичних рішень, практично невичерпний і він не обмежується лише органами державної влади та місцевого самоврядування. Так, опрацювання будь-якої проблеми, пов'язаної з політикою інформаційної безпеки, може бути доручене певним науковим установам, групам експертів [2, с. 172].

Отже, суб'єктами забезпечення інформаційної безпеки є не лише органи державної влади, а й недержавні, що відповідає нормам нормативно-правових актів, що регулюють суспільні відносини у сфері інформаційної безпеки України. Хоч як широке, так і вузьке розуміння інституційного механізму не охоплює такого важливого суб'єкта забезпечення інформаційної безпеки, як громадяни України, зводячи коло суб'єктів виключно до державних і недержавних інституцій. Саме тому вважаємо, що поняття «інституційний механізм інформаційної безпеки» є більш вузьким поняттям щодо поняття «суб'єкти забезпечення інформаційної безпеки».

Інституційна система державного управління інформаційною безпекою є надзвичайно складною та багаторівневою системою, складовими елементами якої є такі: 1) доктрина і правова основа, якими визначаються основні завдання і принципи державної діяльності щодо захисту безпеки; 2) інституціональний механізм, тобто сукупність міжнародних і національних державних і громадських органів, які в своїй діяльності вирішують певні завдання щодо підтримання стану безпеки різних рівнів; 3) методологічна база, тобто способи, засоби і ресурси, що використовуються для реалізації конкретних завдань у межах політики інформаційної безпеки [3]

У Доктрині інформаційної безпеки України [1] визначено коло суб'єктів забезпечення інформаційної безпеки та завдання покладені на них у цій сфері. Так, Рада національної безпеки і оборони України має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.

Кабінет Міністрів України забезпечуватиме здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері [1].

На Міністерство інформаційної політики України покладено заходи щодо позиціонування України в світі; підтримка виробництва вітчизняної аудіовізуальної продукції та популяризація її за кордоном; захист інформаційного простору України від зовнішнього інформаційного впливу.

На Міністерство закордонних справ України має бути покладено: сприяння входженню України до світового інформаційного простору, піднесенню її міжнародного авторитету, формуванню позитивного іміджу держави як надійного і передбачуваного партнера.

Міністерство оборони України має забезпечувати функціонування системи військово-цивільних зв'язків у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань, а також організовувати і забезпечувати: зв'язки з українськими та іноземними засобами масової інформації; супроводження інформаційними засобами виконання завдань оборони України; донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань [1].

Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до компетенції братимуть участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора.

Служба безпеки України у межах компетенції має здійснювати: моніторинг вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій [1].

Розвідувальні органи України у процесі своєї діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави.

Державна служба спеціального зв'язку та захисту інформації України забезпечуватиме в межах компетенції формування і реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України.

Національний інститут стратегічних досліджень має забезпечити науково-аналітичне та експертне супроводження процесу формування і реалізації державної інформаційної політики [1].

У сфері забезпечення інформаційної безпеки беруть участь також органи місцевого самоврядування, підприємства, установи й організації незалежно від форм власності, громадські об'єднання, їх посадові особи та громадяни.

Відповідно до ст. 15 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» органи місцевого самоврядування, підприємства, установи і організації незалежно від форми власності мають надавати інформацію, документи і матеріали, необхідні для виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань. У статті 16 цього закону зазначено, що державні органи та органи місцевого самоврядування, їх посадові та службові особи в межах своїх повноважень сприяють діяльності Державної служби спеціального зв'язку та захисту інформації України у виконанні покладених на неї завдань. А громадяни України, громадські об'єднання сприяють такій діяльності на добровільних засадах [4].

Таким чином, механізм забезпечення інформаційної безпеки України охоплює систему суб'єктів, які забезпечують реалізацію державної політики в інформаційній сфері. Система таких суб'єктів має працювати незалежно від внутрішньополітичної кон'юнктури в Україні та стану окремих елементів системи забезпечення інформаційної безпеки. Системним, інтегруючим чинником для діяльності цих суб'єктів має бути спільна мета – забезпечення інформаційного суверенітету України.

Ефективність захисту інформаційної безпеки держави загалом забезпечується ефективною діяльністю кожної складової її державно-правового механізму, який складається із системи взаємопов'язаних й взаємоузгоджених державно-правових інституцій, завданнями яких є створення умов для успішної реалізації інформаційної політики держави.

-
1. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25.02.2017 № 47/2017. URL: <http://zakon.rada.gov.ua/laws/show/47/2017>.
 2. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія] / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.
 3. Косиця О.О. Інституціональний механізм системи інформаційної безпеки. Порівняльно-аналітичне право. – 2016. – № 4. URL: http://www.pap.in.ua/4_2016/45.pdf
 4. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: <http://zakon.rada.gov.ua/laws/show/3475-15>.

РОЗРОБКА ЕФЕКТИВНОЇ ІНФОРМАЦІЙНОЇ СТРАТЕГІЇ ДЛЯ АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ ПОЛІЦІЇ

Гривняк Сергій Олександрович,

*начальник Управління аналітичного забезпечення та
оперативного реагування ГУ НП у Львівській області*

Кулешник Ярко Федорович,

*доцент кафедри інформатики
Львівського державного університету внутрішніх справ
кандидат технічних наук, доцент*

Створення високопродуктивних поліцейських сил потребує розробки експлуатаційної моделі, яка дозволить забезпечувати більшу ефективність поліцейських послуг, поліпшення довіри суспільства до поліції, збільшити прозорість та підзвітність і зменшити витрати.

Ефективна інформація є ключовою в управлінні, що сприяє можливому підвищенню ефективності і продуктивності поліцейських сил.

Щоб зміцнити поліцейські підрозділи актуальною інформацією, сили поліції повинні розробити консолідований підрозділ – інформаційне управління, яке в першу чергу базується на конкретній інформаційній стратегії.

Стратегія повинна визначати сукупність загальних інформаційних принципів та включати в себе політику, структуру та рекомендації для підтримки прийняття принципових рішень в усій організації.

Мета: сформувати загальні ознаки інформаційного управління, стандарти та практики які забезпечують створення, збирання, передавання, оцінювання та використання якісної інформації, ефективної та надійної підтримки стратегічних цілей організації.

Прийняття всеосяжного, структурованого підходу до управління інформацією (табл. 1), допоможе забезпечити поліцію спеціалізованими підрозділами, що забезпечують і гарантують

актуальну інформацію, котра підвищить ефективність використання служб поліції.

Таблиця 1. Приклад системи керування інформацією для поліцейської діяльності.

Компоненти інформаційно-управлінської діяльності	
Інформаційно-управлінська діяльність	Компоненти
Застосування Застосування інформації та інтелекту для поліпшення стратегічних, оперативних дій та прийняття рішення на основі витрат	Аналітика Візуалізація даних Оптимізація інформаційного потоку Мобільні та віддалені введення даних та доступ до них
Доступність Забезпечення безпечного та ефективного доступу до інформації, що зберігається в дуже поширеному вигляді різних системних середовищ	Управління доступом Виявлення даних Пошук організації (власника)
Спільний доступ Надання поліцейським силам можливості співпрацювати та ефективно обмінюватися інформацією в межах і поза своєю організацією	Технічна сумісність Оперативна сумісність даних Сумісність процесуальна Управління взаємодією
Якість Забезпечення інформацією є багатозначною, точною, внутрішньо послідовною і повинна використовуватись лише за призначенням	Введення даних Виправлення помилок та перевірка даних Сертифікація системи та інтерфейсу Стандартизована архітектура та управління
Безпека Запобігання пошкодженню даних та несанкціонованому доступу	Політика щодо захисту та обробки даних Аудит ІТ-безпеки Цілісність мережі Система самозбереження

На основі досліджень і досвіду роботи з поліцейськими силами цілого світу, визначено набір рекомендацій щодо передового досвіду, та інформаційна стратегія для поліцейських сил, що розвиваються.

Залучити широкий спектр учасників.

Ефективна інформаційна стратегія буде наповнювати організаційні бази та буде впливати на оперативну технологію і стратегічні функції.

Інформація про стратегію повинна бути розроблена і вдосконалюватися через спільний процес, який об'єднує різних представників офіцерського складу, керівників підрозділів та осіб, що приймають критично важливі стратегічні рішення.

Встановити функції центрального управління.

Щоб забезпечити загальною інформацією, стандартами та практиками управління, що приймаються по всій організації, інформаційна стратегія повинна забезпечити міцне центральне управління, що базується на:

- Управлінні комунікаціями та підвищенні обізнаності.
- Отриманні освіти та навчання.
- Розширенні керівництва та підвищенні кваліфікації.
- Розробці та впровадженні технічних стандартів, моделюванні даних.
- Підтримці розвитку та реалізації ключових напрямків, протоколів з обміну інформацією та Правил захисту даних і конфіденційності.

Упорядкувати інформацію за ключовими стратегічними пріоритетами.

Покращення управління інформацією буде мати значний вплив на ефективність і продуктивність організації, чітко визначена інформаційна стратегія повинна бути узгоджена зі стратегічними пріоритетами.

Наприклад, якщо організація орієнтована на зниження вартості, то інформаційна стратегія повинна визначити засоби скорочення

витрат, підвищення ефективності операцій та прийняття рішень на основі витрат.

Не нехтувати етичними та організаційними об’ємами інформації управління.

Підвищення ефективності управління інформацією вимагає як культурні та організаційні зміни а також нові інформаційні системи. Є три основні культурні і організаційні вимоги до стратегії управління інформацією:

- Навчання та тренінг – забезпечення того, що користувачі розуміють, як користуватися ІТ-системами, ефективно вдосконалюються, щоб поліпшити якість і продуктивність.
- Вдосконалення поліції та бізнес-процесів для підвищення значення ІТ-систем та забезпечення більшої співпраці та обміну інформацією.
- Етика поведінки – створення такої культури праці, що забезпечує бажану практику повного та точного введення даних, і гарантує, що організація розглядає інформацію як цінний стратегічний актив.

Інформація повинна бути в центрі уваги сучасної поліції, тому поліція може покладатися на ефективні управління інформацією. Як результат, підсилення інформації управління є критичним елементом в підвищенні ефективності поліцейських сил.

Покращення в інформаційному менеджменті приведе до покращення у всій сфері надання доступу до відповідної якісної інформації, що забезпечить прийняття правильних рішень.

-
- | | | | | |
|----|--|----------------|----------|------|
| 1. | Maurice Philogene | United States | Policing | Lead |
| | maurice.philogene@accenturefederal.com | | | |
| 2. | James Slessor | United Kingdom | Policing | Lead |
| | james.w.slessor@accenture.com | | | |

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Дідик Наталія Іванівна,

*доцент кафедри адміністративного права та
адміністративного процесу*

*Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Сивак Юлія Михайлівна,

здобувач ступеня бакалавра

Львівського державного університету внутрішніх справ

Однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій. Темпи, з якими нові інформаційні технології зараз створюються та впроваджуються в практичну діяльність правоохоронних органів, настільки високі, що іноді навіть фахівці у галузі ІКТ, а тим більше, інші категорії користувачів не встигають оцінити масштаби й глибину всього, що відбувається.

Питання здійснення збору, обробки та використання інформації – надзвичайно актуальне і є елементом кожного кроку реформ у підрозділах Національної поліції. Робота будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних є неможливою. Це є наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом» [1, с. 202].

З кожним роком комп'ютерна злочинність зростає, а це вимагає розроблення якісно нових підходів до підготовки фахівців, у тому числі для підрозділів кіберполіції. Відповідна методика має передбачати не лише навчання прийомам виявлення, розслідування і припинення комп'ютерних злочинів, але й, передусім, озброєння фахівців сучасними знаннями, які дозволяють широко та ефективно застосовувати інформаційні технології на різних

напрямах оперативно-розшукової, слідчої й іншої службової діяльності. Складність організації протидії сучасній злочинності зумовлена низкою причин, серед яких одна з найважливіших – нестача в системі Національної поліції досвідчених професіоналів і необхідного правового, технічного та методичного забезпечення виявлення, попередження й припинення злочинів [2, с. 152].

Також необхідно звернути увагу на проблему вдосконалення нормативно-правової бази інформаційного забезпечення правоохоронних органів і інформаційного забезпечення в цілому. Як показав історичний огляд розвитку інформаційного забезпечення в Україні, протягом останнього часу зазнали змін умови його розвитку – демократія та гласність, а також стрімке провадження новітніх технологій. Цілком логічно, що у зв'язку з цим деякі сфери інформатизації правоохоронної діяльності залишаються не до кінця врегульованими, що вимагає проведення ґрунтовного аналізу змісту нормативно-правової бази.

Ефективно протидіяти злочинності під силу лише правоохоронцям, які досконало володіють законодавчою базою, мають належний рівень професійної підготовки, достатній досвід боротьби з сучасними видами злочинів. Однією з важливих умов підвищення якості підготовки фахівців у галузі інформаційних технологій є формування високих моральних якостей у курсантів та слухачів, вироблення імунітету до скоєння правопорушень. Це завдання є особливо актуальним, оскільки сьогодні досить вільно розповсюджуються видання, де описуються технології здійснення комп'ютерних злочинів [3].

Ми вважаємо, що з метою удосконалення інформаційного забезпечення правоохоронних органів необхідно приводити у відповідність до завдань правоохоронних органів інформаційно-аналітичні системи; забезпечити єдність системи інформаційного законодавства шляхом прийняття Інформаційного кодексу України; здійснювати фінансову підтримку правоохоронних органів з метою забезпечення високотехнологічного озброєння; створити спеціальні курси для працівників правоохоронних органів, з метою підвищення кадрового потенціалу.

Для ефективної реалізації функції інформаційного забезпечення правоохоронних органів, потрібні об'єктивно встановити та закріпити критерії збору інформації, встановити порядок її обробки. Доцільно зауважити, що технологія збору і обробки даних повинна охоплювати усі напрями діяльності складових елементів системи Національної поліції, визначені Законом України «Про Національну поліцію», та складових системи МВС України (Державної служби України з надзвичайних ситуацій, Державної міграційної служби України, Державної прикордонної служби України, Національної гвардії України).

Все це дозволить, ефективному функціонуванні єдиного інформаційного простору, що буде сприяти суттєвому розширенню інформаційної бази, необхідної для інформаційно-аналітичної діяльності, зниженню витрат на процеси пошуку, обробки, зберігання та відбору вихідної інформації, виявлення тих аспектів, в рамках яких слід здійснювати аналітичну обробку інформації, виявлення суті та динаміки просторово-часових і причинно-наслідкових зв'язків між досліджуваними фактами, явищами, процесами. У результаті спочатку наявні дані перетворюються в нову інформацію про стан злочинності та результати оперативно-службової діяльності поліції, оперативно-довідкову, розшукову, криміналістичну, архівну, науково-технічну і іншу інформацію більш високого порядку, яка дозволяє приймати обґрунтовані оперативні і управлінські рішення, здійснювати координацію та взаємодію.

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної в діяльності поліції, базується на конструкті єдиного інформаційного простору системи МВС України, який логічно визначити як сукупність спеціалізованих баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, суб'єктів інформаційно-аналітичної діяльності, які функціонують на основі єдиних принципів і за загальними правилами забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян [14].

Одним з основних завдань функціонування системи інформаційного забезпечення діяльності стала інформатизація підрозділів,

що здійснюють оперативно-розшукову діяльність. В Україні вже накопичено чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. Наказом Національної поліції України від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції «102» Національної поліції України, який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату НП України. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розробленні проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також оброблення персональних даних в органах і підрозділах поліції [4].

Сучасні комп'ютерні системи повинні широко використовуватися і в процесі викладання у вищих навчальних закладах, а також для підвищення кваліфікації суддів, слідчих та оперативних працівників. З цією метою вже створено ряд імітаційних навчальних систем, у яких моделюються як окремі слідчі дії (наприклад, огляд місця події), так і хід розслідування загалом: програми-тренажери «Вбивство», «Слідчий», «Рекет», «Міраж».

Отже, можна зробити висновок, що основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

- 1) удосконалення форм та методів управління системами інформаційного забезпечення;
- 2) централізація та інтеграція комп'ютерних банків даних;
- 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;
- 4) розбудова та широке використання ефективних та потужних комп'ютерних мереж;

- 5) застосування спеціалізованих засобів захисту інформації;
- 6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні [5, с. 12].

Тому, інтеграція інформаційних технологій в діяльність органів Національної поліції України дозволяє удосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а саме, оперативно отримувати доступ до певних відомостей, необхідних для виконання їх службових завдань, кваліфіковано здійснювати їх аналіз, використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп'ютерних технологій дає змогу для створення нових методів роботи, підвищення професіоналізму кожного працівника правоохоронних органів.

-
1. Танкушина Т.Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність // Вісник Запорізького національного університету: збірник наукових праць. Юридичні науки: [у 2 ч.]. Запоріжжя: Запорізький національний університет, 2011. Ч. I. – 224 с.
 2. Мовчан А.В. Модель підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України. Інформаційні технології і засоби навчання. 2018. Том 66. №4. С.149-161.
 3. Маклаков Г.Ю. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crimeresearch.ru/articles/Maklakov0105/10/>
 4. Департамент інформаційної підтримки та координації поліції «І02» Національної поліції України. Національна поліція України: веб-сайт URL: <http://www.npu.gov.ua/uk/publish/article/1820541>.
 5. Інформаційні технології в правоохоронній діяльності: Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. К., НАВСУ. 2013. 82 с.

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Тронько Ольга Володимирівна,

*провідний науковий співробітник відділу з вивчення проблем
протидії організованих злочинності у сфері державної безпеки
Міжвідомчого науково-дослідного центру з проблем боротьби з
організованою злочинністю при РНБО України,
кандидат юридичних наук*

Довгаль Юрій Сергійович,

*молодший науковий співробітник відділу з вивчення проблем
забезпечення інформаційної та кібернетичної безпеки, захисту
вітчизняного інформаційного простору Міжвідомчого науково-
дослідного центру з проблем боротьби з організованою
злочинністю при РНБО України*

Постановка проблеми. У рамках гарантування національної безпеки нашої держави пріоритетного значення набуває мінімізація уразливості державних інформаційних ресурсів, інформаційних ресурсів суб'єктів приватного права, а також мережевої інфраструктури органів державної влади та органів місцевого самоврядування у разі різноманітних надзвичайних ситуацій, зокрема таких, що виникли під час зламу, навмисного пошкодження, кібератак тощо. Зважаючи на це важливу роль відіграє активізація зусиль усіх суб'єктів гарантування інформаційної безпеки держави у напрямі адекватної державної політики інформаційної безпеки, яка також повинна враховувати усі форми та прояви інформаційних загроз і визначати ефективні шляхи протидії їм [1].

Національна поліція України як центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, також не може стояти осторонь проблем, що стосуються інформаційної сфери нашої держави. Адже відсутність адекватних дій на такі загрози є фактором, що призводить

до вчинення багатьох злочинів проти цілісності та недоторканості нашої держави, власності, встановленого порядку дій органів державної влади тощо [1].

Значним кроком на шляху створення системи нормативно-правового регулювання забезпечення інформаційної безпеки України стало прийняття Верховною Радою України Конституції України від 28 червня 1996 р. У ній, зокрема, є норми, що стосуються забезпечення інформаційної безпеки України та які є визначальними для побудови національної системи інформаційної безпеки (статті 1-8; 15; 18; 19; 34; 78; пункти 2 і 9 ч. 1 ст. 85; пункти 19-20 ч. 1 ст. 106; ст. 182; пункти 7 і 10 ст. 138).

Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Щодо національних інтересів інформаційна безпека означає такий стан захищеності інформаційних ресурсів особи, суспільства й держави, який забезпечує реалізацію та прогресивний розвиток життєво важливих для них інтересів. Щодо можливих негативних впливів різних видів інформаційної безпеки – це захищеність інформації та підтримуючої інфраструктури від випадкових чи навмисних природних або штучних впливів, які можуть заподіяти шкоду їхнім власникам або користувачам. Інформаційна безпека також означає рівень захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави і нейтралізації негативних наслідків інформатизації суспільства.

Проблема інформаційної безпеки розглядається у трьох основних аспектах:

- захист інформації,
- контроль за національним інформаційним простором,
- достатнє інформаційне забезпечення державних і недержавних органів, громадських, приватних організацій.

Технічне забезпечення оперативних підрозділів НПУ є актуальним з огляду на новачі, що містяться в положеннях КПК України, які закріплюють сучасні інструменти для боротьби зі злочинністю

та застосування яких повинно чітко відповідати вимогам чинного законодавства.

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

Інформаційні технології – це сукупність методів, інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця розташування.

Для вирішення оперативно-розшукових завдань на сьогодні накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, зокрема негласних слідчих (розшукових) дій.

Інформаційне забезпечення правоохоронної діяльності НПУ відкривають нові можливості для попередження злочинності та сприяють ефективному і точному прийняттю рішень з метою розкриття злочинів. Беззаперечно, що використання інформаційних технологій може стати чи не головним чинником зміцнення законності, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою.

Важлива роль розвитку інформаційного забезпечення у процесі здійснення правоохоронної діяльності НПУ підтверджується у працях таких науковців, як І. Арістова, В. Тацій, В. Супрун, О. Береза тощо [2].

Важливу роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказом НПУ від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції (далі – ДІПКП) «102» НПУ, який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-

аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату НПУ. ДПМКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розробленні проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також оброблення персональних даних в органах і підрозділах поліції [3].

Завданнями використання інформаційно-комунікаційних технологій у підрозділах НП України є:

- забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами НП України для розкриття, розслідування, попередження кримінальних правопорушень і розшуку злочинців;
- збирання, оброблення та узагальнення оперативної, оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності підрозділів НП України;
- забезпечення динамічної та ефективної інформаційної взаємодії всіх галузевих служб і підрозділів
- НП України, інших правоохоронних органів, державних установ, різних груп громадськості, мас-медіа;
- забезпечення захисту інформації [4].

Інформаційно-аналітична робота в органах НПУ здійснюється всіма галузевими службами, всіма підрозділами в межах їх компетенції. Вимоги до організації цієї роботи для кожного рівня системи НПУ різні у зв'язку з різними завданнями цих органів і їх неоднаковими можливостями. Як складова частина управлінської діяльності інформаційно-аналітична робота притаманна кожному органу, кожному його структурному підрозділу, хоча, маючи забезпечуючий характер, вона більш розвинута на рівні МВС України, ГУМВС, УМВС, де створені спеціальні інформаційні та

аналітичні підрозділи. Тому ознайомлення з питаннями інформаційно-аналітичної роботи в органах НПУ повинне стати складовою частиною знань, які отримують курсанти системи МВС України в процесі навчання.

Крім того, якась частина курсантів після закінчення навчання буде працювати в інформаційних та аналітичних підрозділах НПУ, тому знання інформаційно-аналітичної роботи їм необхідне. Треба знайомити курсантів з методикою проведення конкретного аналітичного дослідження, з етапами, які необхідно пройти при проведенні цього дослідження. Треба мати уявлення про джерела отримання інформації при проведенні інформаційно-аналітичної роботи.

Найважливішими джерелами інформації є державна статистична звітність правоохоронних органів, дані економічної, соціальної, демографічної статистики, результати вивчення громадської думки про злочинність і роботу правоохоронних органів. Комплексний аналіз цих матеріалів дає змогу отримати найбільш повну характеристику стану та динаміки злочинів, контингенту осіб, які їх вчинили, факторів, які обумовлюють стан та динаміку злочинності, а також ефективність заходів боротьби зі злочинністю. Курсантів треба знайомити з методикою проведення статистичної роботи в правоохоронних органах як частини інформаційно-аналітичної роботи, документами, які використовуються для обліку правопорушень.

Прийняття управлінських рішень у сфері боротьби з правопорушеннями і забезпечення правопорядку, як правило, повинен передувати прогноз злочинності. Тільки тоді рішення стають ефективними, такими, що дозволяють попереджувати негативні тенденції. Прогнозування злочинності становить процес визначення ймовірності злочинних дій, в основі якого лежить вивчення емпіричних даних і облік тенденцій розвитку. Курсантів необхідно знайомити з формами та методами математичного прогнозування злочинності. Питання інформаційно-аналітичної роботи не можливо вирішувати без використання комп'ютерної техніки. Тому в процесі вивчення цих питань курсантам необхідні знання як з юридичних дисциплін, так і з комп'ютерних наук. Таким чином, інформаційно-аналітичне забезпечення правоохоронних органів є необхідною умовою їх ефективної діяльності, а знання

питань проведення інформаційно-аналітичної роботи є необхідною складовою частиною знань, які повинні отримати курсанти системи МВС України.

Підсумовуючи викладене вище, можна зазначити, що впровадження та використання нових інформаційно-комунікаційних технологій є головною умовою покращення роботи із встановлення підозрюваного або його розшуку, а також діяльності підрозділів НП України та функціонування правоохоронної системи загалом. При цьому є проблеми фінансового забезпечення, низький рівень володіння співробітниками відповідними інформаційними ресурсами та навичками роботи з новою технікою або новими системами. У нинішніх умовах швидкого технічного процесу кожен працівник НП України повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Крім того, оперативним працівникам необхідно проходити курси підвищення кваліфікації з метою отримання нових знань, умінь і навичок під час застосування в повсякденній роботі інформаційних технологій.

-
1. Негодченко В.О. Специфіка діяльності органів Національної поліції України щодо гарантування інформаційної безпеки. URL: http://www.lj.kherson.ua/2017/pravo01/part_2/12.pdf.
 2. Роль і значення інформаційних технологій в оперативно-розшуковій діяльності. URL: http://vjhr.sk/archive/2016_4/part_1/37.pdf
 3. Департамент інформаційної підтримки та координації поліції / Національна поліція України URL: <http://old.npu.gov.ua/mvs/control/main/uk/publish/article/1820541>
 4. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія] Б.А. Кормич. О.: Юридична література. 2003. 271 с.

НОВІТНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ЗНИЖЕННЯ СУБ'ЕКТИВІЗМУ В СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ, АЛЕ НЕ ЗАВЖДИ...

Дуфенюк Оксана Михайлівна,

*доцент кафедри криміналістики,
судової медицини та психіатрії*

*Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Суб'єктивізм супроводжує кожен сферу людської діяльності, у тому числі судово-експертну. Суб'єктивізмом експерта вважається його оцінка певних аспектів криміналістичних досліджень, яка у зв'язку з відсутністю можливості застосування цілковито наукових методик ґрунтується на його досвіді, знанні та внутрішньому переконанні [1, s. 476].

Повністю виключити суб'єктивізм у судово-експертній діяльності практично неможливо, оскільки навіть коли в основі порівняльного дослідження основну функцію виконує складний апаратний комплекс, експерт готує матеріали, проби, зразки, застосовує індикатори, визначає тривалість операцій, температуру, виставляє інші параметри, а отримавши результати, їх інтерпретує. Комп'ютерного наукового робота-експерта, який би виконував усі процеси самостійно поки не існує. Тому, безумовно, перед експертами на порядку денному, передусім, стоїть алгоритмізація діяльності в усіх типових ситуаціях, починаючи від роботи на місці вчинення злочину і завершуючи експериментальними та порівняльними дослідженнями в лабораторних умовах та формулюванні кінцевих висновків. При цьому кожна стадія передбачає комплекс заходів, спрямованих на виключення контамінації чи трансферу слідів; впровадження правил, що забезпечують особистий захист експерта при роботі зі дослідницьким матеріалом та застосуванні методик досліджень; застосування таких технологій, що з великим ступенем ймовірності надають правильні результати з мінімальною участю експерта як в процесі безпосереднього експерименту (дослідження, порівняння, аналізу), так і в процесі тлумачення

отриманих результатів. Експерту на основі отриманих даних залишається тільки формулювання кінцевих висновків.

У науковій літературі триває дискусія щодо критеріїв, якими повинен керуватися експерт при оцінці об'єктів дослідження, визначенні ідентифікаційних ознак, ступеня їх збігу. Одні вчені вважають, що в основі таких оцінок повинні бути якісні параметри, інші науковці говорять про необхідність зміни парадигми криміналістики та перехід до кількісних параметрів. При цьому кількісні дослідження (фізико-хімічні, генетичні, трасологічні, дактилоскопічні та багато ін.) вважаються більш об'єктивними, оскільки в основі висновків лежать заміри і статистичний аналіз. Натомість якісні дослідження суб'єктивні [2, s. 26–46]. Проте і кількісний, і якісний підхід не виключають можливості помилки. Особливої гостроти тема суб'єктивізму судово-експертної діяльності набула після відомої справи Б. Мейфілда (B. Mayfield). Розглянемо цей казус докладніше.

Б. Мейфілд, 1966 р. народження, громадянин США, проживає у штаті Орегон, діючий адвокат, одружився з єгиптянкою та прийняв ісламське віросповідання. У травні 2004 р. був заарештований у зв'язку з підозрою у вчиненні терористичних актів у Мадриді на залізничному вокзалі. На місці події під час огляду було виявлено сумку, в якій містились детонатори, і з неї було вилучено відбиток пальця руки. Мадридська поліція тісно співпрацювала з Інтерполом та ФБР. Останні взялися за проведення дактилоскопічної експертизи і зі стовідсотковою впевненістю категорично констатували збіг у системі та тотожність виявленого сліду та зразка відбитка пальців Б. Мейфілда (його відбитки містилися у базі даних у зв'язку з затриманням у 1984 р.). Втім мадридські спеціальні служби мали сумніви щодо обґрунтованості отриманих результатів і, в підсумку, все ж виявили, що відбиток залишений О. Даудом (O. Daoud), вихідцем з Алжирії, який виявився дійсно виконавцем терористичного акту. Б. Мейфілда звільнили з-під арешту і він зміг відсудити 2 млн. доларів США як відшкодування за неправомірний тимчасовий арешт [3, s. 333–334; 4].

Міжнародна спільнота створила спеціальний комітет для з'ясування причин такої ситуації. Три експерти ФБР були усунені від виконання обов'язків, а їхні висновки, видані за останні два роки,

підлягали перевірці. У підсумку було з'ясовано, що помилка була суб'єктивного характеру, а не методологічного чи будь-якого іншого. У 2006 р. світ побачив звіт ФБР щодо справи Б.Мейфілда [5].

Виявилось, що застосована комп'ютеризована канадська методика ACE-V дактилоскопічної ідентифікації видала 7 мінуцій (minutae) або точок (points), які свідчили про збіг слідів, тому наступний експерт почав перевірку з допомогою системи AFIS. У ході цієї перевірки вдалося підтвердити збіг аж 15 ознак. Експерти, які мали б верифікувати висновок першого (зокрема і керівник відділу) повірили його авторитетній думці та багатолітньому досвіду і тому винесли відповідне рішення, зберігаючи при цьому солідарність та великий ступінь довіри, бо «ми з ФБР!». Коли іспанці вказали на наявність відмінностей у слідах, американці були обурені і навіть збільшили зображення сліду, щоб продемонструвати збіги ознак другого та третього рівнів [3, s. 336].

Суб'єктивізм виявився ще й у тому, що здавалося б неможливим: збіг не тільки ідентифікаційних ознак дугових папілярних відбитків Б. Мейфілда та Д. Охнане, але й оцінка контекстуальної інформації про те, що Б. Мейфілд сповідує іслам, а ще захищав в одному із процесів підозрюваних у тероризмі осіб. Складалася наче повна картина, адже інформація сприяла тому, аби вбачати підстави для арешту невинного як згодом виявилось адвоката. Напевно таких збігів у житті стається мало, але ж можуть бути.

Помилка, яка полягала, передусім, у неврахуванні відмінних ознак, а тільки збігів, була доведена, а тому розпочався процес розробки рекомендацій, що дозволили б усунути суб'єктивізм у дактилоскопічних дослідженнях. На цій підставі було впроваджено додаткові вимоги до документації ACE-V; впроваджено «сліпу верифікацію», коли результат першого дослідження залишається невідомим для експерта-версифікатора; експерт-верифікатора зобов'язано шукати не тільки збіги, але й розбіжності ознак; впроваджено додаткову верифікацію у пріоритетних справах; врегульовано правила розділення справ, відповідно до нового порядку дослідження повинні робити звичайні експерти, а не керівники, оскільки роки праці не завжди впливають на вироблення умінь [3, s. 336–338].

Оцінка чи то результатів конкретних експертних досліджень, чи то всього висновку експерта завжди буде суб'єктивна. Це закономірність, яка впливає із психології людини, незалежно від того, які функції вона виконує (слідчий, суддя, прокурор, експерт, захисник, присяжний). Світова спільнота продовжує працювати над механізмом стандартизації, алгоритмізації, «цифризації» наукових досліджень, адже тоді експерту залишиться невелике поле для самодіяльності, а значить знизиться й ризик допущення помилок суб'єктивної природи при наданні висновку процесуальним та судовим органам у кримінальному провадженні.

-
1. Moszczyński J. Obszary subiektywizmu w badaniach identyfikacyjnych. Wybrane zagadnienia. Kryminalistyka i inne nauki pomostowe w postępowaniu karnym. J. Kasprzak, B. Młodziejowski (red.). Olsztyn: Wydawnictwo PRINT GROUP Sp. z o.o., 2009. S. 475–482.
 2. Moszczyński J. Przejście od badań jakościowych do ilościowych – nowy paradygmat kryminalistyki czy tylko akademicka dyskusja. Paradygmaty kryminalistyki. J. Wójcikiewicz, V. Kwiatkowska-Wójcikiewicz (red.). Kraków: Wydawnictwo UJ, 2016. S. 26–43.
 3. Kwiatkowska-Darul V., Wójcikiewicz J. Czy „niewinny nie musi się bać?» Rozważania na kanwie sprawy Brandona Mayfielda. Kryminalistyka i nauki penalne wobec przestępczości. Księga pamiątkowa dedykowana Profesorowi M. Owocowi. Poznań: Wydawnictwo Poznańskie, 2008. S. 333–342.
 4. Brandon Mayfield. URL: <https://www.nytimes.com/topic/person/brandon-mayfield>.
 5. A Review of the FBI's Handling of the Brandon Mayfield Case. URL: <https://oig.justice.gov/special/s0601/exec.pdf>.

ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ СУБ'ЄКТА В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

Єсімов Сергій Сергійович,

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

Традиційний документ виконує функцію фіксації певної значущої інформації. Коли на практиці використовується такий документ то мова йде про форму, в якій він складений (умовно матеріальна річ, яку можна пред'явити, вивчити, передати, досліджувати, видозмінити) і інформація яка в ньому міститься. За допомогою документа в формі матеріального об'єкта можна встановити істинність інформації, що міститься в ньому. Можливо, для цього необхідно буде піддати його експертизі з перевірки його справжності, на відсутність в ньому змін і ін. Крім того, паперовий оригінал документа є в обмеженій кількості примірників, відомому заздалегідь.

Наприклад, в договорі зазвичай вказується, що він складений у певній кількості примірників, які мають однакову юридичну силу. Відповідно поява ще одного ідентичного екземпляра є копією документа, і може бути перевірено за допомогою відповідного виду експертизи. Однак реалії такі, що суспільство рухається шляхом впровадження електронного документообігу та відмови від традиційних паперових носіїв інформації.

В даний час обмін інформацією в електронному вигляді набула глобального обсягу у всіх сферах життєдіяльності людства. Однак юридичний аспект легальності та легітимності електронного документообігу, на наш погляд відстає від швидкості впровадження його в юридичний оборот.

Питання процесуальної допустимості і доказової сили електронних документів поки не достатньо розроблені, а відповідно інформація, що міститься в електронних документах не є надійною і відповідним чином захищеною. У зв'язку з цим, слідом за вдосконаленням інформаційних технологій необхідно створювати

законодавчу основу не тільки електронного документообігу, а й юридичні механізми захисту даних, що створюються та переданим електронним способом, удосконалювати юридичний статус електронного документа.

В Україні законотворча робота в цьому напрямку ведеться досить активно. Разом з тим, позначена тематика не може бути нами розкрита без посилань на закон України від 5 жовтня 2017 року № 2155-VIII «Про електронні довірчі послуги».

Наприклад, Закон від 5 жовтня 2017 року № 2155-VIII «Про електронні довірчі послуги» закріплює, що інформація в електронній формі, підписана кваліфікованим електронним підписом, визнається електронним документом, рівнозначним документом на паперовому носії, підписаного власноручним підписом, може застосовуватися в будь-яких правовідносинах відповідно до законодавства, якщо тільки в законі не вказано про необхідність складання документа виключно на паперовому носії.

Зазначений закон зрівняв, практично, кваліфікований електронний підпис і власноручний підпис особи, від імені якої складено юридично значущий документ.

Електронний цифровий підпис є обов'язковим реквізитом електронного документа. Електронний цифровий підпис служить захистом від підробки, використовується в процесі криптографічного перетворення інформації за допомогою закритого ключа електронного цифрового підпису та дозволяє ідентифікувати власника сертифіката ключа підпису, повинен підтверджувати справжність інформації в електронному документі, відсутність її спотворення. Електронний підпис необхідний, як правило, для оформлення та подачі різних заяв і документів через Інтернет портали.

Якщо в законах і підзаконних актах, що вступили в силу до 5 жовтня 2017 року передбачалося використання електронного цифрового підпису, то мова йде про застосування кваліфікованого електронного підпису. В інших випадках документи складаються та підписуються простим електронним підписом. Виключення вказувалось безпосередньо в законі, коли він прямо зобов'язує використовувати кваліфікований електронний підпис.

Кабінет Міністрів України визначає вид електронного підпису (простий або кваліфікований), що проставляється при направленні звернень на Інтернет портали за отриманням адміністративних послуг.

Якщо довіреність на отримання послуги, видається організацією, то така довіреність підписується кваліфікованим електронним підписом посадової особи організації, а від імені фізичної особи довіреність свідчить кваліфікованим електронним підписом нотаріус. Якщо в законі або підзаконному акті встановлено обов'язок подати нотаріально завірени копії документів, то електронна копія (електронний образ копії документа) засвідчується кваліфікованим електронним підписом нотаріуса.

Якщо закон не зобов'язує прикладати нотаріальні копії документів, то копії підписуються простим електронним підписом заявника. Необхідно відзначити, що закон передбачає можливість при отриманні адміністративної послуги подавати документи, підписані кваліфікованим електронним підписом в тому випадку, коли потрібна простий електронний підпис, але не навпаки.

Електронно-цифровий підпис (далі за текстом – ЕЦП) забезпечує ідентифікацію (електронна форма документа підписана власником ЕЦП) і автентичність (зміст не зазнало змін з моменту підписання) електронного документа.

Разом з тим, проблема існує в наступному – ЕЦП не може безпосередньо характеризувати особу її власника. Взаємозв'язок ЕЦП з конкретно людиною обумовлено не біологічним, а соціальним фактором, в тому числі прив'язка цифрового коду до конкретної особи опосередковується сукупністю організаційних, технічних і правових умов.

Дійсність ЕЦП передбачає, що особа, яка підписала електронний документ, знає цифровий код – закритий ключ ЕЦП. Для того щоб встановити, хто в дійсності затвердив електронний документ – власник сертифіката ключа або хтось інший, який отримав інформацію про закритий ключ, необхідно встановити факт: справжність ЕЦП і ідентифікацію людини, що її поставив.

Коли ідентифікуємо особу в традиційному розумінні, то можуть бути використані біометричні дані, в тому числі власноручний підпис. А визначити ідентичність особи безпосередньо за ЕЦП неможливо.

Тому в спірних ситуаціях визначити, що саме ця особа проставляє на електронному документі ЕЦП, можна тільки в результаті процесуального доказування в ході судового розгляду. Крім того, цифрова сутність ЕЦП дозволяє не відрізняти копії одного і того ж електронного документа, відповідно всі копії будуть рівнозначні. Природна різниця між оригіналом документа і його копіями, при складанні документів в електронному вигляді відсутня.

Ще одне питання ідентифікації – це проблема забезпечення збереження секретних ключів, так як ЕЦП віддільна від власника, на відміну від власноручного підпису.

Секретний ключ до ЕЦП є не що інше, як комп'ютерний файл, що знаходиться на пристрої підписанта, відповідно може існувати окремо від власника. Доступність до секретного ключа здійснюється за допомогою пароля, що фіксується на інтелектуальній карті або іншому пристрої ідентифікатора. Інтелектуальна карта може в принципі бути втрачена, втрачена або передана іншій особі. При власноручному підпису біометричні параметри людини практично не можуть бути змінені: характер написання, ступінь натиску, індивідуальні петлі, підкреслення тощо. ЕЦП дозволяє зробити лише умовний висновок про автора електронного документа, так як сам підпис не містить в собі біометричну інформацію автора підпису.

Усі стадії застосування ЕЦП (створення, застосування, посвідчення та перевірка) автоматизовані, однак при автоматизації перевірити підпис за допомогою звичних методів (візуального огляду, зіставлення тощо) неможливо. Це може створювати ілюзію дійсності. Тому для використання ЕЦП і перевірки на ідентичність необхідне спеціальне технічне, організаційне та правове забезпечення.

Відсутність повноцінного правового регулювання, що регламентує порядок зв'язування електронного цифрового підпису з

фізичною особою, породило проблеми правозастосовної практики. Якщо третій особі з яких-небудь причин стане відомий закритий ключ, то відрізнити підробку підпису до анулювання ключів буде неможливо. Крім того, можливі випадки, коли застосування аналога власноручного підпису дозволить зацікавленим і не доброчесним особам з легкістю відмовлятися від свого підпису на електронному документі.

-
1. Про електронні довірчі послуги : закон України від 05.10.2017р. № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 400.

БЕЗПЕКА СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Живко Зіна Богданівна,

*професор кафедри менеджменту
Львівського державного університету внутрішніх справ,
доктор економічних наук, професор*

Руда Ольга Іванівна,

*доцент кафедри економіки та економічної безпеки
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент*

Мандрик Михайло Степанович,

*завідувач кафедрою інформатики Львівського державного
коледжу харчової і переробної промисловості НУХТ*

Підвищення рівня захищеності інформаційного середовища підрозділів Національної поліції України (НПУ) є, на сьогодні, актуальним завданням. Одними з визначальних, у цьому плані, є нормативно-правові чинники – закони, стандарти, галузеві нормативні документи, рішення тощо. Мета в них одна – забезпечити виконання організаційно-технічних заходів з захисту інформації (ЗІ), що дозволить підняти рівень захищеності спеціалізованих інформаційних систем (СІС) [1].

В сучасних умовах забезпечення безпеки СІС підрозділів Національної поліції України має стати державним завданням. Особливої уваги вимагає захист критичних інформаційних активів, а також централізованих баз даних.

Несанкціонований доступ до інформаційних активів може істотно ускладнити виконання завдань оперативними підрозділами НПУ, тому проблема створення ефективної системи ЗІ набуває дуже важливого значення. Автори вважають, що така система ЗІ повинна бути, у першу чергу, комплексною і адаптивною.

З розвитком інформаційних технологій (ІТ) і систем ЗІ виникла потреба уніфікувати вимоги до їх проектування та впровадження забезпечивши необхідний рівень стандартизації. Одним з найважливіших напрямів цієї роботи є процеси гармонізації та введення в дію системи сучасних міжнародних стандартів інформаційної безпеки ISO/IEC серії 27000, яка постійно доповнюється новими документами.

Серія стандартів є фреймворком для розроблення, впровадження, функціонування, моніторингу, аналізу, підтримки та розвитку системи менеджменту інформаційної безпеки (СМІБ) на загальному рівні, їх аудиту і сертифікування.

Дотримання принципів стандартів ISO/IEC серії 27000 забезпечує керування і контроль доступом, розроблення та обслуговування апаратно-програмних комплексів, керування безперервністю інформаційних процесів. Відповідність вимогам стандартів ISO/IEC серії 27000 і дотримання національних правових норм з інформаційної безпеки (ІБ) є запорукою створення ефективної системи ЗІ. Разом з тим, відзначимо, що це є всього лише один з аспектів стратегії системи управління інформаційними технологіями у підрозділах НПУ [2].

Такими стандартами є: ISO/IEC 27001 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційною безпекою.

Відповідно до вимог стандарту процес розроблення СМІБ подається такими етапами: планування – етап планування забезпечує правильне завдання контексту і масштабу СМІБ, оцінюються ризики, пропонується відповідний план оброблення цих ризиків;

реалізування – етап реалізування впроваджує ухвалені рішення, які були визначені на етапі планування; аналіз захищеності – етап оцінювання ефективності та надійності функціонування створеної СМІБ, проведення аудиту ІБ, виявлення недоліків; реагування – етап виконання коригувальних дій з покращення функціонування СМІБ, реагування вимагає первісного інвестування, документування діяльності, формалізування підходу до управління ризиками, визначення методів аналізу.

Як основні об'єкти області функціонування СМІБ, розглядаються наступні види активів:

- інформаційні активи: інформація та дані у довільному вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, (до цього виду необхідно віднести знання працівників, бази даних та системи біометричного ідентифікування, документація, методичні матеріали, описи процедур, інформація на фізичних носіях);
- програмне забезпечення: прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та довільне інше програмне забезпечення, незалежно від форми отримання (придбання, власного розроблення, таке, що вільно розповсюджується), яке використовується працівниками для роботи та у процесі взаємодії з іншими службами;
- фізичні активи: працівники, апаратні засоби комп'ютерних мереж і мережеві технології, сервери, робочі станції, міжмережеві екрани, телекомунікаційне обладнання, обладнання зв'язку), приміщення, виробниче обладнання, технічні засоби;
- сервісні активи: інформаційні та комунікаційні сервіси (корпоративні комп'ютерні мережі спеціального призначення, Internet, E-mail, спеціальні канали зв'язку), інші технічні сервіси (опалення, освітлення, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, трансмісії та знищенням активів, усі юридичні та фізичні особи, організації,

установи та підприємства (а також їх працівники), яким передані певні послуги на ІТ-аутсорсинг.

Для кожного активу визначаються можливі ризики та шляхи їх мінімізування, тобто рекомендуємо використати ризик-орієнтований підхід.

СМІБ повинна носити процесний характер і ґрунтуватися на моделі організації процесів PDCA (цикл Демінга-Шухарта: Plan-Do-Check-Act): створення – ідентифікування активів, менеджмент ризиків; впровадження – етап реалізування відповідних заходів з управління ІБ; перевірка – моніторинг і аналіз; дію – підтримання у працездатному стані і досягнення необхідного рівня підготованості працівників.

Істотним чинником ефективного здійснення цих принципів є сполучний цикл діяльності, який гарантує, що СМІБ постійно спрямована на поточні ризики. Важливо своєчасно оцінити наявність ризиків, пов'язаних з безпекою СІС.

Оцінювання ризиків, на думку авторів, повинно провадитися за чотирма основними критеріями безпеки:

- доступність – забезпечення безперервного доступу до інформаційних та супутніх активів СІС, сервісів згідно з наданими користувачам повноваженнями та правами у мінімально необхідному обсязі;
- цілісність – захист точності/коректності та повноти активів і методів оброблення інформації;
- конфіденційність – забезпечення доступності до інформаційних активів тільки для офіційно авторизованих користувачів у мінімально необхідному обсязі;
- спостережність – забезпечення можливості визначення – хто, що і коли робив з тим, або іншим інформаційним активом (забезпечення принципу невідмови від вчинених дій).

Впроваджуючи інформаційну стратегію при розробленні СМІБ вважаємо за необхідне звернути увагу на теорію та практику інформаційного аудиту, який дає можливість отримати цілісну та об'єктивну картину стану всієї СІС та її окремих елементів,

локалізувати притаманні проблеми з метою створення ефективної і оптимальної програми розвитку забезпечення інформаційної безпеки.

В умовах впровадження технології систем з відкритою архітектурою, які вирізняються складною взаємодією СІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (мобільність) та іншими особливостями, питання впровадження СМІБ набуває все більшої ваги.

Тривалий час аудит безпеки СІС розглядався як окремий незалежний сервіс який супроводжувався створенням і впровадженням стандартів аудиторської діяльності у сфері інформаційних технологій. Як правило, це закриті стандарти.

Такий підхід не відповідає одному із головних завдань аудиту – результати аудиту повинні бути об'єктивними, неупередженими і такими, що можуть бути повторені та відтворені довільним аудитом, у кращому випадку – зовнішнім, який використовуватиме таку ж методику аудиту.

На відміну від закритих стандартів аудиту, існують відкриті стандарти аудиту безпеки СІС які окреслюють організаційно-правову структуру аудиту ІБ. Відкриті стандарти пов'язують ІТ і дії аудиторів, об'єднують і погоджують багато критеріїв у єдиний ресурс, що дозволяє на сучасному рівні впровадити систему менеджменту інформаційною безпекою у СІС, враховують практично всі особливості СІС (на програмно-апаратному рівні) довільного масштабу і складності.

Вважаємо доцільним коротко зупинитися на аналізі нового стандарту ISO/IEC 27035 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки», який надає практичні рекомендації з виявлення, реєстрації і оцінки випадків порушення інформаційної безпеки. Стандарт поширюється на широкий діапазон інцидентів інформаційної безпеки, навмисних чи випадкових, викликаних технічними або фізичними причинами [3].

Інциденти ІБ становлять загрозу для СІС внаслідок виникнення потенційної можливості НСД до інформаційних активів, виходу з ладу мережесервісів, перехоплення ідентифікаторів, модифікування Web-сайтів, крадіжки персональних даних та інших інцидентів.

Знання принципів, моделей, процедур відіграє важливу роль для повного розуміння даного стандарту. Ключовим елементом ідеології стандарту є аналіз інцидентів з метою визначення які інформаційні активи СІС від яких інцидентів необхідно захищати і якою мірою у кількісних та якісних показниках оцінити потенційні втрати, а також надає модель оцінювання можливості для оброблення інцидентів, цілі та засоби керування інцидентами ІБ.

Негативні наслідки широкого кола загроз можна зменшити, використовуючи підхід до управління інцидентами інформаційної безпеки, описаний в новому міжнародному стандарті ISO/IEC 27035.

-
1. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: <https://www.cyberpolice.gov.ua/strategy-2020/>.
 2. Rudyj T. Management in specialized information systems of the departments of the National police of Ukraine: monograph / T. Rudyj, Z. Zhyvko, O. Ruda, M. Zhyvko / Management of the 21st century: globalization challenges / In edition I.A. Markina, Doctor of Economic Sciences, Professor // Nemoros s.r.o., Rubna 716/24, 110 00, Prague, Czech Republic, 2018. .P. 84-93.
 3. Серєда В.В. Нормативно-правові аспекти застосування міжнародних стандартів в системі управління безпекою підприємств / В.В. Серєда, З.Б. Живко, Т.В. Рудий / Сучасні проблеми інформатики в управлінні, економіці, освіті та подоланні наслідків Чорнобильської катастрофи: [Матеріали XVI міжнародного наукового семінару] / за наук. ред. д.е.н., проф. М. М. Єрмошенка, д.е.н., доц. І.Ю. Штулер. – К.: Національна академія управління, 2017. – С. 69-73.

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК НЕВІД'ЄМНА СКЛАДОВА ПОЛІЦІЇ У ЕФЕКТИВНІЙ БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Комісарчук Юлія Анатоліївна,

*доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Полійовська Марта Тарасівна,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікації та якомога більш точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і будь-якими іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, їх аналітичної підтримки [1, с. 82].

У країнах Європейського Союзу, США та інших розвинених країнах світу використання можливостей кримінального аналізу є обов'язковим для всіх правоохоронних органів. Його зміст, правила та процедури чітко визначено та врегульовано у правовому відношенні. Це, зокрема, стосується ведення оперативно-розшукової діяльності, досудового розслідування та розгляду кримінальних проваджень у суді [2, с. 2].

У зв'язку із бурхливою динамікою проведення реформ правоохоронних органів та адаптації національного законодавства до вимог міжнародного права в Україні створюється низка нових структурних підрозділів, департаментів, управлінь тощо. Так у 2017 році в структурі центрального апарату Національної поліції створено Управління кримінального аналізу (у складі кримінальної поліції), на яке покладено виконання функцій щодо координації діяльності у сфері аналізу та впровадження і розвитку моделі поліцейської діяльності, керованої аналітикою.

Діяльність кримінального аналізу орієнтовано на проведення безпосередньо аналітичної роботи у трьох напрямках, зокрема це:

Оперативний аналіз – його сутність полягає в аналізі усієї інформації щодо скоєних резонансних злочинів. Основна ціль даного аналізу полягає у координації слідчо-оперативної групи для розкриття злочину.

