Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

18 грудня 2020 року

Львів
2020

УДК 004

І 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 6 від 23.12.2020)

І 78 **Інформаційні технології в освіті та практиці** : матеріали Всеукраїнської науково-практичної конференції (Львів, 18 грудня 2020) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2020. 140 с.

У збірнику вміщено наукові статті та тези за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції «Інформаційні технології в освіті та практиці», що проводилася 18 грудня 2020 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

Цуцкіридзе М. С.,
заступник Голови Національної поліції України – начальник Головного слідчого управління,
доктор юридичних наук, доцент, заслужений юрист України

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасна Україна, що обрала своїм шляхом європейську інтеграцію, зобов'язана всіляко сприяти утвердженню прав і свобод людини і громадянина. Одним основних правоохоронних органів, що здійснюють такі функції є Національна поліція України.

Конституція України, визначає людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю [1], для забезпечення вказаних положень, необхідністю є наявна, ефективно та швидко функціонуюча система органів досудового розслідування кримінальних правопорушень.

Відповідно до чинного законодавства на органи досудового розслідування покладаються завдання із захисту особи, суспільства та держави від кримінальних правопорушень, охорони прав, свобод та законних інтересів учасників кримінального провадження, забезпечення швидкого, повного та неупередженого розслідування кримінальних правопорушень, віднесених до підслідності слідчих органів Національної поліції України та інші [2].

В свою чергу, питання оптимізації роботи органів досудового розслідування Національної поліції України, на сьогоднішній день є актуальним, оскільки в умовах стрімких євроінтеграційних процесів, системної роботи законодавця над удосконаленням чинного нормативно-правового підґрунтя функціонування окремих органів державної влади та стратегічної реформи кримінальної юстиції загалом, окремого опрацювання потребує впровадження електронної системи роботи з даними в досудовому розслідуванні та розвиток інформаційного забезпечення Національної поліції України загалом.

Запровадження єдиної електронної системи роботи з даними і матеріалами досудових розслідувань дозволить суттєво скоротити витрати робочого часу слідчих, дізнавачів Національної поліції України, необхідного для погодження рішень та процесуальних документів з органами прокуратури та судами. З метою підвищення ефективності розслідувань та запобігання корупції рекомендується представлення сучасної єдиної електронної системи роботи з даними і матеріалами досудових розслідувань Національній поліції України.

Як зазначають вітчизняні вчені, значний розвиток світової та вітчизняної електронної комунікаційної інфраструктури, який відбувся в останні десятиліття у різних сферах суспільного життя (особисте спілкування, бізнес, надання адміністративних послуг, державні та приватні он-лайн сервіси, доступ до реєстрів, е-декларування, тендерні закупівлі тощо) [3, с. 167–177], суттєво по впливав на відповідну сферу.

У той же час, відповідно до Плану-графіка виконання Україною умов Меморандуму про взаєморозуміння між Україною та Європейським Союзом щодо отримання Україною макрофінансової допомоги Європейського Союзу, відповідальними органами за виконання аналогічного критерію структурних реформ вказано Офіс Генерального прокурора, Спеціалізовану антикорупційну прокуратуру і Національне антикорупційне бюро України.

Офісом Генерального прокурора утворено робочу групу з розроблення концепції інтегрування до Єдиного реєстру досудових розслідувань програмного модуля «Електронне кримінальне провадження» та підготовки законодавчих змін для його використання в кримінальному процесі (накази Генерального прокурора від 21 лютого 2020 року № 104, від 15 квітня 2020 року № 193, від 15 травня 2020 року № 220).

Наразі в Національній поліції України існує базова кабельна інфраструктура для імплементації єдиної електронної системи роботи з даними і матеріалами досудових розслідувань, однак цей процес лімітований та потребує оптимізації з перспективою подальшої імплементації відповідних положень у функціонування органів досудового розслідування Національної поліції України. Ураховуючи те, що ця система ніколи не існувала в поліції України, є потреба в додатковому аналізі відповідних можливостей.

На сьогодні триває розроблення спільно з Офісом Генерального прокурора програмного забезпечення єдиної електронної системи роботи з даними і матеріалами досудових розслідувань.

Удосконалення безперервності та підзвітності проведення досудового розслідування, ведення електронного діловодства, у тому числі рух електронних документів у межах відповідних органів досудового розслідування та прокуратури та між ними, реєстрація вхідних і вихідних документів та етапів їх руху сприятиме оптимізації функціонування правоохоронних органів.

При цьому пріоритетом є захищеність зберігання документів у єдиній електронній системі роботи з даними і матеріалами досудових розслідувань (несанкціоноване втручання в роботу єдиної електронної системи роботи з даними і матеріалами досудових розслідувань повинно тягти за собою відповідальність, установлену законом). Цілком доцільним є подання, пересилання, обмін документами, учинення інших дій в електронній формі за допомогою єдиної електронної системи роботи з даними і матеріалами досудових розслідувань, що здійснюється з використанням електронного цифрового підпису.

Література:

1. Конституція України. Прийнята на п'ятій сесії Верховної Ради України 2-го скликання від 28.06.1996 р.// Відомості Верховної Ради України. – 1996. – № 30.

2. Кримінальний процесуальний кодекс України від 13 квітня 2012 року №4651-VI// Офіційний вісник України. – 2012. –№37.

3. Д. А. Патрелюк, Електронне кримінальне провадження як напрям подолання протидії кримінальному переслідуванню/ Вісник Південного регіонального центру Національної академії правових наук України, серія «Кримінальний процес та криміналістика;судова експертиза; оперативно-розшукова діяльність», № 15 (2018).

Шинкарук О. М.,
проректор Львівського державного університету внутрішніх справ, заслужений працівник освіти України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, професор

ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ВЕБ-СИСТЕМ ЗАСОБАМИ РОЗРОБКИ

На сучасному етапі розвитку засобів програмування в галузі веб-розробки кількість веб-фреймворків (ВФК) різко зросла. Всі вони володіють певною низкою переваг та недоліків, а тому актуальним є питання вибору правильного та відповідного фреймворку або їх набору для кожного конкретного проекту, адже від правильного вибору залежить якість, час реалізації та надійність кожного розроблюваного програмного продукту.

Взагалі кажучи, веб-фреймворки однозначно змінили та покращили своєю появою можливості програмування і стали невід'ємною частиною процесу розробки. Існує велика кількість інформації, що стосується ВФК, але часто ця інформація містить тільки визначення та складні терміни, які не дають ніякого уявлення про дані засоби. Саме тому питання обґрунтування варіативного вибору фреймворків та їх вплив на якість програмного забезпечення є актуальним завданням на сучасному етапі розвитку програмування.

Не зважаючи на те, що дослідження в галузі застосування фреймворків постійно проводяться, наукових робіт, присвячених варіативності вибору та доцільності їх використання в тій чи іншій сфері розробки та впровадження програмного забезпечення недостатньо, що і обумовило виявлення до даного завдання підвищеного наукового та практичного інтересу.

З урахуванням того, що веб-фреймворк є інструментом полегшення написання і запуску веб-додатків, розробнику не потрібно самостійно прописувати велику кількість коду та витрачати час на пошук потенційних прорахунків і помилок [1, 2, 3]. В сучасних умовах існує можливість вибору з наявних мов для веб-програмування відповідного фреймворку, як для статичних, так і для динамічних сторінок. Так, в залежності від поставленого завдання, необхідним є вибір одного ВФК, що здатний задовольнити всі потреби, або поєднання декількох.

Слід приймати до уваги, що у ВФК є дві основні функції: робота на серверній стороні (бекенд) і робота на клієнтській стороні (фронтенд). При цьому, фронтенд-фреймворки пов'язані із зовнішньою частиною програми, тобто відповідають за інтерфейс, а бекенд-фреймворки відповідають за внутрішню частину додатку, тобто логіку додатку.

Як показує практика, серверні веб-фреймворки (СВФК) не дають можливості створення веб-додатків з насиченим інтерфейсом. Вони обмежені в своїй функціональності, однак забезпечують створення простих сторінок і різних форм. Також, СВФК здатні забезпечити формування вихідних даних і відповідати за безпеку в разі атак. Все це, безумовно, може спростити процес розробки. Серверні фреймворки, в основному, відповідають за окремі, але критично важливі частини програми, без яких неможливе стале функціонування. Найбільш поширеними фреймворками такого типу і мови програмування, з якими вони працюють, слід виділити наступні:

- Django – Python;
- Zend – PHP;
- Express.js – JavaScript;
- Ruby on Rails – Ruby.

