ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

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

20 грудня 2019 р.

Львів 2019

УДК 004 І 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 5 від 24.12.2019)

І 78 Інформаційні технології в освіті та практиці : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 20 грудня 2019 року / упорядник Т. В. Магеровська. – Львів: ЛьвДУВС, 2019. – 246 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції «Інформаційні технології в освіті та практиці», що проводилася 20 грудня 2019 року у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

Розділ 1. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ, ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ, ЇХ ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ТА КОМПЛЕКСНОМУ ПІДХОДІ ДО ПРОБЛЕМ ДЕРЖАВНОЇ БЕЗПЕКИ

Проблемні питання кримінальної відповідальності за злочини, пов'язані із службовим підробленням документів

Гарасим Павло Станіславович

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

Згідно ст. 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі та в межах повноважень та у спосіб, що передбачений Конституцією та законами України [1]. Звідси очевидно, що діяння, яке вчинюється всупереч Конституції України [1] і законам України, є порушенням їх приписів, а також передбачається юридична відповідальність. Поряд з тим, варто зазначити, що сьогодні в Україні відбувається реформування органів державного управління, судової системи та правоохоронних органів, особливого значення набуває питання посилення авторитету органів державної влади, а отже, і протидії злочинам у сфері службової діяльності [2]. За результатами дослідження праці [2] встановлено, що найбільш розповсюдженими та небезпечними злочинами цієї категорії є зловживання владою або службовим становищем та перевищення влади або службових повноважень.

Суспільну небезпеку вчинення цих діянь становить їх руйнівний вплив на різні сфери життя, підрив авторитету влади в суспільстві та ефективності державного управління. Про поширеність такого явища свідчать дані статистики Генеральної прокуратури України та Міністерства внутрішніх справ, відповідно до якої кількість зареєстрованих фактів тільки перевищення влади або службових повноважень, незважаючи на їх незначне зменшення, й надалі залишається досить високим [3]. Тут, за результатами аналізу інфографіки [3] та інших відкритих джерел інформації, необхідно також враховувати й високий рівень латентності вказаного виду протиправних діянь, а також корупційну складову

при вирішенні питань щодо притягнення до кримінальної відповідальності посадових осіб [3; 4].

В контексті цього з'ясовано, що однією з проблем кримінальної відповідальності за службові злочини, можна побачити розглядаючи норми про кримінальну відповідальність за зловживання владою чи службовим становищем, а саме про відповідність та співрозмірність санкцій ст. ст. 364 та 364-1 Кримінального кодексу України (від 05.04.2001 р. № 2341-III) [5] суспільній небезпечності передбачених ними діянь, їх наслідкам, а також між самими нормами. В них міститься широкий перелік альтернативних видів покарань, а також додаткові у виді позбавлення права обіймати певні посади чи займатися певною діяльністю, а також штраф і навіть конфіскація майна. Це, підтримуючи думку науковців [4] (Л. Ковтун, І. Нечипорук), можна вважати позитивним, проте привертає увагу те, що санкції за злочинне зловживання повноваженнями службовою особою приватного права явно значно м'якші, ніж за зловживання владою та службовим становищем посадових осіб, які перебувають на державній службі або працюють у державних підприємствах, установах чи організаціях. А тому значно суворіші санкції ст. 364 від санкцій ст. 364-1 Кримінального кодексу України (від 05.04.2001 р. № 2341-III) [5] можна розглядати як дискримінаційні стосовно громадян України, які перебувають на державній службі або працюють на її підприємствах, в установах або організаціях і при цьому одержують незначне грошове забезпечення [4; 6].

Поряд з тим варто також зазначити, що службова особа намагаючись досягти свого злочинного наміру на одержання будь-якої неправомірної вигоди для самої себе чи іншої фізичної або юридичної особи спираючись на повноваження влади чи службового становища всупереч інтересам служби шляхом використання офіційних документів, як правило, реалізує підроблення такого документа. В чому проявляється таке підроблення. Наприклад, це може бути внесення в офіційний документ не достовірної інформації, загальне підроблення документа (як повне так і часткове) тощо [7]. Тому у випадку наявності таких суспільно небезпечних діянь ми повинні кваліфікувати його за

ст. 366 Кримінального кодексу України (від 05.04.2001 р. № 2341-III) [5], так як диспозиція ст. 364 КК України не передбачає кримінальної відповідальності за підроблення офіційних документів. Внаслідок цього може скластись ситуація коли суспільно небезпечне діяння особи залишиться без юридичної оцінки і, як наслідок цього, особа уникне кримінальної відповідальності за злочин. Це питання сьогодні є актуальним та потребує додаткового вивчення. У випадку зловживання особою владою або своїм службовим становищем, яке поєднане з створенням або використанням підроблених офіційних документів, кваліфікація цього суспільно небезпечного діяння повинна відбуватись за сукупністю злочинів, а саме за ст. 364 та 366 Кримінального кодексу України (від 05.04.2001 р. № 2341-III) [5].

Слід також зазначити, що вчинення злочину службового підроблення (ст. 366 КК України) нерідко є способом приховування інших злочинів (складання завідомо неправдивих документів, видача завідомо неправдивих документів, внесення до офіційних документів завідомо неправдивих відомостей, інше підроблення офіційних документів), наприклад, зловживання владою і службовим становищем (видання неправомірного наказу), перевищення влади і службових повноважень, одержання неправомірної вигоди (внесення неіснуючих осіб у наказ на отримання премії та ін.).

Як зазначає В. Л. Ортинський, якщо сфальсифіковано документи, потрібно провести комплекс слідчих (розшукових) дій, основними завданнями яких є: а) виявлення і вилучення інших екземплярів цього документа; б) встановлення і допит усіх осіб, які брали участь у складанні справжніх або фальсифікації наявних документів; в) встановлення і допит усіх осіб, підписи, посади, прізвища яких є на сфальсифікованому документі; г) допит осіб, відповідальних за ведення в установі бухгалтерського обліку, діловодства; д) встановлення і допит осіб, які брали або повинні були брати участь у фінансових, господарських, правотворчих та інших операціях, з приводу яких складено фальсифікований документ [8]. При цьому як далі вказує

В. Л. Ортинський, тактика побудови прийомів слідчих (розшукових) дій як пошукової інформаційної моделі активного злочинця, насамперед, повинна охоплювати з'ясування таких елементів:

- даних особистого кримінального досвіду злочинця;
- відомостей, що містяться в матеріалах кримінальних проваджень, де фігурувала ця особа, але залишилася без покарання;
- відомостей, що містяться в матеріалах нерозслідуваних кримінальних проваджень про аналогічні злочини.

Тому напрями пізнавальної діяльності визначають, як правило, конкретною слідчою ситуацією, а також низкою чинників, до яких належать: наявність інформації про вчинення протидії підозрюваним; наявність джерела невідомої інформації про протидію; виявлені взаємозв'язки особи злочинця (посадової особи) з вчиненням протидії слідству.

Таким чином, за результатами дослідження літературних джерел [1–8] та аналізу реалій сьогодення можна стверджувати, що сьогодні залишаються проблемні питання вдосконалення Кримінального кодексу України (від 05.04.2001 р. № 2341-III) за вчинення злочинів у сфері службової діяльності. У цьому напрямі вже є певні напрацювання, які заслуговують на увагу, а конкретні наявні сьогодні законодавчі ініціативи (про кримінальну відповідальність за службові злочини) необхідно проаналізувати на базі широкого переліку критеріїв та сформувати оцінку їх якості.

---

1. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. URL: http://zakon.rada.gov.ua /laws/show/254к/96-вр. (із змінами та доповненнями).
2. Григоренко Ю. Неоцінені зміни: Чому українці не бачать покращення від реформ // Матеріали Інформаційного Агентства 112.ua. 25.02.2019 р. URL: https://ua.112.ua/statji /neotsineni-zminy-chomu-ukraintsi-ne-bachat-pokrashchennia-vid-reform-481840.html .
3. Злочинність в Україні: статистика за минулий рік // Матеріали Аналітичного порталу «Слово і Діло». 16.02.2018 р.

URL: https://www.slovoidilo.ua/2018/02/16/infografika/suspilstvo/zlochynnist-ukrayini-statystyka-mynulyj-rik.
4. Ковтун Л. Ю., Нечипорук І. В. Проблеми вдосконалення законодавства про кримінальну відповідальність за службові злочини // Пріоритетні напрямки розвитку правової системи України: Матеріали III Міжн. науково-практ. конф. (м. Львів, 6-7.11.2015 р). Херсон: Вид. дім «Гельветика», 2015. С. 91-94. URL: http://molodyvcheny.in.ua/files/conf/law/13nov2015/23.pdf.
5. Кримінальний кодекс України від 05.04.2001 р. № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14. (із змінами та доповненнями).
6. Гора Р. М. Значення юридичних осіб публічного права для вивчення об'єкта злочину, передбаченого ст. 364-1 КК України // Вісник Асоціації кримінального права України. 2018. № 1 (10). С. 144-152. URL : http://nauka.nlu.edu.ua/wp-content/uploads/2018/07/12_Gora.pdf .
7. Фіалка М. І. Зловживання владою або службовим становищем вчинене шляхом використання підроблених офіційних документів: окремі питання кваліфікації // Особливості застосування антикорупційного законодавства: від розслідування до вироку суду : матеріали Міжнар. наук.-практ. конф. (м. Харків, 17 жовт. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України ; Громад. спілка «Центр запобігання та протидії корупції»; Громад. рада при МВС України. Харків : ХНУВС, 2019. С. 161-164.
8. В.Л. Ортинський. Засоби подолання протидії під час розслідування злочинів у сфері службової діяльності. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2019/aug/17830/3.pdf

Цифрові права: новели законодавства

Єсімов Сергій Сергійович,

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

У січні 2018 року було схвалено Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації, відповідно до якої однією з цілей розвитку України є забезпечення прискореного впровадження цифрових технологій в економіці та соціальній сфері. У економічній діяльності дані в цифровій формі сприяють формуванню інформаційного простору з урахуванням потреб громадян і суспільства в отриманні якісних та достовірних відомостей, розвитку інформаційної інфраструктури України, створення та застосування інформаційно-телекомунікаційних технологій, формування нової технологічної основи для соціальної і економічної сфери [1].

В Україні цифрові технології використовуються практично у всіх сферах соціально-економічної діяльності (наприклад, при наданні адміністративних послуг населенню, в сфері банківської діяльності, перевезеннях, страхування тощо).

У процесі формування єдиного інформаційного простору створюються нові інформаційні системи (єдина інформаційна система нотаріату, єдиний державний реєстр записів актів громадянського стану), в яких інформація міститься в сховищах даних, доступ до яких надається за допомогою призначеного для користувача інтерфейсу.

У сучасному світі з’являється все більше нових цифрових технологій: технології хмарних сервісів (Cloud Computing), технологія Блокчейн (Blockchain), інтернет речей (Internet of Things, IoT), технології віртуальної та доповненої реальностей (VR і AR), штучний інтелект та ін.

Незважаючи на швидке зростання розвитку цифрових технологій, Україна в цій сфері значно відстає від держав-членів

Європейського Союзу, за даними Всесвітнього економічного форуму, займає 39-е місце [2].

Поява нових цифрових технологій спричиняє необхідність формування правових механізмів, які забезпечать сприятливий режим для розвитку нових видів відносин (об'єктів і суб'єктів інформаційних правовідносин, специфічних прав, обов'язків і відповідальності), сприяючи вирішенню проблем збереження цифрових даних користувача, забезпечення безпеки інформації, захисту інтелектуальних прав, приватного життя громадян, боротьби з комп'ютерною злочинністю, запобігання загрозам, пов'язаних з належним функціонуванням хмарних сховищ даних.

Для вирішення перерахованих проблем необхідно, в першу чергу, закріпити на законодавчому рівні терміни, що застосовуються у сфері цифрових технологій, правовий статус суб'єктів і об'єктів названих суспільних відносин. У даний час на розгляді у Міністерстві цифрової трансформації України розробляється проект закону, в якому пропонується доповнити об'єкти цивільних прав цифровими правами.

Відповідно до проекту під цифровими правами слід розуміти права на об'єкти цивільних прав, за винятком нематеріальних благ, що можуть бути засвідчені сукупністю електронних даних (цифровим кодом або позначенням), існуючої в інформаційній системі, що відповідає встановленим законом ознаками децентралізованої інформаційної системи, при умови, що інформаційні технології та технічні засоби цієї інформаційної системи забезпечують особі, яка має унікальний доступ до цього цифровому коду позначенню, можливість в будь-який момент ознайомитися з описом відповідного об'єкта цивільних прав. Цифровий код або позначення визнаються цифровим правом.

Під цифровими правами розуміється сукупність електронних даних (цифровий код або позначення), яка засвідчує права на речі, інше майно, результати робіт, надання послуг, виключні права. Запис про права на такі об'єкти цивільних прав повинна бути в інформаційній системі, яка відповідає встановленим законом ознаками децентралізованої інформаційної системи

(«розподілений реєстр»). Перехід цифрових прав здійснюється за допомогою внесення запису в розподілений реєстр.

Володарем цифрового права може бути особа, яка має цифровим кодом (шифром), за допомогою якого можна розпоряджатися цифровим правом. Це може бути, як фізичне, так і юридична особа.

Окремо розглядається поняття «цифрові гроші», під ними розуміється не задовольняюча право на який-небудь об'єкт цивільних прав сукупність електронних даних (цифровий код або позначення), створена в інформаційній системі, що відповідає встановленим законом ознаками децентралізованої інформаційної системи, використовувана користувачами цієї системи для здійснення платежів. Однак використовувати в Україні цифрові гроші можна буде тільки у віддаленому майбутньому у випадках і на умовах, встановлених законом.

Відповідно до чинного законодавства грошовою одиницею в Україні є гривна, введення і емісія інших грошей в Україні не допускаються, отже, використання цифрових грошей буде можливо тільки після внесення змін до законодавства України.

У тому випадку, якщо цифрові гроші все-таки будуть визнаватися офіційним платіжним засобом, необхідно буде внести зміни в законодавство про обов'язкову реєстрацію власників прав на даний об'єкт (наприклад, на біржі) та вносити записи про власників цифрових грошей в інформаційну систему, щоб можна було відслідковувати відомості про даних суб'єктах.

У Верховній Раді зареєстрований законопроект, яким пропонується легалізувати криптовалюта. Документ під назвою «Про внесення змін до Податкового кодексу та інших законів України щодо оподаткування операцій з кріптоактівами» розроблений представниками блокчейн-спільноти, міжфракційними народними обранцями, Офісом ефективного регулювання BRDO і Міністерством цифровий трансформації. Визначення правового статусу криптовалюта допоможе легалізувати пов'язану з ними діяльність, таку, як покупка та продаж криптовалюти, а також їх видобуток. І виведе гравців ринку з «сірої» зони, що виступить

стимулом для додаткових надходжень до бюджету від сплати податків, заявив Міністр цифровий трансформації М. Федоров [3].

Ще одним з проблемних питань є те, яким чином боржник буде зобов'язаний надати фізичний ключ, якщо його не існує (пароль в голові). Абсолютно незрозумілі дії, які слід вжити суду в разі, якщо особа не виконає постанову суду і скаже, що забув шифр. У цьому випадку виконання зобов'язання за рахунок криптовалюту буде проблематичним.

У даний час більшість країн офіційно не визнають криптовалюту як об'єкти права (наприклад, в Бразилії цифрова валюта не вважається фінансовим активом, і тому прямі інвестиції в неї не допускаються). Однією з небагатьох країн, в яких дана діяльність врегульована, є Японія, де на законодавчому рівні дано визначення криптовалюти і послуг з їх обміну. В Японії криптовалюта визнана віртуальною валютою, а не грошима, еквівалентом майнової цінності, яку можна використовувати як платіжний засіб, купувати та продавати невизначеному колу осіб.

У Сполучених Штатах Америки криптовалюта розглядається різними регуляторами як аналог валюти та грошей, як власність (property) і як біржові товари.

В Україні закріплення на законодавчому рівні поняття «криптовалюта» сприятиме розвитку ринку цифрових технологій. Але в той же час названий законопроект не вирішить проблем, пов'язаних з функціонуванням на ринку криптовалюта та укладенням смарт-контрактів; навпаки, визнання криптовалюта цифровими грошима породить ще більше питань, які потребують вирішення.

---

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL. https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення 07.12.2019).

2. Україна піднялася в рейтингу цифрової конкурентоспроможності. (дата звернення 07.12.2019). URL. https://www.epravda.com.ua/news/2018/06/20/637985/
3. Криптовалюта в законі. Як депутати пропонують легалізувати цифрові гроші. (дата звернення 07.12.2019). URL. https://www.unian.net/economics/finance/10763129-kriptovalyuta-v-zakone-kak-deputaty-predlagayut-legalizovat-cifrovye-dengi.html

Управління інформаційною безпекою у інформаційних системах 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 кафедри інформатики Львівського державного коледжу харчової та переробної промисловості Національного університету харчових технологій

Наразі експертним співтовариством ведеться робота з визначення основних принципів та напрямків для покращення стану інформаційної та кібербезпеки в Україні. Основна ідея реформи – перейти від моделі, коли держава намагається контролювати безпековий сектор, у тому числі в приватних організаціях, до саморегуляції, яка дозволить бізнесу самостійно визначати і контролювати впровадження стандартів інфораційної і кібербезпеки для відповідних галузей. Роль держави у розбудові вітчизняної системи кіберзахисту та інформаційної безпеки (ІБ) потребує переосмислення. [1].

Розв'язання проблем протидії дезорганізації безпечного функціонування інформаційних систем (ІС) Національної поліції України (НПУ), модифікування інформації, яка обробляється в ІС, баз даних, програмного забезпечення на тлі небувалої активності кібератак є на сьогодні актуальними завданнями на державному рівні.

Несанкціонований доступ до інформаційних активів ІС може істотно ускладнити виконання завдань оперативними

підрозділами НПУ, тому проблема створення ефективної системи захисту інформації (ЗІ) набуває дуже важливого значення.

Згадані обставини диктують необхідність системного підходу до ідентифікування організаційних потреб стосовно захисту інформаційних активів ІС та створення ефективної системи менеджменту інформаційною безпекою (СМІБ), що дозволить структурувати наявні інформаційні активи і використовувати їх як моделі консолідованої інформації.

Аналіз наявних матеріалів стосовно проблеми захисту інформаційних активів ІС дає змогу виявити недоліки у методології проектування СМІБ, які суттєво впливають на ефективність функціонування усієї системи безпеки ІС. Серед головних відзначимо: системи безпеки ІС не враховують динаміки зміни загроз, не забезпечують достатній рівень стійкості систем безпеки до відмов та відновлення після збоїв; відсутність методик оцінювання ефективності СМІБ; ігнорування вимогами міжнародних стандартів у галузі ІБ при проектуванні СМІБ [2].

Ефективність системи захисту інформаційних активів ІС Національної поліції України залежить від прийняття виважених рішень, які підтримують, супроводжують і адаптують систему ІБ до постійно змінюваних умов функціонування.

Отже, виокремимо три складові, які безпосередньо пов’язані з порушенням безпеки ІС: загроза – зовнішнє, відносно ІС, джерело порушення властивості захищеності; об’єкт кібератаки – незалежна складова ІС, на яку спрямована загроза; канал дії – середовище перенесення зловмисної дії.

Уразливими є практично всі компоненти ІС. Серед них відзначимо: мережеві протоколи і пристрої, які формують мережеве оточення; операційні системи; СУБД і Web-сервери. Отже, власне забезпечення відсутності уразливостей повинно бути покладено в основу формалізування вимог щодо засобів захисту.

Для того, щоб привести систему захисту у відповідність до сучасних вимог, необхідно доповнити наявні рішення трьома

новими компонентами: аналіз захищеності; виявлення кібератак; управління інцидентами ІБ.

За своєю суттю СМІБ є вибором і управлінням відповідними заходами щодо захисту інформаційних активів ІС від визначених загроз відповідно до їх критичності функціонування. Вона є частиною комплексної системи управління ІТ, яка базується на оцінюванні та аналізі ризиків ІБ для розроблення, впровадження, адміністрування, моніторингу, підтримання, супроводу і розвитку ІБ на засадах використовуваних процедур, розмірів і структури СІС.

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 поліпшення.

Отже, якісне управління ІБ базується на наступних принципах: комплексний підхід – управління ІБ має охоплювати всі компоненти ІС і враховувати актуальні ризикоутворюючі чинники; узгодженість з стратегією ІБ; високий рівень керованості, безперервність управління; процесний підхід – зв'язування процесів управління у замкнутий цикл планування, впровадження, перевірки, аудиту та коригування; ефективність – раціональний баланс між можливостями, продуктивністю і витратами на СМІБ.

СМІБ повинна забезпечувати безпечність та надійність функціонування ІС і, на переконання авторів, проектуватися, впроваджуватися, функціонувати на засадничих принципах законодавства України та міжнародних угод, національних і міжнародних стандартів.

В Україні діє низка законів України та ухвалено ряд концептуальних нормативних документів різних рівнів, які охоплюють проблеми забезпечення інформаційної та кібернетичної безпеки держави, зокрема, Указ Президента України №47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»; 5 жовтня 2017 р. Верховна Рада України

приймає Закон України «Про основні засади забезпечення кібербезпеки України».

Зауважимо, що стандарт – це певна методологія і система формування вимог, у нашому випадку, для оцінювання безпеки інформаційних активів. Системність простежується починаючи від термінів і рівнів абстрагування, закінчуючи їх використанням під час розроблення, впровадження, сертифікування СМІБ.

Фахівцям у галузі ІБ неможливо обійтися без знань державних та міжнародних стандартів, тим більше, що дотримання вимог стандартів в Україні регламентується на законодавчому рівні. Положення і вимоги стандартів є однією з форм накопичення знань (зокрема, на процедурному і програмно-технічному рівнях ІБ). У них зафіксовані апробовані технічні рішення, методології, які розроблені провідними фахівцями. Стандарт надає найкращі практичні поради у галузі менеджменту інформаційною безпекою для тих, хто відповідає за розроблення та обслуговування таких систем.

Основним стандартом, на підставі якого можна провести роботи з створення та супроводу СМІБ є оновлений ISO/IEC 27001. Зауважимо, це не технічний стандарт, а управлінський.

Ще однією важливою особливістю стандарту ISO/IEC 27001 є те, що для контролю якості процесу менеджменту ІБ запроваджено інститут сертифікування. Сертифікат має міжнародний статус.

У процесі розроблення і впровадження СМІБ необхідно виконати: ухвалити рішення про створення СМІБ і визначити межі відповідальності посадових осіб; провести інвентаризування активів ІС; категоріювання активів ІС; аудит захищеності ІС з виявленням кіберзагроз; оцінити інформаційні ризики; розробити систему управління інформаційними ризиками; розробити бази нормативних документів з ІБ і домогтися їх виконання у повному обсязі.

Для процесів СМІБ застосована модель циклічного процесу з використанням принципу управління ІБ, ядро якої становить централізоване адміністрування (враховує специфіку функціонування ІС – дотримання режиму таємності).

Аналіз, оцінювання та управління ризиками, на думку авторів, провадитися на основі класичної моделі CIA (конфіденційності – confidentiality, цілісності – integrity, доступності – availability). Зокрема: конфіденційність – доступ до інформаційних активів винятково для офіційно авторизованих працівників у мінімально необхідному обсязі; цілісність – захист точності/коректності та повноти інформаційних активів ІС і методів оброблення інформації; доступність – забезпечення безперервного доступу до інформаційних та апаратних активів ІС, сервісів згідно з наданими працівникам повноваженнями та правами у необхідному обсязі. Окремо виноситься вимога спостережності – забезпечення принципу невідмови від вчинених дій. Сформульовані правила фіксуються у відповідних документах (документування процедур – одне з основних вимог стандарту ISO 27001) [3].

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми, навмисними та ненавмисними впливами, елементарною необізнаністю працівників у галузі ІТ необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІІБ), яка є базовою частиною загальної СМІБ і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти ІБ. Без реалізації цих процесів неможливо забезпечити рівень захищеності, який відповідає вимогам сучасних стандартів і галузевих норм.

Визначальною проблемою у функціонуванні СМІБ є відсутність системи моніторингу інцидентів ІБ. Тобто, відсутність інцидентів не вказує на те, що СМІБ працює правильно, а означає тільки те, що інциденти не фіксуються або не визначаються [4].

Стандарт ISO/IEC 27005 описує принципи управління інцидентами. Ключовим елементом ідеології стандарту є аналіз інцидентів з метою визначення які інформаційні активи ІС 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. Стандарт є доповнюючим до стандарту ISO/IEC 27001 у частині управління інцидентами ІБ.

Процес управління інцидентами є одним з найважливіших у постачанні даних для аналізу функціонування СМІБ, оцінювання ефективності використовуваних заходів, зниження ризиків і удосконалення захисту ІС.

За своєю суттю СМІБ є вибором і управлінням відповідними заходами щодо захисту інформаційних активів СІС від визначених кіберзагроз відповідно до їх критичності функціонування [4].

Як висновок відзначимо, що проведений аналіз дає підстави стверджувати: прийняття адекватних рішень у сфері створення, експлуатування та супроводу СМІБ матиме успіх лише за умови чіткого визначення і трактування основних понять і термінів; визначальною проблемою у функціонуванні СМІБ є відсутність системи моніторингу інцидентів ІБ; тільки суворий поточний контроль захищеності ІС, який спроможна реалізувати СМІБ на основі моделі адаптивної безпеки дозволить суттєво знизити ризики ІБ.

1. Янковський О. Україні потрібна нова кіберстратегія / Електронний ресурс. Шлях доступу: https://www.pravda.com.ua /columns/2019/09/14/7226291/.
2. 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. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
3. Рудий Т. В. Живко З. Б. Сеник В. В. Технології кримінального аналізу у практиці протидії кіберзлочинності / Т. В. Рудий, З. Б. Живко, В. В Сеник // Соціально-правові студії: науково-аналітичний журнал / гол. ред. О. Балинська. Львів: ЛьвДУВС, 2018. Вип. 2. – С.40-48.
4. Sereda, V., Zhyvko, Z., Balynska, O., Rudyi, T. (2019, July 15). The Organizational Principles of Information Protection Management System Realization. (Z. Cekerevac, Ed.) MEST Journal, 7(2), 73-78. doi:10.12709/mest.07.07.02.09.

Проблеми застосування вимог міжнародних стандартів під час здійснення процесуальних дій з цифровими доказами

Зачек Олег Ігорович

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

Рудий Тарас Володимирович

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

В наш час великого розповсюдження набули кіберзлочини, тобто злочини у сфері інформаційних технологій. За словами першого заступника начальника департаменту кіберполіції Олександра Гринчака, до переліку злочинів, які вчиняють в Україні кіберзлочинці, входять крадіжки з банківських карток, даних з комп'ютерів, інформації з телефонів, запуск вірусів вимагачів, шантаж компаній та здійснення крипто-афер. Найпоширеніший вид злочину – це шахрайство в мережі Internet, таких шахрайств вдалося виявити 2798, з яких у 2314 випадках були пред'явлені підозри про вчинення злочину. Кількість кіберзлочинів в Україні щороку зростає на кілька тисяч [1].

Класифікація кіберзлочинів дається у Конвенції про кіберзлочинність, ратифікованій Україною у 2005 році. Згідно з положеннями цієї конвенції є такі основні види кіберзлочинів: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями, підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами, правопорушення, пов'язані з дитячою порнографією, правопорушення, пов'язані з порушенням авторських та суміжних прав [2].

Під час розслідування таких злочинів важливого значення набуває збір та зберігання цифрових доказів із дотриманням процесуальних вимог, оскільки порушення правил поводження з такими доказами може звести нанівець доказову базу. Однією з проблем є відсутність визначення цифрових (електронних) доказів у Кримінальному процесуальному кодексі України [3]. Зазначена проблема згадувалась у Звіті щодо України від 03.11.2016 № 2016/DGI/JP/3608, підготовленому офісом програми боротьби з кіберзлочинністю на основі підтримки експертів Ради Європи. Автори звіту пропонують запровадити до Кримінального процесуального кодексу спеціальну дефініцію – поняття електронних доказів або запровадити до загального визначення доказу зміни, які б дозволили з належною точністю та передбачуваністю охопити сферу застосування доказу в електронній формі [4].

Певною мірою, хоча і не в повному обсязі, проблема визнання цифрових доказів була вирішена прийняттям змін до КПК України, які були внесені Законом України № 2213-VIII від 16.11.2017 «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування» [5]. Ці зміни визначили статус інформації в цифровому (електронному) вигляді, яка здобута слідчим, прокурором способом копіювання. Згідно частини 4 статті 99 КПК тепер: «Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа». Також стаття 168 КПК була доповнена абзацами такого змісту:

«Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення

кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

У разі необхідності слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста» [5].

До цифрових доказів належить інформація в цифровій (електронній) формі, яка містить дані про обставини, що мають значення для провадження, зокрема:

- електронні документи;
- Web-сторінки та Web-сайти;
- бази даних, метадані та інші дані в електронній формі;
- голосові, мультимедійні та текстові повідомлення.

Ці дані можуть зберігатися на магнітних носіях, оптичних носіях, флеш-накопичувачах, на серверах та в персональних комп'ютерах, в системах резервного копіювання, хмарних сервісах.

Хоча у КПК України наголошується, що копіювання інформації повинно здійснюватися із залученням спеціаліста, це не гарантує якості доказів. Належне поводження з цифровими доказами може бути забезпечене лише з використанням вимог національних та міжнародних стандартів.

Національні стандарти України у галузі ідентифікування, збору, накопичення, оброблення та захисту, збереження цифрових судово-медичних даних, гармонізовані з міжнародними нормативними документами, було прийнято методом підтвердження з наданням чинності з 10 жовтня 2016 року. Головним із них є ДСТУ ISO/IEC 27037:2016 – Інформаційні технології. Методи захисту. Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів. Цей стандарт надає інструкції щодо ідентифікування, збору (збирання), накопичення, оброблення та захисту, збереження цифрових судово-медичних даних, тобто цифрових даних, які можуть бути доказами у суді.

У 2017 році наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 06.12.2017 № 400 [6] було прийнято національні нормативні документи, гармонізовані з європейськими та міжнародними нормативними документами, методом перекладу з наданням чинності з 01 січня 2019 року. Зокрема, ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Він прийнятий на заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT). У цьому Національному стандарті викладені нюанси поводження з цифровими доказами.

Одним із найважливіших завдань цифрової судової експертизи є накопичення та збереження доказів так, щоб забезпечити їх цілісність. Як і у випадку із звичайними фізичними даними, важливо зберегти ланцюг контролю над усіма цифровими доказами, гарантуючи, що вони збираються та захищаються через структуровані процеси, прийнятні для судів. Це вимагає, щоб був досягнутий визначений базовий рівень контролю безпеки інформації. Цифрові судово-медичні докази можуть накопичуватися з довільних електронних носіїв або засобів зв'язку. За своєю природою цифрові криміналістичні докази є уразливими – вони можуть бути легко пошкоджені або модифіковані через неправильне поводження, випадково або з певною метою.

Стандарт надає детальні вказівки щодо ідентифікування, збору та/або накопичення, маркування, зберігання, транспортування та збереження електронних доказів, зокрема, для збереження їх цілісності. Він визначає й описує процеси, за допомогою яких визнаються та ідентифікуються докази, документування місця злочину, збирання та збереження доказів, а також упакування та транспортування доказів [7, с. 295-296].

Основні вимоги стандарту, за умови виконання яких копіювання інформації може бути надійним та допустимим з технічної сторони [8]:

1. Недопустимість внесення змін до первинної інформації, яка є об'єктом копіювання, як до самого копіювання, так

під час і після копіювання. Для цього використовують пристрої блокування запису, які дозволяють лише зчитування інформації без можливості запису, під час підключення носіїв інформації до комп'ютера спеціаліста або слідчого.

2. Верифікація інформації, яка скопійована. Для цього необхідно використовувати хешування первинної інформації, щоб мати можливість перевірити тотожність копії інформації, яка записана на інший електронний носій інформації. У стандарті згадані відомі алгоритми хешування MD5, SHA1.

Але є проблема імплементації вимог ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) в діяльність правоохоронних органів України. Немає нормативних документів, які б вимагали застосування вимог вищезазначеного стандарту під час процесуальних дій. Навіть у Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року [9] не передбачено запровадження вимог ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) у діяльність слідчих підрозділів.

Висновки. Існує нагальна необхідність внесення змін до Кримінального процесуального кодексу України, які б дали чітке визначення цифрових (електронних) доказів та містили вимоги не тільки щодо залучення спеціаліста, але і щодо застосування ДСТУ під час процесуальних дій з такими доказами. Також необхідно запроваджувати вимоги щодо застосування ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) органами системи Міністерства внутрішніх справ до нормативних документів МВС.

---

1. Що варто знати про кіберзлочинців в Україні? [Електронний ресурс]. URL: https://www.radiosvoboda.org/a/details/29031166.html (дата звернення: 29.11.2019).
2. Конвенція про кіберзлочинність: міжнародний документ. Ратифікація від 07.09.2005, підстава - 2824-IV. // Офіційний вісник України. 2007 р. № 65. Стор. 107. Стаття 2535. Код акта 40846/2007.

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI // Відомості Верховної Ради України. 2013. № 9-10. Ст. 88.
4. Студенников С. Електронні докази: які проблеми фіксує судова практика. Судебно-юридическая газета від 23.08.2019. [Електронний ресурс]. (дата звернення: 17.11.2019) URL: https://sud.ua/ru/news/ publication/148501-elektronni-dokazi-yaki-problemi-fiksuye-sudova-praktika.
5. Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування: Закон України від 16.11.2017 № № 2213-VIII // Відомості Верховної Ради України, 2017, № 49-50, ст.444.
6. Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів: Наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 06.12.2017 № 400. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/ rada/show/v0400774-17 (дата звернення: 17.11.2019).
7. Рудий Т. В., Сеник В. В., Рудий А. Т., Сеник С. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. Львів: ЛьвДУВС, 2018. Вип. 1. С. 283-301.
8. Електронні докази в кримінальному процесі України. [Електронний ресурс]. (дата звернення: 29.11.2019) URL: https://www.e-dokaz.info/2019/04/blog-post.html.
9. 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 // Урядовий кур'єр від 13.03.2018, № 48.

Електрошокові пристрої: історія та принципи дії

Зачек Олег Ігорович

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

Синківська І.А.

здобувач вищої освіти
Львівського державного університету внутрішніх справ

Стрімкий розвиток науково-технічного прогресу призвів до розвитку сфери озброєння, що відобразилось на екіпіруванні поліцейських у різних країнах світу. Основним завданням у боротьбі з правопорушниками є їх затримання та відвернення наслідків правопорушення. Для виконання цього завдання з успіхом може застосовуватись електрошоковий пристрій. Електрошоковий пристрій увійшов у спорядження працівників поліції – як спеціальний засіб, який не вбиває, а лише стримує та припиняє небезпечні діяння правопорушників, дозволяючи уникнути застосування вогнепальної зброї.

Електрошоковий пристрій (ЕШП) – один із видів зброї несмертельної дії поряд із газовою зброєю, пістолетами з боєприпасами травматичної дії, гумовими кийками, аерозолями сльозоточивої та дратівної дії [1]. Вперше електрошокову зброю було запатентовано як пристрій для полювання на китів у морі, що вбиває китів електричним розрядом за допомогою електрогенератора, що знаходився в шлюпці китобоїв [2].

У 1915 році американець Генрі Діксон винайшов і запатентував хлист, який, перебуваючи під напругою, давав можливість господареві контролювати дії худоби [3]. У 70-х роках XX ст. у США виникла увага до проблеми невмотивованого застосування вогнепальної зброї під час затримання підозрюваних у здійсненні карних злочинів, а також під час припиненні масових безладів. Виникла потреба в створенні засобу, що дозволяє здійснювати

затримання без нанесення каліцтв і шкідливих наслідків для здоров'я.

У 1974 р американець Джон Ковер отримує патент США № 3,803,463 на винахід «Зброя для знерухомлення і затримання», який ґрунтувався на впливі на людину високовольтними електричними імпульсами [4]. Запатентована зброя, яка була названа електрошокером, була взята на озброєння службами правопорядку і застосовувалося для затримання злочинців у випадках, коли недоцільно було використовувати вогнепальну зброю. Ефективно застосовуваний поліцією в усьому світі, електрошокер незабаром став використовуватися для самооборони і простими громадянами, надаючи можливість захиститися у разі раптового нападу [2]. Однак, тривалий час така новинка залишалась непотрібною для суспільства. І тільки у 90-х роках винайдений Джоном Ковером пристрій заінтригував розробників з декількох компаній. Внаслідок цього на ринку США з'явилося багато зразків ЕШП. Фаворитами в даній області з плином часу стали компанії Tasertron і Taser International [5]. За більш як 40 років, що пройшли відтоді, електрошокери зайняли своє місце на ринку засобів забезпечення громадської безпеки, у тому числі і як засіб самооборони громадян [1].

Перевірка ефективності дії електрошокової зброї на людину в різних країнах здійснюється різними методами. Найбільш об'єктивним способом визначення ефективності ЕШП TASER і дистанційного ЕШП TASER в США вважається випробування на свинях, як на біологічних об'єктах, адже вони фізіологічно і по масі тіла найбільш є близькі до людини. У Росії, де випробування нелетальної зброї на людях заборонені законодавчо, перевірка ефективності ЕШП проводитися порівняльним способом на кроликах породи шиншила. Такий метод перевірки ефективності електрошокової зброї можна вважати ще менш коректним, ніж перевірка ефективності на свинях, через значно більші відмінності у фізіологічних особливостях організму гризунів і людини, а крім того, величезні відмінності маси тіла [2].

Порівняльні випробування на людях проводяться за різними методиками, з обов'язковим залученням до випробувань медичних фахівців і лікарів реаніматологів. Сьогодні проводяться фактично тільки випробування дистанційних ЕШП (ДЕШП), так як у зв'язку з малою петлею струму, випробування ЕШП не дають достовірних результатів. Зазвичай випробування проводять без відстрілу дротиків, з тим щоб даремно не травмувати. Електроди імітують потрапляння в тіло людини дротиків, що розташовуються на відстані один від одного і закріплюються на одежі випробуваного. Вражаючий імпульс подається по проводах від випробуваного виробу. Залежно від обраних умов випробувань по голосовому відліку, або несподівано для випробуваного подаються вражаючі імпульси струму. У деяких випадках випробуваному дається завдання по відчуттю розряду зробити активні дії (наприклад напасти з гумовою палицею, ножем або просто кулаками) на людину, що імітує захист за допомогою ДЕШП [2].

Наукова оцінка дії ЕШП проводиться фактично не менше як 20 років, тобто фактично з часу широких досліджень впливу на людей ДЕШП компанії Taser International. Основною відмінністю впливів промислового струму на людей від впливу електрошокових пристроїв є не значення напруги, а тільки вихідна потужність джерел ураження, яка практично завжди більше, ніж вихідна потужність електрошокових пристроїв в десятки і тисячі разів [2].

Фактичних критеріїв ефективності дії ЕШП по теперішній час не встановлено. Перш за все, тому, що технічно не було створені портативні моделі таких засобів, що викликають з великою часткою ймовірності смертельний результат. Природно, що в цьому випадку межі летальності і нелетальності ЕШП, між просто «больовими відчуттями» і «смертельним ураженням», не були встановлені. У 2007 р. в юридичній практиці вважалося, що зразків автономного (за критерієм можливості прихованого носіння під одягом) летального ЕШП і ДЕШП не існує у вигляді реальних пристроїв, хоча технічну можливість створення таких пристроїв не заперечують. При цьому законодавчого та юридичного визначення летального ЕШП не існує до цього часу [2].

ЕШП досить ефективно знешкоджує зловмисника, не завдаючи при цьому шкоди здоров'ю через малу силу струму. При застосуванні ЕШП одяг не є перешкодою, сила розряду здатна пробити кілька шарів тканини, при щільному зіткненні шокера з тілом супротивника. Застосування електрошокера дозволяє досягти швидкого ефекту і моментально зупинити атаку супротивника [6].

Біофізичні властивості ЕШП пов'язано не тільки з болем від ураження струмом. Енергія, яка накопичена в ЕШП, при контакті дуги електричного розряду зі шкірою перетворюється в змінну електричну напругу зі спеціально розрахованою частотою, що змушує м'язи в зоні контакту скорочуватися надзвичайно швидко. Ця ненормальна надмірна активність м'язів призводить до блискавичного розкладання цукру крові, який живить м'язи. Дія електричного розряду від ЕШП призводить до можливої короткочасної втрати свідомості, а також тимчасового паралічу м'язів, максимальна тривалість якої не перевищує півгодини [7]. Тобто, м'язи в зоні контакту на якийсь час втрачають працездатність. Паралельно імпульси блокують діяльність нервових волокон, за якими мозок управляє даними м'язами. Результатом стає місцевий параліч, який залежно від різних обставин проходить швидше або повільніше [8]. Оскільки струм моментально поширюється по м'язовій тканині і викликає її спазм – агресор буде відчувати сильний і різкий біль, через який може спостерігатися втрата свідомості або ж тимчасове порушення орієнтації в просторі. Подібний ефект спостерігається у людей, які відчувають інтенсивні больові відчуття через отриману травму.

На ефективність застосування ЕШП впливає багато показників. Це стан людини, товщина одягу, тривалість застосування, потужність приладу і інші технічні характеристики [9]. Принцип роботи шокера полягає в перетворенні напруги до 30-110 тисяч вольт, що впливає на довжину дуги і забезпечує пробій одягу, і формуванні правильного високовольтного імпульсу для ефективного біоелектричного впливу [10].

Електрошокери поділяються на контактний електрошоковий пристрій (ЕШП) і дистанційний електрошоковий пристрій

(ДЕШП). Використання контактного ЕШП можливо тільки при безпосередньому контакті з нападаючим. Тобто для того щоб вразити супротивника електрострумом, ви повинні підійти до нього на відстань витягнутої руки, уперти контакти ЕШП в його тіло, після чого і увімкнути електрошокер. Щодо ДЕШП, то таким електрошокером супротивника можна вражати вже не тільки контактним способом, але й перебуваючи на значній відстані від нього. Поразка відбувається завдяки відстрілу електродів, які з'єднані з ЕШП тонкими проводами, по яких і проходить електричний струм. Потрапляючи в тіло супротивника, вони спричиняють такий же ефект, як і звичайні контактні ЕШП [11].

Отже, дослідивши історію виникнення ЕШП, його ефективність у застосуванні з метою припинення правопорушень, біофізіологічний вплив та наслідки впливу електричного імпульсу на організм людини, а також принцип дії та параметри даного пристрою, можна прийти до висновку, що ЕШП є ефективним засобом для припинення правопорушень. Їх вплив на правопорушника є дуже ефективним, оскільки окрім фізичного болю від ЕШП особа ще отримує певний психологічний бар'єр перед працівником поліції. Звук і вигляд високовольтного електричного розряду увімкнутого електрошокера заставляють особу, що скоїла правопорушення, утриматись від подальших дій та припинити свої діяння, що в свою чергу дозволяє працівнику поліції стабілізувати ситуацію.

---

1. Іванілова Н. А., Шевчук М. А. Елекрошоковий пристрій: особливості використання // Сучасна спеціальна техніка. 2009. № 2 (17). С. 43-47.
2. Электрошоковое оружие. [Електронний ресурс]. URL: http://www.interwiki.info/index.php?title=Электрошоковое_оружие (дата звернення: 03.12.2019).
3. История создание электрошокеров. [Електронний ресурс]. URL: http://shokeru.com.ua/index.php?route=information/news&news_id=21 (дата звернення: 03.12.2019).

4. Безопасность, спецоснащение. Все для Вашей безопасности. История электрошокеров как средств самообороны. [Електронний ресурс]. (дата звернення: 03.12.2019). URL: http://www.ois.org.ua/club/bezopasnost/electroshock04.htm
5. Электрошокер как оружие самообороны. [Електронний ресурс]. URL: http://consultpg.com/2170-elektroshoker-kak-oruzhie-samooborony.html (дата звернення: 03.12.2019).
6. Электрошокер – закон и использование. [Електронний ресурс]. URL: httpHYPERLINK «http://guard.lviv.ua /bezopasnost/elektroshoker-zakon-i-ispolzovanie»://HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»guardHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie».HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»lvivHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie».HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»uaHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»/HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»bezopasnostHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»/HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»elektroshokerHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»-HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»zakonHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»-HYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-ispolzovanie»iHYPERLINK «http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-

ispolzovanie»-HYPERLINK
«http://guard.lviv.ua/bezopasnost/elektroshoker-zakon-i-
ispolzovanie»ispolzovanie (дата звернення: 03.12.2019).
7. Последствия использования электрошокеров. [Електронний ресурс]. (дата звернення: 03.12.2019) URL: http://shoker5.in.ua/posledstvia-ispolzovania-electroshokerov.
8. Техника для спецслужб. Электрошокеры. [Електронний ресурс]. URL: http://www.bnti.ru/ showart.asp?aid=63&lvl=08.01.02 (дата звернення: 03.12.2019).
9. Вплив розряду електрошокера на людей. [Електронний ресурс]. URL: http://elektroshokery.in.ua/ ua/how_to_hit_ electroshock_effect_on_human (дата звернення: 09.12.2019).
10. Что такое электрошокер, ЭШУ, ЭШО? [Електронний ресурс]. URL: http://elektroshoker.org/faq (дата звернення: 09.12.2019).
11. Вибір і застосування електрошокера. [Електронний ресурс]. URL: http://www.comm.webfermer.org.ua/rizne /vybir-i-zastosuvannja-elektroshokera.php (дата звернення: 11.12.2019).

Інформаційна підсистема «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»

Омельяненко Оксана Валеріївна

викладач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ

Відповідно до ст.ст. 25-27 Закону України «Про Національну поліцію», ст. 36 Закону України «Про виконавче провадження», підпункту 40 пункту 4 Положення про Національну поліцію, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2015 року № 877, з метою забезпечення оперативного реагування та прийняття ефективних управлінських рішень щодо розшуку транспортних засобів та номерних знаків, а також приведення нормативно-правових актів у сфері діяльності Національної поліції України у відповідність до законодавства України, наказом МВС України від 13 червня 2018 року № 497 (зареєстрованого в Міністерстві юстиції України 06 липня 2018 р. за № 787/32239) запроваджено в експлуатацію та затверджено Інструкцію з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

Інформаційна підсистеми «Гарпун» (далі – ІП «Гарпун») інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі – система ІПНП) призначена для обробки відомостей про транспортні засоби (далі – ТЗ) усіх типів (автомобілі, автобуси, мотоцикли всіх типів, марок і моделей, самохідні машини, причепи та напівпричепи до них, мотоколяски, інші прирівняні до них ТЗ та мопеди) та номерні знаки ТЗ (далі – номерні знаки), що розшукуються у рамках кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду.