Тактичний аналіз – його суть полягає у картографічному нанесення позначок на місця скоєння конкретних видів злочинів, що дає змогу для оцінки оперативної обстановки, прогнозування можливих злочинів, попередження та недопущення їх вчинення.

Стратегічний аналіз – його суть полягає в обробці даних для процесів управління та прийняття рішень.

В результаті аналітичної роботи, оперативні працівники та слідчі отримують можливість використовувати готовий оперативно-аналітичний продукт, зокрема при цьому вони отримують такі переваги:

по-перше, окреслюються конкретні тенденції злочинності не лише за географічною ознакою, а й у часових рамках;

по-друге, продукт надає можливість мати більше інформації щодо місць ймовірного скоєння злочинів, що дозволяє спрямувати більше зусиль на попередження злочинів;

по-третє, працівники поліції мають більше можливостей у наданні допомоги колегам у разі потреби. [3, с. 153].

В ході здійснення аналітичної роботи джерелом інформації виступають:

1. Бази даних – в оперативно-службовій діяльності використовуються такі джерела інформації, як Інтегрована інформаційно-пошукова система Національної поліції «АРМОР» та статистична інформація надана Департаментом інформаційно-аналітичної підтримки.
2. Матеріали досудових розслідувань, у тому числі протоколи огляду місця події, допитів свідків і підозрюваних, матеріали оперативно-розшукових справ.
3. Звіти інших органів та підрозділів.

4. Повідомлення одержані із засобів масової інформації чи в ході опрацювання відкритих джерел інформації.

Обробка таких великих масивів інформації можлива лише при використанні інтелектуальних технологій, які зменшують навантаження на працівника. Найбільш поширеним аналітичним інструментом, що використовується у повсякденній роботі органів Національної поліції, є Microsoft Office (Word та Excel), хоча в деяких департаментах застосовується аналітичне програмне забезпечення (зокрема, i2 Analyst's Notebook, E-Gis maps, ArcGIS тощо) [4].

З усіх існуючих методик аналізу оперативної інформації, прийнятих на озброєння правоохоронними органами більшості розвинених країн світу, найбільш часто використовуються програмні продукти IBM i2 і ANACAPA.

IBM i2 аналітика забезпечує потужний аналіз і надає допомогу можливості візуалізації задля підвищення продуктивності аналітики і скорочення часу, необхідного для доставки високого значення інтелекту в межах швидко зростаючих наборів даних [2, с. 82]. У сфері кримінального аналізу i2, як правило, застосовується із програмними продуктами:

1. iBase – дає змогу збирати, структурувати, зберігати й оновлювати дані з різнорідних джерел, складає звіти й обробляє дані за допомогою системи візуальних запитів.
2. iBridge – дає змогу швидко вивести та об'єднати в одній діаграмі інформацію з усіх доступних баз даних.
3. iGlass – дає змогу здійснювати аналіз даних, використовуючи комбінацію запитів, графіків і діаграм.
4. Analyst's Workstation об'єднує можливості Analyst's Notebook, iBase, iGlass в свою чергу полегшує побудову графіків.

Технології IBM i2 застосовуються в діяльності аналітичних служб правоохоронних структур у процесі організації ефективних заходів із боротьби зі злочинністю.

ANACAPA застосовують для аналізу великого обсягу інформації. Що дає змогу охопити масштабну територію, врахувати значну

кількість подій або суб'єктів. Характеризується розбудованою структурою злочинних зв'язків, у яких не виправдовують себе традиційні методи пошуку та асоціювання фактів.

На даний момент ANACAPA пропонує наступні 4 базових курси:

1. Аналіз інформації в ході проведення розслідувань Criminal Intelligence Analysis.
2. Аналітичні методи розслідування Analytical Investigation Methods.
3. Аналіз фінансових махінацій Financial Manipulation Analysis.
4. Поглиблений аналіз з використанням комп'ютерних технологій Computer-Aided Analysis [5].

Використання аналітичних програм при аналізі даних забезпечує низку переваг, які допомагають підвищити ефективність і результативність роботи. У процесі інтеграції інформації здійснюється її каталогізація та введення в систему контролю і пошуку інформації, яка дозволяє легко знаходити необхідну інформацію та отримувати до неї доступ. Збір відомостей з декількох джерел підвищує ймовірність отримання ключової доказової інформації і забезпечує можливість підтвердження та перевірки достовірності відомостей [6, с. 25].

Отже аналізуючи вище викладене можна з впевненістю стверджувати, що невід'ємною складовою боротьби зі злочинністю являється аналітична робота, оскільки її мета полягає у зміцненні механізмів попередження, виявлення, документування та розслідування кримінальних правопорушень, а також налагодження механізмів моніторингу криміногенної ситуації, обміну інформацією на державному, регіональному та міжнародному рівнях. Успішна реалізація та впровадження кримінального аналізу в систему Національної поліції України надає можливість створення передумов для більш ефективного виконання суб'єктами оперативно-розшукової діяльності своїх завдань і правоохоронних функцій, що в свою чергу сприятиме підвищенню ефективності протидії різного роду злочинів.

1. Власюк О.В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України. Матеріали постійно діючого науково-практичного семінару – Х., Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2011. – Вип. 3. – Ч. 1. – С. 82–85
2. Албул С.В. Кримінальна розвідка як функція оперативно-розшукової діяльності: Європейський досвід та Українські перспективи European Reforms Bulletin: international scientific peer-reviewed journal: Grand Duchy of Luxembourg. – 2015. – № 2. – Р. 2–6.
3. Мовчан А. В. Актуальні проблеми використання кримінального аналізу в органах Національної поліції України URL:http://www2.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/konf_10_11_2017.pdf
4. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності URL: <http://euam.php7.postbox.kiev.ua/ua/news/opinion/intelligence-led-policing-the-cuttingedge-of-modern-law-enforcement/>
5. О компании Anacapa SciencesInc. URL: <http://www.spi2.ru/about/partners/anacapa/>
6. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк: Управление Организации Объединенных Наций по наркотикам и преступности. Вена, 2010. 46 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ПОПЕРЕДЖЕННЯ, ВИЯВЛЕННЯ ТА РОЗКРИТТЯ ПРАВОПОРУШЕНЬ СЕРЕД НЕПОВНОЛІТНІХ

Кононець Віта Петрівна,

*доцент кафедри адміністративного права, процесу та
адміністративної діяльності Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук*

Перша соціальна мережа з'явилась в Інтернеті у 1995 р. З часом колосальної популярності набула комунікація в соціальному сервісі «Facebook», та його російському аналозі «Вконтакте», зараз «Інстаграм», «Телеграм» першочерговою метою створення яких було спілкування, пошук своїх однокласників, колег та друзів. Засновники найпопулярніших соціальних мереж, інтернет – магнати Марк Цукерберг та Павло Дуров, щоразу оновлюють інтерфейс своїх мереж, ретельно дбаючи про стрімке розширення кола віртуальних користувачів.

Проте правоохоронні органи розглядають соціальні мережі в контексті наступних категорій: соціальні мережі як середовище формування особи потерпілого і злочинця, як засіб вчинення та як інструмент запобігання злочинів та правопорушень серед неповнолітніх.

Значна частина вчених схиляється до думки, що соціальні мережі несуть загрозу для активних користувачів-підлітків із нестійкою психікою і можуть стати для них середовищем формування особи злочинця.

У більшості випадків на здатність стати жертвою злочину в соціальних мережах впливає недотримання елементарних правил безпечної поведінки. Недбалість в питанні захисту своєї інформації дає додатковий стимул не тільки для вчинення конкретного злочину, а й є обставиною, що сприяє росту кількості злочинів, вчинених за допомогою Інтернету.

Соціальні мережі найбільш пагубно здійснюють шкідливий вплив на неповнолітніх, які в силу своїх вікових особливостей є однією із найбільш вразливих категорій суспільства. Разом з тим, спілкування в соціальних мережах може призвести до формування установки на вчинення злочину чи правопорушення.

Інформаційна складова соціальних мереж як засобу вчинення злочинів обумовлена тим, що інформація в руках злочинців виступає механізмом маніпуляції свідомістю осіб. В даному контексті розрізняють вчинення злочинів «за допомогою» та «з використанням» соціальних мереж. Актуальним є те, що застосування соціальних мереж може здійснюватись на всіх стадіях вчинення злочину: готування, замах, безпосереднє вчинення суспільно небезпечного діяння.

Сучасний етап розвитку України передбачає проведення комплексу соціально-економічних реформ, спрямованих на збереження й розвиток особистості як умови подолання існуючих у країні проблем. Соціальна дійсність засвідчує, що на тлі виховної пасивності багатьох сімей, зростання бідності, девальвації моральних цінностей, поширення наркоманії, деморалізуючого впливу засобів масової інформації має місце тенденція до збільшення числа підлітків із делінквентною поведінкою. Зараз Україна посідає одне з перших місць серед країн Європи за рівнем притягнення неповнолітніх до кримінальної відповідальності. Так, на кінець 2016 року 22360 неповнолітніх перебували на обліку в органах ювенальної превенції, 12 956 – підозрювалися у скоєнні протиправних дій, 8555 – були засуджені за скоєння різних видів злочинів.

Тому, ми акцентуємо увагу, на необхідності комп'ютерної грамотності, яку слід починати навчати ще в школі, бо діти потребують захисту в першу чергу, і саме це є одним із комунікативних навиків дитини, що є необхідною для розвитку і становлення особистості.

Однак Гонитва за псевдопопулярністю стає справжньою епідемією. Перебуваючи у вільному доступі з відкритими контентами знімки неповнолітніх, мають шанс потрапити в руки зловмисників або можуть бути використані для реклами товарів та послуг

без вашого відома. Серед іншого це ще й наражає дитину на загрозу стати жертвою збоченців, що можуть вистежити свою жертву онлайн.

Другим небезпечним наслідком є «кібербулінг» (англ. Cyberbullying) – знущання з боку однолітків в онлайн-мережі, що спричиняє проблеми з самооцінкою та психологічний дискомфорт. Нерідко до фотографій додають не лише текстовий опис, але й геомітку, що вказує на місце перебування дитини. Відомі випадки, коли злодії вистежували власників акаунтів соцмереж у реальному житті саме за такими фото. Геомітки дають змогу бачити, коли люди перебувають удома, коли ходять на роботу і, зрештою, їдуть у відпустку.

Разом з тим, на даний час соціальні мережі стали сучасним інформаційним простором, який є альтернативою засобам масової інформації і може досить продуктивно використовуватись правоохоронними органами у роботі із запобігання, виявлення та розслідування злочинів серед неповнолітніх, а також розшуку зниклих дітей. Оперативні заходи з відслідковування місцезнаходження дитини може врятувати життя та попередити настання тяжких наслідків.

Пріоритетом превентивної роботи з підлітками у середніх загальноосвітніх школах має бути первинна та вторинна профілактика правопорушень шляхом включення неповнолітнього у позитивні соціальні відносини, залучення до соціально інформаційної корисної діяльності, застосування корекційного впливу.

В даному напрямку доцільно запустити і спільний проект між операторами мобільного зв'язку та органами Національної поліції, а саме підрозділами ювенальної превенції при територіальних органах. Таким чином оператор мобільного зв'язку зможе по факту зникнення дитини розсилати абонентам «Київстар» СМС-повідомлення з даними безвісти зниклих дітей, оголошених у розшук поліцією.

Алгоритм роботи запровадження даного проекту взаємодії має наступний вигляд:

1 крок – після надходження дзвінка на лінію 102 або звернення до підрозділу поліції у батьків (або інших осіб, які їх замінюють) відбирається заява про загублену дитину;

2 крок – поліція вносить до Інформаційного Сервісу персональні дані про дитину та останнє місце її перебування;

3 крок – за згодою батьків (опікунів або особи, що їх замінюють) отримана інформація надсилається до ПрАТ «Київстар» для подальшого СМС-оповіщення абонентів;

4 крок – ПрАТ «Київстар» формує перелік абонентів «Київстар» у зоні приблизного пошуку (від 1 до 3 км) та надсилає зазначеним абонентам короткі текстові повідомлення (SMS).

У тексті повідомлень зазначається: короткий опис загубленої дитини; посилання на веб-сторінку у соціальній мережі «Facebook» «Розшук дітей» з фото та коротким номером для отримання додаткової інформації.

Такий порядок взаємодії буде ще одним прогресивним та ефективним способом використання соціальних мереж для забезпечення безпеки дітей як запорука захищеності в державі.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ В ДІЯЛЬНОСТІ ПОЛІЦІЇ ЗАРУБІЖНИХ ДЕРЖАВ

Луцький Тарас Миколайович,

*ад'юнкта кафедри кримінального права та кримінології
Львівського державного університету внутрішніх справ*

У наш час людство переживає науково-технічну революцію, в якості матеріальної основи якої служить електронно-обчислювальна техніка. На базі цієї техніки з'являється новий вид технологій – інформаційні. До них відносяться процеси, де «вихідним матеріалом» і «продукцією» є інформація.

Інформаційні технології виникають не спонтанно, а в результаті технологізації того чи іншого соціального – психологічного процесу, тобто цілеспрямованого активного впливу людини на ту чи іншу область виробництва. Неодмінною умовою підвищення ефективності праці працівників поліції є оптимальна інформаційна технологія, що володіє гнучкістю, мобільністю, й адаптивністю до зовнішніх впливів. Діяльність працівників поліції не є винятком, і використання інформаційних технологій у розвитку і функціонуванні поліції відіграє важливу роль. Без використання інформаційних технологій не можливо прийняття обґрунтованих, зважених рішень, які стосуються оцінки стану діяльності поліції та взаємозв'язку з населенням, розроблення курсу можливих напрямів реформування та модернізації напрямів діяльності правоохоронних органів в цілому.

Актуальність використання інформаційних технологій зростає й у зв'язку з інтенсивним впровадженням у діяльність правоохоронних органів засобів комп'ютерної техніки. Цей процес впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення працівників Національної поліції України, а здійснення автоматизованого пошуку відомостей щодо будь-яких об'єктів (осіб, предметів, подій) сприяє науково-організаційної праці, оптимізує збирання, зберігання, систематизацію та аналіз доказової інформації. Однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень

науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій. Єдина конкурентна перевага, яку має наша країна в цьому аспекті, це традиційно сильні ІТ-кадри, тобто в Україні дуже високий рівень підготовки програмістів. На сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це є наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом» [1, 202].

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

З розвитком нових інформаційних технологій посилилася тенденція до використання персональної комп'ютерної техніки, розширилися сфери її застосування. Унаслідок цього, виникли позитивні тенденції, серед яких: загальне підвищення рівня комп'ютерної грамотності працівників правоохоронних органів, розширення переліку комп'ютерних інформаційних обліків; розширення «географії» використання сучасних засобів комп'ютерної техніки в усіх сферах діяльності, розвиток технологій електронної обробки інформації; створення комп'ютерної мережі обміну інформацією. Як підсумок, відмітимо, що інтеграція інформаційних технологій в діяльність органів Національної поліції України дозволяє удосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а саме, оперативно отримувати доступ до певних відомостей, необхідних для виконання їх службових завдань, кваліфіковано здійснювати їх аналіз,

використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп'ютерних технологій дає змогу для створення нових методів роботи, підвищення професіоналізму кожного працівника правоохоронних органів.

Ще більше перспектив для протидії злочинності за допомогою засобів і знарядь із протидії злочинності, що притаманні виключно сфері кіберпростору, вже тривалий час використовуються правоохоронцями низки держав. Там правоохоронці намагаються використовувати нові технології, зокрема і ті, що отримані завдяки наявності соціальних мереж, для виявлення, розкриття, розслідування та попередження злочинів. Ними здійснюється постійний моніторинг підозрілих блогів, чатів, сайтів тощо з метою отримання оперативно вагомої для правоохоронців інформації. Зокрема, сьогодні соціальні мережі широко використовуються правоохоронними органами зарубіжних країн як засіб для зв'язків із громадськістю, у тому числі з метою отримання криміналістично значимої інформації. Так, наприклад, поліція графства Великий Манчестер створила обліковий запис мережі Twitter. У мікроблозі даного ресурсу публікують важливі повідомлення, кримінальні відомості, дані про осіб, оголошених у розшук. При цьому британські правоохоронці офіційно визнали важливу роль соціальних мереж у попередженні та розкритті злочинів і включили відповідний курс у програму підготовки молодих співробітників. Для відстеження активності в соціальних мережах у Росії розробили і використовують систему моніторингу соціальних мереж – спеціальні термінали «Призма». Система «Призма» в реальному часі відслідковує 60 млн джерел. Вона показує динаміку позитивних і негативних відгуків у блогах на ту чи іншу подію, а також здатна будувати графіки атак ботів. При цьому відстеження тем моніторингу настроюються індивідуально. «Призма» відслідковує в соцмедіа активності, що призводять до зростання соціальної напруженості: нагнітання безладів, протестні настрої, екстремізм та ін. Аналогічну систему розробляли і в Україні під керівництвом доктора фізикоматематичних наук, професора, член-кореспондента НАН України А. В. Анісімова, але на жаль, через відсутність фінансу-

вання подальшу розробку призупинено. Сьогодні Україна перебуває осторонь цих суспільно-корисних позитивних процесів. Це пов'язано, з одного боку, із майже повною відсутністю у співробітників правоохоронних органів спеціальних інформаційно-пошукових систем, особливо контент-моніторингу, контент-аналізу, недостатньої кількості спеціалістів, підготовлених у цьому напрямку, а, з іншого, – із відсутністю нормативного закріплення прав, повноважень та обов'язків конкретних правоохоронних органів нашої держави щодо здійснення відповідних заходів протидії злочинності з використанням кіберпростору. Також слід підтримати думку про те, що однією з причин неефективного правового впливу на сучасний кіберпростір є відсталість методик і засобів практичної реалізації наявної системи правової бази правоохоронними органами [3, 278-280].

Використання інновацій у діяльності органів правопорядку є особливо важливим елементом для ефективного попередження та розслідування правопорушень, створення умов для недопущення негативних тенденцій у суспільстві, сталого розвитку економіки та політичної стабільності. Своїм розпорядженням «Питання реформування органів внутрішніх справ України» від 22.10.2014 р. №1118-р Кабінет Міністрів України схвалив розроблені Міністерством внутрішніх справ Стратегію розвитку органів внутрішніх справ України та Концепцію першочергових заходів реформування системи Міністерства внутрішніх справ. Згідно з Концепцією запровадження сучасних технологій у діяльності правоохоронців такі: впровадження систем електронного документообігу та автоматизованих інформаційно-пошукових систем, удосконалення електронних баз даних, широке використання систем відеонагляду за правопорядком, використання терміналів реєстрації відвідувачів, упровадження системи безготівкової оплати штрафів. Безумовно, питання використання інноваційних технологій у діяльності правоохоронних органів пов'язане з питанням інформаційної безпеки у країні.

Оглядовий аналіз принципу дії сучасних засобів інформаційних технологій в органах поліції іноземних держав, зокрема Великої Британії та Литви, дають підґрунтя для вдосконалення цих засобів

в Україні. Так, поліція Великої Британії входить у топ-10 найбільш професійних поліцейських структур у світі. Дуже цікавим є досвід використання ІТ поліцією Литовської Республіки, враховуючи спільність історичного минулого, культурних зв'язків та інтересів у сфері безпеки з Україною. У всьому світі технічні спеціалісти розробляють та вдосконалюють комунікаційні технології та інноваційні рішення, зокрема технології зв'язку, а в Україні, на жаль, поліція і спецслужби досі використовують незахищений зв'язок. Безпека зв'язку – не лише захист від несанкціонованого втручання – прослуховування, перехоплення, підміни повідомлень. Мають бути забезпечені кодування інформації й секретність параметрів абонентів. У кожній країні поліція сама обирає систему зв'язку й виробника. Наприклад, система TETRA – це європейський стандарт у роботі правоохоронних служб і служб порятунку. В Америці, Азії, Франції є свої системи. Police National Computer (далі – PNC) – це основна Національна комп'ютерна система поліції Великої Британії. Вона використовується для сприяння розслідуванням та обміну інформацією як національного, так і місцевого значення. Система забезпечує відомостями поліцію та інші правоохоронні органи шляхом наявності розширеної інформації про людей, транспортні засоби, злочини та майно. Інформація доступна в межах захищеної мережі: її можна отримати миттєво та в тисячах терміналів по всій країні в будь-який час. На сьогоднішній день вона включає в себе мобільні перевірки даних на місці злочину або розслідування. PNC містить кримінальні історії всіх злочинців в Англії, Уельсі та Шотландії, а також інформацію від інших поліцейських сил, таких як Британська Транспортна Поліція. У 2010 р. була введена загальнонаціональна база даних – Поліцейська Національна база даних (далі – PND), яка включає в себе всю інформацію про PNC плюс всю інформацію відносно місцевих поліцейських сил, а саме: так звану «м'яку» інформацію, наприклад твердження, зроблені у відношенні особи, які не призводять до арешту, або клопотання, передані в поліцію з інших органів (шкіл або соціальних служб).

Основне завдання литовської криміналістичної інформаційної системи полягає в тому, щоб допомогти всім посадовим особам і

установам системи кримінального правосуддя у виконанні своїх різноманітних обов'язків на загальнодержавній основі шляхом надання цілодобового доступу до необхідної інформації. Литовська криміналістична інформаційна система складається з окремих баз даних, які підконтрольні різним департаментам. Основні бази включають «Населення Литовської Республіки» (інформація про громадян – всі дані посвідчення особи або паспорта), «Транспорт» (інформація про реєстрацію транспортних засобів), «Вогнепальна зброя» (інформація про зареєстровану вогнепальну зброю та її власників), «Особливо небезпечні особи» (інформація про розшукуваних злочинців і зниклих безвісти), «Викрадені транспортні засоби», «Вкрадена вогнепальна зброя», «Злочини і злочинці», «Поліцейські превентивні записи» (інформація про осіб, які сприйнятливі до порушення), «Номерні об'єкти» (інформація про зареєстровані пронумеровані об'єкти), «Адміністративні правопорушення», система автоматизованої ідентифікації відбитків пальців (АДІС), «Пірат-2» та ін. Бази даних функціонують в комп'ютерах з операційною системою UNIX.

В Україні робота з базами даних поліції здійснюється відповідно до Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України від 12.10.2009 р. №436, затвердженого наказом Міністерства внутрішніх справ України. Наявні такі пошукові системи: «Мобільні телефони»; «Транспортні засоби у розшуку»; «Зброя у розшуку»; «Культурні цінності»; «Неопізнані трупи»; «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку». [4, 86-88].

Виходячи з вище викладеного можна зробити висновки, що організація діяльності поліції, яка заснована на використанні інформаційних технологій та підтримці громадськості і направлена на попередження злочинів та правопорушень, аналіз і використання зарубіжного досвіду участі населення у правоохоронній діяльності, в тому числі шляхом використання інформаційних технологій, соціальних мереж, чатів – дійовий інструмент якісного покращення співробітництва поліції і громадськості, реальна можливість підвищення ефективності роботи поліції, тому існує необхідність у розробці та прийнятті нормативних документів, регламентуючих цей аспект правоохоронної діяльності, як на державному,

так і на галузевому рівні (Закони України, накази Міністра внутрішніх справ).

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність // Вісник Запорізького національного університету: збірник наукових праць. Юридичні науки: [у 2 ч.]. Запоріжжя: Запорізький національний університет, 2011. Ч. I. 224 с.
2. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. К.: НАВСУ, 2013. 82с.
3. Гавловський В. Д. Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів//Боротьба з організованою злочинністю і корупцією (теорія і практика): наук.-практ. журн. № 2 (28)'2012
4. Солнцева Х. В. Деякі питання запровадження та використання сучасних технологій в органах поліції//науково-практичне видання «Право та інновації» № 4 (16) 2016 – 166 с.

ВИКОРИСТАННЯ ФУНКЦІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ПІД ЧАС РОЗСЛІДУВАННЯ КДТП

Нагорняк Юліана Василівна,

*аспірант кафедри криміналістики, судової медицини та
психіатрії Львівського державного університету
внутрішніх справ*

Однією з типових слідчих ситуацій, що виникають під час проведення досудового розслідування фактів кримінальної дорожньо-транспортної пригоди (надалі – КДТП) є ситуації, коли слідству не вдається встановити особу, яка керувала транспортним засобом. У таких випадках виникає необхідність впровадження у ході досудового розслідування інновацій, зокрема таких технологій, які б сприяли виявленню та встановленню відповідних осіб.

На даний час на території України функціонує система відеоспостереження під назвою «Безпечне місто», при цьому відеокамери розташовані також на автомобільних шляхах. Однак, вказана система не спрямована на виявлення осіб, які вчинили злочини або переховуються від органів досудового розслідування чи суду. Для перевірки та аналізу, отриманих відомостей з записів камер необхідно мати точні відомості про подію (зокрема, часові межі, індивідуальні ознаки транспортного засобу) та мати можливість порівняти зображення з фотокартки та отриманого відеозапису, що не завжди є ефективним та займає багато часу.

Враховуючи вищевикладене, варто підкреслити, що біометричні системи ідентифікації людини набирають все більшої популярності, оскільки в порівнянні з традиційними засобами вони відрізняються оперативністю та швидкістю отримання даних та їх аналізу. На даний час широко розповсюджена ідентифікація особи за відбитками пальців рук, однак закордоном активно впроваджується досвід використання різних систем розпізнавання обличчя. Такий метод надає змогу розпізнати злочинця серед натовпу. Яскравим прикладом ефективного використання таких технологій слугує досвід його використання в Китаї, коли на концерті гонконгського співака поліція затримала підозрюваного на ім'я

Ао, якого розшукували за економічні злочини. При цьому, використовувалася система розпізнавання осіб, яка впізнала злочинця серед 70 тисяч глядачів [1].

І.В. Голуб'як та Р.Я. Косаревич вказують, що основним завданням біометричної системи розпізнавання обличчя є виділення інформативних ознак з отриманого образу для реєстрації, а в подальшому порівнянні оброблених ознак з вхідним інформативними ознаками, які вже використовуються для отримання певного доступу [2, с. 158].

Під час розслідування КДТП у працівника поліції часто немає відомостей про особу, яка вчинила злочин, однак, при перегляді записів з камер відео спостереження та/або відеореєстраторів можна встановити транспортні засоби, які рухалися на конкретній ділянці автомобільної дороги, а за допомогою програмного забезпечення з пошуку та ідентифікації обличчя отримати зображення осіб, які керували ними. Для вирішення завдання щодо пошуку об'єктів у відеопотоці можна використовувати метод, який набув великої популярності завдяки високій точності. Серед основних принципів його роботи є використання бустінгу для вибору найбільш підходящих ознак для шуканого об'єкта на частині зображення. Алгоритм добре працює і розпізнає риси обличчя під невеликим кутом, приблизно до 30 градусів [3, с. 29].

Варто підкреслити, що такий метод є оптимальним для використання під час ідентифікації водія, оскільки, типовим є те, що положення голови особи, яка керує транспортним засобом, зазвичай не змінюється. Маючи зображення людини, з метою швидкої ідентифікації та встановлення даних, для проведення повного та об'єктивного розслідування доцільно використовувати систему, яка надає змогу розпізнавати та ідентифікувати обличчя. Такий спосіб був запропонований В. Каземі та Д. Суліваном, основна ідея якого полягає в аналізі точок з позиції 68 орієнтирів (мал. 1) [4, с. 87].

Суттєвою перевагою використання програми ідентифікації обличчя є те, що особі, яка отримує інформацію не потрібно володіти специфічними навиками, а достатньо виконати вхід у систему, яка містить необхідні алгоритми.

Наступним завданням програмного забезпечення буде відшукати на зображенні з обличчям ці орієнтири, порівняти їх з наявними в базі даними та надати користувачу відомості про особу.



Мал. 1. Локалізація 68 точок орієнтирів, які необхідно розпізнавати на обличчі для проведення ідентифікації [4, с. 88].

Застосування методу ідентифікації особи за рисами обличчя під час розслідування КДТП надасть змогу оперативно встановити особу, яка керувала транспортним засобом в момент вчинення правопорушення та притягнути її до кримінальної відповідальності. При цьому, відомості, отримані шляхом огляду відеозапису та використання програмного забезпечення будуть визнаватися доказом у кримінальному провадженні. Для підвищення достовірності отриманих даних та формування бази, яка б була основою для ідентифікації за рисами обличчя та містила відомості про осіб, пропонуємо надати доступ до такого роду інформації та забезпечити можливість порівняльного аналізу відомостей, які містяться в документах та надаються під час видачі посвідчення на право керування транспортними засобами та паспорта громадянина України. Вимогою часу є також створення відповідного програмного забезпечення, яке слід надати в розпорядження органам досудового розслідування Національної поліції.

Отже, впровадження практики використання функцій розпізнавання обличчя під час проведення досудового розслідування кримінальних проваджень щодо КДТП надасть змогу працівникам поліції оперативно встановити особу, яка вчинила кримінальне правопорушення. Описані методи надають змогу використовувати програмне забезпечення особами, які без значних витрат часу та ресурсів можуть освоїти навички роботи з такими технологіями, оскільки для їх використання достатньо отримати у встановленому законом порядку відеозаписи, вибрати з них необхідне зображення та завантажити його для ідентифікації.

-
1. Система розпізнавання облич впізнала злочинця серед 70 тисяч осіб [Електронний ресурс] – Режим доступу: <https://tehnot.com/ua/sistema-raspoznavaniya-lits-opoznala-prestupnika-sredi-70-tysyach-chelovek/>.
 2. Голуб'як І.В., Косаревич О.Я. Методи розпізнавання облич / І.В. Голуб'як, О.Я. Косаревич // Проблеми інформаційних технологій. – 2017. – № 22. – С. 158–164.
 3. Леванець Т.В., Кравець О.І. Дослідження методів розпізнавання облич при використанні мобільних технологій / Т.В. Леванець, О.І.Кравець // Комп'ютерні технології. – 2016. – № 271 (283). – С. 28–35.
 4. Шаховська Н.Б., Басистюк О.А. Розпізнавання обличчя за допомогою алгоритмів машинного навчання / Н.Б. Шаховська, О.А. Басистюк // Штучний інтелект. – 2017. – № 3–4. – С. 84–93.

ТЕХНОЛОГІЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Омельяненко Оксана Валеріївна,

*начальник Управління інформаційно-аналітичної підтримки
ГУ НПУ у Львівській області*

Рудий Тарас Володимирович,

*професор кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Денис Руслан Володимирович,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Сучасні загрози обумовлені впливом комплексу політичних, соціально-демографічних, економічних, правових, соціоінженерних, технологічних чинників вимагають системного реагування, адекватної трансформації як загалом сектору безпеки, так і інформаційної та кібербезпеки зокрема [1]. Ціла низка проблем, які стосуються організації, взаємодії і координування роботи правоохоронних органів, розроблення сучасних систем інформаційно-аналітичного забезпечення, автоматизованих інструментальних засобів кримінального аналізу, які працюють у режимі реального часу ще потребують глибокого вивчення [2].

Актуальною залишається проблема недосконалості національного законодавства і відсутності єдиної правової бази правоохоронних органів у протидії кіберзлочинності. Законодавство України у безпековій сфері не визначає загальні фреймові (рамкові) підходи та визначення, а деталізує часткові, покрокові рішення, що пояснюється низьким рівнем знань у галузі інформаційних технологій (ІТ), теорії інформаційної та кібернетичної безпеки як керівництва держави, політичних діячів, так і конкретних виконавців, а найголовніше – відсутність дієвого, ефективного загальнодержавного підходу до протидії кіберзлочинності [3, 4].

Зокрема, на організаційно-правовому рівні необхідно чітко ідентифікувати проблему протидії кіберзлочинності, визначити основні загрози у сфері кібербезпеки.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні є кримінальний аналіз.

Даючи кримінологічну характеристику кіберзлочинів треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів Національної поліції України (НПУ) і це не дає можливості провести комплексний аналіз та характеристику кіберзлочинності.

Тому, власне, одним із головних завдань кримінального аналізу, на рівні взаємодії з іншими силовими структурами держави, які забезпечують протидію кіберзлочинності, є перехід від процесу ситуативних відносин до чіткої та зрозумілої системи їх взаємодії на основі консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом для прийняття обґрунтованих управлінських рішень на усіх керівних рівнях.

Застосування технологій інформаційно-аналітичної діяльності (ІАД) та відповідних інформаційно-аналітичних систем (ІАС) дозволить структурувати наявні інформаційні ресурси і використовувати їх як моделі консолідованої інформації. Головним аспектом функціонування ІАС є переорієнтація з версій різних систем управління базами даних на вищий якісний рівень, який дозволяє виконувати аналітичні експертні дії.

У цьому зв'язку кожна ІАС створюється і розробляється з урахуванням наступних вимог: одержання розрізнених даних з багатьох джерел одночасно (інформація накопичується у різних форматах і згодом підлягає приведенню до єдиної форми і об'єднання у певну структуру); акумулювання даних і створення масивів баз даних, використання технологій пошуку та індексації; для кожного з користувачів у режимі реального часу організовано надання необхідної інформації для прийняття рішень, виконання конкретних заходів, здійснення певних дій; підготовка регулярної та планової оцінки різних станів об'єктів управління на основі використання інструментів інтелектуального і оперативного аналізу;

подання усієї інформації і результатів її аналізу у строго впорядкованій формі для ефективного сприйняття даних користувачами усіх рівнів.

Аналітична інформація повинна відповідати наступним якісним характеристикам: цінність (корисність) – ступінь сприяння досягненню мети ініціатором запиту; точність – допустимий рівень модифікування інформації; достовірність – властивість інформації відтворювати реально існуючі об'єкти з заданою точністю; повнота – необхідний обсяг відомостей для прийняття виваженого та ефективного рішення; оперативність – актуальність, відповідність інформації поточному моменту; коректність – однозначність сприйняття інформації.

Базовими елементами та засобами реалізації ІАД виступають ІАС – системи зв'язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України «Про Національну поліцію» [5]. У свою чергу технологічна платформа ІАС дозволяє здійснювати інтегрування та координування дій між різними підрозділами НПУ. У практиці кримінального аналізу розрізняють наступні типи аналітичних продуктів [6]:

1. Аналітичний звіт:
 - сепарована інформація з внутрішніх і зовнішніх джерел;
 - висновки;
 - рекомендації, прогнози, настанови;
 - додаткові матеріали (графіки, схеми, дані геолокації).
2. Профіль (досьє) особи, об'єкта:
 - максимальний обсяг інформації на об'єкт аналізу у відповідності до запиту ініціатора.
3. Інформаційне зведення:
 - оброблені табличні дані шляхом вибірки з баз даних за критеріями ініціатора.
4. Витяг інформації:
 - вибірка інформації з баз даних за критеріями ініціатора.

Отже, від того, якою мірою підрозділи кримінального аналізу НПУ спроможні якісно аналізувати наявну інформацію і, як результат, надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

На останок, як висновок, на думку авторів успішне реалізування та впровадження технологій кримінального аналізу дасть можливість активно використовувати ІАД, що сприятиме підвищенню ефективності протидії кіберзлочинності.

-
1. Рудий Т.В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні / Т.В. Рудий, В. В. Сенік, А.Т. Рудий, С.В. Сенік / Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2018. – Вип. 1. - С. 283-301.
 2. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: <https://www.cyberpolice.gov.ua/strategy-2020/>.
 3. Рудий Т. В. Організаційно-правовий супровід захисту інформаційних систем підрозділів національної поліції України на основі міжнародних стандартів / Т.В. Рудий, О. В. Захарова, В. В. Сенік, С. В. Сенік, М. І. Ізю // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
 4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. Електронний ресурс. Шлях доступу: <http://www.niss.gov.ua/articles/454/>.
 5. Закон України "Про Національну поліцію" / Відомості Верховної Ради України, 2015, №40-41. – С. 379 // Електронний ресурс. Шлях доступу: <http://zakon3.rada.gov.ua/laws/show/580-19>.
 6. Кримінальний аналіз у діяльності НПУ / Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою "Intelligence Led Policing" // Електронний ресурс. Шлях доступу: www.slideshare.net/NationalPolice/ss-75925350.

ПОНЯТТЯ Й СУТНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇЇ МІСЦЕ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Отчак Неля Ярославівна,

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

Радикальні перетворення у всіх сферах діяльності суспільства, пов'язані зі значним підвищенням ролі інформації, яка стала потужним, реально відчутним ресурсом, що має часом навіть більшу цінність, ніж фінансові, трудові та інші ресурси. У сучасному суспільстві інформація – ефективний важіль впливу на людину та державу, особливо у сфері формування та розвитку транскордонних глобальних телекомунікаційних мереж, що охоплюють усі країни і континенти, які впливають одночасно як на кожну людину зокрема, так, і на величезні спільноти.

Забезпечення інформаційної безпеки сьогодні стає все більш значущою складовою національної безпеки України. Якісне управління сферою інформаційної безпеки як ефективний метод забезпечення національної безпеки є предметом уваги провідних фахівців-юристів. В публікаціях як вітчизняних, так і закордонних вчених все частіше увага присвячена вивченню таких феноменів, як «інформаційна безпека», «інформаційна війна», «інформаційне протистояння» тощо.

Інформаційна сфера стала системоутворюючим фактором життя суспільства та активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України. Проте, оперуючи інформацією потрібно бути переконаним у тому, що використовувана інформація якісна і у процесі передачі, поширення не була спотворена. Тому питання інформаційної безпеки є важливим компонентом усієї системи національної безпеки країни [1, с. 65].

Інформація є суттєвим елементом суспільних відносин, інтелектуальним скарбом держави та її народу, початком розвитку високорозвиненого суспільства. Інформаційні ресурси держави вже сьогодні зайняли своє місце поруч з її найважливішими

ресурсами – економічними, фінансовими, природними тощо. Інформаційні ресурси містять у собі важливу геологічну, геофізичну, економічну інформацію [7, с. 126].

Законодавче визначення поняття «інформація» міститься у Законі України «Про інформацію» та у Цивільному кодексі України. Згідно із ст. 1 зазначеного Закону: «Інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [10].

Деталізоване визначення поняття «інформація» знаходимо в іншому нормативно-правовому акті – Законі України «Про захист економічної конкуренції» це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості (ст. 1 Закону «Про захист економічної конкуренції» [9]).

У контексті нашого дослідження необхідно звернути увагу на зміст категорії «безпека», яка у житті людини відіграє роль ключового світоглядного орієнтиру, навколо якого групуються фундаментальні цінності людського буття. Реалізація безпеки особи безпосередньо пов'язана із захистом основних національних, суспільних, групових та особистих цінностей [8, с. 125].

Поняття «безпека» – багатопланове, про нього в науці існує багато точок зору. У буквальному розумінні безпека означає відсутність небезпеки. Потреба безпеки належить до числа базових мотиваційних механізмів у життєдіяльності людини, і в цьому відношенні людина мало чим відрізняється від будь-кого з інших живих істот. Крім того, безпека являє собою безсумнівну цінність, що має універсальний характер, оскільки визнається всіма людьми, незалежно від їх расової, національної чи соціально-класової приналежності.

«Безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, а також довкілля в різних сферах

життєдіяльності від внутрішніх і зовнішніх загроз» – зазначає професор А. Качинський [5, с. 14].

На думку українських дослідників, сучасним різновидом небезпеки для людини, пов'язаним із інформаційною сферою, вважається також відсутність інформації з актуальних, життєво важливих для людини проблем, чи її викривленість, маніпулювання нею [9, с. 13].

Про важливість захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17 Конституції України) [6].

Законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому 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» (п. 13 Закону) [12].

Зважаючи на те, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, питання її забезпечення має загальнонаціональне і загально державне значення. Як справедливо зазначив В. Ліпкан, відсутність системи забезпечення інформаційної безпеки унеможливило б надійне забезпечення не лише інформаційної, а й національної безпеки» [4, с. 150].

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливіші з яких:

- політична обстановка у світі;
- наявність потенційних зовнішніх і внутрішніх загроз;
- стан і рівень інформаційно-комунікаційного розвитку країни;

- внутрішньополітична обстановка в державі. Водночас, інформаційна безпека являє собою складну, динамічну, цілісну соціальну систему, компонентами якої є безпека людини, держави й суспільства.

Саме їх взаємозалежна, системна єдність складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентно-здатний, прогресивний розвиток [3, с. 154-155].

Інформаційна безпека в загальній системі національної безпеки України посідає особливе місце. З урахуванням темпів інформатизації та розвитку інформаційних технологій, широкого їх втілення у виробництво, оборону, правозахист, науку, освіту тощо, інформаційна діяльність стає обов'язковим і, досить часто вирішальним елементом усіх сфер діяльності суспільства, тому інформаційна безпека є елементом усіх складових національної безпеки країни [2, с. 10].

Отже, завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії її забезпечення може сприяти досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності.

-
1. Задірака В. К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. № 5. С. 65–69.
 2. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2000. № 1. С. 10–15.
 3. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. – Київ: ТОВ «Видавничий дім «АртЕк». 2018. 446 с.
 4. Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. К.: КНТ, 2006. 280 с.
 5. Качинський А.Б. Екологічна політика й екологічна безпека України. Екологічний вісник. 2006. № 1 (січень–лютий). С. 4

6. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28.06.1996 / URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр>.
7. Кулініч О.О. Інформація як об'єкт цивільних прав. Університетські наукові записки. 2005. № 3 (15). С. 126–128.
8. Мельник В. Ціннісний вимір безпеки особи в умовах трансформації та демократизації суспільства. Україна–НАТО: регіональний вимір: матеріали всеукраїнської науково–практичної конференції (м. Львів, 6 грудня 2008 року). Львів. 2008. С. 124–126.
9. Остроухов В.В. Інформаційно-психологічна безпека особи / В.В. Остроухов // Актуальні проблеми управління інформаційною безпекою держави: [зб. матер. наук.-практич. конф.] (м. Київ, 17 березня 2010 р.). Київ: Наук.-вид. відділ НА СБ України, 2010. С. 12–18.
10. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. URL: <http://zakon.rada.gov.ua/laws/show/2210-14>.
11. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <http://zakon.rada.gov.ua/laws/show/2657-12>.
12. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 № 537-V. URL: <http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%EF%E5%E>.

ДО ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРПОЛІЦІЇ УКРАЇНИ ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Расторгуєва Наталія Олегівна,

здобувач ступеня бакалавра

Харківського національного університету внутрішніх справ

Стрімкий розвиток науково – технічного прогресу і широке використання сучасних інформаційних технологій мають беззаперечний позитивний вплив на суспільні процеси. Але поряд з цим є зворотна, темна сторона цього явища – використання віртуального простору в злочинних цілях. Це висуває перед правоохоронними органами нові завдання щодо протидії кіберзлочинності.

Одним із структурних елементів системи кримінологічного забезпечення протидії злочинності є інформаційне забезпечення, роль та сутність якого досліджували у своїх роботах такі вчені, як О. М. Бандурка, Д. І. Голосніченко, О. М. Джуза, А. І. Долгова, А. П. Закалюк, А. Ф. Зелінський, В. М. Зінченко, О. М. Литвинов, О. М. Литвак, В. І. Поклад, В. І. Шакур, П. Л. Фріс, та інші. Метою даної публікації є окреслення основних шляхів удосконалення інформаційного забезпечення протидії кіберзлочинності.

Різке загострення за останній час оперативної обстановки в Україні, події 2014 року висунули на передній план питання підвищення ефективності роботи всіх правоохоронних органів за рахунок впровадження сучасних засобів комп'ютерної техніки, новітніх інформаційних технологій у сферу протидії кіберзлочинності, однак цей процес нерозривно пов'язаний з удосконаленням матеріально технічного забезпечення, покращенням взаємодії кіберполіції з іншими суб'єктами протидії кіберзлочинності, використанням якнайбільшої кількості джерел кримінологічно зачущої інформації і т. ін.

Основним спеціалізованим суб'єктом протидії кіберзлочинності є кіберполіція – міжрегіональний територіальний орган Національної поліції України, який забезпечує реалізацію державної полі-

тики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Створення цього підрозділу забезпечило підготовку та функціонування висококваліфікованих фахівців, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Завданнями кіберполіції є: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної цілодобової мережі контактних пунктів [1].

Сьогодні склалася ситуація, коли департамент кіберполіції, по суті, не тільки є основним споживачем кримінологічної інформації, а й основним джерелом як первинної, так і вторинної інформації для інших відомств. Тому від того, як організовано інформаційне забезпечення діяльності Департаменту кіберполіції, багато в чому залежить і вся діяльність системи попередження кіберзлочинів.

Інформаційне забезпечення діяльності з протидії злочинності не слід звужувати до механічного накопичення статистичної інформації про злочини та осіб що їх вчинили. Це сукупність засобів і методів, необхідних для отримання кримінологічно значущої інформації, яка використовується для подальшого аналізу причин та умов злочинів, прогнозування та планування протидії злочинності.

Основними кроками до покращення рівня інформаційного забезпечення протидії кіберзлочинності ми бачимо наступні:

- Покращення матеріально – технічного забезпечення кіберполіції. Складність виявлення дій комп'ютерного злочинця полягає в його можливості скоювати злочини в кіберпросторі, у якого немає державних кордонів, що багаторазово збільшує ступінь їх суспільної небезпеки. Динамічність поширення комп'ютерних технологій та їх

метаморфози зобов'язують законодавця і правоохоронні органи, що протидіють комп'ютерній злочинності, збільшувати швидкість реакції на появу нових способів протиправної діяльності в даному напрямку, на випередження злочинів.

- Підвищення професіоналізму кадрового складу кіберполіції. Отримання і аналіз доказів у справах про злочини у сфері комп'ютерної інформації – одне з основних і важко вирішуваних на практиці завдань. Це вимагає не лише розробки тактики проведення слідчих і організаційних заходів, але і наявності спеціальних знань у сфері комп'ютерної техніки і програмного забезпечення, а також внесення поправок до чинного законодавства. Співробітники, які безпосередньо займаються розслідуванням даного роду злочинів, і працівники судової системи часто не володіють спеціальними знаннями у сфері нових комп'ютерних технологій, що часто ускладнює процес розслідування злочинів.
- Використання у діяльності кіберполіції результатів наукових розробок з тематики, що стосується протидії кіберзлочинам. На практиці часто виникають помилки при кваліфікації та документуванні злочинних діянь, частими причинами чого є відсутність достатньої кількості методичних рекомендацій і роз'яснень із розслідування цих злочинів, узагальненої судової практики.
- Удосконалення взаємодії кіберполіції з іншими суб'єктами протидії кіберзлочинності. Чітка взаємодія, як форма взаємозв'язку та взаємної підтримки, значення якої важко переоцінити, полягає у тому, що правоохоронні органи у цілому, конкретні їх служби та структурні підрозділи або працівники у взаємодії один з одним досягають значно більших результатів у менші строки із найменшими витратами сил.

Серед надійних партнерів кіберполіції у протидії кіберзлочинності мають бути: служба безпеки України, Міністерство освіти і науки, Державна служба спеціального

зв'язку та захисту інформації України, Інтернет-провай-
дери, передові ІТ-компанії.

Немаловажну роль у протидії кіберзлочинності відіграють громадські організації. Їх основна перевага в тому, що вони можуть інтегруватися, вони більш гнучкі, ніж державні органи, і це дає їм можливість швидко реагувати на зміну ситуації у суспільстві. Громадські організації вільні у виборі форм та методів роботи, вони не зарегламентовані певними нормами і не обмежені функціями та рамками [3, с. 127].

Неоціненною є взаємодія підрозділів Національної поліції України із засобами масової інформації, які по праву називають однією з «гілок влади» через той вплив, який вони можуть чинити на людей. Саме засоби масової інформації мають стати тією неупередженою структурою, яка повинна інформувати суспільство про проблеми, пов'язані із суспільною небезпечністю кіберзлочинів, способи їх вчинення та заходи захисту від такого роду злочинних посягань.

Окремо слід звернути увагу на взаємодію з міжнародними організаціями щодо протидії транскордонним проявам кіберзлочинності. Сьогодні кіберпростір, як п'ятий загальний простір після наземного, морського, повітряного і космічного, вимагає координації, співпраці і особливих правових заходів на міжнародному рівні. Проте, відсутні ефективні заходи міжнародного масштабу з боротьби з кіберзлочинцями, що створює певний вакуум в правовому регулюванні відповідальності і порядку кримінального переслідування осіб, що вчинили транснаціональні злочини, і, відповідно, викликає у кіберзлочинців уявлення про можливість уникнути кримінальної відповідальності [3, с. 89].

- Підвищення рівня довіри населення до кіберполіції. Довіра до поліції має двосторонній характер, з одного боку – це відображення ставлення населення до поліції, з іншого – основа їх взаємодії. Одним з ключових аспектів реформи правоохоронних органів, зокрема, в частині

діяльності Національної поліції, є законодавчо врегульований обов'язок поліції діяти в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства. Однак, на сьогоднішній день назвати цю взаємодію ефективною не можна. За результатами опитування громадян, рівень довіри до поліції дещо зріс (з початку реформування системи МВС України), однак залишається низьким.

Це основні кроки на шляху до покращення інформаційного забезпечення протидії кіберзлочинності, що є запорукою своєчасного та якісного наповнення «інформаційних систем» та відповідних обліків.

Саме Департамент кіберполіції, як зв'язуючи ланка, забезпечує можливість оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді для розкриття, розслідування, попередження кіберзлочинів. Також здійснює обробку та узагальнення оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінки ситуації та прийняття оптимальних рішень щодо забезпечення захисту інформації та протидії кіберзлочинам.

-
1. Про затвердження Положення про Департамент протидії наркозлочинності Національної поліції України: наказ Національної поліції України від 17.11.2015 № 95.
 2. Балакірева О. М. Секс бізнес в Україні: спроба соціального аналізу. К. : Укр. Інститут соціальних досліджень. 2001. 159 с.
 3. Косенков А. Н. Общая характеристика психологии киберпреступника. Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 87–94

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ В СИСТЕМІ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ТА ПРОБЛЕМНІ ПИТАННЯ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ВИКОНАННЯ СЛУЖБОВИХ ОБОВ'ЯЗКІВ

Рижков Едуард Володимирович,

*завідувач кафедри економічної та інформаційної безпеки,
Дніпропетровського державного університету внутрішніх
справ, кандидат юридичних наук, доцент*

Дзех Ярослав Сергійович,

*заступник начальника сектору інформаційної підтримки
Дніпровського відділу поліції ГУНП в Дніпропетровській області*

На етапі реформування діяльності підрозділів інформаційно-аналітичної підтримки органів Національної поліції України необхідно врахувати ряд позицій, які потребують свого вирішення.

Осучаснення матеріально-технічної бази та належне фінансування для придбання техніки та ліцензійного програмного забезпечення. Як приклад, необхідно констатувати, що кількість існуючих на балансі в підрозділах робочих станцій не відповідає кількості підрозділів.

Локальна мережа повинна відповідати актуальним стандартам і мати можливість програмного керування топологією локальної мережі за допомогою розумних комутаторів.

Проблема щодо здійснення доступу до ІПС ОНП («Цунамі», «Армор»), яка полягає у можливості входу одночасно з декількох робочих станцій під одним логіном та паролем, що у свою чергу може призводити до витоку інформації службового характеру, повинна бути у найкоротший час остаточно вирішена. Як варіант, технічно вхід до системи ІПС ОНП може бути організовано за допомогою ЕЦП (по аналогії з системою ЕРДР) та отриманням паролю на мобільний номер телефону.

Відсутність належної взаємодія між підрозділами слідства та підрозділів інформаційної підтримки в частині своєчасного надання статистичних карток до сектору інформаційної підтримки для подальшого внесення в ІП ОНП та коректного внесення інформації до ЕРДР, призводить в подальшому до маніпулювання статистичними показниками та недостовірністю обліків в системі ОНП. Потенційно проблема може бути вирішена за умов реалізації проголошеного принципу централізації.

До сьогодні не вирішена на програмному рівні проблема з наявністю в ІПС ОНП під час перевірки особи в ІП «Особа» двійників з однаковими П.І.Б. та датами народження, але з відмінними одне від одного іншими персональними даними, що призводить к проблемі реальної ідентифікації особи по базах даних ОНП.

Відсутність реального електронного документообороту в системі ОНП, в т.ч. електронного підпису при завірянні документа негативним чином впливає на ефективність всієї роботи. В реаліях він реалізується шляхом сканування раніше роздрукованого та підписаного у керівництва документу та відправлення вже в відсканованому вигляді.