На відміну від серверних, клієнтські веб-фреймворки (КВФК) ніяк не пов'язані з логікою програми. Цей тип фреймворків працює в браузері. З їх допомогою можна поліпшити і впровадити нові користувальницькі інтерфейси. Фронтенд-фреймворки дозволяють створювати різні анімації і односторінкові додатки. Всі клієнтські фреймворки відрізняються по функціональності і використанню. Найбільш поширеними фреймворками такого типу слід виділити наступні:

- Backbone+Marionette;
- Angular;
- Ember.js;
- Vue.js.

Всі ці фреймворки використовують мову програмування – *JavaScript*.

Разом з типами фреймворків, що приведені вище, набули широкого використання для вирішення окремих завдань програмування й багатофункціональні фреймворки. *Meteor* відомий як фул-стек веб-фреймворк. Це означає, що він здатний задовольнити майже всі потреби як з боку клієнта, так і з боку сервера, що робить *Meteor* надзвичайно популярним. Його використання забезпечує заощадження часу, наприклад, на налагодження взаємодії між двома ВФК через *RESTAPI*. Використання, при цьому, ВФК *Meteor* забезпечить виконання відповідних процедур і прискорить процес розробки. Оскільки обидві сторони — серверна та клієнтська — працюють на одній мові, то існує можливість створення і використання для них одного коду. Одна з особливостей даного ВФК — «режим реального часу» — внесення змін в одному інтерфейсі, обумовлює зміни і в інших. Наприклад, при додаванні коментарів або зміні змісту документу або таблиці із загальним доступом, інші користувачі це також будуть бачити.

Окрему увагу слід приділити й розмірам (масштабам) фреймворків. Розрізняють ВФК, що здатні забезпечити рішення для всіх завдань, і більш легкі варіанти, які спеціалізуються на вирішенні конкретних завдань — такі фреймворки називаються мікрофреймворками. Останні не здатні забезпечити вирішення всіх завдань, проте іноді краще розкласти функціональність на кілька підходів (фреймворки, мікрофреймворки, бібліотеки). При цьому, слід зауважити, що розширення функціональності мікрофреймворків можливе за допомогою сторонніх додатків і створенням невеликих проектів на їх основі, або шляхом поєднання мікрофреймворку з основним «великим» фреймворком.

Наприклад, якщо додаток заснований на ВФК *Django* і потрібні веб-сокети, то є доцільним використання мікрофреймворку *aiohttp*. Або, якщо додаток не дуже великий і потрібна лише проста маршрутизація *URL* і шаблони з нескладним контекстом, то можливе використання ВФК *Flask* замість *Django*.

Незважаючи на те, що існуючі ВФК відрізняються один від одного, їх вибір може бути складним завданням, тому, слід навести кілька ознак, які є загальними для них усіх. Це архітектура і особливості, які важливі так, як і функції.

Також, слід зауважити, що мови і фреймворки, особливо на пізніх стадіях розвитку, це ортогональні речі. У розвинених екосистемах фреймворки, як правило, мають *API* для роботи з декількома мовами і навпаки: мови з великою екосистемою мають низку фреймворків, готових для використання. В сучасних умовах, при старті проекту, вибір фреймворку, зазвичай, стоїть на першому місці, ще до вибору мови. Якщо ж, наприклад, дістався *legacy*-проект, то, як правило, вибір мови відсутній. Мікросервіси, один з головних архітектурних трендів сьогоднішнього дня, намагається вирішити в тому числі і цю проблему — «звільнити» розробників від використання конкретної мови або фреймворку, щоб кожна частина проекту розроблялася на найбільш адекватних для неї технологіях.

Слід виділити важливі чинники, що дають гарантію надійності і стабільності фреймворку. Гарантія надійності фреймворка – його відмовостійкість. Правильна розробка, оптимізація запитів, ефективне кешування – ось запорука успіху. Наявність стабільних релізів, велика кількість користувачів, наявність автоматизованих тестів, наявність активності, *opensource* (відкритий код).

Приймаючи до уваги активність застосування ВФК слід систематизувати проведені дослідження напрямів їх розвитку. Так, проведений аналіз свідчить про те, що фреймворки будуть рухатися по шляху «полегшення» розробки. Типові рішення, готові модулі та інше – все для того, щоб непідготовлена людина змогла розгорнути сайт.

Для багатьох популярних платформ період нарощування функціональності пройшов. На даний момент розвиток сфокусовано на збільшенні швидкодії. Це справедливо і для *frontend*-, і для *backend*-фреймворків. В якості часткового рішення розглядається поділ фреймворка на логічні модулі. Для проекту повинен збиратися комплект бібліотек, що вирішують тільки необхідні завдання. А одним з рішень слід вважати щільніше з'єднання клієнтської та серверної частин фреймворків з єдиним синтаксисом та логікою роботи із контентом. Принцип «спрощення», який описано вище, призводить до того, що фреймворки стають складнішими за змістом, але все простішими для користувача.

Розвиток фреймворків залежить від потреб ринку та можливостей браузерів і призначених для користувача девайсів. Подальше удосконалення фреймворків, безпосередньо, залежить від розвитку і появи нових платформ, як, наприклад, розробка технології *Canvas*, *WebGL Node.js*–обумовила появу ВФК по роботі з ними.

Висновки. Отже, проаналізувавши ряд наукових робіт, що стосуються використання фреймворків для розробки програмного забезпечення наочним є висновок, що незважаючи на велику популярність даних засобів, існують й протиріччя у їх використанні.

Вибір відповідного фреймворка є однією з основних засад, що визначає якість майбутнього сайту. Кожну з технологій, що наведені у даній статті можна вважати вичерпною у всіх відношеннях тому, що їх використовують, як у практиці перетворення в графічний інтерфейс (*frontend)*, так і для розробки варіанту архітектури програмного забезпечення (*backend*). Тому, слід обирати платформу у відповідності до зручностей щодо мов програмування.

Отже, *Agile* найбільше підходить для проектів із «відкритим кінцем», наприклад, запуск інтернет-сервісів, розробка комп'ютерних ігор, операційних систем. Однак, гнучкість може приводити до втрати фокусу та втрати передбачуваності. Дуже важливо відокремлювати помилки застосування гнучкого підходу від недоліків самої методології. Перш, ніж будуть реалізовані всі переваги підходу, потрібно буде деякий час на адаптацію до реалій конкретних завдань.

Література:

1. Интернет-аудитория Украины. Статистика 2012-2013 и прогноз на 2014 год [Электронный ресурс] / Netpeak. Режим доступак ресурсу: www/ URL: http://blog.netpeak.ua/internet-auditoriya-ukrainy-statistika-2012-2013-i-prognoz-na-2014- god.
2. Мейерт Д. О. Небольшая книга о HTML /CSS фреймворках [Текст] / Д. О. Мейерт// Орейли. – 2015. – 30 с.
3. Агалаков С. А. Статистические методы анализа данных [Текст] / С.А. Агалков. – 18 с.

Дударець Р. М.,
заступник начальника Головного слідчого управління Національної поліції України,
кандидат юридичних наук

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КОНТЕКСТІ ВЗАЄМОДІЇ СЛІДЧОГО З ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ

Національна поліція України є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [1]. Питання боротьби та протидії злочинності є одним із найбільш пріоритетних завдань як поліції в цілому так і органів досудового розслідування, що їй підпорядковані, зокрема.

Стрімкий розвиток інформаційних технологій, технічний прогрес та інші чинники, дозволяють здійснювати намагання щодо оптимізації роботи слідчих органів та підрозділів з якими вони взаємодіють в даній площині.

Використання інформаційних систем і технологій в контексті взаємодії оперативних підрозділів та органів досудового розслідування Національної поліції України, дозволить суттєво покращити ефективність розслідування та пришвидшити його.