Метою ІП «Гарпун» є:

- об’єднання інформації про розшук ТЗ та номерних знаків в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп’ютерного та телекомунікаційного обладнання;
- забезпечення оперативного реагування та прийняття управлінських рішень посадовими особами органів (підрозділів) поліції щодо розшуку ТЗ та номерних знаків;
- моніторинг тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних ТЗ (номерні знаки – двійники), використання номерних знаків, що за даними Єдиного державного реєстру Міністерства внутрішніх справ України (далі – ЄДР МВС) знищено;
- забезпечення взаємодії з державними та приватними виконавцями під час розшуку ТЗ боржника у виконавчому провадженні.

Формування ІП «Гарпун» здійснюється за допомогою програмно-технічних засобів системи ІПНП.

Облік об’єктів в ІП «Гарпун» ведеться **за такими категоріями**:

- орієнтування про незаконне заволодіння ТЗ;
- орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди;
- орієнтування про залишення ТЗ місця вчинення іншого правопорушення;
- орієнтування оперативне про ТЗ;

Орієнтування – доведення до особового складу органів (підрозділів) поліції інформації про можливу причетність водія або пасажирів ТЗ до вчинення дорожньо-транспортної пригоди (далі – ДТП), кримінального чи адміністративного правопорушення або інформації, яка свідчить про те, що ТЗ чи вантаж можуть бути об’єктом чи знаряддям учинення ДТП, кримінального чи адміністративного правопорушення.

Метою орієнтування є забезпечення оперативного реагування та прийняття ефективних управлінських рішень посадовими особами органів (підрозділів) поліції щодо розшуку ТЗ.

Обліку в ІП «Гарпун» за категоріями «орієнтування про незаконне заволодіння ТЗ», «орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди», «орієнтування про залишення ТЗ місця вчинення іншого правопорушення» та «орієнтування оперативне про ТЗ» підлягають відомості про розшук ТЗ, які стали засобом, предметом кримінального чи адміністративного правопорушення або місцезнаходження яких встановлюється під час здійснення оперативно-розшукової діяльності.

Евакуйовані ТЗ.

Обліку в ІП «Гарпун» за категорією «евакуйовані ТЗ» підлягають відомості про ТЗ, евакуйовані до спеціального майданчика чи стоянки.

Підставою для внесення відомостей до ІП «Гарпун» про евакуйований ТЗ є акт огляду та тимчасового затримання ТЗ, складений поліцейським або інспектором з паркування.

Розшук ТЗ у зв'язку із незаконним заволодінням. Розшук ТЗ, що залишив місце дорожньо-транспортної пригоди.

Обліку в ІП «Гарпун» за категоріями «розшук ТЗ у зв'язку із незаконним заволодінням» та «розшук ТЗ, що залишив місце ДТП» підлягають відомості про розшук ТЗ у зв'язку із незаконним заволодінням, у тому числі про ТЗ, які розшукуються у зв'язку зі зникненням безвісти особи, про розшук ТЗ, водії, власники (співвласники) яких залишили місце ДТП, унаслідок яких загинули або травмовані люди та за фактом подій розпочато кримінальні провадження.

Розшук ТЗ за іншими кримінальними правопорушеннями.

Обліку за категорією «розшук ТЗ за іншими кримінальними правопорушеннями» в ІП «Гарпун» підлягають відомості про розшук ТЗ, інформація щодо яких надходить до підрозділів інформаційно-аналітичної підтримки Національної поліції України (далі – ІАП) з органів досудового розслідування України у рамках кримінального провадження.

Розшук ТЗ боржника державним виконавцем.
Розшук ТЗ боржника приватним виконавцем.

Обліку за категоріями «розшук ТЗ боржника державним виконавцем» та «розшук ТЗ боржника приватним виконавцем» в ІП «Гарпун» підлягають відомості про розшук ТЗ боржника.

ТЗ боржника, надіслається до системи ІПНП в електронному вигляді з використанням електронного цифрового підпису державного або приватного виконавця, який виніс відповідну постанову, через автоматизовану систему виконавчого провадження (далі – АСВП) відповідно до Порядку взаємодії Міністерства внутрішніх справ України, Національної поліції України та органів і осіб, які здійснюють примусове виконання судових рішень і рішень інших органів, затвердженого наказом Міністерства внутрішніх справ України, Міністерства юстиції України від 30 січня 2018 року № 64/261/5, зареєстрованого у Міністерстві юстиції України 05 лютого 2018 року за № 140/31592.

Розшук викраденого номерного знака.
Розшук втраченого номерного знака.
Знищені номерні знаки.

Обліку за категоріями «розшук викраденого номерного знака», «розшук втраченого номерного знака» та «знищені номерні знаки» в ІП «Гарпун» підлягають відомості про викрадені, втрачені та знищені номерні знаки.

Програмний модуль ІП «Гарпун» аналітичної обробки та інформування про розшук ТЗ або номерного знака.

Програмний модуль ІП «Гарпун» аналітичної обробки та інформування про розшук ТЗ або номерного знака – спеціалізоване програмне забезпечення, створене для запобігання вчиненню правопорушень, аналізу тимчасового набору даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних ТЗ (номерні знаки – двійники), використання знищених знаків, а також для автоматизованого інформування про такі факти диспетчерів,

оперативних чергових, нарядів поліції органів (підрозділів) поліції та ініціаторів розшуку.

Для аналітичної обробки використовується фото- і відеоінформація, отримана з технічних засобів та технічних приладів, які мають функції фото- і відеофіксації (запису), закріплених поліцією на службових ТЗ, монтованих/розміщених по зовнішньому периметру доріг і будівель, а також інформація, отримана з автоматичної фото- і відеотехніки, що знаходиться в чужому володінні.

Порядок отримання інформації, використання технологій доступу, типів наборів даних, обсяг та структура даних, до яких надається доступ з автоматичної фото- і відеотехніки, що знаходиться в чужому володінні, відповідно до потреб Національної поліції України визначаються згідно із законодавством України.

Впровадження відеоаналітики в Україні: вітчизняний та зарубіжний досвід

Прокопов Сергій Олександрович

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

Пронічкіна Анастасія Сергіївна

курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

На сьогоднішній день дуже багато злочинів вчиняється на вулиці і для встановлення осіб, які вчинили ці злочини доцільним стало впровадження проекту «Безпечне місто». Держава повинна забезпечити публічну безпеку громадянам нашої країни, а також охороняти їх права та свободи від посягань зі збоку злочинців. З цього і починається протидія злочинності. Камери «Безпечне місто» не так давно почали свою діяльність, проте дали вже значну кількість розкритих злочинів. Необхідність впровадження даного проекту, зумовлена високим розвитком злочинності, їх обізнаності та винахідливості [1].

Запровадження системного підходу до створення єдиної системи відеонагляду та відеоаналітики є одним з пріоритетів подальшої розбудови Національної поліції України.

Нині, в користуванні поліції близько 11,5 тис. відеокамер, зображення з яких передаються до ситуаційних центрів. Із зазначеної кількості півтори тисячі – так звані «розумні камери», які наділені функціональними можливостями розпізнавання номерів транспортних засобів, а також облич [1].

Через досить велику кількість ДТП, раніше, злочинець міг втекти та бути не покараним, якщо не було очевидців та інших свідків аварії, зараз же можливо переглянути подробиці ДТП за камерами «Безпечне місто». Проте, не завжди вдається

розгледіти державний номер машини, адже існують певні нюанси (погане освітлення, бюджетна камера тощо).

Беручи до уваги досвід зарубіжних країн – камери використовуються в європейських країнах досить довго. Вони слугують фіксатором правопорушень та базою для перевірки алібі (переглядаючи запис, можливо зрозуміти де знаходилась особа).

Наприклад, проаналізувавши використання камер відеоспостереження в Польщі, вони використовуються в першу чергу для боротьби з перевищенням швидкості та порушень ПДР. Прилади фіксують всі порушення на дорогах, проте помітити такі засоби фіксації на дорогах дуже важко. Крім того порушенням закону буде застосування засобів для виявлення засобів фіксації. За перевищення швидкості польська поліція може карати не тільки громадян своєї країни, але й всіх учасників ЄС, адже це питання врегульовано міжнародним договором.

Ще однією країною, яка має високотехнологічні камери є Швейцарія. Ця країна має найсуворіші санкції до любителів швидкої їзди. За межами міста заборонено пересуватись зі швидкістю більше 140 км/год. Контроль за пересуванням авто здійснює камера і може фіксувати швидкість пересування одночасно на чотирьох смугах [2].

Також камери «Безпечне місто» дають змогу розкривати й інші злочини. На Чернігівщині з використанням камер відеоспостереження упродовж 2018 року розкрито 30 тяжких та особливо тяжких злочинів, з яких 3 розбої, 14 грабежів, 4 незаконних заволодіння транспортними засобами, 2 хуліганства з використанням зброї.

Завдяки камерам відеоспостереження можливо встановлювати особу, яка вчинила злочин на вулиці – розбій, грабіж, вбивство. Наприклад, у місті Луцьк за аналітичною інформацією з камер відеоспостереження встановлено групу осіб, які в листопаді скоїли умисне вбивство однієї особи та заподіяли тілесні ушкодження іншій.

Камери «Безпечного міста» використовуються у підсистемі «Гарпун» [3] Інформаційного порталу Національної поліції, яка

автоматично перевіряє номери авто на предмет перебування у розшуку. Одним з лідерів у використанні можливостей даної системи є Ситуаційний центр ГУНП в Дніпропетровській області.

Щодо розбудови систем відеонагляду та відеоаналітики в Дніпропетровській області слід зазначити, що найбільш динамічно вона розбудовується у місті Дніпро, де за ініціативою поліції та підтримки Дніпровської міської ради була прийнята програма «Безпечне місто», в рамках якої на території міста встановлено і підключено до єдиної мережі 697 камер відеоспостереження, з яких 280 здатні розпізнавати номерні знаки транспортних засобів.

В інших містах та районах області встановлено 418 відеокамер: у м. Нікополь (122), Кам'янське (100), Павлоград (62), Кривий Ріг (46), Тернівка (13), Марганець (6), Петропавлівка (6), П'ятихатки (2). Крім цього, у березні поточного року встановлено 61 камеру у м. Синельникове.

Всього, у населених пунктах Дніпропетровської області встановлено 1115 відеокамер, з яких 319 здатні розпізнавати номерні знаки транспортних засобів.

На теперішній час до Ситуаційного центру ГУНП надходить відеосигнал з 1067 камер, які встановлені в населених пунктах області, з них 296 здатні розпізнавати номерні знаки.

Отже, даний проект має позитивні відгуки від поліцейських всієї України. Це дозволяє швидше та результативніше розкривати злочини різкої тяжкості, проте через відсутність єдиного підходу до розбудови та використання систем відеоспостереження, це призводить до погіршення можливостей централізованого аналізу відеоінформації, її подальшого використання працівниками територіальних органів поліції (чергової служби, ситуаційного центру, оперативних підрозділів, слідчо-оперативних груп та ін.) та центрального органу управління поліції. Вважаючи, що відеообладнання закупають та встановлюють територіальні громади, необхідно створити загальнодержавний нормативно-технічний акт, який би регламентував технічні вимоги для камер,

які можна використовувати для відеоаналітики не тільки щодо автоматичного розпізнавання автотранспорту, а і ідентифікації осіб, що розшукуються.

---

1. Проект «Безпечне місто» . [Електронний ресурс]. – URL: https://www.datagroup.ua/pro-kompaniyu/socialna-vidpovidalnist /bezpechne-misto
2. Війна з ДТП: які закони дорожнього руху діють в Європі . [Електронний ресурс]. – URL: https://rubryka.com/article /vijna-z-dtp/
3. Наказ МВС України «Про підсистему Інформаційного порталу «Гарпун» від 13.06.2018 за № 497.

Розвиток систем відеоаналітики у правоохоронній діяльності

Прокопов Сергій Олександрович

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

Темрієнко Наталія Володимірівна

курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

На сьогодні метою стрімкого розвитку інтелектуального відеоспостереження в усьому світі є намагання побудувати перехід від монотонного перегляду великої кількості моніторів до комп'ютерного зору, коли оператору надається виключно важлива інформація під час порушення алгоритмів безпеки. В останнє десятиліття системи відеоспостереження стають популярним інструментом, що широко використовується правоохоронними органами держав, проте відеоматеріалів накопичується безліч, систематизувати її досить складно, а іноді зовсім неможливо. Для вирішення поставленого завдання можна задіяти аналіз відеоданих. Так, можливо зробити швидкий та ефективний пошук необхідного фрагменту в архівних записах та своєчасне детектування події у відеоряді, що транслюється в реальному часі, використовуючи сучасні алгоритми обробки. Разом з тим, існує інша проблема – надлишкова інформація, що є вкрай нагальною для сучасних систем відеоспостереження, обсяг даних яких значно збільшився. Однією з відповідей на це питання є автоматична обробка відеоданих або відеоаналіз.

Перш за все слід зауважити, що відеоаналітика працює на базі системи відеоспостереження, матеріали з яких оброблюються та систематизуються.

Отже, системи відеоспостереження (англ. Closed-circuit television, CCTV) – це програмно-апаратний комплекс

(відеокамери, об'єктиви, монітори, реєстратори та ін. обладнання), призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах [1, с. 387].

Слід наголосити, що відеоспостереження сьогодні є невід'ємним елементом будь-якої сучасної системи безпеки. Основними завданнями, розв'язувані за допомогою відеоспостереження, є:

- візуальний контроль ситуації на об'єкті, що охороняється – надає інформацію на пост спостереження в мультиекран (в режимі очікування) або в повноекранному режимі (зображення від однієї телекамери на весь екран) в режимі реального часу. Це забезпечує можливість прийняття оперативних рішень, адекватних конкретній ситуації;
- можливість організації безперервного відеозапису відеоспостереження на цифровий відеореєстратор або комп'ютерну систему – дозволяє документально підтвердити факт порушення і надає можливість для проведення ефективного аналізу кожної ситуації;
- виконання функцій охоронної сигналізації при використанні детекторів руху відеокамер або зовнішніх охоронних датчиків і інформованість оператора системи про виникнення тривоги в контрольованій зоні з допомогою світлового та звукового сигналу оповіщення. При цьому спрацьовування детектора руху може автоматично активувати запис для повної реєстрації тривожної ситуації, запускатися один з безлічі сценаріїв реакції системи – запуск виконавчих механізмів, зміна режиму роботи компонента системи, запуск інших програм або ж комбінація всіх цих подій [1, с. 388].

Таким чином, система відео контролю стає невід'ємною частиною протидії та запобігання правопорушенням правоохоронними органами, зокрема органами Національної поліції України. Окрім цього, програми впровадження систем відеоспостереження здатні поліпшити ставлення громадськості до роботи правоохоронних органів та забезпечити захист поліцейських при виконанні службових обов'язків.

Вникаючи в сутність відеоаналітики, дослідники диференціюють її наступним чином:

- жорстка відеоаналітика, яка заснована на класифікації об'єктів, а її основою стає детектор вказаних об'єктів. У жорсткій відео аналітиці всі моменти визначення класу цілі та її дій вимагають налаштувань, і будь-який збій зони огляду камери (від вітру, вібрації тощо) або перестановки великих об'єктів на місцевості тягнуть за собою збій у функціонуванні;
- гнучка відеоаналітика (відеосемантика), яка не має жорстких параметрів і точної формалізації. Функціональність відеосемантики набагато ширша, ніж реакція на корисну мету. Головне завдання відеосемантики – розмежування подій. Саме вона дає можливість скорочувати величезні обсяги інформації, виділяючи корисні дані;
- прогностична або предикативна аналітика (Predictive analytics) – це безліч методів статистики, аналізу даних і теорії, які використовуються фахівцями для аналізу поточних та історичних даних чи подій для прогнозу даних та подій у майбутньому [2]. Основою технології предикативної відеоаналітики є прогнозування розвитку ситуації і відстеження ймовірності виникнення тієї чи іншої події. Предикативна відеоаналітика найбільш затребувана для забезпечення безпеки об'єктів, що характеризуються масовим скупченням людей [3, с. 9-13].

Повертаючись до практики застосування відеоаналітики, доцільно зауважити, що у 2016 році у місті Маріуполі вперше запрацювала система Єдиного аналітичного сервісного центру, концепція якого покликана була створити умови, за яких мешканці міст та області відчуватимуть себе в безпеці завдяки поєднанню комплексного та стратегічного підходів, світовим технологічним досягненням. Діяльність цього центру базується на роботі інтелектуальних відеокамер та акумуляції усіх дзвінків до єдиного колл-центру. Це дозволяє забезпечити цілодобовий контроль за станом правопорядку на території визначеної області, своєчасно виявляти та фіксувати правопорушення,

забезпечити використання сучасних технологій для управління безпекою міста. Результатом запуску цього проекту стало поєднання безпеки та комфорту, створення умов для соціальної захищеності громадян за допомогою розвиненої інфраструктури та інноваційних технологій відповідно до стандартів майбутнього [4]. Слід також додати, що наразі аналогічний центр працює і в інших регіонах України, у тому числі й у Дніпрі.

Свою діяльність у напрямку використання засобів відеофіксації поліцейські здійснюють на підставі діючих нормативно-правових та відомчих документів, зокрема затверджених Головою Національної поліції України Князєвим Методичних рекомендацій щодо впровадження системи видеоспостереження та відеоаналітики (від 01.03.2019), а також наказу від 12.02.2019 № 141 «Про організацію використання систем відеоспостереження органами (підрозділами) поліції» .

Важливим аспектом є установлення порядку та розподілу функцій і обов'язків за напрямками діяльності підрозділів.

На виконання наказу НПУ № 141 були призначені відповідальні особи із числа працівників УОАЗОР, УПД, УІАП, УПП, які здійснюють невідкладний аналіз відеоінформації із систем відеоспостереження, з метою підвищення ефективності оперативного реагування та розкриття злочинів по «гарячих слідах».

Забезпечення організації та ефективного опрацювання відеоматеріалів з архівів систем відеоспостереження покладено на підрозділи карного розшуку, слідства та кримінального аналізу.

Використання можливостей систем відеоспостереження під час забезпечення публічної безпеки і порядку на підрозділи превентивної діяльності та патрульної поліції.

Наповнення каталогу камер відеоспостереження, у тому числі даними про камери, які не входять до муніципальних та власних систем відеоспостереження, але можуть фіксувати інформацію, що сприятиме належній реалізації завдань поліції – на підрозділи превентивної діяльності та карного розшуку.

Технічне супроводження, а також надання інформації із систем відеоспостерження за письмовими запитами зацікавленим підрозділам поліції – на підрозділи УЗТ, УІАП.

Таким чином, ефективне використання систем відеоспостереження може бути стримуючим фактором для багатьох незаконних дій. А застосування ефективних алгоритмів відеоаналітики дозволить оперативно приймати рішення залежно від обставин. Це у значній мірі допоможе виконувати свої функції підрозділам карного розшуку, досудового розслідування, кримінального аналізу, превентивної діяльності та іншим службам Національної поліції України.

---

1. Фірман В. М., Шишко В. В., Шишко В. Й. IP-системи у відео технологіях безпеки. Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання : збірник наукових статей за матеріалами доповідей Міжнародної науково-практичної конференції 22 грудня 2017 року. Львів: ЛьвДУВС, 2018. С. 387-394
2. Торстен Анштедт. Видеоаналитика: Мифы и реальность. Security Focus, 2012. 176 с.
3. Лопатін С. І. Перспективні напрями розвитку систем відеоаналітики. Сучасна спеціальна техніка. 2016. № 4. С. 9-14.
4. Працівники ХНУВС ознайомилися з роботою Єдиного аналітичного сервісного центру та мобільного додатку «Поліція 102». URL: http://univd.edu.ua/uk/news/4390.
5. Наказ Національної поліції № 141 «Про організацію використання систем відеоспостереження органами (підрозділами) поліції» від 12.02.2019 року.

Окремі проблеми у забезпеченні технічного захисту інформації у корпоративних мережах

Сеник Володимир Васильович

завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Корпоративна мережа – це мережа, головне завдання якої, полягає у підтримці роботи конкретної установи чи організації, що володіє даною мережею. Корпоративна мережа об'єднує підрозділи установи чи організації, і навіть ті, які є географічно віддаленими, та створює єдиний простір для швидкого обміну даними та безпечної спільної роботи співробітників з корпоративними ресурсами. Головний принцип корпоративної мережі базується на використанні каналів глобальної мережі, яка забезпечує зв'язок між територіально віддаленими підрозділами компанії без необхідності побудови окремої фізичної мережі [1].

З даного визначення бачимо, що для таких мереж, як правило, характерним є визначена територіальна належність; гетерогенність (різноманітна комп'ютерна техніка, комунікаційне обладнання та програмне забезпечення), а також підключення та використання глобальних мереж, які підключаються різноманітними видами телекомунікаційних каналів та обладнання.

У зв'язку із сказаним, забезпечення захисту інформаційних ресурсів у такій системі має ряд проблем. Насамперед, це пов'язано з тим, що забезпечення необхідного рівня захисту інформаційних ресурсів від несанкціонованого доступу для різних користувачів (підрозділів) та окремих інформаційних підсистем можуть різнитися. Окрім цього, наявність засобів захисту з великою вірогідністю може мати вплив на продуктивність інформаційно-телекомунікаційної системи та зручність її використання. Така ситуація спонукає враховувати ці особливості під час формування вимог до захисту інформації у таких мережах. Тому для корпоративної мережі під час побудови

системи захисту інформації слід дати відповіді на наступні питання:

1. Яким чином сформувати вимоги до побудови комплексної системи захисту?

2. Який порядок виконання робіт?

3. Як обрати найоптимальніший підхід до проектування та введення у дію комплексної системи захисту інформації?

4. Як визначити порядок проведення оцінки системи захисту у такій складній за структурою системі?

Враховуючи те, що система захисту є невід'ємною складовою інформаційної системи, а її основні механізми лише логічно відокремленою структурою, можна зробити висновок, що архітектура системи захисту має повністю відповідати архітектурі та принципам побудови інформаційної системи.

Оскільки корпоративна мережа сама по собі є системою гетерогенною, то й система захисту може бути неоднорідною, тобто з наявністю різних об'єктів захисту і, відповідно, різними вимогами до захисту інформації у кожній складовій інформаційної системи. Останнє випливає з того, що у кожній складовій інформаційної системи можуть бути наявні критичні інформаційні ресурси, програмно-апаратні засоби, особливості технології оброблення даних, моделі загроз і, відповідно різні політики безпеки [2].

Таким чином, політика безпеки у корпоративній мережі є сумою політик безпеки окремих її складових, що взаємодіють за єдиними принципами і правилами. Тобто, захист інформації у такій інформаційній системі має розглядатися як деякий складний об'єкт, який побудовано за модульним принципом. Кожен окремий модуль є повноцінною системою захисту інформації певної складової корпоративної інформаційної системи. У зв'язку з цим, такий модуль може окремо проектуватися, розроблятися, оцінюватися та експлуатуватися. Таким чином, під системою захисту інформації у корпоративній мережі слід

розуміти суму окремих модулів комплексної системи захисту інформації.

Особливо важливим під час побудови такої системи захисту і такої архітектури є взаємодія та обмін інформацією між окремими модулями та керування системою захисту в цілому. Найпростішим шляхом вирішення даної проблеми є створення у рамках системи захисту окремої підсистеми.

Для побудови такої підсистеми можна вибрати один із варіантів: централізоване адміністрування з однієї точки (при цьому у кожному з модулів має функціонувати агент підсистеми взаємодії і обміну інформацією) або взаємодія рівноправних модулів.

Обидва варіанти відповідають вимогам з огляду забезпечення захисту інформації. Різними лише є процедури проектування та оцінювання. У першому випадку підсистема взаємодії та обміну інформацією розглядається як самостійна система, у другому – проектування та оцінювання проводиться в окремих рамках для кожного модуля, що є складнішим з огляду формування вимог у всіх модулях і оцінки їх реалізації у системі.

При цьому, для забезпечення коректної взаємодії між модулями, слід прагнути до того, щоб архітектура та принципи побудови кожного окремого модуля системи захисту (по можливості) мали однакові протоколи передавання даних, сумісне програмне забезпечення, механізми захисту тощо. Така побудова надає ряд переваг. Серед них: дотримується реалізація відкритої архітектури безпеки; забезпечується можливість розроблення, впровадження, оцінювання та експлуатації кожної складової системи захисту; забезпечується можливість поступового введення окремих модулів без утворення будь-яких перепон для роботоздатності інформаційної системи; спрощується і, відповідно, здешевлюється проектування та розроблення системи захисту; створюються умови для окремої оцінки кожного модуля захисту інформації тощо.

Викладені вище принципи побудови системи захисту можна застосовувати як до корпоративної мережі загалом, так і до окремих її складових елементів. Залишається лише питання

отримання атестату відповідності, який, до речі, може бути як на всю систему захисту, так і на кожний окремий модуль.

Нині діючими нормативними документами вибір будь-якого з підходів до побудови системи захисту не регламентується. Вибір у такому випадку залишається лише за розпорядником інформаційно-телекомунікаційної системи.

---

1. Корпоративна мережа: [Електронний ресурс]: URL: http://xn--r1a3b.xn--b1amgblet.xn--j1amh/index.php/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
2. Сеник В. В., Рудий Т. В., Сеник С. В., Магеровська Т. В. Основи технологій захисту інформації в комп'ютерних системах : навчально-методичний посібник. Львів : ЛьвДУВС, 2019. 192 с.

Аналіз стану розвитку систем відеонагляду в діяльності Національної поліції України

Сидор Віктор Володимирович

здобувач вищої освіти
Львівського державного університету внутрішніх справ

Сеник Володимир Васильович

завідувач кафедри інформаційного та аналітичного
забезпечення діяльності правоохоронних органів
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Забезпечення публічної безпеки та порядку, охорона прав і свобод особистості, а також інтересів суспільства та держави, протидія злочинності, допомога особам, які з різноманітних особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій її потребують віднесено законодавцем до основних завдань органів і підрозділів Національної поліції України [1, 2]. Їх безумовна реалізація є основою діяльності кожного поліцейського.

Водночас у сучасних умовах, що склалися у нашій державі, слід враховувати наявність ряду негативних чинників економічного, соціального, політичного, ідеологічного характеру, які негативно впливають на формування криміногенної обстановки в Україні. Крім цього, постійне технічне удосконалення злочинного середовища, розроблення та використання нових форм і методів протиправної діяльності створюють додатковий тиск як на суспільство загалом, так і на правозахисну систему зокрема.

Такі передумови значно послаблюють здатність поліцейським якісно та ефективно виконувати завдання, визначені Законом України «Про Національну поліцію» [1], та створює поштовх до пошуку, створення і впровадження у діяльність різноманітних підрозділів Національної поліції України нових можливостей у забезпеченні безпеки громадян, публічного порядку, а також їх захисту від протиправних посягань.

Як показує практичний досвід ряду Європейських держав (особливо Великобританії), США та Канади, одним із ефективних таких інструментів є розбудова та використання комплексних систем відеоспостереження з потужною аналітичною складовою.

З огляду на вивчений досвід, пропонуємо у його запровадженні шляхом створення системного підходу до побудови єдиної системи відеонагляду та відеоаналітики, що повинно стати одним із пріоритетів подальшого розвитку Національної поліції України.

Законом України про «Національну поліції» передбачено можливість створення нею власних бази даних, необхідних для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчих інформаційно-аналітичних систем, необхідних для виконання покладених на неї повноважень (ст. 25).

Враховуючи надані законодавцем можливості щодо створення та запровадження в діяльність Національної поліції України власних баз даних та інформаційних підсистем з ініціативи територіальних органів поліції спільно з органами влади на місцях нині розпочато активне запровадження систем відеоспостереження в містах та великих селищах. Заходи щодо розвитку відповідних систем відеонагляду знайшли своє відображення у більшості регіональних програмах профілактики злочинності.

Нині поліцією використовується понад 12,5 тис. відеокамер, зображення з яких передаються до обласних ситуаційних центрів. Із зазначеної кількості близько трьох тисяч – це, так звані «розумні камери», які наділені функціональними можливостями розпізнавання номерів транспортних засобів, а також обличчя, тобто здатні проводити аналітику.

При цьому використання аналітичних систем відеоспостереження, безперечно, має позитивний вплив на розкриття та розслідування кримінальних правопорушень, про що відомо з різних джерел засобів масової інформації та окремими документами Національної поліції України.

Наприклад, на Одещині, де у 2018 році розпочала роботу «Інтегрована система відеоспостереження та відеоаналітики», з

використанням її можливостей розкрито декілька резонансних злочинів, у тому числі вбивство місцевої мешканки, поєднане з відчленуванням голови потерпілої, розбійні напади на водія таксі та на помешкання громадянина Індії, а також ряд інших особливо тяжких злочинів.

Показовими є і декілька прикладів розкриття злочинів завдяки системі відеоспостереження в місті Дніпро.

Так, у листопаді 2018 року за допомогою програмного комплексу системи відеоспостереження виявлено автомобіль із викраденим номерним знаком. За оголошеним в ефірі орієнтуванням нарядом Управління патрульної поліції після застосування вогнепальної зброї автомобіль та осіб, які в ньому перебували, затримано (у подальшому затриманих викрито у вчиненні тяжких та особливо тяжких злочинів на території Дніпропетровської та сусідніх областей).

На Чернігівщині з використанням камер відеоспостереження упродовж 2018 року розкрито 30 тяжких та особливо тяжких злочинів, з яких 4 незаконних заволодіння транспортними засобами, 3 розбої, 2 хуліганства з використанням зброї, 14 грабежів.

Наприклад, 20 жовтня 2018 року нарядом поліції охорони за орієнтуванням з камер відеоспостереження по «гарячих слідах» встановлено особу, яка із застосуванням ножа вчинила на вулиці розбійний напад на громадянку.

За аналітичною інформацією з камер відеоспостереження у місті Луцьк встановлено групу осіб, які в листопаді 2018 року скоїли умисне вбивство однієї особи та заподіяли тілесні ушкодження іншій.

Характерні приклади розкриття злочинів є і у Донецькій області, де запроваджено систему інтелектуального відеоспостереження, яка дозволяє за допомогою спеціального програмного забезпечення розпізнавати реєстраційний номер автомототранспортного засобу та перевіряти його на предмет перебування у розшуку, розпізнавати тип, модель та колір автомобіля, розпізнавати біометричні дані водія (обличчя) та перевіряти їх у відповідних розшукових базах даних, виявляти скупчення людей. Дана система інтелектуального відеоспостереження також має детектор залишених предметів та їх власників.

На перший погляд здається, що такий стан речей є задовільним і лише потребує подальшого розвитку шляхом охоплення територій засобами відеоспостереження. Однак, це не зовсім так. Нині вкрай гостро виникає проблема відсутності єдиного підходу до розбудови та використання систем відеоспостереження органами та підрозділами Національної поліції України. Це зумовлюється тим, що в областях запроваджуються різноманітні технічні та технологічні рішення щодо отримання, передавання, оброблення та зберігання відеопотоків даних з використанням обладнання (відеокамери, відеореєстратори) різних виробників, які у свою чергу мають своє унікальне програмне забезпечення.

Дана ситуація призводить фактично до унеможливлення проведення централізованого аналізу відеоінформації, а значить і її подальшого використання працівниками територіальних органів поліції (ситуаційного центру, чергової служби, оперативних підрозділів, слідчо-оперативних груп тощо) та центрального органу управління поліції.

Тому запровадження єдиних підходів, стандартів під час створення, розбудови, впровадження та використання єдиної комплексної системи відеоспостереження та відеоаналітики, встановлення типових вимог для технічних та технологічних рішень стосовно отримання, оброблення, обміну та зберігання потоків відеоданих, встановлення тісної взаємодії територіальних органів (підрозділів) Національної поліції з місцевими органами державної влади та органами місцевого самоврядування у питанні створення та розбудови систем відеонагляду є одним з першочергових завдань діяльності Національної поліції.

---

1. Про Національну поліцію : Закон України від 2 липня 2015 р. № 580-VIII. База даних «Законодавство України» / ВР України. URL : http://zakon3.rada.gov.ua/laws/show/580-19/.
2. Положення про Національну поліцію : постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877. URL : http://www.kmu.gov.ua/control/uk/cardnpd?docid=248607704

Використання інвазивних та неінвазивних засобів ідентифікації осіб з формами деменції в пошуковій роботі Національної поліції

Рижкова Світлана Анатоліївна

інспектор сектору превенції Шевченківського ВП Дніпровського ВП ГУНП в Дніпропетровській області

Відповідно до ст.23 закону України про «Національну поліцію» серед основних повноважень поліції є: розшук осіб, які пропали безвісти, та інших осіб у випадках, визначених законом; вжиття заходів для надання невідкладної, зокрема домедичної і медичної допомоги особам, які постраждали, в тому числі внаслідок нещасних випадків, а також особам, які опинилися в ситуації, небезпечній для їхнього життя чи здоров'я; вжиття заходів для визначення осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством [1].

Задля більш оперативного пошуку, створюються бази даних, волонтерські центри, використовуються соціальні мережі та інш. Окрім закритих інформаційних баз на сайті Міністерства внутрішніх справ України є база даних – «Розшуку осіб», де серед інших рубрик є окрема категорія пошуку: «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку«[2].

Паралельно до централізованих створюються регіональні масиви інформації. Так, патрульні Львова створили електрону базу, тих осіб, які часто губляться. Вона сформована з понад 300 осіб, яки були відшукані чи повернуті додому. З метою запобігання фактів зникнення літніх осіб з втратою пам'яті, які можуть заблукати або ж взагалі забути де живуть патрульні поліцейські пропонують родичам такі прості поради: покласти записку з адресою і номером контактної особи в кишені, нашити дані на

підкладку верхнього одягу, або зробити інформаційний браслет на руку [3].

Втрата пам'яті серед людей похилого віку може представляти загрозу її життю та здоров'ю, адже особа, яка загубилась, в такому стані дезорієнтована у просторі та самостійно не може надати собі пораду. Такий стан, має медичній термін «деменція». Деменція – синдром, що характеризується набуттям, чисто прогресуючим зниженням інтелекту, що виникає в результаті органічних ушкоджень головного мозку і приводить до порушення соціальної адаптації пацієнта, тобто робить його нездатним продовжувати професійну діяльність, обмежує можливості самообслуговання, порушує його побутову незалежність Це синдром, при якому виникає деградація пам'яті, мислення [4, с.5].

Особа, яка має діагноз поставлений психіатром як деменція, автоматично потрапляє у групу ризику осіб, які потенційно можуть зникнути безвісти внаслідок втрати пам'яті та наражатися на небезпеку у невпізнаному для неї середовищі, яке може привести до травмування, каліцтва або навіть смерті.

Маємо світовий досвід законодавчого вирішення цієї проблеми. Так, наприклад, у США діє Закон HR4919 («The Violence Crime Control and Law Enforcement Act of 1994») [5]. Метою закону є пошук зниклих безвісті осіб з різними формами деменції (в тому числі хворобою Альцгеймера), а також іншими порушеннями розвитку задля зниження ризику травмування, каліцтва або смерті, що у свою чергу пов'язано із зникненням таких осіб. Зазначений закон надає можливість на основі медичних висновків запроваджувати за згоди батьків або опікунів на добровільній основі використання неінвазивних і непостійних засобів відстеження (браслет, брелок або прикріплюється до одягу модуль).

Слід зазначити, що Законом гарантується конфіденційність даних використання пристрою відстеження. Доступ до персональних даних мають тільки правоохоронні органи та органи охорони здоров'я. Збір, використання та збереження даних призначено виключно для запобігання травмування або загибелі пацієнта, якому призначений пристрій стеження.

Окрім цього, закон гарантує здійснення кваліфікованої підготовки працівників правоохоронних органів щодо розпізнавання ознак зловживань під час взаємодії з заявниками на пристрій стеження; захищати громадянські права та свободи осіб, які використовують пристрої стеження.

Однак фахівці наполягають на необхідності вдосконалення механізмів пошукової роботи. Окрім інформаційно-комунікаційної складової, яка реалізуються через бази даних, месенджери, ЗМІ щодо розшуку зниклих осіб з формами деменції, на допомогу в цьому приходять новітні технології.

Так на часі є розробка чипу з GPS та звуковою активацією, який працює від тепла людського тіла. Головне призначення чипу полягає в GPS-слідкуванні за пацієнтами з формами деменції. Вбудований в руку чип зможе зберігати всі медичну історію свого носія, якщо пацієнт знепритомніє або втратить пам'ять, збережені дані зможуть стати незамінними для лікарів швидкої допомоги. Завдяки збереженим даним пацієнта, можна встановити особу, адресу проживання, з'ясувати чи не має у пацієнта алергії на деякі препарати, ліки які вживає пацієнт та історію хвороби. Зазначена технологія планується впроваджуватись виключно на добровільній основі, як інвазивні засоби ідентифікування осіб з формами денменції.

Серед аргументів, які надані організацією Applied Digital Solutions (A.D.S.), розроблення та впровадження чипів-імплантів допоможе в оперативному пошуку людей, можливості здійснення медичного моніторингу за пацієнтами, в тому числі осіб з формами деменції[6].

Інвазивна процедура (від латинської invasivus; от invado) – медична процедура, пов'язана з проникненням через природні зовнішні бар'єри організму (шкіра, слизові оболонки)[7] .

Так, наприклад, у Швеції більше 3,5 тисяч людей добровільно пройшли процедуру імплантації чіпа, який за допомогою спеціального пістолета вживлюється під шкіру між великим і вказівним пальцем. Практика вживлення чіпів під шкіру в Швеції стартувала в 2015 році і кількість таких осіб з часом зростає. Чіп,

що використовує технологію NFC («комунікація ближнього поля»), записує унікальний номер особи, можливості безконтактного RFID-чіпу є досить багатофункціональним, після чіпування, долоню можна використовувати як безконтактну картку для платежів, посвідчення особи, пропуску або ключів, тощо[8].

До речі, німецький професор Патрік Крамер, засновник компанії Digiwell під час конференції Black Sea Summit, яка проходила в Одесі, імплантував в руку киянина комп'ютерний чіп. Слід зазначити, що це перший випадок проведення подібної процедури в Україні. Як зазначає Патрік Крамер, при вживленні чіпу під шкіру, «пристрій» не місить в собі ніякої інформації, тільки після імплантації, застосовується спеціальний додаток, який кодує інформацію, яку обирає власник – носій чипу. Власник чіпа (використовується технологія NFC (NTAG216) для передачі даних, ємність сховища становить 880 байт), може завантажити інформацію ключа від «розумного» будинку, сейфу, кредитної картки, розплачуватися електронною валютою Bitcoin, тощо [9].

З огляду на зазначене, стає очевидним, що розвиток інформаційних технологій та застосування різних цифрових модифікацій розвивається досить інтенсивно, в багатьох випадках випереджає врегулювання таких суспільних відносин у правовому полі. Але слід наголосити на тому, якщо застосування таких технологій має на меті збереження життя і здоров'я людини, за такими новаціями-майбутнє.

Таким чином, поєднання інвазивних (процедура імплантації чіпу) та неінвазивних (браслет, брелок, модуль, який прикріплюється до одягу) засобів ідентифікації осіб з формами деменції за умов її належної правової регламентації підвищить ефективність в пошуковій роботі Національної поліції.

---

1. Про Національну поліцію: Закон України від від 02.07.2015 № 580-VIII. Відомості Верховної Ради. 2015 № 40-41. Ст.379. URL: https://zakon.rada.gov.ua/laws/show/580-19.

2. Розшукові обліки МВС. URL: https://wanted.mvs.gov.ua.
3. Львівські патрульні через соцмережі знайшли домівку заблукалої бабусі URL:https://portal.lviv.ua/news/2019/10/28/lvivski-p
4. Деменція : навчально-методичний посібник / О. А. Козьолкін, М. В. Сікорська, І. В. Візір, Ю. М. Нерянова. – Запоріжжя : [ЗДМУ], 2015. – 90 с.
5. H.R.4919 – Kevin and Avonte's Law of 2016. URL://www.congress.gov/bill/114th-congress/house-bill/4919/tex
6. Американская компания уже год чипирует своих сотрудников. Почему за этим может быть будущее. URL:https://habr.com/ru/company/pochtoy/blog/421737/
7. Термінологія законодавства: «Інвазивна процедура».URL: https://zakon.rada.gov.ua/laws/term/i/page2/name
8. Навіщо шведи масово і добровільно імплантують собі під шкіру мікрочіпи. URL: https://ukr.media/world/364518/Навіщо%20шведи%20масово%20і%20добровільно%20імплантують%20собі%20під%20шкіру%20мікрочіпи//ukr.media/world/364518/
9. Українець матиме у руці вживлений комп'ютерний чіп. URL: https://khm.depo.ua/ukr/khm/ukrayinets-matime-u-rutsi-vzhivleniy-komp-yuterniy-chip-10092016160700

Організаційно-правові аспекти захисту інформації у спеціалізованих інформаційних системах Національної поліції: стан і перспективи

Рудий Тарас Володимирович

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

Сидорук Ігор Ігорович

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

Виходячи із сучасних викликів та загроз з метою забезпечення контролю за національним сегментом інформаційного і кіберпростору політикум будь-якої держави постійно вдосконалює організаційно-правові та техніко-економічні механізми забезпечення безпеки кіберпростору та інформаційно-телекомунікаційних мереж [1].

Безпека інформаційного і кіберпростору, запровадження цифровізації процесів управління, гарантування безпеки й сталого функціонування національної критичної інфраструктури, інформаційних систем повинні стати не тільки складовими державної політики у сфері розвитку кіберпростору та становлення інформаційного суспільства в Україні, а також включення цих чинників у сферу політичних пріоритетів держави.

Сучасні загрози обумовлені впливом комплексу політичних, соціально-демографічних, економічних, правових, соціоінженерних, технологічних чинників вимагають системного реагування, адекватної трансформації секторів інформаційної безпеки (ІБ) та кібербезпеки.

Проте, як свідчить аналіз літературних джерел [2, 3, 4, 5] чітких і зрозумілих нормативно-правових документів щодо забезпечення

національної системи кібербезпеки, захисту інформаційного простору держави нема. Відсутні ефективні та дієві заходи запобігання та протидії загрозам, а наявні є несистемними і, як наслідок, марними.

Чинне законодавство України не враховує проблеми особливостей правової регламентації інформаційно-правових заходів захисту інформації (ЗІ) у спеціалізованих інформаційних системах (СІС) Національної поліції України (НПУ), ще до сьогодні відсутнє наукове обґрунтування визначень та формулювань, а подекуди і їх цілковита відсутність. Як не дивно, але повного переліку злочинів, передбачених Кримінальним кодексом України, які слід вважати кіберзлочинами, на сьогодні поки що теж не існує [6].

Аналіз причин незадовільного забезпечення інформаційної та кібербезпеки держави оголює цілу низку системних проблем у галузі нормативно-правової бази, ігнорувати які стає дедалі важче. Законодавча база – важлива складова у забезпеченні ІБ та кібербезпеки, але уже настав час перейти від слів до дій з огляду на те, що основним недоліком чинного законодавства у безпековій сфері є його пасивний характер – декларується лише необхідність забезпечення ІБ, безпеки кіберпростору та протидії кіберзлочинності на рівні доктрин, указів, рішень тощо. Тобто, задається «напрямок», якого необхідно дотримуватися за відсутності фінансового та кадрового забезпечення і без жодної відповідальності посадових осіб [7].

Розглянемо основні проблеми та прогалини у організаційно-правовому забезпеченні захисту інформації у СІС підрозділів НПУ.

Актуальною залишається проблема недосконалості національного законодавства в інформаційній сфері і відсутності єдиної правової бази стосовно забезпечення ІБ у СІС Національної поліції.

На сьогодні першим та єдиним законодавчим актом є Закон України «Про основні засади забезпечення кібербезпеки України» та Указ Президента України №47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Були очікування, що ці документи стануть основою для розроблення у найкоротші терміни ефективної, сучасної нормативно-правової бази, низки нормативно-правових актів, які повинні відігравати ключову роль у забезпеченні інформаційної і кібербезпеки в Україні. Проте, на превеликий жаль, ми залишилися на тому ж місці, нема жодного поступу вперед у цій важливій сфері. Тому, однією з головних проблем залишається неефективна організаційно-правова база та система управління.

На наше переконання, необхідно врахувати ще один вагомий чинник. Важливою особливістю функціонування інформаційного простору держави є його висока динамічність та мінливість загроз ІБ. Це обумовлює неможливість створення ефективного організаційно-правового забезпечення у сфері ЗІ на тривалий період. Тому, щонайменше, кожні два роки чинне законодавство у цій сфері потребуватиме корегування відповідно до нових загроз, а також змін у геополітичному безпековому середовищі [8].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та серія нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі, хоча на законодавчому рівні зобов'язують впроваджувати Комплексну систему захисту інформації (КСЗІ) у системах захисту СІС органів державної влади та правоохоронних структур, яка впродовж багатьох років довела свою неефективність.

Чинною на сьогодні є і норма Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (ст. 7) відповідно до положень якого державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю.

Тобто, під дію цієї норми потрапляють усі системи ЗІ, їх інформаційна інфраструктура, що вимагає дотримуватись вимог старого стандарту КСЗІ НД ТЗІ 2.5-004-99.

Концепція, внутрішня структура і модель впровадження КСЗІ не відповідають сучасним вимогам до забезпечення інформаційної та кібербезпеки і той факт, що ця норма досі не вилучена з

чинного законодавства, піддається гострій критиці [9]. Це відповідає чинному законодавству, але є дуже суперечливим підходом з урахуванням фундаментальних недоліків і застарілістю концептуальної ідеї КСЗІ.

На нашу думку цьому стандарту притаманні такі головні недоліки [8]:

- застаріла концепція системи ІБ (не охоплює управлінський рівень і реагування на інциденти ІБ, спрямована на захист та сертифікацію систем ЗІ в окремих елементах, а не у СІС у цілому);
- не забезпечує достатнього рівня стійкості системи ЗІ до відмов та відновлення після збоїв;
- статичність і обмежені можливості масштабування (реагування на інциденти та загрози ІБ вимагає динамічно змінювати архітектуру системи ЗІ в режимі реального часу, що суперечить парадигмі КСЗІ);
- громіздкість (значна кількість документації, підтверджень та погоджень).