Відповідно до внутрішніх розпорядчих документів в системі МВС та ОНП існує невідповідність між законодавством України в частині обов'язковості фотографування та дактилоскопіювання осіб яким повідомлено про підозру у вчиненні кримінального правопорушення (особа має право відмовитися від вищевказаних заходів, а для внесення інформації в ІП ОНП зазначені заходи є обов'язковими).

Для повноцінної та стабільної роботи працівниками слідчих підрозділів ОНП необхідний доступ до ЕРДР за допомогою мережі Інтернет, проте відповідно до законодавчих актів ОНП України він заборонений у використанні в внутрішній мережі органів Національної поліції. Проблему необхідно вирішувати нормативним шляхом.

При використанні планшетних пристроїв старшими СОГ та використанні встановлених на них ІП «Цунамі» за рахунок відсутності якісного покриття мобільних операторів, в деяких районах міста

унеможлиблює роботу з базою на планшетному пристрою зв'язку з топографічними особливостями місцевості. Використання карток операторів носить монопольний характер, проте у поліції немає жодних пріоритетів щодо їх експлуатації, що у свою чергу протирічить міжнародним стандартам.

У зв'язку з переходом до єдиної інформаційної системи ОНП, що сприяє об'єднанню великого масиву даних з підсистем ОНП до вищевказаної системи, існує проблема щодо несвоєчасного об'єднання інформації внесеної до інших підсистем, що призводить до постійних розбіжностей. Нові підходи в організації діяльності на старій платформі безумовно призведуть до проблем нового характеру.

Штатний розклад підрозділів інформаційної підтримки повинен відповідати реаліям сьогодення та впровадженню в систему ОНП сучасних моделей інформатизації підрозділів поліції. Так, наприклад, ліквідація посад інженерів-програмістів. в секторах інформаційної підтримки призводить до унеможливлення виконання поставлених завдань в частині розвитку інформатизації та підтримки в належному стані та технічної підтримки наявних технічних засобів, які використовуються співробітниками поліції на місцях для виконання поставлених завдань (встановлення програмного забезпечення, антивірусів, програмних продуктів ІПС, ЕРДР, усунення несправності та інш.). При цьому з 2019 року запроваджуються піврічні курси первинної підготовки працівників низової ланки для підрозділів інформаційно-аналітичної підтримки., що, в свою чергу, породжує питання щодо послідовності політики в кадровому питанні.

В районних відділеннях поліції відсутні штатні посади співробітників інформаційної підтримки. Всі посади вищезазначеної категорії входять до номенклатури посад міського відділу поліції та співробітники відкомандировані дорученням начальника ДВП для організації роботи та надання допомоги з обліково-статистичної роботи на місцях, що призводить до частих маніпулювань з боку керівництва районних відділень поліції, та в окремих випадках з боку самих співробітників в частині розподілу функціональних обов'язків в підрозділі, відсутності належної матеріально

технічної бази (комп'ютерів, МФУ та інше) для повноцінної роботи та виконання покладених обов'язків.

Таким чином, констатуємо, що задля ефективного виконання підрозділами інформаційно-технічної підтримки органів Національної поліції своїх функціональних обов'язків необхідна реалізація чіткої послідовної управлінської політики принаймні у середньостроковій перспективі. Без виправлення ситуації у фінансово-адміністративних аспектах досягти прогресу та забезпечити якісного виконання сучасних задач буде вкрай складно.

ЕТАПИ ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сеник Святослав Володимирович,

*науковий співробітник відділу організації наукової роботи –
здобувач кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ*

Законодавство України, зокрема, закони України «Про інформацію» [1], «Про захист інформації в інформаційно-телекомунікаційних системах» [2], «Про захист персональних даних» [3], вимагають забезпечення захисту інформації, яка є власністю держави і є інформацією з обмеженим доступом.

Оскільки в діяльності підрозділів Національної поліції України циркулює інформація з обмеженим доступом усіх видів (таємна, службова, конфіденційна), виникає необхідність забезпечення її захисту.

Для захисту такої інформації, особливо, якщо вона циркулює в інформаційно-телекомунікаційних системах, застосовують комплексну систему, під якою розуміють сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [4].

Під час побудови такої системи використовують організаційні та інженерно-технічні заходи, комплекси технічного захисту інформації, захисту від витоку інформації через побічні електромагнітні випромінювання та наведення, а також комплекс засобів захисту від несанкціонованого доступу.

Основним компонентом організаційних заходів є розробка політики інформаційної безпеки. Окрім цього сюди відносять і заходи, які передбачають: складання посадових інструкцій для обслуговуючого персоналу та користувачів; розробку правил для адміністрування інформаційної системи (порядку обліку, зберігання, розповсюдження, розмноження, знищення носіїв інформації, ідентифікації користувачів); порядок дій у випадку виявлення спроб несанкціонованого доступу до інформаційних ресурсів сис-

теми, несправностей засобів захисту, виникнення явищ стихійного лиха чи надзвичайних ситуацій. Окреме місце при цьому займає навчання користувачів щодо безпечної роботи в інформаційній системі.

Наступними важливими компонентами під час побудови комплексної системи захисту інформації є використання інженерно-технічних заходів, охоронної сигналізації, встановлення систем управління і контролю доступом, обладнання засобами захисту від витоку мовленнєвої інформації та від витоку інформації каналами побічних електромагнітних випромінювань.

З метою створення єдиного підходу до питань побудови комплексних систем захисту інформації в Україні розроблено та запроваджено ряд нормативних документів. Так, створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [5] на підставі технічного завдання, розробленого згідно з вимогами нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» [6].

У літературі та у практичній діяльності по-різному виділяють етапи створення комплексної системи захисту інформації. На нашу думку, найоптимальнішим є поділ на наступні етапи:

1. Підготовка, створення та затвердження організаційної документації.
2. Обстеження інформаційної інфраструктури.
3. Розробка технічного завдання на створення комплексної системи захисту інформації.
4. Розробка плану захисту інформації.
5. Розробка технічного проекту на створення комплексної системи захисту інформації.

6. Приведення інформаційної інфраструктури у відповідність з технічним проектом на створення комплексної системи захисту інформації.
7. Розробка документації для експлуатації на комплексної системи захисту інформації.
8. Впровадження комплексної системи захисту інформації.
9. Випробування комплексної системи захисту інформації.
10. Проведення державної експертизи комплексної системи захисту інформації і отримання атестата відповідності.
11. Супровід комплексної системи захисту інформації.

У зв'язку із обмеженістю даної публікації детальний аналіз перелічених етапів та обґрунтування необхідності їх проведення буде представлено нами у подальших дослідженнях.

-
1. Про інформацію : Закон України 02 жовтня 1992 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2657-12/>
 2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/>
 3. Про захист персональних даних : Закон України від 01 червня 2010 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2297-17/>
 4. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс]. – Режим доступу : <http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informacii-kszi>
 5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08 листопада 2005 р. №125 [Електронний ресурс]. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835

6. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. (зі зміною №1, затвердженою наказом Департаменту СТСІ СБ України від 18.06.02 № 37 та із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806) [Електронний ресурс]. – Режим доступу : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwj1x_Cyrc_eAhWBo4sKHRKVD94QFjAAegQICBAC&url=http%3A%2F%2Fwww.dsszzi.gov.ua%2Fdsszzi%2Fdccatalog%2Fdocument%3Fid%3D106349&usg=AOvVaw244WydoNtjePKusx4FbJ9z

РОЛЬ ІНФОРМАЦІЙНОГО ПРАВА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сірант Мирослава Миколаївна,

*доцент кафедри конституційного та міжнародного права
Національного університету «Львівська політехніка»,
кандидат юридичних наук, доцент*

Активний процес розвитку в Україні правової системи та системи громадянського суспільства зумовлює потребу в підготовці та перепідготовці юридичних кадрів на фундаментальній юридичній основі з урахуванням традиційного і інноваційного національного та європейського досвіду, внаслідок цього, одним з першочергових напрямів реформування освіти повинна стати необхідністю розвитку та вдосконалення юридичної освіти.

Велика кількість юридичних вищих учбових закладів народжує високу конкуренцію, що сприяє підвищенню рівня професіоналізму в професії.

Однак, однією з головних залишається проблема регулювання ринку з надання якісних юридичних послуг та надання безкоштовної кваліфікованої юридичної допомоги громадянам України в світлі реформи ринку кваліфікованої юридичної допомоги.

Актуальною залишається проблема підготовки високопрофесійних кадрів для судової системи, правоохоронних органів, органів законодавчої та виконавчої влади, органів місцевого самоврядування та підвищення правової культури населення, особливо проведення молодіжної політики в цій сфері. Важливе значення набуває питання підготовки юристів в сфері інформаційної безпеки особи, держави, суспільства.

Разом з тим, Державні освітні стандарти за напрямом і спеціальностями юридичної освіти, не повинні служити перешкодою розвитку наукових і педагогічних шкіл, їх творчого потенціалу. Зміст професійної юридичної освіти формується не тільки в традиційному навчальному процесі.

Постійними складовими навчання повинні стати навчально-професійні тренінги, практичні виїзди, нетрадиційні форми проведення аудиторних занять, діалогові гуртки, робота з освоєння різних професійних видів діяльності, включення в реальну юридичну практику.

Удосконалення юридичної освіти на сучасні виклики суспільства та держави, вимагає, більш ефективного поєднання різних форм і методів навчання та раціонального використання науково-педагогічних кадрів.

Як показує дослідження статистичних даних, за останні чотири роки спостерігається майже шестиразове збільшення злочинів, вчинених у сфері інформації та телекомунікації. Цей ріст обумовлений не тільки тим, що на сьогоднішній день відсутнє чітке законодавче розмежування злочинів в сфері інформаційних технологій і злочинів, скоєних за допомогою інформаційних технологій, як раз складають основну частку шахрайств, але й доступністю програмних засобів, що дозволяють навіть слабо підготовленим користувачам здійснювати досить складні кіберзлочини.

На сьогоднішній день спостерігається нестача кадрів для правоохоронних органів: Національної поліції, митних органів, слідчих органів в сфері інформаційної безпеки.

Гостро стоїть питання про підготовки майбутніх юристів і претендентів, які претендують на посади суддів для судової системи. Наприклад, сьогодні є єдиний судовий орган з вирішення інформаційних спорів.

Освітній процес отримання знань, повинен бути орієнтований на нові виклики інформаційного суспільства, що передбачає відхід від традиційної організації процесу навчання. Тому для досягнення поставленої мети необхідно посилити інформаційну складову підготовки фахівців у галузі юриспруденції, введення нових дисциплін в сфері інформаційної безпеки, інформаційного права.

У Національному університеті «Львівська політехніка» навчальна дисципліна «інформаційне право» читається з 2010 року для сту-

дентів старших курсів різних форм навчання, з 2018 року відкривається магістерська програма «Юрист в сфері інформаційної безпеки».

Практика викладання магістерської програми показує, що знання, отримані в ході вивчення даної дисципліни професійно застосовуються випускниками в різних сферах діяльності.

Аналізуючи вищевикладену ситуацію, слід особливо підкреслити, що підготовка юристів повинна нести фундаментальну основу та вестися виключно на основі Державних освітніх стандартів за напрямками відповідної підготовки.

Досягнення названої мети можливо на основі новітніх інформаційних технологій, технічних засобів зв'язку та інноваційних форм і методів педагогічної майстерності.

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Ткачук Тарас Юрієвич,

*заступник завідувача кафедри Навчально-наукового інституту
інформаційної безпеки Національної академії СБУ,
кандидат юридичних наук, доцент*

Шишко Валерій Валерійович,

*доцент кафедри теорії та історії держави і права,
конституційного та міжнародного права,
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Хитра Олександра Леонтіївна,

*доцент кафедри адміністративного права та
адміністративного процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук*

Не зважаючи на те, що Конституція України з моменту свого затвердження відносить забезпечення інформаційної безпеки до найважливіших функцій держави [1], нормативне визначення інформаційної безпеки є відносно новим. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» передбачав, що інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання 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» [2].

Таке визначення, як бачимо, не дає змоги дійти чіткого висновку щодо сутності складових інформаційної безпеки, так само, як і

низка опосередкованих визначень, які розглядають інформаційну безпеку у контексті більш загального поняття – національної безпеки або ж торкаються її окремих аспектів, на кшталт інформаційної безпеки телекомунікаційних мереж [3].

На методологічному рівні предметна сфера інформаційної безпеки є єдиною, структурованою за завданнями та предметом дослідження, збалансованою за терміносистемою. Її системоутворювальним чинником виступають, безумовно, інформація та інформаційні процеси. Утім, для виокремлення складових інформаційної безпеки на доктринальному рівні використовується досить широкий спектр критеріїв, що зумовлює диференціацію підходів до розуміння системного змісту поняття «інформаційна безпека».

Якщо звернутися до зарубіжних наукових джерел, можна переконатись, що найбільш популярною є точка зору, відповідно до якої складовими інформаційної безпеки визнаються цілісність, доступність та конфіденційність інформації [4; 5]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і/або процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, в т.ч. й достовірність інформації як її відповідність дійсності в аспекті адекватності відображення.

Конфіденційність – це властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов'язана з розмежуванням інформації за режимом доступу.

Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації перебувати у необхідному користувачеві вигляді та місці в той час, коли вона йому необхідна.

Справді, належний стан вищезгаданих властивостей є важливим для забезпечення безпеки інформації. Крім того, завдяки забезпеченню безпеки інформації формується нова її властивість – безпечність, котра також є важливою для інформаційної безпеки. Остання ж, окрім власне безпеки інформації, містить й

інші складові. Так, в окремих випадках заподіяння шкоди належному стану властивостей інформації становить лише один з видів протиправних наслідків. Шкода завдається й іншим елементам інформаційної сфери, до яких, окрім інформації, належать також інформаційні системи (суб'єкти й інфраструктура) та інформаційні відносини. Отже, безпека інформації має розглядатися як частина більш масштабного цілого.

Відповідно, науковці як близького зарубіжжя, так і вітчизняні дослідники приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [6, с. 62; 7]. На підставі критерію функціональності вони пропонують також визнавати складовими інформаційної безпеки її аспекти: соціальний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний та ін. [8].

На думку Б. Кормича, інформаційна безпека має суб'єктно-об'єктний склад, відтак з точки зору критерію основного об'єкта складовими інформаційної безпеки є інформаційна безпека особи, інформаційна безпека суспільства та інформаційна безпека держави. Крім того, держава, людина та суспільство одночасно виступають і в якості суб'єктів інформаційної безпеки, своїми діями здійснюючи захист важливої для них інформації та інформаційних процесів. Зокрема, до сфери інформаційної безпеки держави віднесені конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому, що охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів [9, с.30].

Підкреслюючи за результатами комплексного аналізу системність інформаційної безпеки, О.Тихомиров веде мову передусім про «структурні складові забезпечення інформаційної безпеки» та виокремлює їх за різними критеріями, зокрема: за сферами сус-

пільного життя (забезпечення інформаційної безпеки в економічній, політичній, воєнній, науково-технологічній, екологічній, соціальній та інших сферах); за об'єктами національної безпеки (забезпечення інформаційної безпеки особи, суспільства та держави); за сучасними аспектами розуміння інформаційної безпеки (забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та забезпечення інформаційно-технічної, в т.ч. кібернетичної безпеки); за основними видами інформаційної діяльності (забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо); за формами державного забезпечення інформаційної безпеки (забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері); за напрямками пізнавального процесу в галузі забезпечення інформаційної безпеки (професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо); залежно від елементів змісту діяльності із забезпечення інформаційної безпеки (за об'єктами забезпечення інформаційної безпеки: розвиток і вдосконалення інформаційно-телекомунікаційної інфраструктури, недопущення доведення її до критичного рівня; забезпечення належного використання національних інформаційних ресурсів (захист ресурсів від несанкціонованого втручання, їх інноваційне оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих інформаційних ресурсів і забезпечення доступу до них громадян); захист інформації (забезпечення конфіденційності, цілісності та доступності тощо); захист свідомості суб'єктів від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей); за суб'єктами забезпечення інформаційної безпеки: міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за

кордоном); державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки); недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян, спрямована на сприяння державному забезпеченню інформаційної безпеки); за характером предмета діяльності із забезпечення інформаційної безпеки: протидія негативним інформаційним процесам і явищам; сприяння посиленню позитивних інформаційних процесів; сприяння трансформації нейтральних інформаційних процесів у позитивні; за складовими механізми протидії загрозам інформаційній безпеці: моніторинг інформаційної сфери; ранжування загроз; профілактика й попередження негативного впливу загроз; нейтралізація загроз; за характером здійснення державного впливу: безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері; опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації; за засобами забезпечення інформаційної безпеки: правове забезпечення (правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікації, експертизи тощо); техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації (за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо) [9, с. 31; 10, с. 67].

Проводячи проміжний висновок відзначимо, що вся інформаційна сфера в наш час включає дві основні складові, які, своєю чергою, визначають основні складові інформаційної безпеки держави:

- технічна (штучно створене людиною середовище техніки і технологій);
- психологічна (природний світ з його емоціями).

Джерело: розроблено авторами

Принципові відмінності між визначеними складовими інформаційної безпеки та зміст інформаційно-психологічної складової схематично зображено на рис. 1.

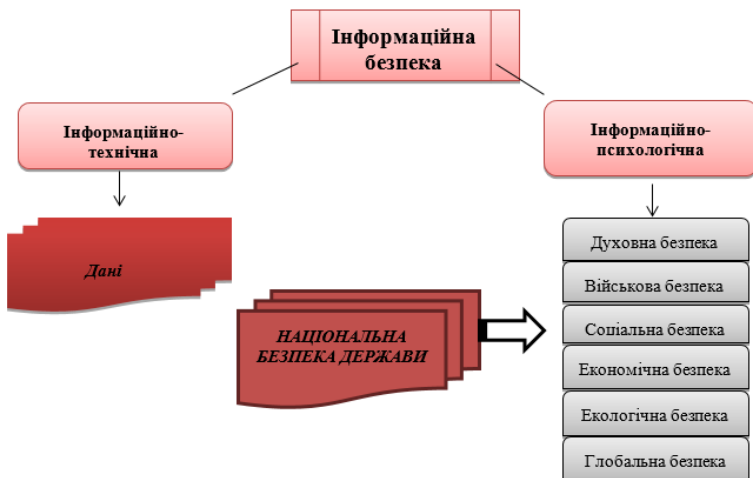


Рис. 1. Складові інформаційної безпеки

1. Конституція України від 28.06.1996 року. URL: zakon5.rada.gov.ua/laws/show/254k/96-вр.
2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 року. URL: zakon5.rada.gov.ua/laws/show/537-16.
3. Про телекомунікації: Закон України від 18.11.2003 року. URL: zakon2.rada.gov.ua/laws/show/1280-15.
4. Michael Nieves, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: [Online tool]. Available at. URL: <https://doi.org/10.6028/NIST.SP.800-12r1>.
5. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): [Online tool]. Available at. URL: www.cnss.gov/Assets/pdf/nstissi_4011.pdf.
6. Баришполец В.А. Информационно-психологическая безопасность: основные положения/ В.Баришполец //Информационные технологии. – 2013. – №2, том 5. С. 62
7. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави. URL: ippi.org.ua/ukhanova-ns-

informatiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi

8. Жатканбаева А. Е. Функциональные компоненты информационной безопасности / А. Жатканбаева// Право и государство. 2013. № 4 (61). С.74.
9. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія]/ Б.Кормич. – Одеса: Юридична література, 2003. С.28-32.
10. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія] / О. Тихомиров; заг. ред. Р. А. Калужний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. С.67.

АСПЕКТИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Форос Ганна Володимирівна,

*професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Сергата Віта Віталіївна,

*здобувач ступеня магістра
Одеського державного університету внутрішніх справ*

На сучасному етапі в Україні продовжується реформування системи правоохоронних органів. Одним із важливих елементів такого реформування є закріплення організаційно-правових основ інформаційного забезпечення правоохоронних органів у сфері протидії злочинності, ліквідації інших загроз національній безпеці як внутрішнього, так і зовнішнього характеру.

Як і всі інші державні органи, правоохоронні органи, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Положення законів України «Про Службу безпеки України», «Про поліцію», «Про оперативно-розшукову діяльність» та інших, а також Закону України «Про інформацію» визначають засади інформаційного забезпечення правоохоронних органів. Таким чином, формування організаційно-правових основ інформаційного забезпечення правоохоронних органів, насамперед, відбувається на законодавчому рівні.

На сьогодні в структурі МВС функціонує Департамент інформатизації МВС, який є провідною організацією, що розробляє та впроваджує комп'ютерні інформаційні підсистеми. До основних завдань Департаменту слід віднести: організація заходів з упровадження програми інформатизації системи МВС та за дорученням Міністра ЦОВВ, здійснення координації та моніторингу її виконання; забезпечення організації взаємодії з інформаційними ресурсами інших державних органів; забезпечення в межах повноважень доступ державних службовців та працівників МВС

до інформаційних ресурсів ЄІС МВС та інших державних органів, а також доступ уповноважених представників інших державних органів до інформаційних ресурсів ЄІС МВС; забезпечення інтеграцію інформаційних ресурсів системи МВС та за дорученням Міністра ЦОВВ у ЄІС МВС та інше. Окрім вказаного також функціонує Департамент інформаційно-аналітичної підтримки Національної поліції України, який здійснює заходи, передбачені законодавством України, що спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення та захист персональних даних при їх обробленні в структурних підрозділах ЦУОП, міжрегіональних територіальних органах Національної поліції України, територіальних органах поліції в Автономній Республіці Крим та м. Севастополі, областях, м. Києві, у тому числі їх територіальних (відокремлених) підрозділах).

Інформаційне забезпечення діяльності правоохоронних органів щодо запобігання злочинам – це насамперед цілеспрямована діяльність, яка спирається на правові, організаційні, технічні і методичні передумови щодо збору, обробки, зберігання і створення умов для використання інформації, що необхідна для ефективного функціонування системи запобігання злочинам. Аналіз наукової літератури, що присвячена питанням інформаційного забезпечення діяльності правоохоронних органів, дозволив дійти висновку, що інформаційне забезпечення це – комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, котрі забезпечують в процесі управління і функціонування системи інформаційні зв'язки та елементів (суб'єктів і об'єктів) шляхом оптимальної організації інформаційних масивів баз даних і знань. Завдяки системі інформаційного забезпечення здійснюється інформаційна підтримка діяльності правоохоронних органів у сфері протидії злочинності, надає багатоцільову статистичну, аналітичну та довідкову інформацію.

Система інформаційного забезпечення правоохоронних органів України, яка являє собою сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог як наявність нормативно-правової бази; організаційно-кадрове забезпечення інформаційних підрозділів; організація підготовки та перепідготовки кадрів; наявність відповідних

технічних, програмних та телекомунікаційних технологій; матеріально-технічне та фінансове забезпечення. Автоматизовані інформаційно-пошукові системи та підсистеми будь якого правоохоронного органу функціонують на відповідних рівнях – центральному, регіональному та територіальному, а їх функціонування забезпечено веденням певних інформаційних обліків.

Враховуючи бурхливий розвиток інформаційних технологій треба зазначити, що налагодження механізму підтримки професійного рівня персоналу, пов'язаного із забезпеченням функціонування інформаційних підсистем, є передумовою розвитку та удосконалення, якісного, своєчасного надання інформації, забезпечення її захисту та надійної роботи. Разом з цим, знання та навички щодо використання інформаційних підсистем співробітниками поліції є складовою частиною загальних вимог до їх професійного та службового зросту.

Комплексний аналіз нормативно-правових актів, що визначають основи діяльності правоохоронних органів України дає підстави визначати два критерії для класифікації напрямів формування організаційно-правових основ їх інформаційного забезпечення, а саме, залежно від виду отримуваної інформації та з огляду на відносини, що потребують урегулювання.

Залежно від виду отримуваної інформації визначаємо такі напрями формування організаційно-правових основ інформаційного забезпечення правоохоронних органів України:

- отримання інформації від громадян і її використання;
- пошук і використання інформації, що належить недержавним юридичним особам;
- використання власних інформаційних ресурсів правоохоронного органу;
- отримання і використання інформаційних ресурсів інших органів держави, у тому числі правоохоронних;
- отримання інформації з інформаційних баз даних спільного користування.

При формуванні організаційно-правових основ отримання інформації від громадян і недержавних юридичних осіб варто враховувати те, що обсяг і строки отримування інформації залежать не

тільки від режиму доступу до неї (інформації), а й від правового статусу запитувача певних відомостей. При цьому існують різноманітні варіанти правовідносин, що можуть виникати, а саме: запит конфіденційної інформації про особу для цілей оперативно-розшукової діяльності й отримання цієї ж інформації в межах кримінального процесу; запит на отримання комерційної або банківської таємниці працівником правоохоронного органу і власне запит від органу СБ України, МВС України тощо.

Таким чином, вирішення завдань сучасного інформаційного забезпечення має бути досягнуто за рахунок упровадження єдиної політики інформаційного забезпечення; створення багатоцільових інформаційних підсистем діяльності Національної поліції; удосконалення організаційно-кадрового забезпечення інформаційних підрозділів; інтеграції та систематизації інформаційних обліків поліції на всіх рівнях; розбудови інформаційної мережі; створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, вірогідності, актуальності та безпеки; переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою; поширення мережі комп'ютерних робочих місць користувачів інформаційних підсистем; подальшої комп'ютеризації інформаційних обліків; установлення взаємодії поліції з населенням у розробці ефективних способів такого забезпечення; упровадження нових форм і методів інформаційного забезпечення Національної поліції; правове виховання через засоби масової інформації; удосконалення законодавства.

-
1. Про затвердження Положення про Міністерство внутрішніх справ України : [Електронний ресурс]:наказ МВС України від 28.10.2015 р.. № 878. - Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрану
 2. Про інформацію [Електронний ресурс]: закон України від 02.10.1992 № 2657-12 в редакції Закону України від 01.01.2017, підстава 1774-VIII – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрана.
 3. Про Національну поліцію [Електронний ресурс]: закон України від 02.07.2015 № 40-41, ст.379 в редакції Закону України від від 29.12.2015, підстава 900-19 – Електрон. дан. (1 файл). – Режим доступу: <http://zakon2.rada.gov.ua>. – Назва з екрану.

ВИЗНАЧЕННЯ ЗАГРОЗ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Чистоклетов Леонтій Григорович,

*професор кафедри адміністративного та інформаційного права
Національного Університету «Львівська політехніка»,
доктор юридичних наук, професор*

Ткачук Тарас Юрієвич,

*заступник завідувача кафедри Навчально-наукового інституту
інформаційної безпеки Національної академії СБУ,
кандидат юридичних наук, доцент*

Аналізуючи положення Закону України «Про основи національної безпеки України» [1] можна стверджувати, що система загроз слугує основою для стратифікації національної безпеки (з урахуванням джерела, характеру і специфіки загроз) на зовнішньополітичну, внутрішньополітичну, державну, воєнну, економічну, соціальну, гуманітарну, екологічну та інформаційну безпеку, а також безпеку державного кордону. Втім, виходячи з визначення національної безпеки, наведеного в тому ж законі, перелік сфер, у яких можуть проявлятися загрози національній безпеці, не є вичерпним. Зокрема, залежно від середовища формування і масштабів загроз національним інтересам, традиційним став поділ національної безпеки відповідно до джерел загроз на зовнішню та внутрішню[2], однак за сучасних умов такий поділ стає умовним, адже зовнішні загрози можуть мати внутрішні джерела, а також інтегруватися із внутрішніми загрозами.

Саме необхідність протидії загрозам зумовлює можливість дослідження національної безпеки з точки зору функціонально-діяльнісного підходу, відповідно до якого національна безпека розглядається як динамічне явище, котре постійно змінюється та еволюціонує. Цей підхід орієнтує на аналіз національної безпеки як процесу збереження і підтримання її сталого стану як єдиного утворення, оптимального розвитку всіх рівнів і видів безпеки як цілого, що забезпечує реалізацію національних інтересів [3] в

умовах можливого розгортання загроз, а також дозволяє оцінювати можливості суспільства щодо належного забезпечення «гомеостатичного стану» об'єктів національної безпеки як сталості певного набору характеристик, за умови підтримання яких зберігається життєздатність вказаних об'єктів, а також здатність до спротиву намаганням зовнішніх чинників змінити сталі внутрішні характеристики [3, с. 40].

Відповідно, національна безпека перебуває у взаємозв'язку із чинниками, які щодо неї можуть розглядатися як загрози, адже «національна безпека є системою оптимізації взаємовідносин між усвідомленими загрозами та ресурсами, що має суспільство для протидії цим загрозам. Загрози для суспільства є завжди, а рівень захищеності від них ніколи не буває максимальним. Тому національна безпека є динамічним засобом досягнення і підтримки балансу між реальними та потенційними загрозами, з одного боку, та здатністю суб'єкта протидіяти їм, з іншого» [4, с. 84].

Попри те, що поняття загрози неодноразово наводилося у різних доктринальних та нормативно-правових джерелах, досі немає єдиного підходу до визначення його змісту та ролі у теорії безпекознавства. Зокрема, А. Антонов і В. Балашов визначають загрозу як процес настання таких змін у стані особи, суспільства й держави, що оцінюються ними як здатні створити перешкоди або унеможливити реалізацію їхніх інтересів [5, с. 48]. Разом з тим, слово «загроза» у словнику С. Ожегова [6, с. 673]. означає можливу небезпеку, тобто, небезпеку, поки що не реалізовану. Тому поняття «загроза» припускає не лише процес настання змін, але й можливість його настання. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь», «те, що може заподіювати яке-небудь зло, якусь неприємність» [7, с. 95].

Що стосується загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників і умов, що створюють небезпеку певному об'єкту. Так, Л. Чистоклетов, визначаючи сутність загрози безпеці господарюючого суб'єкта, вказує, що це є певний розвиток подій, дія або бездіяльність, унаслідок яких можливий негативний вплив на господарюючий суб'єкт, здатний завдати останньому такої шкоди, котра оцінюється як істотна [8, с.62].

В. Гордієнко звертає увагу на багатозначність понять «загроза», «небезпека», «виклик» та «ризик», які в теорії безпекознавства використовуються і як самостійні, і як взаємовизначальні та навіть як синонімічні [9, с. 112]. Дослідник пропонує розглядати загрозу як найвищий ступінь небезпеки (безпосередню небезпеку), а небезпеку – як потенційну загрозу. У свою чергу, небезпека розглядається як завдання шкоди тим або іншим інтересам, для реалізації чого необхідне створення відповідних умов (можливостей і намірів). То ж небезпека припускає наявність або намірів, або можливості завдання збитків, тоді як загроза включає і те, й інше. Небезпеки можуть виходити з багатьох джерел і діяти стосовно багатьох об'єктів, маючи безадресний характер, тоді як загроза, маючи конкретне джерело й об'єкт, завжди має персоніфікований характер. Загроза за такого підходу розглядається як «сукупність умов та факторів, що створюють реальну і потенційну небезпеку (виклик, ризик) об'єктам... безпеки» [9, с.113].

М. Гацко, поділяючи погляди В.Гордієнка на доцільність змістовного розмежування понять «небезпека» і «загроза», вибудовує відповідний причинно-наслідковий ланцюг таким чином: виклик – небезпека – загроза, зазначаючи, що загрози і небезпеки перебувають у відношеннях залежності, які в разі зниження рівня загрози можуть призводити до зростання небезпеки [10].

М. Дзлів і А. Урсул вважають, що загроза – це найбільш конкретна й безпосередня форма небезпеки, створювана цілеспрямованою діяльністю відверто ворожих сил; небезпека – усвідомлювана, але не фатальна ймовірність завдання шкоди кому-небудь, чому-небудь, зумовлена наявністю об'єктивних і суб'єктивних факторів, що володіють вражаючими властивостями; об'єктивно існуюча можливість негативного впливу на соціальний організм, у результаті якого йому може бути заподіяна певна шкода, що погіршує його стан, надає його розвитку небажаних динаміки й параметрів (характер, темпи, форми тощо) [11, с.62].

Погоджуючись із розумінням безпеки й небезпеки як полярних станів об'єкта, пов'язаних зі збереженням або зміною його системних характеристик, під загрозами будемо розуміти чинники, здатні призвести до небезпеки, тобто, до негативних змін системних характеристик об'єктів безпеки [12, с.33].

У теорії забезпечення національної безпеки категорія «загроза» має не менш важливе значення, ніж категорія «життєво важливі інтереси», і тісно пов'язана з останньою, оскільки джерела загроз містяться передусім у багатоманітності й розбіжності інтересів. Загрозу також пропонують розглядати як «посягання на інтерес» [13, с.124], що, однак, є сумнівним з точки зору досягнення мети чіткого визначення змісту цієї категорії, оскільки інтерес – це усвідомлена потреба, а посягання на потребу, так само, як і захист потреби, не впливають ані на її існування, ані на усвідомлення.

Щодо загроз, які посягають на інформаційну безпеку, то з цього приводу Р.Б. Тарасенко її визначає як сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері [14].

Найбільш небезпечні загрози інформаційній безпеці держави, передусім транскордонні та такі, що мають політичне забарвлення, вже тривалий час вивчаються в рамках проблеми інформаційної війни, під поняттям якої об'єднуються. Інформаційна війна, з урахуванням існуючих точок зору на її природу [15, с.124; 16, с. 130], може бути визначена як сукупність цілеспрямованих інформаційних впливів, що здійснюються з використанням інформаційної зброї (алгоритму цілеспрямованого впливу на інформаційну систему шляхом передачі їй інформації або здійснення з інформацією інших запланованих дій), а також дій, не опосередкованих її використанням, спрямованих на заволодіння інформацією, що не є загальнодоступною, її несанкціоноване поширення, модифікацію або знищення, здійснювані задля досягнення запланованої мети. Небезпека, реальність та ефективність проявів інформаційної війни забезпечуються сугестивним характером впливів, таємним або завуальованим характером несанкціонованого одержання інформації чи її застосування, інших шкідливо-результативних дій в інформаційній сфері, які, у свою чергу, безпосередньо створюють умови для утиску інтересів, насамперед національних, або порушення процесів функціонування інформаційних систем [17, с.290].

Одним із джерел загроз інтересам суспільства в інформаційній сфері є також безперервне ускладнення інформаційних систем,

тому особливою групою актуальних для України загроз інформаційній безпеці є загрози, зумовлені віртуалізацією [18, с. 139] – соціальним відчуженням людини, зануренням її в особистісний віртуальний світ.

Відтак, система загроз інформаційній безпеці має комплексний характер і в загальному вигляді включає в себе такі типи загроз: загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери та соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Відповідно, доцільно погодитись із визначенням загроз інформаційній безпеці держави як сукупності умов та факторів, які становлять небезпеку життєво важливим інтересам держави суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [19, с. 89].

Утім, технічний аспект не є головним у структурі інформаційної безпеки. Необхідно забезпечити не лише безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку маршрутизації, але й інформаційну безпеку суспільства. Власне ж суспільство є носієм такої глобальної загрози інформаційній безпеці людини, як інформаційна дискримінація, котра проявляється в розподілі людей на тих, що мають доступ до інформації, і тих, які його позбавлені.

-
1. Про основи національної безпеки України: Закон України від 19.06.2003 року. URL: <http://zakon2.rada.gov.ua/laws/show/964-15>.
 2. Горбулін В.П., Качинський А.П. Засади національної безпеки України: [підручник] /В.Горбулін, А.Качинський. К.: Інтер-технологія, 2009. С. 13-16
 3. Сацута А.А. Национальная безопасность как социальное явление: современная парадигма. Вестник Военного университета. 2007. № 3 (11). С. 39.
 4. Горлач М.І., Кремень В.Г. Політологія: наука про політику. К.: Центр Учбової літератури, 2009. С. 84.

5. Антонов А.Б., Балашов В.Г. Основы обеспечения безопасности личности, общества и государства [учебное пособие]. М.: Институт защиты предпринимателя, 1996. С. 48
6. Ожегов С.И. Словарь русского языка. М.: Рус. яз., 1988. С. 673
7. Словник української мови: [в 11-ти т.]/ АН УРСР, Ін-т мовознавства ім.О.О. Потебні; [редкол.: І.К. Білодід (голова) та ін.]/ Т.3 [ред.: Г.М. Гнатюк, Т.К. Черторизька]. К.: Наукова думка, 1972. С. 95.
8. Чистоклетов Л. Г. Безпека суб'єктів господарювання в Україні: теорія і практика адміністративно-правового забезпечення : монографія. Львів: Растр-7, 2016. 310 с.
9. Гордиенко В.В. Безопасность России в условиях глобализации (криминологические и социально-правовые проблемы): дисс. ... докт. юрид. наук: 12.00.08/ В.Гордиенко. М., 2005. С. 111-113.
10. Гацко М. О соотношении понятий «угроза» и «опасность»/ М.Гацко // Обозреватель – Observer. URL: [observer.materik.ru/observer / N07_97/ 7_06.htm](http://observer.materik.ru/observer/N07_97/7_06.htm).
11. Дзлиев М.И., Урсул А.Д. Основы обеспечения безопасности России: [учебное пособие]/ М.Дзлиев, А.Урсул. – М.: Рос. гос. торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития, 2003. 298 с.
12. Жаглин А.В. Общественная безопасность как социальное явление и элемент системы национальной безопасности . Вестник ВИ МВД России. 2007. №1.
13. Общая теория национальной безопасности: [учебник]/под общ. ред. А.А. Прохожева, изд. 2. М.: РАГС. 2005. С. 124.
14. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. 512 с. URL: [http://www. ukr. vipreshebnik.ru/2012-06-25-18-22-00/563-2011-06-18-18-00-40.html](http://www.ukr.vipreshebnik.ru/2012-06-25-18-22-00/563-2011-06-18-18-00-40.html).
15. Стрельцов А.А. Направления совершенствования правового обеспечения информационной безопасности Российской Федерации // Информационное общество. 1999. № 6. С. 18
16. Красноступ М.Д. Інформаційна війна - міфи чи реальність?/ М.Красноступ// Інформаційні технології та захист інформації. 1999. №1. С. 130
17. Хананашвили М.М. Информационные неврозы/ М. Хананашвили. М.: Медицина, 1986. С. 290.

18. Силаева В.Л. Интернет и подмена реальности. Общество электронных коммуникаций: новые возможности и актуальные проблемы: Материалы VI Энгельмейеровских чтений. Москва-Дубна, 22-23.03.2002, Дубна, 2003. С. 139.
19. Інформаційна безпека (соціально-правові аспекти): [підручник] / В.Остроухов, В.Петрик, М.Присяжнюк та ін.; за ред. Є. Д. Скулиша. К. : КНТ, 2010. С. 89.

Розділ 2.

НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-
ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В
ОСВІТНЬОМУ ПРОЦЕСІ

ВІДЕОКУРС З ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Глинський Ярослав Миколайович,

*доцент кафедри обчислювальної математики та програмування
Національного університету «Львівська політехніка»,
кандидат фізико-математичних наук, доцент*

Пелех Ярослав Миколайович,

*доцент кафедри обчислювальної математики та програмування
Національного університету «Львівська політехніка»,
кандидат фізико-математичних наук, доцент*

Ряжська Вікторія Анатоліївна,

*доцент кафедри обчислювальної математики та програмування
Національного університету «Львівська політехніка»,
кандидат фізико-математичних наук, доцент*

Останнім часом спостерігається невміння, а часто просто небажання студентів працювати з твердими копіями підручників і навчальних посібників. Причиною цього явища є неналежна увага до цього питання під час загальноосвітньої підготовки, а також бурхливий розвиток сучасних інформаційно-комунікаційних технологій і різних альтернативних засобів і способів навчання. Вдало створені відеоресурси (відеоуроки і відеолекції та їх колекції) є такими альтернативними засобами, які можуть виправдати покладені на них очікування щодо мотивування студентів до навчання. Відеоресурси дають змогу автоматизувати навчальний процес, перерозподілити навчальний час на користь позааудиторної самостійної роботи студентів і вивільнити лекційний час для більш повного викладу фундаментальних основ навчальних дисциплін, а також сприяють впровадженню в очну форму навчання елементів дистанційного навчання.

Відеокурс – сукупність електронних освітніх ресурсів (ЕОР), що відображають зміст навчальної дисципліни, розроблених з використанням різних форматів даних, де значну роль відіграють авторські чи запозичені вільнопоширювані відеозасоби. Технічна

реалізація: сукупність ЕОР, структурованих як електронний навчально-методичний комплекс (ЕНМК) чи інакше, де переважна більшість тем розкривається засобами відеолекцій чи комбінованими засобами (текстово-графічними матеріалами і колекцією відеоуроків чи достатньою кількістю коротких відеоеlementів).

В [1] розглядалися класифікації і характеристики електронних освітніх ресурсів (ЕОР) навчального призначення, виокремлювалися електронні освітні відеоресурси (ЕОВ) як окремий вид ЕОР, досліджувалися властивості ЕОВ і на прикладах розробок, виконаних у НУ «Львівська політехніка», описувався досвід розроблення і використання ЕОВ для побудови базового курсу інформатики у закладі вищої освіти.

На даний час близьким до завершення розробки є авторський відеокурс з інформаційних технологій для студентів гуманітарних спеціальностей, реалізований в рамках ЕНМК [2] у ВНС «Львівської політехніки», де п'ять з восьми розділів інформатики («Прикладне програмне забезпечення», «Текстові редактори», «Електронні процесори», «Бази даних» і «Презентації») підтримуються авторськими відеоуроками середньої тривалості по 15 хв, що в сукупності достатньо повно висвітлюють трудні чи особливо актуальні питання основних тем навчальної дисципліни. Весь матеріал курсу, що подається у текстовому і відеоформатах, побудований на основі авторського навчального посібника [3].

Відеокурс пройшов первинну апробацію. Результати апробації показують підвищену зацікавленість студентів до сприйняття інформації у відеорежимі і демонструють покращення результатів поточного навчання порівняно з попередніми роками.

Відеокурс містить дванадцять авторських відеоуроків, десять запозичених і значну кількість відеоеlementів. Особливу увагу рекомендуємо звернути на авторський відеоресурс «Основи комп'ютерної математики з Microsoft Mathematics» [4], що, як ми довели, є тематичним засобом у методичній системі навчання інформатики та вищої математики і дає змогу впровадити зазначену тему у програму навчання навіть викладачами без відповідного практичного досвіду. А авторські відеоуроки з

розділів «Електронні процесори» і «Бази даних» не залишать байдужими не тільки студентів, але й досвідчених викладачів.

Результати виконаних робіт щодо розробки і впровадження відеоресурсів показують їх ефективність і здатність суттєво впливати на зміст, якість і мотивацію навчання інформатичних дисциплін і можливість розбудови різноманітних курсів, що стосуються базових інформаційних технологій, викладачами з різних закладів вищої освіти на основі колекції відеоресурсів, які розміщені на вільнодоступному каналі з назвою «Ярослав Глинський» на відеохостингу Youtube за умови коректних на них гіперпосилань.

-
1. Глинський Я., Федасюк Д., Ряжська В., «Розроблення і використання електронних відеоресурсів навчального призначення», Інформаційні технології і засоби навчання, №2 (58), с. 67–78, 2017. [Електронний ресурс]. Доступно: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1580/1151>.
 2. Глинський Я.М., Ряжська В.А. Електронний навчально-методичний комплекс «Інформатика та сучасні інформаційні технології» для студентів першого курсу Інституту гуманітарних і соціальних наук спеціальності «Соціологія». – Режим гостьового доступу: <https://vns.lpnu.ua>.
 3. Глинський Я.М. Інформатика. Практикум з інформаційних технологій. «Підручники і посібники», Тернопіль – 2014.
 4. Ярослав Глинський. Основи комп'ютерної математики з Microsoft Mathematics. [Електронний ресурс]. – Режим доступу: <https://www.youtube.com/watch?v=nAg-ZmWONGA&t=144s>.

АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕС ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ПРАВООХОРОННОЇ СФЕРИ У ВНЗ З ОСОБЛИВИМИ УМОВАМИ НАВЧАННЯ

Косаревська Ольга Віталіївна,

*доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ,
кандидат педагогічних наук, доцент*

Одним із ключових напрямків «Стратегії розвитку системи МВС України до 2020 року» висувається зміцнення кадрового потенціалу, за рахунок удосконалення відомчої освіти на шляху створення налагодженої системи внутрішніх комунікацій у сфері професійної здатності працівників правоохоронної сфери швидко отримувати, аналізувати велику кількість оперативної інформації та грамотно складати юридичні документи.[1].

ВНЗ зі специфічними умовами навчання є окремим осередком в системі вищої юридичної освіти в Україні.

Інтенсивний розвиток інформаційних технологій в комунікативній системі суспільства, а саме в мережі Інтернет, с кожним роком набирає обертів.

Сучасний злочинний світ має в декількох аспектах перевагу перед системою інформаційно-технічного забезпечення правоохоронних органів, за рахунок:

- нестачі висококваліфікованого ІТ-персоналу;
- об'єктивно замалого виділення бюджетних коштів для необхідного сучасного матеріально-технічного забезпечення оперативних підрозділів НПУ та інших правоохоронних структур.

З огляду цього, інформаційно-технічна підготовка здобувачів вищої освіти у ВНЗ з особливими умовами навчання набуває своєї актуальності.

Останнім часом провідні фахівці інформаційного права та теорії управління, а саме :О.Ю Іохов,К.Ю Ісмайлов,О.Є Користін, О.О Косиченко, О.М Куракін, О.В Придатко, Є.В Рижков, В.В Сеник, В.В Тулупов та інш. активно дискутують стосовно пріоритетних напрямків організації навчально-виховного процесу ВНЗ з особливими умовами навчання з підготовки майбутнього фахівця-правоохоронця нової формації , де наголошується акцент саме на інформаційно- технологічну підготовку.

Сучасний кіберпростір являє собою складне інформаційне утворення, в якому на підставі розвитку інформаційних технологій, може:

- швидко розповсюджуватись не тільки правдива, корисна інформація але й інформація із запрограмованим шкідливим контентом;
- можливе отримання несанкціонованого доступу до закритих інформаційно-телекомунікаційних систем (ІТС), що стосується загроз інформаційній безпеці не тільки державних, але й особистих інтересів громадян;
- відбувається вплив на поширення «інформаційної війни» та політичну напруженість у світі.

З огляду проблем організації інформаційно-технологічної фахової підготовки висококваліфікованих кадрів для системи МВС України у ВНЗ з особливими умовами навчання, на нашу думку, актуальними аспектами постає наступне.

По-перше, це модернізація автоматизації процесів отримання, обробки, передачі базових інформаційних освітніх ресурсів, за рахунок впровадження новітніх інформаційно-педагогічних технологій та удосконалення інформаційно-технологічної підготовки, спрямованих на:

1. опанування інноваційними дидактичними технологіями, а саме:
 - «ґридівська» та «хмарна» технології на навчально-наукових кластерах;
 - технологія «цифрових наративів»;
 - комп'ютерна візуалізація — «мульти-медійна» технологія;

2. створення об'єктивно орієнтованих програмних систем із заданою моделлю «комп'ютерної бази користувача» (наповнення засобів навчання базами даних, електронними таблицями, графічними редакторами тощо);
3. розробку експертних навчальних систем (ознайомлення з сучасними системами штучного інтелекту, які використовуються у практичній діяльності НПУ та інших правоохоронних органах). [2, С.191-192].

По-друге, це організація інформаційно-навчальної та експериментально-дослідної роботи курсантів та студентів, за рахунок створення предметно-орієнтованого середовища навчального і розвиваючого призначення.

Наприклад, в Одеському державному університеті внутрішніх справ під керівництвом завідувача кафедри КБ та ІЗ Ісмайлова К.Ю. створена і функціонує експериментальна моніторингова група (з числа атестованого складу), метою якої є цілодобовий моніторинг мережі «Інтернет» по виявленню шкідливого та протиправного контенту, що створює можливі та наявні загрози для стану громадського порядку та законності.

В рамках роботи наукового гуртка «Правоохоронець» кафедри КБтаІЗ на підставі тренінгової педагогічної моделі Косаревської О.В. проводиться позааудиторна правовиховна робота з протидії наркозлочинності серед молоді.[2,С.192-196].

Також науково-дослідна лабораторія з проблемних питань кримінального аналізу ОДУВС проводить наукові дослідження з проблем протидії кіберзлочинності (в рамках тематики наукових грантів).

По-третє, це удосконалення процесу самостійної навчальної діяльності, за рахунок:

- організації факультативних занять із залученням провідних фахівців кіберполіції, управління кримінального аналізу, практичних підрозділів з протидії наркозлочинності тощо;
- оснащення спеціальних бібліотек ВНЗ з особливими умовами навчання навчально-методичними комплексами у

вигляді електронних підручників з обмеженим доступом інформації, на підставі вивчення сучасної наукової думки в сфері інформаційно-технічного забезпечення діяльності правоохоронних органів України та критичного аналізу недоліків в діяльності практичних оперативних підрозділів НПУ.

По-четверте, у відповідності змін до кадрових вимог щодо забезпечення проведення освітньої діяльності в сфері вищої та післядипломної освіти для осіб з вищою освітою, які зазначені у ліцензійних умовах освітньої діяльності [4], особливим акцентом для науково-педагогічного складу ВНЗ з особливими умовами навчання, на нашу думку, повинна стати нова кваліфікаційна ознака для педагогічних кадрів, які викладають цикл інформаційно-технологічного спрямування, під якою нами розуміється:

- наявність вищої технічної освіти та відповідного наукового ступеню та наукового звання;
- обов'язковий досвід правоохоронної діяльності;
- пріоритетність заняття на конкурсній основі посад викладацького складу ВНЗ для ІТ-фахівців, які мають практичний досвід в сфері інформаційної безпеки.

Завдяки цьому, на наше переконання, буде досягатись як підвищення якості освітніх послуг, так і мотивація проведення наукових досліджень у сфері інформаційних технологій з протидії кіберзлочинності та забезпечення кібербезпеки України.

На підставі вищезазначеного, ми дійшли наступних висновків.

Інформаційно-комунікативна компетенція майбутнього «інтегрованого правоохоронця» являє собою комплекс теоретичних знань та практичних навичок отриманих під час інформаційно-технологічної фахової підготовки у ВНЗ з особливими умовами навчання, спрямованих на вміння працювати з великою кількістю інформації і використовувати її для отримання, обробки, передачі та зберігання за допомогою комп'ютерних інформаційних технологій і сучасних технічних засобів, з метою з'ясування можливостей використання оперативної інформації як доказової бази у розслідуванні злочинів, пов'язаних з використанням комп'ютерної техніки (кіберзлочинність).

Інтенсифікація професійної підготовки у ВНЗ з особливими умовами навчання передбачає, перш за все, інтелектуальну взаємодію науково-педагогічного складу та здобувачів вищої юридичної освіти; формування інноваційного мислення на підставі модернізації пізнавальної навчальної діяльності, за рахунок впровадження сучасних освітніх інформаційних технологій, з метою отримання продуктивного результату – знань, вмінь, навичок, компетенції для майбутньої правоохоронної діяльності.

-
1. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року: розпорядження Кабінету Міністрів України від 15.11.2017 № 1023-р.// БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80> (дата звернення 10.04.2018).
 2. Підготовка поліцейських в умовах реформування системи МВС України, Харків. Нац. ун-т внутр. справ, каф. спец. фіз. підготовки ф-ту №2 – Харків: ХНУВС, 2018. – 246 с.
 3. Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук. практ. конф., м. Одеса, 17 листопада 2017 р. – Одеса: ОДУВС. - 2017. – 204 с.
 4. Постанова Кабінету Міністрів України «Про затвердження ліцензійних умов провадження освітньої діяльності» від 30 грудня 2015р. №1187 (в редакції постанови Кабінету Міністрів України від 10 травня 2018р. №347).