Перш за все, оскільки взаємодію розглядають як спільну, узгоджену за часом, способами, засобами діяльність двох або більше уповноважених компетентних суб'єктів, спрямовану на досягнення спільної мети, на чому слушно акцентує увагу М. П. Климчук, підкреслюючи, що під час взаємодії слідчого й оперативних підрозділів під час досудового розслідування між ними виникають не лише кримінально-процесуальні правовідносини, а й ділове співробітництво, відбувається якісне об'єднання сил, засобів і методів, що забезпечує оптимізацію процесу розслідування злочинів для найбільш якісного й ефективного виконання завдань, що стоять перед досудовим розслідуванням [2, с. 54].

Зокрема, основним завданням взаємодії слідчого з оперативними підрозділами є запобігання, виявлення та розслідування кримінальних правопорушень, притягнення до встановленої законодавством відповідальності осіб, що їх учинили, відшкодування завданої шкоди, відновлення порушених прав і законних інтересів громадян та юридичних осіб, забезпечення безпеки держави загалом.

Вчені зазначають, що сьогодні основними напрямами використання інформаційних технологій у досудовому слідстві є створення та ведення криміналістичних обліків, побудова суб'єктивних портретів, користування базою законодавства України та іншими базами даних. У сучасних вимогах слідчим потрібні інформаційні технології для оптимізації управління процесами інформаційного забезпечення, здійснення автоматизованого пошуку відомостей щодо будь-яких об'єктів (осіб, предметів, подій), одержання формалізованих знань з усіх видів баз даних, що існують у світі, статистичного і географічного аналізу подій, пошуку окремих об'єктів, осіб та інші [3].

Інформатизація соціального середовища призвела до «технологізації» криміналістики, розробки і впровадження інформаційних, цифрових, телекомунікаційних технологій. Інформаційні технології – нова категорія криміналістики, що претендує на належне місце в її структурі. Використання технологічного підходу здійснюється не лише в криміналістичній техніці, а й у криміналістичній тактиці і методиці (технології провадження окремих слідчих дій, слідчі або криміналістичні технології) [4].

Інформаційні технології надають можливість оперативного збирання, зіставлення та аналізу відомостей з різних джерел (повідомлень, результатів оперативно-розшукових заходів, допитів, адресної бази даних тощо), установлення хронологічної послідовності подій за часом та відповідності окремих фактів, дозволяють здійснювати складання планів та схем місця події, моделювання події злочину за допомогою комп'ютерної техніки та ін. [5, с. 196–197].

Важливо підкреслити, що наприклад, до підрозділів кримінальної поліції, зокрема, належить Департамент кіберполіції [6], що найбільш ефективно співпрацює з органами досудового розслідування, в контексті застосування інформаційних технологій у ході проведення слідчих (розшукових) дій, оперативних заходів та інших процесуальних дій і прийнятті процесуальних рішень.

Підрозділи кіберполіції вживають передбачених чинним законодавством заходів: зі збирання й узагальнення інформації стосовно об'єктів, зокрема сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення злочинів; щодо викриття причин та умов, які призводять до вчинення злочинів у сфері протидії кіберзлочинності; щодо аналізу та систематизації даних про злочини, вчинених в сфері протидії кіберзлочинності та з використанням новітніх технологій, що надходять від громадян каналами кол-центрів, електронними листами й терміналами зворотного зв'язку; зі збирання, узагальнення, систематизації й аналізу інформації про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінюють результати за окремими показниками службової діяльності, надають, відповідно до законодавства України, звіти про результати роботи й відповідну інформацію керівництву НПУ, МВС, органам державної влади з питань попередження та протидії кіберзлочинам [7].

Таким чином, взаємодія органів досудового розслідування з оперативними підрозділами (до яких в складі кримінальної поліції Національної поліції України відноситься, в тому числі Департамент

кіберполіції) Національної поліції України, базується на засадах партнерства та співпраці та здійснюється виключно в межах чинного законодавства України.

Основними напрямами взаємодії в контексті використання інформаційних технологій є можливість відстеження кримінальних правопорушень, що вчиняються в мережі інтернет, припинення вже розпочатих кримінальних правопорушень, що вчиняються за допомогою інформаційних технологій загалом та цифрових технологій зокрема.

Перспектива подальших наукових розвідок у зазначеному напрямі, базується на необхідності імплементації напрацювань у сфері створення нових баз даних, пошукових систем, систем обміну інформації, чат-ботів, довідникових програм та іншого програмного забезпечення, а також удосконаленні вже існуючих можливостей.

Література:

1. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: http://zakon5.rada.gov.ua/laws/show/580-19.
2. Климчук М. П. Виконання доручень як форма взаємодії слідчих та оперативних підрозділів у кримінальному провадженні. Вісник кримінального судочинства. 2015. № 1. С. 54–58.
3. Рогатюк Ігор Володимирович, Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку/Науковий вісник Національної академії внутрішніх справ, № 3, 2013.
4. Шепитько В. Ю. Изменчивость криминалистики в XXI веке и ее задачи в современных условиях / В. Ю. Шепитько // Криміналістика XXI століття : матер. міжнар. наук.-практ. конф. (25–26 листоп. 2010 р.). – Х.: Право, 2012. – С. 57–58.
5. Шепітько В. Ю. Інформаційні технології в криміналістиці та слідчій діяльності / В. Ю. Шепітько, Г. К. Авдєєва // Питання боротьби зі злочинністю. – 2010. – № 19. – С. 194–202.
6. Структура Национальной полиции Украины. Инфографика. НВ Украина: [сайт]. URL: https://nv.ua/ukraine/events/struktura-natsionalnoj-politsii-ukrainy-infografika-85757.html.
7. Про затвердження Положення про Департамент кіберполіції Національної поліції України : наказ Національної поліції України від 10 листоп. 2015 р. № 85. URL: http://tranzit.ltd.ua/nakaz.

Корнейко О. В.,
завідувач кафедри інформаційних технологій та кібербезпеки ННІ № 1 Національної академії внутрішніх справ, кандидат технічних наук, професор

Школьніков В. І.,
старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, т.в.о. начальника Центру кримінальної аналітики НАВС

Овсянюк Д. І.,
начальник відділу Департаменту кримінального аналізу Національної поліції України

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ЦЕНТРУ КРИМІНАЛЬНОЇ АНАЛІТИКИ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Останнім часом сучасні інформаційно-аналітичні технології знайшли широке застосування для попередження, розслідування, розкриття та прогнозування кримінальних правопорушень правоохоронними органами України, зокрема підрозділами кримінального аналізу Національної поліції (НП) України.

Тому вивчення та розвиток новітніх технологій та методик здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи є одним із важливих напрямів освітньої та наукової діяльності кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ (НАВС).

Зважаючи на досягнення кафедри в цій сфері, відповідно до спільного рішення керівництва НАВС та Департаменту кримінального аналізу (ДКА) НП України, на підставі рішення Вченої ради НАВС від 7 липня 2020 року в НАВС було утворено Центр кримінальної аналітики (надалі – Центр) як самостійний структурний підрозділ академії.

Головна мета створення Центру полягає в налагодженні тісної співпраці НАВС з ДКА НП України, іншими аналітичними підрозділами НП та правоохоронних органів України щодо спільної діяльності у сфері здійснення наукових досліджень, підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері кримінального аналізу та сучасних інформаційно-аналітичних технологій.

Основними напрямами діяльності Центру є:

- проведення аналітичних досліджень з оцінки, випробування та впровадження новітніх інформаційно-аналітичних технологій та спеціалізованих програмних засобів щодо здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи, широке залучення до цієї діяльності курсантської молоді, слухачів, ад'юнктів, аспірантів, науково-педагогічних та наукових працівників НАВС, а також практичних працівників органів та підрозділів НП й інших правоохоронних органів України;
- надання допомоги підрозділам НАВС, ДКА, інших підрозділів НП та правоохоронних органів України щодо впровадження в їх практичну діяльність відповідних методик та програмних засобів, що розроблені Центром для здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи;
- участь у проведенні інтерактивного навчання з сучасних технологій здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи у формі групових тренінгових занять, дистанційного навчання та традиційних форм навчання з курсантами, слухачами, студентами, науково-педагогічними та науковими працівниками НАВС, а також з практичними працівниками НП та інших правоохоронних органів України;
- надання пропозицій та здійснення участі щодо проведення НАВС наукових заходів (у формі наукових досліджень, конференцій, форумів, круглих столів тощо), а також освітніх заходів (тренінгів, семінарів, вебінарів, підвищення кваліфікації працівників тощо) з питань кримінального аналізу та інформаційно-аналітичної роботи;
- здійснення консультативно-інформаційної підтримки здобувачів вищої освіти, постійного складу НАВС, працівників апарату МВС України, підрозділів НП й інших правоохоронних органів України з питань сучасних технологій здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи, участь у налагодженні НАВС партнерських зв'язків з аналітичними підрозділами НП та інших правоохоронних органів України з цих питань;
- участь у розробці змін до чинного законодавства України, нормативно-правових актів МВС та НП України з метою врегулювання процедури, методик та інформаційно-аналітичного забезпечення здійснення кримінального аналізу в правоохоронних структурах України;
- розповсюдження передового досвіду Центру, НАВС та ДКА, налагодження співпраці з подібними підрозділами, громадськими організаціями, асоціаціями кримінальних аналітиків тощо в Україні та за кордоном.