Найнагальнішим кроком є заміна НД ТЗІ більш ефективним та сучасним базовим стандартом і запровадити галузеві стандарти систем ЗІ. Ця пропозиція не є новою і креативною. Існує ціла низка міжнародних стандартів, які зарекомендували себе в розвинених країнах світу та пройшли перевірку часом.

Для цього необхідно або адаптувати сучасні міжнародні стандарти систем ЗІ, або – розробляти та впроваджувати власні, якісно нові стандарти безпеки для державних органів та силових структур, що є неприйнятним з огляду на часові обмеження і матеріальні витрати [10].

На відміну від найпоширенішої у світі серії стандартів ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5-004-99 є відповідність архітектури та параметрів програмно-апаратних засобів СІС регламенту – КСЗІ.

Окрема проблемна ділянка – аудити систем ЗІ. В системі координат НД ТЗІ дозвіл на проведення аудиту мають лише

акредитовані державою організації. Міжнародні сертифікати з ІБ та ІТ-аудиту наразі не визнаються, що негативно впливає на якість аудиту [11].

На противагу КСЗІ в організаційно-правову структуру системи ЗІ необхідно гармонізувати та впровадити в дію сучасні міжнародні стандарти, насамперед – серію міжнародних стандартів ISO/IEC 27000, розроблених технічним комітетом ISO/IEC JTC 1 підкомітетом SC 27 Міжнародної організації з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими документами. Отже, сучасне організаційно-правове забезпечення систем ЗІ в СІС підрозділів НПУ повинно формуватися відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України.

В Україні одночасно існують дві парадигми систем ЗІ: КСЗІ і СМІБ. Зміна нормативно-правової бази в сфері ЗІ – це виклик часу і тільки якнайскоріша модернізація організаційно-правового забезпечення ЗІ у СІС дасть можливість забезпечити виконання поставленої задачі – сталого функціонування СІС. Всупереч поширеній думці, безпека – це не стан, а процес.

Наступною проблемою є фаховий рівень підготовки посадових осіб. Ця проблема сягає своїм корінням до початкового етапу професійної підготовки. Фахівці можуть розробити та запровадити ідеальний варіант системи ЗІ, відповідні служби та експерти виконають усі необхідні експертизи та заходи з атестування, а відсутність кваліфікованих фахівців з експлуатування СІС зведе нанівець усі попередні зусилля.

Спрощувати закони, а не ускладнювати їх, звільняти, або переводити до інших підрозділів некваліфікованих осіб, які імітують бурхливу діяльність. Тим, хто залишиться – підняти зарплати. Але ні зарплати, ні закони, ні доктрини, ні покарання й ускладнені до божевілля правила самі собою не працюють. Все починається з технічного фахівця, який повинен розуміти, що інформація, яку йому довірили, має цінність, що вона підлягає захисту, що від її збереження залежить не тільки його особиста безпека та добробут, а і безпека держави [12].

Такий стан справ повинен зумовити глибинні зміни у ставленні нашої держави до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого ЗІ, засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу, тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки [7].

Висновки.

1. На підставі проведеного аналізу вважаємо, що на організаційно-правовому рівні необхідно чітко ідентифікувати проблему безпечного функціонування СІС, визначити основні загрози в сфері ЗІ та своєчасно надавати нові, сучасні правові інструменти для протидії цим загрозам.
2. Розроблення і запровадження сучасного організаційно-правового забезпечення ЗІ у СІС повинно базуватися на використанні міжнародних стандартів. Для цього необхідно або адаптувати стандарти ISO/IEC серії 27000, або – розробити власні, якісно нові стандарти безпеки для державних силових структур, що є неприйнятним у кореляції з часовими та матеріальними витратами.
3. Державну акредитацію аудиторів з систем ЗІ та кібербезпеки потрібно замінити акредитацією на основі міжнародних сертифікацій.

---

1. Гребенюк М. В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду / Підприємництво, господарство і право. – Київ: №2/2019. – С. 203-207.
2. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності / «Інформація і право», № 1(24)/2018. Електронний ресурс. Шлях доступу: http://ippi.org.ua/sites /default/files/15_4.pdf.
3. 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/.

4. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: https://www.cyberpolice.gov.ua/strategy-2020/.
5. Рудий Т. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні / Т.В. Рудий, В. В. Сеник, А. Т. Рудий, С. В. Сеник / Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2018. – Вип. 1. – С. 283-301.
6. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності / Інформація і право. – К.: Науково-дослідний інститут інформатики і права Національної академії правових наук України, №1(28)/2019. – С. 118-128.
7. 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. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
8. Рудий Т. В. Живко З. Б. Сеник В. В. Технології кримінального аналізу у практиці протидії кіберзлочинності / Т. В. Рудий, З. Б. Живко, В. В Сеник // Соціально-правові студії: науково-аналітичний журнал / гол. ред. О. Балинська. Львів: ЛьвДУВС, 2018. Вип. 2. – С.40-48.
9. Янковський. О. Що не так із законопроектом про кібербезпеку та як його вдосконалити / Електронний ресурс. Шлях доступу: ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci
10. Середа В. В. Нормативно-правові аспекти застосування міжнародних стандартів в системі управління безпекою підприємств / В. В. Середа, 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.

11. Sereda, V., Zhyvko, Z., Balynska, O., Rudyi, T. (2019, July 15). The Organizational Principles of Information Protection Management System Realization. (Z. Cekerevac, Ed.) MEST Journal, 7(2), 73-78. doi:10.12709/mest.07.07.02.09.
12. Янковський О. Україні потрібна нова кіберстратегія / Електронний ресурс. Шлях доступу: https://www.pravda.com.ua /columns/2019/09/14/7226291/ .

Захист інформації в комп'ютерних мережах

Фірман Володимир Михайлович

доцент кафедри безпеки життєдіяльності
Львівського Національного університету імені Івана Франка,
кандидат технічних наук, доцент

Худик Остап Андрійович

здобувач вищої освіти
Львівського Національного університету імені Івана Франка

Хміль Марта Михайлівна

здобувач вищої освіти
Львівського Національного університету імені Івана Франка

Метою охорони праці є науковий аналіз умов праці, технологічних процесів, апаратури та обладнання з точки зору можливості виникнення появи небезпечних факторів, виділення шкідливих виробничих речовин.[6]

На основі такого аналізу визначаються небезпечні ділянки виробництва, можливі аварійні ситуації та розробляються заходи щодо їх усунення або обмеження наслідків. На всіх підприємствах мають бути створені здорові і безпечні умови праці, встановлені правові засади регулювання відносин у галузі охорони праці між роботодавцями і працівниками, а також створені умови праці, що відповідають вимогам збереження життя і здоров'я працівників у процесі трудової діяльності (згідно закону України «Про охорону праці»).[4]

Безпе́ка мере́жі (*Network security*) – заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів.[3]

Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ,

неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень.[3]

Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів.[5]

Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.[5]

Способи несанкціонованого доступу

Несанкціонований доступ до інформації, що знаходиться в локальних мережах буває:

- непрямим – без фізичного доступу до елементів локальних мереж;
- прямим – з фізичним доступом до елементів локальних мереж.

В даний час існують наступні шляхи несанкціонованого отримання інформації (канали витоку інформації):

- застосування підслуховуючих пристроїв;
- дистанційне фотографування;
- перехоплення електромагнітних випромінювань;
- розкрадання носіїв інформації і виробничих відходів;
- зчитування даних у масивах інших користувачів;
- копіювання носіїв інформації;
- несанкціоноване використання терміналів;

- маскування під зареєстрованого користувача за допомогою розкрадання паролів та інших реквізитів розмежування доступу;
- використання програмних пасток;
- отримання даних, що захищаються за допомогою серії дозволених запитів;
- використання недоліків мов програмування і операційних систем;
- умисне включення в бібліотеки програм спеціальних блоків типу «троянських коней»;
- незаконне підключення до апаратури або ліній зв'язку обчислювальної системи;
- зловмисним виведення з ладу механізмів захисту.[5]

Засоби захисту інформації

Для вирішення проблеми захисту інформації, основними засобами, використовуваними для створення механізмів захисту, прийнято вважати:

Технічні засоби – електричні, електромеханічні, електронні і ін. типу пристрою. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість. Технічні засоби поділяються на:

- апаратні пристрої, що вбудовуються безпосередньо в апаратуру, або пристрої, що сполучаються з апаратурою локальних мереж по стандартному інтерфейсу (схеми контролю інформації з парності, схеми захисту полів пам'яті по ключу, спеціальні регістри);
- фізичні – реалізуються у вигляді автономних пристроїв та систем (електронно-механічне обладнання охоронної сигналізації та спостереження. Замки на дверях, грати на вікнах).[5]

Концепція мережевої безпеки :

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або «ключ», кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.[3]

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).[3]

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.[3]

Останнім часом все більш актуальною стає проблема захисту інформації. Чим більше комп'ютеризуються різні сфери нашого життя, тим більше стає областей можливого проникнення зловмисників, конкурентів і просто комп'ютерних хуліганів. Для протидії зовнішнім атакам необхідно не тільки мати засоби захисту інформації, а й розуміти принципи їх функціонування, вміти правильно їх налаштувати, розуміти слабкі місця операційних систем.[2]

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з таких проблем – забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою комп'ютеризацією всіх видів діяльності людини, при об'днанні ЕОМ у комп'ютерні мережі та підключення до інтернету. Тому для спеціалістів різного профілю актуальною є підготовка в галузі захисту інформації. [1]

Проблема захисту інформації не є новою. Вона з'явилась ще задовго до появи комп'ютерів. Стрімке вдосконалення комп'ютерних технологій позначилося й на принципах побудови захисту інформації. З самого початку свого розвитку системи

інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних жертв, у тому числі й людських. Тому конфіденційності в перших системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення і комп'ютерні бази даних від розголошення і перехоплення може тільки повне їх шифрування. Принципова особливість сучасної ситуації полягає в тому, що найважливішим завдання сьогодні стає захист інформації в комп'ютерних мережах.[1]

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їх обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої дільності.[1]

---

1. http://www.nbuv.gov.ua/node/300
2. http://www.zntu.edu.ua/programa-kursu-zahist-informaciyi-v-kompyuternih-merezhah
3. https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96
4. http://cad.kpi.ua/attachments/093_2015_%D0%9A%D1%83%D0%BB%D1%96%D1%88.pdf
5. Курсова робота студентки ПМа-42 Хміль Марти Михайлівної
6. ЗаконУкраїни про Охорону Праці

Роль та значення інформаційних технологій у практичній діяльності органів досудового розслідування

Цебинога Вікторія Юріївна

слідчий відділу слідчого управління Головного управління Національної поліції в Харківській області

Чумак Володимир Валентинович

т.в.о. начальника відділу організації наукової роботи Харківського національного університету внутрішніх справ, кандидат юридичних наук

Розвиток України як демократичної, правової та соціально орієнтованої держави обумовлений рядом факторів, серед яких чільне місце посідають питання протидії злочинності та забезпечення законності та правопорядку в державі. Злочинність сьогодні стрімко зростає, удосконалюються форми та методи злочинної діяльності, і нажаль, практична діяльність суб'єктів протидії злочинності в цьому питанні відстає, законодавство не встигає адаптуватися під сучасні виклики злочинної діяльності.

Важливим засобом у процесі протидії злочинності виступають інформаційні технології. Так, Г. В. Форос зазначає, що в правоохоронних органах накопичений чималий досвід застосування сучасних інформаційних технологій при розкритті та розслідуванні злочинів, виконанні інших завдань боротьби зі злочинністю. Важливим напрямом діяльності правоохоронних органів в сучасних умовах є запобігання злочинності, в структурі і характері якої останнім часом відбулися зміни. Зросла професійність та жорстокість злочинців, посилюється корумпованість у суспільстві. Усе це відбувається на тлі соціально-економічних негараздів, падіння обсягів промислового виробництва, зростання боргів у заробітній платі і потребує удосконалення законодавства і практики правоохоронних органів з розкриття, розслідування і профілактики злочинів з метою забезпечення прав та законних інтересів громадян, в першу чергу тих, які постраждали від них [1, с. 60].

Відтак, актуальності набирають питання використання інформаційних технологій у практичній діяльності органів досудового розслідування як одного із суб'єктів протидії злочинності та забезпечення правопорядку в державі.

Зазначимо, що 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 [2]. У свою чергу Г. М. Шорохова зазначає, що сучасні інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів [3, с. 275].

Дослідник В. М. Варенко до числа сучасних інформаційних технологій відносить:

- інформаційні технології опрацювання даних;
- інформаційні технології керування;
- інформаційні технології підтримки прийняття рішень;
- інформаційні технології експертних систем [4, 396-397].

У практичній діяльності органів досудового розслідування важливе значення має застосування інформаційних технології опрацювання даних. До числа таких інформаційних технологій віднесені обліки інформаційної підсистеми «Єдиний облік», оперативно-довідкові обліки, дактилоскопічні обліки, криміногічні та криміналістичні обліки.

Слід наголосити, що застосування інформаційних технологій в практичній діяльності органів досудового розслідування Національної поліції України дозволяє удосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а головне – дозволяє швидко розкривати злочини, 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 органів досудового розслідування.

Підсумовуючи вищесказане, зазначимо, що впровадження та використання нових інформаційно-комунікаційних технологій є головною умовою покращення роботи щодо встановлення підозрюваного або його розшуку, а також діяльності органів досудового розслідування Національної поліції 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 Національної поліції України повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Крім того, слідчим необхідно проходити курси підвищення кваліфікації з метою отримання нових знань, умінь і навичок під час застосування в повсякденній роботи інформаційних технологій.

1. Форос Г. В. Інформаційні технології у правоохоронній діяльності // Актуальні питання протидії правопорушенням у сфері використання інформаційно-телекомунікаційних систем (Одеса, 28 жовт. 2016 р.) / МВС України, Одеський держ. ун-т внутр. справ. Одеса, 2016. С. 60-62.
2. Інформаційні технології // Вікіпедія : віл. енцикл. URL : https://uk.wikipedia.org/wiki (дата звернення: 02.12.2019).
3. Шорохова Г. М. Використання інформаційних технологій в діяльності Національної поліції України // VIII Міжнародна науково-практична конференція НАНР Економіко-правові виклики 2017 року (Львів, 14 січ. 2017 р.) / Львів: НАНР-Національна академія наукового розвитку, 2017. Том 2 296с. С.274-278.
4. Варенко В. М. Інформаційно-аналітична діяльність: Навч. посіб. Київ : Університет «Україна», 2014. 417 с.

Трансформації у розумінні інформації як безпекоформуючого чинника інформаційної безпеки України

Чистоклетов Леонтій Григорович

професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права, психології та інноваційної освіти Національного університету «Львівська політехніка», доктор юридичних наук, професор

Стародубцева Тетяна Леонтіївна

дільничний офіцер поліції Шавченківського ВП Головного управління Національної поліції у Львівській області, кандидат юридичних наук

Шишко Валерій Валерійович

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

При дослідженні проблем сучасної інформаційної системи, більшість науковців приходять до єдиного знаменника, що не зважаючи на її позитивну спрямованість, яку вона несе на духовний розвиток суспільства на основі забезпечення інтересів особи, у зміцненні демократії та побудові правової держави, залишаються багато чинників, які набагато більшою мірою, аніж це було раніше, злочинним шляхом намагаються вплинути на систему захисту національних інформаційних ресурсів. Отже, поряд з безпекою інформаційних технологій та інформаційних ресурсів не менш важливим, на наш погляд, є гуманітарний вимір інформаційної безпеки, тобто захист від інформації та інформаційна вразливість особистості, суспільства, держави, цивілізації.

Нинішній етап світової історії характеризується переходом людства від індустріальної до інформаційної цивілізації, в основі

розвитку якої покладено знання, засновані на інформації. Водночас суспільство, на думку багатьох дослідників, «з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації» [1, с. 31].

Не зважаючи на інформаційний прогрес сакральний зміст поняття «інформація» не розкрито до цих пір. Загальноприйнята теорія Клода Шенона вирізняється формальним, чи навіть абстрактним трактуванням інформаційних зв'язків. Проте сама цінність інформації для споживача не береться до уваги. Напевне тому сам Клод Шенон свою теорію назвав «математична теорія зв'язку». За Клодом Шеноном повідомлення – певні кодові пересилання передавача, а не сам зміст повідомлення [2, с. 101].

Наразі людство у своєму розвитку перейшло у фазу змістовного аналізу інформації. Це пов'язано, першочергово, із збільшенням обсягів інформації, розвитком ІКТ, інтернету-речей, ІТ-права тощо. Відповідно, особливого значення набуває критичне мислення, критичний аналіз та екологія інформації. У недалекому майбутньому поняттям інформації буде охоплюватися тільки цінна інформація, яка енергетично збагачує та дає можливість реалізувати мету. Все інше буде на кшталт інформаційного шуму та марних (пустих) даних [3, с. 82].

Таким чином, як перший висновок з вище вказаного полягає у необхідності підвищення медіа грамотності та культурного виховання населення. Сьогодні з цього приводу експерти вже давно ведуть жваву дискусію щодо необхідності захисту суспільної моралі, захисту від впливу шкідливої інформації для дітей, студентів, курсантів культурі, а також навчання їх безпечному користуванню сучасними інформаційно-комунікативними технологіями. З цією метою, пропонуємо організувати та провести спільно з Міністерством освіти і науки України міжнародну науково-практичну конференцію на тему «Медіаграмотність молоді» із залученням спеціалістів з кібербезпеки, інформаційного права, штучного інтелекту, представників відповідних відомств правоохоронних структур.

Особливо небезпечним проявом у сфері інформаційної безпеки виступає кібервійна та кіберзлочинність як форми конфлікту, що породжені у XXI столітті. Але разом з тим, нормативно-правові акти, розроблені в попередні століття щодо убезпечення злочинності, за своєю неспроможністю та відірвані від сучасних вимог їм протистояти, вимагають докорінного їх переосмислення, змін та далекоглядного удосконалення.

У своїй книзі «Кібервійна» експерт з безпеки уряду США Річард А. Кларк визначив кібервійну як дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування» [4]. Саме 23 грудня 2015 року в Україні сталась перша у світі підтверджена атака, спрямована на виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго», було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням третьої версії троянської програми BlackEnergy. Згідно з новими подробицями, встановленими після ретельного дослідження хакерської атаки, це були добре підготовлені й обережні стратеги, які ретельно планували напад протягом багатьох місяців. Вони спочатку провели розвідку, вивчили мережу і здобули реквізити доступу операторів, після чого запустили синхронізовану атаку, дії якої були узгоджені, наче рухи в танці [5].

Підтвердженням тому є також події весни 2017 року, коли у Європі руйнівно пройшовся вірус Petya-A, яким 27 червня було вражено і Украну, а саме, комп'ютерні системи «Укренерго», «Київенерго», «Епіцентр», «Київстар», Vodafone, Lifecell, канал ATR, аеропорт «Бориспіль», мережа автозаправочних станцій WOG, «Укргазвидобування» та інших. «Під удар» потрапив навіть сайт Кіберполіції України.

Безперечно, не можна не погодитися і з тим, що початок використання комп'ютерних програм як зброї – найзначніша подія у військовій галузі після розробки ядерної зброї, а швидкий розвиток цього нового методу воєнних дій створив таку сферу

конфліктів, у якій наразі немає загальноприйнятих норм чи правил. Міжнародна практика також стверджує, що деякі країни працюють над пошуком шляху для вироблення правил, яких має дотримуватися світова спільнота, але різні зацікавлені групи у цій сфері мають настільки різні інтереси, що поки не можна сподіватися на досягнення навіть дуже скромних результатів домовленостей.

Як відомо, для створення кіберзброї потрібні лише комп'ютер, з'єднання з інтернетом і хакер. Розроблення кіберзброї неймовірно складно відстежити. Національні кордони для онлайн-діяльності нічого не важать, тому що користуючись на сьогодні високим рівнем інформаційної технології навряд чи можна зупинити дії професіонала-хакера від полювання на цінну інформацію та документацію, яка носить конфіденційний характер. І саме головне, слід пам'ятати, що як свідчить міжнародна практика, головне завдання при застосуванні інформаційної зброї полягає, в першу чергу, крім несанкціонованого впливу на систему управління, не стільки знищенню, а скільки підпорядкуванню її у майбутньому своїм цілям.

Ситуація більше ускладнюється ще і тим, що сама природа Інтернету суперечить традиційним уявленням про те, що і суверенні країни, і бойові дії прив'язані до географії та фізичного місцезнаходження. Компанія може мати головний офіс в одній країні, а мережі й сервери – в іншій. Якщо кібератаку спрямовано проти цих мереж і серверів, хто має реагувати: країна, де розташовано головний офіс, чи країна, де розміщено мережі й сервери? Якщо, не реагуватиме жодна із цих двох країн, а натомість корпорація захищатиметься сама, організувавши власний кібернаступ, то хто ще опиниться втягненим у цю ситуацію? Якщо немає міжнародних норм і договорів, що дають визначення і встановлюють межі кіберконфліктів, то кібервійна може відбуватися між двома країнами, а може – між країною і компанією.

Важливим у цьому протистоянні є і те, що протягом декількох сторіч пограбування банку було пов'язано із невід'ємною ситуацією, за якою приміщення захоплювалось озброєними

людьми, які за певним розрахунком у декілька хвилин зникали з пограбованими грошима та цінностями у невідомому напрямку.

Нині для пограбування банку не потрібно здійснювати озброєний напад з панчохами на голові, для цього необхідний лише доступ до комп'ютера. Так, першим великим світовим інцидентом вважається викрадення 12 млн. дол. з рахунків американського Citibank хакером-самоуком Володимиром Левіним. Ще у 1994 році, не виходячи з квартири, він пограбував один з найбільших фінансових закладів планети. Для цього йому навіть не знадобилося знання англійської – лише мова програмування. Тоді злочин назвали «пограбуванням сторіччя». Проте сховатися від правосуддя Левіну не вдалося – його спіймали та засудили [6].

Відповідно до вище вказаного постає необхідність розробки критеріїв трактування подібних інцидентів, з метою їх чіткої класифікації на предмет загроз економічної безпеці, людині, суспільству, державі з подальшою їх правовою оцінкою. Особливо ця методика протидії інформаційній війні, кібертероризму та кіберзлочинності, на підставі прийнятого 5 жовтня 2017 року № 2163-VIII Закону України «Про основні засади забезпечення кібербезпеки України» [7], який вступив у дію лише у 2018 року, повинна вивчатися та удосконалюватися у навчальних закладах системи МВС України, для прищеплення необхідних знань майбутнім правоохоронцям.

Разом з тим, не зважаючи на те, що вже понад одного року діє Закон України «Про основні засади забезпечення кібербезпеки України» і цей закон має деякі невдосконалені положення. Так, хоча законом і вказується на цивільну, адміністративну та кримінальну відповідальність за порушення осіб у сфері кібербезпеки, проте у відповідних кодексах відсутні поняття «кіберпростір» та не визначена відповідальність за кіберзлочини.

Таким чином, наступною пропозицією є доцільність розширення взаємодії державних органів з приватним сектором. Прикладом є підписаний Меморандум між Службою безпеки України та компанією «Лінкос груп» у липні 2018 року щодо організації взаємодії з питань обміну інформацією щодо кіберінцидентів. На думку фахівців спецслужби, така співпраця сприятиме не тільки

посиленню спроможності України у протидії кіберзагрозам, але й стимулюватиме індустрію для створення власних програмних продуктів, поліпшить взаємодію суспільства і держави, а також підвищить прозорість діяльності та довіру до органів влади [8].

1. Канигін Ю. М., Кушерець В. І. Біблія та майбутнє науки: орієнтири сучасних знань. Київ: Т-во «Знання України», 2009. 163 с.
2. Шеннон К. Работы по теории информации и кибернетике. М. : ИЛ, 1963. 830 с.
3. Довгань О. Д., Ткачук Т. Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. Інформація і право. №.4. 2018. С. 79-89
4. Clarke, Richard A. Cyber War, HarperCollins (2010) URL: https://www.harpercollins.com /978006 1962233/cyber-war/
5. Кім Зеттер. Хакерська атака Росії на українську енергосистему: як це було. URL: texty.org.ua/pg/article /newsmaker/read/66125/Hakerska _ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak
6. Ограбление «по-новому». Какие банки пострадали от хакеров. URL: https://www. epravda.com.ua/rus/publications /2017/11/16/631231/
7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://pravo.uteka.ua/doc/Pro-osnovni-zasadi-zabezpechennya-kiberbezpeki-Ukraini
8. СБУ створить «єдиний щит» для кібербезпеки українців. URL: https://znaj.ua/society/sbu-stvoryt-yedynyj-shyt-dlya-kiberbezpeky-ukray inciv

Історія розвитку інформаційного забезпечення органів Національної поліції України

Ямкова Тетяна Іванівна

здобувач вищої освіти
Львівського державного університету внутрішніх справ

Сьогодні важко уявити роботу Національної поліції без застосування інформаційних технологій, оскільки інформаційне суспільство стрімко розвивається, а з ним і інформаційне право. Основними тенденціями в розвитку інформаційних систем у правоохоронних органах є вдосконалення системи інформаційного забезпечення, освоєння новітніх технологій, використання спеціальних засобів для захисту інформації, управління системою даних та ін.

Інформаційне забезпечення правоохоронних органів почалося у 50-70-х рр. минулого століття. Цей період відзначався комп`ютеризацією. Відповідно до цього інформація почала ставати централізованою і використовувалася при оперативно-розшуковій діяльності. Саме з цим періодом пов`язують із зародженням теорії про ОРД.

В Україні єдиної системи обліків в ОВС не існувало аж до 1960 р. Та в 1961 р. Міністерством внутрішніх справ була введена в дію Інструкція щодо обліків в органах внутрішніх справ. Науково-практична база інформаційного забезпечення правоохоронних органів України сформувалася на початку 1970- х років. Тоді створено Республіканський науково-дослідний інформаційний центр МВС УРСР, до основних напрямів діяльності якого належали: надання оперативно-довідкової, розшукової, статистичної та іншої інформації; збирання, обробка, зберігання, аналіз інформації про злочини та осіб, які їх учинили; розгляд матеріалів про оголошення та припинення розшуку осіб, які зникли безвісти, невпізнаних трупів тощо. Створено мережу інформаційно-обчислювальних центрів у всіх регіонах країни – обласних управліннях внутрішніх справ, обладнаних електронно-обчислювальними машинами (ЕОМ) типу «Мінськ-32»,

«Мінськ-22», «СМ» та «ЄС». Першими автоматизованими інформаційними системами були «Профілактика-Розшук», «Розшук», «Статистика» та інші. Інформаційні центри стали осередками збору основних масивів інформації і технічних засобів обробки, функціональних автоматизованих інформаційних систем [1, с. 153]. Наступним важливим кроком було у 1985 році створення єдиного автоматизованого банку даних які дали правоохоронцям доступ до багатьох видів інформації, що звичайно, ж ефективно вплинуло на їх діяльність. Зокрема, було створено такі автоматизовані системи: «Автомобіль», «Адмінпрактика», «Номерні речі», «Патруль» та ін.

Після проголошення незалежності України вся правоохоронна система була перебудована. Важливим кроком стало прийняття Закону «Про оперативно-розшукову діяльність» від 18 лютого 1992 року, який говорить, що Оперативно-розшукова діяльність – це система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [2]. Отже, із дефініції зрозуміло, що дозволяється використання також мультимедійних засобів. В цей час також використовуються дані з інформаційних банків інтерполів. У 2002 році створюється підрозділ МВС – Департамент інформаційно-аналітичного забезпечення МВС завданням якого є розробка та впровадження новітніх інформаційних технологій у діяльність правоохоронних органів. Підрозділ, зокрема, створбє такі інформаційні системи як: «Зброя у розшуку», «Мобільні телефони», «Неопізнані трупи», «Особи, які переховуються від органів влади», «Культурні цінності» та ін.

Останній етап розвитку інформаційно-аналітичної роботи тісно пов`язаний з прийняттям у 2012 році нового Кримінально процесуального кодексу, який передбачив проведення негласних слідчих (розшукових) дій, що суттєво змінює організацію оперативно-розшукової діяльності. У 2015 році Наказом Національної поліції було створено Департамент інформаційної підтримки та координації поліції. Проте, у 2018 році він був перейменований на Департамент інформатизації МВС. Департамент є структурним підрозділом апарату МВС, який

організовує і здійснює заходи, передбачені законодавством України та іншими-нормативно правовими актами центральних органів виконавчої влади, спрямовані на інформаційно-аналітичне забезпечення правоохоронної діяльності та захист персональних даних під час їх обробки в органах і підрозділах внутрішніх справ України. Департамент є головним підрозділом у системі підрозділів інформаційно-аналітичного забезпечення та здійснює організаційно-методичне керівництво їх діяльністю, а також формує провідні напрями діяльності Міністерства у сфері інформатизації та захисту персональних даних і розробляє проекти нормативно-правових актів з інформаційно-аналітичного забезпечення й обробки персональних даних у системі МВС [3, с. 266].

Історія розвитку інформатизації МВС говорить, що цей процес є необхідним і важливим, а також є присутнім і на сучасному етапі.

Вирішення завдань сучасного інформаційного забезпечення досягається шляхом:

- впровадження єдиної політики інформаційного забезпечення;
- створення багатоцільових інформаційних підсистем діяльності МВС України;
- удосконалення організаційно-кадрового забезпечення інформаційних підрозділів;
- інтеграції та систематизації інформаційних підсистем МВС України на всіх рівнях;
- розбудови інформаційної мережі;
- створення умов для ефективного функціонування інформаційних банків даних, забезпечення їх повноти, вірогідності, актуальності, безпеки та законності;
- переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою;
- поширення мережі комп'ютеризованих робочих місць користувачів інформаційних підсистем;
- подальшої комп'ютеризації інформаційних фондів;
- впровадження сучасних інформаційних технологій [4].

Отже, інформатизація системи правоохоронних органів через застосування новітніх технологій є обов`язковою, оскільки це допомагає ефективніше боротися зі злочинністю. Історія показує нам створення різноманітних інформаційних систем, які сьогодні ужосконалюються. Також потрвбно зауважити, що впровадження використання різноманітних технологій необхідне для того, щоб відповідати законодавству, зокрема таке положення стосується здійснення негласних слідчих (розшукових) дій.

---

1. С. Банах. Інформаційне забезпечення діяльності правоохоронних органів: історико-правовий аналіз. Актуальні проблеми правознавства. Випуск 2 (18). 2019. – С. 180
2. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року N 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12/ed20110612#o15
3. Г.М. Шорохова. Інформаційне забезпечення діяльності територіальних органів поліції України. Юридичний науковий електронний журнал. 2018. № 6. – С. 425
4. Інформаційне забезпечення органів Національної поліції. URL:https://arm.naiau.kiev.ua/books/inform_zabezpechennia/matherials/rozdil1.html

Розділ 2. НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНОТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ

Змішане навчання інформатики

Глинський Ярослав Миколайович

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

Камінський Богдан Тадейович

директор коледжу «Інфокомунікації» Національного університету «Львівська політехніка», кандидат педагогічних наук, доцент

Пелех Ярослав Миколайович

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

Одним із перспективних напрямків розвитку освіти в сучасному світі вважається змішане навчання (інші терміни: гібридне, комбіноване навчання). Курс змішаного навчання формується із традиційних форм навчання: очного та дистанційного, причому з цих двох форм вибирається лише позитивний досвід. Під змішаним навчанням розуміють [1] деяку комбінацію аудиторного та електронного навчання, де одна частина пізнавальної діяльності суб'єктів навчання відбувається аудиторно під безпосереднім керівництвом педагога, а друга полягає в активній самостійній позааудиторній роботі з електронними ресурсами.

За іншим визначенням [1], змішане навчання – це цілеспрямований процес здобування знань, набуття вмінь та навичок в умовах інтеграції аудиторної та позааудиторної навчальної діяльності суб'єктів освітнього процесу на основі впровадження і взаємного доповнення технологій традиційного, електронного, дистанційного та мобільного навчання за наявності самоконтролю студента за часом, місцем, маршрутами та темпом навчання.

У даній роботі досліджується і узагальнюється досвід використання засобів, характерних для чистого дистанційного навчання, для проведення аудиторних занять зі студентами першого курсу

очної форми підготовки, які вивчають дисципліну «Інформатика» як базову. Опишемо результати проектування методів і засобів організації змішаного навчання на очну форму навчання у випадку даної технічної дисципліни.

Навчальний процес в нас побудований на використанні закритих он-лайн курсів у віртуальному навчальному середовищі університету, створеному на базі LMS Moodle і на його спрощеній моделі для коледжу «Інфокомунікації». Для подання теоретичного матеріалу були використані відомості з навчального посібника [2], структуровані у файлах лекцій у форматі pdf. Теоретичні матеріали, які під час лекції демонструються на великий екран, супроводжуються коментарями лектора, а також відеорядом. Усі матеріали завжди доступні для студентів у позааудиторний час. Тому зникла необхідність у фронтальному конспектуванні. Студенти занотовують лише тему і план лекції, опорні поняття і рекомендації лектора щодо організації навчання. Лектор стає ментором.

Роль, зміст, технології створення і способи використання відеоресурсів для даного курсу висвітлювались в [3]. Результати апробації підтвердили їх ефективність, що дає змогу розглядати курс також з позицій мобільного навчання. Ефект забезпечується головно вдало сформованим контентом відеоресурсів, а також тим, що ці ресурси тепер доступні студентам очної форми навчання для одноразового чи багаторазового перегляду причому у любий час і з любого розташування, де є відповідний зв’язок. Лекція як традиційний вид педагогічної діяльності суттєво змінилася. Таку лекцію, побудовану на фронтальному використання динамічних (у формі відео) і статичних (у формі презентацій) освітніх ресурсів, ми називаємо відеолекцією і вважаємо це новим різновидом педагогічної діяльності, який приходить на заміну традиційним лекціям.

Відповідно до теоретичних вимог змішаного навчання студентам пропонуються чотири можливі траєкторії навчання (мінімальна, середня, висока і поглиблена), які студент може обрати залежно від рівня підготовки, зацікавлення, особистих потреб і вимог навчальної програми. Реалізація цих траєкторій відбувається в

рамках моделі навчання face-to-face, а також у рамках моделі «віртуальний клас». Перебіг лабораторних занять також змінився. Під час заняття студенти можуть виконувати різні види робіт. Тут застосовуються різні прийоми навчання, які чергуються відповідно до ротаційної моделі навчання. Виконані роботи студенти доопрацьовують вдома, завантажують у ВНС і захищають на наступному занятті.

Для фронтального контролю поточних знань і для спілкування викладача зі студентами під час пари чи для дистанційного спілкування викладача з відсутніми студентами використовуємо чат, як технологію характерну для дистанційного спілкування. Запросивши студентів до чату, викладач може задавати запитання, на кшталт, обчисліть =if(3>5; 2; 4) чи = average(2;sum(2;4);4) тощо і отримувати відповіді в режимі бліц-вікторини, що є ефективним педагогічним засобом, який зацікавлює і мотивує студентів, оскільки містить елементи геймифікації навчання. Ми застосували чат-технологію для захисту робіт студентами, які через хворобу знаходилися вдома. Цей досвід дав змогу застосувати прийом дистанційного захисту робіт для студентів, які раніше продемонстрували високу якість і самостійність виконання робіт в очному режимі навчання. Викладач оцінює роботу студента заочно і супроводжує оцінку короткою рецензією. Також зацікавлюємо студентів до виконання робіт на випередження графіка, що є прикладом навчання в моделі «перевернутий клас», коли студент опрацьовує матеріал самостійно дистанційно і звертається до викладача за очною консультацією лише у разі потреби.

Кожна лабораторна робота оцінюється двома, рідше трьома балами. Оцінки заносяться в електронний журнал. На цьому етапі знову застосовується геймифікація, оскільки весь курс розглядається як гра, в які студент повинен набрати певну кількість балів зі ста можливих. На кожному занятті він отримує не формальні оцінки у п’ятибальній системі, а залікові бали, яких за курс можна набрати до 100 за всі види робіт. Серед цих видів є невеликі дистанційні тести для самоконтролю, які студент може пройти в аудиторії чи вдома. Тут надаються три спроби (в ігровій термінології «три життя»), в електронний журнал автоматично

заноситься результат останньої спроби. Для дистанційного тестування є спеціальна система оцінювання. Найважливішим є підсумковий заліковий великий за обсягом матеріалу тест, який студенти проходять очно на останньому занятті. Залікову оцінку (набрану зі 100 балів) студент отримує відразу після закінчення підсумкового тестування як останнього виду робіт, що фіксуються в електронному журналі. Кількість балів, отримані за курс даної дисципліни, можна автоматично передати з ВНС у систему «Деканат» і занести в підсумкову електронну відомість, яку викладач отримає в сесію у своєму віртуальному кабінеті.

Ми переконалися, що серед сучасних підходів змішане навчання заслужено займає провідне місце. Також ми переконались у тому, що як зазначається в дослідженнях багатьох фахівців [1] змішане навчання є руйнівним, оскільки воно руйнує звичні погляди на освітній процес, висуває інколи непрості (для адміністрації) вимоги до зменшення наповненості класів, до рівня матеріально-технічного забезпечення навчального процесу, а головне, до рівня підготовки, самовіддачі педагогічних кадрів, що сьогодні не корелюється з рівнем оплати їх праці.

---

1. Теорія та практика змішаного навчання : монографія / [Кухаренко В. М., Березенська С. М., Бугайчук К. Л. та ін.];за ред. В. М. Кухаренка. – Харків : Міськдрук, НТУ ХПІ, 2016. – 284 с.
2. Глинський Я.М. Інформатика. Практикум з інформаційних технологій. «Підручники і посібники», Тернопіль, 2014 – 304 с.
3. 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.

Інноваційні особливості електронного навчання для державних службовців із використання дистанційних освітніх технологій

Грищук Аліна Борисівна

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

Інноваційні технології у навчанні державних службовців є важливим інноваційним моментом навчання у сфері підвищення їх професійного рівня. Враховуючи важливість навчання державних службовців як важливого елементу проходження служби, слід зазначити, що

На думку Ю. Бистрової: «Інноваційна навчальна технологія та сучасні методи викладання як загально дидактичний процес, полягає у використанні сукупності оригінальних способів і прийомів спільної діяльності суб'єктів освітнього процесу, спрямованих на досягнення мети навчання, розвитку особистості та креативно-фахового здобуття знань і компетенцій відповідно до завдань підготовки професіоналів нового часу».

Серед сучасних технологій навчання вона виокремлює наступні: – Особистісно-орієнтовані; – Інтеграційні; – Колективної дії; – Інформаційні; – Дистанційні; – Творчо-креативні; – Модульно-розвивальні.

Слід зазначити, що професійне навчання державних службовців має свої особливості, оскільки воно здійснюється з урахуванням принципів навчання дорослих, що вимагає інших підходів до організації навального процесу, та має здійснюватись упродовж всього життя [1, с 31-33].

Якщо розглянути особливості дистанційної освіти з погляду комунікацій між викладачем і студентом, то можна визначити такі її характерні риси: – самоосвіта як основа дистанційного навчання, що передбачає само мотивацію студента щодо власного навчання, а також певний рівень самоорганізації

особистості; – спілкування викладача і слухача за принципом «один до одного», що відповідає за формою і змістом індивідуальній консультації; – спілкування і взаємодія «один до одного» не виключає взаємодії «одного до багатьох», оскільки викладач, відповідно до заздалегідь складеного графіка, працює відразу з безліччю студентів. Така форма взаємодії нагадує традиційне навчання в аудиторіях; – взаємодія «багатьох до багатьох» означає, що можливе одночасне спілкування безлічі студентів, які обмінюються між собою досвідом і враженнями.

Електронні навчальні курси є раціональними: – розширюють можливості традиційного навчання; – роблять навчальний процес більш різноманітним; – дозволяють підвищити ефективність самостійної роботи студентів, рівень мотивації до навчання, стимулювати розвиток їх інтелектуального потенціалу; – автоматизувати процес контролю та оцінювання здобутків учнів.

Виходячи з цього, дистанційне навчання має низку переваг у порівнянні з традиційним навчанням: передові освітні технології, доступність джерел інформації, індивідуалізація навчання, зручна система консультування, демократичні стосунки між студентом і викладачем, зручний графік та місце роботи [2, с. 202-203].

Електронне навчання – це гнучке навчання в інтерактивному освітньому середовищі за допомогою контенту з усього світу, що знаходиться у вільному доступі, який дозволяє розширити межі навчання, причому не тільки з точки зору кількості студентів, а й з точки зору часових та просторових показників: навчання стає доступним усюди і завжди [3, с. 127-128].

У зв’язку з цим перехід в системі професійної підготовки державних службовців від традиційного навчання до інноваційного повинен супроводжуватися застосуванням у навчальному процесі таких основних принципів і методик:

1) «Навчання, орієнтоване на результат» – забезпечує цілеспрямованість, транспарентність і результативність процесу підготовки на основі бально-рейтингової оцінки знань.

2) «Модульна організація навчання» – гарантує гнучкість і високу динаміку освітнього процесу.

3) «Навчання через постановку і вирішення конкретної управлінської задачі або управлінської ситуації» – дозволяє адаптувати процес навчання до реальних умов практики управління.

4) «Індивідуалізація процесу навчання через розширення і оптимізацію умов для самостійної навчальної роботи» – передбачає скорочення обов'язкових навчальних дисциплін при розширенні переліку елективних, використання дистанційного та «віртуального» навчання.

5) «Інтенсифікація навчання» – припускає прискорений обмін ідеями, інформацією і результатами, відкритий доступ до джерел професійної інформації та безперервне її оновлення для отримання інтенсивних знань.

6) «Підвищення конкурентоспроможності державних службовців» – за умови високої конкурентоспроможності навчального закладу в контексті його здатності задовольняти, по-перше, попит споживачів освітніх послуг, по-друге, створювати конкурентні переваги з метою залучення споживачів, по-третє, забезпечувати базові професійні компетенції фахівців, формувати у них креативні здібності для вирішення нестандартних управлінських завдань.

Таким чином, фундаментальним умовою підготовки державних службовців є формування у них професійних домінант інноваційного характеру. При розробці освітньої стратегії в системі підготовки державних службовців повинні враховуватися названі особливості та тенденції розвитку з метою забезпечення креативності державної служби, спрямованості державних службовців в майбутнє, надання їм свободи вибору освітніх траєкторій, розширення сфери академічних знань, збільшення професійної мобільності та само ідентифікації [4, с. 38-39].

Теоретичні аспекти дистанційного навчання передбачають наступні ознаки та переваги:

1. Актуальність, що передбачає використання найсучасніших засобів для здобуття інформації за допомогою Інтернету.

2. Порівняно більші обсяги інформації, яку можна отримати в умовах дистанційного навчання у коротші строки.

3. Зручність, за якої кожен студент має можливість обрати власний ритм та режим отримання знань у комфортній для нього обстановці, що сприятливо вплине на сам процес навчання.

4. Індивідуалізація, що дає змогу кожному студенту узгодити навчання зі своїми потребами.

5. Доступність, що передбачає економію часу та коштів за рахунок використання навчальних приміщень та представлення вільного доступу до навчальних матеріалів.

6. Гнучкість, яка надає можливість викладати матеріал відповідно до рівня підготовки та базових знань студентів, створюючи додаткові сайти з необхідною інформацією та сайти, на яких студенти можуть обмінюватися інформацією, відповідаючи на запитання один одного та навчатися, навчаючи інших.

7. Відсутність географічних бар'єрів, за якої відпадає необхідність дорогого переїзду та проживання в інших країнах, а натомість надається можливість спілкування з викладачами та студентами по всьому світу без обмежень. Безумовно, як і в кожній формі отримання знань, у дистанційній є і свої недоліки, але їх подолання стає можливим завдяки рокам практичного застосування цієї форми не лише як допоміжної та однієї з побічних, а як можливо рівної класичній формі здобуття освіти [5].

Проте, система дистанційного навчання має і недоліки. По-перше, для успішної корекції навчання та адекватного оцінювання важливо мати безпосередній контакт із здобувачем. Крім того, неможливо точно перевірити, чи саме та людина працює, виконує завдання чи це робить хтось інший. Тому остаточний контроль якості знань все ж таки проводиться на очній сесії. Крім того, не у всіх населених пунктах є можливість доступу до мережі Інтернет-зв'язку. І найголовніше, при дистанційному навчанні втрачається безпосередній контакт між викладачем та студентом. При тривалому дистанційному навчанні студент перестає правильно формулювати свої думки, висловлюватись та проводити дискусійне обговорення. Разом з

тим, така форма навчання потребує свідомого і мотивованого підходу до отримання освіти. Можливість навчатися у зручний час може перетворитися не на систематичне навчання, а на постійну прокрастинацію цього виду діяльності. Саме тому дистанційна форма потребує особливої самоорганізованості та вміння розрахувати свій час. За умови дистанційного навчання активна роль викладача не зменшується, оскільки він має визначити рівень знань здобувача, та прийняти рішення щодо коригування програми навчання з тим, щоб домогтися найкращого засвоєння пройденого матеріалу [4, с. 41].

Дистанційне навчання потребує сильної мотивації й самоорганізації, вміння працювати самостійно. З метою подолання цієї проблеми необхідно використовувати різні форми активного спілкування між студентами групи і викладачем, проведення дискусій, чатів, що значно посилює мотивацію до навчання, поліпшує засвоєння матеріалу.

Потенціал дистанційних технологій оцінюється високо, значно підвищується адаптованість у професійній сфері. Дистанційна освіта вже зайняла одне із провідних місць у системі вищої освіти, але найбільший ефект досягається завдяки комплексному поєднанню традиційних форм та методів навчання з можливостями дистанційного навчання [6].

Отже, одним із основних напрямків розвитку освітньої діяльності – є запровадження, використання та удосконалення дистанційного навчання. Україна знаходиться на стадії впровадження та використання освітніх дистанційних систем, проте потребує все більшого вивчення та закріплення законодавчої бази загалом. Кількість організацій та структур, які розробляють та впроваджують дистанційні системи є досить незначною, оскільки потребує значних витрат та зміни свідомості українського суспільства.

Для повноцінного функціонування слід забезпечити не лише науково-методичну базу, а й належним чином реалізувати законодавчу базу в освітній сфері України.