РЕАЛІЗАЦІЯ ІНДИВІДУАЛЬНОЇ ТРАЄКТОРІЇ НАВЧАННЯ КУРСАНТІВ ВВНЗ

Лунькова Ганна Володимирівна,

*доцент кафедри електромеханіки та електроніки,
Національної академії сухопутних військ
ім. гетьмана Петра Сагайдачного,
кандидат технічних наук*

Філімонов Сергій Миколайович,

*старший викладач кафедри електромеханіки та електроніки,
Національної академії сухопутних військ
ім. гетьмана Петра Сагайдачного*

Міхалєва Марина Станіславівна,

*професор кафедри електромеханіки та електроніки,
Національної академії сухопутних військ
ім. гетьмана П. Сагайдачного,
кандидат технічних наук, доцент*

Перехід до особистісно-орієнтованої моделі навчання курсантів, зумовлена з однієї сторони актуальністю проблеми оптимізації затрат на навчання під час ведення бойових дій на сході країни та соціально-економічним станом України, з іншої сторони неоднорідністю підготовки курсантів, враховуючи великий відсоток військовослужбовців, які прийшли до навчання після проходження військової служби з зони бойових дій. Остання зумовили актуальність задачі трансформації сучасного освітнього середовища на основі комп'ютерних технологій навчання. Основна тенденція розвитку учбово-виховного процесу у військовому вузі полягає у: суттєвому збільшенні часу на самостійну роботу курсантів; побудові методики учбової діяльності курсантів на основі використання інформаційних технологій; в об'єднанні накопиченого арсеналу методів, засобів та форм навчання для самоорганізації наукової, учбової і практичної діяльності курсантів; підвищення мотивації до вивчення питань експлуатації озброєння та військової техніки. Специфіка функціонування

військового навчального закладу передбачає можливість відсутності курсантів на планових заняттях через забезпечення внутрішнього наряду, несення вартової служби, службових відряджень та інших планових заходів. Крім того, курсанти можуть бути відсутніми й за традиційних причин: хвороби, участь в спортивних змаганнях тощо.

Тому необхідна якість підготовки майбутніх офіцерів може бути досягнута тільки при такій організації навчального процесу, яка б дозволила курсантам, які мають пропуски планових занять отримати: необхідну навчальну інформацію з питань, вивчених на припущеннях заняттях; бути забезпеченими необхідними інструментами самоконтролю; виконати лабораторні експерименти; мати необхідну методичну підтримку в самостійному виконанні робіт; отримати оперативну необхідну консультацію.

Виникає проблема формування індивідуальних траєкторій навчання з вирішенням завдань в предметній області дисципліни яка вирішується впровадженням інформаційно-комунікаційного навчального середовища з використанням в процесі навчання особистісно-орієнтовану технологія навчання.

Сутність особистісно орієнтованого підходу у підготовці військових фахівців полягає в диференціації завдань і методики навчання залежно від можливостей курсанта. Диференційований підхід викладача дає можливість в умовах навчання в Національній академії сухопутних військ використання усіх можливостей освітніх компонентів, таких як: розробка індивідуальних траєкторій навчання, спецкурсів, спецсемініарів та факультативів: вибір тем рефератів, курсових та дипломних робіт; вибір тем науково-дослідної роботи; вибір довготривалих завдань самостійної роботи тощо.

Сутність диференціації навчання курсантів у НАСВ полягає у відкритості та варіативності навчання, різноманітності методів, засобів і форм організації навчальної діяльності шляхом заходів, які забезпечують кожному курсанту засвоєння знань та умінь відповідно необхідного рівня компетентності, враховуючи можливості курсанта. У навчальному процесі НАСВ використовуються навчальні курси дисциплін факультетів Академії, розроблені в

модульному об'єктно - орієнтованому динамічному навчальному середовищі MOODLE.

В такий спосіб у навчальний процес НАСВ впроваджується методика реалізована на основі діяльнісного підходу, мета впровадження якої – змістити акцент в навчанні із засвоєння фактів (результат – знання) на оволодіння способами взаємодії зі світом (результат – уміння). Інформаційно-навчальне середовище містить на сьогоднішній день 435 курсів, 2574 користувачів, 3075 ресурсів.

Вихідними даними для наповнення контенту курсу є робоча навчальна програма та відповідне інформаційно-методичне забезпечення дисципліни.

Впровадження інтелектуальної системи організації навчального процесу з можливістю реалізації індивідуальних траєкторій формування компетентностей військових фахівців представляємо на прикладі курсу «Інформаційні технології» кафедри електро-механіки та електроніки факультету Ракетних військ та артилерії НАСВ. У навчальному процесі кафедри ЕМЕ активно використовуються навчальні курси дисциплін факультетів Академії, розроблені в модульному об'єктно - орієнтованому динамічному навчальному середовищі MOODLE.

Таким чином в навчальний процес впроваджується методика реалізована на основі діяльнісного підходу, мета впровадження якої – змістити акцент в навчанні із засвоєння фактів (результат – знання) на оволодіння способами взаємодії зі світом (результат – уміння). Інформаційно-навчальне середовище кафедри ЕМЕ містить 38 курсів.

Контент курсів дисциплін включає в себе:

1. Інформаційні ресурси. Методичне забезпечення дисципліни: робочі програми, основну та додаткову літературу в форматі PDF, електронні підручники. Методичне забезпечення навчальних занять: лекції, презентації та методичні розробки до самостійних занять; допуск до лабораторних робіт у вигляді тестів; методичні розробки до лабораторних та практичних занять; завдання до лабораторних занять; варіанти виконуваних робіт; матеріал до опрацювання.

2. Систему тестування. Контрольні тести та навчальні тести в складі лабораторних та практичних робіт. Безпосередньо на аудиторних заняттях курсанти проходять вхідне тестування. Перед виконанням лабораторної роботи курсанти складають тест вхідного контролю, що складається з 15 питань по заданій темі. Питання вибираються випадковим чином. Курсанти, які набрали менш як 70%, до лабораторної роботи не допускаються і повинні перездати тест – це дозволяє значно збільшити час продуктивної роботи викладача з курсантами. Для підготовки курсантам пропонується дистанційно пройти навчальний тест. Підсумкова оцінка за курс складається за результатами виконання всіх робіт за кожен пропонований модуль, який викладач вважатиме за потрібне включити в розрахунок.
3. Систему адміністрування, що забезпечує доступ до особистої інформації, дошки оголошень адміністрації, інтерактивним форумам, опитуванням тощо. Статистика моніторингу навчальної діяльності курсантів накопичується, узагальнюється і систематизується. Створюється портфоліо кожного курсанта: всі здані ним роботи, оцінки та коментарі викладача, повідомлення на форумі, контроль за відвідуваністю і активністю курсантів, час їх навчальної роботи в мережі. Ця інформація дозволяє викладачеві реалізувати оптимальні освітні траєкторії для кожного курсанта, своєчасно вплинути на навчальну діяльність курсантів, скоригувати проблеми в навчанні, розвинути у курсантів розуміння і потребу в систематичній самостійній роботі.
4. Засоби спілкування, що забезпечують процес взаємодії курсанта як з викладачем (адміністратором) , так і з іншими курсантами.
5. Систему захисту інформації відповідно до специфіки функціонування ВВНЗ.

В подальшій роботі передбачено:

- наповнення контенту курсів мультимедійною інформацією;
- оновлення матеріалів курсів;
- організація відео зв'язку за наявності відповідної апаратури;

- за умови оновлення системи до версії 3.XX, застосувати модуль компетентностей, для реалізації компетентнісного підходу до організації навчання.

На першому лабораторному занятті курсанти проходять зріз залишкових знань, які визначають ступінь підготовленості курсанта до вивчення дисципліни «Інформаційні технології». Подальший аналіз дозволяє формувати індивідуальної траєкторії навчання дисципліни. За результатами наукової роботи – вищого рівня **індивідуальної траєкторії навчання** кожного року поспіль курсантські роботи подаються на конкурси: Всеукраїнський конкурс студентських наукових робіт з природничих, технічних та гуманітарних науки; конкурс наукових робіт Національної академії Державної прикордонної служби України імені Б. Хмельницького; конкурс на кращу наукову роботу курсантів (слухачів) Національної академії сухопутних військ імені Петра Сагайдачного. Для реалізації індивідуального підходу до навчання курсантів викладачами використовуються методичні прийоми, які використовуються під час проведення занять, а саме: використання системи MOODLE, спеціалізованих комп'ютерних програм, відеоуроків, посібників, фільмів, презентацій, макетів, а також: творчий, персонально-компетентнісний підхід до викладання матеріалу, співпраця з курсантами, проектно-побудоване навчання дисциплін тощо. Розроблені в модульному об'єктно-орієнтованому динамічному навчальному середовищі MOODLE 90% дисциплін.

Використання концептуальних понять індивідуального підходу до навчання має на меті досягнення чотирьох головних завдань сучасної освіти:

- формування особистостей, які будуть навчатись протягом усього життя.
- створення навчального середовища, яке базується на взаємній повазі та принципах демократії.
- забезпечення безперервності процесу інтелектуального розвитку й вироблення відповідних умінь (забезпечення зв'язку теорії та практики).
- гарантоване оволодіння теорією та практичними вміннями для успішної участі в демократичному суспільстві.

ОСОБЛИВОСТІ ВИКЛАДАННЯ ІНФОРМАЦІЙНИХ ДИСЦИПЛІН В ДНІПРОПЕТРОВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

Прокопов Сергій Олександрович,

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

Використання інформаційної підтримки діяльності працівників Національної поліції України є одним з надважливих елементів ефективності виконання ними службових завдань. Найкраще опановувати практичні навички щодо використання інформаційно-пошукових та телекомунікаційних систем Національної поліції під час навчання у навчальних закладах. Інформаційні дисципліни у поліцейських закладах викладаються у вигляді двох дисциплін «Інформаційні технології» (10 годин, в рамках початкової підготовки курсантів) та «Інформаційне забезпечення професійної діяльності» (24 години з викладачем). Відсутність доступу навчальних закладів до реальних баз даних та систем Інформаційного порталу Національної поліції знижує рівень підготовки поліцейських за інформаційним напрямом.

Вважаючи, що авторським колективом кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ була розроблена та впроваджена у навчальний процес інформаційно-технічна платформа комплексних навчань «Лінія 102» [1], частина якої є емулятором інформаційно-телекомунікаційної системи «ЦУНАМІ» Інформаційного порталу Національної поліції. Даний емулятор вивчається курсантами Дніпропетровського державного університету внутрішніх справ у дисципліні «Інформаційне забезпечення професійної діяльності» під час розгляду теми «Навчальна інформаційно-технічна платформа комплексних оперативно-тактичних навчань «ЛІНІЯ 102».

На практичному занятті з цієї теми курсанти виконують наступні практичні справи:

1. Створюють нову електронну «Картку 102» [2], вводючи інформацію про подію (рис. 1).

Рис. 1. Вигляд електронної картки 102 емулятора «ЦУНАМІ».

2. Переглядають інформацію на умовних робочих місцях диспетчера Ситуаційного центру або чергового відділу поліції (рис. 2).

Рис. 2. Робоче місце диспетчера емулятора.

3. Виконують дії на планшеті наряду поліції «Прийняв», «Прибув» та «Виконав» [3] (рис. 3).

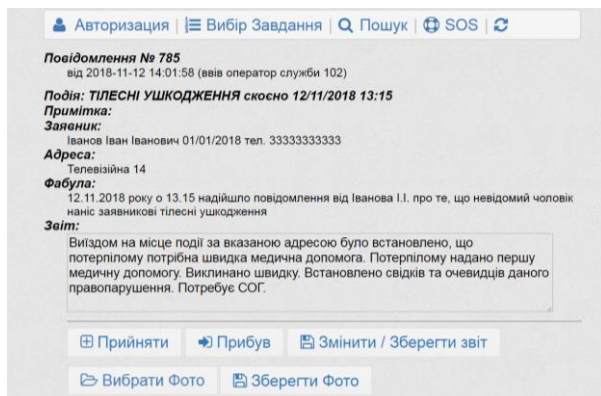


Рис. 3. Вигляд електронної картки реагування на подію наряду поліції (патрульного, СОГ та ін.) емулятора.

Причому на планшеті наряду поліції реалізована функція збереження фотоматеріалів з місця події. Якщо при звітування наряд поліції додає фотозображення, та на картці диспетчера (чергового відділу поліції) відображується «скріпка» та збережені фотографії (рис. 4).

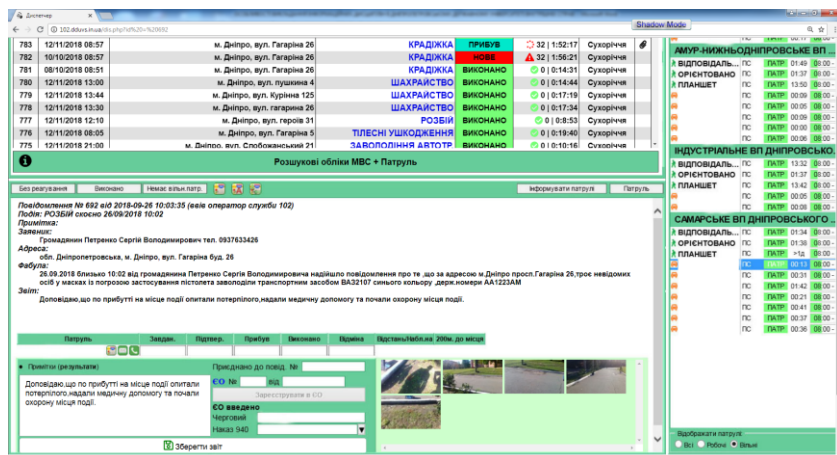


Рис. 4. Електронна картка диспетчера (чергового) емулятору після звітування на завдання наряду поліції.

Як видно з вищевикладеного емулятор передає основні елементи реальної інформаційно-телекомунікаційної системи «ЦУНАМІ». І може надати не тільки уявлення, але і необхідні практичні навички щодо використання даної інформаційної системи.

Кожному з поліцейських навчальних закладів наданий доступ до розробленої фахівцями Дніпропетровського державного університету внутрішніх справ інформаційно-технічної платформи тренінгу «Лінія 102» (рис. 5).

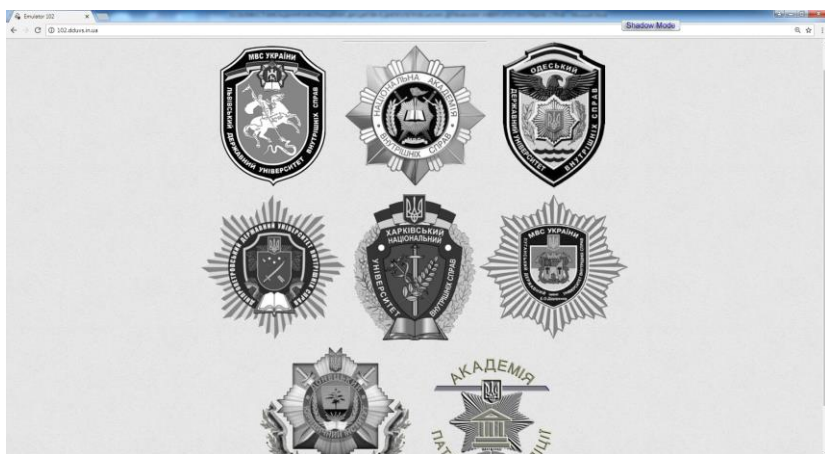


Рис. 5. Загальний вигляд веб-ресурсу <http://102.dduvs.in.ua/>.

Пропонується ввести в навчальний процес поліцейських навчальних закладів при вивченні теми «Інформаційно-телекомунікаційна система «ЦУНАМІ» Інформаційного порталу Національної поліції» дисципліни «Інформаційне забезпечення професійної діяльності» розглянутий у даній доповіді емулятор реальної системи «ЦУНАМІ». Це позитивно відобразиться на рівні інформаційної підготовки майбутніх правоохоронців.

1. Гавриш О.С., Махницький О.В., Прокопов С.О. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС/ Наукова стаття. Науковий журнал Право і суспільство. – 2017. – № 1-1. – С. 128–141.

2. Прокопов С.О. Інформаційне забезпечення професійно-орієнтованої ділової гри «Лінія 102»/ Матеріали II міжнародної науково-практичної конференції (15.03.2018 м. Дніпро).– Дніпропетровський державний університет внутрішніх справ, 2018. – С. 439-443.
3. Прокопов С.О. Навчальне автоматизоване робоче місце патрульного поліцейського в інформаційно-технічній платформі інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції у ДДУВС/ матеріали Всеукраїнської науково-практичної конференції (14 квітня 2017 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – С. 153-160.

МЕРЕЖЕВІ МОДЕЛІ ВЗАЄМОДІЇ В ІНФОРМАЦІЙНО-ОСВІТНЬОМУ СЕРЕДОВИЩІ З ПІДГОТОВКИ ДЕРЖАВНИХ СЛУЖБОВЦІВ ПРАВООХОРОННОЇ СФЕРИ

Прокоф'єв Микола Миколайович,

*ад'юнкт кафедри адміністративного права та
адміністративного процесу*

Львівського державного університету внутрішніх справ

Інформатизація суспільства та зростання ролі новітніх інформаційних технологій виступають індикаторами переходу до нового типу суспільства – інформаційного суспільства, з новими факторами взаємодії в сфері освіти. Стратегія розвитку органів системи МВС України значне підвищення якості освіти у спеціалізованих вищих навчальних закладах [1]. Особливо важливо одержати високу якість освіти для майбутніх державних службовців правоохоронної сфери, які будуть працювати у Державній міграційній службі України та Експертній службі Міністерства внутрішніх справ України [2; 3].

В умовах становлення та розвитку інформаційно-освітнього товариства, мережева організація спільної діяльності виступає в якості оптимальної і ефективної форми досягнення цілей в будь-якій сфері, включаючи освітню сферу правоохоронної діяльності. Цей процес особливо актуальний для навчання фахівців у сфері безпеки та інших професій, які задіяні в різних сферах правоохоронної діяльності.

Необхідність перетворень в інформаційно-освітньому середовищі правоохоронної сфери обумовлена тим, що у даний час знання, отримані індивідом, стають капіталом і основним ресурсом, а освітній рівень індивідів виступає ключовим показником конкурентоспроможності держави.

Мережева взаємодія будується на горизонтальних взаєминах, що засновані на рівноправ'ї та взаємній зацікавленості один в одному, та спільне ухвалення рішень. Мережева взаємодія освітніх уста-

нов виступає в якості інноваційної технології, що сприяє ефективному функціонуванню та розвитку, процесу діалогу між освітніми установами та процесу поширення інноваційних розробок, орієнтованого на досягнення результату.

Цільовим пріоритетом створення мережі є отримання конкурентної і економічної переваги, на основі добровільного об'єднання зацікавлених суб'єктів, для вирішення конкретної проблеми або конкретного проекту.

Сукупність цілей мережевої взаємодії освітніх організацій професійної освіти, носять багатоплановий характер, можуть бути згруповані, на основі врахування специфіки організацій професійної освіти та форми, в наступні дві групи:

- загальні цілі мережевої взаємодії включають: створення єдиного освітнього простору з вільним рухом всіх факторів освітніх ресурсів; проведення єдиної освітньої політики з метою підвищення конкурентоспроможності випускників для правоохоронної сфери; розвиток співпраці освітніх організацій професійної освіти, що сприяє підвищенню ефективності функціонування.
- приватні цілі процесів взаємодії, що включають: різноманітність і варіативність професійної підготовки фахівців в умовах взаємодії єдиного освітнього простору; підвищення ролі галузевих вишів в інноваційному, технічному, технологічному розвитку правоохоронної сфери; підвищення рівня комерціалізації виробленої освітньої продукції та послуг, управління об'єктами інтелектуальної власності.

Застосування мережевих моделей взаємодії в інформаційно-освітній сфері сприяє: оптимальному розподілу ресурсів учасників взаємодії для досягнення спільної мети; можливості прояву ініціативи будь-якого конкретного учасника; прямому контакту учасників взаємодії по горизонталі; розробці адекватної стратегії досягнення мети в умовах зміни зовнішнього середовища; використання загального потенціалу мережі для ефективного функціонування конкретного учасника взаємодії.

Мережева взаємодія в системі вищої освіти, виступає фактором ефективної і якісної побудови освітньої діяльності, на основі мережевої форми реалізації освітніх програм.

Використання мережевої форми реалізації освітніх програм здійснюється на підставі договору між вишами, в якому зазначаються: вид, рівень і (або) спрямованість освітньої програми, реалізованої з використанням мережевої форми; статус здобувачів вищої освіти, правила прийому на навчання за освітньою програмою, що реалізується з використанням мережевої форми, порядок організації академічної мобільності здобувачів вищої освіти, які освоюють освітню програму, реалізовану з використанням мережевої форми; умови та порядок здійснення освітньої діяльності за освітньою програмою, що реалізовується за допомогою мережевої форми, в тому числі розподіл обов'язків між вишами, порядок реалізації освітньої програми, характер і обсяг ресурсів, використовуваних кожним вишем, що реалізує освітні програми за допомогою мережевої форми; видаються документ або документи про освіту та (або) про кваліфікацію, документ або документи про навчання, виші, що здійснюють освітню діяльність, якими видаються зазначені документи; термін дії договору, порядок зміни та припинення.

Мережева форма освітніх програм сприяє реалізації програм міжнародної та національної академічної мобільності науково-педагогічних працівників вищих навчальних закладів за наступними напрямками: організація стажувань, курсів підвищення кваліфікації та професійної перепідготовки; впровадження у вишах нових освітніх програм спільно з провідними європейськими та національними університетами і науковими організаціями, Європолом [4]; залучення здобувачів вищої освіти з провідних європейських університетів для навчання у вищих навчальних закладах, в тому числі шляхом реалізації партнерських освітніх програм з іноземними університетами та асоціаціями університетів.

Розглядаючи ресурсну концепцію мережевого навчання, як елемент сталої взаємодії освітніх установ, виділимо наступні групи освітніх ресурсів.

Кадрові ресурси, розглядаються як сукупність експертів, викладачів, які в процесі навчання використовують сучасні педагогічні технології, особисті методики з підготовки бакалаврів і спеціалістів відповідно до вимог державних стандартів та МВС України, інших правоохоронних установ.

Інформаційні ресурси представлені у вигляді: бази даних, що накопичують інформацію про зміни вимог до якості професійної підготовки у сфері правоохоронної діяльності; електронні бібліотеки; сховища мультимедійних продуктів тощо.

Матеріально-технічні ресурси: лабораторні об'єкти; спеціалізовані приміщення (навчальні майданчики); навчальне обладнання, інструменти та матеріали, включаючи реальне криміналістичне устаткування, що використовується в освітніх цілях; аналоги для тренажерів (комп'ютерні моделі, імітатори тощо).

Освітні ресурси розкривають сутність основних і додаткових професійних освітніх програм, професійних модулів; методичні матеріали (посібники, рекомендації для викладачів і здобувачів вищої освіти тощо); діагностичні інструменти для оцінки рівня навчального матеріалу; комп'ютерна підготовка та діагностичні програми.

Соціальні ресурси – встановлення партнерських відносин з правоохоронними організаціями регіону; горизонтальні зв'язки у професійно-педагогічному співтоваристві регіону; відносини з громадськими об'єднаннями, що виражають інтереси міжнародних і національних правозахисних організацій та професійних спільнот.

На основі вищесказаного, можна сформулювати висновок про те, що сетізація інформаційного і освітнього середовища забезпечує збільшення академічної мобільності, підвищуючи якість підготовки спеціалістів для державної служби у правоохоронній сфері.

-
1. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : Розпорядження Кабінету Міністрів України від 15.11.2017 р. № 1023-р. URL. <http://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80> (дата звернення 08.12.2018).

2. Про затвердження Положення про Державну міграцій службу України : Постанова Кабінету Міністрів України від 20.08.2014 № 360. URL. <http://zakon.rada.gov.ua/laws/show/360-2014-%D0%BF> (дата звернення 08.12.2018).
3. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 03.11.2015 р. № 1343. URL. (дата звернення 08.12.2018).
4. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво : Закон України від 12.07.2017 р. № 2129-VIII. Відомості Верховної Ради України. 2017. № 33. Ст. 361.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Савайда Олена Іванівна,

*доцент кафедри теорії та історії держави і права,
конституційного та міжнародного права
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Розглядаючи питання теоретико – методологічних аспектів застосування інформаційних технологій в житті людини не можливо обійти й такі сферу людської діяльності як сферу освіти, відповідно не освоївши яку, людина не здобуде необхідних професійних навиків та знань, що будуть їй потрібні в практичному професійному житті. А при сучасному стані та розвитку суспільних відносин, технічно-наукової революції та швидкісного й плинного життя людини забезпечення її освітнього рівня на базі навчальних закладів держави є нагальною та вкрай важливою сферою для її життєдіяльності та для саморозвитку й самоосвіти.

Безперечно, що сфера освіти в першу чергу повинна володіти тими сучасними та прогресивними методами, засобами та інноваційними технологіями, які не лише покращують якість самого процесу навчання (що важливо та актуально для науково-педагогічного складу будь-якого навчального закладу), а й вдосконалюють сам навчальний матеріал, що розширює горизонти для більш широкого засвоєння освітніх програм тих, хто навчається.

Наша зацікавленість даної тематики, в першу чергу, буде стосуватися саме тих теоретико-методологічних засад інформаційних технологій, які будуть вдосконалювати якість подання та викладу навчального матеріалу, а також можуть впливати на достовірність та істинність інформації (що так важливо в контексті сучасних подій в нашій державі, проти якої використовують «чорні» інформаційні та телекомунікаційні технології), яка надається навчачому під час навчання.

З цієї причини стає актуальною розробка певних методичних підходів до використання засобів нових інформаційних технологій для реалізації ідей розвиваючого навчання, розвитку особистості людини.

Зокрема, для розвитку творчого потенціалу індивіда, формування в нього вміння здійснювати прогнозування результатів своєї діяльності, розробляти стратегію пошуку шляхів і методів вирішення завдань – як навчальних, так і практичних. Метод (грец. Methodos – спосіб пізнання) – сукупність правил дії (наприклад, набір і послідовність певних операцій), спосіб, знаряддя, які сприяють розв'язанню теоретичних чи практичних проблем [1, с.35].

Зараз, вже не можливе засвоєння матеріалу та здобуття відповідей на широке коло питань без засобів зв'язку, теле – та інтернет комунікацій, без цифрової інформації. Проте ключовим під час такого використання та засвоєння лишається питання методів, якими ця інформація формується, добувається та зреалізовується в житті людини й держави також.

Методологічними засадами та основами під час використання та застосування інформаційних технологій можуть виступати й певні положення теорій філософії, філософії права та природного права.

Сучасний світ, як відомо не можливо вже уявити без інформаційних технологій, які намагаються охоплювати все більше й більше сфер життя людини. Проте використання сучасних технологій (особливо в науковій, освітній сферах) містить як позитивні елементи, так і негативні.

Візуалізація. Це один із основних методів осягнення інформації, її фіксуванні та явної наочності. Проте, в більшості випадків візуалізація носить миттєвий характер освоєння дійсності, різних навчальних матеріалів, життя в цілому. Цей метод може сприяти для розвитку тих особистостей, які в першу чергу мають добре розвинену наочну пам'ять та швидко усвідомлюють значення даного матеріалу чи інформації й не потребують подальшого нагадування чи повторення. В більшості людей зазначений метод працює ефективно.

Діалектика. Це один з методів філософії, згідно з яким будь-яке явище перебуває у процесі зміни, розвитку, в основі якого – взаємодія (боротьба) протилежностей. Він найпоширеніший серед філософських методів. Термін походить від давньогрецького *dialektike* – мистецтво вести бесіду, полеміку, діалог[2, с.115]. Так от, інформаційні технології якраз в навчальному процесі чи правоохоронному житті суспільства дають можливість швидко, оперативно реагувати на сучасні потреби та виклики часу.

Постійна зміна та оновлення сучасного українського законодавства це вимога інформаційної сучасності, вдосконалення та реформування певних систем держави це потреба сучасності за допомогою інформаційних технологій в першу чергу (електронна реєстрація, ведення платежів за допомогою технологічних розробок, доступ до освітніх програм на відстані, в різних країнах та на різних континентах тощо). Якісна освіта та медицина вже не може обійтися без сучасних розробок інформаційних технологій, що покращує та ефективно впливає на розвиток суспільства, держави та людини.

Реалізація людини своїх освітніх потреб за допомогою інформаційних технологій, а в подальшому використання цих же засобів, навичок та вмінь на основі інформаційних технологій в професійній діяльності дає колосальний поштовх до особистісного розвитку та зростанню професіоналізму.

-
1. Л. Нагорна. Метод // Політична енциклопедія. Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. – К.: Парламентське видавництво, 2011. – с.443
 2. Діалектика : навчальний посібник / Василь Лисий. – Львів : ЛНУ імені Івана Франка, 2014. – 480 с.
 3. Тихонов О.М. Інформаційні технології та телекомунікації в освіті і науці (IT & T ES'2007): Матеріали міжнародної наукової конференції, ФДМ ДНДІ ІТТ «Інформіка». – М.: ЕГРІ, 2007. – 222 с.
 4. Зайцева С. А. Иванов В. В. «Інформаційні технології в освіті» <http://sgpu2004.narod.ru/infotek/infotek2.htm>

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ДИСТАНЦІЙНОГО НАВЧАННЯ В ОСВІТНІЙ ПРОЦЕС

Сватюк Оксана Робертівна,

*доцент кафедри менеджменту
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент*

Миронов Юрій Богданович,

*доцент кафедри туризму та готельно-ресторанної справи
Львівського торговельно-економічного університету
кандидат економічних наук, доцент*

Миронова Мар'яна Ігорівна,

*вчитель економіки середньої загальноосвітньої школи № 90
м.Львова, кандидат економічних наук*

У зв'язку з динамічним розвитком інформаційних технологій за останні десятиліття особливого значення та актуальності набувають можливості використання дистанційної форми навчання у роботі закладів вищої освіти. Оскільки професійні знання втрачають свою актуальність дуже швидко, необхідне їх постійне вдосконалення. За сучасних умов саме дистанційна форма навчання дає можливість створення систем загального обміну інформацією, масового постійного самонавчання.

Впроваджуючи дистанційні технології в освітній процес, адміністрація закладу вищої освіти неодмінно стикається з вибором стратегії його впровадження. Отож, навчальному закладу необхідно вирішити такі стратегічні завдання в управлінні:

- 1) заклад вищої освіти повинен продумати організацію управління системою дистанційної освіти, щоб ефективно використовувати сучасні інформаційні технології відповідно до потреб будь-яких навчальних програм;
- 2) заклад вищої освіти повинен визначитися з адміністративними, навчальними, технічними цілями і перспективами розвитку дистанційного навчання;

3) заклад вищої освіти повинен розробити свою модель взаємодії з іншими установами. Обрана модель повинна відображати потенційні відносини зі школами, коледжами, іншими університетами, з бізнесом, промисловістю тощо

Наступне, з чим стикається адміністрація закладу вищої освіти при введенні нових дистанційно-освітніх технологій – це вибір моделі дистанційного навчання.

У таблиці 1 подається характеристика трьох найпоширеніших моделей дистанційного навчання.

Розроблено авторами на основі [1; 2].

На нашу думку, прийняття рішення про вибір тієї чи іншої моделі повинно здійснюватися на аналітичному етапі управління впровадженням дистанційно-освітніх технологій. Проте слід відзначити, що ці моделі не можуть відображати всіх можливих підходів до дистанційної освіти.

Таблиця 1. Моделі дистанційного навчання

	Особливості застосування	Характеристика
Модель розподіленого класу	Застосовується у тих випадках, коли дистанційні курси розраховані в основному на студентів, які перебувають у різних місцях. Типовим для цієї моделі є змішаний клас, який об'єднує «звичайних» і «дистанційних» студентів. Навчальний заклад і деканат контролюють їх успішність. Це найефективніша, але і найскладніша для студентів, трудомістка для викладачів і дорога для закладу освіти модель.	- заняття включають в себе синхронні комунікації; студенти і викладачі повинні перебувати в певному місці у визначений розкладом час; - кількість учасників коливається від одного до п'яти і більше; чим більшою є кількість учасників, тим вища технічна складність організації дистанційної роботи; - у процесі навчання упускається міміка, інша важлива невербальна інформація.

Модель самостійного навчання	<p>Студенти забезпечуються набором матеріалів, що включає виклад курсу і детальну програму, й отримують можливість звертатися до викладача, який здійснює керівництво, відповідає на питання й оцінює роботу. Контакт між студентом і викладачем досягається за допомогою електронної пошти, Skype, Viber, телефону. Ця модель є найпростішою як для студентів, так і для викладачів; економічною, оскільки зводить до мінімуму контакти з викладачем. Однак при цьому страждає ефективність контролю знань.</p>	<ul style="list-style-type: none"> - немає необхідності перебувати в певному місці у певний час; - не проводяться заняття в аудиторії, студенти навчаються самостійно, слідуючи докладним інструкціям програми; - студенти взаємодіють дистанційно з викладачем (та майже не взаємодіють з іншими студентами); - представлення змісту курсу відбувається через веб-сторінки або відеозаписи, які студенти можуть вивчати у зручний для себе час; - матеріали курсу зазвичай використовуються упродовж тривалого часу, який може досягати декількох років.
Модель відкритого навчання + клас	<p>Включає в себе використання друкованого викладу курсу та відеозаписів, які дозволяють вивчати курс самостійно у поєднанні з інтерактивними телекомунікаційними технологіями для організації спілкування студентів всередині «дистанційної групи». Ця модель дозволяє поєднувати переваги двох попередніх при значній економії витрат. Тому вона оптимально підходить для освоєння закладом освіти інноваційних дистанційних технологій навчання.</p>	<ul style="list-style-type: none"> - представлення змісту курсу відбувається через веб-сторінки або відеозаписи, які студенти можуть вивчати в будь-який зручний час індивідуально або в групі; - студенти періодично збираються разом для проведення занять за участю викладача. При цьому використовуються інтерактивні технології (як у моделі розподіленого класу); - аудиторні заняття проводяться для того, щоб студенти могли обговорити і уточнити основні поняття, отримати навички вирішення завдань, групової роботи, для виконання лабораторних робіт, моделювання та інших прикладних досліджень.

Надзвичайно важливою є також проблема вибору платформи, на якій буде працювати система дистанційної освіти, тому при виборі конкретної системи варто врахувати критерії функціональності, зручності користування, можливості для перевірки

знань, стабільності, локалізації, наявності техпідтримки, вартості та ін. Критерії та особливості вибору платформи для системи дистанційної освіти розглядалися нами у праці [3, с. 289].

Створення інформаційно-освітнього середовища вузу, а також розвиток внутрішніх засобів телекомунікацій є вкрай важливим кроком в розробці управлінських питань.

Пріоритетними напрямками в процесі створення інформаційного середовища закладу вищої освіти для реалізації дистанційного навчання є:

- розробка та затвердження навчально-методичного матеріалу для навчання адміністративного і допоміжного персоналу системи дистанційної освіти;
- розробка і впровадження сучасної технологічної бази для створення навчальних дистанційних курсів;
- визначення оцінки якості програмних засобів та системи дистанційної освіти загалом.

Для реалізації даних напрямів необхідно:

- формувати творчі колективи розробників дистанційних курсів, куди необхідно включати програмістів, методистів, викладачів;
- розробляти електронні курси лекцій, відеолекції, інтерактивні навчальні посібники та інші навчально-методичні матеріали в електронному вигляді;
- використовувати сучасні інтерактивні технології для ефективної комунікації учасників системи дистанційного навчання (студентів, викладачів, методистів).

Таким чином, дистанційні технології є ефективним засобом організації навчального процесу за сучасних умов та перспективною формою підготовки майбутніх фахівців до професійної діяльності, проте вимагають високопрофесійного підходу до прийняття рішень про вибір моделі навчання, системи дистанційної освіти, а також фахового управління процесом впровадження дистанційного навчання в освітній процес.

1. Бордияну И. В. Совершенствование организации и управления дистанционным обучением в системе высшего образования Республики Казахстан : дисс. на соискание ученой степени доктора философии / И. В. Бордияну. – Алматы, 2011. – 144 с.
2. Корнеев И. К. Информационные технологии в управлении : учебное пособие / И. К. Корнеев, Т. А. Година. – М. : Финстатинформ, 2000. – 201 с.
3. Сватюк О. Р. Критерії та особливості вибору системи дистанційної освіти / О. Р. Сватюк, Ю. Б. Миронов, М. І. Миронова // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : матеріали Всеукр. наук.-практ. конф. (м. Львів, 23 грудня 2016 р.). – Львів : ЛьвДУВС, 2017. – 313 с. – С. 285-290.

ДО ПИТАННЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ОБРОБКИ СТАТИСТИЧНИХ ТА АНАЛІТИЧНИХ ДАНИХ

Сеник Володимир Васильович,

*завідувач кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Магеровська Тетяна Валеріївна,

*доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Карагодіна Юлія Юріївна,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

В умовах реформування Національної поліції, суттєвого підвищення вимог до професійної майстерності її персоналу, постійного загострення криміногенної ситуації в Україні під час військового стану, науково-педагогічні кадри вищих освітніх закладів із специфічними умовами навчання (в тому числі системи МВС України) потребують проведення вдосконалення існуючих та розроблення нових форм і методів теоретичного та практичного навчання здобувачів вищої освіти, з врахуванням застосування сучасних досягнень в галузі інформаційних технологій. Їх стрімкий розвиток, зокрема, призвів до потреби вдосконалення аналітичного забезпечення діяльності практично кожного з підрозділів Національної поліції, створення нових структурних підрозділів інформаційно-аналітичного забезпечення, таких як підрозділи інформаційної підтримки, аналітичного забезпечення та оперативного реагування, кримінального аналізу тощо. Для забезпечення їх діяльності виникає необхідність не лише проведення вдосконалення існуючих та розроблення нових форм і методів теоретичного та практичного навчання майбутнього персоналу, а й впровадження у навчальний процес нових дисциплін, спекурсів та тем.

Упродовж 2017-2018 років кафедрою інформатики Львівського державного університету внутрішніх справ активно здійснювались різноманітні заходи у даному напрямі діяльності. Зокрема, у дисципліну «Інформаційне забезпечення професійної діяльності» введено тему «Комп'ютерні технології обробки статистичних та аналітичних даних», а також розроблено відповідне навчально-методичне забезпечення даної теми.

Така необхідність внаслідок того, у що правоохоронній діяльності існує певний клас задач, пов'язаних з аналізом інформаційних потоків як оперативного так і адміністративного (управлінського) характеру. Наприклад, робота конкретних підрозділів якісно оцінюється системою численних показників (кількістю розглянутих справ, прийнятих заяв, виявлених правопорушень тощо). Аналіз таких показників на сьогоднішній день не можливо уявити без застосування комп'ютерної техніки та використання різноманітних пакетів для опрацювання статистичних та аналітичних даних. У зв'язку із тим, що освітні заклади із специфічними умовами навчання достатньо часто не мають можливості закуповувати коштовне спеціалізоване програмне забезпечення, для проведення занять, пов'язаних із обробкою статистичних та аналітичних даних за основу прийнято програмне забезпечення фірми Microsoft р офісного пакету – це Excel. Під час вибору даного програмного забезпечення також враховувалося, що здобувачі вищої освіти, як правило, вже мають його інсталюване на персональних домашніх комп'ютерах та ноутбуках, що у подальшому дасть їм змогу проводити самовдосконалення з даної теми. Також враховувалось Microsoft Excel має ряд зручних переваг під час практичного застосування. Наприклад: введення даних у таблиці (числові дані, текстові дані, послідовності дат, днів тижня, місяців тощо); обчислення в таблицях; візуалізація інформації (графіки та діаграми); аналіз даних (підведення підсумків, створення зведених таблиць тощо); створення баз даних із засобами автоматизації пошуку, впорядкування та фільтрації.

Для забезпечення якісного проведення занять з вказаної теми, надання можливості самовдосконалення здобувачів вищої освіти кафедрою розроблені методичні рекомендації «Комп'ютерні технології обробки статистичних та аналітичних даних» [1]. Дані

рекомендації складаються з чотирьох розділів: 1. Структура електронної таблиці. Типи даних. Набір, редагування та форматування даних; 2. Формули та функції в електронних таблицях. Захист даних; 3. Робота з базами даних; 4. Аналіз даних; 5. Організація графічної інформації. До кожного з розділів, окрім теоретичного матеріалу, представлено практичні вправи для закріплення знань. Перед використанням у навчальному процесі дані методичні матеріали апробувалися членами наукового гуртка кафедри інформатики, де отримали схвалення здобувачами вищої освіти. Окрім цього, дані методичні рекомендації можуть використовуватися практичними працівниками під час підвищення кваліфікації чи виконанні практичних завдань.

Загалом вважаємо, що використання даної розробки кафедри інформатики сприятиме у подальшому формуванню фахівця для потреб Національної поліції з новим рівнем якості знань та практичних навичок. Окрім цього, здобувачі вищої освіти матимуть можливість отримати і інші міждисциплінарні знання та уміння, що ґрунтуються на комплексному підході до навчання.

-
1. Сенік В.В., Магеровська Т.В. Комп'ютерні технології обробки статистичних та аналітичних даних: методичні рекомендації для вивчення навчальної дисципліни «Інформаційні технології в правозастосовчій діяльності» та практиків, що здійснюють аналітичну діяльність у сфері кримінального аналізу / В. В. Сенік, Т. В. Магеровська – Львів: ЛьвДУВС, 2017. – 92 с.

Розділ 3.

СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АКТУАЛЬНІ
СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ
ДІЯЛЬНОСТІ

АКТУАЛЬНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНОГО РЕАГУВАННЯ ПОЛІЦІЇ НА ПОВІДОМЛЕННЯ ПРО ЗЛОЧИНИ ТА ІНШІ ПОДІЇ

Біденчук Тетяна Миколаївна,

здобувач ступеня бакалавра

Дніпропетровського державного університету внутрішніх справ

Кононець Віта Петрівна,

*доцент кафедри адміністративного права, процесу та
адміністративної діяльності*

*Дніпропетровського державного університету внутрішніх справ,
кандидат юридичних наук*

Ефективне виконання головних завдань, які покладені на Національну поліцію щодо боротьби із злочинністю, забезпечення конституційних прав громадян та громадського порядку неможливо без належної організації та ефективного виконання ряду внутрішньо-організаційних функцій (матеріально, кадрового, медичного, фінансового, документального, інформаційно-аналітичного) забезпечення. Для дотримання прав та свобод людини, які прописані в Конституції України, а також для виконання усіх інших вищезазначених завдань Національної поліції, в Україні створюються спеціальні підрозділи [1].

На території обслуговування Національної поліції працюють підрозділи ОАЗОР. Саме вони реалізують зазначений адміністративно-правовий засіб забезпечення обігу інформації з метою подальшої оцінки й аналізу такої інформації в межах закріплених функцій [2]. Безпосередньо функція реагування на повідомлення про злочини закріплена на регіональному рівні за управліннями ОАЗОР, які повинні проводити збір, оцінку, аналіз інформації про криміногенну ситуацію на території обслуговування, кримінальні правопорушення, порушення публічної безпеки й порядку, інші надзвичайні події та заходи реагування, що вживаються підрозділами головних управлінь для усунення недоліків. Звичайно, реалізація цього адміністративно-правового засобу забезпечення обігу інформації в органах Національної поліції підрозділами

ОАЗОР нерозривно пов'язана з їх взаємодією із черговими частинами. Належну увагу слід приділити черговим частинам, які безпосередньо отримують повідомлення про вчинені злочини. При цьому начальник чергової частини повинен безпосередньо забезпечувати щоденний збір оперативної інформації. У свою чергу за управліннями ОАЗОР закріплена функція організації діяльності чергових частин ГУ (на території обслуговування) [7]. У зв'язку із цим необхідно зазначити, що Наказ МВС України № 181, який базується ще на Законі України «Про міліцію», потребує коригування.

Департамент ОАЗОР готує оперативні зведення та інформаційні документи про кримінальні правопорушення й події, у встановленому порядку здійснює обмін такою інформацією з іншими правоохоронними органами; готує комплексні аналітичні матеріали про стан оперативної обстановки в державі, проекти управлінських рішень щодо підвищення ефективності діяльності поліції з протидії злочинності та зміцнення правопорядку.

Джерелом інформації про вчинені кримінальні правопорушення та інші події є: повідомлення осіб, які надходять до органу поліції або особи, уповноваженої здійснювати досудове розслідування (слідчий); самостійно виявлені слідчим або іншою посадовою особою органу поліції з будь-якого джерела обставини кримінальних правопорушень; повідомлення осіб, які затримали підозрювану особу на місці вчинення кримінального правопорушення. Для роз'яснення населенню порядку прийняття, реєстрації заяв і повідомлень про вчинені кримінальні правопорушення та інші події в органах поліції в спеціальних кімнатах для прийому громадян або у вестибюлях повинна бути вивішена пам'ятка щодо ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події [4]. У ній зазначаються номери телефонів (місцезнаходження) керівників центрального органу управління поліцією, головних управлінь Національної поліції в Автономній Республіці Крим та м. Севастополі, областях та м. Києві, на яких покладено контроль за додержанням законності при прийнятті та реєстрації заяв і повідомлень про вчинені кримінальні правопорушення та інші події, а також органів прокуратури, що здійснюють нагляд [3].

Прийняття заяв і повідомлень про вчинені кримінальні правопорушення та інші події незалежно від місця і часу їх учинення, повноти отриманих даних, особи заявника здійснюється цілодобово і невідкладно тим органом поліції, до якого надійшла заява чи повідомлення про вчинене кримінальне правопорушення та іншу подію, або слідчим, або іншою посадовою особою органу поліції, якою самостійно виявлено з будь-якого джерела обставини, що можуть свідчити про вчинення кримінального правопорушення [6].

Облік таких заяв та повідомлень проводиться уповноваженими працівниками чергових частин органів поліції, працівниками інших структурних підрозділів цих органів, яких призначено підмінними черговими в установленому порядку, оператором телефонної лінії «102» або іншою посадовою особою.

При особистому зверненні заявника до органу поліції із заявою чи повідомленням про вчинене кримінальне правопорушення та іншу подію уповноважений працівник чергової частини або інша службова особа в кімнаті для приймання громадян цілодобово оформляють протоколи усних заяв і відразу реєструють заяви в журналі єдиного обліку заяв і повідомлень про вчинені кримінальні правопорушення та інші події [4].

Повідомлення про кримінальні правопорушення та інші події, отримані оператором телефонної лінії «102», вносяться до робочого зошита, в якому зазначаються відомості про дату та час надходження повідомлення, хто повідомив (П.І.Б., місце проживання/місцезнаходження, телефон), стислий зміст заяви. Уся отримана інформація про кримінальні правопорушення та інші події після її внесення до робочого зошита відразу передається до органів поліції для реагування, про що робиться відмітка в робочому зошиті (кому передано повідомлення, номер реєстрації в журналі ЄО органу поліції). Уповноважений працівник чергової частини органу поліції, отримавши заяву (повідомлення) про вчинене кримінальне правопорушення та іншу подію, відразу реєструє її (його) в журналі ЄО та направляє на місце події слідчо-оперативну групу чи групу реагування. Інформацію, яка надійшла до чергової частини органу поліції, про вчинене кримінальне

правопорушення та іншу подію на території обслуговування іншого органу поліції уповноважений працівник чергової частини відразу реєструє в журналі ЄО та невідкладно інформує про це той орган, на території оперативного обслуговування якого мала місце така подія [6].

Матеріали з ознаками вчинення кримінального правопорушення заборонено передавати до іншого органу поліції без реєстрації в журналі ЄО та внесення відомостей до Єдиного реєстру досудових розслідувань.

Посадова особа органу поліції при виявленні чи отриманні інформації про вчинене кримінальне правопорушення та іншу подію негайно повідомляє про це чергову частину органу поліції. Заяви або повідомлення фізичних або юридичних осіб про вчинене кримінальне правопорушення та іншу подію можуть бути усними або письмовими. Усні заяви про вчинення кримінального правопорушення заносяться до протоколу прийняття заяви про вчинене кримінальне правопорушення [5].

Заяви і повідомлення про вчинені кримінальні правопорушення та інші події реєструються цілодобово в чергових частинах органів поліції уповноваженими працівниками відразу після їх надходження, вносяться до журналу ЄО та інтегрованої інформаційно-пошукової системи з усіма відомостями з журналу ЄО.

У черговій частині органів поліції ведеться журнал ЄО, який забороняється виносити з чергової частини. Журнали ЄО заповнюються уповноваженими працівниками чергових частин органів поліції. Записи за кожною інформацією повинні містити стислі і вичерпні дані про те, коли надійшла заява чи повідомлення про вчинені кримінальні правопорушення та інші події, хто, коли і в якій формі повідомив про вчинене кримінальне правопорушення та іншу подію, що і коли сталося, час та дату реєстрації, яких заходів ужито за заявою чи повідомленням про вчинені кримінальні правопорушення та інші події, ким та кому доручено розгляд заяви чи повідомлення про вчинені кримінальні правопорушення та інші події, час та дату отримання заяви чи повідомлення про вчинені кримінальні правопорушення та інші події для внесення відповідних даних до Єдиного реєстру досудових

розслідувань. Закінчені журнали ЄО та журнали видачі талонів разом з талонами-корінцями передаються до підрозділів документального забезпечення органів поліції [8].

Про наявність письмових заяв про вчинені кримінальні правопорушення та інші події, що надійшли до чергової частини органу поліції, та повідомлень, що надійшли усно, у яких наявні відомості, що вказують на вчинення кримінального правопорушення, після реєстрації в журналі ЄО уповноважений працівник чергової частини доповідає начальникові слідчого підрозділу для внесення слідчими відповідних відомостей до Єдиного реєстру досудових розслідувань та інформує начальника органу поліції.

Про заяви і повідомлення, які надійшли до чергової частини органу поліції і в яких відсутні відомості, які вказують на вчинення кримінального правопорушення, після їх реєстрації в журналі ЄО доповідається уповноваженим працівником чергової частини начальникові органу поліції або особі, яка виконує його обов'язки, для розгляду та прийняття рішення згідно із Законом України «Про звернення громадян» або Кодексом України про адміністративні правопорушення.

У разі встановлення начальником органу поліції в заяві (повідомленні) відомостей, які вказують на вчинення кримінального правопорушення, він за своєю резолюцією (не пізніше однієї доби з часу реєстрації заяви в журналі ЄО) повертає її (його) до чергової частини для негайної передачі начальнику слідчого підрозділу [3].

У разі якщо письмова заява, повідомлення про вчинені кримінальні правопорушення надійшли до відділу, відділення поліції при особистому зверненні заявника, водночас з його реєстрацією в журналі ЄО в черговій частині відділу, відділення поліції уповноважений працівник чергової частини оформляє талон-повідомлення [7].

Заяви і повідомлення про вчинені кримінальні правопорушення та інші події, що надійшли до органу поліції поштою, телеграфом, факсимільним зв'язком або зв'язком іншого виду, реєструються в підрозділах документального забезпечення цих органів, про них

доповідається начальникові органу поліції або особі, яка виконує його обов'язки. Останні, у свою чергу, накладають письмові резолюції щодо подальшого розгляду заяв і повідомлень про вчинені кримінальні правопорушення та інші події з ознаками кримінальних правопорушень у порядку.

Про заяви та повідомлення про вчинені кримінальні правопорушення та інші події, що надійшли до центрального органу управління поліцією та головних управлінь Національної поліції, в яких зазначаються обставини, що вказують на вчинення кримінального правопорушення, після їх реєстрації в журналі вхідної кореспонденції працівниками підрозділів документального забезпечення негайно доповідається керівництву цих органів, після чого за резолюцією вони передаються до органів поліції нижчого рівня, а копії – до уповноваженого структурного підрозділу відповідного органу поліції.

Структурні підрозділи центрального органу управління поліцією або головних управлінь Національної поліції зобов'язані поінформувати заявника про направлення такої заяви або повідомлення до органів поліції нижчого рівня, а також забезпечити контроль за внесенням відомостей до журналу ЄО у відповідному органі поліції [2].

У журналі ЄО чергових частин центрального органу управління поліцією або головних управлінь Національної поліції реєструються заяви та повідомлення про вчинені кримінальні правопорушення та інші події, досудове розслідування за якими здійснюється слідчими підрозділами цих органів [3].