Для забезпечення діяльності Центру в НАВС є відповідна сучасна матеріально-технічна база. Так, академія зареєстрована на відповідних освітніх порталах (Octopus Cybercrime Community, «SPACE» – The Secure Platform for Accredited Cybercrime Experts) та приймає участь в навчальних програмах (Microsoft Office for Education, Gsuit for Education, IBM Academic Initiative), які дозволяють отримувати ліцензоване програмне забезпечення та проводити освітній процес на високому методологічному рівні.

Хоча Центр тільки розпочав свою діяльність, але за час свого функціонування його співробітниками:

- на підставі звернення керівництва ДКА було проведено на платформі Google Classroom онлайн тренінги «MS Excel у кримінальному аналізі» та «Аналітичні програмні продукти в кримінальному аналізі (Microsoft Excel, IBM i2 Analyst's Notebook, Power BI, ArcGIS)» для співробітників підрозділів кримінального аналізу, внутрішньої безпеки, кіберполіції, карного розшуку, оперативно-технічних заходів, оперативної служби, протидії наркозлочинності та боротьби зі злочинами, пов'язаними з торгівлею людьми НП України;
- спільно з працівниками ДКА, кафедри оперативно-розшукової діяльності та кафедри інформаційних технологій та кібербезпеки НАВС підготовлено ряд практичних посібників, що детально розкривають специфічні методики проведення кримінального аналізу, а саме: «Кластерний аналіз інформації про телефонний трафік»; «Обробка та аналіз за допомогою MS

Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами»; «Обробка та аналіз інформації з Державного реєстру нерухомого майна Міністерства юстиції України»; «Обробка та аналіз інформації з інформаційно-аналітичного комплексу «Безпечне місто»;

- взято участь у розробленні законопроєктів № 4003 від 1 вересня 2020 року «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» і № 4004 від 1 вересня 2020 року «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів»;
- здійснюється науково-аналітичне опрацювання результатів проведеного онлайн курсу з кібергігієни для працівників апарату МВС України (у межах спільного проєкту Консультативної місії Європейського Союзу й української компанії з кібербезпеки ISSP), а також підготовка відповідних методичних рекомендацій.

Центром спільно з працівниками ДКА, кафедрою оперативно-розшукової діяльності та кафедрою інформаційних технологій та кібербезпеки НАВС підготовлено ряд практичних посібників, що детально розкривають специфічні методики проведення кримінального аналізу, а саме:

- «Кластерний аналіз інформації про телефонний трафік»;
- «Обробка та аналіз за допомогою MS Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами»;
- «Обробка та аналіз інформації з Державного реєстру нерухомого майна Міністерства юстиції України»;
- «Обробка та аналіз інформації з інформаційно-аналітичного комплексу «Безпечне місто».

Окрім цього, Центром розроблюються методики встановлення та візуалізації спільних маршрутів перетину осіб, транспортних засобів на основі телефонного трафіку, даних з інформаційно-аналітичного комплексу «Безпечне місто» тощо. Це стало можливим внаслідок апробації геоінформаційного комплексу ArcGIS в освітню та наукову діяльність НАВС, який є найбільш потужним програмним продуктом для здійснення аналізу інформації з використання можливостей геовізуалізації.

Більш детальна інформація про впровадження геоінформаційного комплексу ArcGIS в діяльність НАВС висвітлено на XXIII щорічній конференції «ESRI Ukraine. User Conference» за посиланнями:

1. https://youtu.be/PP87OEtl_Ro?t=6500

2. https://youtu.be/PP87OEtl_Ro?t=7981

Іншим актуальним напрямком діяльності Центру є напрацювання відповідних методик обробки та аналізу інформації з відкритих джерел, у тому числі мережі Інтернет. Крім того, на сьогодні працівниками Центру розроблено алгоритми завантаження інформації про біткоїн транзакції з використанням технології API-інтерфейсу з метою подальшого аналізу цієї інформації в програмному продукті IBM i2 Analyst's Notebook.

Таким чином, стрімкий розвиток сучасних інформаційно-аналітичних технологій зумовлює переосмислення змісту поліцейської діяльності, розвиток відповідних методик задля ефективного попередження, розслідування, розкриття та прогнозування кримінальних правопорушень. Здійснення освітньої та наукової діяльності закладів вищої освіти системи МВС України у сфері кримінального аналізу є одним із напрямів підготовки нової генерації сучасних українських поліцейських.

Гнусов Ю. В.,
завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

Струков В. М.,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ДО ПИТАННЯ ГАРМОНІЗАЦІЇ ІНДИВІДУАЛЬНОГО ПРАВА З ГРОМАДСЬКИМИ, ДЕРЖАВНИМИ І МІЖНАРОДНИМИ ПРАВАМИ В УМОВАХ ВИСОКОТЕХНОЛОГІЧНОГО ТУРБУЛЕНТНОГО СВІТУ

Світ стрімко входить в епоху глобалізації на тлі блискавичних змін у сфері високих технологій, які вже у найближчі 5-7 років докорінно змінять світ. Ці зміни супроводжуються зростаючими масштабами загроз з боку злочинних угрупувань і ставлять світову спільноту перед необхідністю розробки нових підходів до гармонізації століттями напрацьованих демократичних цінностей і потребами адекватної реакції правоохоронних органів на нові виклики з боку вуличної і організованої злочинності. Справа в тому, що в контексті стрімкого розвитку найсучасніших технологічних інструментів, які вже стали доступними не тільки організованим злочинним угрупуванням, а й невеликим вуличним бандам і, навіть, окремим злочинцям, правоохоронні структури у всьому світі постають перед безумовною необхідністю переходу від реактивної парадигми діяльності до проактивної. А це, в свою чергу, ставить питання про отримання необхідної інформації з будь-яких джерел про підготовку до скоєння злочинів. Радикальний спосіб полягає у всеосяжному відеоспостереженні і законному отриманні інформації про будь-які фінансові транзакції, так як це зроблено, наприклад, у Китаї. Але в країнах західної Європи і США, де сторіччями сформовані і закріплені на законодавчому рівні традиції недоторканості приватного життя і приватної власності, такий підхід викликає у спільноти несприйняття і протидію. З цим зіткнулися, зокрема, розробники відомої платформи ePOOLICE [1, 2]. Але і в демократичному суспільстві обставини спонукають уряди рухатися в напрямку сприяння проактивним діям правоохоронних органів.

Незважаючи на протиріччя, які все більш загострюються, в базових документах, що розглядаються міжнародним правом, як основоположні документи у сфері національної безпеки, чиї вимоги і принципи мають пріоритет по відношенню до змісту будь-яких інших документів, а саме, в доповіді ООН «Про безпеку людини» (2003 р.) і в Європейській Доктрині з безпеки (2004 р.) безпека визначається як «безумовне забезпечення прав, свобод і недоторканості приватного життя законослухняних громадян при дотриманні вимог національної та міжнародної безпеки».

Така юридична конструкція в казуїстичному, буквально юридичному сенсі слова ставить індивідуальне право вище не тільки групових і державних, а й громадських прав. Однак в Стратегії безпеки ЄС, прийнятій в тому ж 2004 році, підкреслюється «необхідність діяти активно в рішенні ключових загроз національній безпеці та прав громадян». Аналіз цих документів свідчить про те, що навіть в Європі, яка має найбільш давні правові традиції, на сьогодні є двозначне трактування взаємин між національною і приватної безпекою. У численних документах ООН, ЄС, НАТО, інших міжнародних організацій є ідентичні заголовні пункти, які передбачають «активну позицію держави і міжнародного

співтовариства щодо ризиків і загроз, включаючи нові непізнані ризики і загрози, пов'язані з тероризмом, ОЗ, кіберкримінальними угрупуваннями, міжнародною мережею тіньового банкінгу, корупції і відмивання грошей».