1. Бистрова Ю. В. Інноваційні методи навчання у вищій школі України. Ю. В. Бистрова. Право та інноваційне суспільство. 2015. №1. С. 31-36
2. Долинський Є. В. Дистанційне навчання – одна з прогресивних форм підготовки фахівців. Є. В. Долинський. Теоретичні питання культури, освіти та виховання: Збірник наукових праць. Вип.42 За заг. ред. проф. Матвієнко О. В. К.: Вид. центр КНЛУ, 2010. С. 202-207.
3. Методика организации повышения квалификации педагогов в условиях внедрения системы електронного обучения : методич. Пособие. Г. К. Ахметова, Ж. А. Караев, С. Т. Мухамбетжанова. Алматы: АО НЦПК «Өрлеу», 2013. 408 с.
4. Клокар Н. Методологічні основи запровадження дистанційного навчання в системі підвищення кваліфікації. Н. Клокар. Шлях освіти. 2012. № 4 (46). С. 38-41.
5. Болюбаш Н. М. Фактори та умови формування професійної компетентності майбутніх економістів засобами інформаційного середовища Moodle. Н. М. Болюбаш. Інформаційні технології і засоби навчання. 2010. № 3 (17). URL: http://www.ime.eduua.net/em17/emg.html.
6. Напрями підготовки та спеціальності у Харківському національному економічному університеті. URL: http://www.hneu.edu.ua/Specialities.

Перспективи впровадження навчально-інформаційних курсів в системі професійної підготовки державних службовців

Грищук Аліна Борисівна

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

Проць Іванна Миколаївна

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

Одним із напрямків реформування та розвитку сучасної вищої освіти, що вимагає всебічної інформаційної підтримки, є дистанційне навчання, яке стає все популярнішим в світі.

Проте, не варто недооцінювати дистанційну освіту, яку окремі фахівців відносять до, так званої, підривної інновації для вищої школи. Згідно з відомим у теорії бізнесу поділом інновацій на підтримувальні й підривні, останні (на відміну від перших, що покликані вдосконалювати, модернізувати існуючі системи й процеси в освіті) завдяки своїй технологічній новизні та бізнес-моделі змінюють освітній ринок аж до його завоювання.

Лі Юань і Стефан Пауелл, фахівці Бостонського університету (Великобританія) вважають, що уже зараз університетам необхідно сповна скористатися підривним потенціалом масового відкритого навчання, оскільки «існує явна необхідність у нових бізнес-моделях та інноваціях у вищій освіті для того, щоб впоратися з труднощами соціальних і економічних змін у подальшому» [1].

Інформаційно-технологічна тенденція розвитку дистанційної освіти в Україні тісно пов’язана з інформатизацією, яка на сучасному історичному етапі має стратегічне значення для нашої країни. У наш час виробництво інформаційного продукту через

його високу товарну вартість є важливим чинником економічного розвитку країни. Інформаційні технології, проникаючи в усі галузі діяльності людини, змінюють характер праці як у виробничій, так і у невиробничій сферах, впливають на структуру національної економіки, підвищують рівень інформування широких верств населення й таким чином сприяють демократизації суспільства. Ці тенденції, що в усьому світі визначаються як процес інформатизації, позначаються на житті суспільства. Порівняно з традиційними індустріальними методами їх застосування дає можливість забезпечити підвищення рівня матеріалізації інтелектуальної праці і якості виробів. Саме через це найбільш розвинуті країни світу отримують на міжнародних ринках значні переваги. На відміну від зарубіжних моделей, українська дистанційна освіта більш наближена до нашого споживача і є більш демократична. Органічно поєднуючи в собі змішані технології відкритої освіти (кейс-технології, TV-технології, мережеві технології), українська дистанційна освіта стає найбільш доступна широким масам населення, роблячи можливим здобувати освіту не на все життя, а все життя.

Дистанційна освіта розвивається дуже швидко, і для України є перспективною формою вищої освіти. На Заході ця форма з'явилася вже досить давно і має велику популярність серед студентів через її економічні показники і навчальну ефективність. Дистанційну форму навчання ще називають «освітою на протязі всього життя» через те, що більшість тих, хто навчається – дорослі люди. Багато хто з них вже має вищу освіту, проте через необхідність підвищення кваліфікації або розширення сфери діяльності у багатьох виникає потреба швидко і якісно засвоїти нові знання і набути навички роботи. Саме тоді оптимальною формою може стати дистанційне навчання. Для вдосконалення та поширення високих дистанційних технологій необхідне рішення двох основних проблем. Головна, знаходиться в області права, інша – в сфері фінансування робіт з розробки та впровадження інноваційних технологій [2, с. 149].

З метою їх успішного вирішення об'єктивно необхідна реалізація наступних першочергових заходів і напрямів:

- розробка і реалізація Загальноукраїнської програми дистанційної безперервної освіти; викорінення протиріч в законодавстві про освіту в Україні, приведення його у відповідність з об'єктивними потребами і тенденціями розвитку дистанційних форм навчання;
- розробка наукових основ, що забезпечують інноваційність і дистанційних форм, і рівнів освіти, програм та навчальних планів;
- наукове обґрунтування ринку навчальної літератури, комп'ютерних та мультимедійних баз даних, виключення можливості його монополізації;
- створення варіативних методик з дистанційного навчання людей з різними рівнями здібностей, віком і потребами;
- забезпечення переходу до інтерактивних методів та практичної спрямованості дистанційного навчання;
- створення системи підтримки проектів, нововведень в технології дистанційної освіти, її заочних та інших форм;
- надання права навчання студентів,
- отримання атестатів і дипломів у різних освітніх закладах.

Відкрита освіта дає широке поле для наукових досліджень, що сприяють розвитку творчих ініціатив розробників і педагогів, переходячи з об'єкта вивчення в об'єкт прогнозування, конструювання та проектування [3].

Крім цього, система дистанційного навчання розрахована, в основному, на людей достатньо свідомих, які не потребують постійного контролю з боку викладача, тому важливу роль у цьому випадку відіграє мотивація студентів, їх здатність до самоорганізації. Якщо за традиційних форм навчання основною задачею студента було запам'ятати матеріал та потім його відтворити, то за умови застосування дистанційних технологій у студентів розвиваються уміння співставлення, синтезу, аналізу, оцінювання виявлення зв'язків, планування, групової взаємодії з використанням інформаційно-комунікаційних технологій та технології дистанційного навчання. Технологія дистанційного навчання посилює роль методів активного пізнання. Реалізацію технології дистанційного

навчання можна забезпечити шляхом розробки моделі використання віртуально-навчальних середовищ.

Впровадження у навчальний процес віртуально-навчальних середовищ і надання студентам та викладачам необхідних методичних рекомендацій щодо використання віртуально-навчальних середовищ у фаховій підготовці забезпечить просування за критеріями та рівнями якості застосування технології дистанційного навчання у фаховій підготовці фахівців з обліку і аудиту та надасть змогу підвищити якість фахової підготовки. Таким чином, на сьогоднішній день, виникає потреба розробки і запровадження у навчальний процес програм дистанційного навчання, що відповідають кращим світовим зразкам і забезпечують підготовку фахівців на високому професійному рівні. Використання мережі Internet дає можливість оперативного доступу до інформаційних ресурсів навчального закладу та можливість ефективної взаємодії «викладач-студент», як в on-line, так і в offline режимах [4].

Суспільство починає сприймати й оцінювати дистанційну освіту передусім як доступний і зручний формат отримання особистісно і професійно-значущої інформації. Масове звернення аудиторії з різних куточків світу до он-лайн-курсів як систематизованої, адаптованої й дидактично структурованої інформації свідчить про актуальну потребу в ній. У цьому сенсі он-лайн-освіту можна трактувати як самостійну інформаційно-пошукову діяльність користувача всесвітньої електронної мережі.

Традиційним академічним студіям бракує конективізму як методології процесу спільного навчання, яка відбиває в собі особливості інформаційної навчальної діяльності в мережі. Потрапляючи в цифровий інформаційний простір, той, хто навчається он-лайн, використовує як наявні вузли джерел і зв'язків, так і формує персональну навчальну мережу. Пошук розпорошеної в базах даних інформації, відбір і зв'язування її елементів у більш-менш цілісну картину знань та їх поширення здійснюється в он-лайн – навчанні не лише індивідуальними зусиллями, а й колективними, тобто за допомогою інших суб'єктів. Результатом чого стає спільне формування знань,

інтегративний процес їх вироблення. Словом, цінність конективізму як нетрадиційного дидактичного підходу зумовлена тим, що слухачі он-лайн - курсів навчаються один в одного.

До них належать ресурси, створені самими учасниками он-лайн - курсів: пости в блогах, веб-сторінки, ментальні карти (інтелект-карти, карти пам'яті, асоціативні карти, діаграми зв'язків), інфограми, підкасти, стрінкасти, конспекти і т. ін. Кожен окремо взятий артефакт, як зазначає Костянтин Бугайчук «можна розглядати, як знімок ділянки мережі і зв'язків між поняттями й ідеями, які автор зміг встановити в ході вивчення теми курсу. Це мережа, яку він побудував у своїй свідомості й подав для обговорення рис інших учасників» [2, с. 153-155].

Суспільство починає сприймати й оцінювати дистанційну освіту передусім як доступний і зручний формат отримання особистісно і професійно значущої інформації. Масове звернення аудиторії з різних куточків світу до он-лайн-курсів як систематизованої, адаптованої й дидактично структурованої інформації свідчить про актуальну потребу в ній. У цьому сенсі онлайн-освіту можна трактувати як самостійну інформаційно-пошукову діяльність користувача всесвітньої електронної мережі.

Впровадження в освіту технологій дистанційного навчання значно підвищує продуктивні можливості вищої школи, розширює інформаційне освітнє середовище, збільшує можливості комунікації студентів і педагогів з колегами інших ВНЗ, надає доступ до світових інформаційних ресурсів. Під впливом дистанційної освіти, яка не в змозі повністю перебрати на себе класичну місію традиційного університету, нині формується модель гібридного університету, яка покликана поєднати аудиторне та он-лайн навчання. Глибина розуміння інформації повинна стати індикатором ступеня її опрацювання й засвоєння, а це неможливо без комплексного поєднання традиційних видів навчання з дистанційними технологіями [5].

Слід зазначити, що дистанційна освіта в Україні почала свій розвиток із 2000 року. І вже на сьогодні, займає широку ланку на теренах освітнього процесу. Звичайно, не кожна сфера суспільного та професійного життя спромоглась на активне

використання електронного навчання. Проте останнім часом розвивається такий важливий напрям, як створення дистанційних курсів. Це досить складний вид діяльності, що потребує значного рівня знань і кваліфікації. Адже, навчання відбувається за допомогою новітніх технологій, а саме: використання тренінгів та вебіранів; проведення он-лайн конференцій та зустрічей; залучення нових методів, таких як дидактичні ігри, документальні фільми та виступи всесвітньовідомих людей.

Таким чином, дистанційна освіта – є досить новою формою освіти, яка потребує все більшого розвитку та вдосконалення зі сторони. Впроваджуючи нові шляхи для отримання інформації, державні органи, структури та організації будуть забезпечені професіоналами, які володіють навичками та знаннями, що дають змогу приймати актуальні рішення, пропонувати та формувати якісні пропозиції в державотворчому процесі.

1. Юань Ли. МООК и открытое образование: Значение для высшего образования. Белая книга Ли Юань, Стефан Пауэлл; пер. Виталина Лаптева. URL: http://publications. cetis.ac.uk/2013/667
2. Бугайчук К. Л. Массовые открытые дистанционные курсы: история, типология, перспективы. К. Л. Бугайчук. Высшее образование в России. 2013. № 3. С. 148–155.
3. Перелік освітньо-кваліфікаційних рівнів та напрямів підготовки (спеціальностей), за якими оголошується прийом на навчання до Національного педагогічного університету імені М. П. Драгоманова URL: http://www.npu.edu.ua/index.php?option=com_content&view=article&id=2003%3A2012-12-21-0938-54&catid=248%3A2013-06-19-07-36-08&Itemid= 299&lang=ua.
4. Концепція розвитку дистанційної освіти в Україні /затверджено Постановою МОН України від 20.12.2000 р. URL: http://www/ osvita.org.ua/distance/pravo.
5. Офіційні матеріали наради-семінару з питань нормативного забезпечення дистанційної форми навчання в Україні; Національний технічний університет України «КПІ», м. Київ, 2012 URL:http://ipo.kpi.ua/ua/distance/dlabout.html

Застосування паралакс ефекту у ВЕБ-дизайні

Зевако Катерина Олександрівна

здобувач вищої освіти кафедри інформатики і кібернетики
Мелітопольського державного педагогічного університету
імені Богдана Хмельницького

Стрімкий розвиток науки надає збільшені можливості щодо створення нових ефектів у веб-дизайні. Зі збільшенням різновидів також підвищується рівень конкурентності та з'являється загроза втрати індивідуальності. В той самий час, аби це змінити необхідно застосовувати конкуруючі ефекти, які будуть підвищувати попит на ресурс. До таких ефектів можна віднести паралакс.

Сьогодні проблема щодо знаходження ефекту, який би підвищував конверсійний рівень веб-ресурсу, перебуває у центрі уваги. Про це свідчать численні дослідження, присвячені цій темі (Катанова В., Попеня Н., Судун Н., Фастовець В., Шуляков В., та ін.). Останнім часом веб-дизайнери спрямовують увагу на застосування в інтерфейсі анімації та зокрема паралакс ефекту що було описано в роботах Бондарь Л., Жаденова Є., Зеленюк О., Потапенко Н., та Ясюкович Є.. Одна з найбільш авторитетних праць, що всебічно розкриває історію веб-дизайну є праця американського графічного дизайнера, мистецтвознавця Меггс Ф. «Історія графічного дизайну» [3, с. 592]. Незважаючи на наявність різнопланових і масштабних досліджень з цієї теми, сьогодні потребує цілісного й всебічного вивчення проблема застосування паралакс скролінгу у веб-дизайні.

Метою статті є аналіз застосування паралакс ефекту у веб-дизайні, та його вплив на підвищення показників конверсії веб-ресурсу.

На сьогоднішній день сучасні інформаційні технології звертають свою увагу на впровадження широкого спектру сучасних технічних засобів.

З розвитком технічних засобів, набуває розповсюдження веб-розробка, що бере свій початок з 1990-х років, саме на період

заснування інтернету. Також, паралельно з цим, розвивалась галузь веб-дизайну.

Перші норми веб-дизайну були досить примітивними. Але на сьогоднішній день веб-дизайн охоплює цілі ряди напрямів та методів. Саме технічний дизайн враховує всі важливі аспекти: функціональність, комфортність та ергономічність, він на пряму контактує з користувачем, що у свою чергу виправдовує його популярність.

Веб-дизайнери поступово задіюють нові технічні можливості, які в свою чергу дозволяють застосовувати все більш складні ефекти, з них виділяють анімаційну графіку. Це візуальним оформлення, яке оживляє статистичні об'єкти. Одним з яскравих підвидів є паралакс ефект та паралакс скролінг.

Паралакс ефектом є зміна видимого об'єкта відносно положення віддаленого фону в залежності від знаходження спостерігача. Розглянемо цей ефект детальніше.

Досліджуваний вид анімації бере початок з тригонометрії, широко застосовується в астрономії та фізиці. Для обчислення цього ефекту використовується наступна формула:

$$L = \frac{D}{2sin\alpha/2}$$

де **L** – відстань до об'єкта. **D** – базис, **α** – кут зміщення.

Також явище безперервно спостерігається в природі. Паралакс є похідним від роботи з об'ємом і перспективою, адже при русі здається, що ближчий об'єкт рухається швидше ніж той, що знаходиться на більшій відстані [2, с. 295].

Візуально, спостерігається розшарування паралакс ефекту на так звані три частини: фон, об'єкт та приближений до спостерігача шар (рис.1).

Всупереч різним перетворенням з шарами паралакс ефекту при русі об'єкт не змінює своє положення.

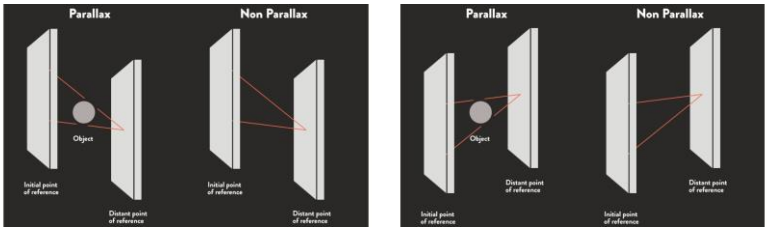

Рис. 1. Приклад паралакс ефекту

Найпростішим способом застосування паралаксу ефекту в веб-дизайні можна вважати закріплення фонового зображення на сторінці при гортанні тексту, але на сьогоднішній день такі сайти зустрічаються доволі рідко.

В свою чергу скролінгом є передання інформації, при якій вміст (текст або зображення) рухається вертикально чи горизонтально. Таким чином вміст залишається тим самим, тільки змінює своє розміщення. Деякі дизайнери використовують кілька фонових зображень для створення паралакс скролінгу [2, с. 295]. Плавне перемикання інформації чи використання скролінгу замість натискань у навігації зменшує час для завантаження, що робить даний ефект ще більш популярним. Паралакс скролінг – це 2D-ефект, при якому на сторінці декілька об’єктів переміщуються з різною швидкістю, роблячи її інтерактивною з плавними переходами від точки до точки. Цей прийом дозволяє залучити на сайт до 70 % уваги користувачів [1, с. 146].

Завдяки ефекту параллакс скролінгу веб-дизайн привертає більше уваги користувачів та є більш інтерактивним порівняно зі звичайним статичним сайтом. Якщо прокрутка сайту супроводжується візуальними ефектами, то користувач проводить більше часу на сайті, адже тривале контактування з продуктом збільшує її конверсію.

Висновки. Узагальнюючи вищезазначене робимо висновок, що параллакс ефект цікавий як для користувача так і для самого сайту.

1. Вакуленко О. В. Періоди та технологічні передумови розвитку веб-дизайну / О. В. Вакуленко // Вісник КНУКіМ. Серія: Мистецтвознавство. – 2017. – №. 36. – С. 139-149 – Режим доступу :–http://arts-series-knukim.pp.ua/article/view/157686/156985
2. Meggs P. A History of Graphic Design / P. Meggs. 3rd ed. – New York : John Wiley & Sons, Inc., 1998. – 592 pp.
3. Robbins J. N. Learning Web Design a beginners guide HTML, CSS, Javascript / J. N. Robbins [Електронний ресурс]. – Canada : Gravenstein Highway North Sebastopol, 2012. – 295с. – Режим доступу : http://wtf.tw/ref/robbins.pdf

Електронна освіта, як спосіб підвищення професійного рівня державних службовців

Зубанський Микола Костянстинович

аспірант кафедри кримінально-правових дисциплін
Львівського державного університету внутрішніх справ

Система розвитку та становлення дистанційної освіти в Україні тісно пов'язана з інформатизацією, яка на сучасному історичному етапі має стратегічне значення для нашої країни. У наш час виробництво інформаційного продукту через його високу товарну вартість є важливим чинником економічного розвитку країни. Порівняно з традиційними індустріальними методами їх застосування дає можливість забезпечити підвищення рівня матеріалізації інтелектуальної праці і якості виробів. Саме через це найбільш розвинуті країни світу отримують на міжнародних ринках значні переваги.

На відміну від зарубіжних моделей, українська дистанційна освіта більш наближена до нашого споживача і є більш демократична. Органічно поєднуючи в собі змішані технології відкритої освіти (кейс-технології, TV-технології, мережеві технології), українська дистанційна освіта стає найбільш доступна широким масам населення, роблячи можливим здобувати освіту не на все життя, а все життя. Сучасне інформаційне суспільство висуває вимоги до системи освіти, основні з яких можна сформулювати так: вміння самостійно знаходити, накопичувати і переосмислювати наукові знання; вміння студентів самостійно орієнтуватися в сучасному інформаційному суспільстві [1].

Успіх соціально-економічних та політичних перетворень в Україні багато в чому залежить від ефективної роботи органів державного управління. Висока динамічність сучасного світу, реалізація конституційних засад демократичної, правової, соціальної держави, формування громадянського суспільства обумовлюють необхідність удосконалення кадрового забезпечення державного апарату та модернізації системи підготовки, перепідготовки і підвищення кваліфікації державних службовців.

Зміни, які відбуваються у суспільстві, призводять до усвідомлення потреби у фахівцях із фундаментальною освітою, високим рівнем розвитку професійної компетентності, самостійності, здатних до саморозвитку та швидкої перекваліфікації. Особистісний та професійний розвиток і саморозвиток особистості, її професійну та соціальну мобільність, конкурентно-здатність на ринку праці забезпечують інноваційні технології у професійній освіті. Їх упровадження у систему неперервного навчання державних службовців створює умови для реалізації кар'єрного потенціалу державного службовця та спрямовує його на розробку інноваційних рішень при реалізації повноважень державної служби. Значний потенціал для підвищення ефективності професійної освіти та забезпечення формування професійних якостей, які відповідають вимогам сьогодення, надає дистанційне навчання, що базується на широкому використанні сучасних інформаційних технологій [2, с. 189].

Стратегічним курсом політики уряду України передбачено необхідність модернізації існуючої системи державного управління, здійснення суттєвих інституційних змін, гармонізації національного законодавства з європейським, адаптації процесів управління публічними інституціями до сучасних європейських реалій. Зазначене актуалізує потребу у висококваліфікованих управлінських кадрах, здатних ефективно працювати на користь держави та реалізовувати системні зміни для забезпечення її конкурентоспроможності у світі. У цьому контексті особливого значення набувають процеси розроблення стратегій та програм розвитку освіти в цій сфері, запровадження до навчального процесу інноваційних освітніх технологій, реалізація науково-практичних та навчально-методичних комунікаційних заходів [3, с. 95].

Електронна чи як її подекуди називають дистанційна система професійної підготовки для державних службовців є достатньо комплексною, проте, з огляду на знану чисельність держслужбовців, навантаження на цю систему є надто високим, а якість навчання не завжди відповідає сучасним реаліям. Сучасний стан професійного навчання державних службовців має інформаційний або академічний характер і меншою мірою характеризується

динамічністю та практичною цілеспрямованістю щодо здобуття певних навичок, необхідних для виконання службових обов'язків.

Освіта є основою інтелектуального, духовного, культурного, економічного, соціального розвитку суспільства і держави. Вона спрямована на всебічний розвиток людини яка є особистістю та найвищою цінності суспільства, виховання високих моральних якостей, розвиток її талантів і фізичних здібностей, формування громадян, які мають здатність до свідомого суспільного вибору, збагачення на цій основі інтелектуального, культурного, творчого потенціалу народу, підвищення рівня освіченості народу, забезпечення усіх сфер діяльності кваліфікованими фахівцями. Сучасний рівень розвитку наукових досліджень у галузі державної служби сприяє забезпеченню постійної, послідовної, кваліфікованої освіти державних службовців та посадових осіб місцевого самоврядування, яка визначається Постановою Кабінету Міністрів України «Про затвердження Положення про систему підготовки, перепідготовки та підвищення кваліфікації державних службовців і посадових осіб місцевого самоврядування» [4].

У державотворчому процесі освіта управлінських кадрів упродовж життя забезпечує стабільність розвитку суспільного виробництва, є засобом розширеного відтворення його інтелектуального, духовного й культурного потенціалу, а тому має стати пріоритетом соціальної державної політики.

Професійне становлення і розвиток державних службовців у системі безперервної професійної освіти можна розглядати як багатогранний феномен, основні характеристики якого відповідають цілісній, динамічній та відкритій системі, найважливішими атрибутами якої є належна структура, мета й завдання, зміст, методи і форми діяльності [5, с.14].

Найперше це зумовлено унікальним місцем і роллю освіти в житті кожного державного службовця. Проте досить часто ми зустрічаємося з нерозумінням ролі і значення безперервної освіти державних службовців, яке пов'язане головним чином з почасти

спрощеним, примітивним розумінням суті освіти як складника соціального, духовно перетворювального явища взагалі.

Розглянемо одне з визначень «освіта», яке є найбільш оптимальним і точним: це певне надбання особистості, що проявляється у її поведінці. Звідси мінімум кілька принципово важливих висновків для продовження розгляду проблеми, власне пошуку інноваційної моделі безперервної освіти державних службовців у контексті навчання впродовж життя:

- освіта належить головним чином до індивідуальної, спеціальної культури людини і перебуває в психіці суб'єкта (особистості);
- освіта формується у процесі навчання, пізнання світу, набуття людиною власного життєвого досвіду, соціальної практики;
- освіта – безперервний процес, що залежить від стану середовища, в якому відбувається розвиток людини, і від індивідуальної творчості людини [6, с. 213-214].

Освіта державних службовців в сучасному світі має бути максимально індивідуалізованою; будуватися на найкращих освітніх технологіях; бути в безперервному розвитку. Серед основних характеристик безперервної освіти державних службовців, можна визначити такі: масовий, всеохоплюючий характер освіти. Тобто освіта перестає бути певною мірою елітарною сферою, предметом небагатьох – еліти. Освіта стає предметом більшості, передусім дорослого населення тих країн, які гостро відчувають необхідність переходу від індустріальних та постіндустріальних суспільств до суспільств інформаційних [7, с. 99-100].

Неперервна освіта державних службовців включає їхню підготовку, перепідготовку, підвищення кваліфікації та професіоналізму з метою задоволення потреби центральних та місцевих органів виконавчої влади, органів місцевого самоврядування, інших органів і організацій у високопрофесійних та висококультурних працівниках, здатних компетентно і відповідально виконувати управлінські функції, впроваджувати новітні соціальні технології, сприяти інноваційним процесам.

Дистанційна технологія навчання базується на принципах відкритого навчання, широко використовує сучасні інформаційні технології та телекомунікації з метою доставки навчального матеріалу та спілкування, у тому числі, в реальному часі та є педагогічним процесом, який направлений на розвиток дидактичних цілей навчання, реалізований у певній послідовності, під опосередкованим управлінням викладача на відстані [8, с. 34].

Аналіз теорії та практики застосування дистанційних технологій у навчальному процесі дозволив виявити їх найбільш привабливі особливості: гнучкість, модульність, паралельність, асинхронність, нова роль викладача, нові функції студента, спеціалізований контроль якості освіти, використання спеціалізованих інноваційних технологій та засобів навчання.

Останнім часом отримав розповсюдження термін «електронне навчання», який означає процес дистанційного навчання в електронній формі через мережу Інтернет із використанням освітніх інформаційних технологій на базі систем управління навчанням. «Електронне навчання» на сьогодні є розширенням поняття «дистанційне навчання» та означає різні форми та способи навчання на основі сучасних інформаційних технологій та мережі Інтернет. Упровадження сучасних дистанційних технологій в освітню систему традиційного професійного навчання доповнює, удосконалює, розвиває її за рахунок створення мобільного інформаційно-освітнього середовища, на базі яких для вивчення окремих навчальних дисциплін створюються дистанційні курси з навчальними матеріалами для мережевого навчання [7, с. 278].

Упровадження у професійну підготовку державних службовців дистанційних технологій обумовлене такими перевагами у порівняні з традиційним навчанням, як наочність, наявність оперативного зв’язку, можливість індивідуального підходу, можливість здійснювати навчання на своєму робочому місці, можливість організації групових форм навчання розподілено у просторі та часі з використанням навчального інформаційного середовища. Використання дистанційних технологій дозволяє опосередковано керувати самостійною підготовкою студентів,

використовуючи для цього засоби телекомунікацій та Інтернету, та закладає основи для реалізації принципу «навчатися все життя» у подальшій професійній діяльності державного службовця. У разі використання як бази для реалізації дистанційних технологій навчання інформаційних систем, які мають розвинені мережеві засоби комунікацій, з'являється можливість оптимізувати та частково автоматизувати процеси вивчення нового матеріалу, формування професійних умінь та навичок, передачі результатів та оцінювання самостійної роботи студентів [9].

Розвиток інноваційної освіти державних службовців та посадових осіб місцевого самоврядування передбачає розвиток наступник складових, що обумовлюють її функціонування у сучасному суспільстві: – створенням сприятливих, творчих умов у сфері освіти державних службовців з метою генерації та культивування інноваційного процесу, що обумовлюються політичними і економічними процесами у суспільстві; – забезпеченням матеріальних можливостей педагогічних інновацій, обумовленим економічною політикою держави; – формування особистості, що володіє інноваційної здатністю аналізувати, прогнозувати і моделювати професійний результат своєї діяльності, а також планувати впровадження інновацій у професійну діяльність; – створенням інноваційної системи навчання, що складається з, інноваційного процесу навчання та спирається на інноваційну концепцію професіоналізації державного управління та розвитку громадянського суспільства; – включенням в інноваційну систему освіти інноваційної системи виховання, яка передбачає формування духовної та моральної особистості.

Сучасна система підготовки та підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядуванням знаходиться на переломному методологічному і технологічному етапі свого розвитку і її головним завданням має стати формування «нового управлінця» – професійного, високоморального та здатного до інноваційного мислення [10, с. 69-70].

Отже, з вищенаведеного можна зробити висновок, що електронне навчання державних службовців є важливим елементом проходження служби. Варто підкреслити, що електронне

навчання серед інших традиційних видів навчання має ряд позитивних рис серед них можна виділити такі, як наочність, наявність оперативного зв'язку, можливість індивідуального підходу, можливість здійснювати навчання на своєму робочому місці тощо. Також новітні інноваційні технології професійного навчання державних службовців сприяють по-перше: розвитку їх критичного мислення та підвищення ефективності діяльності, по-друге: виконують важливу роль у здійсненні навчання впродовж роботи у сфері державної служби. В умовах глобалізації теперішнього суспільства для забезпечення безперервного навчання державних службовців серед інноваційних технологій слід застосовувати технології критичного мислення (наприклад ігровим технологіям, методам стимулювання творчої активності тощо) та електронному навчанню на основі смарт-технологій.

1. Про систему дистанційного навчання «Віртуальний Університет». URL: http://vu.net.ua.
2. Коваль Т. І., Сисоєва С. О., Сущенко Л. П. Підготовка викладачів вищої школи: інформаційні технології у педагогічній діяльності: навч.-метод. посіб. К.: Вид. центр КНЛУ, 2009. 380 с.
3. Шуневич Б. Обґрунтування наукової термінології з дистанційного навчання. Б. Шуневич. Проблеми української термінології : Вісник. – Львів: Нац. ун-т «Львів. політехніка». 2003. № 490. С. 95-104.
4. Про затвердження положень про прийом, стажування в органах державної влади і органах місцевого самоврядування слухачів, працевлаштування випускників Національної академії державного управління при Президентові України, а також переліку органів державної влади, органів місцевого самоврядування, в яких проводиться у 2013–2018 роках стажування слухачів Національної академії : постанова Кабінету Міністрів України від 01.04.2013 № 255. URL: http://zakon4.rada.gov.ua/ laws/main.
5. Леліков Г. Організаційно-правове удосконалення державної служби. Г. Леліков. Вісник УАДУ. 1999. № 4. С. 13-19.

6. Фоменко Н. А. Правова педагогіка. Н. А. Фоменко, М. І. Скрипник, О. В. Фатхутдінова. Херсон: Олді-плюс, 2015. 326 с.
7. Полат Е. С. Теория и практика дистанционногообучения: учеб. пособие для студ. высш. пед. учеб. заведений. Е. С. Полат, М. Ю. Бухаркина, М. В. Моисеева; под. ред. Е. С. Полат. М. : Академия, 2004. 416 с.
8. Луговий В. Організаційно-правове забезпечення заочно-дистанційної форми навчання в Національній академії державного управління при Президентові України. В. Луговий, В. Куценко, С. Калашнікова. Вісник Академії дистанційної освіти. 2003. № 1. С. 34-37.
9. Болюбаш Н. М. Фактори та умови формування професійної компетентності майбутніх економістів засобами інформаційного середовища Moodle. Н. М. Болюбаш. Інформаційні технології і засоби навчання.2010. № 3 (17). URL: http://www.ime.eduua.net/em17/emg.html.
10. Дегтярьова Л. М. Роль наочності в процесі дистанційного навчання. Л. М. Дегтярьова, А. О. Дегтярьова. Вісник СНУ ім. В. Даля. Луганськ, 2008. № 9 (127). С. 69-71.

Електронне навчання в системі професійної підготовки державних службовців МВС України

Ковалів Мирослав Володимирович

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

Шимечко Іван Богданович

здобувач вищої освіти центру післядипломної освіти,
заочного та дистанційного навчання
Львівського державного університету внутрішніх справ

Інформатизація освіти – частина інформатизації суспільства, процесу, який набув рис інформаційної революції, що дає підставу характеризувати сучасне суспільство як інформаційне. Конкурентні переваги сучасних високорозвинених країн, що пов'язані з можливістю розвитку людського потенціалу, більшою мірою визначаються станом системи освіти.

Проаналізувавши чинне законодавство у сфері використання інформаційно-комунікаційних технологій в освіті, доцільно розробити пропозиції та доповнення до освітнього законодавства, які стосуються визначення предмета та змісту вимог експертизи з боку Національного агентства із забезпечення якості вищої освіти, що висуваються до освітніх установ, які реалізують дистанційні освітні технології [1]. Зокрема, актуальним є:

- пропозиції про нормативне закріплення на відомчому рівні дистанційної форми професійної підготовки державних службовців;
- визначення у національному освітньому законодавстві статусу, функцій і повноважень представництв відомчих вузів відповідно до діючих норм Цивільного кодексу України й освітньої практики вишів;
- виокремлення особливого типу філій освітніх установ системи МВС України, що реалізують основні і додаткові

професійні освітні програми з використанням дистанційних освітніх технологій;

- уточнення і зміни низки галузевих нормативних документів, що регламентують і забезпечують ефективне використання освітніми установами дистанційних освітніх технологій для забезпечення підвищення якості освітньої діяльності у розподілених мережах структурних підрозділів МВС України та підпорядкованих організацій на регіональному рівні.

Створення нормативного правового простору, що визначає взаємини учасників освітнього процесу в умовах функціонування різних інформаційних освітніх систем, є одним із найважливіших напрямів діяльності державних органів, зокрема Міністерства освіти та науки України та МВС України.

Цілком природно, що питання застосування освітніх технологій на різних рівнях розвитку освітніх процесів регламентуються системою нормативних правових актів. Не випадково, що Законом України «Про вищу освіту» передбачає встановлення порядку розробки та використання дистанційних освітніх технологій [2].

Доцільно запропонувати рекомендацій щодо гармонізації нормативної бази в галузі дистанційних освітніх технологій. Рекомендації щодо вдосконалення основ правового регулювання освіти із застосуванням дистанційних освітніх технологій у системі професійної підготовки державних службовців МВС України повинні охоплювати:

- аналіз локальних нормативних актів, що регламентують процес впровадження та використання дистанційних технологій навчання в освітньому процесі вищих навчальних закладів, які спеціалізуються на підготовці державних службовців;
- аналіз напрацьованої практики впровадження технологій дистанційного навчання в освітній процес.

Розробка рекомендацій щодо реформування правової системи професійної підготовки сфери державної служби буде

спрямована на забезпечення її розвитку відповідно до сучасних темпів реформування системи МВС України.

Використання дистанційних освітніх технологій загалом не регламентується, за винятком визначення поняття «дистанційні освітні технології» у базових законах України, що регламентують освітню діяльність. Порядок використання дистанційних освітніх технологій також не дає відповіді на більшість виникаючих питань.

При впровадженні дистанційних освітніх технологій в освітній процес необхідне створення чіткої нормативно-правової моделі відомчої освітньої установи. Передбачувана законодавством діяльність має ґрунтуватися на принципі випереджаючого розвитку нормативно-правової бази. Вкрай важливо не допустити ситуації, коли недостатнє законодавче забезпечення гальмувало б упровадження нових освітніх технологій.

Попри те, що електронне навчання впроваджується в національну практику без сформованої нормативно-правової бази, ігнорування необхідності опрацювання законодавчої бази призводить до уповільнення практичного впровадження електронного навчання. Підготовка фахівців залежить від форм і методів навчання. У країнах Європейського Союзу застосовується модель навчання державних службовців, яку можна назвати розподіленою. Розподілене навчання використовує безліч технологій навчання, зокрема інформаційно-телекомунікаційну мережу Інтернет і дистанційне навчання.

Сьогодні актуальними є питання щодо оплати праці викладачів, які використовують дистанційні технології навчання, співвідношення дистанційних і лекційних годин (їх рівнозначність в освітньому процесі), електронної та очної (стаціонарної) частин освітніх програм.

Беручи до уваги Рекомендації парламентських слухань «Законодавче забезпечення розвитку інформаційного суспільства в Україні» найважливішими принципами вдосконалення нормативно-правовий бази України повинні стати:

- пріоритет інтересів державних службовців в отриманні якісної доступної освіти будь-якого рівня, результати якого матимуть для них практичну цінність;
- пріоритет адаптації відомчого нормативно-правового законодавства МВС України до вимог Європейського Союзу, за безумовного паритету інтересів і взаємної вигоди від встановлення відносин у сфері освіти тих держав, що входять до єдиного (загального) освітнього простору державної служби Європейського Союзу;
- дотримання міжнародних домовленостей і угод, зокрема взаємної зацікавленості у формуванні єдиного (загального) освітнього простору у межах поліцейської освіти;
- системність у вдосконаленні та гармонізації нормативно-правових актів;
- мінімізація норм, регульованих органами управління освіти України;
- дотримання міжнародних стандартів і тенденцій [3].

Отримання освіти будь-якого рівня за допомогою електронного навчання не обумовлено у правових нормах. З одного боку, це не забороняє використання електронного навчання, з іншого – не дає змоги враховувати специфіку електронного навчання, а також не стимулює його розвиток. Водночас до різнопланового навчання на основі електронного реалізується підхід, ідентичний традиційним способам здобуття освіти. Відтак виникають серйозні непорозуміння та конфліктні ситуації.

Другий аспект полягає в ідентифікації статусу електронного навчання в системі освіти держави. У чинному законодавстві України йдеться лише про дистанційні освітні технології, які застосовуються у рамках традиційних форм навчання. Водночас можна говорити про існування нової форми отримання освіти – дистанційної. Отже, доцільно законодавчо закріпити поняття електронного навчання як особливої форми здобуття освіти. Водночас слід зауважити на тому, що введення нової форми отримання освіти потребує ґрунтовної корекції цілої низки правових норм.

1. Про затвердження Статуту Національного агентства із забезпечення якості вищої освіти : Постанова Кабінету Міністрів України від 15.04.2015 № 244 URL. http: www.kmu.gov.ua/document/.../P0244.doc
2. Про вищу освіту : Закон України від 01.07.2014 № 1556-VII. Відомості Верховної Ради. 2014. № 37–38. Ст. 2004.
3. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : Постанова Верховної Ради України від 03.07.2014. Відомості Верховної Ради. 2014. № 33. Ст. 1163.

Особливості використання вебінарів у дистанційній освіті

Миронов Юрій Богданович

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

Сватюк Оксана Робертівна

доцент кафедри менеджменту та суспільно-гуманітарних дисциплін Львівського навчально-наукового інституту ДВНЗ «Університет банківської справи», кандидат економічних наук, доцент

Миронова Мар'яна Ігорівна

доцент кафедри міжнародних економічних відносин Львівського торговельно-економічного університету, кандидат економічних наук

Постійний розвиток інформаційних технологій, їх удосконалення, перехід на рівень віртуальних комунікацій неминуче ведуть до змін інформаційного освітнього середовища закладу вищої освіти. На сьогодні широкого поширення в освітній сфері отримало дистанційне навчання як одна з перспективних технологій навчання. Форми організації дистанційних навчальних заходів численні та різноманітні – це і навчальні програмні продукти, і віртуальні заняття в режимі онлайн, а також вебінари, які можуть проходити у формі семінарів, дискусій, конференцій.

Вебінари (від англ. *webinar* – *web-based seminar*, що перекладається як «семінар, організований на базі веб-технологій») – це онлайн семінари, організовані через мережу Інтернет у режимі реального часу [2, с. 106].

Такий формат заходу як вебінар має вагомі переваги для організації самостійної роботи студентів. Істотними перевагами вебінарів є мінімальні витрати на їх підготовку, низька собівартість, можливість залучення великої кількості слухачів,

значна економія часу. Для участі у вебінарі не потрібно нікуди їхати, не потрібно дбати про велике приміщення для проведення заходу. Це дозволяє дуже істотно скоротити витрати. Від студентів не вимагається зайвих зусиль, не пов'язаних з самим процесом навчання. Вебінар дозволяє студентам здобувати необхідні знання, перебуваючи біля персонального комп'ютера чи навіть смартфону в комфортному для навчання середовищі.

У процесі вебінару як виду заняття викладач і кожен студент повинні бути забезпечені індивідуальними обладнанням (персональним комп'ютером або смартфоном з мікрофоном і відеокамерою), використовується необхідний дидактичний матеріал (презентації, відеоматеріали, таблиці, схеми), для здійснення контролю застосовуються опитування, чат, тестування та ін.

Використання аудіовізуальних матеріалів забезпечує високий рівень запам'ятовування, не виключаючи різноманітності видів діяльності, а також дозволяє повною мірою забезпечити зворотний зв'язок з викладачем. З іншого боку, завдяки застосуванню високотехнологічної апаратури кожен слухач має можливість спілкуватися з викладачем онлайн, задавати йому питання, але при цьому не відчувати психологічних бар'єрів, пов'язаних з дискомфортом спілкування на публіці. Подоланню психологічного бар'єру сприятимуть диференційований підхід і орієнтація на індивідуальне навчання.

Вебінар, володіючи основними характеристиками традиційного семінару, є його більш складною формою. Це пов'язано з безперервним аудіовізуальним контактом слухача і викладача. Викладач перебуває у віртуальному просторі щодо студентів, тому аудіоінформація сприймається простіше. Можна повною мірою використовувати засоби невербального спілкування: міміку, жести, артикуляцію.

Важливою перевагою вебінару є те, що вебінар можна записати і згодом використовувати для повторного перегляду, формування бібліотеки вебінарів, самоаналізу викладачем змісту, стилю і техніки мови вебінару. Відеозаписи вебінару важливі для слухачів, яким потрібно більше часу для аналізу отриманої інформації, більш глибокого її засвоєння. Таким чином, саме

орієнтація на індивідуальні особливості кожного студента дозволяє ефективно використовувати вебінар при організації самостійної роботи студентів.

При організації самостійної роботи студентів закладів вищої освіти вебінари дозволяють студентам більш якісно засвоювати теоретичний матеріал навчальної дисципліни, отримувати консультації викладачів, чути думки інших учасників курсу, формувати свої загальнокультурні та професійні компетенції. Викладачам вебінари дозволяють забезпечити науково-педагогічну та методичну підтримку самостійної роботи студентів [1, с. 33].

Підготовка вебінарів схожа з організацією очних заходів із урахуванням специфіки Інтернет-технологій. Організаторам необхідно:

- визначитися з тематикою і датою заходу, поінформувати про це потенційних учасників;
- визначитися з видом вебінару: відкритий (доступний кожному, хто приєднався) або закритий (доступ тільки за попередньою реєстрацією, паролем – використовується, наприклад, при організації платних або корпоративних вебінарів);
- визначити формат вебінару за кількістю лекторів. Камі Гріффітс та Кріс Петерс у статті «10 кроків планування успішного вебінару» [3] наводять такі варіанти (табл. 1):

Таблиця 1

Переваги та недоліки різних форматів вебінару

Формат вебінару	Переваги	Недоліки
Один ведучий, який представляє матеріал, і відповідає на питання	Потрібно координувати і навчати інструментів вебінару меншу кількість людей	Може виникнути ефект більшої дистанції з аудиторією, через що деякі з слухачів можуть відмовитися задавати питання

У стилі інтерв'ю – лектору задається серія питань від інтерв'юера	Інтерв'юер «заохочує» аудиторію наслідувати його приклад і задавати питання лектору	Потрібно координувати і навчати інструментів вебінару більшу кількість людей. Планування вебінару стає складнішим
Модерована панельна дискусія	Багато учасників і точок зору, що цікаво для аудиторії	Потрібно координувати і навчати інструментів вебінару більшу кількість людей. Виникають труднощі з тим, що багато дискутантів говорять одночасно
Інтерактивний вебінар	Аудиторія бере участь в ході вебінару. При успішній реалізації учасники отримують краще розуміння про предмет вебінару	Проведення можливо в невеликій групі і при досвідченому організаторі (модераторі)

Побудовано за матеріалами [3].

Також можливий наступний формат: у вебінарі беруть участь 2-3 лектори, які доповідають почергово та після цього спільно коментують запитання слухачів. У будь-якому випадку розуміння формату вебінару дає можливість подальшого планування виходячи як з технічних, так і кадрових ресурсів.

Організатори вебінару заздалегідь визначають програмну платформу для проведення вебінару. При виборі необхідно орієнтуватися на наступні параметри:

- чи є вебінар окремим заходом чи компонентом великого дистанційного курсу;
- передбачувана кількість учасників вебінару;
- частота проведення вебінарів;
- можливості, пропоновані сервісом (онлайн інструменти реєстраційних форм та опитувань, підтримуване програмне забезпечення, можливість інтеграції з сайтом організатора, запис вебінару, відгуки і т. д.) [2, с. 108].

Таким чином, вебінари – це формат заходів, що володіє вагомими перевагами, особливо для організації самостійної роботи студентів. Використання аудіовізуальних матеріалів забезпечує високий рівень запам'ятовування, не виключаючи різноманітності видів діяльності, а також дозволяє забезпечити зворотний зв'язок з викладачем. Завдяки застосуванню високотехнологічної апаратури кожен слухач має можливість спілкуватися з викладачем онлайн, задавати питання, при цьому не відчуваючи психологічного бар'єру, пов'язаного з дискомфортом спілкування на публіці. Вебінар надає потужні можливості для організації самостійної роботи студентів, дозволяє працювати над вдосконаленням загальноосвітніх та фахових компетентностей. Викладачі мають можливість працювати зі студентами, ділитися досвідом і знаннями, перебуваючи у будь-якій точці земної кулі.

1. Ваганова О. И. Вебинар как средство организации самостоятельной работы студентов в условиях дистанционного обучения / О. И. Ваганова, М. Н. Гладкова, А. В. Гладков, М. О. Сундеева, М. А. Татаренко // Азимут научных исследований: педагогика и психология. – 2016. – № 2 (15). – С. 31-34.
2. Иванова Е. Б. Организация дистанционного обучения в формате вебинаров (рекомендации по проведению вебинара от и до) / Е. Б. Иванова // Управление образованием: теория и практика. – 2012. – № 3 (7). – С. 106-113.
3. Griffiths K. 10 Steps for Planning a Successful Webinar / K. Griffiths, C. Peters [Electronic Resource]. – Access Mode : https://www.socialbrite.org/2010/08/09/10-steps-for-planning-a-successful-webinar/.