Таким чином, під адміністративно-правовим засобами забезпечення обігу інформації необхідно розуміти сукупність адміністративно-правових норм, які розглядаються з позиції їх функціонального призначення щодо збирання, зберігання, використання й поширення інформації в органах Національної поліції. До адміністративно-правових способів забезпечення обігу інформації необхідно віднести такі: 1) збір інформації про криміногенну ситуацію на території обслуговування Національної поліції; 2) підготовку інформаційних документів; 3) обмін інформацією з

правоохоронними органами та іншими органами державної влади; 4) інформування керівництва про стан виконання підрозділами Національної поліції покладених на них завдань; 5) формування та ведення інформаційних ресурсів; 6) оповіщення населення про виникнення надзвичайних ситуацій. Незважаючи на те, що було прийнято низку нормативно-правових актів, спрямованих на узгодження діяльності у сфері обігу інформації з новим законодавством про Національну поліцію України, значна частина нормативно-правової бази в цій сфері потребує суттєвого оновлення [4].

На сьогоднішній день, Україна розвивається далі і вже слідчі та оперативні підрозділи Національної поліції створюють і використовують локальні автоматизовані інформаційні системи, але у повній мірі забезпечення потреб запобігання та розслідування кримінальних правопорушень в інформаційних ресурсах покладається на Інтегровану інформаційно-пошукову систему органів внутрішніх справ України. У процесі створення та введення в експлуатацію Інтегрованої інформаційно-пошукової системи штабні підрозділи виконують наступні функції: дослідження інформаційного простору окремого міськ-, рай-, ліноргану; визначення переліку інформаційних відомостей; рівня оброблення та зберігання інформації відповідно до категорій обліку; контроль стану формування інформаційних підсистем [8]. Інтегрованої інформаційно-пошукової системи; забезпечення авторизації користувачів інформаційної підсистеми «Факт»; аналітичне забезпечення розробки та затвердження нормативно-правових актів з організації функціонування Інтегрованої інформаційно-пошукової системи; створення та забезпечення функціонування науково-технічної ради з проблем інформатизації; запровадження новітніх технологій в організацію діяльності чергових частин ОВС, контроль за своєчасністю та якістю введення черговими частинами відомостей до Інтегрованої інформаційно-пошукової системи; вимірювання за ранговою шкалою, визначення рейтингів інформаційної діяльності оперативних та слідчих підрозділів, оцінка результатів їх діяльності.

1. Конституція України // Відомості Верховної Ради України від 23.07.1996 – 1996 р., № 30. – Ст. 141.
2. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII: [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua.http://zakon4.rada.gov.ua/laws/show/580-19>.
3. Наказ від 06.11.2015 № 1377 «Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події»: [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/z1498-15>
4. Кримінально процесуальний кодекс України від 13 квітня 2012 року № 2341-III // Відомості Верховної Ради України - 2013. - № 25. - Ст. 131.
5. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (станом на 17.08.2014) // Відомості Верховної Ради УРСР. – 1984. – Кодекс України, Закон, Кодекс від 07.12.1984 № 8073-X поточна редакція – Редакція від 05.01.2017, підстава 1798-19.
6. Проблемы теории государства и права : [учеб. пособие] / под ред. М.Н. Марченко. – М. : Юрист, 2002. – 620 с. 9. Общество и сознание / пер. с нем. М.Б. Колдаевой ; общ. ред. и вступ. ст. А.К. Уледова. – М. : Прогресс, 1984. – 239 с. 154 3/2017 АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС
7. Бахрах Д.Н. Административная ответственность / Д.Н. Бахрах. – Пермь : Книжное изд-во, 1966. – 193 с.
8. Колпаков В.К. Адміністративне право України : [підручник] / В.К. Колпаков. – К. : Юрінком Ін- тер, 1999. – 736 с.

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ВАНТАЖОПЕРЕВЕЗЕНЬ НА ЗАЛІЗНИЦІ

Вишня Володимир Борисович,

*професор кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх
справ, доктор технічних наук, професор*

Гавриш Олег Степанович,

*викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ*

Вантажний залізничний транспорт будь-якої держави повинен забезпечувати нормальне функціонування промислового і сільськогосподарського виробництва, безперебійну і надійну доставку вантажів. Сьогодні на частку залізничного транспорту України припадає понад дві третини всього вантажообігу країни. Великі матеріальні цінності, що зосереджені на транспорті, вимагають надійної охорони їх від злочинних посягань.

У той же час, в оперативній обстановці, що склалася за останні роки на залізничному транспорті, відзначається тенденція збільшення злочинності, в тому числі і найбільш небезпечних злочинів – розкрадань вантажів. Причому на залізницях України найбільшому розкраданню піддаються вагони з вугіллям, металом і металопродуктом, ферромарганцем і нафтопродуктами.

Розкрадання вантажів на залізницях відносяться до найбільш небезпечних і складних видів злочинів, специфічною особливістю яких є те, що місце, де було скоєно розкрадання, і місце, де воно було виявлено, як правило, не збігаються, перебуваючи, один від одного, на значному відстані і навіть в сфері обслуговування різних управлінь внутрішніх справ на транспорті. Іншими словами, основною причиною недостатньої ефективності боротьби з розкраданням вантажів на залізницях, є відсутність доказової бази здійснення розкрадання на конкретній ділянці залізниці і часу його здійснення, оперативного контролю за вантажами на шляху від постачальника до одержувача.

Створена та функціонує в Укрзалізниці єдина база електронних перевізних документів (Єдина автоматизована інформаційна система Держмитслужби) що дає можливість розширення полігону використання обміну даними в межах організації співробітництва залізниць.

Однак, вона не усуває причин, які ускладнюють своєчасне виявлення та припинення розкрадань вантажів, а саме відсутність оперативного оповіщення підрозділів Національної поліції про факт скоєння розкрадання і відсутність об'єктивних даних про місце і час здійснення злочину.

Шляхи вирішення цієї проблеми нами бачаться в розробці автоматизованої системи технічного контролю та супроводу вантажів, що транспортуються. В рамках викладеної концепції пропонується обладнати на вузлових, стикових і великих залізничних станціях вагоконтрольні пункти, які б здійснювали зважування вагонів складу в русі, без розчеплення вагонів. Для реалізації функцій, які покладаються правоохоронними органами на вагоконтрольні пункти, їх необхідно об'єднати в єдину мережу контролю вантажоперевезень.

Тобто мережа повинна включати електронні вагоконтрольні пункти (ВКП), об'єднані між собою і обчислювальними центрами дороги засобами електронної пошти. З цієї мережі, в напрямку руху поїзда з вантажами, від одного ВКП до іншого повинна передаватися інформація супровідного листа на поїзд, а саме, порядковий номер розміщення вагона з високоліквідним вантажем в його складі, вага вантажу і вагона, станція відвантаження і призначення, номер вагона.

У разі розбіжності показань вагоконтрольного пристрою на ВКП і даних супровідних документів на вантаж фіксується факт недостачі вантажу в вагоні і відповідна інформація про це пересилається в лінійний підрозділ поліції. Тобто, маємо приклад оперативного реагування на факт скоєння злочину, яке дозволить по «свіжим» слідах більш ефективно його розкривати і розслідувати, приймати правильні управлінські та організаційні рішення.

Використання запропонованих вагоконтрольних пунктів на залізницях дозволить також локалізувати ділянку залізниці (між двома

ВКП), де було скоєно розкрадання, а графік руху поїзда – встановити час проходження кожної умовної точки на цій ділянці, що вагомо полегшить розслідування злочину. Слід враховувати, що чим більше ВКП буде використовуватися органами внутрішніх справ на залізницях країни, тим менш протяжним буде ділянка залізниці, на якій фіксується можливе розкрадання вантажів, і отже кращі можливості відкриваються для успішного пошуку злочинців.

На нижньому рівні інформаційної підтримки системи вирішуються питання програмного забезпечення для виділення в поїзді вагонів з конкретним вантажем, реалізації операції зважування вагонів, відділення тари вагонів, порівняння фактичної маси і прийняття конкретного рішення про стан вантажу, архівування та збереження результатів контролю. Для використання запропонованої системи авторами також розроблена карта розміщення ВКП і види маршрутів, які підлягають контролю.

ЕКСПЕРТНЕ ОЦІНЮВАННЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ ПЕЛЮСТКОВИХ ДІАГРАМ

Грицюк Юрій Іванович,

*професор кафедри програмного забезпечення
Національного університету «Львівська політехніка»,
доктор технічних наук, професор*

Далявський Владислав Сергійович,

*здобувач ступеня бакалавра
Національного університету «Львівська політехніка»*

Вступ. У галузі інформаційних технологій якість програмного забезпечення (ПЗ) є основною характеристикою його ефективного використання [5], позаяк вказує на ступінь його відповідності встановленим вимогам [2]. Зазвичай, під якістю ПЗ розуміють набір властивостей програмного продукту, що характеризують його здатність задовольнити встановлені або передбачувані потреби замовника, які він вказав у вигляді користувацьких вимог до ПЗ на початку його розроблення [1].

На сьогодні експертні технології – невід’ємна складова процесу прийняття управлінських рішень [5] як при розробленні ПЗ, при управлінні змінами вимог до нього та ризиками його реалізації, так і під час управління його якістю [4]. Прийняття рішень професійними експертами ґрунтується практично на достовірному поданні наявної ситуації, правильному розумінні суті проблеми і повноті характеристик її складових. Кожний експерт, який бере участь в процесі оцінювання якості ПЗ і від думки якого залежить остаточне рішення керівника проекту, повинен володіти необхідними знаннями у своїй предметній області, має мати певний досвід і навики роботи [3]. За їх відсутності такі експерти до участі в оцінюванні якості ПЗ не допускають. Низька їх кваліфікація може призвести до того, що надані експертами оцінки сприятимуть невиправним помилкам і значним втратам – фінансовим, матеріальним і часовим.

Подання оцінок експертів у вигляді пелюсткових діаграм. Під візуалізацією результатів експертного оцінювання якості ПЗ розумітимемо подання інформації у графічному вигляді для максимальної зручності її розуміння та швидкого сприйняття, а також надання осяжної та зрозумілої форми будь-якому об'єкту, процесу чи явищу. Проте, серед значної кількості теоретиків і практиків у галузі інформаційних технологій побутує думка, що таке розуміння візуалізації інформації сприяє мінімальній розумовій і пізнавальній активності аналітика, а візуальні інструментальні засоби виконують для нього тільки ілюстративну функцію. Спробуємо дещо спростувати такі, як на наш погляд, хибні думки і довести неабияку користь візуалізації інформації в галузі розроблення ПЗ та оцінювання його якості.

Для візуалізації результатів опитувань експертів за деякими критеріями оцінювання якості ПЗ [1] та отримання його комплексного показника спробуємо використати полярні діаграми. Зазвичай, під полярною діаграмою розуміють графічний спосіб відображення абстрактних даних у вигляді круга, поділеного на три і більше секторів відповідними векторами (змінними). Ці змінні відображають на осях полярної системи координат, що мають спільний початок. Початок відліку та кут нахилу векторів, зазвичай, у полярній діаграмі вказують, що є корисним як для кількісного, так і якісного відображення інформації. У різній науковій літературі [3] можна натрапити на такі назви полярної діаграми: павукоподібна діаграма, карта зоряного неба, зоряна діаграма, неправильний багатокутник і пелюсткова діаграма.

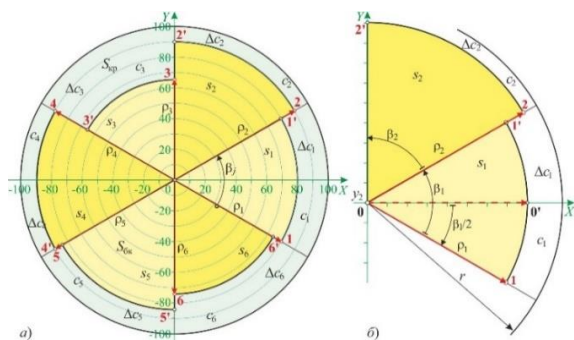


Рис. 1. Подання критеріїв оцінювання якості ПЗ у полярній системі координат

Критерії оцінювання якості ПЗ подамо у вигляді векторів (змінних) в полярній системі координат, які ділять круг на сектори, що загалом утворюють полярну діаграму (рис. 1,а). Кожний вектор має такі показники, як довжину і кут нахилу до попереднього вектора. Вважатимемо, що довжина вектора відповідає кількісному показнику якості ПЗ за відповідним критерієм. Як виняток, максимальна довжина будь-якого з векторів має відповідати стовідсотковій якості ПЗ за відповідним критерієм. Зазвичай, реальна довжина кожного з векторів становить тільки певну частину від його максимальної довжини, що відповідає реальній якості ПЗ за відповідним критерієм.

Автори у роботі [1] стверджують, що кут β між векторами утворює сектор, величина якого характеризує вплив відповідного критерію на загальний результат оцінювання якості ПЗ. Якщо всі критерії мають однаковий вплив на якість ПЗ, то вектори відповідних критеріїв будуть рівномірно розподілені по колу полярної системи координат. Наприклад, для шести критеріїв цей кут між усіма векторами становитиме $\beta = 2\pi/6$. У випадку неоднакового впливу критеріїв на якість ПЗ, то кути між відповідними векторами визначають за формулою

$$\tilde{B} = \left\{ \beta_j = 2\pi \cdot w_j / \sum_{i=1}^N w_i, j = \overline{1, N} \right\}, \quad (1)$$

де: $\tilde{W} = \{w_j, j = \overline{1, N}\}$ – ваговий коефіцієнт j-го критерію оцінювання якості ПЗ; N – кількість критеріїв оцінювання якості ПЗ.

Автори у роботі [1] стверджують, що кут β між векторами утворює сектор, величина якого характеризує вплив відповідного критерію на загальний результат оцінювання якості ПЗ. Якщо всі критерії мають однаковий вплив на якість ПЗ, то вектори відповідних критеріїв будуть рівномірно розподілені по колу полярної системи координат. Наприклад, для шести критеріїв цей кут між усіма векторами становитиме $\beta = 2\pi/6$. У випадку неоднакового впливу критеріїв на якість ПЗ, то кути між відповідними векторами визначають за формулою

$$\tilde{W} = \left\{ \beta_j = 2\pi \cdot w_j / \sum_{i=1}^N w_i, j = \overline{1, N} \right\}, \quad (1)$$

де: $\tilde{W} = \{w_j, j = \overline{1, N}\}$ – ваговий коефіцієнт j -го критерію оцінювання якості ПЗ; N – кількість критеріїв оцінювання якості ПЗ.

Якщо відкласти вектори-критерії (ρ_1, \dots, ρ_6) у полярній системі координат і через кожну точку їхніх вершин у кожному секторі провести дугу радіусом ρ_j , то матимемо так звану пелюсткову діаграму **1-1', 2-2', ..., 6-6'** (рис. 1,а), а отримана площа фігури ($S_{\text{пл}}$) кількісно характеризуватиме якість ПЗ за всіма критеріями одночасно. Площі секторних пелюстків (s_1, \dots, s_6), обмежені полярними секторами (c_1, \dots, c_6) з кутом β_j між векторами, будуть кількісно характеризувати якість ПЗ за відповідними критеріями його оцінювання.

Форма пелюсткової діаграми дає якісну характеристику ПЗ за усіма критеріями одночасно, а форма секторного пелюстка (наприклад, **0,1,1', 0,2,2'** і т.д.) – за відповідним критерієм. Якщо поділити площу пелюсткової діаграми ($S_{\text{пл}}$) на площу круга ($S_{\text{кр}}$), в якому вона знаходиться, то отримаємо частку якості ПЗ, яку маємо на даний момент за оцінками певного експерта. Незаповнена площа круга ($\Delta S_{\text{кр}} = S_{\text{кр}} - S_{\text{пл}}$) – та частина якості ПЗ, яку ще потрібно досягти для стовідсоткової її повноти. Якщо поділити площу секторного пелюстка (s_j) на площу сектора (c_j), в якому він знаходиться, то отримаємо частку якості ПЗ за j -им критерієм, яку маємо на даний момент за оцінками певного експерта. Незаповнена площа сектора круга ($\Delta c_j = s_j - c_j$) – та частина якості ПЗ, яку ще потрібно досягти за відповідним критерієм. Звернемо увагу на те, що радіус круга (r) має відповідати стовідсотковій якості ПЗ за кожним критерієм його оцінювання.

Наведений вище підхід до визначення комплексного показника якості ПЗ та її (якості) подальшого аналізу є правомірним за певних умов: 1) критеріїв-векторів потрібно не менше трьох; 2) початковий вектор-критерій **00'** (рис. 1,б) має знаходитися на додатній осі ординат полярної системи координат, зміщеній проти годинникової стрілки на кут $\beta_1/2$.

Для знаходження площ (s_1, \dots, s_6) секторних пелюстків (див. рис. 1,б) через кут (β_j) між його радіусами (ρ_j) використаємо таку формулу:

$$s_j = \pi \rho_j^2 \beta_j, j = \overline{1, n}. \quad (2)$$

Відповідно площі секторів круга (c_1, \dots, c_6), складовими яких є секторні пелюстки, через кут (β_j) між його радіусами (r) визначають за формулою

$$c_j = \pi r^2 \beta_j, j = \overline{1, n}. \quad (3)$$

Отже, формула (2) дає змогу розрахувати площі секторних пелюстків, за допомогою яких обчислюють й оцінюють якість ПЗ за відповідними критеріями. Також ці площі дають змогу визначити ту частину якості ПЗ за певним критерієм, яку маємо на даний момент за оцінками одного з експертів, а також ту частку якості ПЗ, яку ще потрібно досягти для стовідсоткової її повноти.

Як було зазначено роботі [3], довжини векторів у полярній системі координат мають відповідати пропорційно значенням відповідних критеріїв оцінювання якості ПЗ, які визначають через оцінки респондентів і ролі кожного з них [1]. Зазвичай, респонденти ПЗ є учасниками процесу оцінювання його якості, які можуть виступати в двох ролях – як відповідного експерта, так і безпосереднього користувача. Відмінність ролей у тому, що оцінка якості ПЗ, яку надає певний експерт, повинна мати більшу важливість в зазначеному процесі, ніж оцінка, яку надає користувач, позаяк їхня кваліфікація є різною. Для уникнення подальшої плутанини усіх респондентів будемо називати експертами. Кожному експерту надамо певні вагові коефіцієнти для кожного з критеріїв оцінювання якості ПЗ, значення яких вказуватимуть на їхню обізнаність у певній предметній області.

Отримання оцінок від експертів має проходити у вигляді їхнього опитування з використанням ранжованої шкали за кожним з критеріїв [3]. Експерти мають виставити відповідні оцінки, кожна з яких потім враховують через відповідні вагові коефіцієнти.

Зрозуміло, кожен з критеріїв буде по різному впливати на комплексний показник якості ПЗ, значення якого згодом визначають для кожного з експертів. Залежно від кваліфікації експерта кожний з них також матиме різні значення коефіцієнтів вагомості.

Алгоритм розрахунку площі пелюсткової діаграми. Комплексні показники якості ПЗ подамо у вигляді векторів полярної системи координат, які мають утворити пелюсткові діаграми для кожного експерта зокрема і узагальненого експерта загалом. Кожний такий вектор характеризується відповідно довжиною і кутом до попереднього вектора. Як було зазначено вище, довжина вектора у будь-якому випадку має відповідати кількісному значенню комплексного показника якості ПЗ за відповідним критерієм.

Звернемо увагу на те, що площа пелюсткової діаграми кількісно характеризує якість ПЗ за всіма критеріями одночасно, а форма діаграми дає якісну характеристику ПЗ. Для знаходження координат вершин пелюсткової діаграми 1-1',2-2',...,6-6' (див. рис. 1,а) використаємо такий алгоритм розрахунку.

У випадку неоднакового впливу критеріїв на якість ПЗ (див. формулу (1)) кути між відповідними векторами з врахуванням (4) визначають за такою формулою

$$\tilde{B}_k = \left\{ \beta_{i,k} = 2\pi \cdot w_{i,k} / \sum_{j=1}^M w_{j,k}, i = \overline{1, M} \right\}, k = \overline{1, K}, \quad (4)$$

а для середнього значення оцінок якості ПЗ (тобто, $k = K+1$) з врахуванням (5) ця формула матиме вигляд

$$\tilde{B}_k = \left\{ \beta_{i,k} = 2\pi \cdot w_i^c / \sum_{j=1}^M w_j^c, i = \overline{1, M} \right\}, k = K+1. \quad (5)$$

Оскільки полярний сектор з кутом β_j потрібно починати з вектора-критерію (див. формулу (1)), то перший вектор-критерій має знаходитися на осі ординат у полярній системі координат, але зміщеному проти годинникової стрілки на кут $\beta_1/2$. Тому початок відліку кута $\beta_{1,k}$ ($\forall k \in K+1$), який відповідає 1-му полярному сектору, почнемо зі значення кута $\alpha_{1,k} = -\beta_{1,k}/2$ ($\forall k \in K+1$), а всі інші кути обчислимо за такою формулою

$$\tilde{A}_k = \{ \alpha_{1,k} = -\beta_{1,k} / 2; \alpha_{i,k} = \alpha_{i-1,k} + \beta_{i,k}, i = \overline{2, M} \}, k \in K + 1. \quad (6)$$

Для побудови пелюсткової діаграми потрібно з кінців кожного вектора провести дуги на відповідний кут $\alpha_{i,k}$ ($\forall i \in M, \forall k \in K+1$). Маючи значення довжин векторів-критеріїв, а також кути між ними, отримані за формулою (6), можна побудувати пелюсткові діаграми для будь-якого з експертів зокрема, в т.ч. і для узагальненого $(K+1)$ -го експерта загалом (рис. 2).

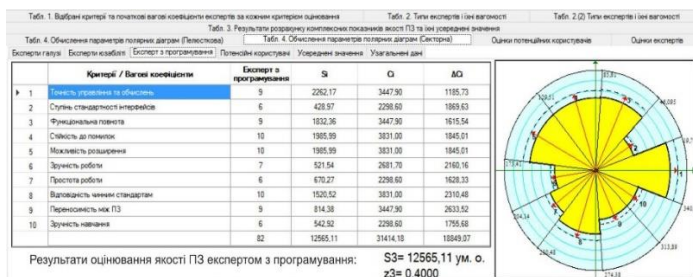


Рис. 2. Подання результатів оцінювання якості ПЗ у вигляді пелюсткових діаграм для відповідних експертів

Форма пелюсткової діаграми, побудованої за вершинами векторів-критеріїв, для будь-якого експерта дає якісну характеристику ПЗ за вибраними критеріями його оцінювання. Водночас, отримана площа пелюстка буде кількісно характеризувати якість ПЗ одночасно за всіма критеріями. Для знаходження площі пелюсткової діаграми за координатами вершин її векторів-критеріїв можна використати таку формулу

$$S_k^{пд} = \pi \sum_{i=1}^M g_{i,k}^2 \cdot \beta_{i,k}, k \in K + 1. \quad (7)$$

Для встановлення частки наявної якості ПЗ, яку маємо на даний момент за оцінками певного експерта, потрібно поділити площу пелюсткової діаграми на площу круга, в якому вона знаходиться, а саме

$$z_k = \frac{S_k^{пд}}{\pi r^2}, k \in K + 1, \quad (8)$$

де: z_k – частка наявної якості ПЗ, яку встановлено за даними k -го експерта; r – радіус круга. Як було зазначено вище, комплексний

показник якості ПЗ ($g_{i,k}$) матиме максимальне значення 100, тобто радіус круга становитиме 100 од. Незаповнена ж площа круга – та частка якості ПЗ, яку ще потрібно досягнути для стовідсоткової її повноти.

Висновки. Розроблено методику візуалізації інформації, яку отримують внаслідок оброблення експертних оцінок якості програмного забезпечення (ПЗ) за різними критеріями його оцінювання з використанням пелюсткових діаграм. Розроблено алгоритм розрахунку площ секторних пелюстків у полярній системі координат, за допомогою яких можна обчислити і оцінити відносну якість ПЗ за відповідними критеріями. Визначено підсумкові комплексні показники якості ПЗ для кожного з експертів і узагальнений комплексний показник його якості.

-
1. Боцула, М. П., & Моргун, І. А. (2011). Метод отримання комплексної оцінки якості веб-матеріалів з використанням полярної системи координат // Вісник Вінницького політехнічного інституту, 1, 84–88. Режим доступу: [https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/1367/confere nces.vntu.edu.ua](https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/1367/confere%20nces.vntu.edu.ua).
 2. Грицюк, Ю. І., & Бучковська, А. Ю. (2017). Візуалізація результатів експертного оцінювання якості програмного забезпечення з використанням полярних діаграм. Науковий вісник НЛТУ України, 27(10), 137–145. Львів: РВВ НЛТУ України. <https://doi.org/10.15421/40271025>.
 3. Грицюк Ю. І., Далявський, В. С. (2018). Використання пелюсткових діаграм для візуалізації результатів експертного оцінювання якості програмного забезпечення. Науковий вісник НЛТУ України. Серія економічна, 28(9), 95–104. <https://doi.org/10.15421/40280919>
 4. Моргун, І. А. (2011). Метод експертної оцінки якості програмного забезпечення // Інженерія програмного забезпечення: матер. Міжнар. наук.-практ. конф. аспірантів і студентів, 2(6), 33–37. Вінниця. – Режим доступу до журналу: <http://jrn1.nau.edu.ua/index.php/IPZ/article/view/3086>.
 5. ISO/IEC 9126. (1991). Information technology – Software product evaluation – Quality characteristics and guidelines for their use. Geneva: International Organization for Standardization, International Electrotechnical Commission, 136 p. – (International Standard).

КРИМІНАЛЬНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПОВ'ЯЗАНИХ ІЗ ТОРГІВЛЕЮ ЛЮДЬМИ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ ОТРИМАННЯ ПІДСТАВ ДЛЯ ПРОВЕДЕННЯ ОКРЕМИХ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Гуцуляк Юрій Васильович,

*доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ*

Інформаційно-технічний бум ХХІ століття, яким, беззаперечно, є ріст числа суб'єктів використання глобальної інформаційної системи Internet, розвиток можливостей доступу до неї, надшвидка зміна форм і техніки, що використовується для доступу в цю систему, докорінно змінює окремі суспільні відносини. Разом з тим, розповсюдження по всьому світі нових інформаційно-комунікаційних технологій викликало появу чисельних злочинів, пов'язаних з використанням комп'ютерів, інформаційних мереж, програмного забезпечення обміну інформацією. Інструментарій злочинця стає швидкозмінним та латентним. Використання комп'ютерних технологій та ресурсів є як окремими видами злочинів, так і невід'ємною складовою вчинення інших кримінальних правопорушень, зокрема тероризму, наркозлочинності, торгівлі людьми. Всі ці злочини не мають лиш національного значення, вони є транснаціональними, що в свою чергу свідчить про стійку організаційну складову.

Зважаючи на таку швидко зміну щодо форм та способів підготовки, вчинення і приховання кримінальних правопорушень, погоджуємося із твердженням, що загрозу, яка йде від транснаціональної організованої злочинності, можна ліквідувати лише в тому випадку, якщо правоохоронні органи будуть точно так само, як і самі злочинні організації, виявляти винахідливість, організаційну гнучкість та співпрацю. Зокрема, для того щоб домогтися

успіху, їм слід більш творчо підходити до використання існуючих і нових двосторонніх і багатосторонніх правових механізмів, а діяльність на національному рівні має бути однаковою або узгодженою для того, щоб співробітники правоохоронних органів володіли такою ж мобільністю й діяли так само ефективно, як і самі злочинці [1, с.90].

Основним фактором, який впливає як на підвищення рівня сучасної кіберзлочинності (в тому числі і рівень та якість злочинів, що вчиняються за допомогою кіберпростору) є розвиток систем підключення до глобальних мереж. В 2014 році нараховувалось майже 3 мільярди користувачів мережі Інтернет, на долю яких припадало близько 40 відсотків всього населення земної кулі. Більшість користувачів продовжують отримують доступ до Інтернету за допомогою широкополосних систем, якими користуються 32 відсотки всього населення світу – за 5 років станом на 2014 рік, це в 4 рази більше ніж у 2009 році[3].

Очікується, що до кінця 2018 року кількість пристроїв, підключених до мереж з інтернет-протоколом (IP) буде більшим майже в два рази ніж населення планети [4]. В силу таких темпів зростання використання електронного обміну інформацією, виклики кіберзлочинності стають дедалі загрозливішими, як в контексті окремих видів кримінальних правопорушень в межах окремих держави і її національних інтересів, так і для держав, що втягнуті в транснаціональну злочинність.

Ефективна протидія з боку держави цьому негативному явищу лежить в кількох площинах: соціально-економічній; міжнародній; сфері кримінального судочинства. Остання, на наш погляд, має визначальне значення і полягає в вдосконаленні та реформуванні двох блоків: завдань та функцій окремих правоохоронних органів з моніторингу та аналізу масиву інформаційних даних з мережі Internet, які місять інформацію про вчинюване, вчинене або таке, що готується кримінальне правопорушення; а також розроблення концептуального підходу у формуванні нових джерел доказів у кримінальному провадженні та процесуальному порядку їх формування, перевірки, оцінки та використання.

В контексті кримінально-аналітичного забезпечення досудового розслідування, перший згаданий нами блок, цікавить результатами органів кримінального аналізу та моніторингу кіберпростору. Результатами діяльності відповідних структурних одиниць правоохоронних органів, таких як Кіберполіція зокрема, є масив інформації що мають потенційний оперативний та слідчий інтерес. Такі дані можуть бути підставою для початку досудового розслідування, тобто внесення відомостей в ЄРДР, як повідомлення про вчинене кримінальне правопорушення – у випадку якщо містять в собі ознаки вчиненого кримінального правопорушення, на підставі ч.1 ст. 214 КПК України. Також отримана інформація може бути підставою для проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та застосування відповідних заходів забезпечення кримінального провадження, і випадку якщо містить дані про відомості, які гарантують при проведенні слідчої (розшукової) дії досягнення мети її проведення (ч.2 ст.223 КПК України); якщо наявні підстави передбачені ч.2 ст. 246 КПК України; зміст отриманих в результаті моніторингу чи кримінального аналізу даних дозволяє слідчому чи прокурору довести обставини, передбачені ч.3 ст. 132 КПК України чи наявність ризиків вказаних в ч.1 ст. 177 КПК України.

На наш погляд, використання результатів моніторингово-аналітичної інформації в даному випадку може мати місце у випадку, коли така інформація є в матеріалах кримінального провадження з юридично визначеного джерела і перевірена процесуальним шляхом на стадії досудового розслідування, або й без такої перевірки, якщо вона не «випадає» з контексту зібраних доказів в кримінальному провадженні, а логічно вписується в такий.

Щодо другого, згаданого нами блоку, то на ці тенденції звертається увага на міжнародному рівні, про що свідчать підсумки XIII конгресу ООН щодо попередження злочинності та кримінальному правосуддю. Зокрема зазначалось про тенденцію до зникнення межі відмінності від звичайною злочинністю та кіберзлочинністю, а також зміни форм та засобів протидії їй. По мірі того як більш широко застосовуються електронні пристрої обміну інформацією і систем підключення до глобальних мереж використання електронних доказів, таких як: текстові повідомлення, листи

надіслані електронною поштою, дані перегляду мережі Інтернет та інформація із соціальних мереж, стають звичною справою при проведенні багатьох звичайних кримінальних переслідувань [2]. Як бачимо, в досвіді іноземних країн, розуміння електронного доказу в кримінальному судочинстві вже не обговорюється, а констатується як факт. В національній науці кримінального процесу, криміналістики можливість запровадження такого процесуального інституту обговорюється. Так, Д.М.Цехан визначає необхідність введення категорії «цифрового доказу» під яким слід розуміти фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [5, с. 259]. О. І. Котляревський, Д. М. Киценко пропонують використовувати поняття «електронні докази», під якими вони розуміють сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [6]. Існують подібні напрацювання і в науковців суміжних з Україною держав, зокрема, в науці кримінального процесу РФ, попри тоталітарний стан управління державою та здійснення судочинства (якщо його таким можна назвати). Так, М. А. Іванов пропонує виокремити її в якості самостійного та специфічного джерела відомостей, що обумовлюється її особливою неречовою природою, природно-технічними особливостями її створення, обробки, збереження, передачі, кримінально-процесуальними процедурами та техніко-криміналістичними прийомами її пошуку та вилучення, доступу до неї, дослідження та перетворення в форму, що може бути сприйнята людиною [7].

З поданого вище, вважаємо, що враховуючи сучасний розвиток людства в обміні інформацією та запровадженні новітніх технологій у даній сфері, ріст та стрімка зміна форми злочинності із звичної у кіберформу, наукове розроблення підходів у розумінні цифрових чи електронних доказів, порядку їх отримання та використання в ході досудового розслідування (зокрема як підстави для проведення негласних слідчих (розшукових) дій), а також як

доказів в кримінальному провадженні має перспективне значення як для наукових розробок, так і для нормативного врегулювання практичної складової діяльності органів досудового розслідування. А разом з тим, потребує негайного відображення у реформах органів досудового розслідування Національної поліції тощо.

-
1. Основы борьбы с организованной преступностью: [монография] / под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. – М.: Инфра-М, 2000. – 400 с.
 2. Тринадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество. – [Электронный режим доступа]: – www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12
 3. International Telecommunication Union. (2014)/ The world in 2014: ICT facts and figures. Geneva: Author. – [Электронный режим доступа]: - www.itu.int/ITU
 4. Cisco, «The zettabyte era: trends and analysis», Cisco Visual Networking Index (San Jose, California, 2014). – [Электронный режим доступа]: – www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni
 5. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування / Д. М. Цехан // Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. – 2013. – № 5. – с.256-259.
 6. Котляревський О. І. Комп'ютерна інформація як речовий доказ у кримінальній справі / О. І. Котляревський, Д. М. Киценко : [Електронний ресурс]. – Режим доступу : <http://www.bezpeka.com/ru/lib/spec/crim/art70.html>
 7. Иванов Н. А. Доказательства и источники сведений в уголовном процессе: проблемы теории и практики: моногр. /Н.А. Иванов. – М.: Юрлитинформ, 2015. – 232 с. – С. 165–166

ЮРИДИЧНА ПРИРОДА ПЕРСОНАЛЬНИХ ДАНИХ

Єсімов Сергій Сергійович,

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

Яцина Остап Ігорович,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Виникнення персональних даних як категорії в інформаційному праві та праві в цілому тісно пов'язане з ідеєю захисту приватного життя, яка в умовах розвитку інформаційного суспільства все частіше піддається різного виду загрозам. Саме бажання забезпечити належний рівень захисту особи від інформаційних загроз призвело до ідеї контролю над обігом інформації про індивідів – персональних даних, виділивши їх в особливий вид інформації, яка потребує захисту. У зв'язку з цим говорити про юридичну природу персональних даних, не розглядаючи їх в ракурсі співвідношення з категорією права на недоторканність і повагу до приватного життя неможливо.

У даний час право на захист інформації про приватне життя, так само як і необхідність поваги приватної, особистої сфери життя індивіда, так само як і право індивіда на захист інформації про нього (персональних даних) вважаються невід'ємними правами будь-якої людини.

З метою запобігання численним загрозам правам і свободам людини, викликаних «маніпулюванням» даних про фізичних осіб, з'явилися спеціальні норми про захист останніх шляхом обмеження їх поширення та обробки. Згодом це стало причиною появи нової правової категорії – персональних даних як особливого різновиду інформації про фізичну особу, з особливим правовим режимом, необхідність якого була обумовлена серйозною потенційною небезпекою заподіяння шкоди правам і свободам індивіда при порушенні правил її обробки.

У країнах Європейського Союзу та США зазначена категорія була введена в обіг вже більше 30 років тому, спочатку як один з важливих елементів захисту права на недоторканність і повагу до приватного життя. На поточний момент законодавство про персональні дані прийнято більш ніж в 43 країнах світу, яке в багатьох положеннях схоже між собою. У всіх випадках необхідність захисту персональних даних розглядають як необхідний в суспільстві розвинених інформаційних технологій елемент захисту прав і свобод особи.

У той же час це породило питання про співвідношення зазначених категорій хоча, без сумніву, ці поняття пов'язані між собою.

На підставі аналізу міжнародного досвіду можна прийти до аналогічного висновку. Візьмемо, зокрема, положення Рекомендацій Організації економічного співробітництва та розвитку, що стосуються основних положень про захист недоторканності приватного життя і міжнародних обмінів персональними даними, а також преамбули Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою даних.

В обох випадках вказується в якості мети гармонізації національного законодавства – зміцнення гарантій прав особистості, і перш за все – права на недоторканність приватного (особистого) життя індивіда в умовах автоматизованої обробки даних про нього.

Преамбула Директиви Європейського парламенту та Ради ЄС 95/46 / ЄС про захист прав приватних осіб стосовно обробки персональних даних та про вільний рух таких даних в п. 10 явно говорить про те, що предметом національного законодавства про персональні дані є захист фундаментальних прав і свобод, перш за все – права на приватне життя.

Європейський суд у своїй практиці, що стосується статті 8 Конвенції про захист прав людини і його основних свобод, також визнав, що захист персональних даних від розголошення є одним з найважливіших елементів здійснення права особи на повагу до особистого і сімейного життя.

Національне законодавство спочатку не пов'язувало безпосередньо захист персональних даних і право на повагу та недоторканність приватного життя. Остаточна крапка в цьому питанні була

поставлена в прийнятому спеціальному Законі України від 1 червня 2010 року № 2297-VI «Про захист персональних даних», де в ст. 1 в якості основної мети захисту персональних даних вказується забезпечення прав і свобод людини та громадянина, в тому числі захисту прав на недоторканність приватного життя.

Отже, буде логічно зробити висновок про наявність прямого зв'язку між захистом персональних даних і правом на недоторканність приватного життя та включених до нього права на таємницю приватного життя, особисту, сімейну таємницю, таємницю сповіді, таємницю голосування і інші.

У той же час, орієнтуючись на законодавче визначення персональних даних, як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, де останні включають в себе всю інформацію про фізичну особу, можна цілком обґрунтовано зробити висновок про те, що коло відомостей, інформації, яка може бути представлена у вигляді персональних даних, не обмежується приватною чи особистою, сімейною сферою життя індивіда.

Зокрема, персональні дані можуть цілком включати в себе відомості про суспільне життя індивіда, про службову та професійну діяльність і багато іншого, що не завжди може охоплюватися поняттям приватне життя або, принаймні, викликати сумнів такого віднесення до зазначеної категорії.

З аналізу існуючих положень законодавства випливає, що потенційно персональні дані включають в себе, поряд з відомостями про приватне життя особи (таємницею приватного життя), ціле коло відомостей, які охоплюються багатьма іншими правовими категоріями, які існували та з'явилися в правовій матерії раніше категорії «персональні дані».

Зокрема, за текстом Закону України «Про захист персональних даних», можна прийти до висновку, що в окремих положеннях йдеться про персональні дані, що становлять одночасно відомості, що охороняються на умовах інших режимів: державної таємниці; особистої, сімейної таємниці; таємниці приватного життя; лікарської таємниці; таємниці слідства; таємниці правосуддя і оперативно-розшукової діяльності.

У всіх цих випадках очевидним загальним моментом є те, що ця інформація – про індивіда, та щодо неї введено правовий режим таємниці. За загальним правилом, режим таємниці відповідно до законодавства означає охорону від поширення інформації щодо третіх осіб, з огляду на те що подібне поширення здатне завдати шкоди правам і законним інтересам, в даному випадку – таємниці приватного життя конкретної фізичної особи або його близьких родичів. Такий стан справ цілком можна співвіднести з режимом конфіденційності, який встановлюється Законом України «Про захист персональних даних». Отже, говорячи про співвідношення персональних даних і права на недоторканність приватного життя, цілком обґрунтовано можна зробити висновок, що вони є пов'язаними між собою поняттями, але в той же час не тотожними.

Останнім часом цьому питанню присвячено достатню увагу в цілому ряді публікацій та дисертаційних дослідженнях. У дослідженнях персональні дані визначаються як комплексне та самостійне утворення – новий правовий інститут, підкреслюючи його мобільність і динамічний розвиток.

У ряді публікацій розглядається проблема визначення персональних даних через виділення правового інституту «захисту персональних даних», що носить міжгалузевий комплексний характер.

Деяка розбіжність розбіжність в термінології не применшує в такому випадку загальну ідею виділення правових норм, що регулюють порядок обігу персональних даних, в самостійний правовий інститут.

З зазначеними пропозиціями важко не погодитися, з огляду на кількість законодавчих актів у цій сфері, що приймаються останнім часом.

Приблизно схожі міркування про самостійність як інституту персональних даних в порівнянні з правом на недоторканність приватного життя можна зустріти і у цілому ряду авторів з країн-членів Європейського Союзу, що ще раз підтверджує загальний вектор розвитку права в цьому напрямі, який орієнтує на самостійність правового інституту персональних даних.

Ще одне суттєве питання, що обговорюється у науковій літературі це формування права на захист персональних даних, в числі фундаментальних прав особи. Безумовно, ідея «прав людини» є утворенням що динамічно розвиваються та поступово еволюціонує, приростаючи новими значеннями, смислами, а інакше кажучи, новими правами та свободами, які з розвитком суспільства починають сприйматися невід'ємними та фундаментальними.

Аналогічно зародженню права на захист приватного життя з ідеї особистої свободи, можна з усією обґрунтованістю припускати про появу нового права – права на захист персональних даних, як багато в чому необхідного елемента інформаційної культури демократичного суспільства, без якого неможливо було б забезпечити необхідний рівень захисту особи.

Захист персональних даних і право на захист персональних даних є різновидом юридичних гарантій конституційних прав людини, що може бути реалізовано через механізм конфіденційності. Але конфіденційність є скоріше вимогою, зверненням до операторів персональних даних, і є безумовною, якщо інше не передбачено законом або самим суб'єктом, а в деяких випадках взагалі не залежить від волі останнього. Конфіденційність варто розглядати як один з елементів захисту персональних даних як інформації особливого роду, але далеко не єдиний. Таким чином, право на конфіденційність даних швидше варто розглядати не більше ніж елемент права на захист персональних даних.

Водночас, режим конфіденційності персональних даних все ж сприяє встановленню режиму конфіденційності інформації, що становить таємницю приватного життя, особисту та сімейну таємницю індивіда, гарантує за допомогою цього недоторканність приватного життя, обмежуючи доступ до такої інформації з боку третіх осіб, надаючи індивіду можливість контролювати поширення такої інформації на підставі Закону України «Про захист персональних даних».

-
1. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради. 2010. № 34. ст. 481.

МОДЕРНІЗАЦІЯ ЕЛЕКТРОШОКЕРА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BODYCOM ДЛЯ ЗАПОБІГАННЯ ЙОГО НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ

Зачек Олег Ігорович,

*доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Дмитрик Юрій Іванович,

*доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Одним з ефективних засобів спеціальної техніки, що дозволяють швидко припинити протидію агресивно налаштованих правопорушників, в тому числі таких, що перебувають під дією алкоголю чи психоактивних речовин, є електрошокер. В Україні виробляється електрошокер IP-4 [1] – єдиний електрошокер, який на даний час дозволений для використання правоохоронними органами України. Але під час використання електрошокера, як і іншої зброї, є небезпека його захоплення та використання правопорушником, внаслідок обеззброєння працівника поліції. З метою запобігання цій небезпеці потрібна модернізація електрошокера шляхом додавання в його схему блока ідентифікації користувача.

Нами був розроблений та запатентований модернізований електрошокер зі сканером відбитків пальців IP-4М [2]. Недоліком такої схеми є неможливість повноцінного використання у зимовий час в перчатках.

Одним з варіантів вирішення цієї проблеми є використання для ідентифікації користувача RFID-ключів (від англійського Radio Frequency IDentification – радіочастотна ідентифікація). В такому випадку RFID-ключ міститься в браслеті, одягнутому на руку поліцейського, а у електрошокері міститься RFID-зчитувач, налаштований таким чином, щоб зчитувати інформацію з RFID-ключа

на відстані не більше 20 см. RFID-зчитувач керує електронним ключем, який подає живлення до кнопки включення електрошокера. Ключ містить RFID-мікросхему, яка дозволяє електрошокеру ідентифікувати користувача. Якщо зчитувач електрошокера не «побачить» в своїй зоні дії конкретний ідентифікатор, то електрошокер не включиться. Це дозволяє виключити можливість використання електрошокера зловмисником, якщо він обеззброїть поліцейського. Електрошокер з використанням RFID-ключів IP-4M2 був нами запатентований [3].

Але використання для ідентифікації користувача RFID-ключів потребує досить великого споживання енергії від елементів живлення. Ще одним способом збільшити безпеку використання електрошокера шляхом ідентифікації законного користувача (в тому числі одягнутого в перчатки) з одночасним зменшення енергії, яка споживається системою ідентифікації, є використання ключового периферійного пристрою та технології BodyCom компанії Microchip Technology Inc., в основі якої лежить ємнісний зв'язок через тіло людини. Технологія BodyCom може перетворити тіло людини в безпечний канал передачі інформації.

Технологія BodyCom дозволяє істотно скоротити споживану енергію, бо під час її використання енергія не витрачається даремно у вигляді радіочастотного електромагнітного випромінювання. Приймально-передавальні тракти технології BodyCom працюють на фіксованих частотах, 125 кГц і 8 МГц, які входять до складу дозволених FCC частина 15-B частот [4].

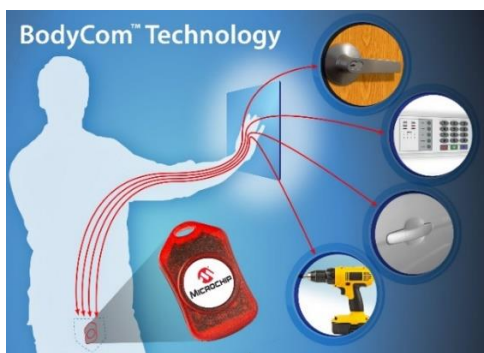


Рис. 1. Технологія BodyCom

Модернізований електрошокер з використанням технології BodyCom IP-4M3 має корпус, в якому містяться батарея, електронна схема електрошокера, на яку подається живлення через послідовно включені вимикач без фіксації та вимикач з фіксацією, ще міститься плата центрального контролера на основі мікроконтролера PIC компанії Microchip Technology Inc., яка отримує живлення по проводам живлення плати центрального контролера через вимикач з фіксацією, ключовий елемент, на який через провід подається сигнал включення електрошокера з плати центрального контролера, за умови перебування ключового периферійного пристрою, з яким здійснюється бездротовий емісійний зв'язок через тіло людини на фіксованих частотах 125 кГц і 8 МГц з використанням криптографічних алгоритмів шифрування KeeLoq і AES, у кишені законного користувача, роз'єм MicroUSB для підключення плати центрального контролера до комп'ютера з метою його програмування на розпізнавання ключового периферійного пристрою, який використовується в комплекті з електрошокером. Це дозволяє виключити можливість використання електрошокера зловмисником, якщо він обеззброїть поліцейського.

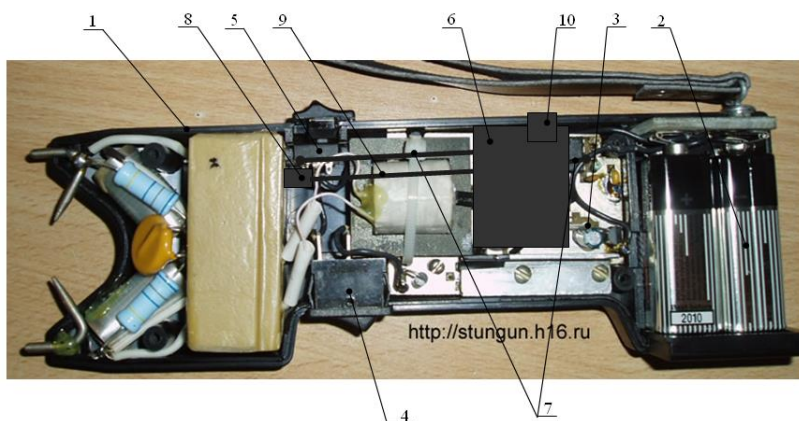


Рис. 2. Внутрішня будова модернізованого електрошокера з використанням технології BodyCom IP-4M3

Внутрішню будову модернізованого електрошокера з використанням технології BodyCom IP-4M3 показано на рис. 2, де 1 –

корпус, 2 – батарея, 3 – електронна схема електрошокера, 4 – вимикач без фіксації, 5 – вимикач з фіксацією, 6 – плата центрального контролера на основі мікроконтролера PIC компанії Microchip Technology Inc., 7 – провода живлення плати центрального контролера, 8 – ключовий елемент, 9 – провід, яким подається сигнал включення електрошокера з плати центрального контролера на ключовий елемент, 10 – роз'єм MicroUSB.

Блок-схема модернізованого електрошокера з використанням технології BodyCom IP-4M3 показана на рис. 3. Тут нумерація відповідає нумерації на рис. 2.

Для включення електрошокера необхідно включити вимикач з фіксацією (аналог запобіжника вогнепальної зброї). Умовою включення електрошокера є наявність у кишені законного користувача ключового периферійного пристрою. Якщо законний користувач розпізнаний, ключовий елемент відкривається і подається живлення до кнопки без фіксації. Натискаючи на цю кнопку, приводимо електрошокер в дію.

Електрошокер з використанням технології BodyCom IP-4M3 був нами запатентований [5].

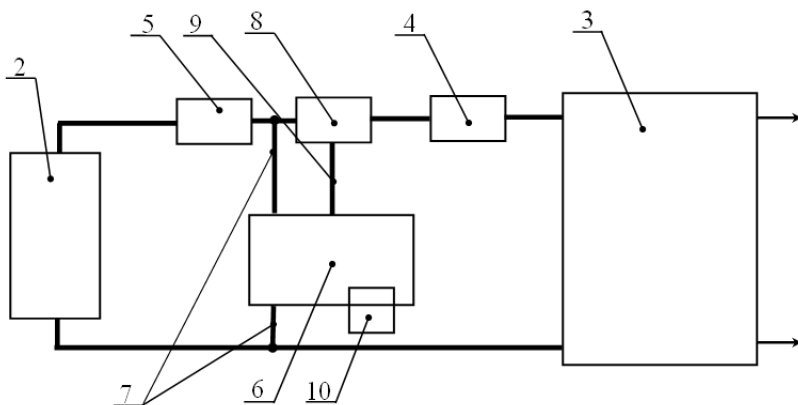


Рис. 3. Блок-схема модернізованого електрошокера з використанням технології BodyCom IP-4M3



Рис. 4. Ключовий периферійний пристрій.

-
1. Електрошокер ІР-4. [Електронний ресурс]. URL: <https://uos.ua/produktsiya/neletalnoe-oruzhie/26-ielectroshoker-ir-4> (дата звернення: 04.12.2018).
 2. Захаров В.П., Зачек О.І. Патент України на корисну модель № 91503 «Модернізований електрошокер зі сканером відбитків пальців ІР-4М» // Видано згідно заявки № у 2014 00215 від 13.01.2014 р. – 4 с.
 3. Зачек О.І., Дмитрик Ю.І. Патент України на корисну модель № 115670 «Модернізований електрошокер зі зчитувачем RFID-ключів ІР-4М2» // Видано згідно заявки № у 2016 10935 від 31.10.2016 р. – 4 с.
 4. BodyCom™ Technology. [Електронний ресурс]. URL: <https://www.microchip.com/design-centers/embedded-security/technology/bodycom-trade-technology> (дата звернення: 04.12.2018).
 5. Зачек О.І., Дмитрик Ю.І. Патент України на корисну модель № 127196 «Модернізований електрошокер з використанням технології BODYCOM ІР-4М3» // Видано згідно заявки № у 2018 00580 від 22.01.2018 р. – 4 с.

ПРИНЦИП ІНФОРМАЦІЙНОЇ ВІДКРИТОСТІ ЯК НЕВІД'ЄМНА СКЛАДОВА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ

Ковалів Мирослав Володимирович,

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

Дужак Андрій Володимирович,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Інформаційна робота є невід'ємною складовою управлінської діяльності на всіх рівнях функціонування органів виконавчої влади. Не знаючи реального стану справ на місцях, не можна попередити негативні тенденції, оперативно керувати силами та засобами, вчасно подавати підпорядкованим органам та підрозділам необхідну допомогу, впливати на організацію та кінцеві результати їх роботи. Без достовірної та повної інформації, всебічного та ґрунтовного аналізу не може нормально функціонувати жоден управлінський апарат. Обґрунтованість та ефективність його рішень перебуває у прямій залежності від стану інформаційної роботи.