Проактивна діяльність правоохоронних структур на сучасному рівні передбачає можливість застосовувати передові методи аналізу Великих Даних, штучного інтелекту, а також системи збору інформації про поодинокі події, осіб, суб'єктів та об'єктів, не тільки залучених до злочинної діяльності або пов'язаних з нею, а й тих, чиї інформаційні файли можуть підвищити якість прогнозів.

З цієї причини все більше політиків, представників правоохоронних органів, розвідувального співтовариства, відповідальних мислителів приходять до висновку, що тотальне цифрове спостереження стає невід'ємним компонентом політики безпеки в високоризикованому цифровому суспільстві.

У цих умовах перед демократичними державами постає завдання встановити відповідно до обстановки, що змінилася, новий баланс між двома акторами безпеки - державами і громадянами. Цей новий баланс повинен дозволити не на словах, а на ділі реалізовувати проактивну, а не реактивну стратегію боротьби зі злочинністю, а й поступово переходити від підвищення рівня розкриття злочинів до превентивного їх припинення вже на стадії їх планування.

Відомо, що права і прозорість громадянина для суспільств і держав не суперечать один одному. Виходячи з історичних традицій, інформаційна прозорість життя громадянина не суперечить демократії тоді і тільки тоді, коли держава сама по собі контролюється і підзвітна громадянам, а не тоталітарним правителям. Кордон між демократією і авторитаризмом проходить не за ступенем відкритості приватного життя громадян в умовах високотехнологічного, а відповідно і нестійкого ризикового суспільства, а по межі підзвітності держави суспільству, можливості суспільства змінити в легітимному порядку будь-яку посадову особу в разі, якщо вона порушила найважливіший принцип демократії - рівність прав і відповідальності.

«Експерти Європолу вважають, що держава може запропонувати за згодою всіх основних політичних сил громадянам новий контракт безпеки, який змінить контракт, який проіснував майже століття. Попередній контракт базувався на тому, що головні загрози суспільству несуть зовнішні вороги, а тому держава може забезпечити безпеку громадян в умовах недоторканності їх приватного життя. У новому соціальному контракті держава повинна чесно повідомити громадянам, що в високоризикованому турбулентному світі немає більше внутрішніх і зовнішніх ворогів, є законослухняні громадяни, ті, хто налаштований на творення і живе не тільки за законами, а й за цінностями - з одного боку, і злочинці , терористи, зловмисні мафіозні держави - з іншого. У цих умовах держава може забезпечити безпеку лише тих громадян і організацій, які добровільно підуть на пом'якшення стандартів недоторканності приватного життя і комерційної таємниці в межах, необхідних для дотримання вимог національної, континентальної або іншої колективної безпеки. При цьому в контракті повинні бути чітко прописані заходи, за допомогою яких громадяни, суспільство і бізнес можуть контролювати не абстрактну державу, а конкретні інститути і персонально чиновників - від голів урядів до голів департаментів – в частині невикористання ними даних в будь-яких цілях, ніж відбиття загроз безпеки» [1].

Будь-які обмеження цифрових прав громадян на приватність повинні бути строго сформульовані з таким ступенем точності, щоб громадяни точно розуміли, в яких випадках, з чиєї санкції і як будуть збиратися їх особисті дані, як використовуватися, як і коли знищуватися. Все це повинно бути прописано не у відомчих документах, а в законодавствах окремих країн. Крім того, додаткові можливості збору персональної інформації повинні бути збалансовані з реальними потребами розслідувальних і прогнозно-моніторингових інформаційних платформ.

Ці обмеження повинні носити часовий характер, і бути ув'язані не з конкретними побажаннями парламентарів і урядовців, а спиратися на підтверджені компетентними фахівцями вимоги до інформації, що збирається з боку проектантів прогнозно-моніторингових і розслідувальних платформ. Треба чітко усвідомити, що в даному випадку не програмно-апаратні рішення слідують за законом, а навпаки, закон відгукується на нові потреби правоохоронців, при цьому чітко встановлюючи терміни дозволу. Якщо з'ясується, що система виявилася неефективною, дозвіл має бути відкликано. З іншого боку, якщо з'явилося нове покоління систем, дозвіл має бути модифіковано.

Щоб звести до мінімуму порушення прав на недоторканність приватного життя і оцінити обґрунтованість обмежень, необхідно на основі узгоджених оцінок встановити отриманий ефект в боротьбі

з ОЗ за рахунок експлуатації платформи, чия база даних поповнюється даними, що знову збираються. Можливо, в першу чергу слід покінчити з приватністю у власності і джерелах її придбання. З одного боку, на цей рахунок є відповідні конвенції ООН, є численні рішення на рівні урядів, парламентів і ЄС щодо припинення відмивання грошей і проникнення злочинних доходів в легальні сфери. В останні роки уряди низки країн, перш за все США, Великобританії, Швейцарії, багатьох країн ЄС прийняли законодавство про обов'язкове розкриття кінцевих бенефіціарів, зареєстрованих юридичних осіб. Крім того, здійснюються активні заходи щодо поступового переходу на електронні гроші.

Нарешті, широка громадськість спонукає уряди і парламенти вжити активних заходів проти тих мільярдерів і мультимільйонерів, які не платять податки або за допомогою податкових юристів законними або зовсім законними способами мінімізують власне оподаткування.

Існують також певні технічні механізми і засоби компромісного вирішення поставленої проблеми. Прикладом компромісного вирішення протиріччя конфіденційності персональних даних і потреб поліцейських розслідувань може слугувати застосування гомоморфного шифрування при використанні правоохоронними органами хмарних платформ в цілях збереження і обробки даних.

В цілому, зауважимо, що шляхи вирішення сформульованої проблеми лежать як у технічній площині так і в правовій. Причому будь-який один із них не визначає повного розв'язання. Технічні варіанти рішення повністю не розв'язують проблеми. Питання про її принципове вирішення лежить у правовій площині. І оскільки організована злочинність в умовах глобальної цифровізації світового суспільства все більше і більше набуває транснаціонального характеру, то, в першу чергу, це є сфера міжнародного права.

Література:

1. Ларина Е.С. Искусственный интеллект. Большие данные. Преступность. / Ларина Е.С., Овчинский В.С.: М.: Книжный мир; 2018. 166 с.

2. Інформаційні технології у правоохоронній діяльності. Частина 1: Високотехнологічні тренди у правоохоронній сфері зарубіжних країн: навч. посіб. / Харків. нац. ун-т внутр. справ; [В.М. Струков, Д.Ю. Узлов, Ю.В. Гнусов та ін.] ; за заг. ред. канд. техн. наук, доц. В.М. Струкова. Харків : ТОВ «ДІСА ПЛЮС», 2020. 276 с.

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

Мирошниченко В. О.,
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ТРАНСФЕР ТЕХНОЛОГІЙ В ЧАСТИНІ ПАТЕНТНОЇ ДІЯЛЬНОСТІ ЯК ЗАПОРУКА УСПІХУ ВІДОМЧОЇ НАУКИ ТА ОСВІТИ

Патентна діяльність притаманна віщий школі за своєю суттю та є складовою оцінки інноваційності діяльності науково-педагогічних колективів. Врахування її результативності на рівні рейтингів типу ТОП-200, стимулює появу нових заявок на винаходи та корисні моделі із року в рік [1]. При цьому учасники патентної діяльності на рівні кафедр та лабораторій гарантовано отримують позитивне обчислення у своєму годинному навантаженні позиції, що є первинним стимулом їх діяльності з цими продуктами інтелектуальної творчості. Цей стимул не зникає у разі невдалої спроби, тобто при відмові визнати придатним представлений до експертизи матеріал. У разі позитивного рішення щодо визнання матеріалу заявки та отримання відповідного патенту ініціатор крім іншого отримує додаткові облікові години та рейтингові бали відносно себе, на рівні свого підрозділу та навчального закладу. Проте, у переважній більшості випадків патент залишається на папері без перспектив його подальшого розвитку та існування на рівні матеріального об'єкту, здатного принести конкретну користь суспільству, відомству, практиці. Основною проблемою є відсутність знань, досвіду та можливостей у авторів патентів щодо трансферу технологій без яких предмет патентної діяльності значно втрачає шанси на свою матеріалізацію.