Модель професійної підготовки фахівців з кримінального аналізу для підрозділів Національної поліції України

Мовчан Анатолій Васильович

професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
доктор юридичних наук, професор

Модель професійної підготовки фахівців з кримінального аналізу відображає комплекс взаємопов'язаних компонентів (мотиваційного, когнітивного, організаційно-методичного і професійно-діяльнісного) та передбачає поетапне формування готовності майбутніх кримінальних аналітиків до професійної діяльності впродовж усіх етапів їхньої професійної підготовки.

Аналіз наукових досліджень розробок моделей професійної підготовки фахівців дає підстави стверджувати, що найбільш перспективною для використання є неіституційна модель освіти. Зазначена модель може поєднувати в собі технологічний процес та закордонний досвід в області системи освіти. Така модель може поєднати освітні об'єкти та суб'єкти освітнього процесу в умовах єдиного освітнього середовища незалежно від місця розташування.

З метою вдосконалення системи професійної підготовки кримінальних аналітиків для підрозділів Національної поліції України нами розроблено та обґрунтовано модель професійної підготовки фахівців з кримінального аналізу, яка складається з цільового, змістовного, навчально-технологічного, процесуального та діагностично-результативного компонентів.

Цільовий компонент відповідає завданням і потребам закладів вищої освіти МВС України щодо професійної підготовки кримінальних аналітиків. Метою даної моделі є професійна підготовка фахівців з кримінального аналізу для підрозділів Національної поліції України.

Суб'єктами професійної підготовки фахівців з кримінального аналізу є:

- науково-педагогічні працівники;
- слухачі центрів первинної професійної підготовки «Академія поліції», слухачі курсів підвищення кваліфікації та курсанти закладів вищої освіти МВС;
- практичні працівники аналітичних підрозділів кримінальної поліції, які залучаються до освітнього процесу на освітньо-професійних та навчальних програмах;
- інші працівники закладів вищої освіти МВС України.

Завдання запропонованої моделі професійної підготовки полягає в досягненні готовності майбутнього фахівця з кримінального аналізу до роботи в аналітичних підрозділах Національної поліції України.

Змістовний компонент складається зі змісту професійної підготовки фахівців з кримінального аналізу, який визначається:

- Національною рамкою кваліфікацій;
- стандартами вищої та професійної (професійно-технічної) освіти;
- освітньо-професійними програмами;
- робочими навчальними програмами;
- навчальними планами;
- планами практичних, семінарських та лабораторних занять;
- програмами проходження практики.

Професійна підготовка майбутніх фахівців з кримінального аналізу базується на принципах системності, науковості, практичної орієнтованості, технологічності, інноваційності. Ці принципи є провідними дидактичними положеннями сучасної педагогічної теорії та практики, їх використовують для організації освітнього процесу в закладах вищої освіти.

Принципи навчання – це система дидактичних вимог, дотримуючись яких можна забезпечити ефективне функціонування

освітнього процесу. Принципи навчання опираються на виявлені наукові закономірності і кращий досвід педагогічної діяльності.

Принцип системності – один із класичних принципів навчання, який характеризується системним плануванням, організацією виконання й оцінки процесу навчання відповідно до поставлених цілей, застосуванням людських і технологічних ресурсів для того, щоб підвищити ефективність навчання.

Принцип системності є базовим при розробці електронних навчальних посібників та дистанційних курсів, які набувають все більшого практичного застосування у професійній підготовці майбутніх фахівців з кримінального аналізу.

Принцип практичної орієнтованості (принцип зв'язку теорії з практикою) теоретичну основу бере з практико-орієнтованого підходу, який передбачає поєднання методів викладання та навчання з практичною діяльністю. Ми вважаємо, що зазначений принцип має сприяти формуванню професійного досвіду слухача (курсанта) щодо його входження у професійне середовище в процесі проходження різних видів практик та виконання практично-лабораторних завдань. Принцип практичної орієнтованості лежить в основі багатьох професійно-орієнтованих технологій навчання, до яких слід віднести технологію дистанційного навчання, кейс-технологію (case-study), інтерактивні технології, технологію «портфоліо» тощо.

Принцип науковості – провідний принцип організації освітнього процесу, що передбачає розкриття причинно-наслідкових зв'язків явищ, процесів, подій, включення в засоби навчання науково перевірених знань, які відповідають сучасному рівню розвитку науки. Зазначений принцип реалізується через зміст навчального матеріалу, обумовленого нормативними документами та навчально-методичною літературою.

Принцип науковості виступає провідним у такому контексті, як:

- необхідність та важливість ознайомлення слухачів (курсантів) з новими досягненнями з метою демонстрування перспектив розвитку науки загалом;

- показ та об’єктивний аналіз наукових фактів, понять, теорій;
- засіб коригування самостійно отриманих знань;
- реальний приклад пояснення значення теоретичних знань для розвитку практичних напрямів дослідження.

Принцип технологічності належить до інноваційних принципів навчання, поява якого зумовлена інтенсивним розвитком освітніх технологій, їх активним впровадженням у мережу освітніх інституцій, професійну підготовку майбутніх фахівців.

Головна мета інноваційної освіти − збереження і розвиток творчого потенціалу людини. Проте сьогодні освіта має бути пронизана загальнолюдськими цінностями. Для цього вона повинна розвивати гармонійне мислення, побудоване на поєднанні внутрішньої свободи особистості і її соціальної відповідальності, а також терпимості до інакомислення.

Принцип інноваційності виявляється у варіативності, динамічності змісту, форм, методів і технологій підготовки фахівців до професійної діяльності. Інноваційний характер освіти формує світогляд фахівців, в основі якого лежить здатність і можливість творчого перетворення соціальної дійсності, проектування, організації та здійснення професійної діяльності, що припускає варіативність розв’язання задач, визначає доцільність різних критеріїв контролю та оцінки досягнутих результатів.

Навчально-технологічний компонент складається з матеріально-технічного і програмно-технологічного забезпечення підготовки фахівців з кримінального аналізу.

Підготовка кримінальних аналітиків передбачає використання, зокрема:

- хмарно-орієнтованої інфраструктури: захищеної локальної мережі, Інтернет, Wi-Fi; серверів з технологіями віртуалізації та кластеризації; баз даних; комп’ютерних лабораторій;
- програмно-технологічного забезпечення: аналітичного програмного забезпечення (i2 Analyst’s Notebook,

ArcGIS, ANACAPA, E-Gis maps тощо); програмного забезпечення управління даними (MEMEX); автоматизованих інформаційно-пошукових систем МВС та Національної поліції; середовища програмування, геоінформаційного моніторингу, управління базами.

Реалізація всіх складових моделі професійної підготовки фахівців з кримінального аналізу передбачає виконання сукупності педагогічних умов, зокрема:

- змістовно-методичних: конструювання змісту теоретичного матеріалу для навчальних дисциплін спеціалізації «Кримінальний аналіз»;
- суб'єктних: формування ціннісно-мотиваційної сфери майбутніх фахівців з кримінального аналізу;
- технологічних: організації процесу професійної підготовки майбутніх фахівців з кримінального аналізу для аналітичних підрозділів Національної поліції України.

Процесуальний компонент охоплює форми організації навчання, засоби, методи, методики, технології викладання навчальних дисциплін спеціалізації «Кримінальний аналіз», серед яких: «Кримінальний аналіз», «Інформаційні технології», «Комп'ютерні мережі та телекомунікаційні технології», «Інформаційна безпека», «Основи програмування», «Особливості розкриття кіберзлочинів», «Інформаційно-аналітична робота в оперативно-розшуковій діяльності» тощо.

Зокрема, у межах дисципліни «Кримінальний аналіз» вивчають: загальну концепцію поліцейської діяльності, керованої аналітикою; концепти оперативного, тактичного, стратегічного аналізу; аналітичні інструменти для проведення аналізу даних з відкритих джерел, ризик-аналізу, складання карт злочинності з використанням інструментів геоінформаційних систем / GIS, концентрації злочинності, графіків і схем зв'язків тощо.

Головним завданням дисципліни «Комп'ютерні мережі та телекомунікаційні технології» є розгляд принципів будови комп'ютерних мереж; отримання знань про їх види, системну архітектуру; ознайомлення з їх топологіями, протоколами

передачі даних; отримання уявлення про безпровідні комп'ютерні мережі.

У дисципліні «Основи програмування» розглядаються сучасні мови програмування в середовищі HTML; серверна мова PHP; мова роботи з базами даних MYSQL; основи мови Java-Scrspt тощо.

У межах дисципліни «Інформаційна безпека» вивчаються правові та організаційно-технічні засади захисту інформації, апаратні і програмні засоби захисту інформації в інформаційно-телекомунікаційних системах тощо.

Професійну підготовку фахівців з кримінального аналізу здійснюють у таких формах: лекції, семінарські та практичні заняття, індивідуальна та самостійна робота, практична підготовка; освітній процес поєднує як традиційні, так і інформаційні технології навчання.

У ході професійної підготовки кримінальних аналітиків використовуються такі методи навчання:

- традиційні (організація й здійснення навчально-пізнавальної діяльності; стимулювання мотивації навчальної діяльності; контроль, аналіз і оцінювання результатів навчання);
- інноваційні (проблемне навчання, мультимедійні лекції, ділові ігри, тренінги, презентації, практико-орієнтована діяльність).

Заслуговують на увагу окремі з них, зокрема, навчальне проєктування, зокрема, практико-орієнтовані та дослідницькі проєкти.

Практико-орієнтовані проєкти передбачають, що результат діяльності учасників чітко визначено з самого початку, він орієнтований на соціальні інтереси учасників (документ, програма, рекомендації, проєкт закону, словник, проєкт профілактичних заходів тощо). Проєкт потребує складання та узгодження послідовності (у вигляді чітко спланованих дій та заходів) всієї діяльності його учасників з визначенням функцій кожного з них.

Особливо важливими є чітко координована організація роботи у вигляді поетапних обговорень та презентація одержаних результатів, а також демонстрування можливих засобів їх упровадження в практику.

Окремим напрямом проєктної технології є дослідницькі проєкти, які потребують чітко продуманої та логічно обміркованої структури, визначеної соціальної значущості мети, актуальності предмета дослідження для всіх учасників, продуманості методів (сюди варто віднести також експериментальні методи обробки результатів).

Означені проєкти повинні повністю підпорядковуватися логіці дослідження і мати відповідну структуру: визначення теми дослідження, аргументація її актуальності, обґрунтування предмета й об'єкта, завдань і методів, визначення методології дослідження, висування гіпотез розв'язання проблеми і орієнтованих шляхів її розв'язання.

Діагностично-результативний компонент передбачає розроблення методики вимірювання рівнів сформованості загальних і спеціальних компетентностей у процесі професійної підготовки кримінального аналітика та визначення якісної характеристики рівнів професійної підготовки майбутніх фахівців з кримінального аналізу.

Пропонується професійну підготовку фахівців з кримінального аналізу здійснювати на основі переліку компетентностей, які дають можливість кримінальному аналітику виконувати посадові обов'язки як у підрозділах кримінального аналізу, так і в аналітичних підрозділах Національної поліції України, зокрема:

- загальнопрофесійні компетентності;
- ключові компетентності;
- професійні компетентності поліцейського;
- фахові компетентності кримінального аналітика.

Результатом моделі є готовність майбутнього фахівця з кримінального аналізу до практичної діяльності в аналітичних підрозділах Національної поліції України.

Інформаційні технології в освіті

Рейдало Таїса Миколаївна

ад'юнкт Дніпропетровського державного університету внутрішніх справ України

Мирошниченко Володимир Олексійович

професор Дніпропетровського державного університету внутрішніх справ України, кандидат технічних наук, доцент

На сьогоднішній день спостерігається тенденція зростання ролі інформаційних технологій в житті людини. Сучасне суспільство повністю увійшло в процес, який прийнято називати інформатизацією. Такий процес передбачає наявність доступності будь-якої людини до різних джерел інформації, проникнення інформаційних технологій в наукову, виробничу і громадську сфери, високого рівня інформаційного обслуговування. Разом з тим, процес інформатизації тісно пов'язаний з прискоренням науково-технічного прогресу, інтелектуалізацією будь-якого виду людської діяльності, й появою якісно нового інформаційного середовища соціуму, яке дозволяє забезпечувати розвиток творчого потенціалу індивіда.

Серед пріоритетних напрямків процесу інформатизації суспільства виділяється інформатизація освіти, яка полягає в наявності системи методів, процесів та програмно-технічних засобів, інтегрованих для збору, обробки, зберігання, поширення й застосування інформації з метою її споживачів. Іншими словами, основна мета інформатизації полягає в глобальній інтенсифікації інтелектуальної діяльності за допомогою застосування нових інформаційних технологій (комп'ютерних та телекомунікаційних) [1].

Інформатизація освіти дає можливість відкривати нові шляхи для розвитку методів і організаційних форм навчання та розвитку здобувачів освіти. На сьогодні інформаційні технології є тим новим способом передачі знань, який відповідає якісно новому змісту навчання і розвитку індивіда, в рамках процесу

реформування всієї вітчизняної системи освіти та її інтеграції в європейський освітній простір.

Проблемою застосування сучасних інформаційних технологій в освітньому процесі займаються багато дослідників. Серед них можна назвати А.І. Агапова, С.А. Вавренюка, С.М. Домбровську, В.І. Гриценко. У своїх роботах автори вказують, що інформаційні технології навчання являють собою сукупність методів і технічних засобів, які спрямовані на розширення знань індивіда, дозволяючи тим самим розвивати їх можливості по управлінню технічними та соціальними процесами.

Інформаційно-комунікаційні технології в освіті є комплексом навчально-методичних матеріалів, технічних та інструментальних засобів обчислювальної техніки в навчальному процесі, враховуючи форми і методи їх використання з метою вдосконалення діяльності фахівців в освітніх організаціях.

Застосування інформаційних технологій дозволяє відкривати такі можливості:

- представляти наочно ті явища, які неможливо донести іншими способами;
- створювати позитивну мотивацію до навчання за допомогою застосування засобів привернення уваги;
- активізувати пізнавальну діяльність здобувачів освіти;
- досягнути оптимальне використання часу в процесі навчального заняття.

Тим самим, інформатизація навчального закладу являє собою процес впровадження інформаційних технологій в усі напрямки здійснення освітньої діяльності.

Що стосується основної мети інформатизації в освіті, то вона представлена наступними положеннями:

- підвищення якості освіти;
- підвищення доступності та гнучкості освітніх послуг;
- підвищення ефективності управління освітнім процесом на всіх рівнях;
- формування інформаційної культури здобувачів освіти.

Слід зазначити, що зміст освіти, яка передбачає використання інформаційних та комунікаційних технологій, дозволяє забезпечувати ряд ключових компетенцій, необхідних для розвитку здобувачів освіти. Однак важливо враховувати, що забезпечення соціальної, комунікативної, інформаційної, когнітивної компетенції буде більш ефективним, якщо дотримуватися ряду умов:

- створення реальної можливості забезпечити підготовку педагогічних кадрів;
- підвищення рівня професійної та загально гуманітарної взаємодії викладачів і учнів за допомогою наявності можливості виконувати спільні проекти;
- підвищення ефективності самостійної роботи.

Враховуючи вище зазначене, забезпечення інформатизації освітнього закладу може проводитися у наступних взаємопов'язаних напрямках [2]:

1. Оновлення змісту, яке передбачає розвиток компетенції, адекватної сучасній практиці. Цей зміст повинен бути добре структурований та представлений у вигляді мультимедійних навчальних матеріалів, які передаються за допомогою сучасних засобів комунікації.
2. Впровадження сучасних методів навчання – активних методів формування компетенції, які основані на взаємодії навчаємих та їх залучення до навчального процесу.

Активне та ефективне використання інформаційно-комунікаційних технологій в освітніх організаціях ставиться важливим чинників оновлення всієї системи освіти, викликаної вимогами сучасного суспільства. Тому інформаційні технології не використовуються ізольовано в процесі навчання іноземної мови, а в своїй взаємодії дозволяють побудувати більш ефективний і продуктивний процес передачі знань. Тим самим, використання сучасних освітніх технологій дає можливість досягати продуктивності і ефективності освітнього процесу, роблячи його більш цікавим та інформаційно насиченим.

Інформаційні технології в освіті в даний час є необхідною умовою переходу суспільства до інформаційної цивілізації. Сучасні технології та телекомунікації дозволяють змінити характер організації навчально-виховного процесу, повністю занурити здобувачів освіти в інформаційно-освітнє середовище, підвищити якість освіти, мотивувати процеси сприйняття інформації і отримання знань. Нові інформаційні технології створюють середовище комп'ютерної та телекомунікаційної підтримки організації та управління в різних сферах діяльності, в тому числі в освіті. Інтеграція інформаційних технологій в освітні програми повинна здійснюватися на всіх рівнях: шкільному, вузівському та після вузівському навчанні.

1. Вавренюк С.А. Підходи та інноваційні технології в освітньому просторі / С.А. Вавренюк// XIV Міжнародна конференція «Стратегія якості у промисловості і освіті» (4-7 червня 2018 р., Болгарія, Варна): Матеріали. У 2 томах. Том І. Упорядники: Хохлова Т.С., Ступак Ю.О. – Дніпро-Варна, 2018. – 396 с.
2. Концепція впровадження медіа-освіти в Україні // Інститут соціальної та політичної психології Національної академії педагогічних наук України [Електронний ресурс]. – Режим доступу: http://www.ispp.org.ua/news_44.htm

Розділ 3. СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АКТУАЛЬНІ СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ ДІЯЛЬНОСТІ

Застосування алгоритму PageRank для швидкого пошуку втрачених речей

Барбарич Володимир Ігорович

здобувач вищої освіти
Львівського національного університету імені Івана Франка

Івануса Юрій Романович

здобувач вищої освіти
Львівського національного університету імені Івана Франка

Фірман Тарас Володимирович

оперуповноваженний карного розшуку Галицького ВП ГУ НП у Львівській обл.

Важко уявити життя на сьогоднішній день без інтернету, адже він усюди – у телефонах, планшетах, комп'ютері і навіть у телевізорі. За даними Міжнародного союзу електрозв'язку, 4.1 мільярда (53.6% від загальної кількості) людей у світі підключені до інтернету, станом на 2019 рік. Кількість користувачів глобальної мережі зросла на 5.3 відсотка порівняно з 2018 роком.[1] Але це не є чимось шкідливим для людей, бо допомагає швидко вирішити якусь проблему і зв'язатись вчасно з рідними, колегами чи з іншими потрібними вам особами. Процес диджиталізації важливий в глобальному плані, адже кожного дня створюються утиліти, які спрощують роботу навіть у примітивних речах, таких як оплата за комунальні послуги, тощо.

Ні для кого не є таємниця, що в наш час є багато злочинців, які викрадають велосипеди, автомобілі та інші речі. Незважаючи на те, що ми живемо вже у 2019 році, в різних куточках світу відбуваються пограбування та розбої. Потерпілі люди звертаються в правоохоронні органи з метою знайти крадія і повернути втрачені речі, але не завжди працівникам поліції вдається швидко знайти викрадене майно чи взагалі знайти. Для цього працівникам поліції помагала б універсальна пошукова машина, яка працює згідно алгоритму PageRank, що позволить швидко надати потерпілому чи працівнику правоохоронних органів

інформацію з оголошень в інтернеті, що міститимуть будь-які деталі щодо втрачених речей. Використовуючи бібліотеку urllib2, яка входить дистрибутив мови програмування Python, ми зможемо скачувати і добавляти в базу даних похідні від головної сторінки посилання.

Алгоритм PageRank був придуманий засновниками компанії Google, і варіації цієї ідеї тепер застосовуються у всіх великих пошукових машинах. Цей алгоритм приписує кожній сторінці ранг, що оцінюють її значимість. Значимість сторінки обчислюється виходячи з тих значимостей, які посилаються на неї і загальної кількості посилань, наявних на кожній з них.[2]

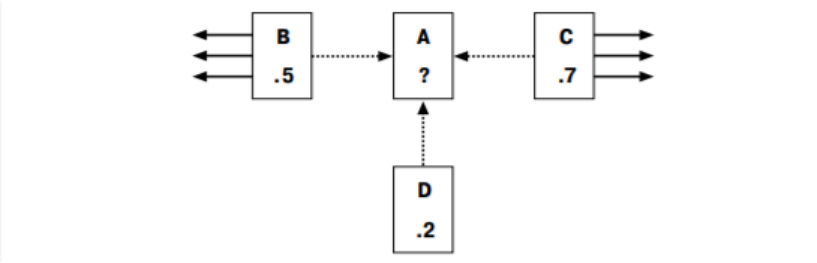

Рисунок 1 – структура PageRank

Кожна зі сторінок B, C і D посилається на A, і для них ранг вже обчислений. На сторінці B є посилання ще на три сторінки, а на сторінці C – на чотири. D посилається тільки на A. Щоб обчислити ранг A, беремо ранги (PR) кожної сторінки, що посилається на A сторінки, ділимо їх на загальне число посилань на цій сторінці, складаємо отримані значення, потім множимо результат на коефіцієнт загасання 0,85 і додаємо мінімальну величину 0,15. Ось як виробляється обчислення PR(A):

$$PR(A) = 0{,}15 + 0{,}85 \times \times \left(\frac{\text{PR(B)}}{\text{ссылки(B)}} + \frac{\text{PR(C)}}{\text{ссылки(C)}} + \frac{\text{PR(D)}}{\text{ссылки(D)}}\right) = = 0{,}15 + 0{,}85 \times (0{,}5/4 + 0{,}7/5 + 0{,}2/1)$$

$$= 0{,}15 + 0{,}85 \times (0{,}125 + 0{,}14 + 0{,}2) =$$

$$= 0{,}15 + 0{,}85 \times 0{,}465 = 0{,}54525$$

Зверніть увагу, що D дає більший внесок в ранг A, ніж B або C, хоча її власний ранг менше. Це викликано тим, що D посилається тільки на A і, отже, привносить в результат свій ранг цілком. На жаль, в даному прикладі для всіх сторінок, що посилаються на A, вже обчислений ранг. Але неможливо обчислити ранг сторінки, поки невідомі ранги посилаються на неї, а ці ранги можна обчислити, тільки знаючи ранги сторінки, які посилаються на них. Так як же обчислити значення PageRank для безлічі сторінок, ранги яких ще невідомі? Рішення полягає в тому, щоб привласнити для всіх сторінок довільний початковий ранг (в нашому випадку 1.0) і провести кілька ітерацій. Після кожної ітерації ранг кожної сторінки буде все ближче до істинного значення PageRank.

Підсумовуючи вище наведене, користувачі пошукових систем (звичайні люди чи працівники правоохоронних органів), використовуючи дану технологію зможуть не тільки швидко знаходити втрачені чи вкрадені речі, але й співпрацюючи з працівниками компетентних органів – боротись із злочинністю.

---

1. Міжнародний союз електрозв’язку [Електронний ресурс] : https://www.itu.int/en/ITU-D/Statistics/Documents/facts /FactsFigures2019.pdf
2. Сегеран. Т. Программируем коллективный разум. – Пер. с англ. – СПб: Символ-Плюс, 2008. – 368 с., ил.

Цифровий порядок денний у правовому механізмі формування «Простору знань» в Європейському союзі

Бортник Надія Петрівна

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

Майже 20 років тому в Декларації тисячоліття ООН були сформульовані глобальні пріоритети в галузі розвитку [1]. У 2015 році ООН прийняла стратегічний документ «Порядок денний в галузі сталого розвитку на період до 2030 року», в якому підтвердила прихильність зазначеним пріоритетам, визначила розрахований на перспективу набір з універсальних орієнтованих на перетворення 17 цілей і 169 завдань. Серед них:

- нарощування технологічного потенціалу економіки у всіх країнах шляхом державного і частого фінансування наукових досліджень і розробок;
- створення механізму сприяння розвитку технологій, який ґрунтується на багатосторонній співпраці між державами, громадянським суспільством, приватним сектором, науковим співтовариством, структурами ООН та іншими зацікавленими сторонами.

Втілення в життя Порядку денного в галузі сталого розвитку здійснюється в умовах переходу сучасного суспільства до четвертого технологічного укладу – «Індустрії 4.0», фундаментальним ознакою якого є домінуюча роль знань і відповідно найбільш «знання-ємних» цифрових технологій [2].

Випереджальна цифровізація соціальних, зокрема, економічних, процесів розглядається представниками економічної науки в якості технологічної основи «реіндустріалізації».

На переконання вчених, «реіндустріалізація» національної економіки на новій технологічній основі, передбачає, що в якості основи реіндустріалізації виступатимуть технології наступного

рівня знання ємкості. Сьогодні їх називають високими технологіями. У програмі сталого розвитку поширення інформаційно-комунікаційних технологій і глобальне взаємне підключення мереж позначені серед ключових завдань, оскільки вони відкривають величезні можливості для прискорення людського прогресу, подолання «цифрового розриву» та формування суспільства, заснованого на знаннях.

Суб'єкти економічної діяльності сьогодні використовують широкий спектр цифрових технологій, здатних принести значні економічні результати. Хоча кожен з технологічних укладів характеризується кластером типових технологій, перелік останніх варіюється. Стосовно до «Індустрії 4.0», найбільш часто згадуються: аналітика великих даних; блокчейн; Інтернет речей; 3D-друк; робототехніка; сенсорика; доповнена реальність; штучний інтелект, хмарні обчислення.

Держави, інтеграційні об'єднання держав (Європейський Союз, НАТО) констатують наявність взаємозалежності між стійким розвитком, цифровизацією і іншими процесами, що протікають в економічній і соціальній сферах, в тому числі в сфері політики та права.

В Аддіс-Абебской програмі дій Третій міжнародній конференції з фінансування розвитку відзначається, що поряд з нарощуванням потенціалу у галузях науки, техніки, інновацій необхідно вдосконалювати правові умови сталого розвитку, до яких відносяться: верховенство права на національному та міжнародному рівні; гарантії основних прав і свобод; стабільна нормативно-правова та договірна основа [3].

Країни Організації економічного співробітництва і розвитку (ОЕСР) визначили, що з метою отримання максимальних переваг від цифрової трансформації для інновацій, зростання економіки та соціального процвітання необхідно зосередити зусилля на розробці всебічного політико-правового підходу до зростаючої екосистеми цифрових технологій, що приділяє переважне увагу капіталу, заснованого на знаннях, і аналізу даних.

У координації зі стратегією стійкого розвитку ЄС і НАТО, сформулювали та затвердили цифрові порядки денного. Поряд з програмами досліджень і інновацій, цифрові порядки денного є основоположними юридичними документами, що регламентують розгортання «цифрових просторів», сумісних і гармонізованих з «просторами знань» в названих інтеграційних об'єднаннях.

У цифрових порядках денних знаходять відображення глобальні та універсально застосовні правові підходи до цифрової взаємодії, яких дотримуються держави у межах інтеграційних об'єднань, сформульовані ООН принципи, відповідно до яких цілі та завдання в галузі сталого розвитку забезпечують облік відмінностей в національних реаліях, можливості та рівнях розвитку, повагу національних стратегій і пріоритетів.

В Європейському Союзі стимулювання створення проривних знання-ємних технологій засновано на Лісабонської стратегії, Стратегії «Європа-2020», в яких наукові дослідження, інновації та відкритий доступ до знань у межах Європейського Союзу характеризуються як активні фактори зміцнення конкурентоспроможності ЄС і держав-членів [4].

У зв'язку з цим в програмі «Горизонт 2020» («Horizon 2020») поставлено завдання інтенсивного просування технологій, відкриттів і перспективних розробок з наукових організацій і лабораторій на ринок [5].

Названим стратегічним документам кореспондується правова модель Європейського дослідницького простору (European Research Area (ERA), єдине дослідницьке середовищк, що охоплює внутрішній ринок ЄС і «відкрите світу». Пріоритетами ERA є:

- ефективні національні дослідницькі системи;
- транснаціональне співробітництво, включаючи «спільне рішення грандіозних завдань» і «дослідницьку інфраструктуру»;
- відкритий ринок праці для дослідників; оптимальне поширення та передача наукових знань, включаючи «вільний доступ» до знань;

- міжнародне співробітництво і ряд інших.

У Доповіді про функціонування ERA в 2016-2018 роки поряд з досягнутим прогресом, відзначається уповільнення внаслідок значних відмінностей між країнами, що свідчить про необхідність спільних зусиль на всіх рівнях, включаючи узгодження правових підходів до реформування національних науково-дослідних систем.

У зв'язку з цим наступний стратегічний документ ЄС «Horizon Europe» (2021-2027 р) містить особливий компонент, покликаний сприяти зміцненню ERA [6].

У розвиток лісабонської стратегії програма «Цифрова порядок денний для Європи» (DAE) була задумана як одна з флагманських ініціатив стратегії «Європа 2020». Визначає ключову стимулюючу роль, яку відіграє використання інформаційно-комунікаційних технологій в реалізації задач стратегії «Європа-2020».

З метою формування відкритого та безпечного цифрового середовища цифрова стратегія єдиного ринку передбачає забезпечення кращого доступу споживачів і підприємств до цифрових товарів та послуг у всій Європі; створення оптимальних умов для збільшення потенціалу цифрової економіки шляхом розвитку цифрових навичок і високопродуктивних обчислень, цифрування промисловості та послуг, розвитку штучного інтелекту та модернізації державних послуг.

У 2015 році Європейська комісія дала старт цифровому єдиному ринку і окреслила основні законодавчі пропозиції, які відносяться до стимулювання електронної торгівлі, авторського права, аудіовізуальних засобів, телекомунікацій, гармонізації цифрових прав, конфіденційності та кібербезпеки. Відповідно до «Стратегією цифрового єдиного ринку для Європи» та програмою «Горизонт 2020», Європейська комісія оголосила про розробку «Європейської відкритої наукової хмари» (EOSC) віртуального загального простору, створюваного в якості єдиного середовища для розміщення та обробки дослідних даних з різних джерел з метою підтримки науки в ЄС.

Ініціатива об'єднає існуючі та майбутні інфраструктури даних, пропонуючи безпечний і безперешкодний доступ до європейських студій. Комісія прийняла 14 березня 2018 року дорожню карту впровадження «Європейської відкритої наукової хмари». Дорожня карта містить шість напрямків розгортання EOSC: архітектуру, дані, послуги, доступ і інтерфейси, правила, управління. Впровадження EOSC належить до числа політико-правових пріоритетів для європейських досліджень та інновацій [7]. Європейська комісія прийняла в січні 2017 роки програму «Побудови європейської економіки даних», яка передбачає, зокрема, розробку регулювання доступу до даних і їх передачі.

Відповідно до новітніх рішень європейських законодавців, завершення формування цифрового єдиного ринку та розширення простору знань потребують додаткових інвестицій. ЄС створює нову програму «Цифрова Європа», яка буде ініційована в 2021 році і надасть фінансування проектів у галузях як: суперкомп'ютери, штучний інтелект, кібербезпека, передові цифрові навички та забезпечення широкого використання цифрових технологій в економіці та суспільстві. Програма зміцнює мережу цифрових інноваційних центрів, що забезпечують доступ до технологічного досвіду для підприємств, зокрема малих і середніх підприємств і органів державного управління. Цифрова Європа буде доповнювати інші програми, що підтримують цифрову трансформацію, такі як Горизонт Європи 2021-2027 р. (Horizon Europe).

---

1. Декларація тисячоліття Організації Об'єднаних Націй. Офіційний сайт Верховної Ради України. URL. https://zakon.rada.gov.ua/laws/show/995_621 (дата звернення 07.12.2019).
2. Перетворення нашого світу: Порядок денний у сфері сталого розвитку до 2030 року. URL. https://www.ua.undp.org/content/ukraine/uk/home/library/sustainable-development-report/the-2030-agenda-for-sustainable-development.html (дата звернення 07.12.2019).

3. Аддис-Абебская программа действий третьей Международной конференции по финансированию развития (Аддис-Абебская программа действий). URL. https://unctad.org/meetings/en/SessionalDocuments/ares69d313_ru.pdf (дата звернення 07.12.2019).
4. Європейська Рада схвалила Стратегію Європа-2020 / Євробюлетень. 2010. № 4. С. 16.
5. Програма Horizon 2020. URL. https://eu-ua.org/horizon-2020 (дата звернення 07.12.2019).
6. Horizon Europe 2021-2027. URL. http://www.unife.org/tags/179-horizon-europe-2021-2027.html (дата звернення 07.12.2019).
7. Меморандум: Європейська Хмара Відкритої Науки для дослідження (30 жовтня 2015 року). URL. http://ung.in.ua/ua/news/107/ (дата звернення 07.12.2019).

Співпраця щодо обміну інформацією між вітчизняними правоохоронними органами та західними правоохоронними інституціями: сучасний стан та перспективи подальшого розвитку

Волянюк Артем Віталійович

здобувач вищої освіти Чорноморського Національного Університету імені Петра Могили

Починаючи від самого моменту визнання незалежності Україною в 1991 році питання всебічної співпраці с європейськими країнами займало дуже вагоме значення в зовнішній політиці нашої держави, тісні відносини були сформовані не тільки в дипломатичній, економічній, чи гуманітарній площині, але і в правоохоронній сфері також.

На доказ вищенаведеному твердженню можна навести факт плідної співпраці національних правоохоронних органів з Інтерполом, Україна з 1992 року є членом даної організації, саме тоді Кабінет Міністрів України постановою №220 створив та ввів у дію «Положення про Національне центральне бюро Інтерполу», сумісна робота проводиться переважно в питаннях запобігання економічної злочинності, організованої злочинної діяльності та питаннях незаконного обігу наркотиків.

Про те на мою думку, загострити увагу треба саме на відносинах за останні 5 років, тобто починаючи з 2014 року і по наші дні, проблемність питання полягає в тому, що на даному етапі в Україні склалась дуже складна політична та економічна ситуацію, яка викликана гібридною війною з Російською Федерацією, створенням терористичних квазідержав на Сході України, та окупацією Криму та частини Сходу країни.

В такий тяжкий час питання співпраці між правоохоронними органами, а також між урядами країн та профільними міністерствами відіграє значну роль в утверджені національної безпеки та суспільного спокою в державі.

Перші спроби винесення цих відносин на більш глобальний рівень були проведені в 2014 році, саме тоді була підписана «Угода про асоціацію між Україною та Європейським союзом», і в ІІІ розділі були зафіксовані питання співробітництва між Україною та Європолом та Євроюстом, тобто зі спеціальними профільними інституціями Європейського союзу.

А вже згодом в 2014 році було підписано пряму Угоду про стратегічне і оперативне співробітництво між Україною та ЄВРОПОЛОМ, з боку України підписантом було Міністерство Внутрішніх Справ,.

А вже в 2016 році аналогічна угода була підписана між нашою державою та Європейською організацією з питань юстиції (Євроюстом). В ній було чітко передбачено положення про співпраця сторін, яка буде здійснюватиметься через створення спільних слідчих груп, оперативного обміну інформацією, координації дій з протидії транскордонній злочинності та надання правової допомоги

Таким чином співпрацюючи з європейськими правоохоронними інституціями українським правоохоронцям надана можливість бути учасниками міжнародних поліцейських заходах, разом з іноземними колегами, брати участь у сумісних навчаннях, і що найголовніше здійснювати обмін та обробку стратегічною та оперативною інформацією, для розкриття тяьжких та особливо тяжких злочинів.

Шляхи співробітництва були прокладені не тільки в виключно правоохоронній сфері, але і в правозастосовній сфері, в сфері утвердження правосуддя, незаконній міграції та забезпечення демократичних засад в державі.

Профільним органом який би координував цю співпрацю було створено Підкомітет з питань свободи, безпеки та юстиції Комітету асоціації Україна – ЄС, засідання якого проводять щороку.

Таке співробітництво відіграє значну роль в питаннях інформаційного забезпечення вітчизняних правоохоронних органів, а як наслідок відповідно і в показниках результативної роботи по попередженню чи розкриттю злочинів.

Як в політичній так і в правоохоронній площині одним із найбільших союзників виступають Сполученні Штати Америки, глобальна сумісна правоохоронна діяльність почалася з 2014 року, коли до України прибули американські спеціалісти для допомоги у розслідуванні вітчизняному МВС факту та обставин збиття малайзійського Боїнга, на території Сходу України.

Правоохоронна співпраця між Україною та США закріпилася у 2018 році, коли Міністерство Внутрішніх Справ України підписало «Меморандум про взаємне співробітництво з ФБР», підписання цієї угоди дає змогу Національній поліції України обмінюватися оперативною інформацією стосовно злочинних формувань які діють на території обох країн, наркотрафіків, економічної злочинності та корупційних зв'язків.

Дана угода окрім простого обміну інформацією передбачає також тісну співпрацю в технічній сфері, тобто взаємну допомогу країн у науково технічному плані та процесі встановлення фактів, та загальному процесі попередження та розкриття злочинів.

Окремим питанням виступає обмін інформацією з правоохоронними органами такої країни як Фінляндія, заява про співробітництво правоохоронних відомств була підписано у 2016 році, і закріпила механізми співробітництва та обміну інформацією з метою попередження та розслідування злочинів, втому числі які мають транснаціональний характер.

Для нашої держави ця угода має колосальне значення бо Фінляндія це країна Балтійського регіону, і відповідно теж знаходиться в сфері злочинних, загарбницьких інтересів РФ, і відповідно обмін між нашими силовими відомствами може зупинити багато злочинних проявів агресора ,відразу на двох плацдармах.

Тож, якщо підбити підсумок всього зазначеного то можна сказати, що питання співробітництва стосовно обміну інформацією між вітчизняними та європейськими правоохоронними органами відіграє дуже значну роль, і в процесі попередження злочинів і в безпосередньо вже в процесі розслідування скоєних противоправних діянь.

За останні роки було підписано багато угод щодо обміну інформацією,створення спільних слідчих груп, цей факт дає надію на підвищення результативності роботи Національної поліції, Генеральної Прокуратури, Міграційної Служби України,і відповідно створює позитивну тенденцію позитивних змін в країні.

Загрози інформаційній безпеці в умовах гібридної війни та напрями удосконалення системи інформаційної безпеки України

Гаврильців Марія Теодорівна

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

Чітке розуміння і виокремлення факторів, що зумовлюють загострення загроз інформаційній безпеці, мають системний характер, а тому вони охоплюють усі без винятку сфери життєдіяльності людини, суспільства і держави. На практиці аналіз викликів – це завжди суб'єктивний процес сприйняття суб'єктом певних факторів через призму власних інтересів і професійності.

Важливий компонент гібридної війни – вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування світового політичного стандарту, узгодженого з інтересами агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: втручанням у функціонування інформаційно-телекомунікаційних систем та мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації та маніпуляція суспільною думкою [3, с. 18].

Характер ведення російсько-української війни свідчать, що її метою є зміна самоідентифікації населення і перетворення східного регіону нашої держави на «сіру зону», яка залишить РФ важелі свого впливу через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки і душі людей. А оскільки контроль над інформаційною інфраструктурою дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях то в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади [4, с. 40-41].

Нині основними визначальними факторами, що негативно впливають на інформаційний простір в Україні дослідники вважають: постійні втрати серед особового складу (загиблі, полонені, поранені), які ведуть до формування недовіри до українського воєнно-політичного керівництва, що нібито нездатне контролювати ситуацію, що склалася в Україні; недосконала національна система інформаційної безпеки сприяє зниженню рівня патріотизму; активність зовнішніх інформаційних заходів з боку Росії впливає на формування основного твердження про прийнятність для України федерального державного устрою та завершення бойових дій на Сході країни на умовах кремлівського режиму [6, с. 39].

Нова редакція Доктрини інформаційної безпеки України 2017 р. актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері визначила: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда федералізму та сепаратизму в Україні [5].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [1, с. 12]. Не менш гостро в умовах гібридної війни постає питання кібербезпеки. В сучасному світі кібернетичний простір все частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму [3, с. 18].

Перш за все, мережі та інформаційні системи містять конфіденційні дані та економічно цінну інформацію, що підвищує стимул для атак. Атаки на інформаційні системи можуть мати серйозні у національному масштабі наслідки, як то перебої у роботі систем комунікацій, витік конфіденційної інформації тощо [2, с. 28].

Зрозуміло, що сьогодні українське суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоєчасного надходження, шпигунства, комп'ютерної злочинності тощо. Ці фактори є елементами гібридної війни, що сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки.

Основними складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства. Відтак, першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності РФ проти України та запобігання її подальшому розгортанню. Вирішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації [7, с. 38].

В умовах гібридної війни держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних

правових і адміністративних заходів, а з іншого – може супроводжуватись істотним згортанням демократичних прав і свобод.

Україні варто ініціювати міжнародні переговори з проблем забезпечення безпеки в інформаційній сфері. Зокрема, повинні бути досягнуті угоди між максимальною кількістю країн з координації діяльності у сфері боротьби з інформаційним тероризмом і інформаційним криміналом, із запобігання цих загроз і узгодження дій та в мінімізації їх наслідків. Предметом переговорів повинен також стати міжнародно-правовий захист національних інформаційних ресурсів та інтелектуальної власності, а також авторських прав на матеріали, поширювані світовими відкритими мережами, в першу чергу через Інтернет. Повинні бути вироблені узгоджені національні та міжнародні правові норми, що встановлюють відповідальність за хакерство та інші комп'ютерні злочини, зловмисне проникнення в державні та корпоративні інформаційні мережі, порушення прав і законних інтересів громадян у процесі інформаційного обміну. Необхідно розглянути можливості контролю за поширенням у мережі Інтернет непристойної і такої, що наносить шкоду суспільній моралі, інформації, недобросовісну рекламу, розпалювання війни, шахрайські операції тощо, які чинять негативний вплив на масову свідомість, фізичне, психічне і соціальне здоров'я людей.

В умовах проведення країною-агресором РФ деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору і забезпечення національної системи інформаційної безпеки України: по-перше, удосконалити нормативно-правову базу у сфері інформаційної політики держави, яка б визначала взаємодію силових структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійснював керівництво, координацію та контроль заходів інформаційної безпеки; по-третє, створити систему комплексного моніторингу популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів; по-

четверте, заохочувати подальші комплексні наукові дослідження у сфері інформаційної безпеки.

Необхідно зауважити, що система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни представляє собою сукупність органів державної влади, недержавні структури і громадяни, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам у сучасних умовах.

1. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Київ: Національна академія Служби безпеки України. 2018. 408 с.
2. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.
3. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. №4. С. 16–26.
4. Дмитренко М. А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236-243.
5. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25.02.2017 № 47/2017. URL: http://zakon.rada.gov.ua/laws/show/47/2017.
6. Косогов О. М., Сірик А. О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. Системи озброєння і військова техніка. 2017. С. 38–41.
7. Левченко Ю. О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16-17 листопада 2017 року). Хмельницький: МВС УКРАЇНИ, 2017. 50 с.

Інформаційно-конституційні права людини і громадянина в сучасних реаліях

Грищук Аліна Борисівна

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

Чабак Вікторія Юріївна

здобувач вищої освіти ПрАТ «ВНЗ» «Міжрегіональна академія управління персоналом»

Інформаційні права людини – це гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації.

Гарантоване Конституцією України право на інформацію стає все більш важливим для існування демократичного суспільства. Та не варто ототожнювати право на інформацію й інформаційні права людини.

У сучасному конституційному праві існує багато визначень конституції. За основу як правило береться одна або декілька ознак, що відносяться до предмету конституційного регулювання, місця, яке посідає конституція в ієрархії джерел права, в національній правовій системі. Так, французький політолог Бюрдо Ж. визначав конституцію як «сукупність правил, що відносяться до способу призначення, організації і функціонування політичних влад». Американський дослідник К. Берд додає до цього таку ознаку як «визначення свобод громадян». Конституція постає як основний, головний закон держави в юридичній науці й практиці. Вона регламентує найважливіші з погляду держави суспільні відносини. До них належать засади суспільного ладу й політики, правового становища особи, державного устрою, організації та діяльності органів держави [1, с. 28].

Право на доступ до інформації є одним з основоположних прав людини і громадянина, вираженням демократичної політичної системи українського суспільства.

Право на інформацію є одним із фундаментальних прав, яке забезпечує розвиток особистості, функціонування правової держави, розвиток та становлення громадянського суспільства, і є передумовою існування демократичного устрою держави. Комплекс питань, пов'язаних із правом на інформацію, власне, наявністю чи відсутністю таких прав, визначає рівень демократичності суспільства, дотримання загальновизнаних у світі прав і свобод людини та громадянина.

Відповідно до ст. 32 Конституції не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, а згідно зі ст. 34 кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом лише в передбачених ч. 3 ст. 34 Конституції випадках [2].

Відповідно до статті 3 Конституції України права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави [2]. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Саме інформаційні права гарантують громадянам можливість мати певні переконання та не піддаватися у зв'язку з цим переслідуванням, вільно висловлювати свою думку, відстоювати свої ідеї та контролювати діяльність влади. Сьогодні ми живемо в інформаційному суспільстві, в якому інформаційні права відіграють надзвичайно важливу роль. Комплекс прав та свобод в інформаційній сфері вважається непорушним та невідчужуваним. Набуття інформаційною сферою всепроникливого характеру зробило інформацію та інформаційно-правові явища міждисциплінарним об'єктом правової науки. Практично кожен науковець, розглядаючи поняття інформаційних прав, намагався навести власне його трактування, тому наявні декілька десятків дефініцій. Слід

вказати і на те, що з плином часу, з розумінням значення інформаційних прав та їх суспільної необхідності для кожного індивіда інтерес до досліджуваної категорії лише зростав і, як наслідок, науковий доробок з кожним роком збагачувався [3].