Поряд з цим поняттям існує поняття інформаційної відкритості органів державної влади, яке отримало назву транспарентність. Під нею розуміється така організація діяльності органів державної влади, при якій громадянам, їх об'єднанням, комерційним структурам, іншим державним і місцевим органам забезпечується можливість отримувати необхідну та достатню інформацію про діяльність, прийняті рішення та іншу суспільно значиму інформацію при дотриманні встановлених законами обмеженнями.

Принцип інформаційної відкритості закріплений у Законах України «Про інформацію», «Про Кабінет Міністрів України», «Про доступ до публічної інформації» і інших нормативних актах [1-3].

Цей принцип виражається в доступності для громадян інформації, що становить суспільний інтерес або зачіпає особисті інтереси

громадян; систематичному інформуванні громадян про передбачувані або прийняті рішення; здійсненні громадянами контролю за діяльністю державних органів, організацій і підприємств, громадських об'єднань, посадових осіб та прийнятими ними рішеннями, пов'язаними з дотриманням, охороною і захистом прав і законних інтересів громадян.

Специфіка діяльності органів влади полягає в постійному зверненні за інформацією, що одержується з зовнішніх джерел, і безпосередньо в її створенні.

Сучасне суспільство зацікавлене в розвитку прозорості та відкритості державного управління. Широкий доступ до інформації про державні і місцеві органи розширює можливості оцінювати їх діяльність.

Доступність інформації про діяльність органів влади спрямована на забезпечення особистих інтересів індивідуума, пов'язаних з можливістю реалізувати свої права та свободи, на його участь у справах суспільства та держави. Доступ фізичних та юридичних осіб до інформації про діяльність органів влади є основою здійснення громадського контролю над діяльністю державних органів, органів місцевого самоврядування, громадських, політичних і інших організацій.

Особливого значення доступність інформації для громадян має у сферах економіки, екології.

У переважній більшості випадків об'єктом правовідносин у контексті відкритості влади виступає інформація про діяльність того чи іншого суб'єкта публічної влади. Практично жодний суспільний інтерес не обходиться без інформаційного взаємодії учасників.

Нормами міжнародного права встановлюється презумпція розкриття інформації державою як гарантія права на інформацію. Це означає обов'язок гарантувати право на інформацію, введення реальних і ефективних механізмів для його реалізації.

Право на інформацію є ключовим інструментом для боротьби з корупцією та неправомірними діями органів державної влади, органів діяльність яких регулюється корпоративними нормативними актами.

Такий підхід дає змогу розширити систему стримувань і противаг адміністративній владі за допомогою права на інформацію та громадський контроль, який дане право активізує. Підвищення відкритості органів виконавчої влади дозволяє досягти відразу кількох цілей:

- зробити державу більш демократичною, інформаційно відкритою для громадян;
- підвищити ефективність діяльності державного апарату;
- встановити громадський контроль над владою.

Відкритий доступ до інформації дозволяє підвищити відповідальність державних службовців і службовців органів місцевого самоврядування, позитивно впливає на ефективність боротьби з корупцією, з зловживанням службовим становищем.

Хоча відкритість не може бути абсолютною, вона повинна бути необхідною і достатньою. Для підтримки балансу принципово важливо дотримуватися деяких обмежень, тобто обмеження доступу до інформації, наприклад, для поваги прав і репутації інших осіб, а також для охорони державної безпеки, громадського порядку, здоров'я населення.

Специфіка інформації про діяльність державних органів і органів місцевого самоврядування полягає у тому, що ці органи є власниками великого обсягу суспільно важливої інформації, що викликає підвищений суспільний інтерес в силу свого впливу на всі сфери людської діяльності.

Право на доступ до інформації є ключовим елементом розвитку громадянського суспільства і є дієвим механізмом боротьби з негативними соціальними явищами.

Умови, при яких значна частина інформації про діяльність органів влади залишається недоступною для суспільства, створюють сприятливий ґрунт для неефективного державного управління.

-
1. Про інформацію: Закон України від 21.05.1997 № 280/97-ВР // Відомості Верховної Ради. – 1992. – № 48. – Ст. 650.

2. Про Кабінет Міністрів України: Закон України від 27.02.2014 № 794-VII // Відомості Верховної Ради. – 2014. – № 13. – Ст.222.
3. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI // Відомості Верховної Ради. – 2011. – № 32. – Ст.314.

ДЕЯКІ ПРОБЛЕМНІ АСПЕКТИ ВИКОРИСТАННЯ ПОЛІГРАФІВ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Ковтун Вікторія Олександрівна,

здобувач ступеня бакалавра

Харківського національного університету внутрішніх справ

Рвачов Олексій Михайлович,

старший викладач кафедри кібербезпеки

Харківського національного університету внутрішніх справ

У 1892 році англійський кардіолог Дж. Маккензі сконструював перший технічний засіб, який нині має назву «поліграф», але він застосовувався з медичною метою. Даний технічний засіб міг одночасно реєструвати зміни артеріального та венозного тиску, але його застосовували лише з медичною метою.

Перші спроби проконтролювати шкірно-гальванічну реакцію для виявлення фізіологічних ознак брехні були зроблені у 1897 році Б. Стікером, який вважав, що в особи, на яку впливають продемонстровані їй певні зображення чи слова-подразники, виявиться більша різниця показників електричної провідності шкіри. Як приклад учений застосовував гальванометр з електродами, приєднаними до пальців опитуваної особи для реєстрації зазначених параметрів [1].

Аналізу теоретичних і прикладних аспектів застосування поліграфа присвячені дослідження В.І. Барко, Г.С. Берланда, В.А. Варламова, С.Д. Гусарева, С.Н. Зерина, І.С. Зубрилова, В.М. Князева, О.Р. Малхазова, О.І. Мотляха, А.Н. Обухова, С.В. Поповічева, А.І. Скрипникова, Р.А. Фергersona, Ю.І. Холодного, В.В. Чернєя, С.С. Чернявського С.І. Яковенко, С.А. Яни та ін.

Першим нормативно-правовим актом, яким офіційно було передбачено застосування поліграфа в Україні, став наказ МВС України «Про застосування поліграфів у кадровій роботі та оперативно-

розшуковій діяльності підрозділів по боротьбі з організованою злочинністю», який був виданий в 2000 році.

Можливість використання комп'ютерних поліграфів в органах внутрішніх справ України було передбачено Інструкцією щодо застосування комп'ютерних поліграфів у роботі з персоналом органів внутрішніх справ України, яка була затверджена наказом МВС України від 28.07.2004 № 842, який 13.11.2017 втратив чинність [2].

При створенні Національної поліції України можливість використання поліграфів була закріплена на рівні законодавства, а саме згідно з ч. 2 ст. 50 (перевірка кандидата на службу в поліції) Закону України «Про Національну поліцію» «громадяни України, які виявили бажання вступити на службу в поліції, за їхньою згодою проходять тестування на поліграфі» [3].

Згідно з Інструкцією про порядок використання поліграфів у Національній поліції України (далі – Інструкція), яка затверджена наказом МВС України від 13.11.2017 № 920, у діяльності Національної поліції України опитування з використанням поліграфа проводяться в таких випадках:

- під час вступу кандидатів на службу до поліції;
- у разі проведення атестування поліцейських;
- перевірка з власної ініціативи особи, яка виявила бажання бути опитаною з використанням поліграфа, у тому числі під час проведення службових розслідувань;
- здійснення оперативно-розшукової діяльності [4].

Після закінчення роботи спеціаліст готує довідку про результати опитування з використанням поліграфа у двох примірниках, в якій також зазначає модель поліграфа, що використовувався, кількість каналів реєстрації психофізіологічних показників.

У зазначеній Інструкції наведено визначення терміну поліграф – різновид спеціального психофізіологічного технічного засобу, який здійснює реєстрацію динаміки протікання не менше п'яти незалежних психофізіологічних процесів людини (грудного і діафрагмального дихання, серцево-судинної активності, електро-

провідності шкіри, рухової активності) у відповідь на пред'явлення за спеціальною методикою певних психологічних стимулів (запитань, зображень, предметів), не завдаючи шкоди життю, здоров'ю людини та навколишньому середовищу [4].

Як бачимо, в нормативних документах МВС України до поліграфів, що можуть використовуватися у діяльності Національної поліції України, висунуто тільки декілька вимог:

- повинен здійснювати реєстрацію динаміки протікання не менше п'яти незалежних психофізіологічних процесів людини;
- не завдавати шкоди життю, здоров'ю людини та навколишньому середовищу.

На відміну від цього в Інструкції про порядок використання поліграфа в діяльності органів прокуратури України, яка затверджена наказом Генерального прокурора України від 12.06.2017 № 180, міститься вимога, що «для проведення опитування використовується поліграф, який відповідає вимогам державного стандарту, має декларацію про відповідність і висновок державної санітарно-епідеміологічної експертизи України. Використання поліграфів, які не відповідають цим вимогам, забороняється» [5].

Також згідно з п. 8 Порядку проведення психофізіологічного дослідження із застосуванням поліграфа у Державному бюро розслідувань, який затверджений постановою КМУ від 11.05.2017 № 449 «для проведення дослідження працівником структурного підрозділу внутрішнього контролю Бюро використовується поліграф, який відповідає вимогам ДСТУ 8692:2016. Використання працівником структурного підрозділу внутрішнього контролю Бюро поліграфа, який не відповідає зазначеним вимогам, забороняється. Для проведення дослідження стороннім спеціалістом використовується поліграф, який відповідає вимогам щодо нешкідливості для життя і здоров'я людини» [6].

Як бачимо, вимоги до поліграфів в діяльності органів прокуратури та Державного бюро розслідувань України більш суворі та конкретизовані, ніж вимоги до поліграфів, що можуть використовуватися у діяльності Національної поліції України.

20.01.2017 в Україні почав діяти ДСТУ 8692:2016 «Поліграфи. Технічні умови». Отже, поліграфи, які використовуються в Україні, повинні відповідати вимогам даного Державного стандарту України [7].

За даними Всеукраїнської асоціації поліграфологів станом на липень 2017 року всім вимогам ДСТУ 8692:2016 із представлених на комерційному ринку України відповідав тільки поліграф «Rubicon» (Україна) [8] та частково – поліграфи «Ахсition» (США), «Lafayette» (США), «Кріс» (Росія), «Спос» (Росія) [9].

Але за даними, представленими в мережі Інтернет [10, 11], поліграф торгової марки «Рубікон» не має власного програмного забезпечення, а використовує російське забезпечення «SHERIFF 6» та «SHERIFF 6М». За даними же сайту розробника поліграфу «Рубікон» модель «ПІ-02» комплектується програмним забезпеченням «Rubicon-v1» [12].

Висновки. На сьогодні правоохоронні органи в Україні для використання в своїй діяльності можуть придбати тільки єдиний поліграф, який відповідає вимогам ДСТУ 8692:2016, – «Рубікон». Але необхідно звертати увагу на те, яке програмне забезпечення іде у комплекті поставки з поліграфом.

-
1. Kerry S. Lie detectors. A social history URL: https://books.google.com.ua/books/about/Lie_Detectors.html?id=Kr3xmUi6lgoC&redir_esc=y (дата звернення: 03.12.2018).
 2. Про подальший розвиток служби психологічного забезпечення оперативно-службової діяльності органів внутрішніх справ України : наказ МВС України від 28.07.2004 № 842 // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/z1365-04> (дата звернення: 03.12.2018).
 3. Про Національну поліцію : Закону України 02.07.2015 № 580-VIII // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/580-19> (дата звернення: 03.12.18).
 4. Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України : наказ МВС України від 13.11.2017 № 920 // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/z1472-17> (дата звернення: 03.12.2018).

5. Про затвердження Інструкції про порядок використання поліграфа в діяльності органів прокуратури України : наказ Генерального прокурора України від 12.06.2017 № 180 // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/z0764-17> (дата звернення: 03.12.2018).
6. Про затвердження Порядку проведення психофізіологічного дослідження із застосуванням поліграфа у Державному бюро розслідувань : постанова КМУ від 11.05.2017 № 449 // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/449-2017-%D0%BF> (дата звернення: 03.12.2018).
7. ДСТУ 8692:2016 Поліграфи. Технічні умови : наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 15.11.2016 № 378, початку дії 20.01.2017 // Будстандарт: Сервіс документів Online. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67991 (дата звернення: 03.12.2018).
8. Оборудование и аксессуары для полиграфа // Рубикон. URL: <http://www.polygraph-rubicon.com/equipment/> (д.зв.: 03.12.2018).
9. Аналітика відповідності поліграфів ДСТУ 8692:2016 // Всеукраїнська асоціація поліграфологів. URL: <https://polygraph.ua/analitika-vidpovidnosti-poligrafiv-dstu-8692-2016/> (дата звернення: 03.12.2018).
10. В Україні діє державний стандарт ДСТУ 8692:2016 «Поліграфи. Технічні умови» якому в повному обсязі не може відповідати жоден вітчизняний чи закордонний поліграф // Журнал «Судово-психологічна експертиза. Поліграф. Спецзнання». 05.08.2018. URL: <http://expertize-journal.org.ua/all-news/931-v-ukrajini-die-derzhavnij-standart-dstu-8692-2016-poligrafi-tekhnichni-umovi-yakomu-ne-vidpovidaie-zhoden-vitchiznyanij-chi-zakordonnij-poligraf> (дата зв.: 03.12.2018).
11. Назаров О.А. Дістало: бізнес-торгівля українськими поліграфами «Рубікон» або скільки держава готова платити за поліграфи, які не відповідають у повному обсязі вимогам ДСТУ 8692:2016 «Поліграфи. Технічні умови»? // Протокол: юридичний інтернет-ресурс. 12.08.2018. URL: https://protocol.ua/ua/distalo_biznes_torgivlya_ukrainskimi_poligrafami_rubikon_abo_skilki_dergava_gotova_platiti_za_poligrafi_yaki_ne_vidpovidayut_u_povnomu_obsyazi_vimogam_dstu_8692_2016_poligrafi_tehnichni_umovi/ (дата звернення: 03.12.2018).
12. Базовая комплектация полиграфа РУБИКОН П-02 // Рубикон. URL: <http://www.polygraph-rubicon.com/models/rubicon-p02.htm> (дата звернення: 03.12.2018).

ПРАВОВІ ЗАСАДИ РЕЄСТРАЦІЇ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ В СПРАВАХ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

Козут Валентина Миколаївна,

*здобувач кафедри адміністративного та інформаційного права
Національного університету «Львівська політехніка»,
викладач Львівського національного університету ім.І.Франка*

З огляду на стрімке зростання обсягів інформаційних ресурсів, які використовує сьогоденне людство, важливим завданням є пошук можливостей підвищення ефективності використання інформації. Тому в пріоритеті є впорядкування та розробка нових методів і технологій зберігання й доступу до інформації та забезпечення захисту інформації.

Організація роботи зі службовими документами – це створення умов, які забезпечують зберігання необхідної документної інформації, її швидкий пошук, оперативність переміщення й виконання, а також забезпечення умов для всіх видів робіт з документами з моменту складання чи отримання до знищення або ж передавання в архів – становить єдиний технологічний цикл і є важливим організаційним чинником управлінської діяльності [1, с. 324].

Реєстрація документа – це фіксування факту створення або надходження документа шляхом поставлення на ньому умовного позначення – реєстраційного індексу з подальшим записом у реєстраційних формах необхідних відомостей про документ.

Реєстрація документів проводиться з метою забезпечення їх обліку, контролю за виконанням і оперативним використанням наявної в документах інформації.

Реєстрації підлягають як традиційні машинописні (рукописні) документи, так і створені за допомогою персональних комп'ютерів.

Основним принципом реєстрації документів є однократність. Кожний документ реєструється лише один раз:

- вхідні документи реєструються в день надходження або не пізніше наступного дня, якщо документ надійшов у неробочий час;
- документи, створювані в закладі, реєструються в день підписання або затвердження.

У разі передачі зареєстрованого документа з одного структурного підрозділу в інший він повторно не реєструється.

При реєстрації документів впроваджується принцип реєстрації в межах груп залежно від назви, виду, автора і змісту.

Під час реєстрації документа надається умовне позначення – реєстраційний індекс, який складається з кореспондента, порядкового номера в межах групи документів, що реєструються, і доповнюється індексами за номенклатурою справ [1, с. 327].

Система електронної взаємодії державних електронних інформаційних ресурсів призначена для автоматизації та технологічного забезпечення обміну електронними даними між суб'єктами владних повноважень з державних електронних інформаційних ресурсів під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань шляхом використання сервіс-орієнтованої архітектури, що є інтерфейсами прикладного програмування доступу до державних електронних інформаційних ресурсів, побудованими згідно з єдиними вимогами, а також шляхом використання єдиних форматів, протоколів, довідників, шаблонів та класифікаторів [2, с.1].

Основними функціями системи електронної взаємодії державних електронних інформаційних ресурсів є:

- ведення обліку інтерфейсів прикладного програмування суб'єктів владних повноважень, інтегрованих до системи, за допомогою відповідного реєстру;
- надання доступу суб'єктам владних повноважень до інтерфейсів прикладного програмування;
- забезпечення документованого обміну електронними повідомленнями між інформаційними та/або інформаційно-телекомунікаційними системами суб'єктів владних

повноважень з використанням телекомунікаційних мереж загального користування або спеціальних телекомунікаційних мереж;

- забезпечення електронної ідентифікації та автентифікації суб'єктів владних повноважень;
- забезпечення фіксації часу відправки та отримання електронних повідомлень;
- забезпечення цілісності та автентичності електронних повідомлень та надання відомостей, що дозволяють простежити історію руху електронних повідомлень;
- забезпечення протоколювання дій суб'єктів владних повноважень під час обміну даними;
- забезпечення моніторингу працездатності інтерфейсів прикладного програмування та дотримання виконання регламентованих процедур під час здійснення електронної взаємодії.

Забезпечення електронної взаємодії відбувається за такими принципами:

- інформування громадян про запити щодо їх персональних даних;
- технологічної нейтральності;
- використання єдиних правил електронної взаємодії, відкритих форматів даних, протоколів та стандартів обміну;
- повторного використання даних та програмних засобів;
- зменшення інформаційної надлишковості та дублювання даних [2, с.2]

Подальший розвиток Державної системи електронних звернень громадян дозволить забезпечити створення єдиного адресного простору органів виконавчої влади на державному загальнодоступному інформаційному веб-ресурсі, автоматизоване формування звітів щодо організації звернень громадян, оперативний контроль за реєстрацією та опрацюванням звернень громадян, підвищення якості надання електронних послуг громадян та рівня виконавської дисципліни в державних органах.

Державна система електронних звернень – це єдиний загально – доступний інформаційний веб-ресурс звернень громадян до органів виконавчої влади та місцевого самоврядування створений для:

- підвищення якості та прозорості процесу опрацювання звернень громадян та запитів на отримання публічної інформації в органах державної влади та органах місцевого самоврядування;
- впровадження механізму подання юридично значимих електронних звернень до органів державної влади та органів місцевого самоврядування в електронному вигляді із застосуванням електронного цифрового підпису;
- забезпечення оперативного контролю за розглядом звернень громадян та запитів на отримання публічної інформації;
- створення єдиного адресного простору органів державної влади та органів місцевого самоврядування на державному загальнодоступному інформаційному веб-ресурсі;
- формування статистики обліку звернень громадян та запитів на отримання публічної інформації.

Державна система електронних звернень надає:

- громадянам: можливість формування, гарантованого надсилання юридично значимих звернень в електронному вигляді а також запитів на отримання публічної інформації до органів державної влади та органів місцевого самоврядування через єдину точку доступу (за принципом «єдиного вікна») через мережу Інтернет, а також контролю за розглядом звернень та запитів на отримання публічної інформації в режимі on-line;
- посадовим особам органів державної влади та місцевого самоврядування: можливість приймання, розгляду, надання відповідей на електронні звернення та запити на отримання публічної інформації а також формування статистичного обліку звернень та запитів на тримання публічної інформації;
- до Державної системи електронних звернень можуть підключатися всі зацікавлені державні та недержавні

структури, які працюють із зверненнями громадян та запитами на отримання публічної інформації. Для користування Системою обов'язковим є доступ до мережі Інтернет та для відправки юридично значимого електронного звернення наявність електронного цифрового підпису [2, с.5].

Основна мета розвитку електронного урядування в Україні – створення сучасних механізмів, спрямованих на удосконалення діяльності судової влади, місцевих органів виконавчої влади й органів місцевого самоврядування, результатом яких повинно стати забезпечення прав фізичних і юридичних осіб на отримання об'єктивної та достовірної інформації про діяльність державних органів і якісних адміністративних послуг, а також впровадження ефективних інструментів забезпечення розвитку електронного урядування та становлення електронної демократії.

-
1. Беспяньська Г. В. Діловодство: навчальний посібник для дистанційного навчання / Г. В. Беспяньська. – К. : Вид-во ун-ту «Україна», 2007. – 469 с.
 2. Положення про електронну взаємодію державних електронних інформаційних ресурсів, затверджено постановою Кабінету Міністрів України від 8 вересня 2016 р. № 606: Урядовий кур'єр від 14.09.2016 – № 172.

ПРОЦЕСУАЛЬНЕ ОФОРМЛЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ЗА ДОПОМОГОЮ ТЕХНІЧНИХ ЗАСОБІВ: ДЕЯКІ АСПЕКТИ

Комісарчук Юлія Анатоліївна,

*доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ
кандидат юридичних наук, доцент*

Клим Любов Михайлівна,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Слідчі (розшукові) дії є одним із різновидів кримінальних процесуальних дій, що мають пізнавальну спрямованість та відносяться до основних засобів збирання і перевірки доказів. Система слідчих (розшукових) дій передбачає такі процесуальні форми здійснення пізнавальних дій, які включають у себе всі необхідні та допустимі методи пізнання і у своїй сукупності дають можливість встановити об'єктивну істину.

Відповідно до ч.1 ст. 223 Кримінального процесуального кодексу України (далі – КПК) слідчі (розшукові) дії є діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні [1].

Відповідно до ст. 103 КПК процесуальні дії під час кримінального провадження можуть фіксуватися:

- у протоколі;
- на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії;
- у журналі судового засідання.

Про факт проведення будь-якої слідчої (розшукової) дії складають протокол з відповідними додатками. Протокол є основною формою фіксації ходу і результатів проведення слідчих (розшукових) дій. Даний процесуальний документ має важливе доказове значення адже він є процесуальним джерелом доказів

Складання протоколу слідчої (розшукової) дії являє собою не тільки розумовий, але й технічний процес, пов'язаний із значною затратою часу і сил [2, с.227].

Протокол складається від руки, або друкується слідчим чи прокурором, які здійснюють відповідну слідчу (розшукову) дію, під час її проведення або після її закінчення.

Протокол складається з вступної, описової і заключної частини.

Вступна частина має містити: 1) місце, час проведення та назву процесуальної дії; 2) особу, яка проводить процесуальну дію (прізвище, ім'я, по батькові, посада); 3) всіх осіб, які присутні під час проведення процесуальної дії (прізвища, імена, по батькові, дати народження, місця проживання); 4) інформацію про те, що особи, які беруть участь у процесуальній дії, заздалегідь повідомлені про застосування технічних засобів фіксації, характеристики технічних засобів фіксації та носіїв інформації, які застосовуються при проведенні процесуальної дії, умови та порядок їх використання.

Описова частина повинна містити відомості про: 1) послідовність дій; 2) отримані в результаті процесуальної дії відомості, важливі для цього кримінального провадження, в тому числі виявлені та/або надані речі і документи.

Заключна частина повинна містити: вилучені речі і документи та спосіб їх ідентифікації; спосіб ознайомлення учасників зі змістом протоколу; зауваження і доповнення до письмового протоколу з боку учасників процесуальної дії (ст. 104 КПК).

До протоколу можуть долучатися додатки.

Згідно статті 105 КПК додатками до протоколу можуть бути:

- спеціально виготовлені копії, зразки об'єктів, речей і документів;
- письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії;
- стенограма, аудіо-, відеозапис процесуальної дії;
- фототаблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу.

Факт долучення додатків до протоколу обов'язково зазначають у протоколі.

Учасникам слідчої (розшукової) дії надається можливість ознайомитися зі змістом протоколу. Протокол підписують усі учасники процесуальної дії. Зауваження і доповнення зазначаються у протоколі перед підписами.

Якщо, особа, яка брала участь у проведенні процесуальної дії відмовилася підписати протокол, про це зазначається у протоколі. Дана особа може надати пояснення щодо причин відмови від підписання, які вносяться до протоколу. Факт відмови від підписання протоколу та факт надання письмових пояснень щодо причин такої відмови засвідчується підписом її захисника, а за його відсутності – підписом понятих (ст. 104 КПК).

Слідчі (розшукові) дії можуть також фіксуватися на носіях інформації за допомогою технічних засобів.

Під науково-технічними засобами, які застосовують у сучасному досудовому розслідуванні, слід розуміти систему загальних технічних, пристосованих і спеціально розроблених інформаційних технологій, а також приладів, апаратів, устаткування, інструментів, пристосувань, матеріалів і методів їх застосування з метою забезпечення найбільш ефективного проведення досудового розслідування [3, с.91].

У разі застосування науково-технічних засобів під час слідчої (розшукової) дії, у протоколі слідчої (розшукової) дії зазначається детальна інформація про використовуваний засіб, також зазначається особа, яка використовувала його тощо.

Фіксація слідчих (розшукових) дій за допомогою науково-технічних засобів дозволяє об'єктивно зафіксувати хід та результати їх проведення. Тому, з урахуванням зміни кримінального процесуального законодавства, сьогодні фіксації ходу та результатів слідчих (розшукових) дій за допомогою науково-технічних засобів приділяється велика увага [4, с.297].

Отже, протокол слідчих (розшукових) дій є одним з процесуальних джерел доказів, який повинен чітко відповідати вимогам

КПК, для того, щоб відомості, які він містить зберігали своє доказове значення. Використання науково-технічних засобів підвищує та розширює тактичні можливості слідчих під час проведення слідчих (розшукових) дій.

-
1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: <http://zakon3.rada.gov.ua/laws/show/4651-17>
 2. Гулкевич З. Т. Основні напрями удосконалення технології документування слідчих (розшукових) дій: Вісник Чернівецького факультету Національного університету «Одеська юридична академія» – 2014. – Вип. 2. – С. 223-236. URL: http://nbuv.gov.ua/UJRN/vchfo_2014_2_23
 3. Баулін О.В., Ляш А.О. Використання науково-технічних засобів під час досудового розслідування. Криміналістичний вісник. – 2013. – №1(19). – С.88-93.
 4. Тимчишин Д.В. Використання науково-технічних засобів під час проведення слідчих (розшукових) дій за участю підозрюваного у вчиненні вбивства. Науковий вісник Національної академії внутрішніх справ. – 2013. – №2. – С.295-302

ПРОБЛЕМИ ЗАСТОСУВАННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Комісарчук Юлія Анатоліївна,

*доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Миханюк Марія Миколаївна,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Уведення до системи досудового розслідування негласних слідчих (розшукових) дій (далі – НС(Р)Д) є надзвичайно прогресивним кроком законодавця, що спрямований на її удосконалення. Передусім у органів досудового розслідування з'явилася можливість самостійного прийняття рішень щодо того, які саме процесуальні дії необхідно здійснити для розслідування злочину. Окрім того, проведення НС(Р)Д забезпечує виявлення, попередження та розкриття найбільш складних та латентних злочинів, що традиційними засобами кримінального провадження, здійснити було би надзвичайно складно або просто неможливо.

Разом з тим, НС(Р)Д є способом збирання доказової інформації, який істотно обмежує права і законні інтереси людини. Практика застосування НС(Р)Д свідчить про значну кількість помилок, що виникають при їх застосуванні. Тож, відповідно до європейських стандартів можливість використання НС(Р)Д повинна передбачати існування механізмів контролю за дотриманням прав та свобод людини, найбільш дієвим серед яких на сьогодні вважається судовий контроль. Це зумовлює підвищену значущість проблем забезпечення правового статусу особистості під час проведення НС(Р)Д.

Згідно зі ч.1 ст.246 КПК України, НС(Р)Д є різновидом слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених КПК України.

Відповідно до ч.6 ст. 246 КПК України проводити НС(Р)Д має право слідчий, який здійснює досудове розслідування злочину, або за його дорученням уповноважені оперативні підрозділи Національної поліції, органів безпеки, Національного антикорупційного бюро України, Державного бюро розслідувань, органів, що здійснюють контроль за додержанням податкового і митного законодавства, органів Державної кримінально – виконавчої служби України, органів Державної прикордонної служби України. За рішенням слідчого чи прокурора до проведення НС(Р)Д можуть залучатися також інші особи.

Більшість НС(Р)Д проводяться на підставі ухвали слідчого судді, за клопотанням прокурора чи за клопотанням слідчого погодженого з прокурором.

Проведення НС(Р)Д дозволяє швидше та ефективніше розслідувати злочини, крім того застосування НС(Р)Д допомагає виявляти латентні злочини у кримінальному провадженні.

Не можна залишати поза увагою той факт, що при проведенні негласних слідчих (розшукових) дій часто трапляється обмеження конституційних прав та свобод людини, тому дуже важливим є те, щоб розслідування одного кримінального правопорушення не призвело до вчинення іншого, тільки вже з боку працівника правоохоронних органів [2, с. 144, 146]. Конституцією та спеціальними законами України не дозволяється збирання, збереження та використання і розповсюдження інформації, яка не має відношення до цілей і завдань оперативно-розшукової діяльності. Обмеження конституційних прав і свобод розглядається як виняток із загального положення про необхідність їх найбільш повного і всебічного захисту. Застосування обмежень допускається при дотриманні ряду вимог і в суспільно значимих цілях, заради захисту яких і здійснюється тимчасове обмеження прав людини [3, с.94].

Аналіз практики надання дозволу на проведення НСРД свідчить про те, що серед основних причин отримання відмов у задоволенні клопотань про проведення НСРД є необґрунтованість необхідності проведення саме такого виду НСРД; недоведеність слідчим у клопотанні неможливості отримання доказів без прове-

дення зазначених дій; порушення слідчим питання про проведення НСРД у провадженнях про розслідування злочинів невеликої та середньої тяжкості; порушення підслідності; неналежне оформлення прокурором погодження клопотання тощо [4, с. 18].

На наш погляд, така практика судів є правильною, оскільки забезпечує дотримання прав і свобод громадян від їх необґрунтованого обмеження. Як приклад, слідчі судді відмовляють у задоволенні клопотання про проведення НСРД, якщо слідчий, прокурор не зазначив у клопотанні відомості про особу, в житлі чи іншому володінні якої необхідно провести дію, точну адресу житла чи іншого володіння особи; якщо це автомобіль, то не зазначають марку автомобіля та державний реєстраційний номер; про те, що саме в телефонних розмовах містяться дані про причетність особи до вчинення діянь, які внесені до ЄРДР, тощо [5, с.71].

Запровадження негласних слідчих (розшукових) дій надає можливість правоохоронним органам на основі процесуального закону використовувати цілий спектр заходів і засобів, які раніше можна було проводити тільки в рамках оперативно – розшукової діяльності. Спираючись на статистичні дані та спілкування з працівниками органів Національної поліції, можна сказати про недостатнє використання вищевказаних можливостей.

Це зумовлено рядом факторів, у тому числі:

- недостатнім фінансовим забезпеченням практичних підрозділів органів Національної поліції з боку держави,
- недосконалістю нормативно – правового забезпечення такої діяльності,
- відсутністю практичних і теоретичних навиків проведення таких дій, у тому числі із застосуванням спеціальних технічних засобів працівниками слідчих та оперативних підрозділів органів Національної поліції,
- складність процедури отримання дозволу на проведення таких дій тощо.

Належне забезпечення спеціальними технічними та оперативно-технічними засобами практичних підрозділів органів Національної поліції, а також підготовка кваліфікованих працівників із

застосування такої техніки, безумовно, стало б кроком до більш ефективного проведення всіх видів негласних слідчих (розшукових) дій.

-
1. Кримінальний процесуальний кодекс України: чинне законодавство із змінами та доп. на 16 березня 2018 року: Оф. текст. К.: Алерта, 2018. 290 с.
 2. Бандурка О.М Теорія і практика оперативно-розшукової діяльності: монографія. Харків: Золота миля. 2012. 620 с.
 3. Веприцький Р.С. Використання негласних слідчих (розшукових) дій у протидії злочинності в регіоні. Кримінальне право, кримінальний процес та криміналістика. 2015. Вип.№2. С. 92 – 95.
 4. Городовенко В. Судовий контроль за проведенням слідчих (розшукових) і негласних слідчих дій. Слово Національної школи суддів України. 2013. № 1. С. 15–20.
 5. Татаров О.Ю. Окремі проблеми при проведенні негласних слідчих (розшукових) дій. Вісник кримінального судочинства. 2016. Вип.№3. С. 69 – 77.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Комісарчук Юлія Анатоліївна,

*доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент*

Ярко Христина Володимирівна,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Відповідно до Закону України «Про Національну поліцію» п.9 ч.1 ст.32, поліція може застосовувати технічні прилади і технічні засоби, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису.

Спеціальна техніка поліції – це комплекс технічних засобів, а також тактичних прийомів їх використання, що застосовуються поліцією для боротьби зі злочинністю та для забезпечення всіх напрямків практичної діяльності при безумовному дотриманні законності [2, с.12] .

Спеціальна техніка в роботі оперативних і слідчих підрозділів має такі характеристики:

- спеціальна техніка, яка надходить у готовому вигляді (деякі види автотранспорту, апаратура зв'язку, оптико-механічні прилади спостереження, вимірювальні прилади, фото— і відеотехніка, обчислювальна та інша налаштована на спеціальні потреби техніка).
- спеціальна техніка, модернізована з метою її пристосування до виконання специфічних завдань і умов діяльності оперативних і слідчих підрозділів (автозасоби, обладнані радіостанціями, засобами підсилення звуку; засоби маскування та дистанційного управління для різних фото— та відеокамер; персональні ЕОМ, на базі яких створені автоматизовані робочі місця для співробітників оперативних і слідчих підрозділів, органів безпеки).

- спеціальна техніка, розроблена та виготовлена спеціально для оперативних і слідчих підрозділів з найбільш повним урахуванням їх специфічних завдань та умов роботи [3].

У науковій та спеціальній літературі питання класифікації та застосування технічних засобів на стадії досудового розслідування досліджували П. П. Артеменко, В. К. Гончар, О. В. Золотар, Ю. Ю. Орлов, М. В. Салтевський та інші. Їхні праці є значним внеском у розвиток теорії та практики застосування спеціальних технічних засобів при розкритті злочинів та їх запобіганні. Загалом автори віддають перевагу системі та структурі технічних засобів на змішаній основі, а саме: за галуззю наукового знання, суб'єктом застосування та цільовим призначенням

Для ефективного застосування спеціальної техніки працівники органів Національної поліції мають самостійно набувати навичок їх використання, а за потреби запрошувати спеціаліста, експерта до участі в проведенні слідчих (розшукових) дій, мати вичерпну інформацію про можливості наявних експертних установ. Нехтування цими вимогами призводить на практиці до певних труднощів у виявленні, збиранні та фіксації матеріальних слідів злочину, внаслідок чого докази назавжди втрачаються. Однак, слід зазначити, що відображувані в протоколах оглядів, обшуків, впізнань і багатьох інших дій, фактичні дані засвідчуються підписами понятих. Існує суперечність між необхідністю фіксування в протоколах слідчих (розшукових) дій всієї отриманої інформації та реальною можливістю її засвідчення. Зумовлено це тим, що дослідження матеріальних слідів злочину можуть проводитися з використанням фахових знань за методикою, яка не завжди може бути зрозумілою понятим, а результати таких досліджень іноді потребують спеціальної розшифровки [3].

Проблема, однак, полягає у тому, що для встановлення істини при використанні відповідних технічних засобів, вона, можливо буде досягнута, але втрачається зміст та основне завдання кримінального судочинства щодо дотримання законів і прав людини. Більш того, сучасні технології негласного отримання інформації в принципі дозволяють не тільки виявляти факти підготовки до здійснення злочину, але також і наміри щодо його здійснення при

організації тотального контролю за усіма сферами життя суспільства і кожним громадянином окремо [4].

Призначення спецтехніки полягає у створенні умов, що сприяють запобіганню злочинам. Так, застосування охоронної сигналізації дозволяє фіксувати незаконне проникнення на об'єкти, що охороняються, та оперативно вжити заходів для затримання порушників, а використання оперативних обліків дає можливість визначити коло осіб, причетних до певних видів злочинів, а також у полегшенні розкриття вчинених злочинів. Наприклад, використання пошукових приладів забезпечує високу якість проведення огляду місця вчинення злочину, сприяє виявленню речових доказів під час проведення обшуків, створенню можливостей одержання достовірних відомостей про осіб, причетних до підготовки або вчинення злочинів.

Тактика застосування науково-технічних засобів, у свою чергу, впливає на тактику проведення слідчої (розшукової) дії в цілому. «Тактика провадження тих або інших процесуальних дій змінюється залежно від характеру задіяних засобів та прийомів криміналістичної техніки. Використання технічних засобів передбачає їх тактичне обґрунтування та доцільність», – зазначає В. Ю. Шепітько [5, с. 8] .

Сьогодні засоби спеціальної техніки застосовуються на всіх етапах розслідування злочинів, починаючи зі збору інформації про подію, пошук матеріальних слідів і їхніх відображень, а саме у вигляді образів, відтворених різними технічними засобами фіксації інформації. Одержання процесуально значимої інформації здійснюється на етапі досудового розслідування, ґрунтуючись на дослідженні подій, фактів, предметів і образів, доступних для сприйняття людиною. Однак органи сприйняття, можливості обробки одержуваної інформації, здатність до її упорядкованого запам'ятовування і наступного відтворення за допомогою фізіологічних особливостей людського організму, істотно обмежують діапазон і обсяг інформації про об'єкти, що можуть бути сприйняті, зафіксовані і згодом оброблені за допомогою ресурсів людського мозку. Коли ж можливості людського сприйняття будуть вичерпані, їхня роль переходить до технічних засобів (приладів), як

особливих матеріальних засобів, інструментів дослідження, що виступають як продовження органів сприйняття судового експерта, фахівця, слідчого, оперативного працівника [6, с.11].

За видами діяльності спеціальна техніка поділяється на три класи :1) адміністративно-управлінська техніка; 2) слідчо-криміналістична техніка; 3) оперативна техніка. В адміністративно-управлінській діяльності спеціальна техніка застосовується гласно. До техніки адміністративно-управлінської діяльності належать: засоби організаційної техніки, спеціальні транспортні засоби, технічні засоби охорони, засоби регулювання дорожнього руху, автоматики і телемеханіки, комп'ютерна та офісна техніка. Слідчо-криміналістична техніка застосовується гласно та призначена для збирання і дослідження доказів. Її використання регулюється нормами кримінального процесуального закону. Оперативна техніка,що використовується для запобігання злочинам та їх розслідування, а також розшуку злочинців, застосовується переважно негласно. Недоліком цієї класифікації є універсальний характер використання деяких технічних засобів. Одні й ті ж технічні засоби можуть використовуватися на всіх основних напрямках діяльності поліції. Це стосується, наприклад, засобів радіозв'язку, фото- та відеоапаратури, приладів звукозапису, пошукової техніки. Ця обставина має важливе практичне значення і враховується під час розробки нової зразків техніки, під час організації технічного оснащення поліції, а також у процесі організації роботи із застосуванням спеціальних технічних засобів працівниками різних підрозділів поліції. Це уможливило класифікацію спеціальної техніки за призначенням і сферою застосування [2, с. 15-16].

Конкретне призначення спеціальної техніки полягає у полегшенні розкриття та розслідування вчинених злочинів. Наприклад, використання пошукових приладів забезпечує високу якість проведення огляду місця вчинення правопорушення, сприяє виявленню речових доказів під час проведення обшуків; – створення можливостей одержання достовірних відомостей про осіб, причетних до підготовки або вчинення правопорушень. Статистика доводить, що за допомогою низки оперативно-технічних засобів можна швидко та надійно отримати та зафіксувати

відомості про конкретних осіб, які замислюють чи готують злочини, а після цього вжити заходи щодо їхнього недопущення. Прикладами застосування таких засобів можуть бути апаратура аудіо– та відеозапису, прилади спостереження та інше; – фізичне припинення опору з боку злочинних елементів. Це може бути досягнуто через застосування спеціальних засобів захисту особового складу та проведення спеціальних операцій. У попередженні злочинів і в превентивній діяльності органів досудового розслідування, та й під час судового розгляду, широко використовують фото– й кінокамери, відео– та звукозаписувальні пристрої. Значну роль вони відіграють в адміністративно-профілактичній діяльності, попередженні проступків і правопорушень. На базі криміналістичної техніки розроблено різні пристрої спостереження, зокрема такі, що автоматично реєструють ознаки злочинів і правопорушень. Спеціальні засоби в разі спроби протиправної поведінки (отримання неправомірної вигоди) можуть залишати сліди або давати сигнал. Телевізійні та звукові системи спостереження, спеціальні електронні замки та багато інших пристроїв, які є засобами криміналістичної профілактики, розробляють за ініціативою та участю криміналістів [3].

Таким чином, у дослідженнях вищевказаних науковців та у нормативно-правових актах, що регламентують порядок використання технічних засобів щодо виявлення, розкриття і розслідування злочинів, можна зустріти такі поняття, як «спецтехніка», «спеціальна техніка», «засоби спецтехніки по боротьбі зі злочинністю», «спеціальні засоби», «спецзасоби», «спеціальні технічні засоби», «науково-технічні засоби», «технічні засоби», «криміналістична техніка», «оперативна техніка» тощо. Однак, практично кожне з них не має чіткого визначення слова «спеціальний», і чіткої вказівки на те, про які саме «технічні засоби» йде мова. Зустрічаються також дослідження та нормативні документи, у яких одночасно використовуються два або більше з перерахованих вище термінів, частіше без відповідних коментарів і роз'яснень, що порушує логіко-сміслову структуру тексту. Розгляд наукових робіт та нормативно-правових актів показав, що серед термінологічних словосполучень, у яких використовуються зазначені лексичні одиниці стосовно сфери кримінального судочинства і діяльності правоохоронних органів, найбільшого поширення

одержали: «спецтехніка», «спеціальна техніка», «спеціальні технічні засоби» і «технічні засоби», «науково-технічні засоби» і похідні від них [4].

-
1. Про Національну поліцію: Закон України від 02.07.2015 р. № 40-41. С.379.
 2. Гнусов В.А., Світличний Ю.М. Спеціальна техніка Національної поліції України: навч. посіб. Харк. нац. ун-т внутр. справ, факультет № 4, каф. кібербезпеки. – Х. : ХНУВС, 2017. 175 с.
 3. Козенко О.О. Спеціальна техніка під час проведення досудового розслідування, оперативно-розшукових і контррозвідувальних заходів. URL: <https://dspace.uzhnu.edu.ua>
 4. Хараберюш І.Ф. Спеціальна техніка в правоохоронній діяльності: гносеологічний підхід. Часопис Академії адвокатури України. 2012. №17. С.9.
 5. Бирюков В. В. Цифровая фотография: перспективы использования в криминалистике: монография. Луганск: РИО ЛИВД, 2000. 138 с.
 6. Вольнский В.А. Криминалистическая техника: наука-техника – общество – человек. М.: ЮНИТИ-ДАНА, 2000.. 311 с.

ІНФОРМАЦІЙНО-ПРАВОВІ ОСОБЛИВОСТІ КРИМІНАЛІСТИКИ У ВІРТУАЛЬНОМУ ПРОСТОРІ

Крижановський Анатолій Станіславович,

*старший викладач кафедри кримінального права та
кримінального процесу*

Національного університету «Львівська політехніка»

У час активного впровадження інформаційних технологій в життя кожної людини, прогресивного зростання ролі мережі Інтернет не можна не помітити збільшується зростання злочинів, вчинених у даній сфері. Людство на всьому протязі існування ніколи не зупинялося в розвитку. З огляду на безперервну динаміку суспільних відносин і появу нових злочинів, законодавець і правоохоронець не повинні бути статичними. Необхідно швидке правове реагування, розслідування та розкриття нетипових, нових злочинів, якими в останні час все з більш зростаючою статистикою стають злочину в електронному віртуальному просторі. Комп'ютерні та інші цифрові електронні пристрої все частіше стають засобом вчинення злочинів.

Науково-технічний прогрес неминуче впливає на розвиток юридичної науки та практики, але могутній вплив, відчуває наука криміналістики. Наявні і усталені за багато років методики та тактики розслідування злочинів стрімко застарівають, особливо не встигає за стрімким і інтенсивним розвитком віртуального простору криміналістична техніка.

У зв'язку з цим актуальним напрямом розвитку криміналістики є облік і аналіз зростаючого впливу нових інформаційних технологій на процес розкриття та розслідування злочинів.

На сьогоднішній день назріла необхідність піддати кардинальним змінам і доопрацюванням всі наявні традиційні методи розслідування злочинів вчинених у даній сфері.

З огляду на, що криміналістика є наукою про сліди та механізм їх утворення, слід звернути увагу на те, що злочини в кіберпросторі, злочини з використанням нових інформаційних технологій зали-

шають специфічну слідову картину, для якої характерні нетрадиційні механізми утворення [1, с. 6]. Крім безпосередньо матеріальних або ідеальних слідів, сліди злочину залишаються в пам'яті електронних пристроїв.

Деякі автори, ґрунтуючись на нововведення науково-технічного прогресу, пропонують доповнити класичну класифікацію слідів в трасології у галузі диференціювання в залежності від зовнішнього відображення специфічною групою віртуальних слідів.

Віртуальні сліди, не будучи матеріальними, мають особливу специфіку їх виявлення, фіксації, збирання та дослідження. Це повинно враховуватися слідчими при провадженні окремих слідчих дій у справі, що розслідується.

При правильній організації роботи віртуальні сліди можуть послужити доказами незаконного проникнення в пам'ять комп'ютера або іншого пристрою (злому), доказами можливого вчинення або планування певного злочину конкретною особою або групою осіб (наприклад, при наявності доступу до терміналу тільки у певної особи або групи осіб). Вони можуть вказувати на рівень комп'ютерної грамотності зловмисника.

Неможливо прибути на місце злочину, так як самого місця фактично у фізичному, матеріальному сенсі не існує. Воно знаходиться в віртуальному просторі, на Інтернет серверах. Слідчому необхідно володіти не тільки глибокими правовими знаннями, а й бути першокласним програмістом, а з його навантаженням це практично нереально. У разі, коли сліди злочину відображаються в електронній формі, їх виявлення, вилучення та фіксація представляють достатню складність для більшості слідчих працівників.

Щоб грамотно проводити слідчі дії необхідно досконально знати особливості кіберпростору, володіти термінологією, щоб контактувати зі злочинцем не використовуючи допомогу фахівця.

Для кожного виду слідів існує давно використовувана практика, знайшла свій відбиток у нормах права. У Кримінальному процесуальному законі закріплені правила роботи з матеріальними слідами. Але специфічних норм для виявлення, вилучення, фіксації та збереження віртуальних слідів в чинному законодавстві

немає. На даний момент виникла гостра необхідність законодавчого регулювання порядку роботи з віртуальними слідами.

Для кримінального судочинства це актуально не тільки на національному рівні, а й міжнародному в зв'язку з почастищенням кібератак, що, як правило, висвітлюються тільки в засобах масової інформації, засуджуються громадськістю та представниками держав, але так і залишаються не розкритими. Однак наслідки залишаються досить відчутними. Матеріальні збитки налічується мільярдами доларів. Як свідчить статистика, темпи зростання числа злочинів в ІТ-сфері високі.

Практичні рекомендації для роботи з класичними матеріальними слідами неефективні, часом абсурдні. Наприклад, правова норма, закріплена в Кримінальному процесуальному кодексі України передбачає огляд, виїмку, накладення арешту на поштово-телеграфні відправлення, повністю не може бути застосована для проведення цих дій для повідомлень електронної пошти або інших засобів передачі текстових повідомлень. Але, аналогія закону в кримінальному процесуальному законі не передбачена. У особи, яка застосовує право, немає необхідних правових засобів розслідування злочинів за криміналістичними слідами.

На підставі цього вважаємо, що необхідно прийняти закон, який би регулював процесуальні аспекти збору, фіксації віртуальних слідів і використання їх в якості речових доказів у кримінальному провадженні. Є гостра необхідність у створенні абсолютно нової методики розслідування та розкриття кіберзлочинів, яка буде враховувати властивості та характерні особливості Інтернет простору.

Підводячи підсумки доцільно відзначити, що з появою інформаційних технологій злочинці вийшли на новий дистанційний рівень вчинення злочинів. Тому законодавцю і особи, яка застосовує право, необхідно йти в ногу з часом, розробляти законодавство у даному напрямку, удосконалити методи боротьби зі злочинністю. У майбутньому місце віртуальних слідів складно буде переоцінити, оскільки саме за їх допомогою будуть розслідуватися злочини.

-
1. Криміналістика : навчально-методичний посібник. За заг. ред. В. Л. Ортинського. Львів : Видавництво Львівська політехніки, 2016. 103 с.

РОЛЬ ІНФОРМАЦІЇ УПРАВЛІННЯ В ПОЛІЦІЇ

Кулешник Ярема Федорович,

*доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент*

Кочетов Євгеній Сергійович,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Пилаєва Олена Сергіївна,

*здобувач ступеня магістра
Львівського державного університету внутрішніх справ*

Інформація – це жива кров поліції.

Ефективна інформація управління забезпечує поліцейські сили доступом до необхідних інформаційних даних і поліпшує результат їх використання шляхом:

- Зниження вартості у часі та економія ресурсів в процесі накопичення та введення даних.
- Надання своєчасного доступу до високої якості інформації, що зберігається різними організаціями.
- Надання можливості поліцейським силам поділитися високоякісною надійною та ефективною інформацією з партнерами.
- Підтримка бізнесу та продуктивна аналітика, яка дає змогу зрозуміти методи покращення прийняття рішень та розподілення ресурсів.
- Підтримка агрегації даних і розвідувальний аналіз, що перетворює інформацію в дію, інтелект, дозволяючи виявлення зв'язків між людьми, об'єктами, місцями та подіями і формує об'єднаний спільний погляд на певний індивідуум, групу, чи мережу подій.

Вся діяльність поліції повинна бути підкріплена надійним управлінням інформацією для забезпечення ефективного використання ресурсів та активів даних.

Проте, поліція стикається з цілим рядом проблем, пов'язаних з створенням, збором, зберіганням, пересиланням, оцінюванням, обміном та використанням даних.

На рис. 1 показана операційна модель, що демонструє можливості управління інформацією, котра відіграє важливу роль у підтримці всіх поліцейських та адміністративних процесів і забезпечує надання послуг підрозділами національної поліції.

Якщо прийняте неправильне рішення, то це може стати викликом який буде гальмувати об'єднану співпрацю та доступ до даних. В іншому випадку поліція може запобігти некоректному доступу до інформації, якою вона володіє і покращити ефективність і продуктивність своєї роботи.

Для вирішення цих проблем, поліція повинна розробити надійну інформацію управління.

Операційна модель управління інформацією



Збір інформації

Зменшити час, витрачений на адміністративні завдання та максимізацію збору інформації, поліцейські сили повинні мати віддалений доступ до підрозділів, оснащених ІТ-системами, що забезпечують єдину точку введення даних, оцифрування паперових документів, записи та розгортання ефективних автоматичних рішень для захоплення даних.

Доступ до інформації

Для підвищення ефективності поліцейських служб, поліцейські органи повинні забезпечити, щоб офіцери могли отримати своєчасний доступ до коректної інформації. Для цього поліцейський повинен вміти віддалено отримувати доступ до інформаційних систем поліцейських служб і ефективно знаходити інформацію в розподілених середовищах.

Обмін інформацією

Щоб забезпечити співпрацю з громадськістю, приватними та неурядовими організаціями та забезпечити точність і повноту інформації, поліцейські сили повинні мати можливість поділитися надійною і ефективною інформацією з іншими організаціями. Ефективний обмін інформацією вимагає можливості обмінюватися даними у різних форматах і забезпечити пошук даних, що зберігаються в системах поза організацією.