Ланцюг проходження ідеї до її практичного втілення обумовлює співпрацю теоретика-дослідника, дослідника-практика, дослідника-технолога, технолога-виробника, маркетолога-продавця на рівнях взаємодії інноваційного центру, адміністрації, преси, банківської установи, допоміжного виробництва [2].

Технічним вишам подолати цю проблему легше, бо вони, як правило, пов'язані із виробництвом у силу своєї специфіки [3]. Навчальним закладам із особливими умовами навчання, які функціонують в системі Міністерства внутрішніх справ складніше. Особливо тим, які готують фахівців для органів та підрозділів Національної поліції. Традицій щодо трансферу патентної діяльності в них, як правило, немає. Є лише окремі позитивні випадки. Проте ця позиція як оціночний критерій діяльності науково-педагогічних колективів, в тому числі при проведенні відомчого конкурсу наукових робіт за номінацією патенти, є і вже не один рік. Сама ж ідейна складова патентної діяльності дуже різнопланова: від створення пристрою визначення ділянки електричної мережі з несанкціонованим підключенням електроприймачів, до вдосконалення відомчої системи «ЦУНАМІ» та вдосконалення радіолокаційних пристроїв в період військового протистояння в країні [4].

Як подолати цю проблему та підвищити ефективність патентної діяльності у кінцевому рахунку – кожний із суб'єктів вирішує окремо. Проте завдання настільки важливе та одночасно складне, що потребує, на наш погляд, колективного осмислення проблеми та знаходження варіантів щодо свого вирішення.

З огляду на зазначене, цьому буде сприяти:

- підвищення обізнаності щодо патентної діяльності взагалі для більш широкого загалу наукових та науково-педагогічних працівників з метою їх подальшого залучення до патентної діяльності як потенційних винахідників;
- вивчення первинними суб'єктами патентної діяльності теорії і практики трансферу технологій. Обов'язково із врахуванням особливостей сфери діяльності Міністерства. Обмін набутим досвідом;
- визначення можливостей навчального закладу (наукової установи, кафедри, лабораторії) на рівні дослідження ринку, запровадження наукових розробок у виробництво на рівні регіону/країни;
- напрацювання досвіду встановлення договірних відносин із суб'єктами виробничих потужностей задля подальшого просування на ринок результатів патентної діяльності;
- сприяння та стимулювання цієї діяльності на рівні свого Міністерства та навчального закладу як одного із інноваційних видів діяльності, здатного потенційно вплинути на позитивну оцінку з боку суспільства. Позиціонування цієї діяльності як фактору, який сприяє підвищенню конкурентоздатності країни в цілому.

Таким чином, трансфер технологій в частині патентної діяльності у вищих навчальних закладах системи МВС зі специфічними умовами навчання повинен набути свого логічного розвитку, з часом стати постійною позитивною практикою та практичним закріплення інтелектуальних здобутків науково-педагогічних колективів.

Література:

1. Незалежне оцінювання університетів: академічний рейтинг "ТОП-200 Україна 2020" //URL: http://euroosvita.net/index.php/?category=11&id=6556

2. Что же такое "трансфер технологий"?: Инновации и предпринимательство: гранты, технологии, патенты // URL: http://www.innovbusiness.ru/content/document_r_A8A395F8-516E-4E8C-A828-C5B563210574.html

3. Промислова власність у цифрах за 2019 рік: ЗВО з найвищою винахідницькою активністю //URL: http://www.euroosvita.net/index.php/?category=1&id=6359

4. Система управління нарядами мобільної патрульної служби [Вишня В.Б., Глуховеря В.А., Золотоноша О.В., Рижков Е.В.] Патент України на корисну модель № 118449, Україна., Заявка № u201701677, МПК H04B 1/04. Бюл. №15., 10.08.2017; Пристрій радіолокаційного розпізнавання об'єктів [Гавриш О.С., Махницький О.В., Мирошниченко В.О., Рижков Е.В., Фоменко А.Є.] Патент та корисну модель № 139240 МПК G01S 13/00, G01S 13/52 (2006.01)., Бюл. № 24/2019., 26.12.2019

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

Міхалєва М. С.,
професор кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Атаманюк В. В.,
заступник завідувача кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

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

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

МЕТОДИКА ОЦІНКИ ПОТЕНЦІЙНИХ РЕСУРСІВ ГЕНЕРАЦІЇ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ЗА РАХУНОК ВИКОРИСТАННЯ РОЗСІЮВАНОЇ ЕНЕРГІЇ ВОГНЕПАЛЬНОЇ ЗБРОЇ

Озброєння і військова техніка, які використовуються в підрозділах силових відомств України постійно оновлюються, модернізуються або дооснащуються різноманітними системами і механізмами, які потребують для свого функціонування електричної енергії. Вирішення задачі забезпечення їх електричною енергією традиційно вирішується за рахунок використання електрохімічних джерел (гальванічні батареї, акумуляторні батареї), електромеханічних генераторів з приводом від двигунів внутрішнього згоряння. Останніми роками арсенал цих засобів поповнився джерелами відновлювальної енергетики, це вітрові електрогенератори, сонячні фотогальванічні перетворювачі та паливні елементи [1]. Однак зазначені вище, як традиційні так і нетрадиційні джерела електричної енергії мають ряд недоліків. Виконаємо їх короткий аналіз.

Електрохімічним джерелам електричної енергії властива обмеженість в потужності, обмеженість в часі зберігання запасу енергії, деградація, пов′язана з кількістю циклів заряду-розряду для акумуляторних батарей, а також добре виражена залежність ємності від температури зовнішнього середовища. Електромеханічні генератори з приводом від двигунів внутрішнього згоряння не можуть бути задіяні миттєво, вони потребують певного часу на розгортання, крім того їхня робота пов′язана з створенням демаскуючих ознак та потребує значних паливних ресурсів. Зазначені вище нетрадиційні джерела електричної енергії відрізняються насамперед нестабільністю свого функціонування оскільки вони, за виключенням паливних елементів, цілковито залежать від погодно-кліматичних умов. Паливні елементи є відносно новим видом електрохімічних джерел енергії. Завдяки зовнішньому постачанню необхідних для їх роботи реагентів вони мають ряд суттєвих переваг, однак основна проблема для їх ефективного використання полягає у тому, що класичним ′пальним′ для них є водень, а цей газ важко і небезпечно зберігати та добувати.

Таким чином за підсумками цього коротенького аналізу можна зробити висновки про те, що сьогодні спостерігається певне протиріччя між зростанням потреби в електричній енергії для озброєння, військової техніки та особового складу підрозділів силових відомств з одного боку, та певною неспроможністю, пов′язаною з низкою факторів, задовольняти ці потреби відомими джерелами електричної енергії з іншого боку. Відзначене протиріччя породжує проблему, суть якої полягає у необхідності розроблення нових джерел електричної енергії, які здатні надійно і у повній мірі задовольняти потреби озброєння, військової техніки та особового складу підрозділів силових відомств під час виконання ними службових завдань. Основні підходи до розв′язку цієї проблеми вперше були опубліковані в роботах [2, 3, 4], однак важливим і нерозв′язаним до кінця завданням залишається задача оперативної оцінки ресурсного потенціалу нових джерел електричної енергії, які базуються на використанні описаних в зазначених роботах процесів перетворення енергії, що розсіюється під час пострілів вогнепальної зброї.

Аналіз явища пострілу вогнепальної зброї дозволив оцінити розподіл вивільненої в результаті згоряння порохового заряду енергії за її видами і об'ємами. Діаграма такого розподілу на прикладі пострілу з гармати типу Д-30 наведена на рис. 1.

Рис. 1. Діаграма розподілу енергії артилерійського пострілу.

В таблиці 1 наведений кількісний розподіл енергії, що виділяється під час пострілів типових артилерійських систем.

Таблиця 1.