З огляду на те, що до основних структурних елементів права на інформацію Основний Закон включає низку правоможливостей: право збирати, право зберігати, право використовувати та право поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, які, у свою чергу, структуруються в інші численні інформаційні права, можна вважати, що назване право є комплексним. Водночас змістовими складниками інших конституційних прав і свобод закріплені такі, зокрема, права, як: право давати згоду на збирання, зберігання, використання та поширення конфіденційної інформації про неї; право кожного громадянина на доступ до відомостей про себе (крім тих, що становлять захищену законом таємницю) в органах державної влади, органах місцевого самоврядування, установах і організаціях; право кожного перевіряти достовірність інформації про себе і членів своєї сім'ї; право спростовувати недостовірні відомості в судовому порядку; право вимагати вилучення будь-якої інформації про себе; право кожного на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням недостовірної інформації про себе і членів своєї сім'ї; право на забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції; право на вільний доступ і поширення інформації про стан навколишнього середовища (право на екологічну інформацію), про якість харчових продуктів і предметів побуту та інші, які певним чином можна визначити як саме «інформаційні права» в межах досліджуваного поняття [4, с. 115]

Конституцію можна коротко визначити як основний закон держави, який закріплює організацію державної влади та регулює взаємовідносини цієї влади, суспільства та індивідів. Під конституцією в матеріальному значенні розуміється здебільшого сукупність юридичних норм, які закріплюють основні права та свободи людини і громадянина, визначають інформаційні права громадянина, визначають засади суспільного ладу, форми

державного правління і державного устрою, основи організації центральних і місцевих органів державної влади, їх компетенцію та взаємовідносини, державні символи і столицю. Критерієм (підставою) для віднесення правових норм до норм конституції у матеріальному значенні є не стільки форма та юридична сила акту (актів), в якому (в яких) вони містяться, скільки характер відносин, які цими нормами регулюються. Назване вище коло відносин якраз і складає предмет конституційного регулювання. Конституцією у формальному значенні іменується єдиний акт або ж кілька актів, що мають вищу юридичну силу стосовно всіх інших нормативних актів.[2, с. 51]

Конституція в даному значенні – це свого роду закон законів. Вона може бути змінена тільки в особливому, встановленому, як правило, нею самою порядку, зміна конституції тягне за собою перегляд раніше прийнятих законів та інших нормативних актів на предмет їх відповідності зміненим положенням конституції.

Найважливішими юридичними ознаками конституції є:

конституція – це основний закон держави, тобто документ, який повинен виступати основою національного законодавства;

конституція – це закон, який має вищу юридичну силу, тобто всі інші нормативно-правові акти мусять відповідати положенням конституції (наприклад, Конституційний Суд України може скасувати положення будь-якого закону, який не відповідає Конституції України, як от у рішенні, частина з якого приведена праворуч);

конституція – це закон, що має підвищений ступінь стабільності.

Сучасна Конституція України це не тільки підсумок процесів державотворення, це й своєрідний дороговказ подальшого вдосконалення нашої держави, наповнення її сформованих інститутів реальним змістом, перетворення їх на реальні чинники правового регулювання суспільних відносин в Україні. Слід зазначити, що прийняття Конституції стало результатом компромісу різноспрямованих політичних сил, тому її можна розглядати як запоруку майбутньої злагоди в нашому суспільстві, гарантію його розвитку на засадах забезпечення врівноваженості різних

соціальних верств та політичних течій за умови неодмінного визнання непорушності політичного суверенітету нашої держави [3, с.4-8].

Конституція України закріплює за народом виключне право визначати і змінювати конституційний лад. Інакше кажучи, тільки з волі народу, виявленої на всеукраїнському референдумі, можлива зміна принципів організації та функціонування механізму держави [4, с. 234].

Основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації та свобода щодо її обміну; об'єктивність, достовірність інформації; її повнота й точність; законність одержання, використання, поширення та зберігання інформації. Відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації врегульовані в Законі України «Про інформацію».

Відповідно до ст.1 Закону України «Про інформацію» інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [5].

---

1. Історія української Конституції/ А.Г.Слюсарено, М.В.Томенко. – К.:Право, 1997. – 464 с. – URL: http://irbis-nbuv.gov.ua/ulib/item/0001857
2. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28.06.1996 р. // URL: http://zakon5.rada.gov.ua /laws/show/254к/96-вр.
3. Леонов Б. Д. Особливості правової інформації/ Б. Д. Леонов. URL: ippi.org.ua/sites/default/files/bdopi.pdf.
4. Костецька Т. А. Конституційно-правове регулювання інформаційних прав: деякі терміноло- 159 2/2018 ІНФОРМАЦІЙНЕ ПРАВО гічні аспекти / Т. А. Костецька // Часопис Київського університету права. – 2013/2. – С. 114-117.
5. Про інформацію: Закон України від 13.01.2011 № 2657-XII. URL: http:zakon5.rada.gov.ualawsshow265712

Застосування алгоритму k-середніх у діяльності поліції

Дзвоник Ігор Андрійович

здобувач вищої освіти
Львівського Національного університету імені Івана Франка

Фірман Володимир Михайлович

доцент кафедри безпеки життєдіяльності
Львівського Національного університету імені Івана Франка,
кандидат технічних наук, доцент

В Україні спостерігається економічний та соціальний розвиток. Збільшення виробництва основних видів продукції та покращення умов проживання. [1] Разом з тим росте і рівень злочинності, що залежить від багатьох факторів. Тільки за останні 9 місяців 2019 року зареєстровано 686 573 кримінальних правопорушень. В той же час відсоток розкриття злочинів в Україні в 2019 році складає лиш 41%.[2]

Проводячи аналіз статистичних даних варто і необхідно провести систематизацію умов і причин, що призводять до вчиненя злочинів. Необхідно ввести автоматизацію відслідковування їх в ІБД. З розвитком комп'ютеризованих систем та аналітики даних, можна використовувати засоби для запобігання злочинності та забезпечення безпеки населення. Поточні стратегії поліції працюють у напрямку пошук злочинців, в основному, після скоєння злочину.[3] Тому ефективніше буде використовувати програму на основі алгоритму k-середніх, системний підхід, якої базується на основі аналізу та виявлення умов і причин злочинності. Так як близько 50% усіх злочинів вчиняють громадяни, які раніше притягались до кримінальної відповідальності.[4] При введені програми, надається змога відслідковувати попередні злочини, для передбачення виникнення нових злочинів. Це покращить ефективність роботи поліції в розкриті злочинів та їх попередженя.[5]

Переваги використання програми на основі алгоритму k-середніх:

- простота і швидкість у використанні;
- передбаченя регіони, які мають високу ймовірність виникнення злочинів;
- можливість візуалізувати зони, схильні до злочинів;
- допомагає правоохоронцям пришвидшити процес розкриття злочинів;

Таким чином, за допомогою інформаційних технологій, ми можемо використовувати дані злочинів, щоб визначити закономірності злочинців при їх вчинені і використовувати ці моделі для попереднього прогнозування вчиненя злочинів. Все це ефективно вплине на службову діяльність правоохоронної системи.

1. Економічні підсумки та перспективи України - http://icps.com.ua/ekonomichni-pidsumky-ta-perspektyvy-ukrayiny-prohres-rehres-chy-status-kvo/
2. Інформація про результати діяльності органів прокуратури - https://www.gp.gov.ua/ua/vlada.html
3. Стратегія розвитку органів внутрішніх справ - http://khpg.org/index.php?id=1411470323
4. Кримінологічний аналіз стану злочинності в Україні - http://studies.in.ua/analiz-ta-prognoz-zlochynnosti/3932-krimnologchniy-analz-stanu-zlochinnost-v-ukrayin.html
5. Crime Prediction using K-means Algorithm - http://www.grdjournals.com/uploads/article/GRDJE/V02/I05/0176/GRDJEV02I050176.pdf
6. Дзвоник І. А. курсова робота «Застосування алгоритму k-середніх у кластерному аналізі», 2019.

Напрями використання безпілотних літальних апаратів (дронів) органами поліції

Дуфенюк Оксана Михайлівна

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

Тема потенційних можливостей використання безпілотних літальних апаратів (далі – БПЛА) або дронів (від анг. *drone*) під час виконання службових обов'язків правоохоронними органами вже не нова, однак залишається актуальною і важливою. Інноваційні технології рухаються вперед і їх пристосування для реалізації завдань пов'язаних із забезпеченням безпеки, попередженням злочинів, якісним фіксуванням інформації в ході досудового розслідування є однією із пріоритетних умов ефективної протидії сучасній злочинності. Світовий досвід доводить, що застосування БПЛА у діяльності поліцейських та інших спеціальних служб набуває дедалі більшої популярності та підтверджує винятково важливе значення цих технологій, оскільки вони дозволяють значною мірою оптимізувати виконання правоохоронних функцій. Проте в Україні сьогодні використання підрозділами Національної поліції БПЛА не набуло широкої практики. З огляду на це, важливо знати переваги та визначити основні напрямки використання дронів та технологій аерозйомки.

Отже, *перший напрям – картографічна робота*, тобто створення карт територій обслуговування підрозділів поліції для моніторингу ситуації в режимі реального часу, оцінки шкоди, завданої під час стихійних лих тощо [1].

Другий напрям – забезпечення безпеки працівників поліції при виконанні службових обов'язків. БПЛА можна використовувати для обстеження тих ділянок місцевості чи навіть приміщень, доступ до яких для поліцейських з певних причин закритий або перебування на такому об'єкті є потенційно небезпечним для життя чи здоров'я. Йдеться про загрозу обвалу конструкцій, вибухів, пожеж, збройного опору осіб тощо. Наприклад, озброєний злочинець, який перебуває за певною перешкодою становить

загрозу для групи затримання. Використання дрона допомагає залишати його в полі зору, стежити за його діями, пересуванням і відповідно корегувати дії команди поліцейських з метою уникнення тактичних ризиків завдання шкоди життю чи здоров'ю. Особливого значення питання безпеки набуває при документуванні кримінальних правопорушень у зоні ООС. Безпекові функції, за словами закордонних фахівців, також актуалізуються при виявленні та знешкодженні незаконних та незареєстрованих дронів злочинцями [1].

Третій напрям – забезпечення безпеки при проведенні масових заходів. Деякі моделі БПЛА оснащені додатковими спеціальними інфрачервоними та руховими сенсорами для виявлення осіб навіть у темну пору доби, датчиками GPS, камерами для розпізнавання облич, що дозволяє ідентифікувати осіб у парковій зоні, поблизу шкіл, при політичних зборах та мітингах [2, с. 2–3]. Для моніторингу та забезпечення безпеки осіб при проведенні масових заходів дрони застосовуються у Великій Британії, США, Китаї та багатьох інших країнах [3, с. 43].

Четвертий напрям – проведення пошукових та рятувальних операцій. БПЛА можна використовувати для розшуку та затримання осіб, які намагаються втекти з місця події, обстеження значних ділянок територій з метою виявлення незаконного видобутку корисних копалин (піску, бурштину тощо), порубки лісів, незаконних посівів нарковмісних культур тощо. Виконання таких дій наземними силами і засобами вимагатиме значно більше витрат часу, ресурсів, координації зусиль, тоді як піднятий в небо БПЛА справиться із цими завданнями за лічені хвилини. До прикладу, американські колеги слушно вказують, якщо злочинець піднімається на дах, важко визначити якими шляхами він втікатиме, а піднятий у повітря БПЛА може допомогти прослідкувати маршрут руху, відстежити чи має при собі особа зброю та/або інші речі. Крім того, дрони можуть допомогти виявити місцезнаходження потерпілих від злочину, допомогти в роботі рятувальних служб під час реалізації рятувальних операцій [1].

П'ятий напрям – попередження кримінальних правопорушень. У багатьох країнах дрони застосовуються для патрулювання громадських місць та попередження протиправних дій, оскільки така техніка дозволяє не тільки моніторити територію в режимі реального часу, фіксувати відомості з високою якістю, а відповідно й пришвидшити час реагування на події в певному районі та доведення/спростування певних фактів з допомогою відео та фотоматеріалів. Так, зокрема, ще кілька років тому у ФРН на різні інфраструктурні об'єкти й рухомий склад Німецької залізниці було нанесено понад 14 тис. графіті, вартість робіт із видалення яких становила понад 7 млн євро. З метою вдосконалення методів боротьби з правопорушниками, патрулювання мостів, підстанцій та інших об'єктів залізничної інфраструктури, виявлення й фіксації заподіювачів шкоди було прийнято рішення використовувати дрони [4, с. 73].

Шостий напрям – використання під час досудового розслідування. Сферами використання БПЛА є, по-перше, тактичні операції розкриття злочинів «за гарячими слідами»; по-друге, виготовлення 2D схем та інших картографічних додатків до протоколів огляду та інших слідчих (розшукових) дій, виготовлення аерофотоілюстрацій та матеріалів аеровідеозйомки; по-третє, обстеження об'єктів перед проведенням та відеоконтроль за об'єктами під час проведення обшуків. Типовим є використання безпілотних аеротехнологій при огляді місць вибухів, пожеж, ДТП, авіатрощ. Польські колеги підтвердили ефективність роботи БПЛА при здійсненні фотографування важко доступних прибережних ліній та русла рік [5, с. 37]. За даними американських колег, два дрони навіть можуть сформувати 3D модель місця події [1]. Крім того, науковці працюють над розробкою технологій використання БПЛА під час розслідування окремих видів кримінальних правопорушень [6; 7].

Безумовно, перелік вищевказаних напрямів не можна вважати вичерпним, адже щодня технології вдосконалюються. Перешкодами на шляху до широкого впровадження безпілотних аеротехнологій може стати брак фінансування відповідних програм та брак досвіду у потенційних користувачів. З іншого боку для оптимістичного прогнозу дає підстави той факт, що Україна є

одним із світових лідерів на ринку розробників БПЛА, тож можна сподіватися, що з часом картографічні додатки та аерозйомка стануть рутинним елементом роботи кожного відділу поліції.

1. Rice S. 10 Ways That Police Use Drones To Protect And Serve. URL: https://www.forbes.com/sites/stephenrice1/2019/10/07/10-ways-that-police-use-drones-to-protect-and-serve/#5dd8e1616580.
2. Hearing on «Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?» Before the Subcommittee on Oversight, Investigations, and Management of the U.S. House of Representatives, Committee on Homeland Security. Washington: Cannon House Office Building, 2012. 10 p.
3. Микитюк, М. А. Роль та місце безпілотних літальних апаратів при забезпеченні безпеки осіб під час проведення масових заходів. Scientific Notes of Lviv University of Business and Law. 2018. № 18. С. 41–47. URL: https://nzlubp.org.ua/index.php/journal/article/view/33/.
4. Білоус В. В. Безпілотні літальні апарати: інтегрованість у життєдіяльність суспільства й держави та використання в криміналістичній практиці. Науковий вісник Херсонського державного університету. 2016. Випуск 4. Том 2. С. 72–77.
5. Rusek M. Dron na oględzinach. Problemy kryminalistyki. 2016. 293 (3). S. 34–39.
6. Атаманенко Ю. Ю. Геоінформаційна технологія реєстрації та картографування дорожньо-транспортних пригод з використанням безпілотних літальних апаратів. Дис. на здобуття наук. ступеня канд. техн. наук 05.24.01. ДВНЗ «Криворізький національний університет»; Київський національний університет будівництва і архітектури; МОН України. Київ, 2018. 178 с.
7. Спасенко К. О. Застосування аерофотозйомки в огляді місця події в разі розслідування порушень правил безпеки під час виконання робіт з підвищеною небезпекою. Порівняльно-аналітичне право. 2018. № 3. С. 290–292. URL: http://pap.in.ua/3_2018/83.pdf.

Використання еволюційних алгоритмів для автоматизованого генерування віршових творів

Загайний Богдан Миколайович

здобувач вищої освіти
Національного університету «Львівська політехніка»

Грицюк Юрій Іванович,

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

Вступ. На сьогодні інформаційні технології вже не тільки замінили механічну роботу людини, а й починають вирішувати більш творчі завдання, такі як створення музикальних композицій, компонування відео, тощо. Написання поезії можна віднести до тих творчих завдань, куди штучний інтелект ще не дійшов повною мірою, але уже на підході, оскільки має всі технічні можливості, щоб опанувати і цей вид діяльності. На даний момент вже існують програмні засоби для пошуку рими, визначення віршового розміру, які допомагають творчим особистостям у написанні віршів.

Відповідне ПЗ для генерування віршових творів відкрило би нові можливості для сфери шоу бізнесу, наприклад, підготовки пісень. Написання текстів пісень займає багато часу та вимагає творчої роботи як поетів, так і музикантів. Доволі часто пісні з текстами без особливого змісту стають успішними через відсутність складних сюжетів і легкість їхнього сприйняття. Саме такі тексти змогла б продукувати програма, використовуючи для цього еволюційний алгоритм, який би автоматизував процес створення віршових творів із логічним змістом. Звісно, програма не може повністю побудувати зміст твору так, як це робить справжній митець, тому її основне завдання полягатиме в побудові логічно зв’язаних словосполучень, котрі будуть дотримуватися приблизно одного стилю та форми.

Одним з підходів до вирішення цієї проблеми є розроблення адекватного алгоритму, який на підставі проаналізованих текстів і дослідження їхнього змісту буде створювати нові тексти. Приблизно так само працює і підсвідомість людини: насправді те, що людина вважає виявом своєї творчості, є нічим іншим, як синтезом попереднього аналізу прочитаних, почутих чи побачених матеріалів. «Усе нове – це добре забуте старе».

1. Стан проблеми дослідження. Віршований твір – це зв'язана і послідовна сукупність слів, які розподілені по рядах так, що вони слідуватимуть певним законам римування. Такі твори найчастіше використовують в літературі та музиці. В літературі віршові твори зазвичай виступають у вигляді віршів, поем, сонет та інших літературних віршових форм.

Автоматизоване генерування віршових творів на сьогодні ще не зовсім є поширеною практикою, але вже існують певні аналоги сучасного ПЗ, які реалізують це завдання. Методи, за якими працюють ці програми, є різними, тому й створюють тексти різної якості залежно від складності алгоритму, закладеного в програму. Загалом, методи програмного створення віршових творів поділяють на чотири основні категорії [1]: на підставі шаблонів; генерування та тестування; еволюційні алгоритми; на підставі конкретних випадків.

Зупинимось дещо детальніше на еволюційних алгоритмах. Їхня робота ґрунтується на виконанні еволюційних обчислень, реалізованих у вигляді нейронної мережі, попередньо навченої на даних, отриманих від людських тестувальників. Важливим принципом цього алгоритму є прийняття реального процесу написання людської поезії за взірець, з якого створюватиметься інтуїція комп'ютерної системи. Як відправну точку еволюційний алгоритм використовує дуже проникливий та інтуїтивний опис творчого процесу створення поезії. На підставі цього опису представлена загальна його архітектура, яка має декілька генераторних модулів, які створюють певну кількість творів-кандидатів і модифікують їх у наступних ітераціях оброблення текстів. Також ця архітектура має декілька модулів оцінювання, які вибирають твір з найвищим рейтингом, базу даних, у якій

зберігаються претенденти, лексикографічний аналізатор, концептуальну та синтаксичну бази знань. Цікава особливість цієї архітектури полягає в тому, що модулі оцінювання організовані у два рівні – нижній, де відбувається лексичне, граматичне та ритмічне оцінювання кожного варіанту твору і вища, що відповідає за оцінювання логіки та змісту твору [2].

Внаслідок синтезу зазначених вище методів програмного створення віршових творів [3, 4, 5] було розроблено ПЗ для автоматизованого їх написання з використання еволюційних алгоритмів. Очікувані наукові результати направлені на вирішення проблеми програмної підготовки логічно зв'язаних словесних структур та побудови з них віршових творів шляхом оброблення даних нейронною мережею.

З технічної точки зору програмний продукт передбачає систему із чотирьох основних елементів – базу даних, нейронної мережі, серверу та клієнта. Клієнтська частина безпосередньо взаємодіє із користувачем, приймає вхідні дані та видає результати роботи ПЗ. Серверна частина приймає дані від клієнтської, формує їх для подальшого оброблення їх нейронною мережею, взаємодіє із базою даних, отримує результати роботи нейронної мережі та надсилає їх до клієнтської частини. Нейронна мережа обробляє великі масиви даних, які зберігаються у базі даних, результатом оброблення яких є віршові твори, які подаються до серверної частини для подальшої передачі користувачеві.

Як було зазначено в розд. 1, для реалізації логічної складової ПЗ було обрано поєднання еволюційного алгоритму та методу на підставі конкретних випадків. Їхнє поєднання дає змогу досягти найкращих результатів у створенні віршових творів, оскільки еволюційний алгоритм має на увазі реалізацію штучного інтелекту, який буде працювати подібно до того, як це робить людина. Дослідження процесу створення людиною віршів або текстів пісень показали [2], що людський мозок аналізує та запам'ятовує попередньо прочитані або почуті вірші та тексти пісень, які слова в них найчастіше вживаються та загальні настрої, які панують в цих творах. Базуючись на цих даних, під час творчого процесу написання лірики, мозок «виштовхує»

здобуті перед тим знання та знаходить їм унікальні застосування. Саме для того, щоб реалізувати аналітичну частину роботи мозку було вибрано метод на підставі конкретних випадків, який зберігає оригінали готових творів і використовує їх для створення нових. Відмінність від стандартного методу полягає в тому, що зберігатися будуть не цілі твори і навіть не їх частини, а зв'язки між словами у творах.

Для реалізації еволюційного алгоритму розроблено нейронну мережу (рис. 1), яка має аналізувати запропоновані користувачем твори та визначати слова, які найчастіше трапляються разом. Враховуючи частоту цих слів і їхню приналежність до певних змістових груп, нейронна мережа має створювати послідовність слів, яка буде логічно зв'язаною завдяки попередньо отриманим результатам.

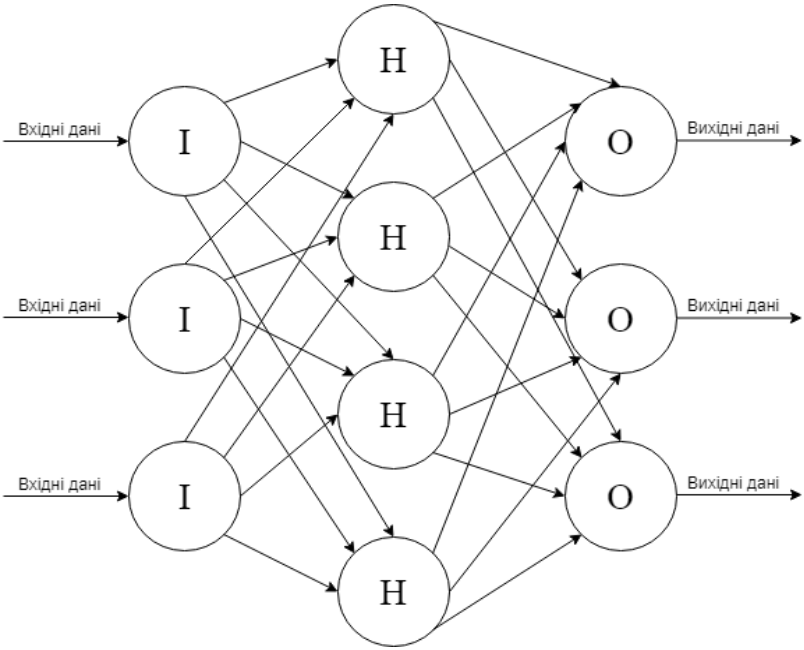

Рис. 1. Схема нейронної мережі

На рис. 1 показано базову схему нейронної мережі, де I – вхідний нейрон (Input), H – прихований нейрон (Hidden), O – вихідний

нейрон (Output). Вихідні дані визначаються функцією активації адекватності

$H_{\text{output}} = F_{\text{act}}(H_{\text{input}})$.

Ця функція здійснює перетворення вхідного сигналу в вихідний сигнал шляхом нормалізації вхідних даних. Залежно від потреб у різних прихованих нейронів функції активації можуть бути різні:

- лінійна функція: $F_{act}(x) = x$;
- сигмоїдна: $F_{act}(x) = \frac{1}{1+e^{-x}}$;
- гіперболічний тангенс: $F_{act}(x) = \frac{e^{2x}-1}{e^{2x}+1}$.

Лінійна функція не є достатньо ефективною, а гіперболічний тангенс потрібно застосовувати тоді, коли присутні як позитивні, так і негативні значення. Тому в роботі розробленого алгоритму використано сигмоїдну функцію активації.

Еволюційний алгоритм є багатоточковим стохастичним алгоритмом пошуку [2], тобто це форма евристичного пошуку, яка одночасно досліджує декілька точок у просторі пошуку і стохастично переміщається у пошуковому просторі, щоб запобігти досягненню локальних максимумів. Генетичний алгоритм – одна з реалізацій еволюційних алгоритмів для задач оптимізації шляхом послідовного підбору, комбінування та варіації шуканих параметрів з використанням механізмів, що нагадують біологічну еволюцію. Його особливістю є акцент на використанні операторів схрещення, який виконує операцію рекомбінацію рішень-кандидатів, роль якої аналогічна ролі схрещення в живій природі і мутації, який виводить нові властивості рішень-кандидатів після їхньої перевірки та оцінки.

2. Результати роботи ПЗ. Отже, продуктом проекту є веб-додаток, що складається із клієнтської частини (веб-сторінки) та серверної частини. Навігацію по клієнтській частині ПЗ було спроектовано якомога простішою у використанні, щоб забезпечити користувачам можливість перейти до необхідної їм сторінки

без зайвих дій. Навігація по сторінках не порушує «правило трьох кліків», тобто на будь-яку сторінку можна потрапити не більше, ніж трьома переходами.

Потрапивши на головну сторінку (рис. 2), користувач має можливість авторизуватися, зареєструватися або переглянути інформацію про програму. Після авторизації користувач побачить свою особисту сторінку, з якої він матиме змогу перейти до сторінок де можна генерувати віршові твори, аналізувати твори або переглянути інформацію про роботу нейронної мережі.

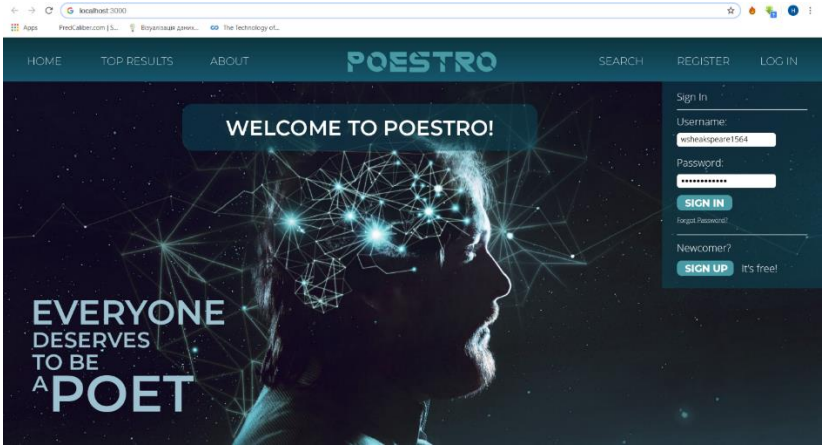

Рис. 2. Головна сторінка веб-сайту

Після успішної авторизації користувач потрапляє на свою особисту сторінку, звідки він може подавати свої тексти для аналізу програмою, або перейти на сторінку генерування віршових творів. Робота зі сторінкою аналізу текстів дуже проста: користувач просто вносить текст та вказує, чи даний текст є прозою, чи віршем. За бажанням користувач може задати параметри тексту, а саме настрій та ключові слова (рис. 3).

На сторінці «генерування» користувачу надається необхідний інтерфейс для генерування віршових творів. Користувач може задати вхідні параметри віршового твору, або довірити це програмі, яка згенерує ці параметри відповідно до проаналізованих творів. Користувач може обрати два режими генерування

творів: покроковий та повний. Покроковий режим генерує рядок за рядком, а користувач погоджує або вносить правки у цей рядок. Отже, нейронна мережа буде краще натренована, оскільки залучається еволюційний алгоритм, який вносить правки у відповідні обчислення. Повний режим генерує весь вірш за однин раз, а правки, які були внесені користувачем тренують нейронну мережу шляхом зворотного поширення.

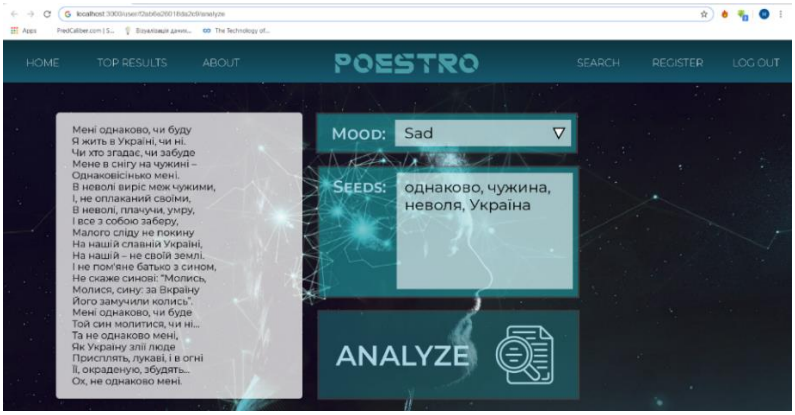

Рис. 3. Сторінка аналізу текстів

1. Gervas, P. (2002). Exploring Quantitative Evaluations of the Creativity of Automatic Poets. 15th European Conference on Artificial Intelligence, (pp. 24–31). http://nil.fdi.ucm.es/sites /default/files/GervasECAIws2002.pdf
2. Manurung, H. (2004). An evolutionary algorithm approach to poetry generation. Doctoral Dissertation for Technical Sciences. University of Edinburgh. College of Science and En., 367 p.
3. Poem Generator. (2019). Masterpiece Generator. https://www.poem-generator.org.uk/.
4. Стихоробот. (2019). Neogranka.ru. http://neogranka.ru /generator_stihov.html.
5. Oliviera, H. G. (2016). PoeTryMe: a versatile platform for poetry generation. CISUC, University of Coimbra, Portugal. https://eden.dei.uc.pt/~hroliv/pubs/GoncaloOliveira2012_c3gi _CRC.pdf.

Використання програмного забезпечення та пристроїв (гаджетів) в службовій діяльності НПУ під час реєстрації повідомлень про правопорушення та реагування на останні нарядами поліції

Кобелька Дмитро Михайлович

начальник управління організаційно-аналітичного забезпечення та оперативного реагування ГУ НП у Львівській області

Шаркадій Петро Іванович

інженер-програміст організаційно-аналітичного відділу управління організаційно-аналітичного забезпечення та оперативного реагування ГУ НП у Львівській області

На сьогоднішній день в службовій діяльності Національної поліції в системі реєстрації та реагування на повідомлення громадян про скоєння правопорушень використовується наступне програмне забезпечення та технічні засоби:

- телефонний зв'язок по спецлінії служби «102» організовано шляхом впровадження програмно-апаратного комплексу Call-Way, який автоматично визначає номера телефонів заявників, записує звукове повідомлення;
- оператор відділу служби «102» заповнює електронну картку де вказує інформацію про подію, кваліфікацію попередню та дані заявника, відмічає місце події на ГІС карті;
- звуковий файл телефонного повідомлення автоматично прикріпляється до електронної картки «102»;
- диспетчер СЦ УОАЗОР ГУНП отримавши повідомлення «102» призначає завдання нарядам поліції шляхом передачі останнього на логістичний пристрій;
- поліцейський після прийняття рішення на місці події зазначає в електронному рапорті всю необхідну інформацію та фото;
- узагальнена інформація попадає до електронного рапорту на АРМ чергового ТВП, який може списати матеріали

ЄО за спрощеною системою (за відсутності відомостей про скоєння кримінального правопорушення»;

- реєстрація ЄО (призначення номера ЄО) відбувається в автоматичному режимі;
- у всій системі реагування на повідомлення та контролю за діями нарядів допомагає геоінформаційна система (далі – ГІС) карта на котрій відображаються в онлайн місце скоєння правопорушення, місце знаходження нарядів поліції, встановлення камер відеоспостереження, ТВП, медустанов, шкіл, ломбардів та інших об'єктів необхідних НПУ для виконання службових завдань. Відомості про будь які об'єкти можна нанести на карту безпосередньо працівникам.

В свою чергу в ІПНП реалізовано наступні підсистеми:

Розшук дітей:

за допомогою створення електронної картки про безвісті зниклу неповнолітню особу за допомогою можливостей мобільного оператора на визначену диспетчером площу всім громадянам розсилаються push-повідомлення на мобільні гаджети (смартфони) із орієнтуванням (розшук дітей).

ГАРПУН:

системою відеоаналітики з камер спостереження встановлених на території м.Львова та Львівської області інформація про визначені номерні знаки автотранспорту передається до ІПНП потім порівнюється із інформацією про зареєстровані автомобілі та розшук останніх. При виявлені за встановленим номерним знаком факту викраденої а/м створюється автоматично електронне повідомлення (орієнтування), яке надходить на АРМ диспетчера, а при значній близькості безпосередньо на логістичний пристрій наряду поліції.

MyPol:

мобільний додаток за допомогою якого здійснюється безпосереднє інформування диспетчера СЦ УОАЗОР ГУНП про скоєння кримінального або адміністративного правопорушення,

а також негайного повідомлення про загрозу життю та здоров'ю громадян (шляхом натискання тривожної кнопки «SOS» на інтерфейсі програми). Даний додаток дає можливість без спілкування з операторами служби «102» по телефону передати повідомлення про правопорушення на АРМ диспетчера та в подальшому на планшет наряду поліції, який прибуде на місце пригоди. Також є можливість додатком сфотографувати місце скоєння правопорушення що дасть допомогу під час розгляду звернення громадян.

Система відеоспостереження:

з метою забезпечення публічного порядку та профілактики злочинності працівниками НПУ широко використовуються можливості системи відеоспостереження та відеоаналітики. В СЦ УОАЗОР розгорнуто АРМ системи відеоспостереження (відеостіна, та робоче місце оператора) на якому в цілодобовому режимі працівники поліції забезпечують моніторинг ситуації в м. Львові, Львівській області та автошляхах міжнародного значення. В даній системі із врахуванням різних власників та провайдерів використовується різне програмне забезпечення (у Львівській області Milestone, Hikvision, ISS) в наслідок чого приходиться користуватись різними віддаленими робочими столами із різним програмним забезпеченням. На сьогоднішній день впроваджуються в основному наступні аналітичні можливості систем відеоспостереження: визначення номерних знаків автотранспорту, обличчя людини, пересікання умовної лінії, виявлення залишеного предмету, виявлення групи осіб (бійка) та інше.

Пульт моніторингу місця перебування осіб відносно яких було обрано запобіжний захід домашній арешт із застосуванням електронних засобів контролю:

за допомогою програмного забезпечення та електронних засобів контролю працівники поліції здійснюють цілодобове спостереження за поведінкою осіб до яких застосовано запобіжний захід у вигляді домашнього арешту із застосуванням ЄЗК. В даному програмному комплексі на карті визначається приписна зона контролю та час перебування особи під наглядом. При

порушені приписної зони або інших технічних порушеннях роботи системи, надходить сигнал тривоги та на місце події скеровується наряд поліції.

Вся вищевказана діяльність працівників поліції супроводжується роботою із звітами, таблицями та базами даних (SQL), в свою чергу формуються службові документи із використанням офісних програм, та інших. В свою чергу слід вказати що широко в діяльності НПУ використовуються мобільні додатки, месенджери, програмні комплекси для відеоконференції, відеострімінгу, цифрові радіостанції IP телефонія та інше.

Роль інформаційного менеджменту в поліції

Кулешник Ярема Федорович,

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних 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

Дослідження та міжнародний досвід показують, що близько 75 % процесів розкриття злочинів, складних до розкриття, чи не дуже, місцевих чи міжнародних, де б вони не були, відбуваються, однаково.

Професіонали всього світу, спираючись на досвід провадження, виділяють в управлінні інформацією наступні важливі складові частини: спільний доступ до інформації, якість та безпека інформації.

Спільний доступ до інформації

Зростаюча складність ситуацій для забезпечення співпраці вимагає від поліцейських сил та інших підрозділів ефективнішого обміну актуальною інформацією. Ефективний обмін даними вимагає достатнього рівня взаємодії між системами та підрозділами. Загалом, існує три категорії сумісності:

- технічна сумісність – системи здатні обмінюватися даними;
- сумісність даних – системи здатні автоматично обробляти та відображати дані, що обмінюються між ними;
- взаємодія оперативних підрозділів – підрозділи здатні ефективно використовувати спільну інформацію.

Досягнення та підтримка сумісності між системами та підрозділами вимагає загальних процесів управління, які розгортають, застосовують та керують стандартами сумісності. Практика свідчить, що для забезпечення ефективного обміну даними архітектура управління інформацією повинна включати чотири компоненти:

Технічна сумісність – інфраструктури, мережеві рішення та протоколи зв'язку, які дозволяють системам спілкуватися та приймати дані. Високий рівень технічної сумісності дозволяє системам ефективно та надійно обмінюватися великими обсягами даних, а також підвищує гнучкість системи. Технічна сумісність є найнижчим рівнем сумісності, оскільки вона включає лише обмін даними, а не обробку або показ цих даних.

Сумісність даних – стандарти даних, що дозволяють автоматично обробляти та відображати дані та інформацію, передані між системами. Високий рівень взаємодії даних вимагає, щоб стандартні моделі даних забезпечували послідовну структурування даних, а загальні онтології, щоб забезпечити послідовність визначення понять і зв'язків між поняттями. Взаємодія оперативних даних дозволяє системам точно інтерпретувати зміст і значення даних і інформації, що передаються між ними.

Взаємодія операційних процесів – спільні робочі процеси, спільні стандарти введення даних та спільні інформаційні потоки, що дозволяють організаціям використовувати спільну інформацію для прийняття рішень та вдосконалення процесів адміністративного управління. Взаємодія операційних процесів дає змогу організаціям максимізувати значення технічної та інформаційної сумісності даних.

Управління взаємодією – функція, що працює в рамках організаційних та інформаційних накопичувачів для розробки, управління та застосування загальних стандартів, протоколів та процесів, забезпечення технічної сумісності процесів та даних. Ефективне управління взаємодією збільшує широту та глибину обміну даними, збільшуючи кількість інформаційних та організаційних накопичувачів, здатних ділитися інформацією, та рівень взаємодії між цими накопичувачами.

Якість інформації

Поліцейські структури повинні керувати дуже великими обсягами даних із широкого кола джерел. Забезпечення якості цих даних є критично важливим. Дані високої якості є значущими, точними, внутрішньо послідовними і можуть використовуватися за призначенням. Цілісність даних – достовірність, точність та надійність даних після їх зберігання, передачі, вилучення чи обробки – має значний вплив на якість даних. Дані низької якості можуть підірвати ефективність використання ІТ-систем підрозділів та обміну даними. Як результат, дуже важливо, щоб поліцейські сили підтримували та покращували якість даних. Вони можуть це зробити, застосовуючи навчальні програми, комунікаційні стратегії та критерії ефективності, які заохочують точне і повне введення даних, а також генерують рішення, що запобігають, виявляють та виправляють помилки даних та зберігають цілісність даних.

Для підтримки та покращення якості даних архітектура управління інформацією повинна включати чотири компоненти:

Введення даних – політика, навчання та програми, що мінімізують помилки, пов'язані з використанням даних, у точці введення та забезпечують точне та повне введення даних. Розгортаючи зручні для користувача, інтелектуальні та мобільні рішення для введення даних, можна підвищити ефективність введення даних, одночасно покращуючи якість даних.

Виправлення помилок та перевірка даних – ручні та автоматичні процеси, що виявляють та виправляють помилки в даних, та правила перевірки, що підтверджують відповідність даних специфікаціям формату, якості, цілісності, точності та структури. Забезпечення поширених процесів виправлення помилок та правил перевірки даних у системах та підрозділах, які обмінюються інформацією, підвищує якість даних за рахунок зменшення помилок у даних, переданих між системами.

Сертифікація системи та інтерфейсу – ролі, процеси та рішення, які підтверджують відповідність систем та інтерфейсів

специфікаціям, визначеним регуляторами, організаціями управління інформаційними технологіями та організаціями з розвитку стандартів (SDO). Забезпечення відповідності систем та інтерфейсів загальним технічним умовам підтримує цілісність даних під час їх обробки та передачі між сумісними системами.

Стандарти, керовані архітектурою та управлінням стандартами – системні архітектури, які використовують загальні стандарти для збору, зберігання та обробки даних, тим самим сприяючи високому рівню якості даних завдяки подібній обробці даних у компонентних системах. Управління стандартами включає ролі, процеси та рішення, які розробляють, керують та застосовують загальні технічні, комунікаційні, повідомлення та стандарти даних. Управління стандартами дозволяє підсистемам обмінюватися високоякісною інформацією.

Безпека інформації

Запобігання корупції даних та, що ще важливіше, несанкціонований доступ до даних є критичними питаннями для поліції, оскільки вони зберігають та керують великими обсягами конфіденційної інформації. Безпека даних повинна бути пріоритетним завданням поліції, оскільки порушення даних значною мірою порушує довіру та впевненість у суспільстві, є головним питанням існування, може мати згубний вплив на ефективність роботи, а в деяких випадках призводить до загибелі людей. Забезпечення безпеки даних вимагає, щоб поліцейські підрозділи розробляли політику, процеси, функції та рішення, які активно керують ризиками безпеки, ефективно ідентифікують і визначають пріоритети загроз та швидко усувають уразливості.

Для забезпечення безпеки даних архітектури управління інформацією повинні включати чотири компоненти:

Політика безпеки та обробка даних – політика, яка мінімізує ризики щодо захисту інформації та запобігає несанкціонованому доступу до інформації, заохочуючи користувачів бути обізнаними щодо безпеки. Ефективні методи безпеки та обробки даних включають:

- Безпечне збирання, зберігання та обмін даними за допомогою відповідних технологій безпеки, таких як зашифровані пристрої зберігання даних та захищені канали зв'язку.
- Мінімізація ризику втрати чи неправильного використання даних, підтримуючи ефективність контролю доступу, наприклад, не обмінюючись паролями та гарантуючи, що паролі відповідають певним критеріям.
- Активно визначати та мінімізувати ризики безпеки та конфіденційності.
- Повідомлення про порушення безпеки та несанкціоноване або неналежне використання інформації.
- Обмеження фізичного доступу до обладнання (включаючи ноутбуки, настільні ПК, мобільні пристрої та мобільні телефони), які зберігають або дозволяють користувачам отримувати доступ до конфіденційних даних.
- Навчання інших користувачів підвищувати рівень обізнаності щодо ризику безпеки та конфіденційності даних та заохочувати їх усвідомлювати безпеку.

Аудит безпеки IT – ручні та автоматичні процеси, які перевіряють та оцінюють ефективність заходів інформаційної безпеки IT-систем. Аудити безпеки IT забезпечують належну захист даних від несанкціонованого доступу, виявлені всі відповідні загрози та вразливості безпеці та правильність налаштування процесів обробки даних для мінімізації ризиків для безпеки. Аудит безпеки IT може проводитися третьою стороною і, як правило, включає низку компонентів. Серед них: перевірка відповідності, сертифікація стандартів безпеки, оцінки безпеки, тестування на проникнення та перевірка обізнаності користувачів.

Цілісність мережі – рішення та функції, які дозволяють мережам підтримувати очікувану функціональність, продуктивність та доступність послуги, незважаючи на несподівані події, такі як загрози безпеці та високі вимоги. Високий рівень цілісності мережі забезпечує доступність процесів і служб, що підтримують безпеку даних по всій мережі. Рішення цілісності

мережі повинні автоматично виявляти та вирішувати загрози безпеці та небажаний мережевий трафік, зберігати пропускну здатність мережі, керуючи та визначаючи пріоритетність законного трафіку та генеруючи звіти про ефективність мережі, щоб допомогти адміністраторам мережі більш ефективно керувати мережами.

Профілактика системи – періодичні або тривалі процеси, які дозволяють за рахунок адекватної оцінки архітектури безпеки, видалення вразливих та непотрібних служб і додатків та оновлення конфігурації безпеки і контролю доступу значно знизити ризики безпеки.

---

1. Manuel Sanchez LopezPolice Centre of Excellence Lead manuel.sanchez.lopez@accenture.com
2. James Slessor United Kingdom Policing Lead james.w.slessor@accenture.com

Правові аспекти формування політики інформаційної безпеки в інформаційних системах

Лозинський Ігор Андрійович

здобувач вищої освіти
Львівського державного університету внутрішніх справ

Рудий Тарас Володимирович

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

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

За своєю сутністю нормативно-правові чинники становлять правову основу організаційно-технічних принципів захисту інформації, формують вимоги до способів та засобів захисту інформаційних активів у ІС і накладають обов'язкові вимоги, згідно з чинним законодавством, невиконання яких може стати причиною несанкціонованого витоку інформації, що тягне за собою адміністративну та кримінальну відповідальність [1].

Структуру нормативно-правових актів України у галузі інформаційної безпеки, обов'язкових до виконання, на рівні правової доктрини можна подати наступним чином: Конституція України; Закони України; укази та розпорядження Президента України; постанови та розпорядження Кабінету Міністрів України; нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України;

міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість виконання яких надана Верховною Радою України [2].

Політика інформаційної безпеки (ПІБ) документально описує і регламентує систему управління інформаційною безпекою (СУІБ) в ІС, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів [3].

Метою ПІБ є впровадження та ефективне управління системою забезпечення інформаційної безпеки (ІБ), спрямованої на захист інформаційних активів, забезпечення безперервного функціонування сервісів ІС, мінімізування ризиків.

ПІБ розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для зловмисних діянь у разі несанкціонованого доступу.

Аналіз матеріалів стосовно проблеми безпеки інформаційних активів ІС дає змогу виявити недоліки у методології розроблення ПІБ систем захисту, які суттєво впливають на ефективність їх функціонування [3, 4]. Відзначимо основні з цих недоліків: ПІБ системи захисту інформаційних активів ІС не враховує динаміки зміни загроз; недостатній рівень стійкості системи захисту ІС до відмов та відновлення після збоїв; необхідність зосередження ресурсів підтримки систем безпеки інформаційних активів ІС на найбільш критичних напрямах; відсутність ефективних методик попереднього оцінювання ефективності системи безпеки інформаційних активів ІС; ігнорування нормативно-правовими аспектами та вимогами міжнародних стандартів у галузі ІБ при проектуванні надійної системи захисту.

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми впливами, елементарною необізнаністю працівників у галузі інформаційних технологій (ІТ) необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІІБ), яка є базовою частиною загальної СУІБ. СУІІБ дозволяє виявляти, враховувати, реагувати

і аналізувати події та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог міжнародних стандартів і галузевих норм [4].

Цілі, які ставлять перед СУІБ є такими: відновлення штатної роботи сервісів у найкоротші терміни; зведення до мінімуму вплив інцидентів на функціонування ІС забезпечення злагодженого; оброблення всіх інцидентів і запитів обслуговування; зосередження ресурсів підтримки ІБ на найбільш важливих напрямах; надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Для реалізування СУІБ необхідно виконати такі роботи [5]:

- надати ресурси для розроблення та впровадження системи СУІБ;
- здійснити фахову підготованість працівників;
- визначити область функціонування СУІБ;
- розробити комплекс процесів СУІБ;
- впровадити процеси СУІБ та інтегрувати їх з уже функціонуючими процесами, такими як інвентаризування активів, аналіз ризиків та оцінювання ефективності;
- розробити архітектуру і комплекс програмно-технічних засобів з автоматизації процесів СУІБ і моніторингу подій.