Захист і збереження інформації

Для забезпечення відповідності законодавству і регулятивним зобов'язанням по збереженню якості даних та запобіганню порушень, поліцейські сили потребують ефективного менеджменту корпоративної безпеки. Ефективна організація безпеки побудована на активному управлінні ризиками безпеки, ефективній ідентифікації та визначенні пріоритетності загроз і інформаційної вразливості організації. Захист даних також базується на тому, що користувачі повинні стежити за надійністю правила обробки даних та політики безпеки щоб мінімізувати ризик несанкціонованого доступу до система або до даних. Моделі та рішення управління доступом повинні запобігти несанкціонованому доступу і призначити відповідні дозволи користувачам на основі реального стану функціональних обов'язків.

Керівні принципи дотримання законодавчої, нормативної та законної діяльності

Для забезпечення безпеки особливих даних, управління даними, аудиту і оперативного управління даними, сили поліції вимагають узгодженого підходу до організаційного і інформаційного використання баз даних, що дозволить ефективно застосовувати для співпраці ІТ, поліцейські, адміністративні та функції управління. Для захисту даних, крім того, користувачі повинні стежити за надійністю правил обробки даних та політики безпеки щоб мінімізувати ризики несанкціонованого доступу до даних. Моделі та рішення управління доступом повинні запобігти несанкціонованому доступу, реєстрація записів дозволу доступу користувачів на запити і відповідні робочі функції.

Забезпечення якості інформації

Цінність поліцейського ІТ-підрозділу полягає в тому, що інформація, яку він надає повинна бути точною, значимою і такою що може використовуватися за призначенням. Для забезпечення якісних даних, поліцейські сили повинні забезпечити загальні стандарти введення даних. Ці стандарти повинні підтримуватися додатками які налаштовані для підтримки користувачів. Для забезпечення якості даних в розподілених середовищах також потрібні рішення, які підтримують цілісність переданих даних між системами в повідомленнях.

Ефективне використання інформації

Покращення ефективності послуг поліцейської діяльності, підвищення ефективності поліцейських та адміністративних процесів вимагають від поліцейських сил ефективного аналітичного рішення на основі контролю витрат на забезпечення поліцейських підрозділів якісною інформацією.

-
1. Manuel Sanchez Lopez Police Centre of Excellence Lead
manuel.sanchez.lopez@accenture.com
 2. James Slessor United Kingdom Policing Lead
james.w.slessor@accenture.com

ДЕРЖАВНА ТАЄМНИЦЯ ЯК ОДИН ІЗ ВИДІВ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Лозинський Юрій Романович,

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

Півень Софія Геннадіївна,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

На даний час важливою основою діяльності є забезпечення інформаційних прав осіб. Важливу роль в діяльності держави, суспільства, громадянина відіграє інформація. Від її якості та достовірності, оперативності одержання залежать численні рішення, що приймаються на різних рівнях – від глави держави до громадянина. Суспільство повинно дотримуватися рівності у обміні певною інформацією, а держава має стати захисником у даних відносинах, запровадивши такі механізми, які, по-перше, дозволили громадянам мати повну інформацію для власного розвитку, по-друге, не відчувати пригноблення своїх прав. Одним із таких механізмів і є створення державою системи захисту інформації з обмеженим доступом. Закріплення інформації в ЦК України було зумовлено державною значимістю інформації, її цінністю та необхідністю захисту як нематеріального, вільно розповсюдженого та доступного блага, яке необхідне людині у її життєдіяльності. Специфіка відносин, що складаються в суспільстві з приводу інформації полягає в основі цивільно-правового поняття таємниці, відображає універсальні закономірності, відкриті в інших галузях наукових знань. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні та інші права, свободи, законні інтереси інших громадян.

Проте, віднесення певних відомостей до інформації з обмеженим доступом у будь-якому випадку має бути правомірним, тобто здійсненим чітко у відповідності і на підставі чинних правових норм.

Система державної таємниці – це організаційне утворення, яке повинне створювати заходи для правоохоронних органів, які б конкретизувалися на: захисті державного суверенітету, територіальної цілісності, конституційного ладу, науково-технічного й оборонного потенціалу України, законних інтересів та прав людини, громадянина й держави від розвідувальної діяльності іноземних спеціальних служб; запобігання, припинення та розкриття злочинів проти миру, безпеки людства, тероризму, корупції та інших протиправних дій, що завдають загрозу національній безпеці України. Регулювання відносин у сфері охорони державної таємниці здійснюється відповідно до чинного законодавства України та визначається Конституцією України, Законами України «Про державну службу», «Про інформацію», міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України [2].

Відповідно до Закону України «Про державну таємницю» причиною обмеження доступу до державної таємниці є можливість нанесення шкоди національній безпеці у випадку її розголошення, а також віднесення відомостей до державної таємниці проводиться шляхом визначення можливої шкоди національній безпеці України у разі розголошення даних відомостей. Основою державної таємниці є захист інформації з обмеженим доступом. Науковець Марченко Л. зазначає, що інформація з обмеженим доступом – це інформація доступ до якої є обмеженим згідно із чинним законодавством [3, с.68]. Щоб вирішити питання стосовно державної таємниці, запроваджуються певні етапи, які б могли зупинити та ліквідувати незаконний доступ до закритої інформації у сфері безпеки. Державна політика щодо державної таємниці є основою внутрішньої та зовнішньої політики держави, на мою думку, потрібно покращити умови захисту інформації з обмеженим доступом та перешкодити витоку секретної інформації із різноманітних носіїв. Загалом розрізняють чотири сфери, яких стосується інформація, що становить державну таємницю України, а Звід відомостей ці сфери чітко конкретизує, оскільки складається на основі рішень державних експертів з питань таємниці. В Законі України «Про державну таємницю» міститься норма, яка передбачає створення в органах державної влади, органах

місцевого самоврядування, на підприємствах, в установах, організаціях, що проводять діяльність пов'язану з державною таємницею, розшуково-секретних органів на правах окремих структурних підрозділів[4]. Для кращої роботи розшуково-секретних органів необхідно забезпечити прийняття тих нормативно-правових актів, які б належним чином регулювали допуск до державної таємниці структурних підрозділів, покращити систему захисту секретної інформації. Важливу роль щодо недоліків, які погіршують якість роботи в даній сфері посідає таке питання, як необґрунтована відмова допуску осіб до державної таємниці, яка інколи не виконується. Також порушення умов зберігання секретних документів чи певних матеріалів, відсутність належної охорони, незначна кількість спеціальних приміщень. Суттєвої шкоди національній безпеці може завдати не тільки розголошення державної таємниці, але й втрата її матеріальних носіїв та розвідувальна діяльність іноземних спецслужб (шпигунство), утім, як перелік загроз збереженню державної таємниці в узагальненому вигляді в жодному із законів України це на сьогодні не визначено.

Державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом України «Про державну таємницю», державною таємницею і підлягають охороні державою. Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці [4]. Невідома третім особам інформація дає реальні відомості тільки для їхнього власника.

Таємниця – це, насамперед, інформація, яка повинна бути відома або довірена вузькому колу осіб. Дана інформація не підлягає розголошенню, оскільки це може призвести до настання негативних наслідків (може спричинити матеріальну чи моральну шкоду особам) [2, с.167]. Розголошення державної таємниці можливе лише тоді, коли збирання державної інформації не полягає у використанні відомостей на шкоду суверенітету, територіальній цілісності або зовнішній безпеці [1, с.147 – 151]. Законодавство

передбачено три ступені секретності для інформації, що становить державну таємницю: «особливої важливості», « цілком таємно», «таємно». Строк, протягом якого діє рішення про віднесення інформації до державної таємниці з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності «особливої важливості» - 30 років, для інформації «цілком таємно» - 10 років, для інформації «таємно» - 5 років. Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюється на підставі рішення державного експерта з питань таємниць або на підставі рішення суду [4]. Відомості з різним ступенем секретності мають неоднакове значення для національної безпеки України і, відповідно, передбачається різна відповідальність за порушення законодавства про державну таємницю. Дані вимоги режиму таємності є постійними і загальнодержавними, необхідними для виконання на території України та за її межами органами державної влади і місцевого самоврядування, підприємствами, установами, організаціями незалежно від їх організаційно-правової форми і форми власності, посадовими особами і громадянами України, що взяли на себе зобов'язання виконувати вимоги законодавства про державну таємницю. Допуск до державної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-технічної діяльності або навчання, органами Служби безпеки України після проведення їх перевірки. У сфері захисту інформації з обмеженим доступом сучасне суспільство має право вимагати, щоб законодавство забезпечувало досягнення балансу інтересів громадян, оскільки охорона державної таємниці повинна відповідати інтересам не лише держави, а й суспільства та конкретної особистості. Громадянину як патріоту повинно бути небайдуже і саме збереження державної таємниці, і матеріальні витрати, які несуть держава та суспільство заради підтримки режиму таємності та для ліквідації наслідків розголошення інформації з обмеженим доступом. Однак, постають проблемні питання щодо віднесення тієї чи іншої інформації до категорії «державна таємниця» у зв'язку з відсутністю законодавчо визначених критеріїв оцінки цієї інформації. Кожна держава з метою охорони

інформації, що містить державну таємницю, формує спеціальну систему її захисту. У кожній країні розроблено власні механізми, особливий порядок отримання, обробки, зберігання, захисту та розсекречування інформації. Це пов'язано зі специфікою державного устрою, політичного ладу, традиціями державотворення.

Отже, правовий інститут державної таємниці є найбільш розвинутим у порівнянні з іншими видами інформації з обмеженим доступом. Оскільки, збереження державної таємниці – це одна із гарантій незалежності кожної держави, її недоторканості та безпеки. Основною умовою якої виступає захист національних інтересів та створення належної системи охорони державної таємниці, яка формується на основі законодавчих актів.

-
1. Кучанський С. М. Особливості кримінально – правової охорони інформації з обмеженим доступом (Міжнародний досвід) / С. М. Кучанський // Правова держава. – 2012. – №15. – С. 147 – 151.
 2. Смолькова И. В. Проблемы охраняемой законом тайны в уголовном процессе. – М.: Изд-во Луч, 1999. – 335с.
 3. Семилетов С. И. Информация как нематериальный объект права // Государство и право. – 2000. – №5. – С. 67 – 74.
 4. Про державну таємницю: Закон України від 21.09.1999р. // Відомості Верховної Ради. – 1999. – №49.

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ МЕХАНІЗМУ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ СФЕРОЮ

Лук'янова Галина Юріївна,

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

Завдяки швидкому розвитку інформаційних технологій, збільшення обігу інформації, особливу увагу слід приділяти правовим механізмам, які здатні забезпечити правове регулювання інформаційних відносин, адже сама природа інформації відмінна від інших предметів правового регулювання, а отже не потребує нових, спеціальних механізмів правового регулювання.

Зарубіжний досвід переконує, що держава є ключовим стрижнем у становленні інформаційного суспільства як координатор діяльності учасників інформаційних відносин, як законодавець, що забезпечує правові засади розвитку відповідних правовідносин, юридичний гарант реалізації права на інформацію, здатний захистити суб'єктів права від несанкціонованого доступу до інформації, забезпечити реалізацію права на інтелектуальну власність в інформаційній сфері тощо [1, с. 10].

У юридичній науці під нормативно-правовим регулюванням інформаційної безпеки України пропонується розуміти форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення. Чинне законодавство містить величезний масив норм, які прямо чи опосередковано регулюють діяльність в інформаційній сфері. Чільне місце серед них належить нормам Конституції України, які встановлюють фундаментальні засади розвитку суспільства і держави. Конституція України містить цілий ряд спеціальних норм, що стосуються інформаційної сфери.

Втім, їх аналіз слід почати з важливої конституційної норми, що міститься в ст. 3 Конституції України і закріплює основоположний принцип взаємовідносин суспільства і держави, визначає

головне призначення останньої. Відповідно до цієї норми «права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави..., а утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [2].

Вказане означає, що держава ставить для себе за головну мету в процесі державного регулювання інформаційною сферою забезпечити практичну реалізацію інформаційних прав і свобод людини та їх гарантій, передбачених спеціальними нормами, зокрема ст. 31, відповідно до якої кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції; ст. 32, якою не допускається збирання, зберігання, використання конфіденційної інформації про особу без її згоди; надається право громадянам знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе тощо; ст. 34, якою надається право на свободу слова, на вільне вираження своїх поглядів і переконань, право вільно збирати, зберігати, використовувати і поширювати інформацію [2].

Важливе значення для здійснення державного регулювання інформаційних процесів в країні мають положення ст. 10 Конституції України, яка прямо покладає на державу обов'язок забезпечувати всебічний розвиток і функціонування української мови як державної в усіх сферах суспільного життя на всій території України. Так само ст. 17 Основного Закону визначає, що забезпечення інформаційної безпеки України, поряд із захистом її суверенітету і територіальної цілісності, забезпеченням економічної безпеки, є однією з найважливіших функцій держави [2].

Важливою гарантією вільного і плюралістичного розвитку інформаційної сфери в Україні є норма, закріплена в ст. 15 Конституції України, якою заборонено цензуру. Конституція України містить і ряд спеціальних норм, що стосуються інституційних засад державного регулювання в інформаційній сфері. Це, зокрема норми, закріплені в п. 12, п. 20 ст. 85, п. 13 ст. 106 Конституції, які вказують на особливості формування органів державного управління в інформаційній сфері, таких, приміром, як Національна рада України з питань телебачення і радіомовлення.

Специфіка забезпечення національної інформаційної безпеки знайшла відображення в законах України «Про національну безпеку України», «Про концепцію національної програми інформатизації», «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», а також у затвердженій указом Президента Стратегії національної безпеки України, у зв'язку з реалізацією Стратегії Національна рада безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національний координаційний центр кібербезпеки. Створення такого центру є обґрунтованим, оскільки повноваженнями щодо забезпечення інформаційної безпеки наділена значна кількість державних органів та установ (Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Держспецзв'язку України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство культури України, Міністерство юстиції України та інші).

Значна кількість норм, що регулюють державний вплив в інформаційній сфері, вимагає їх певної класифікації для системного сприйняття. Найбільш доцільним для цілей нашого дослідження є їх розмежування за призначенням в системі державного управління, а також за об'єктом державного регулювання. Залежно від призначення тієї чи іншої правової норми в регулюванні функціонування складових елементів інформаційної сфери ці норми можливо об'єднати в наступні чотири групи:

1) норми, що закріплюють цілі, основні завдання та напрями діяльності держави в інформаційній сфері, визначають основні параметри розвитку останньої. Ця група норм, до яких належать, зокрема норми, закріплені в ст.ст. 3, 10, 17, 31, 32, 34 Конституції України, в ст. 6 Закону України «Про інформацію», в розділах IV, VI Закону України «Про Концепцію Національної програми інформатизації», Законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» та в інших, має цілеспрямовує значення для функціонування всієї системи державного управління в інформаційній сфері;

2) норми, що визначають систему органів (суб'єктів) державного регулювання в інформаційній сфері та їх адміністративно-правовий статус. До таких норм належать вже згадані норми Конституції України, що стосуються Держкомтелерадіо та Національної ради. Правовий статус окремих органів влади визначається і нормами законів. Так, зокрема ст. 20 Закону України «Про Кабінет Міністрів України» серед його повноважень визначено проведення державної політики у сфері інформатизації, сприяння становленню єдиного інформаційного простору та ін.

Важливе місце в цій групі норм займають також норми, закріплені в підзаконних нормативно-правових актах, передусім, ті з них, що містяться в актах Президента України та Кабінету Міністрів України, якими визначається адміністративно-правовий статус міністерств, інших органів державного управління в інформаційній сфері;

3) норми, що регулюють порядок взаємодії органів (суб'єктів) влади з керованими ними суб'єктами інформаційних та інформаційно-інфраструктурних відносин в процесі реалізації прямих і зворотних зв'язків між ними. До цієї групи належать норми, які регламентують процедури застосування різних методів державного регулювання в інформаційній сфері, визначають форми їх реалізації. Такі норми, закріплені, наприклад, в ст.ст. 23–37 Закону «Про телебачення і радіомовлення», які регламентують процедуру здійснення такого методу регулювання як ліцензування в галузі телебачення і радіомовлення. В Законі України «Про друковані засоби масової інформації (пресу) в Україні» врегульовано порядок здійснення обов'язкової державної реєстрації друкованих засобів масової інформації. У ст. 22 Закону «Про державну таємницю» регламентовано порядок надання допуску громадян до державної таємниці. Застосування цілої низки заходів адміністративного примусу врегульовано нормами Кодексу України про адміністративні правопорушення. У цих же законах та інших нормативно-правових актах визначаються і вимоги до форми правових актів, що приймаються при застосуванні зазначених методів. Закон «Про доступ до публічної інформації», яким встановлено більш ефективні механізми звернення до органів державної влади для отримання інформації, яка перебуває в їх розпорядженні;

4) норми, що визначають адміністративно-правовий статус суб'єктів інформаційних відносин. Так, наприклад, ст. 39 Закону України «Про телекомунікації» на операторів телекомунікацій покладаються обов'язки: своєчасно надавати щорічно до центрального органу виконавчої влади в галузі зв'язку інформацію про свої телекомунікаційні мережі для відпрацювання мобілізаційних планів; за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів тощо.

Таким чином, нормативно-правова регламентація формування єдиного інформаційного простору України повинна сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні. Важливість проблеми розвитку законодавства у сфері інформації та інформаційної безпеки, становлення інформаційного суспільства визначається тією обставиною, що норми законів цієї сфери суттєво впливають на законодавче регулювання відносин суб'єктів у всіх сферах життя держави.

-
1. Вознесенська О.А. Механізм державного регулювання в галузі аудіовізуальних засобів масової інформації. Часопис Академії адвокатури України. 2010. № 2(7). С. 10–1.
 2. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28.06.1996 / URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр>.

АНАЛІЗ СУЧАСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАКОРДОННИХ ЮРИДИЧНИХ ФІРМ ТА ПРИВАТНИХ ЮРИСТІВ

Магеровська Тетяна Валеріївна,

*доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук, доцент*

Пукач Петро Ярославович,

*завідувач кафедри обчислювальної математики та програмування
Національного університету «Львівська політехніка»,
доктор технічних наук, професор*

Пелех Ярослав Миколайович,

*доцент кафедри обчислювальної математики та програмування
Національного університету «Львівська політехніка»,
кандидат фізико-математичних наук, доцент*

Сьогодні успіх в юридичній практиці прямо залежить від того, які інструменти юристи використовують у своїй роботі. Працювати в 21 сторіччі і не користуватися спеціальними додатками вже стає не те що неправильно, а навіть є економічною помилкою.

Той правник, який буде використовувати спеціальне забезпечення, завжди буде продуктивнішим за того, хто цього не робить.

На сьогоднішній день, юристи за кордоном широко використовують інформаційні технології незалежно від їх віку, статусу та юридичної практики. При чому, юридичні компанії надають не лише юридичні послуги. За кордоном це також прибуткова справа, бізнес.

В теорії, програмне забезпечення організації юридичної діяльності починає приносити результат у довготривалій перспективі. Найбільш корисним таке програмне забезпечення буде для:

- молодих юристів що відкриватимуть власний кабінет;

- невеликих юридичних компаній, які повинні настроїти свої виробничі процеси, й попри те мають кваліфікований персонал;
- фірм, що шукають засоби для покращення існуючих систем програмного забезпечення.

Великі компанії, в свою чергу, мають свої рішення, зумовлені контрактами та корпоративними стандартами. Також, переважно, такі компанії мають IT-підрозділ, що розробляє для їхніх правників вузькоспеціалізоване програмне забезпечення. Дані програми у вільному доступі не знайти.

В загальному, можна виділити 6 груп інформаційного програмного забезпечення, яке буде корисне юристам:

- програмне забезпечення ведення часу й витрат для юристів;
- програмне забезпечення ведення документів (розпізнавання символів, презентації, тощо);
- програмне забезпечення для конвертування у .pdf-формат;
- ведення документообігу, автоматизація та збірка документів;
- рішення для ведення юридичних послуг;
- системи управління відносинами із клієнтами (CRM).

Програмне забезпечення ведення часу й витрат для юристів

Для юристів вкрай необхідно вести статті розходів та часозатрат. За кордоном часто використовують такі системи як Freshbooks, QuickBooks, Quicken, Херо. Вони не є вузькоспеціалізованими та використовуються на загальних основах багатьма компаніями. Проте, для ведення юридичної діяльності переважно використовується більш вузьконаправлене програмне забезпечення. Воно забезпечує такі особливості закордонної юридичної діяльності як:

- ведення часових затрат, видача рахунків, базовий підрахунок для бізнесу, тощо;
- функції генерування звітів;
- розділений менеджмент для довірених та IOLTA рахунків;
- можливість фільтрування по рахунках кожного із працівників підприємства;

- можливість фільтрування рахунків за часом, статусом про оплату, тощо;
- можливість приймати розрахунки карткою, та через платіжні системи echeck, PayPal, та Square;
- можливість ведення безпечного діалогу із клієнтами, що стосується пересилання рахунків, тощо.

Найбільш популярними система на зарубідному ринку програмного забезпечення для юристів є Bill4Time та Amicus Attorney.

Bill4Time – це програмне забезпечення, що базується на хмарних технологіях та дозволяє вести витрати часу та коштів, виписувати рахунки та чеки, а також вести менеджмент підприємства в залежності від версії продукту. Для юридичної практики використовують «the law firm edition». Систему розроблено для використання малими компаніями або приватними особами. Також вона має 30 днів пробного періоду.

Amicus Attorney є десктопним рішенням із подібним до bill4time функціоналом. Попри нижчі рейтинги (середня оцінка продукту – 3,4) продукт можна використовувати підприємствам де є вимоги до безпеки даних та обмежений доступ до мережі інтернет.



Рис. 1. Веб-інтерфейс системи bill4time

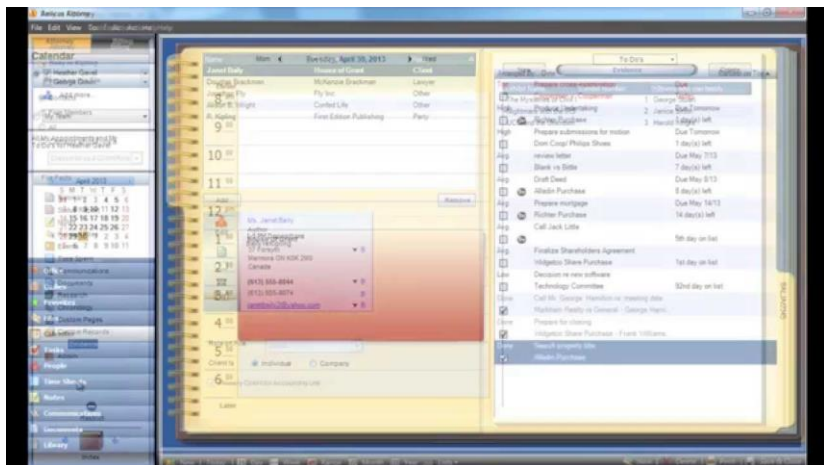


Рис. 2. Інтерфейс системи Amicus Attorney

Програмне забезпечення ведення документів

Для задоволення вимог невеликого юридичного підприємства та приватного зарубіжного юриста немає відмінностей між нашими умовами. Використовується платна ліцензія MS Office – Office 365. Також варто зазначити плагін G-Suite. Він дозволяє вести та зберігати документи з допомогою сервісів Google: docs, tables, gmail, тощо.

Програмне забезпечення для конвертування у .pdf-формат

Даний тип програмного забезпечення необхідний юристам для укладання документів, що друкуватимуться. Також корисною особливістю буде конвертація pdf у текстовий формат із метою редагування документа. Спеціалізоване програмне забезпечення не потребується, як й інші використовують продукти компанії Adobe – PDF та Acrobat Reader.

Ведення документів, автоматизації та їх збірка

Даний тип програмного забезпечення необхідний у юридичній практиці, оскільки вона передбачає ведення великої кількості документації. Для правника, що веде понад 1000 документів водночас, можливість автоматизованого менеджменту документообігу є вкрай необхідною. Для цього є корисними такі опції:

- плагіни для використання текстових процесорів;
- сумісність із сервісами хмарного зберігання даних;
- шаблонування;
- користувацька підтримка;
- система контролю версій;
- можливість доступу до документів без підключення до мережі;
- розширені можливості пошуку і категоризації.

Найбільш широко використовуваними у юридичній практиці системами є HotDocs та The Form Tool.

HotDocs – система генерування документів. Вона дозволяє створювати документи з чистого листа, або готового джерела. До плюсів даної системи можна віднести:

- кінцевий користувач може дуже швидко згенерувати документ;
- шаблони легко змінювати, є багато можливостей для цього;
- швидкість роботи системи;
- при отриманні даних з іншої системи, визначає потреби користувача задаючи їм питання.

Недоліками системи є:

- високий поріг входження у розробку шаблонів;
- вартість програмного продукту є високою навіть для зарубіжних компаній, особливо за необхідності створювати власні шаблони;
- старі версії не працюють із новими версіями Microsoft Office.

Порівняно із HotDocs, The Form Tool надає менш просунутий функціонал, проте вона не потребує від користувача програмістських навичок, й загалом є більш зручною. За рейтингом користувачів система отримала 4.5 зірок з 5 на основі 99 оцінок.

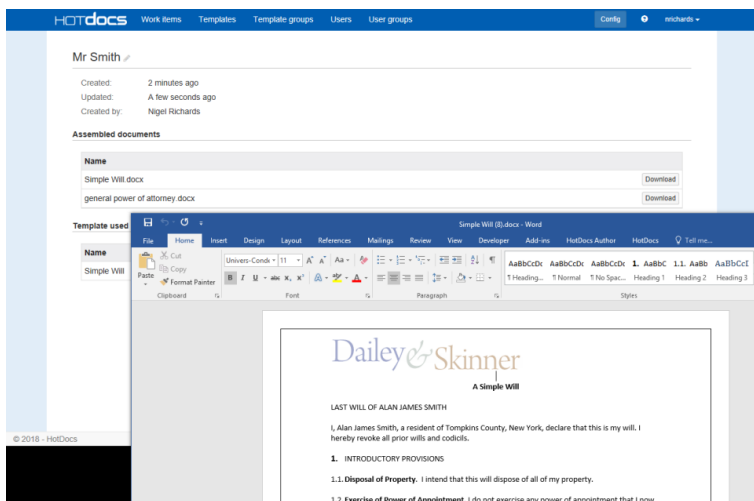


Рис. 3. Приклад роботи системи HotDocs

Рішення для ведення юридичних послуг

На сьогоднішній день, більшість невеликих зарубіжних компаній використовують системи LexisNexis та Westlaw. Окрім того, що дані системи базуються на зарубіжній законодавчій базі, а також високій вартості таких рішень – використання такого роду інформаційних систем значно би полегшило роботу українським особам та організаціям, що займаються наданням юридичних послуг.



Рис. 4. Система LexisNexis

Системи управління відносинами із клієнтами

Для зарубіжних юристів репутація грає ключову роль. Для цього необхідно щоб зв'язок із клієнтами був правильно налагоджений, а також повинно вести детальну статистику відносин із клієнтами для покращення їх обслуговування. Правнику немає потреби зберігати всю інформацію про клієнта, проте використання CRM дозволить мати всі контакти у потрібному місці, а також отримувати звіти про якість роботи із клієнтами та що можна покращити. Корисними функціями CRM для ведення юридичної діяльності є:

- документування телефонних розмов;
- збереження нотаток наданих клієнтом або працівником;
- візуальні звіти;
- інтеграція у соціальні мережі;

Із систем загального користування можна виділити Salesforce, із вузькоспеціалізованих західні спеціалісти виділяють систему Ignite by Avvo.

Також характеризують Salesforce як надпотужну CRM, яка дозволяє надавати кваліфікаційну підтримку користувачів. Також вона позитивно оцінена кінцевими споживачами (4.5/5 на основі 9432 оцінок). Головним мінусом даної системи є доволі високий поріг входу, що обмежує її використання на початках власної кар'єри або компанії.

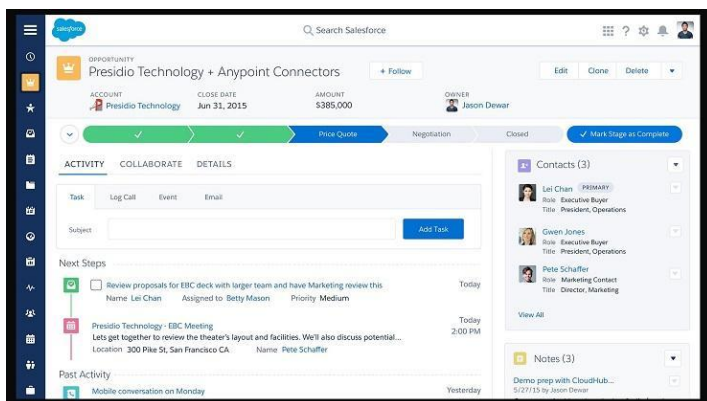


Рис. 5. Інтерфейс Salesforce

Ignite by Avvo є менш просунутим засобом порівняно із Salesforce, проте вона широко використовується юристами через орієнтир системи на їхні потреби.

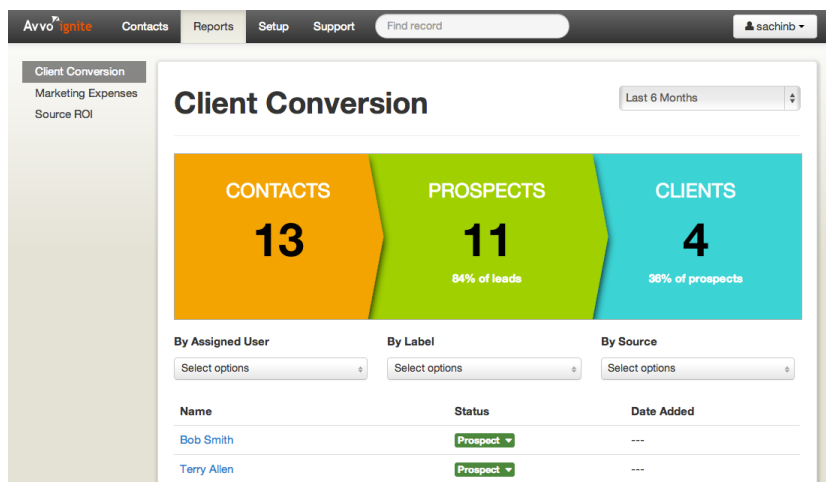


Рис. 6. Інтерфейс Ignite

Висновок. Незважаючи на розповсюдження допоміжних систем у зарубіжній юридичній практиці, найбільшу роль і надалі відіграє веб-сторінка та репутація юриста. Проте, за наявності інформаційного забезпечення, описаного у цій роботі, ведення юридичної справи може значно прискоритися, а також за правильного використання може зрости якість обслуговування кінцевого клієнта і прибуток компанії. Дані системи варто використовувати підприємствам з надання юридичних послуг, а також приватним юристам якщо вони мають змогу оплатити ліцензію.

ДЕЯКІ АСПЕКТИ АНАЛІЗУ ЗЛОЧИННОСТІ З ВИКОРИСТАННЯМ СЕРЕДОВИЩА R

Мандзюк Тетяна Василівна,

здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ

Неспляк Дмитро Михайлович,

доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук

Тучапський Роман Ігорович,

науковий співробітник відділу моделювання композитних структур
і складних систем, кандидат фізико-математичних наук
Інституту прикладних проблем механіки і математики
ім. Я. С. Підстригача НАН України

Бичинюк Ігор Васильович,

викладач кафедри інформатики
Львівського державного університету внутрішніх справ

Аналіз злочинності є функцією правоохоронних органів, яка передбачає системний аналіз для виявлення тенденцій у сфері злочинності. Інформація про типові ситуації може допомогти правоохоронним органам більш ефективно розподіляти ресурси та допомагати детективам у виявленні та затриманні підозрюваних. Аналіз злочинів також відіграє роль у вирішенні проблем злочинності та формуванні стратегій попередження злочинності.

Аналіз злочинів може відбуватися на різних рівнях, включаючи тактичні, оперативні та стратегічні. Аналітики з питань злочинності аналізують звіти про злочини, звіти про арешти, а також максимально швидко виявляють нові моделі та тенденції. Вони аналізують ці явища для всіх чинників та іноді прогнозують майбутні події. Потім вони працюють з поліцейськими установами для розробки ефективних стратегій і тактики для подолання злочинів. Інші обов'язки аналітиків з питань злочинності можуть

включати підготовку статистики або карти на вимогу; підготовку інформації для громадських та судових виступів; відповіді на запити громадськості та преси.

Політика прогнозування є багатовимірною проблемою оптимізації, коли правоохоронні органи намагаються ефективно використовувати обмежений ресурс для мінімізації випадків злочину. У спробі вирішити проблему в реальному світі наша основна увага зосереджується на аналізі даних. Аналіз злочинів включає в себе вивчення даних з двох різних вимірів – просторового та часового. Просторовий вимір включає в себе спостереження за характеристиками певного регіону поруч із сусідами. Часовий вимір включає в себе спостереження за характеристиками певного регіону за часом. Тоді питання полягає в тому, наскільки далеко від епіцентру ми шукаємо аналогічні моделі і як далеко в часі з дати події ми хочемо відобразити тенденцію. В ідеалі ми хотіли б отримати максимально можливі дані. І це робить аналіз даних творчим процесом, що пов'язаний математичною логікою і зосереджений на статистичній достовірності. Обробка просторових і часових атрибутів є складним завданням.

Перед тим як розпочати аналіз даних ми імпортуємо їх в R Studio. Це можна зробити використавши функцію `read.csv()`. Однак, ми не можемо негайно розпочати аналіз даних без інформації про структуру наших даних. За допомогою функції `str()` ми можемо бачити, які типи даних та поля присутні в наборі даних. [1, 2] Щоб визначити загальні характеристики даних, ми можемо запустити команду `summary()`. Для того щоб побачити перші декілька спостережень даних/стовпця можна скористатись функцією `head()`. Візуалізація даних здійснюється за допомогою функцій `plot()` та `ggplot()`. [3, 4]

Використання сучасного спеціалізованого середовища обробки статистичних даних R Studio суттєво спрощує і полегшує аналіз кримінальних даних.

-
1. John M. Quick. The Statistical Analysis with R Beginners Guide. Packt Publishing, 2010. – 300 p.

2. Matthias Kohl. Introduction to statistical data analysis with R. bookboon.com, London, 2015. – 228 p.
3. Thomas Rahlf. Data Visualisation with R. Springer International Publishing, New York, 2017. – 385 p.
4. John Maindonald and John Braun. Data Analysis and Graphics Using R. Cambridge University Press, Cambridge, 2nd edition, 2007. – 549 p.

ПРО КРИТЕРІЇ ЕФЕКТИВНОСТІ ФОРМ ЗАХИСТУ АВТОРСЬКИХ ПРАВ

Миджсин Галина Євгенівна,

*аспірант кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ*

В умовах реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, порушення авторських прав і законних інтересів різних учасників правовідносин у сфері авторського права актуалізували проблеми захисту та підвищення ефективності захисту. Основні напрями роботи у зазначеній сфері визначені у статті О. П. Орлюк «Захист прав інтелектуальної власності в контексті європейської інтеграції» [1].

Матеріали правозастосовної (судової та адміністративної) практики свідчать про недостатню якість правозахисних механізмів, підбиваючи до необхідності пошуку шляхів і способів вдосконалення форм захисту авторських прав і законних інтересів авторів. З двох категорій «механізми» і «форми» захисту, перша вживається значно частіше другої, відноситься до числа найбільш апробованих і науково розроблених. Виходить слід із співвідношення як цілого і частини: форми захисту включені в категоріальний апарат механізмів, являють собою певний його структурний елемент, ефективність якого залежить від системи оціночних критеріїв.

Вибір форм захисту зумовлюється різними факторами і обставинами, що можуть служити підставами (критеріями) класифікації. Захист авторських прав та законних інтересів авторів забезпечується та здійснюється з використанням різних, встановлених законом процедур, правил, способів, прийомів, їх застосовують суб'єкти, наділені відповідними повноваженнями, які реалізують захисні функції. Сукупність усіх дій, що виконуються в ході захисту авторських прав та законних інтересів авторів (далі – захисту прав та законних інтересів) традиційно об'єднується

визначенням форм захисту, починаючи з самозахисту та завершуючи формалізацією діяльності офіційних державних органів і посадових осіб.

Часто форми захисту зорієнтовані на правозахисну діяльність різних суб'єктів з державним чи громадським статусом. Від цілей і завдань цих суб'єктів, змісту функцій та повноважень залежить ефективність застосовуваних форм.

Найбільш ефективними визнаються форми захисту, що використовуються органами державної влади: судової, виконавчої, законодавчої. Помітною і ефективною все частіше виявляється захисна робота громадських організацій.

В останні роки помітно зростає авторитет форм, застосовуваних у межах громадських правозахисних механізмів. У такій якості розглядається діяльність трьох рівнів громадських організацій, різних громадських рад при офіційних владних структурах, інститутів уповноважених, сформованих з різних сфер реалізації прав і свобод суб'єктів права, інститутів громадянського суспільства.

Зростає авторитет не тільки історично сформованих інститутів громадянського суспільства, які отримали визнання держави. Все частіше надії на ефективний захист постраждалих суб'єкти – фізичні і юридичні, покладають на інститути, трансформовані в діалоговий формат. Організація, результативність і відновні наслідки таких форм привертають все більше уваги.

Інституціоналізація правозахисних механізмів, а конкретніше – механізмів захисту прав суб'єктів авторських правовідносин, що склалося в останні десятиліття минулого століття, сьогодні тісно кореспондує з ознаками та компонентами концепції правової держави. З цим має бути пов'язане пояснення критеріїв ефективності всіх елементів механізму, включаючи форми захисту.

Формування механізму захисту відбувалося в умовах гострих наукових дискусій, концептуальних і аргументаційних протиріч, що з неминучістю позначається на такому елементі, як форми захисної діяльності, які часом пропонуються розглядати на противагу механізмам, а не в їх єдності.

Необхідність адаптації національного законодавства до вимог Європейського Союзу представляє підхід до визначення механізмів і форм захисту як інтегрування регулюючих, право-реалізуючих, правоохоронних та правозахисних механізмів і форм. У сукупності вони спрямовані на досягнення мети вирішення конфлікту різних інтересів і відновлення балансу. Інтегративний підхід дає можливість вбачати сумісність перерахованих елементів з елементами гуманітарного правозахисного механізму (позиціонується інакше як «механізм охорони і захисту прав людини»), запропонованого в юридичній науці П. М. Рабіновичем [3, с. 3]. Крім цього інтеграція забезпечує орієнтацію на прогресивні та ефективні форми взаємодії особи, суспільства та держави, на пошук оптимальних моделей такої взаємодії.

Пропонована модель націлена на виконання державою забезпечувальної функції, на створення дієвої системи захисту прав і свобод, на встановлення юридичних процедур захисту. Концептуальне наповнення даної моделі слід забезпечити обґрунтуванням причин неефективності форм захисту, що застосовуються в практиці. Як зазначає О. П. Орлюк, що у професійному середовищі схиляються до думки, що функції із виявлення порушень у сфері інтелектуальної власності мають перейти до правоохоронних органів. Для цього у їх структурі необхідно створити спеціалізовані відділення чи служби, які опікуватимуться захистом прав інтелектуальної власності: від виявлення та фіксації порушень до доведення справ до суду і покарання винних [4].

У їх числі: неякісний стан законодавства, відсутність належних заходів юридичної відповідальності та процедур застосування до порушників прав і законних інтересів суб'єктів авторських прав і до тих, на кого покладено обов'язок захищати та відновлювати порушені права; суперечливість в можливості застосування різних санкцій, що дозволяє не захищати та відновлювати порушені права, а посилювати положення постраждалих за рахунок поліпшення становища порушників; корупція не тільки у владних структурах, а й в діяльності громадських утворень; криміналізація правозахисних механізмів, обумовлена залученням до діяльності осіб з кримінальним минулим і відповідними інтересами; нерозв'язний характер конфлікту окремих категорій інтересів, що

вимагає застосування складних механізмів державного примусу при відсутності таких в законодавстві країни; неприпустимо низька правова інформованість і правова культура основної маси населення; посилення соціального розшарування суспільства.

Перераховані причини можуть бути нівельовані проведенням масштабних реформ в економічній, політичній, соціальній, духовній сферах життя, реформ, науково обґрунтованих з урахуванням національного та зарубіжного досвіду, з включенням ряду заходів. Наприклад: реформування законодавства, всіх правових явищ на оновленому правовому просторі; організація масової якісної освіти і освіти з питань захисту прав і законних інтересів; вдосконалення контрольних механізмів, підвищення ефективності форм і методів контролю в сфері захисту прав та законних інтересів суб'єктів різних видів правовідносин у сфері авторського права; розробка та реалізація програм, способів, прийомів боротьби з корупцією, посилення відповідальності винних на принципах пропорційності вчиненого заходам юридичної відповідальності; реалізація комплексу принципів соціальної справедливості в усіх відновних процесах на основі оновленого та вдосконаленого законодавства і інші заходи.

Запропоновані напрями та заходи потребують концептуального та методологічного опрацювання на основі сучасних досягнень юридичної науки. В основу реформ повинні бути покладені пріоритети управління, сформовані в Європейському Союзі – факторна обумовленість, світоглядна стабільність, соціальна збалансованість, матеріально-енергетична достатність, паритетність в досягненні компромісу інтересів.

-
1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 № 1678-VII. Відомості Верховної Ради України. 2014. № 40. Ст. 2021.
 2. Орлюк О. П. Захист прав інтелектуальної власності в контексті європейської інтеграції. Вісник Національної академії правових наук України. 2016. № 3. С. 58-74.

3. Рабінович П. М. Права людини та їх юридичне забезпечення (основи загальної теорії держави та права). Київ : НМК ВО, 1992. 100 с.
4. Орлюк О. П. Як «авторські» норми, підтримані Європарламентом, вплинуть на Україну. 17.09.2018. Укрінформ. URL. <https://www.ukrinform.ua/rubric-society/2538342-ak-avtorski-normi-pidtrimani-evroparlamentom-vplinut-na-ukrainu.html> (дата звернення 08.12.2018)

ІНФОРМАЦІЙНА СИСТЕМА ПОШУКУ ПАРКОМІСЦЬ

Мельничин Андрій Володимирович,

*доцент кафедри теорії оптимальних процесів
Львівського національного університету імені Івана Франка,
кандидат технічних наук, доцент*

Однією з актуальних проблем сьогодення, що гостро стоїть у великих містах, є облаштування паркінгів у громадському просторі не лише Львова, з урахуванням особливостей його історичної забудови, а й інших великих міст України.

У запропонованому дослідженні використовується підхід, який ґрунтується на детальній імітації паркомісць міста комп'ютерною програмою. Використання такого підходу дає можливість залучати для аналізу значно більше важливих інформаційних даних таких як, наприклад, відведений та залишковий час перебування автомобіля на паркомісці, розпізнавання вільних та зайнятих паркомісць. У програмній реалізації відбувається формування об'єкту із заданими координатами паркомісць, де зайняте паркомісце позначене червоним кольором, а вільне зеленим. Системою визначається місцезнаходження автомобіля, для якого потрібно знайти вільне паркомісце. Користувач має можливість бачити усі паркомісця, відрізнити вільні від зайнятих, отримати інформацію про залишковий час на вибраному місці. Також візуально зображено оптимальний шлях, за яким користувач може здійснювати рух.

Для розробки основної частини програмної реалізації використано *Google Maps JavaScript API*. Код *JavaScript* для *Google Maps API* завантажено у форматі, який відповідає <https://maps.googleapis.com/maps/api/js>. Як додатковий елемент – реалізовано кластеризацію маркерів (у даному конкретному випадку – це місця для паркування). Щоб об'єднати близько розташовані маркери в кластери і спростити їх відображення на карті, використано бібліотеку *MarkerClusterer* в поєднанні з *Google Maps JavaScript API*. Слід зауважити, що при збільшенні масштабу для пунктів з кластерами, останні починають розпадатися: числа на кластерах зменшуються, а на карті з'являються

окремі маркери, що забезпечує кращу деталізацію відображених об'єктів. Розглянемо детальніше ключові моменти реалізації.

Розташування користувача.

Для додавання розміщення користувача реалізовано функцію *addMarker*, яка викликається при перехопленні події «*OnClick*». Функція приймає координати кліку та перемальовує маркер. Позначка місцезнаходження зображена як стрілка чорного кольору, яка й відображатиме користувача системи на карті.

Відображення паркомісць.

Функція *setMarkers*, яка промальовує усі паркомісця на карті *Google Maps*. Координати маркерів збережені в масиві у файлі *locations.js*.

Під час ініціалізації програми, кожному паркомісцю виділяється залишковий час для перебування автомобіля на вказаному місці та максимально можливий час (зараз це 2 години). Залишковий час задається випадковим чином та зберігається в масиві *timestampArray*.

У момент промальовки кожного маркера функція *setIconByTime* перевіряє виділений час. Якщо залишковий час дорівнює нулю, то функція додає іконку зеленого кольору, якщо ні, то червоного. Також додано інформаційне вікно для кожного маркера, щоб користувач міг бачити скільки часу залишається на перебування автомобіля на тому, чи іншому місці (див. рис. 1.)

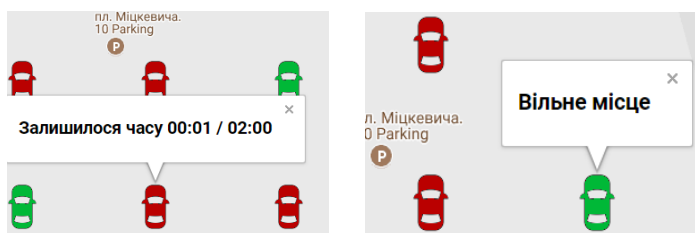


Рис. 1. Вільне та зарезервоване паркомісце.

Програма у режимі реального часу змінює в масиві *timestampArray* час та, в разі потреби, перемальовує маркери використовуючи функцію *updateMarker*.

Пошук найближчого вільного паркомісця.

Для обчислення найкоротшого шляху (геодезичної лінії) розроблено функцію `findClosestMarker`, яка відсікає усі зайняті місця та викликає метод `computeDistanceBetween` для кожного вільного місця. Таким чином функція `findClosestMarker` знаходить найближчий маркер та передає його ідентифікатор. У цьому випадку ідентифікатор користувача з'являється біля паркомісця і відображається відлік часу.

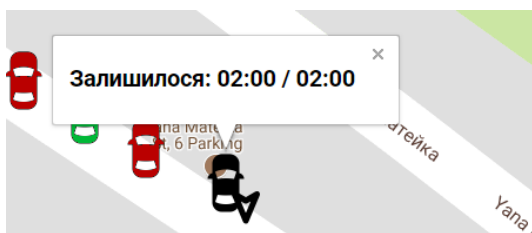


Рис. 2. Користувач «припаркувався».

Промальовування маршрутів.

Для використання маршрутів, створено об'єкт типу *Directions Service*, який містить результат запиту маршрутів, що автоматично забезпечить відображення результату на мапі (див. рис. 3).

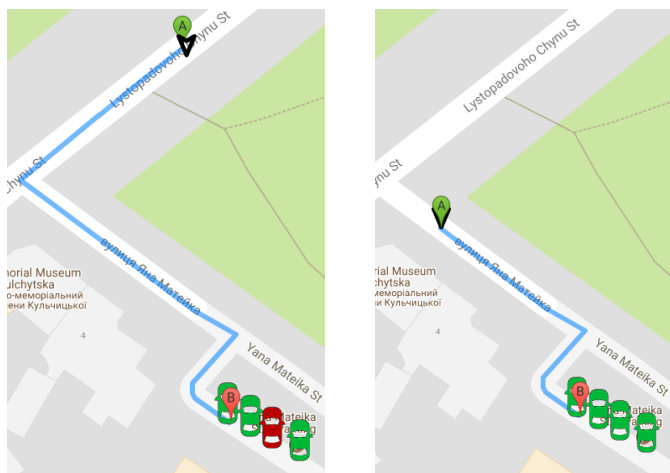


Рис. 3. Прокладений початковий та оновлений маршрути.

Робота застосунку починається із завантаження та вибору ділянки, де потрібно знайти парковку (рис. 4.), після чого встановлюється місце розташування користувача і відбувається промальовування маршруту (рис. 5.).



Рис. 5. Фрагмент карти із зображеними паркомісцями.

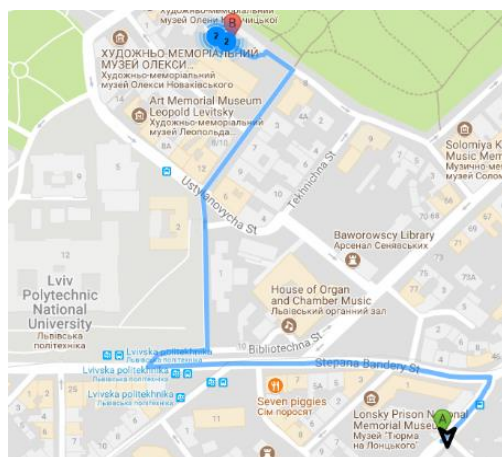


Рис. 5. Прокладений маршрут.

У даній роботі спроектовано та реалізовано модель системи забезпечення паркомісць міста для пошуку найближчого вільного місця та прокладання шляху до нього. Програмна реалізація є зручна в користуванні, оскільки користувач має можливість здійснити пошук оптимального шляху, а також бачити усі паркомісця, відрізняти вільні від зайнятих.

-
1. Geocoding Service [Электронный ресурс] – Режим доступа: <https://developers.google.com/maps/documentation/javascript/geocoding>. – Назва з екрана.
 2. Geometry Library [Электронный ресурс] – Режим доступа: <https://developers.google.com/maps/documentation/javascript/geometry>. – Назва з екрана.
 3. Marker Clustering [Электронный ресурс] – Режим доступа: <https://developers.google.com/maps/documentation/javascript/marker-clustering>. – Назва з екрана.

ПРОБЛЕМНІ АСПЕКТИ ОПЕРАТИВНОГО РЕАГУВАННЯ ПОЛІЦІЇ ЗА ФАКТОМ СПРАЦЮВАННЯ ЕЛЕКТРОННИХ БРАСЛЕТІВ, ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАПОБІЖНОГО ЗАХОДУ В ЧАСТИНІ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ЗА МІСЦЕЗНАХОДЖЕННЯМ ОСІБ ЗА УХВАЛОЮ СЛІДЧОГО СУДДІ

Перепьолкіна Юлія Андріївна,

*здобувач ступеня бакалавра Дніпропетровського державного
університету внутрішніх справ*

Кононець Віта Петрівна,

*доцент кафедри адміністративного права, процесу та
адміністративної діяльності Дніпропетровського державного
університету внутрішніх справ, кандидат юридичних наук*

Правоохоронна функція є однією з основних функцій держави, реалізація якої здійснюється завдяки визначеним законом суб'єктами, що здійснюють правоохоронну діяльність на основі певних принципів та чітко визначеними методами та засобами, тобто законодавець чітко визначив, що центральним елементом в механізмі реалізації правоохоронної функції держави виступає правоохоронна система [1].

Саме задля виконання державою своїх основних функцій різними органами та підрозділами існують певні засоби, які полегшують та сприяють зазначеному процесу. Для прикладу можна взяти електронні засоби контролю.