	Артилерійська система				
	122 мм СГ 2С1	152 мм СГ С3	152 мм СГ 2С19	152 мм СП 2С5	152 мм СП С7
Кількість енергії, що виділяється, кДж	18050	38070	39330	87400	204915
Кінетична енергія снаряду, кДж	5135	9344	9689	20583	50688
Кількість енергії, що втрачається, кДж	12915	28726	29641	66817	154227
Відсоток траченої енергії, %	71,55	75,46	73,36	76,45	75,26
Види розсіюваної енергії:					
Дисипація порохових газів (ПГ)	Рух порохових газів				
Механічний рух відкотних частин	Врізання ведучих поясків в КС				
Теплопередача від ПГ до ствола	Інші види енергії				

Аналіз наведених у таблиці даних показує, що в процесі пострілів артилерійських систем втрачаються великі об'єми енергії. Причому найбільша кількість енергії втрачається за рахунок дисипації порохових газів у атмосферу. Таким чином необхідно здійснити пошук можливостей використання саме цієї енергії. Варто зазначити, що подібний розподіл енергії властивий для будь-яких видів вогнепальної зброї в тому числі і стрілецької.

Очевидною умовою використання розсіюваної під час пострілів вогнепальної зброї енергії є умова відсутності негативного впливу засобів перетворення енергії на тактико-технічні характеристики зброї. Виходячи з зазначених обмежень нами прийнято рішення стосовно використання енергії дисипації порохових газів, які виходять не з центрального каналу ствола гармати чи інших видів вогнепальної зброї, а газів, які виходять з отворів дульного гальма. Відомо, що ці гази відбирають 25 – 30% від загального об'єму енергії, яка виділяється у вигляді дисипації порохових газів у атмосферу.

Оцінка особливостей процесів дисипації дозволяє виділити наступне: температура газів сягає 2500 – 4000 ^{0}C, тиск 300 – 400 Мпа, тривалість процесу вільного витікання не більше 300 мікросекунд. Проведене математичне моделювання дозволило побудувати діаграми зміни кінетичної енергії і температури порохових газів, які наведені на рисунках 2 і 3.

Високі температури порохових газів і надзвукові швидкості їх розповсюдження з урахуванням наявності в них солей лужних металів дозволяють зробити припущення про виникнення значної концентрації іонізованих часток.

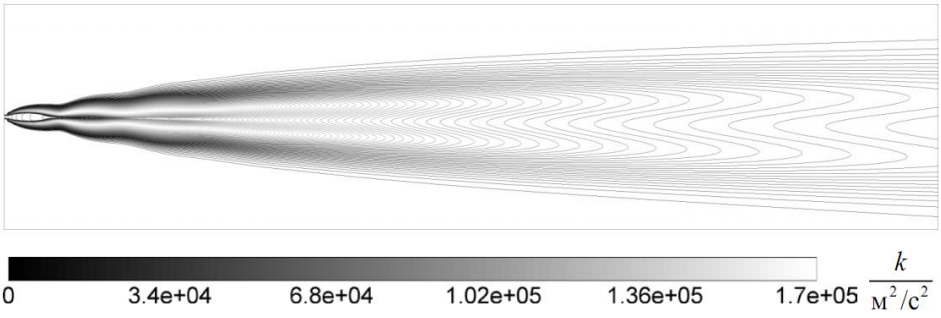


Рис. 2. Ізолінії поля кінетичної енергії на довжині вільного витікання порохових газів.

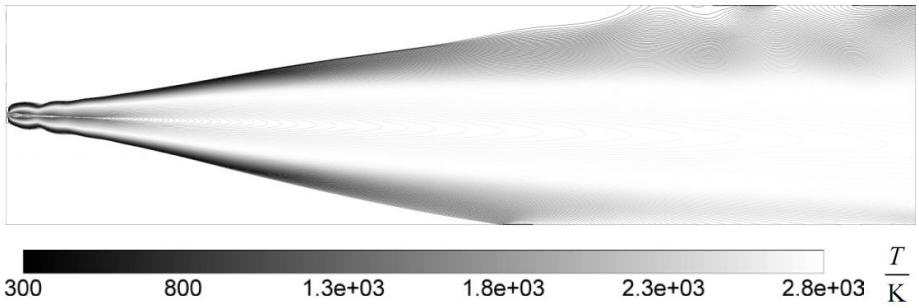


Рис. 3. Ізолінії поля статичної температури порохових газів на довжині вільного витікання.

Це створює потенційну можливість використання порохових газів у якості робочої речовини у магнітогідродинамічному генераторі електричної енергії, узагальнений вигляд якого наведений на рис. 4.

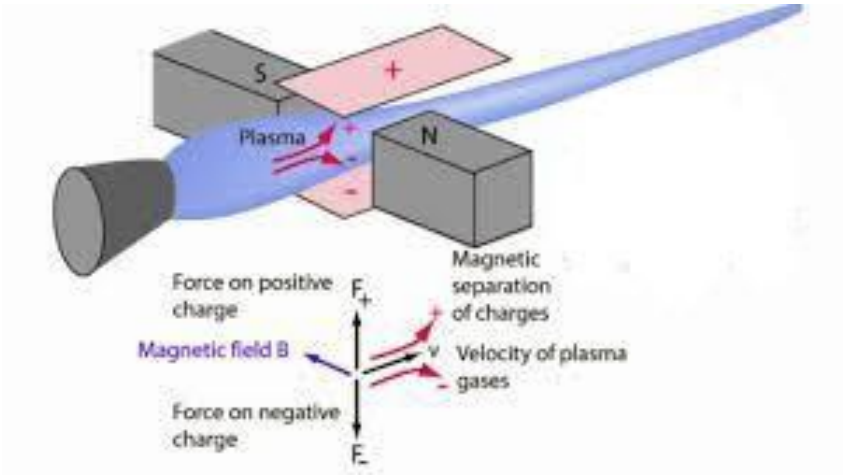


Рис. 4. Узагальнена схема магнітогідродинамічного генератора.

Робота такого генератора матиме короткочасний імпульсний характер і супроводжуватиметься генерацією електричних імпульсів високої потужності, які можуть бути акумульованими лише в іоністорах, після чого збережену електричну енергію можна використати для заряджання звичайних акумуляторів або для постачання споживачам з потрібними для них параметрами. Теоретичні оцінки ефективності такого перетворення енергії дисипації порохових газів, що витікають з отворів дульного гальма лежать у межах 12 – 25%. Ефективність перетворення можна збільшити за рахунок підвищення концентрації іонізованих часток в порохових газах шляхом додавання в порох сполук лужних металів. Однак у цьому випадку необхідно проводити додаткові дослідження стосовно можливого впливу на тактико-технічні характеристики зброї.

Таким чином у підсумку необхідно зазначити, що використання таких розсіюваних в процесі пострілів вогнепальної зброї видів енергії як: енергія віддачі, енергія теплового нагріву ствола і енергія

дисипації порохових газів через отвори дульного гальма дозволятимуть отримувати значні обсяги електричної енергії, які будуть забезпечувати кращу живучість, ефективність і автономність озброєння, військової техніки та особового складу.

Література:

1. Operational Energy [Електронний ресурс] // Office of the Assistant Secretary of Defense for Sustainment. – 2018. – Режим доступу до ресурсу: https://www.acq.osd.mil/eie/OE/OE_index.html.
2. Пат. 110392 України, МПКН02N2/18F03G3/00. Спосіб і пристрій для отримання електричної енергії на основі використання розсіювання енергії гарматного пострілу/ Ю.В.Шабатура, М.В.Баландін. заявл. 26.08.2014; опубл. 25.12.2015, Бюл. №24.
3. Шабатура Ю. В., Баландін. М. В. Аналіз і оцінка ефективності методів і засобів відбору та перетворення розсіюваної енергії, яка виділяється в процесі пострілу артилерійської гармати.// Військово-технічний збірник Національної академії сухопутних військ. – 2018. – №18(т). – С.52-61.
4. Шабатура Ю. В., Баландін М. В. Підвищення бойових можливостей артилерійських підрозділів за рахунок застосування альтернативних джерел живлення / Ю. В. Шабатура, // Збірник наукових праць Житомирського військового інституту. – 2017. – №14. – С. 31–41.