Для оброблення подій та інцидентів ІБ необхідно організувати процес реагування на інциденти [4, 5]. Основними задачами процесу реагування на інциденти інформаційної безпеки є:

- забезпечення координування реагування на інцидент;
- підтвердження/спростування факту виникнення інциденту;
- забезпечення збереження і цілісності доказів виникнення інциденту, створення умов для накопичення і зберігання точної інформації про інциденти, що мали місце;
- мінімізування порушень порядку роботи і пошкодження даних, відновлення в найкоротші терміни працездатності ІС при її порушенні у результаті інциденту;

- мінімізування наслідків порушення конфіденційності, цілісності і доступності інформації у ІС;
- створення умов для порушення цивільної або кримінальної справи проти зловмисників;
- захист активів ІС;
- швидке виявлення та/або попередження подібних інцидентів у майбутньому.

Як висновок відзначимо, що аналіз нормативно-правових актів України в інформаційній сфері свідчить, що без подальшого розвитку правової бази забезпечення захисту інформаційних активів спеціалізованих ІС може втратити свою ефективність.

---

1. 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. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
2. Рудий Т. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні / Т. В. Рудий, В. В. Сеник, А. Т. Рудий, С.В. Сеник / Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів : ЛьвДУВС, 2018. – Вип. 1. – С. 283-301.
3. Рудий Т. В. Захист спеціалізованих комп'ютерних мереж підрозділів Національної поліції України на основі адаптивного підходу / Т. В. Рудий, Я. Ф. Кулешник, І. С. Піцюра // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі : збірник наукових статей за матеріалами доповідей науково-практичної конференції 23 грудня 2016 року. – Львів : ЛьвДУВС, 2016. – С. 101-108.
4. Середа В.В. Нормативно-правові аспекти застосування міжнародних стандартів в системі управління безпекою підприємств / В.В. Середа, 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.

5. Sereda, V., Zhyvko, Z., Balynska, O., Rudyi, T. (2019, July 15). The Organizational Principles of Information Protection Management System Realization. (Z. Cekerevac, Ed.) MEST Journal, 7(2), 73-78. doi:10.12709/mest.07.07.02.09.

Автоматизація методу визначення реальних розмірів об’єктів на зображенні із застосуванням референтного об’єкта

Лукащук Богдан Сергійович

аспірант кафедри інформаційних технологій Національного лісотехнічного університету України

Вступ. Визначення геометричних характеристик об’єктів на цифровому зображенні є традиційною задачею комп’ютерного бачення, а також, – необхідною складовою для вирішення більш комплексних задач. Першим кроком є визначення відповідності розміру об’єкту на зображенні (у пікселях), до реального.

В медичній сфері, однією із задач, де ця проблема постає гостро, є визначення геометричних характеристик областей рани на зображенні. Точна оцінка та вимірювання ран є важливим аспектом у визначенні ефективності лікування[1]. Є традиційні методи, які вимагають прямої взаємодії:

- просте вимірювання: найпростіший і найдешевший метод – обчислити площу поверхні рани, вимірявши її лінійні розміри рулеткою або лінійкою. Однак цей двовимірний метод передбачає, що рана має просту геометричну форму поверхні, наприклад прямокутник чи еліпс [2]. Розміри отримуються накладанням лінійки; При складних формах значно зростає похибка
- обведення рани: ще одним способом для вимірювання є обведення рани, при якому ручка використовується для виділення контуру безпосередньо на стерильній прозорій плівці [2].

До автоматизованих методів можна віднести використання сканерів, пристроїв на основі однієї або декількох камер [3][4] а, також, аналіз цифрових зображень (фотографій) із ранами. Одним із традиційних способів автоматизації розрахунку площі рани, є обведення контурів на фотографії, з подальшим розрахунком площі чисельними методами.

Оскільки контактний метод із використанням лінійки є дуже поширеним, наявна велика кількість цифрових зображень ран із прикладеною лінійкою, яку зручно використовувати в якості референтного об’єкту при визначенні реальних розмірів.

Методи і матеріали

Необхідно виділити пункти, які випливають із специфіки задачі:

- площа реальних об’єктів на фотографіях не є великою
- фотографії зроблені із відносно малої відстані (рідко дальше 30-ти сантиметрів)
- приймається спрощення, що об’єкти на зображенні знаходяться на одній площині один відносно одного (ті, геометричні розміри яких потрібно визначати, розміщенням фонових об’єктів можна знехтувати)
- на даному етапі нехтується дисторсією (викривленням) зображення

На рис.1. вхідні дані – типове цифрове зображення із раною та лінійкою, прикладеною біля неї.

Рис.1. Зображення рани із лінійкою в ролі референтного об’єкту

Для подальшого вимірювання, використовується програмне забезпечення, яке дозволяє отримати довжину референтного об’єкта в пікселях (лінійки, або однієї секції лінійки в даному

випадку). Відтак, за пропорцією можна отримати співвідношення кількість пікселів до не цифрових одиниць.

$$pixels\_per\_unit = px\_width / ut\_width, \quad [1],$$

де px_width – ширина об'єкту в пікселях, і ut_width- у реальних одиницях.

Виділення референтного об'єкту вручну може забирати час. Із зображення видно, що колір лінійної стрічки є близьким до білого і сильно контрастує порівняно із рештою об'єктів на зображенні. пришвидшити процес можна за допомогою автоматизації виділення референтного об'єкту, шляхом сегментації зображення. Варто виділити такі кроки:

- завантаження зображення
- переведення у відтінки сірого
- використання фільтру Гауса для усунення шумів
- використання алгоритму сегментації на основі виділення контурів
- виконання морфологічних операцій «розширення» (dilation) і «звуження» (erosion), для усунення отворів у контурах
- пошук найбільшого контуру, який в середньому заповнений білим кольором
- розрахунок кількості пікселів на реальні одиниці, задавши реальну довжину лінійки

В якості алгоритму виділення контурів, використовується ефективний алгоритм Кенні [5], який використовує градієнт зображення для пошуку границь та імплементує подвійну порогову фільтрацію.

Висновок. Автоматизація виділення референтного об'єкту для розрахунку реальних розмірів дозволяє прискорити процес і зменшити вплив людського фактору, проте не забирає повністю його, оскільки, довжина лінійки повинна бути введена людиною вручну. Описаний спосіб ефективно інтегрується у якості першого кроку у метод розрахунку геометричних характеристик конкретно раневої поверхні. Також варто звернути увагу на

методи і способи визначення реальних розмірів без використання референтного об'єкту, а також впровадження нормалізації зображення для уникнення ефектів викривлення.

1. Jansen S. The Evolving Field of Wound Measurement Techniques: A Literature Review [Електронний ресурс] / S. Jansen, K. Rachel. – 2016. – Режим доступу до ресурсу: https://www.woundsresearch.com/article/evolving-field-wound-measurement-techniques-literature-review.
2. Fette A. A clinimetric analysis of wound measurement tools [Електронний ресурс] / Andreas Fette // World Wide Wounds. – 2006. – Режим доступу до ресурсу: http://www.worldwidewounds.com/2006/january/Fette/Clinimetric-Analysis-Wound-Measurement-Tools.html.
3. Krouskop T. A noncontact wound measurement system [Електронний ресурс] / T. Krouskop, R. Baker, M. Wilson // Journal of Rehabilitation Research and Development. – 2002. – Режим доступу до ресурсу: https://www.rehab.research.va.gov/jour/02/39/3/pdf/krouskop.pdf
4. PHOTOGRAMMETRIC WOUND MEASUREMENTWITH A THREE-CAMERA VISION SYSTEM [Електронний ресурс] / S.Boersma, F. van den Heuvel, A. Cohen, R. Scholtens. – 2000. – Режим доступу до ресурсу : https://www.researchgate.net/publication/229044995_Photogrammetric_wound_measurement_with_a_three-camera_vision_system.
5. CANNY J. A Computational Approach to Edge Detection [Електронний ресурс] / JOHN CANNY. – 1986. – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.420.3300&rep=rep1&type=pdf.

Використання технології доповненої реальності для оцінки економічних ризиків функціонування підприємства

Лукащук Юрій Андрійович

аспірант кафедри автоматизованих систем управління технологічними процесами Національного університету «Львівська політехніка»

Четверта науково-технічна революція передбачає створення штучного інтелекту, зростання ролі механізмів, машин, загалом автоматизації, інформатизації та, зрештою, глобалізації у житті людства, вплив результатів інтелектуальної діяльності на якість життя. Дослідники здійснюють пошук механізмів розвитку та використання досягнень цієї революції на розвиток суспільства у всіх його проявах, у т.ч. і виробничій галузі. Доповнена реальність є одним з таких механізмів.

Доповнена реальність (AR) – технологія майбутнього, технологія, яка вирішує проблему когнітивного перевантаження, що виникає внаслідок перевищення можливостей людського мозку кількістю необхідних до виконання завдань. Вона містить величезний потенціал, оскільки переносить елементи з віртуального світу в реальний, доповнюючи речі, які людина може бачити, чути, відчувати. Вона здійснює доповнення фізичного світу за допомогою цифрових даних, яке забезпечується комп'ютерними пристроями в режимі реального часу. Доповнена реальність – змішана реальність, створювана за допомогою комп'ютера з використанням «доповнених» елементів сприйняття реальності, коли реальні об'єкти монтуються в поле сприйняття [1].

AR використовує середовище навколо людини та накладає поверх нього певну частинку віртуальної інформації, наприклад графіку, звуки та реакцію на дотики. Віртуальна інформація використовується як додатковий корисний інструмент, що забезпечує допомогу в повсякденній діяльності. Отже, доповнена реальність – поняття, яке описує процес доповнення існуючої

реальності віртуальним об’єктами, дозволяючи і допускаючи візуалізацію інформації. Комунікація з віртуальною реальністю виконується в режимі on-line, а для забезпечення необхідного ефекту необхідна лише вебкамера – зображення з якої буде доповнюватись віртуальним об’єктами. Це технологія накладення інформації в формі тексту, графіки, аудіо та інших віртуальних об’єктів на реальні об’єкти в режимі реального часу. Саме взаємодія обчислювальних пристроїв з картинкою реального світу відрізняє доповнену реальність від віртуальної.

Сфера застосування технології AR охоплює безпеку, рекламу і промо-акції, медицину, ігри, навчання, косметичну та машинобудівну галузі, текстильну індустрію, промисловість і т.п.

У галузі промисловості доповнена реальність дозволяє наочно продемонструвати те, що показати на реальних моделях неможливо. Наприклад, робочу гідроелектростанцію з докладним текстовим описом її роботи прямо в повітрі. При цьому, доповнена реальність не вимагає якогось особливого устаткування.

Актуальність впровадження технології доповненої реальності в виробничий процес полягає в тому, що використання такої новітньої системи безсумнівно збільшить мотивацію працівників, а також підвищить рівень засвоєння інформації за рахунок різноманітності і інтерактивності її візуального представлення. Водночас буде полегшена діагностика обладнання на підприємстві, що дасть можливість запобігти поломкам. А демонстрація обладнання та устаткування дозволить новим працівникам швидше оволодіти навиками роботи з ними.

Для впровадження технології AR здійснюється розробка відповідного програмного забезпечення. Одними з ефективних інструментів для створення додатків на базі технології доповненої реальності є платформа Vuforia. Крім якісного програмного продукту для ефективного функціонування промислового підприємства необхідна наявність зрозумілого, доступного у користуванні, яскравого інтерфейсу.

Зрештою, використання технології AR дозволяє здешевити весь цикл виробництва певного умовного продукту: від навчання та інструктажу персоналу, дизайну, монтажу, сервісу, організації та проведенні виставок і презентацій з демонстрацією цього продукту, логістичних витрат і т.п.

Крім того, застосування технології доповненої реальності, як інструменту зменшення когнітивних навантажень, дозволяє знизити вплив когнітивних спотворень на прийняття економічних рішень. Адже саме значна кількість когнітивних спотворень є визначальною у прийнятті рішень. Одним з універсальних (характерних для виробництв у будь-якій галузі) способів мінімізації економічних ризиків є здобуття додаткової інформації [2, с. 122]. Технологія AR сприяє всебічному отриманню, засвоєнню й обробці цієї інформації та своєчасному виявленню спотворень у сприйнятті. А, отже, як наслідок, запобігти прийняттю невірних, економічно необґрунтованих рішень. Таким чином, зменшується рівень економічних ризиків функціонування підприємства.

---

1. Іванова А. Технологии виртуальной и дополненной реальности: возможности и препятствия применения // Стратегические решения и риск-менеджмент / А. Іванова., 2018. 108 с. (3).
2. Економічний ризик: методи оцінки та управління [Текст] : навч. посібник / [Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін.] ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. Суми : ДВНЗ «УАБС НБУ», 2015. 208 с.

Проблеми ідентифікації суб'єкта при отриманні публічних послуг в електронному вигляді

Луців Іванна Іванівна

аспірантка кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

У даний час обмін інформацією в електронному вигляді набув глобального обсяг у всіх сферах життєдіяльності людства. Однак юридичний аспект легальності та легітимності електронного документообігу, на наш погляд відстає від швидкості впровадження в юридичний обіг.

Питання процесуальної допустимості та доказової сили електронних документів поки не достатньо розроблені, відповідно інформація, що міститься в електронних документах не є надійною та відповідним чином захищеною. У зв'язку з цим, слідом за вдосконаленням інформаційних технологій необхідно створювати законодавчу основу не тільки електронного документообігу, а й юридичного механізму захисту даних, що створюються та переданим електронним способом, удосконалювати юридичний статус електронного документа. В Україні законотворча робота в цьому напрямі ведеться досить активно. Позначена тематика не може бути нами розкрита без посилань на закон України від 5 жовтня 2017 року № 2155-VIII «Про електронні довірчі послуги» [1].

Наприклад, закон 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, кваліфіковану електронний підпис і власноручний підпис особи, від імені якого складено юридично значущий документ.

Електронний цифровий підпис є обов'язковим реквізитом електронного документа, вона служить захистом від підробки, яка використовується в процесі криптографічного перетворення інформації за допомогою закритого ключа електронного цифрового підпису та дозволяє ідентифікувати власника сертифіката ключа підпису, повинна підтверджувати справжність інформації в електронному документі, відсутність її спотворення.

Електронний підпис необхідна для оформлення та подачі різних заяв і документів через Інтернет портали для отримання публічних послуг. Якщо в законах і підзаконних актах, які вступили в силу до прийняття зазначеного закону, мова йде про застосування кваліфікованого електронного підпису. В інших випадках документи складаються та підписуються удосконаленим електронним підписом, виключення вказуються безпосередньо в законі, коли він прямо зобов'язує використовувати кваліфікований електронний підпис.

Кабінет Міністрів України визначає вид електронного підпису (удосконалений або кваліфікований), який проставляється при направленні звернень на Інтернет портали за отриманням публічних (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 своїм кваліфікованим електронним підписом нотаріус.

Якщо в законі або підзаконному акті встановлено обов'язок подати нотаріально завірені копії документів, то електронна копія завіряється кваліфікованим електронним підписом нотаріуса. Якщо закон не зобов'язує прикладати нотаріальні копії документів, то копії підписуються удосконаленим електронним підписом заявника. Необхідно відзначити, що закон передбачає можливість при отриманні публічної послуги подавати документи, підписані кваліфікованим електронним підписом в тому випадку, коли потрібна удосконалений електронний підпис, але не навпаки.

Електронно-цифровий підпис забезпечує ідентифікацію і автентичність електронного документа. Проблема існує в наступному,

електронно-цифровий підпис не може безпосередньо характеризувати особу власника.

Взаємозв'язок електронно-цифрового підпису з конкретною людиною обумовлено не біологічним, а соціальним фактором, в тому числі прив'язка цифрового коду до конкретної особи опосередковується сукупністю організаційних, технічних і правових умов. Справжність електронно-цифрового підпису припускає, що особа, яка підписала електронний документ, знає цифровий код – закритий ключ електронно-цифрового підпису. Для того щоб встановити, хто в дійсності підписав електронний документ – власник сертифіката ключа або хтось інший, який отримав інформацію про закрите ключі, необхідно встановити факт: справжність електронно-цифрового підпису та ідентифікацію людини, яка її поставила.

Коли ідентифікуємо особу в традиційному розумінні, то можуть бути використані біометричні дані, в тому числі щодо власноручного підпису. А визначити ідентичність особи безпосередньо за електронно-цифровим підписом неможливо. Тому в спірних ситуаціях визначити, що саме ця особа яка проставляє на електронному документі електронно-цифровий підпис, можна тільки в результаті процесуального доказування в ході судового розгляду. Цифрова сутність електронно-цифровий підпис дозволяє не відрізняти копії електронного документа, відповідно всі копії будуть рівнозначними.

Природна різниця між оригіналом документа та копіями, при складанні документів в електронному вигляді відсутня. Ще одне питання ідентифікації – це проблема забезпечення збереження секретних ключів, так як електронно-цифровий підпис відділький від власника, на відміну від власноручного підпису. Секретний ключ до електронно-цифрового підпису – комп'ютерний файл, який знаходиться на пристрої підписанта, може існувати окремо від власника.

Доступність до секретного ключа здійснюється за допомогою пароля, який фіксується на інтелектуальній карті або іншому пристрої ідентифікатора. Інтелектуальна карта може в принципі бути втрачена або передана іншій особі. При власноручному

підпису біометричні параметри людини практично не можуть бути змінені: характер листа, ступінь натиску, індивідуальні петлі, підкреслення тощо.

Електронно-цифровий підпис дозволяє зробити лише умовний висновок про автора електронного документа, підпис не містить біометричну інформацію автора підпису. Всі стадії застосування електронно-цифрового підпису автоматизовані, однак при автоматизації перевірити підпис за допомогою звичних методів неможливо, що може створювати ілюзію дійсності. Тому для використання електронно-цифрового підпису та 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 безліч проблем правозастосовчої практики. Якщо третій особі з стане відомий закритий ключ, то відрізнити підробку підпису до анулювання ключів буде неможливо. Можливі випадки, коли застосування аналога власноручного підпису дозволить зацікавленим і не доброчесним особам з легкістю відмовлятися від підпису на електронний документ.

---

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

Оптимізація алгоритму колаборативної фільтрації на основі подібності профілів користувачів

Магеровська Тетяна Валеріївна

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

Магеровський Дмитро Вікторович

викладач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ

Полянська Анастасія Олександрівна

здобувач вищої освіти Національного університету «Львівська політехніка»

Сьогодні триває стрімкий розвиток загальної автоматизації усіх сфер суспільства. Новітні технології на базі останніх досягнень інформатики та комп'ютерного обладнання міцно увійшли не тільки у науку та техніку, але й стали невід'ємною частиною повсякденного життя. Таким чином, процес рекомендування клієнтам різноманітних послуг (освітніх закладів для вступу, навчальної літератури, туристичних подорожей, тощо) теж зазнав впливу глобальних інформаційних процесів. Впровадження програмного забезпечення для надання консультацій, що базується на алгоритмі подібності профілів користувачів, дозволило б автоматизувати та оптимізувати цей процес.

На даний момент рекомендаційні алгоритми (наприклад, використання штучного інтелекту) не знайшли широкого застосування у сфері надання рекомендацій. У більшості випадків веб-системи пропонують використовувати фільтрування та пошук для підбору бажаних послуг. Такі підходи не демонструють високу результативність та вимагають участі консультантів.

Було виявлено, що серед існуючих методів рекомендацій достатньо багато переваг має алгоритм колаборативної фільтрації, до якого існують три основні підходи:

- заснований на пам'яті – використовує інформацію про обчислений раніше рейтинг користувача для розрахунку схожості між користувачами або предметами. Це був початковий підхід, що використовувався в багатьох сучасних торгових системах. Він ефективний і простий у реалізації. Має багато модифікацій, оптимізацій та адаптацій до конкретних предметних областей. Даний підхід докладно описано у публікаціях [1-3] великою кількістю авторів, таких як Аваніс Ромлі, Хасан Кахтан, Клаудіо Адріан Левінас та інші;
- заснований на сусідстві – обчислює подібність двох користувачів або виробів, виробляє прогноз для користувача, приймаючи розраховане середнє зважене всіх оцінок. Обчислення схожості між виробами або користувачами є важливою частиною цього підходу. Існують деякі модифікації підходу, що дозволяють адаптувати алгоритм до конкретних предметних областей. Даний підхід описано у публікаціях [4-6];
- заснований на моделі – надає рекомендації, базуючись на вимірюванні параметрів статистичних моделей для оцінок користувачів, побудованих за допомогою різних методів (наприклад, методу баєсівських мереж, кластеризації та інших). Не існує широковідомих модифікацій даного підходу. Докладніше підхід описано у публікації [7] автором Дун Ван Нгуеном.

Крім того, використовується гібридний підхід до колаборативної фільтрації, що об'єднує позитивні ознаки підходів, заснованих на сусідстві та на моделі, а також зменшує вплив на процес рекомендування їхніх основних уразливостей, описаний у статтях [8-10] такими авторами як Нітін Прадіп Кумар, Чженчжень Фен, Адам Лінейбер та інші. У наш час гібридний підхід є найпоширенішим для розробки рекомендаційних систем для комерційних сайтів, адже він допомагає поліпшити якість

прогнозів. З іншого богу, даний підхід є надзвичайно складним і дорогим у реалізації та застосуванні, що зменшує можливості для його застосування.

Відповідно до проведених досліджень [4-6] та попереднього досвіду використання наведених підходів до алгоритму колаборативної фільтрації, найбільш доцільним варіантом для створення системи із функцією рекомендації зазначених послуг буде підхід, заснований на сусідстві.

У джерелі [4] автором Рамеш Домметрі описано значення можливості визначення подібності користувачів для електронної комерції і те, які можливості це відкриває. Також описано різні види підходу, заснованого на сусідстві та їх можливі імплементації.

Публікація [5] за авторства Грег Лінден, Брент Сміта та Джеремі Йорка описує вид цього підходу, що опирається на подібність між виробами та надає рекомендації, базуючись на їх визначних особливостях і попередніх рішеннях користувачів веб-системи. Така ідея може доповнювати чи використовуватись замість класичного підходу до алгоритму колаборативної фільтрації, заснованому на сусідстві, в якому враховується подібність саме користувачів системи між собою.

У статті [6] автором Чару Агарвал досліджено порівняння користувачів між собою, але враховує ідею використання рейтингу користувача для якіснішої та точнішої оцінки схожості клієнтів між собою. Така концепція ускладнюватиме алгоритм і не є обов'язковою, але може бути використана за деяких умов для підвищення ефективності системи.

Підхід, заснований на сусідстві має такі переваги:

- прогнозованість результатів, що є надзвичайно важливим аспектом для рекомендаційних систем, оскільки дозволяє перевіряти роботу системи у найрізноманітніших ситуаціях;
- відносна простота реалізації у порівняння з іншими подібними алгоритмами та підходами;

- простота використання у системі;
- простота внесення змін в алгоритм та створення оптимізації;
- хороші показники масштабованості для більшої кількості даних.

Пропонований оптимізований алгоритм для надання рекомендацій наступний:

1. Пошук користувачів, подібних до того, якому надаються рекомендації:

1.1. Співставлення характеристик даного користувача із характеристиками інших користувачів. Якщо характеристика є значенням зі скінченної множини, вона порівнюється безпосередньо. Для віку використовується діапазон. Для текстових полів використовується аналіз тексту на предмет однакових слів (без врахування службових).

1.2. Відбір користувачів, для яких було знайдено хоча б п’ять співпадінь.

2. Сортування всіх пропозицій, сконструйованих для вибраних користувачів, за поставленою їм іншими користувачами оцінкою (від найвищої 5 до найнижчої 1) та за довжиною коментаря в межах оцінки. Об’єкти, що не були оцінені і мають оцінку 0, обробляються як ті, що мають середню оцінку 3.

3. Надання користувачу до трьох рекомендацій, які мали в результаті роботи алгоритму найвищий рейтинг.

Даний алгоритм не вичерпує усіх аспектів проблеми. Для задач даної категорії існує проблема «холодного старту», описана у джерелах [11-13], – для того, щоб використовувати метод у системі, її база даних вже має містити певні записи про оцінки послуг певної предметної області, надані користувачами. У такому випадку найбільш вдалим варіантом вирішення проблеми є робота системи без опції надання рекомендацій протягом деякого часу. У цей час будуть доступними функції вибору та оцінки, а отже відбуватиметься збір інформації для подальшого її аналізу та використання.

Крім того, існує проблема зниження продуктивності роботи підходу до алгоритму за умови розрідженості даних у базі даних. Це деякою мірою ускладнює масштабованість та спричиняє складнощі у роботі із великими обсягами інформації.

1. Romli M.A. An improved memory-based collaborative filtering method based on the TOPSIS technique [Електронний ресурс] / M.A. Romli, H. Kahtan – 2018. – Режим доступу до ресурсу: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204434.
2. Valcarce D. Collaborative filtering embeddings for memory-based recommender systems [Електронний ресурс] / D. Valcarce, A. Landin, J. Parapar, A. Barreiro – 2019. – Режим доступу: https://www.sciencedirect.com/science /article/abs /pii/S0952197619301599.
3. Levinas C. A. An Analysis of Memory Based Collaborative Filtering Recommender Systems with Improvement Proposals [Електронний ресурс] / C. A. Levinas – 2014. – Режим доступу до ресурсу: https://upcommons.upc.edu/bitstream /handle/2099.1/22602/102384.pdf.
4. Dommetri R. Neighborhood Based Methods For Collaborative Filtering [Електронний ресурс] / R. Dommetri – Режим доступу: http://cs229.stanford.edu/proj2007/Dommeti-NeighborhoodBasedMethodsForCollaborativeFiltering.pdf.
5. Linden G. Item-to-Item Collaborative Filtering: Журнал / G. Linden, B. Smith, J. York // IEEE Internet Computing, Los Alamitos, CA USA – 2003. – P. 76 - 80.
6. Aggarwal C. C. Neighborhood-Based Collaborative Filtering [Електронний ресурс] / C. C. Aggarwal – 2016. – Режим доступу: https://www.researchgate.net/publication/314921150_Neighborhood-Based_Collaborative_Filtering.
7. Nguyen D. V. Model-based approach for Collaborative Filtering [Електронний ресурс] / D. V. Nguyen – 2010. – Режим доступу: https://www.researchgate.net/publication /321753015_Model-based_approach_for_Collaborative_Filtering.

8. Kumar N. P. Hybrid User-Item Based Collaborative Filtering [Електронний ресурс] / N. P. Kumar, Z. Fan – 2015. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S1877050915023492.
9. Lineberry A. Creating a Hybrid Content-Collaborative Movie Recommender Using Deep Learning [Електронний ресурс] / A. Lineberry, C. Longo – 2018. – Режим доступу: https://towardsdatascience.com/creating-a-hybrid-content-collaborative-movie-recommender-using-deep-learning-cc8b431618af.
10. Geetha G. A Hybrid Approach using Collaborative filtering and Content based Filtering for Recommender System [Електронний ресурс] / G. Geetha, M. Safa, C. Fancy, D. Saranya – 2018. – Режим доступу: https://iopscience.iop.org/article/10.1088/1742-6596/1000/1/012101/pdf.
11. Gaspar, H. The Cold Start Problem for Recommender Systems [Електронний ресурс] / H. Gaspar – Режим доступу: https://www.yuspify.com/blog/cold-start-problem-recommender-systems/.
12. Oshiba K. Tackling the Cold Start Problem in Recommender Systems [Електронний ресурс] / K. Oshiba – Режим доступу: https://kojinoshiba.com/recsys-cold-start/.
13. Lika B. Facing the cold start problem in recommender systems [Електронний ресурс] / B. Lika, K. Kolomvatsos, S. Hadjiefthymiades. – 2013. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S0957417413007240.

Інтелектуальні права на цифрові розробки

Миджин Галина Євгенівна

аспірантка кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

Розробка цифрової продукції в більшості випадків пов'язана з необхідністю дотримання та захисту авторських прав, оскільки в ряді випадків функціональне призначення відповідних цифрових розробок безпосередньо пов'язано з необхідністю розміщення відповідної продукції у відкритому доступі, або існує можливість вільного несанкціонованого копіювання цифрового контента.

Надмірний захист цифрових розробок не завжди є виправданим, а у певних ситуаціях, як наприклад, у випадку з популяризацією та просуванням нових цифрових сервісів, музичного, якого літературного контенту, що генерується авторами-початківцями, може мати негативний ефект для інтересів правовласника. У зв'язку, з чим у кожному конкретному випадку необхідно чітке уявлення про застосування виправданою мірою захисту того, чи іншого цифрового продукту.

Переведення у цифрову форму громадських і економічних взаємовідносин, викликана розвитком електронних технологій, формуванням розвиненої та доступної цифрової інфраструктури у всьому світу, до теперішнього часу вже оформилося в якості глобального тренду розвитку міжнародної економіки, що зробило сферу регулювання прав інтелектуальної власності одним із пріоритетних в законодавстві країн Європейського Союзу.

Плоди інтелектуальної діяльності все частіше висловлюються або безпосередньо в якості цифрового продукту, або перетворюються в цифрову форму, що надходить в загальнодоступний віртуальний простір, як наприклад цифровані версії медіа продукції, електронні версії книг, графічних творів, документів.

У мережі Інтернет створюються та формуються такі принципово нові елементи інтелектуальної власності, як наприклад масиви великих даних. Цифрове середовище не тільки дублює

навколишню дійсність, а й породжує принципово нові об'єкти. Тому щоб зробити оборот об'єктів інтелектуальної власності цивілізованим, врахувати інтереси гравців ринку, очевидна необхідність в профільних цифрових рішеннях.

У законодавстві правовідносини в сфері захисту та дотримання авторських прав та інтелектуальної власності регулюються Цивільним Кодексом України [1].

Таке поняття як інтелектуальні права визначені Цивільним кодексом України, яка говорить, що на результати інтелектуальної діяльності та прирівняні до них засоби індивідуалізації визнаються інтелектуальні права, які включають виключне право, що є майновим правом, а у випадках, передбачених Цивільним кодексом, також і особистим немайновим правом та інші права, в тому числі право слідування, право доступу та інші.

Необхідно розуміти, що будь-який інтелектуальний продукт, що з генероване в електронному вигляді, будь то відеозапис, літературний твір, фотографія, програмне забезпечення або масив даних, може вважатися цифровий розробкою. Отже, інтелектуальні права, права інтелектуальної власності на цифрові розробки є сукупністю прав, наданих особі або групі осіб, в результаті реалізованої інтелектуальної діяльності, що відносяться до категорії суб'єктивних прав на нематеріальні блага, оскільки об'єктами таких прав є результати виключно інтелектуальної діяльності, а не речові матеріальні об'єкти.

Варто зазначити, що особисті немайнові права, безпосередньо пов'язані з автором цифрового продукту, включають: право на авторство, право на ім'я, що випливає з норм Цивільного кодексу України, при цьому всі особисті немайнові права, не підлягають відчуженню від автора і передачі третім особам.

Автор лише володіє та користується особистим немайновим правом, а розпоряджатися ним, або відмовитися від нього він не може. Інтелектуальні права в принципі, на відміну від прав майнової власності, поширюються виключно на нематеріальні результати інтелектуальної діяльності, при цьому вони незалежні від прав на володіння матеріальними об'єктами (речами), за

допомогою яких можна отримати цей результат, таким чином, отримання у власність будь або речі не означає автоматичного набуття інтелектуальних прав на неї. З вищенаведеного випливає, що ступінь захисту інтелектуальної власності повинен встановлювати сам володар відповідних прав.

Тільки правовласник вправі вирішувати, на яких умовах надавати потенційним користувачам цифровий продукт. На практиці зустрічаються ситуації, коли, цифрова розробка є цінністю, тільки в разі наявності доступу до неї відносно широкого кола потенційних користувачів, наприклад програмне забезпечення електронного торговельного майданчика, або web-додатки для клієнтів онлайн-банкінгу, або погодний віджет для смартфона. Очевидно, що подібний цифровий продукт має інтерес тільки в якості прикладного програмного забезпечення послуг, що поставляються користувачеві, тому, наприклад захист від копіювання такого продукту є не тільки не виправданим, але й веде до скорочення обсягу відповідних послуг.

Розростання цифрового середовища, яке втягує в обіг все більше об'єктів інтелектуальної власності в цифровій формі, змушує адаптувати до цифрових правовідносин, що формується, вже усталені правові принципи та конструкції, наділяючи інтелектуальну власність на цифровий продукт ознаками об'єктів цивільного права.

---

1. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV / *Відомості Верховної Ради України.* 2003. № 40-44. Ст. 356.

Способи захисту особистих даних в інтернеті

Мілянець Тарас Михайлович

здобувач вищої освіти Львівського національного університету імені Івана Франка

Супик Ростислав Богданович

здобувач вищої освіти Львівського національного університету імені Івана Франка

Фірман Тарас Володимирович

оперуповноважений карного розшуку Галицького ВП ГУ НП у Львівській обл.

В Інтернеті відбувається переплетіння величезного потоку користувачів. За даними Internet World Stats кількість користувачів мережею Інтернет в 2019 році перевищує 4,5 млрд осіб [1]. Тому сьогодні Інтернет став універсальним способом і засобом зберігання інформації. Проте ми не можемо бути впевнені, що наші персональні дані в мережі стовідсотково будуть захищенні.

Право на захист персональних даних та конфіденційність є основоположним правом людини, яке отримало нову та особливу актуальність з поширенням і розвитком інформаційних технологій. Саме це право нам гарантує Закон України «Про захист персональних даних» [2]. Протягом 2018 року в Україні було зареєстровано понад 11 тисяч кримінальних проваджень пов'язаних з кіберзлочинністю [3]. Щоб бути більш захищеним в Інтернеті потрібно розуміти основні загрози та знати, як їх уникнути. Ось декілька способів, які можна використовувати для захисту персональної інформації.

Пароль – це набір символів, унікальний для користувача, який використовується для отримання доступу в систему [4]. Використовуйте унікальні, складні паролі з комбінацією великих і малих букв, цифр та символів та не використовуйте однаковий пароль у своїх облікових записах.

Переконайтесь, що веб-сайт, на якому ви перебуваєте є безпечним. Перевірте, чи починається URL-адреса з https – «s» означає «безпечний».

Уникайте підключення до громадського Wi-Fi. Хакери можуть створити мережу-двійника із такою ж назвою та перехопити ваші дані. За словами експерта Positive Technologies Дмитра Каталкова це один з найпоширеніших інструментів, які зловмисники пускають в хід для крадіжки цінної інформації користувачів [5].

Не натискайте на підозрілі посилання чи вкладення, зазвичай вони ведуть на «фішингові сайти» – це шахрайський веб ресурс, метою якого є отримання цінних даних, які можуть бути продані або використані для зловмисних цілей, таких як вимагання, викрадення грошей або особистих даних [6].

Є ще десятки інших способів захисту даних в мережі, але всі вони потребують вдосконалення. Тому радимо дбайливо ставитися до інформації яку ви передаєте через Інтернет та дотримуватися вищеперерахованих правил.

---

1. https://www.internetworldstats.com/stats.htm – Статистика користувачів Інтернетом
2. https://zakon.rada.gov.ua/laws/main/2297-17 – Закон України «Про захист персональних даних»
3. https://cyberpolice.gov.ua/results/2018/ – Статистика кібер-злочинів
4. https://en.wikipedia.org/wiki/Password – Значення слова «пароль»
5. https://cybercalm.org/novyny/bezkoshtovnyj-wi-fi-yak-syr-u-mysholovtsi-shho-potribno-zadlya-bezpeky/ – Загрози громадського Wi-Fi
6. https://eset.ua/ua/support/entsiklopediya_ugroz/fishing – «Фішингові сайти»

Застосування «Психотехнологій» при здійсненні кримінального провадження

Навроцька Віра Вячеславівна

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

З середини минулого століття набув поширення термін «психологічна війна», що охоплює методи й способи впливу на людей для зміни їх психологічних характеристик (поглядів, переконань, ціннісних орієнтацій, мотивів, установок, масових настроїв). Це, зокрема, сучасні методи комерційної реклами й державно-політичних стратегій. Як приклад можна навести ситуацію, що відбулася в Україні у ході однієї із президентських виборчих кампанії. Тоді за порадою політтехнологів, з метою створення у населення негативного враження про одного із кандидатів на найвищу в Україні посаду, по телебаченню демонструвалися ролики з його виступами на тлі черепа – так званого «25-кадра», невидимого оку, що сприймається на рівні підсвідомості.

Термін «психотехнології» виник у США в кінці 1960-х років для позначення електромагнітних і електричних технічних засобів впливу на людей. Зокрема, винайдені методи «аккустичной психокорекції» і «кодування зображення», коли свідомість не помічає вставленого у відеоряд зображення, адресованого підсвідомості.

Така електронна апаратура впливає на емоції. Певний ритм електромагнітних хвиль викликає той або інший фізіологічний стан. Можна підібрати тип електромагнітного випромінювання, корелюючи його частоту й силу, з метою виникнення почуття страху або тривожності. Апаратура для випромінювання надвисоких частот здатна спричинити стан «наведеного трансу». СВЧ-генератор можна включити або вимкнути в певний момент на тлі тієї або іншої словесної інформації, що відповідно емоційно її забарвлює. Така інформація психопрограммирує, вона здатна обумовлювати певні емоції: стенічні (які мобілізують

на дію) й астенічні (що, навпаки, гасять активність людини). Для впливу на підсвідомість існують різні методики: словесні (словесні маніпуляції, нейролінгвистичне програмування) та техногенні (сугестивні зображення, вставлені у відеоряд, трансовая музика), використання надвисоких частот. Мета їх використання – обійти розум людини та вкласти відповідне послання безпосередньо у підсвідомість.

У психологічній літературі детально описані технології словесного маніпулювання. Зокрема, використовуються методи неправдивої аналогії, відвернення уваги, створення асоціацій, псевдопсихологічних причинних зв'язків. Техніку емоційного резонансу застосовують для створення у широкої аудиторії певного настрою з одночасною подачею пропагандистської інформації. Скажімо, для нагнітання масового психозу, інформація подаються на тлі відповідної музики, парадів і зображень.

На жаль, у законодавстві не прописана можливість контролю за використанням таких методик психологічних маніпуляцій та відповідальність за зловживання ними. Проте держава повинна захищати осіб від деструктивного впливу на психіку. Тому одним із першочергових заходів для усунення загроз психологічному здоров'ю людини було б ухвалення Закону «Про психологічний захист населення». Щоб забезпечити його ефективність, потрібно розробити критерії оцінки шкоди, нанесеної психологічному здоров'ю людей із-за неправомірного втручання в психічну сферу. Необхідно створити вітчизняну систему ліцензування, сертифікації експертизи і контролю у сфері інформаційно-психологічної безпеки і розробити відповідні державні стандарти.

Не виключено, що подібні спеціальні маніпулювання свідомістю застосовуються і при розслідування злочинів чи інших суспільно-небезпечних діянь. Так, стверджується, що останнім часом, з урахуванням високих технологій, набув поширення супровід оперативних заходів (наприклад, переговорів з терористами) записом голосів родичів злочинця із закликами припинити насильство. Голоси цих осіб, відтворюються на надвисоких частотах, не вирізняються загалом на звуковому фоні, а сприймаються на рівні підсвідомості, і, судячи з результатів

дослідження використання цієї технології, є ефективним засобом переговорів з терористами. Подібну технологію радять застосовувати і при проведенні допитів. З метою уникнення окремих зловживань (наприклад, якщо замість заклику до правдивих свідчень буде заклик до самообмови), радять відповідний запис проводити відповідно до закону «Про оперативно–розшукову діяльності», оформивши результат відповідним протоколом, а після закінчення допиту касету з цим записом опечатувати і долучати до протоколу допиту.

Стверджується також, що створення і використання відповідного музичного фону під час допиту є допустимим впливом на особу, яка дає неправдиві показання. Людина, що знаходиться під вартою, відчуває так званий сенсорний голод: він відчуває значно більше зовнішніх подразників порівняно з тими, хто знаходиться на волі. Тому заарештовані можуть підвищено реагувати на такий подразник як музика. Внутрішня установка обвинуваченого на надання неправдивих показань може бути нейтралізована (хоч би на короткий час) сильнішим музичним впливом.

Також радять використовувати в оперативно-розшуковій та слідчій практиці і такий психологічний реагент як запах. Наголошується, що запахи здатні створювати або утримувати певний настрій, встановлювати моделі поведінки, вони впливають на працездатність людини, його серцево-судинну систему, тонус м’язів, зір, слух, пульс і тому подібне Психологи і фізіологи указують на особливе сприйняття жінок до запахів, роль нюху в зміні жіночої поведінки. У 1974-1990 роках слідчий Микола Китаєв більше 40 разів здійснив успішне використання парфюмерних запахів під час допиту жінок, взятих під варту за скоєння тяжких злочинів, які заперечували свою провину. У всіх випадках використовувалася інформація про улюблені парфуми обвинуваченої, встановлювалися асоціативні причини цього (отримання їх в подарунок, приємні спогади тощо). Практика показала, що іноді достатньо навіть невеликої кількості запаху – нагадування минулого життя, аби емоційний вплив слів слідчого посилився, підштовхнув людину до визнання. При цьому у всіх епізодах ніхто з допитуваних не здогадувався про спеціальне застосування запахів.

Ч.1 ст.373 КК України («Примушування давати показання») передбачено кримінальну відповідальність за примушування до дачі показань на допитах шляхом незаконних дій з боку особи, яка проводить дізнання або досудове слідство. При тлумаченні поняття «незаконні дії, на які законодавець вказує як на спосіб примусу до дачі показань (ст.373 КК України) виникає немало питань. Передусім, у КК України відсутнє визначення цього поняття. Нічого не пояснювала свого часу в цьому плані ні ч.3 ст.22 КПК України 1960 р., що містила заборону домагатися показань обвинуваченого та інших осіб, які беруть участь в справі, шляхом насильства, погроз та *інших* незаконних заходів». Не можна зробити такого висновку й на підставі аналізу ч.2 ст.11 КПК України 2012 р. (де йдеться про те, що під час кримінального провадження забороняється піддавати особу катуванню, жорстокому, нелюдському чи такому, що принижує її гідність поводженню чи покаранню, вдаватися до погроз застосування такого поводження, утримувати особу у принизливих умовах чи примушувати до вчинення дій, що принижують її гідність).

Вказівка законодавця на такий спосіб скоєння злочину як «незаконні дії», тоді як це поняття не має конкретного визначення у нормативних актах, не дозволяє правозастосувачу отримати чітке уявлення про ознаки об'єктивної сторони даного злочину. У зв'язку з цим справедливою здається думка, відповідно до якої у кримінальному законодавстві слід використовувати термін «незаконний» тоді, коли мова йде про дії, врегульовані іншим нормативним актом. У цих випадках термін «незаконний» означатиме порушення цього акту і вказувати суб'єктові, що застосовує дану правову норму, на необхідність звернення до іншого нормативного матеріалу для з'ясування всіх ознак складу злочину. Якщо ж кримінальний закон встановлює заборону на проведення певних дій, неврегульованих іншим (не кримінально-правовим) нормативним актом, або ж врегульованих у певній частині, слід виключити використання цього терміну у тексті кримінального закону».

В деяких коментарях до КК України наголошується, що допит шляхом незаконних дій має місце, якщо він проводиться з використанням шантажу, обману, гіпнозу і тому подібне.

Здійснення особою, яка проводить допит, дій, узгоджених з чинним законодавством, (наприклад, багаторазове попередження про кримінальну відповідальність за завідомо неправдиве показання, правомірне використання тактичних прийомів проведення допиту) не становить складу цього злочину. Проте щодо питання про те, що ж вважати «правомірними тактичними прийомами» при проведенні цієї слідчої дії досі серед криміналістів немає єдності думок.

Тому законодавцеві варто було б сформулювати кримінально-правову заборону конкретніше: необхідно з урахуванням позицій криміналістів, психологів, конфліктологов, медиків дати характеристику, вичерпний перелік таких заборонених заходів, які розглядатимуться як способи примушення до дачі показань, що переслідуються у кримінальному порядку.

Інформаційний простір як важіль державної безпеки

Савайда Олена Іванівна

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

Інформаційний потік та інформаційні технології, які використовуються в сучасному світі людиною тісно переплітаються майже з всіма сферами людської діяльності. Проте ключовим моментом в інформаційному просторі та використані таких інформаційних технологій лишається питання інформаційної безпеки як однієї з багатьох функцій держави, в тому числі й функції безпеки та охорони.

Інформаційний простій, який є на сьогодні доступним будь-кому та може бути використаний кожної хвилини будь-якою людиною й містить як і корисні так і небезпечні моменти для державної цілісності та державної політики зокрема, а отже й для безпеки в цілому.

Інформація завжди є одиницею суспільної свідомості та в сучасних реаліях важелем впливу на неї. Проте, як ми бачимо на прикладі нашої держави, неконтрольований інформаційний простір призводить не лише до викривлення дійсності, але й може призвести до інформаційної війни, яка перетворюється з часом на реальну.

Сучасна інформаційна політика нашої держави зараз є одним з пріоритетних напрямків її розвитку. Зараз в процесі політичного дисбалансу та агресії ворога й особистісний інформаційний прості (для громадянина держави), й громадський, й суспільний і в кінці й державний мають бути спрямовані на підвищення рівня безпеки держави. Важливою рисою для інформаційного простору є достовірність та правдивість поданої інформації.

Інформаційний прості також є одним із засобів формування правової культури, що в подальшому при ефективному

використані вказаного явища позитивно впливає на формування й правової держави.

Так чи інакше, а інформаційний прості залежить від сприйняття його людиною, тому важливим аспектом в ньому виступає комунікативна безпечність. Вона стосуватиметься трьох частин інформаційного простору, а саме:

- інтегрального електронного інформаційного простору, що створюється при використанні електронних мереж;
- інформаційної комунікації, як сфери в сучасному суспільному житті світу (у цьому значенні поняття інформаційного простору близьке, але не тотожне поняттю інформаційного середовища);
- є об'єктом уваги державних спецслужб.

Основні характеристики інформаційного простору

- він є завжди неоднорідним і структурованим з акцентами на різні соціальні групи і теми;
- є динамічним у силу постійних змін, які відбуваються у різних сферах життя окремих країн, регіонів та світу загалом, а також нових акцентів в інформаційній політиці;
- інформаційний простір країни має бути захищеним від впливу інших держав. (особливої уваги вимагають певні сегменти й агресивні дії відповідних держав);
- формується з урахуванням національно-культурних і психологічних особливостей країни;
- має універсальний вплив на всі сфери життя суспільства і окремих індивідів. [1, с.345].