Застосування електронних засобів контролю (далі - ЕЗК) полягає в закріпленні на тілі підозрюваного, обвинуваченого електронного пристрою, який дає змогу відслідковувати та фіксувати його місцезнаходження. Згідно з Порядком застосування електронних засобів контролю, затвердженого Наказом МВС України від 08.06.2017 №480 метою застосування ЕЗК є забезпечення виконання обов'язків, що покладаються на підозрюваного, обвинуваченого ухвалою слідчого судді, суду про застосування

запобіжного заходу, не пов'язаного з позбавленням волі або у вигляді домашнього арешту [2]. Досліджуючи теорію та практику кримінальної процесуальної діяльності органів досудового розслідування, можна помітити, що існує багато проблемних питань, пов'язаних із застосуванням ЕЗК, таких як нормативно-правові, організаційні, фінансового та матеріально-технічного забезпечення проблеми нормативно-правового забезпечення. Вони полягають в тому, що загалом кримінально-процесуальне законодавство України не завжди відповідає стандартам і вимогам де досить чітко встановлюються критерії застосовування засобів електронного контролю в конкретних ситуаціях розслідування. Так, у США електронні браслети носять особи, підозрювані чи вже засуджені за викрадення автомобілів, за злочини, пов'язані з наркотиками, а також особи, що порушують правила дорожнього руху чи зловживають алкогольними напоями. Тобто основним критерієм застосовування ЕЗК в США є тяжкість вчинення кримінального правопорушення. На відміну від цього, в Україні ЕЗК застосовуються лише з урахуванням виду запобіжного заходу, не враховуючи ступеня тяжкості кримінальних правопорушень. У випадку їх застосування разом із запобіжним заходом у вигляді домашнього арешту зрозуміло, що ЕЗК будуть відповідно носити підозрювані, обвинувачені у вчиненні злочину, за вчинення якого законом передбачено покарання у виді позбавлення волі, як це визначено КПК України. А у випадках застосування ЕЗК для забезпечення виконання обов'язків, що покладаються на підозрюваного, обвинуваченого ухвалою слідчого судді, суду про застосування запобіжного заходу, не пов'язаного з позбавленням волі, не визначено ступеня тяжкості злочину, за підозрою або обвинуваченням в якому особу можуть зобов'язати носити ЕЗК. На мій погляд, необхідно було б конкретно визначити в КПК України, що ЕЗК можуть застосовуватися лише у кримінальних провадженнях щодо злочинів, за які передбачено покарання у виді позбавлення волі. Проблеми організаційного забезпечення полягають у невизначеності суб'єктів контролю за дотриманням підозрюваними, обвинуваченими обов'язків щодо носіння ЕЗК. Ані в КПК України, ані в Порядку застосування електронних засобів контролю не встановлено конкретний підрозділ Національної поліції, що має здійснювати контроль за виконанням підозрюваними,

обвинуваченими обов'язку носити ЕЗК, адже вказано, що такі функції покладаються на «поліцейського, який виконує ухвалу». Доцільно було б таку контролюючу функцію покласти на працівників оперативних підрозділів або дільничних офіцерів поліції, які б уже безпосередньо на місцях перевіряли дотримання підозрюваними, обвинуваченими правил користування ЕЗК.

Проблемним питанням при застосуванні ЕЗК на території України є значна вартість ЕЗК [3]. На мою думку, альтернативним варіантом могло б стати налагодження власного виробництва ЕЗК, внаслідок чого б їх вартість набагато знизилась, що дозволило б економити кошти Держбюджету та водночас збільшити кількість та покращити якість ЕЗК. Недоліки матеріально-технічного забезпечення полягають у неналежній якості електронних браслетів, що проявляється в тому, що більшість з них є ненадійними і швидко виходять з ладу.

Підсумовуючи вищевикладене, можна зробити висновки, що застосування електронних засобів контролю за особою в кримінальному процесі України є певним нововведенням, тому широкого поширення і великої частоти застосування вони не набули, зокрема через наявність багатьох невіршених питань у нормативно-правовому, організаційному, фінансовому та матеріально-технічному забезпеченні. Такі нововведення потребують певного коригування на законодавчому рівні, а також створення сприятливих умов, для ефективного застосування ЕЗК, тобто, щоб воно виконувало на належному рівні функцію технічного засобу забезпечення реалізації запобіжних заходів. Україна має спрямовувати зусилля для вирішення цих питань, щоб покращити якість ЕЗК, можливо і налагодити їх власне виробництво, збільшити варіанти застосування таких засобів, у тому числі й при відбуванні покарання у вигляді обмеження волі. «Електронні браслети» є ефективним засобом лише в тому випадку, коли вони є якісними та сертифікованими та контролюючі органи вміють користуватися ними належним чином. Зачасту не всі співробітники поліції мають навички користування такими приладами, що призводить до того, що підозрюваний може самостійно зняти браслет та покинути приміщення в якому повинен перебувати. Також можна зазначити про проблему якості засобів, які надаються для

виконання завдань поліцією – не всі електронні засоби є якісними. Це пояснюється тим, що можливо, через недобросовісність, було закуплено більш дешеві та неякісні браслети, що не є ефективними. Неефективність «електронних браслетів» пояснюється ще й їхньою недостатністю. Адже на їх закупівлю потрібні значні кошти, які не завжди виділяються. Щоб хоч якось подолати цю проблему, пропонуємо не обмежуватися лише цих засобом контролю. Можливі та навіть більш ефективніші раптові відвідування підозрюваного або дзвінки чи опитування сусідів.

-
1. Конституція України // Відомості Верховної Ради України від 23.07.1996 – 1996 р., № 30. – Ст. 141.
 2. Наказ Міністерства внутрішніх справ України від 08.06.2017 №480 «Про затвердження Порядку застосування електронних засобів контролю», зареєстрований у Міністерстві юстиції України 14.07.2017 за № 860/30728
 3. Україна зіткнулася з гострим дефіцитом електронних браслетів для стеження за підсудними [Електронний ресурс] // DT.UA. – 2017. – Режим доступу до ресурсу: https://dt.ua/UKRAINE/ukrayina-zitknulasya-z-gostrim-deficitom-elektronnih-brasletiv-dlyastezhennya-za-pidsudnimi-238379_.html

ЗБІЛЬШУЄМО МОЖЛИВОСТІ QR-КОДУ

Подоліух Максим Михайлович,

здобувач ступеня магістра

Національного лесотехнічного університету України

Дендюк Михайло Володимирович,

доцент кафедри інформаційних технологій

Національного лесотехнічного університету України

QR-код був розроблений японською компанією Denso Wave у 1994 році на заміну штрих-коду. Так як у штрих-кодi може міститися тільки до 30 символів, тому з метою збільшення закодованого обсягу інформації та для автоматизації його читання електронними пристроями прийшов QR-код – двомірне зображення, в яке закладається певний контент.

Найменший QR-код (версія 1) має розмір 21×21 піксель, найбільший (версія 40) – 177×177 пікселів.

Максимальним контентом, що поміщений в один QR-код, може бути (Tsukanova, 2013):

- Цифри – 7089;
- цифри і букви (включаючи кирилицю) – 4296;
- двійковий код – 2953 байт;
- ієрогліфи – 1817.

Зазвичай контентом QR-коду є текст, інтернет-посилання, e-mail, контактні дані, номери телефонів, SMS, картографічна інформація тощо (Skriabina, 2011).

Використання QR-коду надає певний ряд переваг та недоліків (Chaplinskyi, 2014), аналіз яких показує, що основною перевагою використання QR-коду є простота читання мобільними пристроями. Також великою перевагою QR-коду є те, що завдяки системі корекції помилок інформацію можна розшифрувати навіть при 30% пошкодженні коду (James, 2003).

Основним же недоліком використання QR-коду є те, що розшифрувати його можна лише за наявності спеціальних програм.

На сучасні смартфони та планшети, що мають вбудовані камери, можна встановити безкоштовне програмне забезпечення для розпізнавання QR-коду:

- I-NIGMA (www.i-nigma.com);
- Kaywa Reader (<http://reader.kaywa.com/>);
- QuickMark (www.quickmark.cn);
- iMatrix (www.imatrix.lt);
- NeoReader (<http://get.neoreader.com>).

Перспективи використання QR-кодів у різноманітних напрямках впровадження висвітлено в працях В. Бондаренко (Bondarenko, 2014), Т. Г. Діброва, І. В. Цуканова, (Tsukanova & Dibrova, 2013), Ковалева А.І. (Kovalev, 2016), В. Логачева (Logachova, 2013), М. Оказакі, М. Хіроші (Okazaki & Hirose, 2012) тощо. З огляду на тотальне поширення мобільних пристроїв та доступності до мережі Інтернет застосування QR-кодів є актуальним.

Мета: Створення програмного інтерфейсу (API) та мобільного додатку «Розпізнавання QR-кодів на візитних картках», що надасть можливість реалізувати єдину систему для зберігання додаткових даних, що на даний момент не використовується у жодній з систем розпізнавання QR-кодів.

Програмний інтерфейс надає API-методи розробнику для будь-якої системи, що спрощує написання багато-платформних додатків.

Мобільний додаток же з допомогою створеного API має можливість зв'язати цей додаток з системою та розширює можливості використання QR-коду, зокрема в QR-коді можна розміщувати не лише символи та цифри, а також зображення, відео, музику, презентації тощо.

Постановка завдання дослідження: Даний програмний продукт має реалізовувати наступний функціонал:

Програмний інтерфейс (API) надає змогу:

- створення нового користувача;
- авторизації на основі JWT-токена;
- авторизації анонімного користувача;

- створення додаткових даних та прив'язка до QR-коду;
- редагування додаткових даних вже існуючого QR-коду;
- видалення додаткових даних QR-коду;
- перегляд усіх створених QR-кодів даним користувачем;
- перегляд збережених QR-кодів з додатковою інформацією;
- редагування інформації про користувача;
- видалення користувача.

Мобільний додаток забезпечує:

- розшифрування QR-коду;
- визначення орієнтації QR-коду;
- генерація QR-коду;
- реалізацію додаткового функціоналу згідно з API.

Розшифрування QR-коду відбувається за наступним алгоритмом.

1. Читаємо QR-код, який містить системну інформацію і дані. Системна інформація дублюється, що дозволяє значно знизити ймовірність виникнення помилок при детектуванні коду і зчитуванні. Щоб засвідчити, що прочитано власне QR-код, за шаблоном (International Standard ISO/IEC 18004, 2000) співставляємо області детектування QR-коду (Position Detection Patterns).

2. Визначаємо формат QR-коду (Format Information) та його версію (Version Information) за маскою. Від коду залежить максимальний обсяг даних, які можуть бути записані в код. Крім того, для захисту системної інформації використовується статична маска (табл. 1).

Таблиця 3. Можливі маски

Код маски	Формула
000	$(i + j) \bmod 2 = 0$
001	$i \bmod 2 = 0$
010	$j \bmod 3 = 0$
011	$(i + j) \bmod 3 = 0$
100	$((i \div 2) + (j \div 3)) \bmod 2 = 0$
101	$(i \cdot j) \bmod 2 + (i \cdot j) \bmod 3 = 0$
110	$((i \cdot j) \bmod 2 + (i \cdot j) \bmod 3) \bmod 2 = 0$
111	$((i+j) \bmod 2 + (i \cdot j) \bmod 3) \bmod 2 = 0$

3. Завдяки корекції ключових слів виявляємо помилки і, якщо вони є, тоді необхідно їх виправити.

4. Визначаємо режим кодування відповідно до правил розташування та відновлення даних в заголовку повідомлення. У роботі реалізовано два режими: числовий і 8 бітний. Числовий – закодує дані з десяткового набору цифр від 0 до 9, при нормальній щільності 3 символи на 10 біт. У 8 бітний режим кодується набір символів відповідно до JISX0201 unicode. В даному режимі щільність даних 8 біт на символ.

5. Зчитування виконується змійкою, починаючи з нижньої правої комірки. Старший біт кожного кодового блоку знаходиться у першому доступному розміщені модуля (International Standard ISO/IEC 18004, 2000).

6. Останнім кроком є розкодування отриманих даних до відповідного режиму.

- API-додаток складається з:
- бази даних (QRcode_DataBase.mdf);
 - серверної частини;
 - рівень доступу до бази даних (qrcode.dal.dll);
 - рівень бізнес-логіки (QRcode.BLL.dll);
 - рівень представлення (QRcode.API.dll).

У процесі проектування програмного інтерфейсу було виділено наступні сутності: User, Sex, Role, BuisnesCard, Personal, Commercial, Data. Ці сутності зберігаються у відповідних таблицях бази даних.

Для створення веб-додатку використано трирівневу архітектуру. Прототип додатку та форму реєстрації наведено на рис. 1.

Реєстрація користувача необхідна для надавання йому повного функціоналу додатку. Деякі функціональні можливості наведено на рис. 2.

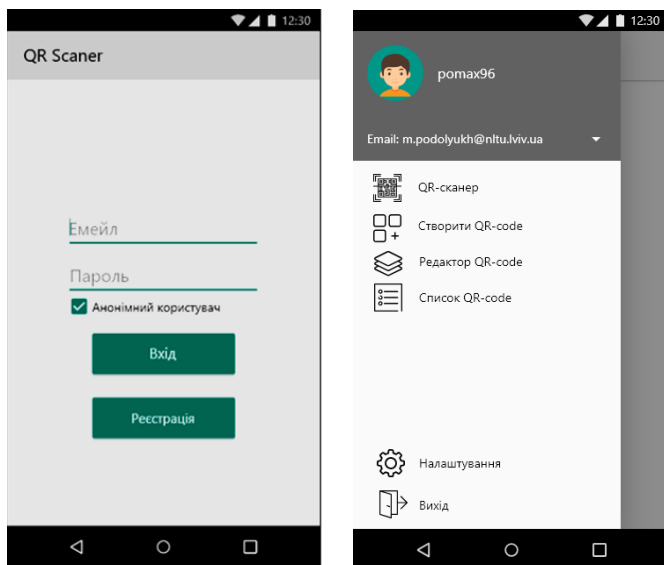


Рис. 1. Головна форма програми та Меню

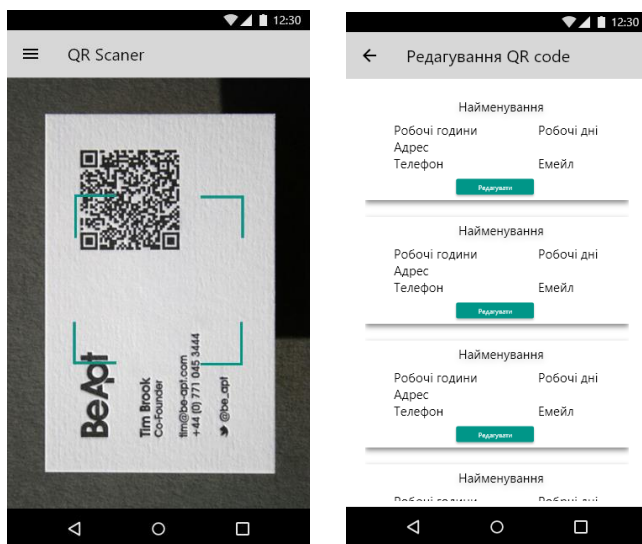


Рис. 2. Функціональні можливості програми QR-сканер та Редактор QR-коду

Висновки. Таким чином, на відміну від наявних QR-сканерів, розроблений API надає змогу розширити функціональні можливості при написанні програм не тільки для розпізнавання QR-коду візиток мобільними пристроями, створення QR-кодів, але і використання додаткових даних та реалізацію їх прив'язки до QR-коду.

-
1. Tsukanova I.V., Dibrova T.H. (2013). Osoblyvosti zastosuvannia QR-kodu v integrovanykh marketynhovykh komunikatsiiakh. *Ekonomichniy visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy «Kyivskiy politekhnichnyi instytut»*, #49, 429-434. [In Ukrainian].
 2. Anna Skriabina. (2011). 20 sposobov ispolzovania QR-kodov. Retrieved from: <http://www.lookatme.ru/flow/posts/internet/117583-20-sposobov-ispolzovaniya-qr-kodov>. [In Russian].
 3. Chaplinskyi Yu., Manhul A. (2014). QR-kod yak suchasnyi zasib v marketynhovykh komunikatsii. Retrieved from: http://www.rusnauka.com/6_185617.doc.htm. [In Ukrainian].
 4. James S. Plank. (2003). GFLIB – C Procedures for Galois Field Arithmetic and Reed-Solomon Coding. Retrieved from: <http://web.eecs.utk.edu/~plank/plank/gflib/>.
 5. Bondarenko V. (2014). Mobilni tekhnolohii u bibliotetsi: QR-kod. *Bibliotechnyi visnyk*, #6, 28–32. [In Ukrainian].
 6. Kovalev A.I. (2016). QR-kody, ikh svoistva i primenenie. *Molodoi uchenyi Mezhdunarodnyi nauchnyi zhurnal*, #10.1 (114.1), 56-60. [In Russian].
 7. V. Logachov. (2013). Shto neset QR-kod. Retrieved from: <http://www.ridcom.ru/publications/131/>. [In Russian].
 8. Okazaki S., Li H., Hirose M. (2012). Benchmarking the Use of QR Code in Mobile Promotion. *Three Studies in Japan. Journal of Advertising Research*, 102–117.
 9. (2000). International Standard ISO/IEC 18004. Information technology – Automatic identification and data capture techniques – Bar code symbology – QR Code. Retrieved from: https://www.swisseduc.ch/informatik/theoretische_informatik/qr_codes/docs/qr_standard.pdf.

РОЛЬ ІНФОРМАЦІЇ В УПРАВЛІННІ ОРГАНІВ ВИКОНАВЧОЇ ВЛАДИ

Собакарь Андрій Олексійович,

*завідувач кафедри тактико-спеціальної підготовки,
Дніпропетровський державний університет внутрішніх справ,
доктор юридичних наук, професор*

В усіх ланках і на всіх рівнях управління циркулюють численні потоки інформації, різноманітної за способом утримання, формою та носіями. Щоб виконувати відведену їй функцію, вона повинна якомога повніше відображати реальність, що дає можливість керівникові органу чи підрозділу виконавчої влади ухвалювати правильне управлінське рішення. Тому сьогодні пріоритетними визнано такі завдання, як удосконалення системи збирання максимально повних даних про обстановку в державі, аналіз тенденцій і перспектив її розвитку, підготовка рішень щодо оперативного реагування на негативні процеси та надзвичайні події.

Управління, незалежно від характеру систем, в яких воно відбувається, може бути успішно здійснене лише на базі інформаційних процесів. Інформація, за твердженням вчених, являє собою одну із сторін процесу відображення, це – форма відображення реального світу. Інформація властива лише керованим, самоорганізованим системам.

Вищим типом інформації є соціальна інформація, оскільки вона – продукт мислення. Отже, це вищий тип відображення. Соціальна інформація – це отримані в процесі мислення знання, повідомлення, відомості про соціальний та інші форми руху матерії, які використовуються суспільством.

Природу соціальної інформації можна визначити, виходячи з таких положень:

- життєдіяльність суспільства являє собою процес постійного обміну між природою і суспільством, основними факторами якого є речовина, енергія й інформація;
- соціальну інформацію людина отримує або безпосередньо із суспільної практики, або через різні джерела, в яких

сконцентровані результати суспільної практики, отриманої іншими людьми;

- взаємодія та взаємозв'язок усіх сфер суспільного життя (економічної, соціально-політичної, духовної, сімейно-побутової) реалізуються через інформаційні процеси;
- виробник і споживач соціальної інформації – людина. Рівень «виробництва» і «споживання» соціальної інформації тим вищий, чим вищий рівень розвитку людини;
- соціальна інформація виконує в суспільстві комунікативну функцію, тобто є засобом комунікації між людьми, окремою людиною і природою; крім того, вона виконує науково-пізнавальну функцію, а також, що найважливіше, – функцію соціального регулювання.

Інформацію, в її життєво-практичному розумінні можна, трактувати як відомості, що передаються людьми усно, письмово чи іншим способом, а також як знання про ті чи інші явища, процеси, об'єкти тощо. Наукове визначення поняття «інформації» через поняття «дані» («відомості»), «знання» вимагає з'ясування цих понять та їх співвідношення.

Відповідно до п. 3 ст. 1 Закону України «Про інформацію» інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Ці самі дані, але вже співвіднесені з певною галуззю їх використання, являють собою знання. Знання, які служать вирішенню будь-якого завдання, є інформацією.

Отже, інформація є необхідним атрибутом, основною умовою та засобом реалізації управління.

Інформація – це знання про стан об'єкта і суб'єкта управління, оточуючого середовища та про результати керуючих впливів.

Під інформацією слід розуміти відомості про будь-які події, чийось діяльність, повідомлення про щось, що цікавить нас з метою ефективного вирішення поставлених завдань.

Вимоги, які висуваються щодо інформації: безперервність; вірогідність; повнота; своєчасність; оновлюваність; систематичність; вибір оптимального рівня; доступність для машинної обробки.

За змістом прийнято розрізняти такі види інформації:

- соціально-політична, що стосується питань внутрішньої і зовнішньої політики держави, ідеологічної та політико-виховної роботи;
- планово-економічна, яка висвітлює складні й різноманітні господарські, трудові та фінансові процеси в народному господарстві;
- наукова, у тому числі науково-технічна, яка забезпечує всі ланки управління відомостями про досягнення науки і техніки, кращий досвід у сферах виробництва, техніки, управління тощо;
- організаційна, що охоплює всі питання структурної побудови і функціонування соціальних систем (органів, ланок управління);
- нормативно-правова, яка містить регламенти, вимоги, заборони.

Найважливішими кількісними і якісними характеристиками інформації є її повнота і цінність.

Повнота інформації – це конкретна вимога, зміст якої визначається залежно від характеру та умов вирішених завдань і, відповідно, від інформаційних запитів споживачів.

Суб'єкт управління, виконуючи те чи інше завдання, в кожному випадку, визначає межі необхідної йому інформації. Отримання повної, саме потрібної інформації, і є реалізацією зазначеної вимоги. Ступінь повноти інформації визначається як відношення наявної інформації до тієї, яка вважається необхідною. Якщо отримана інформація відповідає необхідній – значить, вона є повною; у протилежному випадку можна говорити про її неповноту або надлишок.

Зміст поняття цінності інформації залежить від ряду факторів.

По-перше, чим більший обсяг інформації міститься у тому чи іншому повідомленні, сприяючи уникненню невизначеності, тим вона цінніша.

По-друге, цінність обумовлена тим, наскільки часто чи постійно вирішуються на її основі завдання. Інформація, необхідна для

вирішення найактуальніших, основних і таких завдань, що часто виникають, є ціннішою від відомостей, що використовуються при вирішенні поодиноких питань, що рідко виникають.

По-третє, цінність інформації безпосередньо залежить від її достовірності, тобто об'єктивності відображення нею досліджуваних явищ.

Система інформації того чи іншого апарату управління визначається, по-перше, сукупністю всіх видів інформації, яка використовується у процесі управління даною системою та її функціонування; по-друге, характером інформаційних зв'язків, тобто рухом потоків інформації в системі управління, і, по-третє, засобами і формами організації інформаційного процесу.

Інформацію, яка використовується в органах виконавчої влади, поділяють за такими ознаками:

- за юридичними властивостями: має юридичне значення; не має юридичного значення;
- за строками: щоденна; декадна; місячна; квартальна; піврічна; річна;
- за місцем виникнення: внутрішня; зовнішня;
- за змістом: звітно-статистична; оперативно-службова; оперативно-довідкова;
- за методом отримання: гласна; негласна;
- за ступенем таємності: таємна (обмеженого користування); нетаємна (відкритого користування);
- за характером впливу: керуюча; повідомляюча.

Одна із суттєвих особливостей управління в органах виконавчої влади полягає в тому, що звичайні, загальноприйняті способи отримання та передачі інформації тут не завжди виявляються достатніми.

-
1. Про інформацію: Закон України від 02 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 651. [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show>

ПРАВОВІ ПРИНЦИПИ ОТРИМАННЯ ІНФОРМАЦІЇ ОРГАНАМИ ДЕРЖАВНОЇ ВЛАДИ В УКРАЇНІ

Чорна Софія Зіновіївна,

суддя Сихівського районного суду міста Львова

Протягом останньої чверті століття у світі відбувся глобальний процес розвитку обчислювальних та інформаційних мереж, який можна вважати унікальним поєднанням комп'ютерів і комунікацій соціуму. Людська цивілізація вступила в еру інформаційного суспільства, в якому інформація стає вирішальним чинником у багатьох сферах життєдіяльності. Сьогодні практично неможливо знайти площину соціальної активності людини, що не зазнала б впливу інформаційних технологій: політика, економіка, медицина, право, освіта, культура, релігія, сфера послуг і розваг. Відтак зростає потреба у засобах систематизації, накопичення, зберігання, пошуку та передачі інформації, забезпечення її безпеки.

Правова регламентація формування єдиного інформаційного простору України повинна сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та засобів інформаційного виробництва в країні у процесі її руху до інформаційного суспільства. Відносини щодо отримання органами влади інформації є частиною відносин, що виникають із приводу доступу до інформації.

Дослідники даної проблематики галузі інформаційного права основними принципами доступу до інформації вважають: презумпцію доступності і відкритості інформації; достовірність і повноту інформації; своєчасність надання інформації; дотримання обмежень, встановлених законом; захист права на доступ до інформації; відповідальність за порушення права на доступ до інформації [1, с. 195].

Проаналізуємо ці принципи з огляду на можливість органами державної влади отримувати інформацію. По-перше, термін «презумпція» у цьому випадку не зовсім коректний, оскільки не має належного науково-теоретичного обґрунтування. По-друге, принцип доступності й відкритості інформації полягає в тому, що

будь-яка інформація є відкритою і до неї має забезпечуватися доступ до того моменту, коли можливість отримати (ознайомитися з) такою інформацією не буде обмежена на законних підставах і у спосіб, передбачений законом. Так реалізується конституційне положення про винятковий характер обмеження права на інформацію.

Принцип відкритості обґрунтовують і вітчизняні дослідники, які зазначають, що «відкритий і безперешкодний доступ до суспільно значущої інформації гарантує ефективне управління і вільний розвиток суспільства, сприяє освіті громадян, стимулює прогрес і допомагає вирішенню складних економічних, наукових і соціальних проблем» [2, с. 5].

Однак, принцип доступності й відкритості інформації актуальний для доступу фізичних осіб до інформації і не поширюється на отримання органами державної влади відомостей, що належать фізичним і юридичним особам приватного права. Адже ключовим для регулювання таких відносин є передбаченість законом можливості органів державної влади отримати інформацію.

Достовірність і повнота інформації, яка надається органам державної влади, є актуальним принципом регулювання відповідних суспільних відносин. Науковці акцентують увагу на дотриманні достовірності та інших вимог до якості інформації: повнота, своєчасність, регулярність, комплексність тощо [3, с. 23].

При отриманні органами державної влади інформації особливо важливими є використання принципів достовірності (вірогідності, об'єктивності, точності, правдивості) інформації. Вважаємо, достовірність (вірогідність, об'єктивність, точність, правдивість) інформації є необхідним елементом регулювання інформаційних відносин. Цей принцип полягає у відсутності спотворення змісту інформації і може бути підставою для накладення на органи державної влади додаткових повноважень у тих випадках, коли поширюється неправдива (недостовірна, необ'єктивна) інформація [4, с. 24-25].

Повнота отримання інформації означає, що органи державної влади отримують увесь обсяг інформації, яку вони потребують

(запитують). Гарантією реалізації цього принципу є встановлення юридичної відповідальності за порушення прав чи обов'язків органів державної влади на отримання інформації.

Передумовою для належного врегулювання суспільних відносин із приводу отримання органами державної влади інформації є встановлення чітких термінів отримання інформації, котрі мають важливе значення при реалізації органами державної влади своїх повноважень. Потрібно виокремити такий принцип регулювання відповідних відносин, як своєчасність отримання органами державної влади інформації. Цей принцип передбачає отримання інформації чітко відповідно до термінів, передбачених законодавством або договором.

Загальний принцип регулювання відносин щодо доступу до інформації – дотримання обмежень, встановлених законом, варто детально проаналізувати для відносин, які предметом дослідження. Принцип обмеження доступу до інформації виключно на підставі закону стосується усієї інформації (такої, що належить державі, і що є власністю приватних суб'єктів). Однак реалізація цього принципу відрізняється залежно від власника інформації. Для органів державної влади має бути не лише передбачене обмеження доступу до інформації, але й закріплено перелік категорій таких відомостей (як державна таємниця), визначено порядок поводження із такими відомостями, повноваження суб'єктів тощо [4, с. 25–26].

Особливі правові характеристики має конфіденційна інформація про особу. З урахуванням конституційного положення про те, що збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, формулюємо принцип: отримання органами державної влади інформації про особисте життя за згодою фізичної особи. Винятком із цього загального правила можуть бути випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Усім учасникам інформаційних відносин держава забезпечує рівні права і можливості отримання інформації, якщо тільки така інформація не є таємною. З урахуванням того, що крім таємної, існує й конфіденційна інформація як вид інформації з обмеженим доступом, слід сформулювати принцип рівності прав органів державної влади та інших учасників інформаційних відносин на отримання відкритої інформації. Стосовно інформації з обмеженим доступом, то для кожного органу державної влади законом мають передбачатися підстави для отримання конкретного виду таємної або конфіденційної інформації для виконання покладених на органи державної влади завдань [4, с. 26].

Важливим принципом регулювання відносин щодо отримання органом державної влади інформації має бути закріплення юридичної відповідальності за порушення права органу отримувати інформацію. Причому відповідні санкції мають враховувати шкоду, яка завдаватиметься інтересам держави, юридичних або фізичних осіб у зв'язку з невиконанням державної функції через ненадання інформації. Так, ненадання інформації правоохоронним органам при розслідуванні кримінальних справ може спричинити значні негативні наслідки для охоронюваних державою інтересів фізичних і юридичних осіб [4, с. 27].

З огляду на зазначене можемо сформулювати спеціальні принципи правового регулювання відносин щодо отримання органами державної влади України інформації, до яких віднесено: достовірність і повнота інформації, яка надається органам державної влади; своєчасність отримання органами державної влади інформації; отримання такими органами інформації про особисте юридичних осіб надавати інформацію органам державної влади на їх законний запит; погодження з власником інформації питання про передачу стороннім суб'єктам отриманих від нього цінних відомостей (об'єктів права інтелектуальної власності, інформацію з обмеженим доступом, недоторканість якої охороняється законом).

-
1. Бачило И.Л. Информационное право / И.Л. Бачило; [под ред. академика Б.Н. Топорнина]. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005. 343 с.

2. Громадяни у пошуках інформації: українські реалії / [упорядники: І. Підлуська, С. Горобчишина]. Київ: Агентство «Україна», 2005. 180 с.
3. Костецька Т.А. Право на інформацію в Україні / Т.А. Костецька ; НАН України; Інститут держави і права ім. В.М.Корецького. Київ: Вища школа права, 1998. 39 с.
4. Сопілко І.М. Методологічні засади виокремлення спеціальних принципів отримання інформації органами державної влади в Україні. Інформаційна безпека людини, суспільства, держави. 2012. № 1 (8). С. 23–28.

ЗАСТОСУВАННЯ АЛЬТЕРНАТИВНИХ ДЖЕРЕЛ ЖИВЛЕННЯ В БОЙОВИХ (СПЕЦІАЛЬНИХ) МАШИНАХ

Шабатура Юрій Васильович,

*завідувач кафедри електроніки та електромеханіки
Національної академії сухопутних військ ім. гетьмана Петра
Сагайдачного, доктор технічних наук, професор*

Баландін Максим Володимирович,

*ад'юнкт штатний Національної академії сухопутних військ
ім. гетьмана Петра Сагайдачного*

Протягом останніх десятирічь спостерігається загальносвітова тенденція розвитку альтернативних систем енергоживлення. Найбільш динамічний розвиток спостерігається в галузі автомобілебудування. Усі без виключення автомобільні компанії світу переконалися, що майбутнє у цій галузі за електричною тягою. Тому провідна наукова і конструкторська думка тепер зосереджена на розвитку цього напрямку і в першу чергу, на покращенні характеристик акумуляторних батарей – ємності, часу заряджання, струмових навантажень та ін., а також на тактико-технічних характеристиках самих транспортних засобів на електричній тязі – величині пробігу на одному заряді акумулятора, вантажопідйомність, максимальна швидкість, час розгону до заданої швидкості і т.д. На даний час характеристики деяких зразків вантажних електромобілей значно перевищують характеристики транспортних засобів, що використовуються у військовій сфері.

Крім того, використання електричних силових установок в озброєнні і військовій (спеціальній) техніці дозволяє отримати додаткові переваги, а саме: відсутність шуму від роботи двигуна, відсутність інтенсивного тепловиділення, що знижує ймовірність ураження ракетним озброєнням з головками теплового наведення, можливість миттєвого запуску електродвигуна з максимальним крутним моментом.

Таким чином, використання очевидних переваг поставило актуальне питання розвитку технологій електричної тяги у сфері Національної безпеки.

Поряд з тим, основним недоліком, який стримує застосування електричної енергії в озброєнні і військовій техніці в якості джерела енергії, достатньої для виконання завдань є залежність від джерел енергопостачання.

Одним із варіантів створення альтернативного джерела живлення електричних силових установок бойових (спеціальних машин) є використання енергії, яка розсіюється в процесі пострілу артилерійської гармати.

Проведені розрахунки показують, що понад 70% енергії порохових газів втрачається, більша її частина розсіюється та витрачається на виконання другорядних робіт. Безповоротна втрата таких обсягів енергії під час артилерійських пострілів, є неприпустимою і становить важливу і актуальну задачу.

Вирішення цієї задачі передбачає відбір енергії, що розсіюється під час пострілу, її перетворення в інші види енергії, їх накопичення, збереження і використання для виконання бойових завдань.

Разом з тим, необхідно зауважити, що енергія, яка розсіюється, має різнорідну фізичну природу, то система її відбору, перетворення і накопичення повинна мати комплексний характер.

Аналіз конструктивних особливостей і доступних технічних можливостей, показує, що відбір розсіюваної енергії, її перетворення у найбільш зручну для використання – електричну енергію можливий за рахунок використання наступних другорядних робіт порохових газів: лінійного переміщення відкотних частин гармати; нагріву ствола, внаслідок інтенсивної стрільби; дисипації порохових газів в атмосферу.

Кінетичну енергію руху відкотних частин можливо перетворювати у інші види корисної енергії за допомогою встановлення системи енергетичних перетворювачів – п'єзоелектричних, індукційних, пневматичних.

Конструктивно п'єзоелектричний перетворювач складається з натискних роликів, які закріплені на відкотних частинах, п'єзоелектричних елементів з пружною прокладкою, які закріплені на нерухомих частинах гармати. При лінійному переміщенні

протівідкотні пристрої натискними роликами через пружну прокладку здійснюють ударну дію на п'єзоелектричні елементи, внаслідок чого отримується електрична енергія.

Індукційний перетворювач представляє собою лінійний електро-механічний генератор. Він складається з постійних магнітів великої потужності встановлених через діамагнітну прокладку на стволі гармати (ротор) та закріплених на нерухомих частинах гармати котушки (статор), причому, під час пострілу ротор переміщується всередині статору, внаслідок чого в магнітній котушці статору збуджується електрорушійна сила та генерується електрична енергія. Основною перевагою лінійного електро-механічного генератора є те, що він не має жодних механічних зчеплень, а тому в процесі експлуатації він не зношується і має високу надійність.

Пневматичний перетворювач – складається з робочого поршня, з'єднаного з відкотними частинами та робочого циліндру, який закріплений на нерухомих частинах гармати, випускного клапану, балону для зберігання стисненого повітря. При лінійному переміщенні протівідкотні пристрої переміщують разом із собою робочий поршень, який переміщаючись всередині робочого циліндру стискає повітря, яке при досягненні необхідного тиску через вихідний клапан поступає до ємності для його зберігання. У подальшому енергія стисненого повітря може використовуватись для потреб гармати – підкачки шин, підтримання тиску у врівноважувальному механізмі, накатнику або поступати до пневматично-електричних перетворювачів та перетворюватись у електричну енергію.

Застосування енергетичних перетворювачів, принцип дії яких оснований на використанні енергії лінійного руху відкотних частин, крім основного завдання – отримання електричної енергії та енергії стисненого повітря буде виконувати ще й додаткове завдання – поглинання частини енергії відкату, що знизить навантаження на протівідкотні пристрої, що позитивно вплине на живучість гармати.

Ще одним методом отримання альтернативного джерела електричної енергії є використання нігріву ствола гармати внаслідок інтенсивної стрільби.

В процесі горіння порохового заряду, переміщення порохових газів всередині ствола, взаємного тертя ствола та снаряду, частина теплової енергії, внаслідок тепловіддачі буде передаватись до стінок ствола що призведе до підвищення його температури, а під час інтенсивної стрільби призведе до його значного розігріву. Температура розігріву ствола гармати може сягати 400°C і більше. Крім цього, охолодження ствола відбувається досить тривалий час, так, наприклад ствол середнього калібру, нагрітий до температури 300...350°C, охолоджується на повітрі до температури 100°C за 30...60 хв., а для охолодження до температури навколишнього повітря необхідно 2-3 години, в залежності від калібру гармати та зовнішніх умов. Перетворення теплової енергії ствола в електричну енергію можливе за рахунок встановлення на ствол гармати термоелектричних перетворювачів.

Термоелектричні перетворювачі – складаються з елементів «Пельтьє» які розміщені на стволі артилерійської системи. Під час інтенсивної стрільби ствол гармати буде нагріватися, внаслідок чого на термоелектричних перетворювачах буде генеруватись електричний струм. Крім основного завдання, термоелектричний перетворювач буде додатково виконувати функцію охолодження ствола під час інтенсивної стрільби, що позитивно вплине на живучість ствола та точність вогню.

В системі відбору та перетворення енергії, яка розсіюється в процесі пострілу артилерійської системи можливе використання як окремих перетворювачів так і їх комбінації для збільшення загальної енергетичної потужності системи.

Встановлення в бойовій машині додаткової комплексної системи електроживлення на основі відбору та перетворення енергії, яка розсіюється в процесі пострілу гармати, дозволить збільшити кількість пострілів, які можна виконати без використання енергії двигуна базової машини, що призведе до зменшення витрат паливно-мастильних матеріалів, підвищення автономності дій підрозділу, зменшення логістичних витрат на забезпечення ведення бойових дій, а в мирний час дозволить знизити витрати на бойову підготовку. Крім того, запропонована система позитивно вплине на живучість гармати через зменшення витрати

моторесурсу базової машини та через зменшення навантаження на противідкотні пристрої.

Важливим також є те, що встановлення даної комплексної системи жодним чином не буде погіршувати основні тактико-технічні характеристики бойової машини.

ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ: ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ В УКРАЇНІ

Ярема Оксана Григорівна,

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

Чабак Вікторія Юріївна,

*здобувач ступеня бакалавра
Львівського державного університету внутрішніх справ*

Право на доступ до публічної інформації в сучасному інформаційному суспільстві одним із ключових прав людини, передбачених у Конституції України. Доступ до публічної інформації є основою встановлення та налагодження ефективного спілкування та комунікації між органами державної влади та населенням країни. До того ж володіння інформацією про державну політику, діяльність органів державної влади та органів місцевого самоврядування дозволяє громадянину бути не пасивним спостерігачем у вирішенні місцевих проблем, обговоренні проектів нормативно-правових актів, проведенні державних реформ, а стати їх співтворцем і учасником.

Дослідженнями окремих питань щодо правового регулювання права громадянина на доступ до публічної інформації в Україні займалися такі науковці, як В. Авер'янов, І. Бачило, Н.М. Тимченко, А. Колодій, В. Копилов, П. Шляхтун, В. Цимбалюк, А.Л.Садовська. Однак, ряд проблем у даній галузі потребують детальнішого дослідження й аналізу.

Доступ до інформації став невід'ємною частиною в механізмі функціонування демократичного режиму в будь-якій країні. Це пояснюється тим, що існування правової держави можливо за умови прозорості діяльності органів влади, адже на основі цього можливе забезпечення участі громадян у формуванні та здійсненні державної політики. Прийняття рішень та здійснення політики органами державної влади відбувається від імені громадян.

А це має забезпечувати право доступу громадян до публічної інформації [1, с. 169].

Відповідно до положень національного законодавства громадянин України має право звертатися до органів державної влади та місцевого самоврядування з метою ознайомлення з інформацією, а отже вимагати надання будь-якого офіційного документа, незважаючи на те, стосується такий документ його особисто чи ні, окрім випадків передбачених Законом. Механізм забезпечення отримання громадянами публічної інформації відображений в Законі України «Про доступ до публічної інформації» від 13.01.2011 року.

Закон України «Про доступ до публічної інформації» закріплює принцип відкритості інформації про діяльність державних та місцевих органів влади, закріплює право людей знати, чим займається влада. Цей закон змушує владу враховувати думку громадян при розгляді найважливіших питань [2, с. 341].

Ст. 14 Закону України «Про доступ до публічної інформації» встановлює обов'язок розпорядника інформації мати спеціальний структурний підрозділ або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації та оприлюднення інформації. Саме із цим положенням виникає перша проблема забезпечення права на доступ до інформації а також захисту такого права у суді. При розгляді у суді справ про відмову у наданні інформації, можуть виникнути певні труднощі. Незрозуміло, кого ж вважати відповідачем по справі – розпорядника інформації чи структурний підрозділ або відповідальну особу, чи розпорядника інформації в особі відповідного структурного підрозділу або відповідальної особи, адже всі вони є суб'єктами відносин у сфері доступу до публічної інформації. До того ж, виходить, що самостійний суб'єкт має в своєму складі такого ж самостійного суб'єкта. Тому варто внести деякі зміни у Закон, щоб не виникало труднощів у визначенні відповідача та належному забезпеченні прав громадян на доступ до публічної інформації.

Ще однією проблемою ненадання або неналежного надання публічної інформації є брак коштів. Через недостатнє фінансування і слабку матеріальну базу деякі розпорядники інформації не

можуть виконати положення про обов'язок оприлюднити певну інформацію невідкладно, але не пізніше ніж через 5 робочих днів із дня затвердження документа. При цьому не визначено, в яких джерелах ця інформація повинна бути оприлюднена. Лише зазначено, що у разі наявності у розпорядника інформації офіційного веб-сайту така інформація оприлюднюється на ньому. Але на сьогодні багато селищних рад та інших органів державної влади не мають власного веб - сайту, доступу до мережі Інтернет, свій власний друкований орган. Тому потрібно доповнити норму Закону України «Про доступ до публічної інформації» нормою про те, що суб'єкти інформації можуть оприлюднювати свої рішення та інші документи таким способом, що відповідає їхньому матеріальному становищу та не ускладнює донесення до населення такої інформації. Це можуть бути наприклад публікації у міських, районних засобах масової інформації, де б їм надавалась змога безкоштовно друкувати інформацію про свою діяльність та результати такої діяльності.

Також в Україні варто було б створити орган, який би здійснював контроль за дотриманням Закону «Про доступ до публічної інформації». Наприклад у Канаді введено посаду Комісара з питань доступу до інформації, який є посадовою особою Парламенту. Він є незалежним від влади і наділений повноваженнями розгляду скарг від громадян щодо порушення їхнього права на інформацію. Оскільки в Україні великою проблемою є корупція, то введення такої посади було б доцільним [3, с. 55].

Також можна створити єдиний веб – сайт, на якому б розміщувалась інформація про діяльність всіх державних органів, та рішення які прийняті цими органами. Це б значно полегшило доступ громадян до публічної інформації. Наприклад у Великобританії створено он-лайн платформу, яка є єдиним пунктом доступу до інформації та діяльності державних органів [4, с.336].

Отже, прийняття Закону України «Про доступ до публічної інформації» є великим кроком України у задоволенні інтересів громадян у сфері доступу до публічної інформації. Він надає громадянам право бути учасником у вирішенні місцевих проблем, а також право бути обізнаним із діяльністю та результатами такої діяльності органів державної влади.

Але із метою забезпечення права громадян на доступ до публічної інформації Україні варто перейняти досвід інших держав, які краще справляються із цим завданням і більшою мірою задовольняють інтереси своїх громадян.

Також варто переглянути чинні нормативні акти, які стосуються доступу до публічної інформації та внести відповідні зміни до них, щоб не виникало незрозуміlostей та не порушувались права громадян на отримання повної, достовірної і необхідної інформації, яка перебуває у володінні органів державної влади та місцевого самоврядування.

-
1. Садовська А.Л. Посилення гарантій права на доступ до публічної інформації в системі комунікацій між державою та громадянами / А.Л.Садовська // Актуальні проблеми державного управління. – 2013. – № 2. – С. 169 – 177.
 2. Карась Є. Проблематика доступу до публічної інформації в громадянському суспільстві України/ Є. Карась // Гілея: науковий вісник. – 2013. – № 73. – С.340 – 342.
 3. Стадник Р. Відкритість органів влади в контексті законодавства про доступ до публічної інформації / Р. Стадник // Публічне управління: теорія та практика. – 2012.– № 2. – с.55 – 59.
 4. Національні та міжнародні механізми фінансування громадянського суспільства. Міжнародні заходи зміцнення довіри між державою та громадянським суспільством. – К. : Фенікс, 2011. – 336 с.

Зміст

Розділ 1. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО–ПРАВОВІ, ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНО–ЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ, ЇХ ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ТА КОМПЛЕКСНОМУ ПІДХОДІ ДО ПРОБЛЕМ ДЕРЖАВНОЇ БЕЗПЕКИ	3
Бортник Н.П. Правові та технічні питання безпеки в інформаційному просторі	4
Власюк О.М., Копанецька Н.В., Сеник В.В. Основні цілі, завдання та принципи інформаційної безпеки в умовах сьогодення	10
Гаврильців М.Т. Державно-правовий механізм забезпечення інформаційної безпеки в Україні	14
Гривняк С.О., Кулешник Я.Ф. Розробка ефективної інформаційної стратегії для аналітичного забезпечення підрозділів поліції.....	19
Дідик Н.І., Сивак Ю.М. Застосування інформаційних технологій в діяльності працівників Національної поліції	23
Тронько О.В., Довгаль Ю.С. Роль інформаційних технологій у діяльності Національної поліції України	28
Дуфенюк О.М. Новітні технології як засіб зниження суб'єктивізму в судово-експертній діяльності, але не завжди... ..	34
Єсімов С.С. Проблеми ідентифікації суб'єкта в електронному документообігу	38
Живко З.Б., Руда О.І., Мандрик М.С. Безпека спеціалізованих інформаційних систем підрозділів Національної поліції України	43
Комісарчук Ю.А., Полійовська М.Т. Кримінальний аналіз як невід'ємна складова поліції у ефективній боротьбі зі злочинністю	49

Кононець В.П. Актуальні питання використання соціальних мереж для попередження, виявлення та розкриття правопорушень серед неповнолітніх	54
Луцький Т.М. Використання інформаційних технологій та систем в діяльності поліції зарубіжних держав	58
Нагорняк Ю. В. Використання функцій розпізнавання обличчя під час розслідування КДТП	65
Омельяненко О.В., Рудий Т.В., Денис Р.В. Технології протидії кіберзлочинності.....	69
Отчак Н.Я. Поняття й сутність інформаційної безпеки та її місце в системі національної безпеки України.....	73
Расторгуєва Н.О. До питання інформаційного забезпечення кіберполіції України щодо протидії кіберзлочинності	78
Рижков Е.В., Дзех Я.С. Проблемні питання інформаційно-аналітичного забезпечення в системі органів Національної поліції та проблемні питання щодо захисту інформації під час виконання службових обов'язків	83
Сеник С. В. Етапи побудови комплексних систем захисту інформації у підрозділах Національної поліції України.....	87
Сірант М.М. Роль інформаційного права у сфері інформаційної безпеки	91
Ткачук Т.Ю., Шишко В.В., Хитра О.Л. Особливості визначення складових інформаційної безпеки України	94
Форос Г.В., Сергата В.В. Аспекти інформаційного забезпечення діяльності правоохоронних органів.....	101
Чистоклетов Л.Г., Ткачук Т.Ю. Визначення загроз в сфері інформаційної безпеки	105
Розділ 2. НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНОТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ	112

Глинський Я.М., Пелех Я.М., Рязська В.А. Відеокурс з інформаційних технологій.....	113
Косаревська О.В. Актуальні питання впровадження сучасних інформаційних технологій в процес підготовки майбутніх фахівців правоохоронної сфери у ВНЗ з особливими умовами навчання	116
Лунькова Г.В., Філімонов С.М., Міхалева М.С. Реалізація індивідуальної траєкторії навчання курсантів ВВНЗ.....	121
Прокопов С.О. Особливості викладання інформаційних дисциплін в Дніпропетровському державному університеті внутрішніх справ	126
Прокоф'єв М.М. Мережеві моделі взаємодії в інформаційно-освітньому середовищі з підготовки державних службовців правоохоронної сфери.....	131
Савайда О.І. Теоретико-методологіч аспекти застосування інформаційних технологій в освіті	136
Сватюк О.Р., Миронов Ю.Б., Миронова М.І. Особливості впровадження дистанційного навчання в освітній процес ...	139
Сеник В.В., Магеровська Т.В., Карагодіна Ю.Ю. До питання підвищення ефективності підготовки фахівців у галузі обробки статистичних та аналітичних даних	144
Розділ 3. СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ ІТ ТЕХНОЛОГІЙ В АКТУАЛЬНІ СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ ДІЯЛЬНОСТІ	147
Біденчук Т.М., Кононець В.П. Актуальні питання щодо забезпечення оперативного реагування поліції на повідомлення про злочини та інші події.....	148
Вишня В.Б., Гавриш О.С. Автоматизована система контролю вантажоперевезень на залізниці	156
Грицюк Ю.І., Далавський В.С. Експертне оцінювання якості програмного забезпечення з використанням пелюсткових діаграм	159

Гуцуляк Ю.В. Кримінально-аналітичне забезпечення досудового розслідування кримінальних правопорушень пов'язаних із торгівлею людьми з використанням інформаційних технологій в контексті отримання підстав для проведення окремих негласних слідчих (розшукових) дій.....	167
Єсімов С.С., Яцина О.І. Юридична природа персональних даних	172
Зачек О.І., Дмитрик Ю.І. Модернізація електрошокера з використанням технології BodyCom для запобігання його несанкціонованого використання	177
Ковалів М.В., Дужак А.В. Принцип інформаційної відкритості як невід'ємна складова управлінської діяльності.....	182
Ковтун В.О., Рвачов О.М. Деякі проблемні аспекти використання поліграфів у діяльності Національної поліції України	186
Когут В.М. Правові засади реєстрації електронної інформації в справах про адміністративні правопорушення	191
Комісарчук Ю.А., Клим Л.М. Процесуальне оформлення слідчих (розшукових) дій за допомогою технічних засобів: деякі аспекти.....	196
Комісарчук Ю.А., Миханюк М.М. Проблеми застосування негласних слідчих (розшукових) дій у практичній діяльності Національної поліції.....	200
Комісарчук Ю.А., Ярмо Х.В. Особливості застосування спеціальної техніки під час кримінального провадження	204
Крижановський А.С. Інформаційно-правові особливості криміналістики у віртуальному просторі.....	210
Кулешник Я.Ф., Кочетов Є.С., Пилаєва О.С. Роль інформації управління в поліції.....	213
Лозинський Ю.Р., Півень С.Г. Державна таємниця як один із видів інформації з обмеженим доступом	217
Лук'янова Г.Ю. Нормативно-правове регулювання механізму державного управління інформаційною сферою	222

Магеровська Т.В., Пукач П.Я., Пелех Я.М. Аналіз сучасного програмного забезпечення закордонних юридичних фірм та приватних юристів	227
Мандзюк Т.В., Неспляк Д.М., Тучапський Р.І., Бичинюк І.В. Деякі аспекти аналізу злочинності з використанням R	235
Миджин Г.Є. Про критерії ефективності форм захисту авторських прав	238
Мельничин А.В. Інформаційна система пошуку паркомісць	243
Перепьолкіна Ю.А., Кононець В.П. Проблемні аспекти оперативного реагування поліції по факту спрацювання електронних браслетів, для забезпечення запобіжного заходу в частині забезпечення контролю за місцезнаходженням осіб за ухвалою слідчого судді.....	248
Подолух М.М., Дендюк М.В. Збільшуємо можливості QR-коду	252
Собакарь А.О. Роль інформації в управлінні органів виконавчої влади	258
Чорна С.З. Правові принципи отримання інформації органами державної влади в Україні	262
Шабатура Ю.В., Баландин М.В. Застосування альтернативних джерел живлення в бойових (спеціальних) машинах.	267
Ярема О.Г., Чабак В.Ю. Доступ до публічної інформації: проблеми забезпечення в Україні	272

НАУКОВЕ ВИДАННЯ

**ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ СТРУКТУРАМИ
УКРАЇНИ ТА ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ ЗІ
СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ**

**Збірник наукових статей за матеріалами доповідей
Всеукраїнської науково-практичної конференції
21 грудня 2018 р.**

Відповідальний за випуск В.В. Сеник
Упорядник Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська

Опубліковано в авторській редакції

Підписано до друку 10.01.2019 р.
Формат 60х84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк. 18,2
Тираж 100 прим.

Львівський державний університет внутрішніх справ
79007, м. Львів, вул. Городоцька, 26

Свідотство про внесення суб'єкта видавничої справи до державного
реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.