Виходячи з вказаних характеристик інформаційного простору, нагальним постає державна безпека, яка не лише має на меті контролювати та виявляти, а в першу чергу формувати правильне інформаційне поле, що так чи інакше впливає на свідомість громадян держави. В такому контексті інформаційний простір доцільно розглядати у взамозв'язку з культурним простором, освітнім та простором ментальності.

Перед нашою державою нагально постає питання інформаційної безпеки, як одного із важелів охорони держави від несанкці-онованого та викривленого потоку інформації. Тому, інформацію, яка подається в різних інформаційних просторах ретельно потрібно аналізувати та усвідомлювати через уявлення про реальний світ та справжні події. Але безпека держави в інформаційному просторі теж залежить і від потреб та політики самої держави, й безперечно від зовнішніх чинників інших сторін. Тому носії та поширювачі офіційного інформаційного простору повинні весь час пам'ятати про заходи національної безпеки. Адже як з'ясувалося в сучасному світі слово (як атомна частина інформації) може нанести величезну шкоду та перетворити життя високоінтелектуальної людини на примітивне існування.

Проте не потрібно забувати, що інформація це один із способів пізнати світ та вміле й вдале користування такими засобами призводить до кращого усвідомлення світової реальності. Інформаційний простір для забезпечення безпеки держав, однозначно, має носити національне забарвлення. Дух національного права закладає основи для простору інформації на теренах держави. Національна основа інформаційного простору несе в собі основи державної національної безпеки.

---

1. Слюсаревський М. М. Інформаційний простір : критика існуючих визначень і спроба побудови теорії. Вісн. ХДУ. Серія «Психологія, політологія» : Особистість і трансформаційні процеси в суспільстві. Психолого-педагогічні проблеми сучасної освіти. Харків. 1999. Ч. 4-5. С. 337-342.
2. Довгий С. О. Інститут телекомунікацій і глобального інформаційного простору [Електронний ресурс] / С. О. Довгий / Режим доступу: http://www.itel.nas.gov.ua. – Назва з титул. екрана.
3. Інформаційний простір [Електронний ресурс] / Матеріал з Вікіпедії – вільної енциклопедії / Режим доступу: http://uk.wikipedia.org/wiki.

Використання інформаційних технологій у галузі охорони здоров'я

Сибірна Рома Іллінічна

професор кафедри психології діяльності в особливих умовах Львівського державного університету внутрішніх справ, доктор біологічних наук, професор

Зарічна Ольга Зіновіївна

асистент Львівського національного медичного університету імені Данила Галицького, кандидат біологічних наук

Загальні тенденції сучасного етапу, відзначуваного як «ера інформаційного суспільства» – прискорення темпу життя, зростання кількості комунікативних зв'язків, урбанізація і бурхливий розвиток науково-технічного прогресу – визначають необхідність переходу до нової стратегії розвитку на основі знань та високоефективних інформаційних технологій, які невблаганно вторгаються в усі сфери діяльності людства. Зміщення акцентів у сферу інформаційних технологій потребує реалізації концепції «чотирьох і» (інформатизація, індивідуалізація, інтеграція та інтелектуалізація), переосмислення інформаційних аспектів та інформаційної специфіки реформування галузі охорони здоров'я, зокрема, психічного здоров'я.

Основним завданням державної політики у сфері інформатизації системи охорони здоров'я України, в тому числі і психіатричної допомоги, є розвиток галузевого інформаційного середовища, створення умов економічно виправданого використання сучасних інформаційних технологій для забезпечення інформаційної, системно-аналітичної та експертної підтримки прийняття рішень в усіх сферах діяльності в системі охорони здоров'я [2, 3, 4]. Однією з найважливіших складових частин існуючих і майбутніх програм реформування галузі охорони здоров'я повинна стати інформатизація, яка має об'єднати комплекс заходів по розробці і впровадженню організаційного, методичного, програмного та технічного забезпечення усіх проектів.

Аналіз тенденцій інформатизації медичної галузі в Україні дозволяє виділити наступні її напрями:

- розвиток системи комп'ютерних комунікацій в сфері охорони здоров'я з метою забезпечення доступу до інформаційних ресурсів глобальних мереж, ефективного використання вже створених інформаційних ресурсів, інтеграції українських медичних наукових та лікувально-практичних закладів в світову медичну систему;
- вдосконалення інформаційної інфраструктури з метою створення сучасної науково-технічної бази впровадження інформаційних технологій.

Інформаційно-комунікаційні технології у медичних дослідженнях не замінять якісний, змістовний аналіз, проте можуть зробити його ефективнішим, якщо фахівець, що їх використовує, не лише володіє матеріалом і предметом свого дослідження, але й застосовує комп'ютерну технологію відповідно до мети власного дослідження і наявних можливостей програмного продукту. При цьому виділяються такі завдання використання інформаційних технологій у судово-медичній практиці:

- забезпечення виходу в світові медичні комп'ютерні мережі, надання доступу до міжнародних інформаційних, обчислювальних та програмних ресурсів широкому колу медичних працівників;
- впровадження сучасних інформаційних і телекомунікаційних технологій, використання інформаційних ресурсів глобальних комп'ютерних мереж, поширення культури Internet;
- забезпечення доступу членів світової інформаційної спільноти до інформаційних ресурсів вітчизняної медичної науки;
- підвищення ефективності експлуатації інформаційних ресурсів України, передусім на регіональному рівні;
- проведення єдиної технічної політики в області комп'ютерних комунікацій в системі охорони здоров'я.

Умови теперішнього часу потребують створення єдиного медичного інформаційного простору України, основу якого з позиції пацієнта складає електронна історія хвороби [2], яка забезпечує оперативний доступ лікаря до необхідної медичної інформації, в яку б медичну установу не звернувся пацієнт. В умовах страхової медицини тільки такий вид документації забезпечує оперативний облік пов'язаних з діагностичним чи лікувальним процесом витрат, використанням медикаментів і матеріалів, оплатою послуг медичного персоналу тощо. Крім того, розвиток телемедичних технологій, які сьогодні можуть реально забезпечити інтеграцію України в єдиний світовий медичний інформаційний простір, дозволить суттєво покращити рівень надання медичної допомоги: з одного боку, на базі профільного НДІ або лікувального закладу можна організувати телемедичний консультаційний центр для обслуговування всіх закладів області, з іншого, при необхідності, можна проконсультувати хворого з цього центру в будь-якому провідному медичному центрі за кордоном. Нарешті, телемедичні технології можуть застосовуватися навіть у межах окремого лікувального закладу [2].

Єдина інформаційна мережа має базуватися на новітніх інформаційних технологіях мереживних телекомунікацій та медичних інформаційно-аналітичних системах, до її складу повинні входити галузеві та регіональні бази даних, системи медико-статистичної інформації та аналізу [1, 3, 4].

Так, зокрема, з точки зору даних про загальний стан здоров'я кожного громадянина, медично значущими є показники навколишнього середовища, стан психіатричної, наркологічної та інших служб. За допомогою постійного аналізу отриманих показників можна цілеспрямовано залучати державні та громадські організації, систему медичної освіти та науки до вирішення нагальних проблем охорони здоров'я населення, визначати шляхи подальшого реформування та прогнозувати майбутні зміни у сфері медицини.

На даний час інформаційні технології широко використовуються при проведенні наукових медичних досліджень [2]. Разом з тим,

слід зазначити що робота в умовах інформатизації вимагає постійної підготовки відповідних кадрів, які спроможні обслуговувати, використовувати і розвивати інформатизаційну структуру системи охорони здоров'я.

---

1. Богатырёва Р. В., Бережнов С. П., Горбань Е. Н. Государственная компьютерная информационная система мониторинга эпидемического процесса в Украине. Технология мониторинга // Лікарська справа. – 1999. – № 3. – С. 3–12.
2. Інформатизація галузі – необхідна умова реформування системи охорони здоров'я / В. Ф. Москаленко, О. Ю. Майоров, Є. М. Горбань, В. М. Пономаренко, В. П. Яценко, В. В. Кальниш // Проблеми медичної науки та освіти. – 2000. – № 4. – С. 5–8.
3. Картиш А. П., Горбань Є. М., Пономаренко В. М. Використання сучасних інформаційних технологій для підвищення ефективності управління науковими дослідженнями в системі міністерства охорони здоров'я // Лікарська справа. – 1998. – № 6. – С. 168–173.
4. Пономаренко В. М., Кальниш В. В., Майоров О. Ю. Шляхи інформатизації медичної галузі // Журнал соціальної гігієни та організації охорони здоров'я. – 2000. – № 1. – С. 35–47.

Сучасні інформаційні технології у діяльності науковця

Сибірний Андрій Володимирович

доцент Львівського національного медичного університету імені Данила Галицького, кандидат біологічних наук, доцент

Хомів Олена Володимирівна

доцент Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

Сучасні інноваційні зміни впливають на стрімке оновлення інформації й приводять до підвищення темпів приросту, накопичення, передачі наукової інформації, що, у свою чергу, вимагає нового розуміння та нових форм в організації науково-дослідного процесу. Подальший модернізаційний розвиток наукових досліджень потребує відповідної інформаційно-ресурсної бази, яка передбачає інформатизацію науково-дослідних процесів, зокрема: техніко-інформаційну реконструкцію наукових бібліотек, нарощування інформаційно-пошукових систем, створення наукових баз і банків даних, баз знань, інформаційних центрів, архівних фондів, широке використання інтернет-ресурсів. Відповідно, запровадження й широке використання інформаційно-комунікаційних технологій суттєво впливає на якість та ефективність наукових досліджень, створює сприятливі, комфортні умови для науковців та підвищує рівень інформаційного забезпечення наукового процесу.

На сьогоднішній день пошук інформації часто трудомісткий не тільки через великий обсяг літератури, але і через розпорошення даних, тобто, внаслідок публікації статей певної тематики у непрофільних джерелах [1, с. 102]. Тому, сучасні автоматизовані методи пошуку інформації, отримання консультацій, довідок і різних копій дозволяють значно скоротити час пошуку та зменшити його трудомісткість [1, с. 116].

Інформатизація як один із головних напрямів сучасної науково–технічної революції, на якому ґрунтується перехід від

індустріального етапу розвитку суспільства до інформаційного охоплює три взаємопов'язаних процеси:

а) медіатизацію – удосконалення засобів збирання, збереження і поширення інформації;

б) комп'ютеризацію – удосконалення засобів пошуку та оброблення інформації;

в) інтелектуалізацію – розвиток здібностей, сприйняття і продукування інформації, тобто підвищення інтелектуального потенціалу суспільства, в т. ч. використання засобів штучного інтелекту [2 с. 7].

На даний час Internet надає безліч інформаційних ресурсів, у тому числі і в галузі науки і техніки. Мережу Internet можна визначити як величезну цифрову магістраль – систему, що пов'язує мільйони комп'ютерів, під'єднаних до тисяч мереж у всьому світі [1, с. 119].

Internet забезпечує можливість легко взаємодіяти різним видам комп'ютерних систем, тому що в ньому застосовуються стандартизовані методи передачі даних, які дозволяють звільнити користувача від освоєння розмаїття мереж і машин [1, с. 120].

В Internet розміщено багато документів і часто досить складно знайти необхідні файли. Для знаходження необхідної інформації на деяких вузлах пропонується спеціальне програмне забезпечення, що називається пошуковим сервером (search engine). Використовуючи пошуковий сервер, необхідно ввести одне або декілька слів, що відповідають темі, в якій є зацікавленість. Пошуковий Web-сервер відображає перелік документів, що містять необхідну для користувача інформацію. Існують як закордонні, так і вітчизняні пошукові системи. Практично всі системи вже внесені до каталогів, а зареєстровані у них сервери розташовані за категоріями [1, с. 123–124].

Інтернет і WEB стали інформаційним джерелом для науковців, оскільки вони отримують доступ до інформації без будь-якої допомоги, участі чи керівництва другої особи і можуть користуватись нею в будь-який час за потребою.

Найпотужнішим ресурсом у забезпеченні наукових досліджень на сьогодні залишається інформаційно-бібліотечний ресурс.

Новітні інформаційні технології у сучасних бібліотеках надають можливість значно полегшити та розширити цю діяльність.

Для визначення комплексу інформаційних джерел, доступних через глобальні комп'ютерні мережі, що в сукупності утворюють Internet використовується «віртуальна бібліотека». Вона не має єдиного місцезнаходження – її ресурси розподілені по всьому світу а інформаційний потенціал на кілька порядків перевищує ресурси будь-якої книгозбірні.

Під «цифровою бібліотекою» мається на увазі вся інформація, що зберігається у оцифрованому вигляді та не передбачає наявності документів на традиційних носіях. В електронній бібліотеці основні процеси здійснюються з використанням комп'ютерів, однак у таких бібліотеках документи на машинних носіях співіснують з аудіо-, аудіовізуальними та іншими матеріалами. Електронна бібліотека включає в себе й цифрову, в якій, окрім суто дискретного подання документів, допускається і їх відображення в іншій електронній формі. Цифрова та електронна бібліотеки, на відміну від віртуальної, являють собою сукупність документів, що мають конкретне місцезнаходження

Таким чином, з метою поліпшення інформаційного забезпечення науково-дослідницької діяльності необхідно змінювати психологічне ставлення суспільства до інформатизації, створювати умови для оптимального доступу до інформаційного середовища, розвивати та підвищувати ефективність використання сучасних інформаційних технологій. Вітчизняним науковцям слід інтенсивно вдосконалювати відповідні знання з метою ширшого використання інформаційних видань, довідково-інформаційних фондів та пошуку наукової інформації [3, с. 295–296].

Отже, Internet надає безліч інформаційних ресурсів, у тому числі і у галузі науки і техніки, та забезпечує можливість легко взаємодіяти різним видам комп'ютерних систем, тому що в ньому застосовуються стандартизовані методи передачі даних, які дозволяють звільнити користувача від освоєння розмаїття

мереж і машин. Для знаходження необхідної інформації на деяких вузлах пропонується спеціальне програмне забезпечення, що називається пошуковим сервером

---

1. Антонюк В. С., Полонський Л. Г., Аверченков В. І., Малахов Ю. А. Методологія наукових досліджень : навч. посіб. К. : НТУУ «КПІ», 2015. 274 с.
2. Пожуєв В. І. Інформатизація як ресурс розвитку сучасного українського суспільства. Гуманітарний вісник ЗДІА. 2009. Випуск 38. С. 4–12.
3. Сибірна Р. І., Сибірний А. В., Хомів О. В. Сучасні інформаційні технології у науково-дослідницькій діяльності. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська. Львів: ЛьвДУВС, 2017. С. 294-297.

Інтренет-речі: гносеологічні засади розвитку та онтологічні константи сучасності

Ткачук Тарас Юрійович

заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор юридичних наук, доцент

Хитра Олександра Леонтіївна

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

Переваги використання технологій штучного інтелекту очевидні, тому не дивно, що IoT з кожним роком набирає обертів і буде мати позитивну тенденцію. Пристрої, гаджети і розумні системи при цьому покликані не замінити спеціалістів, а полегшити і оптимізувати їх роботу. Так, спеціалісти Tractica прогнозують, що поставки клінічних і неклінічних підключених натільних датчиків досягнуть 92,1 млн одиниць в 2022 році (для порівняння: 2,4 млн одиниць було в 2016 році) [1].

Термін IoT (анг. «Internet of Things», скор. – IoT) вперше було сформульовано у 1999 році засновником дослідницького центру Auto-ID Center в Массачусетському технологічному інституті Кевіном Ештоном [2].

Проте, історія IoT має свій футурологічний аспект, зокрема у творах письменників фантастів. Так, у 1950-ті роки Рей Бредбері створив кілька творів, в яких напрочуд точно передбачив технології та тренди, що з'явилися в майбутньому. З кожним роком все більше винаходів, описаних в його книгах, втілюються в життя. Ось кілька з них.

1. *Віртуальна реальність.* В оповіданні «Вельд» Р. Бредбері описує кімнату з ефектом присутності. Вона може створювати

зображення, звуки і запахи, а також, судячи з подій сюжету, ще й впливати на матеріальні об'єкти.

2. Безпілотні автомобілі. В оповіданні «Пішохід» фігурують автомобілі, які їздять самі по собі, а також вміють вести з людьми діалог.

3. Bluetooth-навушники. У романі «451 градус за Фаренгейтом» описані радіопередачікі-»черепашки», які щільно прилягають до вух і відтворюють звук без проводів. Понад 50 років пішло в людства, аби втілити передбачення Бредбері в життя – у 2016 році Apple представила AirPods.

4. Розумний годинник і стільниковий зв'язок. В оповіданні «Вбивця» 1953 року фантаст передбачив появу пристроїв, які дозволять розмовляти один з одним на відстані без проводів. В його уяві це були радіобраслети – невеликі девайси у вигляді годинника з вбудованим мікрофоном і динаміком. Виходить, Бредбері передбачав відразу дві технології: мобільний зв'язок і розумні годинник. Наприклад, дзвінки можна здійснювати з Apple Watch – точно так, як описано в книзі.

5. Розумний будинок. У кількох оповіданнях Р. Бредбері зустрічаються розумні будинки. Вони вміють розуміти голосові команди, готувати їжу, прибирати, прати, навіть мити і одягати власників. У 1999-му році Disney випустила фільм, в якому сім'я заїжджає в «будинок майбутнього», яким керував віртуальний асистент Пет.

Рей Бредбері зміг передбачити багато винаходів і тренди майбутнього. Але головний посил практично всіх його творів – що розвиток технологій перетворить людей у бездушні біомашини – поки, на щастя, не був втілений в життя. Хай-тек, скоріше, допомагає вирішувати проблеми людства, ніж створює їх.

Серед інших письменників, які змогли досить точно зазирнути у майбутнє поправу можна вважати Жуль Верна, який у 1865 році написав книгу «Із Землі на Місяць», в якій йшла розповідь про першу подорож людей на Місяць. Письменник не лише передбачив сам факт польоту людини на Місяць, у його книзі

безліч інших точних передбачень. Цікаво те, що між книгою Жуля Верна та польотом людини на Місяць пройшло 104 роки!

Попри очевидні переваги практичного застосування IoT на сучасному етапі суспільного розвитку, актуалізується і зворотна сторона даних процесів – кібербезпека. За оцінкою компанії Hewlett-Packard (2015 рік), більше 70% пристроїв, що входять в IoT, мають уразливості, у 60% з них – небезпечний web-інтерфейс. При цьому більшість з них мають у своєму розпорядженні доступом до таких даних своїх власників, як адреса, e-mail і навіть банківський рахунок [3].

Часто це пов'язано з тим, що виробники, прагнучи знизити свої витрати, радикально економлять на забезпеченні безпеки. У свою чергу, фірми-постачальники дешевих відеокамер практично ігнорують включення в свої продукти засобів захисту, оскільки, за їхніми оцінками, для більшості користувачів камер низька вартість набагато важливіше. 9 січня 2017 року Федеральна торгова комісія США навіть подала позов проти D-Link через неякісний захист веб-камер і роутерів [4].

У 2016 році значного розголосу набула інформація про успішний злом інсулінової помпи, який здійснив на прикладі власного пристрою хакер, який страждає діабетом. Він отримав доступ через незахищений Wi-Fi канал [5].

У своїй новій книзі під назвою «Click Here to Kill Everybody» («Натисніть сюди, щоб убити всіх»), співробітник центру Berkman Klein Center for Internet and Society в Гарварді, член ради Фонду Electronic Frontier Foundation, головний фахівець з технологій у компанії IBM Resilient, яка допомагає іншим кампаніям підготуватися до потенційних кіберзагроз Брюс Шнайер стверджує, що уряди повинні змусити компанії, що займаються розробкою гаджетів, які виходять в Інтернет, поставити безпеку на перше, а не на останнє місце [6].

Ці та ряд інших важливих проблем кібербезпеки IoT слугували підставою випуску Технічним комітетом Європейського інституту телекомунікаційних стандартів (ETSI) з кібербезпеки стандарту кібербезпеки в Інтернет речей TS 103 645 [7].

Документ встановлює базовий рівень безпеки для споживчих товарів, підключених до Інтернету, і закладає основу для майбутніх схем сертифікації IoT.

TS 103 645 вимагає від розробників відмовитися від використання універсальних паролів за замовчуванням, які стали джерелом багатьох проблем безпеки. Він також передбачає дотримання політики розкриття вразливостей, щоб дозволити дослідникам безпеки і іншим особам повідомляти про проблеми. Крім того, стандарт дозволить забезпечити дотримання норм Загального регламенту щодо захисту даних (General Data Protection Regulation, GDPR) IoT-пристроями і сервісами, що зберігають і обробляють персональні дані користувачів.

Крім того, на основі TS 103 645 розробники планують впровадити схеми сертифікації, які допоможуть захистити особисті дані користувачів.

Одна з важливих функцій стандарту – скоротити кількість паролів, які використовуються за замовчуванням. Саме стандартні паролі є однією з головних причин загроз кібербезпеки IoT-сфери. TS 103 645 також передбачає політику розкриття вразливостей: це простимулює користувачів повідомляти про проблеми з функціонуванням пристроїв.

Застосування цього стандарту дозволить також повноцінно дотримуватися норм Загального регламенту щодо захисту даних (GDPR) – спеціальної постанови ЄС, спрямованого на захист і уніфікацію персональних даних всіх громадян Європейського союзу. У свою чергу використання GDPR допоможе захистити персональну інформацію користувачів та підвести єдину нормативну базу під весь сектор IoT і IT-технологій.

Відповідний суб'єкт, такий, як постачальник послуг або виробник пристрою, зобов'язаний забезпечити обробку персональних даних відповідно до чинного законодавства про захист персональних даних (таким, наприклад, як європейський GDPR), а також відповідно до чинного законодавства і нормативних вимог до питань безпеки.

Так, згаданий стандарт, у частині захисту персональних даних, крім іншого, передбачає:

Положення 4.8-1. Виробники пристроїв і постачальники послуг зобов'язані надавати споживачам чітку і прозору інформацію про те, як, ким і з якою метою використовуються їхні персональні дані. Це також відноситься до третіх сторін, які можуть бути залучені, включаючи рекламодавців.

Положення 4.8-2. Якщо особисті дані обробляються на основі згоди споживачів, ця згода має бути отримана належним чином.

Положення 4.8-3. Споживачам, які дали згоду на обробку своїх персональних даних, повинна бути надана можливість відкликати згоду в будь-який час.

Отримання згоди «належним чином» (in a valid way) як правило передбачає надання споживачам, у цьому випадку – пацієнтам, вільного, очевидного і явного вибору (*причому за замовчуванням вважається, що такої згоди немає – варіант opt-in*) щодо використання їх персональних даних для певної мети третіми особами.

Пацієнти очікують, що їм будуть надані засоби для захисту недоторканності їх приватного життя, за допомогою належного налаштування функціональних можливостей пристроїв і послуг IoT, які використовуються у процесі надання їм медичних послуг.

Розробка стандарту кібербезпеки є важливим кроком для правової нормалізації всієї сфери IoT, у тому числі й у сфері медицини. На сьогоднішній день персональні дані користувачів IoT-пристроїв залишаються незахищеними, тоді як сама сфера застосування подібних пристроїв зростає.

---

1. How IoT enhances medicine. M-Health Conference Tallinn. URL: https://tallinn.mhealth.events/article/iot-v-meditsine-kak-internet-veshchey-sovershenstvuet-sferu-zdravoohraneniya-97414
2. Kevin Ashton That 'Internet of Things' Thing. RFID Journal. URL: https://www.rfidjournal.com/articles/view?4986

3. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. News Advisory. URL: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676
4. Federal trade commission d-link corporation and D-link systems, INC. Case 3:17-cv-00039 URL: https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf
5. Johnson & Johnson says insulin pump 'could be hacked' BBC NEWS. 4 October 2016. URL: https://www.bbc.com/news/business-37551633
6. Bruce Schneier Click Here to Kill Everybody Security and Survival in a Hyper-connected World. September 2018 W. W. Norton & Company. 288 Pages URL: https://www.schneier.com/books/click_here/
7. CYBER; Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02) URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Мікроконтролерний інформаційно-керуючий комплекс в системі змащування двигунів внутрішнього згоряння зразків озброєння та військової техніки

Шабатура Юрій Васильович

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

Гера Володимир Ярославович

ад'юнкт Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Міхалєва Марина Станіславівна

професор кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Смичок Василь Дмитрович

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

Ветренко Євген Дмитрович

курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Сучасні інформаційні технології здатні вирішувати не тільки задачі пов'язані з обробкою великих цифрових масивів інформації, вони придатні і для ефективного розв'язування чисто прикладних задач пов'язаних з контролем і управлінням різного роду технічними об'єктами і процесами. Прикладом такого об'єкту є двигун внутрішнього згоряння (ДВЗ). Такий двигун є достатньо складною системою, яка поєднує в собі велику кількість механічно взаємопов'язаних механізмів і деталей, для надійної і злагодженої роботи яких необхідне обов'язкове і якісне

змащування [1,2]. Традиційно цю задачу виконує спеціальна система змащування, яка забезпечує подачу мастила під тиском по спеціальних каналах до усіх, найбільш механічно навантажених вузлів і механізмів двигуна. Основою системи змащування є механічний шестерінчастий насос, який безпосередньо механічно зв'язаний з колінчастим валом двигуна. Така компоновка забезпечила надійність і мінімальні вимоги для обслуговування системи. Однак, у такої системи виявляється і ряд суттєвих недоліків. Зокрема, після довгого простою, під дією сили гравітації рідке мастило стікає з усіх робочих поверхонь двигуна, які потребують змащування, особливо критичним це є для кривошипно-шатунного механізму (КШМ), який є найбільш навантаженим вузлом двигуна внутрішнього згоряння. В результаті, після запуску двигуна, певний час в кривошипно-шатунному механізмі спостерігається стійке масляне «голодування», що призводить до інтенсивного зношування робочих поверхонь і, як наслідок, до суттєвого зменшення ресурсу двигуна та його енергетичних характеристик. І лише після того, як масляний насос закачає масло в усі масляні канали і створить там необхідний тиск проблема масляного «голодування» буде ліквідована. Аналогічна проблема, проте меншої гостроти виникає і під час режиму зупинки двигуна.

Враховуючи те, що чимало зразків озброєння і військової техніки мають значний термін експлуатації, тому внаслідок зносу в них спостерігається підвищений розхід масла в підшипниках кривошипно-шатунного механізму, це спричиняє необхідність збільшення обертів холостого ходу для підтримування необхідного значення тиску масла, а отже і до підвищеної витрати пального.

Однак, найбільш критичними з точки зору можливості виходу з ладу кривошипно-шатунного механізму є режими екстремальної експлуатації зразків озброєння і військової техніки, які нерідко відбуваються під час бойових дій. Адже в цих режимах часто виникають значні перевантаження двигунів зовнішніми моментами опору, які виникають під час різкої зміни напрямку руху, прискорення руху, руху в умовах бездоріжжя, з значними кутами підйому і т.д. Зазначені фактори спричиняють

виникнення в зонах робочих поверхонь шатунних підшипників колінчастого валу таких питомих тисків для яких тиск масла виявляється недостатнім внаслідок чого відбувається зрив масляної плівки з виникненням «сухого» тертя, яке швидко виводить головний механізм двигуна з ладу.

Раніше проведені дослідження показують, що максимального ресурсу двигуна можна досягти при підтримуванні оптимального режиму змащування, який характеризується необхідністю забезпечення чітко визначеної товщини масляної плівки між поверхнями, що труться. Графічно цей режим добре ілюструється діаграмою Герсі-Штрібека, яка наведена на рис. 1.

На даній діаграмі можна чітко виділити три характерних області, які визначають режими змащування: I – граничний, II – оптимальний (змішаний), III - гідродинанічний.

При граничному режимі змащування поверхні деталей контактують між собою, це викликає появу «сухого» тертя. Знос деталей механізму при цьому є максимальним.

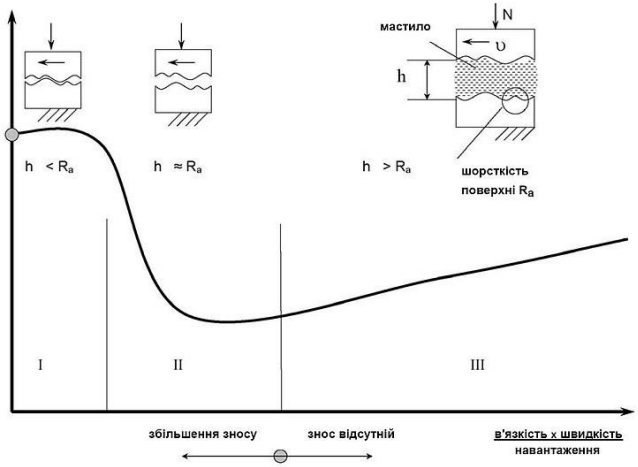

Рис. 1. Діаграма Герсі-Штрібека.

При гідродинамічному режимі змащування робочі поверхні деталей повністю відокремлені шаром масла. Тертя між ними

знову починає зростати, воно зумовлене об'ємними гідродинамічними властивостями товстих плівок масла. Знос деталей відсутній, але відбуваються перевитрати моторного масла. При змішаному режимі змащування ділянки робочих поверхонь знаходяться між режимами гідродинамічного та граничного режиму змащування. Відстань між поверхнями є співрозмірною з величиною їх шорсткості. Цей режим і є оптимальним режимом змащування ДВЗ.

Проведений в роботах [3,4] аналіз засвідчує, що домогтися оптимального режиму змащування ДВЗ у різних режимах експлуатації при використанні механічної системи змащування в принципі не можливо, оскільки єдиний регулювальний параметр цієї системи – це кількість обертів шестерінчастого насоса, прямо пропорційно залежить виключно від кількості обертів колінчастого валу двигуна.

Вирішити зазначену проблему пропонується на основі використання мікроконтролерного інформаційно-керуючого комплексу, який здійснює збір і обробку інформації про усі параметри руху та фактори впливу на процес змащування ДВЗ, на основі чого формується сигнал управління електричним двигуном приводу масляного насосу. За рахунок використання сигналів зворотного зв′язку та обчислень за синтезованою математичною моделлю комплекс забезпечує постійну підтримку оптимального режиму змащування ДВЗ незалежно від умов його експлуатації та інших факторів впливу.

За допомогою комп'ютерного моделювання на основі експериментально отриманих даних була проведена інтерполяція залежності тиску масла в головній масляній магістралі від моменту опору на колінчастому валу ДВЗ. Математична модель у вигляді інтерполяційного поліному має вигляд:

$$P_w(M_o) = 11.2 - 0.73 \cdot M_o + 0.018 \cdot M_o^{\,2} - 0.15 \cdot 10^{-3} \cdot M_o^{\,3} \quad (1)$$

Основним параметром відносно якого можна визначити режим змащування підшипників колінчастого валу є мінімальна товщина масляного шару h_{min}. Важливо відмітити, що за раніше проведеними дослідженнями [5], цей параметр залежить від

багатьох чинників і може бути визначений за такою функціональною залежністю:

$$h_{min} = \frac{n \cdot \mu \cdot d^2}{18.36 \cdot p_{\text{сер}} \cdot \Delta \cdot c}, \qquad (2)$$

де h_{min} – мінімальна товщина масляного шару, м;

n – кількість обертів колінчастого валу двигуна, об/хв.;

μ – в'язкість масла, кгс с/м^2;

d – діаметр шатунної шийки колінчастого валу, м;

$p_{\text{сер}} = R/d \cdot l$ – усереднений питомий тиск, Па;

R - навантаження на шатуну шийку, Н;

d – діаметр шатунної шийки, м;

l – довжина шатунної шийки;

Δ – діаметральний зазор, м; $c = (1 + d/l)$ коефіцієнт, що характеризує геометрію підшипника.

На військовий колісний засіб (ВКЗ) під час руху діє ряд сил спротиву, які створюють момент опору M_o на обертання колінчастого валу. До таких сил належать: F_f – сила опору руху (сила тертя), F_p – сила скочування під час руху на підйом, F_w – сила опору повітря [4]. Вище перераховані сили створюють момент опору M_o який розраховується за формулою.

$$M_o = F_{\text{сум}} \cdot n_{\text{к}} \cdot n_{\text{т}} \cdot \tau_{\text{КП}} \cdot \tau_{\text{т}} \cdot R_{\text{к}}, \qquad (3)$$

де $F_{\text{сум}} = F_f + F_p + F_w$ – сумарна сила опору, Н;

$n_{\text{т}}$ – передаточне число трансмісії ВКЗ;

$\tau_{\text{КП}}$ – ККД коробки передач;

$\tau_{\text{т}}$ – ККД трансмісії;

$R_{\text{к}}$ – радіус колеса.

Аналітична залежність для розрахунку необхідної зміни тиску в головній масляній магістралі з врахуванням змін моменту навантаження на колінчастому валу двигуна, що виникає в залежності від умов руху ВКЗ має вигляд:

$$p_e = 0.025 \cdot \sqrt[3]{\frac{\left(R + {M_o}/{r_{\text{кв}}}\right)^2 \cdot \mu \cdot n}{18.36 \cdot l^2 \cdot h_o \cdot \Delta \cdot c}}. \quad (4)$$

Результати комп′ютерного моделювання на основі виразу (4) дозволили отримати графічну залежність зміни тиску масла в головній масляній магістралі, яка необхідна для забезпечення оптимальної товщини масляного шару в підшипниках КШМ, від зміни кількості обертів колінчастого валу двигуна та зміни моменту навантаження на колінчастому валу двигуна. Дана залежність представлена на рис.2.

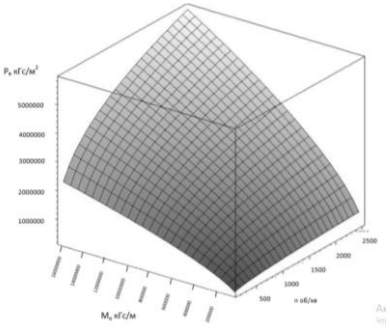

Рис.2. Залежність зміни тиску в головній масляній магістралі від зміни кількості обертів колінчастого валу двигуна та зміни моменту.

1. А. В. Гуляєв Підвищення ефективності функціонування системи технічного обслуговування та ремонту озброєння та військової техніки. – К. : Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, 2018. – 48с.

2. Калімуллин Р. Ф., Коваленко С. Ю. Концепция ресурсосберегающей эксплуатации автомобильних двигателей // Вестник СГТУ, 2013 – Вып2(71). – 29-34 с.
3. Шабатура Ю.В., Гера В.Я., Смичок В.Д Інформаційно-вимірювальна система для експериментального дослідження режимів змащування двигуна внутрішнього згоряння// V Всеукраїнська н.т.к. у царині метрології «Technical Using of Measurement-2018» 29 січня – 2 лютого 2019р. Славське. Львів: ТзОВ «Галицька видавнича спілка», 2019. С. 78-80
4. Volodymyr Hera, Yuri Shabatura. Analytical model of the optimal lubrication mode for internal combustion engines of arming and military machinery// SDirect24.org. International scientific journal published under the auspices of NATO Defence Education Enhancement Program.
5. https://docs.wixstatic.com/ugd/527eac_34095e707491497d87d24e830e62d995.pdf
6. Гера В. Я., Шабатура Ю. В. Підвищення бойових можливостей ОВТ за рахунок керованої мікропроцесором електромеханічної системи змащування ДВЗ // Збірник тез доп. НПК «Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності». 14-15 листопада 2019 року. – Львів:НАСВ, 2019. – С.22

Інформаційна безпека: сутність категорії

Ярема Оксана Григорівна

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

Проць Іванна Миколаївна

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

Відповідно до ст.17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Осягнення сутності категорії поняття «інформаційна безпека» є на сьогодні важливим і пріоритетними завданнями широкого наукового аналізу. Будь-яке вчення тоді лише досягає зрілості та досконалості, коли розкриває зміст досліджуваних явищ, має певні можливості передбачати майбутні зміни не тільки у сфері явищ, а і у сфері сутностей. Пізнання сутності поняття інформаційної безпеки стає можливим виключно на основі абстрактного мислення, формуваннясистемної теорії досліджуваного предмета, виявлення певних характерних ознак, розкриття основних характеристик та особливостей поняття, що вивчається.

Слід зазначити, що дефініція «інформаційна безпека» виникла із появою певних засобів інформаційних комунікацій між членами суспільства.

Інформаційна безпека це одне з найважливіших понять як в науці, так і в різних сферах людської діяльності [2, с. 293]. Зміст і сутність цього поняття знаходить свій вираз у характеристиці сучасного інформаційного суспільства. Інформаційна безпека не може, здебільшого розглядатися тільки як окремий стан, адже це поняття охоплює багатогранну сферу, основними елементами якої є життєво важливі інтереси певної соціальної системи, що

співвідносяться із зовнішніми чинниками як інтереси державних структур у рамках міжнародного співтовариства. Відповідно видове поняття «інформаційна безпека» означає стан захищеності національних інтересів в інформаційній сфері від внутрішніх і зовнішніх загроз.

Інформаційна безпека за сферою застосування в наукових колах поділяють на: інформаційну безпеку держави, інформаційну безпеку організації, інформаційну безпеку особистості. Однак, на нашу думку, у зв'язку з розвитком та впливом Інтернет ресурсів на свідомість людини, доцільно виділити ще один вид інформаційної безпеки під назвою інформаційна безпека дитини, адже саме у молодого покоління формуються хибні елементи світосприйняття через негативну інформацію, якою рясніє Інтернет. Отже, слід розглянути дані види інформаційної безпеки.

Інформаційною безпекою держави – можна вважати стан захищеності прав і свобод людини, життя і здоров'я якої визнаються найвищою соціальною цінністю в державі, при якому унеможливлюється нанесення шкоди через негативний інформаційний вплив, незаконне розповсюдження, поширення використання та порушення конфіденційності та доступності інформації.

Визначення інформаційної безпеки організації можна сформулювати як цілеспрямовану діяльність державних органів чи відповідних посадових осіб, яка полягає у використанніне заборонених сил та засобів, щодо досягнення стану захищеності певного інформаційного середовища підприємства, установи, організації, який сприяє забезпеченнюїї нормального функціонування і розвитку.

Інформаційна безпека особистості здебільшого характеризується як певний стан захищеності особистості від шкідливих впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору та свободу дій.

Інформаційну безпеку дитини можна вважати складовою інформаційної безпеки особистості та охарактеризувати як стан захищеності дитини від отримання небажаної інформації, що

може ставити під загрозу особистісну безпеку дитини як, наприклад, наслідок спілкування з небезпечними людьми [3].

На сьогоднішній день в Україні виникла потреба законодавчого регулювання поняття «інформаційної безпеки» з метою уникнення неоднозначного трактування даного терміну а також передбачення переліку інститутів, які охоплюватимуться даним поняттям. Щодо видів інформаційної безпеки, варто зазначити, що в наукових колах розрізняють три основні її види: інформаційну безпеку держави, інформаційну безпеку організації, інформаційну безпеку особистості, проте, вважаємо, що даний перелік не є досконалим, і можливо вартує термін інформаційна безпека організації, замінити більш ширшим терміном – інформаційна безпека юридичних осіб, а інформаційну безпеку особистості розглядати як інформаційну безпеку фізичних осіб, чи суспільства в цілому, що включатиме й поняття інформаційної безпеки неповнолітніх (дітей).

---

1. Конституція України від 28 черв. 1996 р. (зі змінами і допов.). Відом. Верхов. Ради України. 1996. № 30. Ст. 141.
2. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук : 12.00.07 Одеса. 2004. 427 с.
3. Ярема О. Г., Височанська І. В. Інформаційна безпека дитини в інтернет-просторі. Гендерні детермінанти вчинення насильства у сім'ї та правові основи протидії : *електронн. зб. матеріалів міжнародної науково-практичної Інтернет-конференції* 26-27. 05. 2016 р. Івано-Франківськ. Київ: Нац. акад. внутр. справ, 2016. С. 111-115.

Зміст

Розділ 1. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ, ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ, ЇХ ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ТА КОМПЛЕКСНОМУ ПІДХОДІ ДО ПРОБЛЕМ ДЕРЖАВНОЇ БЕЗПЕКИ 3

Гарасим П.С. Проблемні питання кримінальної відповідальності за злочини, пов'язані із службовим підробленням документів 4

Єсімов С.С. Цифрові права: новели законодавства 9

Живко З.Б., Руда О.І., Мандрик М.С. Управління інформаційною безпекою у інформаційних системах Національної поліції України 14

Зачек О.І., Рудий Т.В. Проблеми застосування вимог міжнародних стандартів під час здійснення процесуальних дій з цифровими доказами 20

Зачек О.І., Синківська І.А. Електрошокові пристрої: історія та принципи дії 26

Омельяненко О.В. Інформаційна підсистема «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» 33

Прокопов С.О., Пронічкіна А.С. Впровадження відеоаналітики в Україні: вітчизняний та зарубіжний досвід 38

Прокопов С.О., Темрієнко Н.В. Розвиток систем відеоаналітики у правоохоронній діяльності 42

Сеник В.В. Окремі проблеми у забезпеченні технічного захисту інформації у корпоративних мережах 47

Сидор В.В., Сеник В.В. Аналіз стану розвитку систем відеонагляду в діяльності Національної поліції України 51

Рижкова С.А. Використання інвазивних та неінвазивних засобів ідентифікації осіб з формами деменції в пошуковій роботі Національної поліції 55

Рудий Т.В., Сидорук І.І. Організаційно-правові аспекти захисту інформації у спеціалізованих інформаційних системах Національної поліції: стан і перспективи.....60

Фірман В.М., Худик О.А., Хміль М.М. Захист інформації в комп'ютерних мережах.....68

Цебинога В.Ю., Чумак В.В. Роль та значення інформаційних технологій у практичній діяльності органів досудового розслідування.....73

Чистоклетов Л.Г., Стародубцева Т.Л., Шишко В.В. Трансформації у розумінні інформації як безпекоформуючого чинника інформаційної безпеки України.....76

Ямкова Т.І. Історія розвитку інформаційного забезпечення органів Національної поліції України.....82

Розділ 2. НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНОТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ.....86

Глинський Я.М., Камінський Б.Т., Пелех Я.М. Змішане навчання інформатики.....87

Грищук А.Б. Інноваційні особливості електронного навчання для державних службовців із використання дистанційних освітніх технологій.....91

Грищук А.Б., Проць І.М. Перспективи впровадження навчально-інформаційних курсів в системі професійної підготовки державних службовців.....97

Зевако К.О. Застосування паралакс ефекту у ВЕБ-дизайні..103

Зубанський М.К. Електронна освіта, як спосіб підвищення професійного рівня державних службовців.....107

Ковалів М.В., Шимечко І.Б. Електронне навчання в системі професійної підготовки державних службовців МВС України.....115

Миронов Ю.Б., Сватюк О.Р., Миронова М.І. Особливості використання вебінарів у дистанційній освіті.....120

Мовчан А.В. Модель професійної підготовки фахівців з кримінального аналізу для підрозділів Національної поліції України.....125

Рейдало Т.М., Мирошниченко В.О. Інформаційні технології в освіті 132

Розділ 3. СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АКТУАЛЬНІ СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ ДІЯЛЬНОСТІ 136

Барбарич В.І., Івануса Ю.Р., Фірман Т.В. Застосування алгоритму PageRank для швидкого пошуку втрачених речей 137

Бортник Н.П. Цифровий порядок денний у правовому механізмі формування «Простору знань» в Європейському Союзі 140

Волянюк А.В. Співпраця щодо обміну інформацією між вітчизняними правоохоронними органами та західними правоохоронними інституціями: сучасний стан та перспективи подальшого розвитку 146

Гаврильців М.Т. Загрози інформаційній безпеці в умовах гібридної війни та напрями удосконалення системи інформаційної безпеки України 150

Грищук А.Б., Чабак В.Ю. Інформаційно-конституційні права людини і громадянина в сучасних реаліях 155

Дзвоник І.А., Фірман В.М. Застосування алгоритму k-середніх у діяльності поліції 160

Дуфенюк О.М. Напрями використання безпілотних літальних апаратів (дронів) органами поліції 162

Загайний Б.М., Грицюк Ю.І. Використання еволюційних алгоритмів для автоматизованого генерування віршових творів 166

Кобелька Д.М., Шаркадій П.І. Використання програмного забезпечення та пристроїв (гаджетів) в службовій діяльності НПУ під час реєстрації повідомлень про правопорушення та реагування на останні нарядами поліції 173

Кулешник Я.Ф., Шишко В.В. Роль інформаційного менеджменту в поліції 177

Лозинський І.А., Рудий Т.В. Правові аспекти формування політики інформаційної безпеки в інформаційних системах 183

Лукащук Б.С. Автоматизація методу визначення реальних розмірів об'єктів на зображенні із застосуванням референтного об'єкта 188

Лукащук Ю.А. Використання технології доповненої реальності для оцінки економічних ризиків функціонування підприємства 192

Луців І.І. Проблеми ідентифікації суб'єкта при отриманні публічних послуг в електронному вигляді..... 195

Магеровська Т.В., Магеровський Д.В., Полянська А.О. Оптимізація алгоритму колаборативної фільтрації на основі подібності профілів користувачів 199

Миджин Г.Є. Інтелектуальні права на цифрові розробки 205

Мілянець Т.М., Супик Р.Б., Фірман Т.В. Способи захисту особистих даних в інтернеті 208

Навроцька В.В. Застосування «Психотехнологій» при здійсненні кримінального провадження 210

Савайда О.І. Інформаційний простір як важіль державної безпеки..... 215

Сибірна Р.І., Зарічна О.З. Використання інформаційних технологій у галузі охорони здоров'я..... 218

Сибірний А.В., Хомів О.В. Сучасні інформаційні технології у діяльності науковця 222

Ткачук Т.Ю., Хитра О.Л. Інтренет-речі: гносеологічні засади розвитку та онтологічні константи сучасності 226

Шабатура Ю.В., Гера В.Я., Міхалєва М.С., Смичок В.Д., Ветренко Є.Д. Мікроконтролерний інформаційно-керуючий комплекс в системі змащування двигунів внутрішнього згоряння зразків озброєння та військової техніки..... 232

Ярема О.Г., Проць І.М. Інформаційна безпека: сутність категорії 239

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

Збірник наукових статей за матеріалами доповідей
Всеукраїнської науково-практичної конференції

20 грудня 2019 р.

Відповідальний за випуск Сеник В.В.
Упорядник Магеровська Т.В.
Макетування Магеровська Т.В.

Опубліковано в авторській редакції

Формат 60х84/16.
Гарнітура Times New Roman. Умов.друк.арк. 14,3
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.