Бурлака В. В.,
начальник відділу Головного слідчого управління Національної поліції України

КРИМІНАЛІСТИЧНІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОБШУКУ В КОНТЕКСТІ ЗБИРАННЯ ДОКАЗІВ В ЕЛЕКТРОННІЙ ФОРМІ

Питання кримінального процесуального регулювання провадження слідчим професійної діяльності, в умовах демократизації сучасних процесів, розбудови правової держави в Україні є досить актуальними. Поряд із цим, малодослідженими є питання окремих криміналістичних особливостей здійснення певних слідчих (розшукових) дій, щодо збирання доказів в електронній формі.

Цифрологізація процесів, вихід суспільства на новий, більш якісний інтерактивний рівень та тенденції в сфері науки і техніки, дають підстави та штовхають вітчизняні правоохоронні органи на розвиток, динамізують його та створюють умови, в яких електронна та цифрова грамотність слідчого як процесуальної особи в кримінальному провадженні є необхідністю.

Збирання доказів в електронній формі є достатньо нелегким процесом, що зумовлено складністю об’єктів, а разом із тим, що не кожний слідчий володіє спеціальними знаннями у сфері сучасних інформаційно-комунікаційних технологій у достатній мірі, щоб успішно організувати розслідування необхідності, подекуди набуває допомога відповідного фахівця (експерта), який є достатньо підготовленим у цій сфері, оскільки навіть незначна некваліфікована дія з доказами в електронній формі може спричинити незворотну втрату цінної інформації.

Відповідно до основних положень державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набув чинності з 1 січня 2019 року було розроблено ряд методичних рекомендацій та пропозицій до кримінального процесуального кодексу, що дозволять оптимізувати процесуальний порядок збирання електронних доказів [1].

Зазначений національний стандарт гармонізований методом перекладу з відповідним міжнародним стандартом, що розроблений спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) і де наведений сталий зарубіжний досвід щодо ідентифікації, збирання, здобуття та збереження потенційних електронних (цифрових) доказів.

Загальною правовою підставою, що надає відповідним суб’єктам кримінального процесу повноваження на проведення обшуку, слід вважати розпочате досудове розслідування. На це вказують положення частини третя статті 214 Кримінального процесуального кодексу України, відповідно до яких забороняється здійснювати досудове розслідування до внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань.

За загальним правилом, право проводити обшук мають суб’єкти кримінального процесу, які представляють сторону обвинувачення: слідчий та прокурор (частина перша статті 236 Кримінального

процесуального кодексу України). Згідно з пунктом 2 частини другої статті 40 Кримінального процесуального кодексу України, слідчий уповноважений проводити слідчі (розшукові) дії у випадках, встановлених Кримінального процесуального кодексу України.

Поряд із цим, звертаючи увагу на криміналістичні особливості, перед обшуком з метою відшукування та збору електронних доказів, необхідно з'ясувати такі питання: Яке комп'ютерне обладнання та програмне забезпечення може бути на місці обшуку? Хто відповідає за обладнання (системний адміністратор)? Яка кількість обладнання може бути виявлена? Який обсяг даних потрібно буде скопіювати? Чи існують резервні копії даних та де вони зберігаються?

Підготовчий етап, безпосередньо перед проведенням обшуку, перш за все характеризується необхідністю створення слідчо-оперативної групи до складу якої включаються слідчий, працівник оперативного підрозділу, інспектор-криміналіст та інші учасники відповідно до наказів: МВС України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» та від 03.11.2015 № 1339 «Про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події»; створити групу спеціалістів з числа працівників кіберполіції та інших підрозділів для виїзду на місце події з метою виявлення слідів, їх фіксації, вилучення, опису та інтерпретації з урахуванням спеціальних знань; проінструктувати членів слідчо-оперативної групи щодо порядку роботи; забезпечити групу необхідними інструментами та обладнанням; забезпечити швидкий та безпечний шлях для проникнення в приміщення [2; 3].

З метою збирання електронних (цифрових) доказів використовують такі інструменти та обладнання: 1. Носії інформації, на які безпосередньо копіюватимуться дані: жорсткі диски (вінчестери); змінні носії (CD-DVD-диски); зовнішні пристрої з накопичувачами та для роботи з оптичними носіями інформації тощо. 2. Інструменти для демонтажу обладнання: викрутки (плоскі та фігурні); кусачки; плоскогубці; пінцет тощо. 3. Інструменти для документування процесу: фото- та відеокамера; бирки для нумерації доказів. 4. Матеріали для упаковки та транспортування вилучених об'єктів: антистатичні пакети; кабельна стяжка; коробки для DVD-дисків; коробки різноманітних розмірів для інших вилучених об'єктів. 5. Інші засоби та матеріали: транспорт для перевезення слідчо-оперативної групи, інструментів та вилучених матеріалів; папір для друку; роздруковані тексти із правами та обов'язками учасників слідчих дій; ноутбук зі стандартним програмним забезпеченням; спеціалізовані програмно-апаратні пристрої цифрової криміналістики (форензіки), криміналістичні загрузочні диски тощо [4].

Разом із тим, звертаємо увагу, що легалізація електронних (цифрових) доказів та процесуальна процедура їх отримання є предметом розгляду законодавця на сучасному етапі державотворення. У Верховній Раді України зареєстровано декілька законопроєктів, що маються на меті: 1) врегулювання визначення поняття та видів електронних доказів, доповнивши перелік процесуальних джерел доказів, та розмежувавши поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі; 2) регламентації порядку спеціальної конфіскації віртуальних активів, а саме:

- проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (реєстр. № 4003 від 01.09.2020), унесений народним депутатом України Монастирським Д.А. та іншими.
- проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» (реєстр. № 4004 від 01.09.2020), унесений народним депутатом України Монастирським Д.А. та іншими.

Таким чином, слід підвести підсумок про те, що порядок збору електронних (цифрових) доказів у кримінальному провадженні, процедура їх вилучення, отримання, зберігання та іншими способами долучення до матеріалів кримінального провадження неодноразово ставала предметом як наукових досліджень вчених так і законодавця.

Поряд із цим, окремі криміналістичні особливості проведення обшуку з метою отримання доказів в електронній (цифровій) формі на сьогоднішній день, хоч і врегульовані окремими нормативними

документами, проте дана процедура, її методика та правовий статус осіб, що здійснюють їх найбільш небезпечний для результатів досудового розслідування збір потребують вдосконалення.

Література:

1. Наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 06.12.2017 № 400 «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів – [електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/rada/show/v0400774-17#Text
2. Наказ Міністерства внутрішніх справ України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» – [електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/laws/show/z0937-17#Text
3. Наказ Міністерства внутрішніх справ України від 03.11.2015 № 1339 «Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події» – [електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/laws/show/z1392-15#Text
4. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. — Вид. 2-ге, доп. — Київ: Вид-во Нац. акад. внутр. справ, 2020. – 104 с.

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів, Львівського державного Університету внутрішніх справ, кандидат технічних наук, доцент

ОКРЕМІ АСПЕКТИ ЗАХИСТУ ДАНИХ В АКАУНТАХ ПІД ЧАС РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ

Захисту даних присвячено чималу кількість нормативно-правових актів (наприклад [1–3]), наукових досліджень та публікацій, як у галузі нормативно-правового, організаційного, так і програмно-технічного напряму (наприклад [4, 5]). Однак, як правило, користувачі інформаційно-телекомунікаційних систем та мереж через ряд об'єктивних та суб'єктивних причин недостатньою мірою ознайомлені з їх результатами і, таким чином, самі цього не підозрюючи створюють для зловмисників умови, які сприяють отриманню даних, у тому числі і персональних, через взламування різного роду акаунтів. Проведені опитування серед здобувачів вищої освіти та слухачів курсів підвищення кваліфікації у Львівському державному університеті внутрішніх справ свідчать про те, що цьому питанню ними найбільше уваги приділяється лише під час роботи з платіжними додатками, наприклад, такими, як «Приват 24». Тому, науково-педагогічними працівниками кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів досліджено основні правила дотримання безпеки роботи з обліковими записами в мережі Інтернет, які постійно доводяться до здобувачів вищої освіти, слухачів курсів підвищення кваліфікації під час викладання дисциплін «Безпека роботи з інформацією», «Інформаційне забезпечення професійної діяльності», «Сучасні інформаційні технології» тощо. Відповідно дані правила безпеки роботи з інформацією висвітлюються і в навчально-методичних виданнях [6, 7]. У даній публікації ми б хотіли викласти оновлені узагальнені результати проведених досліджень у даному напрямі забезпечення інформаційної безпеки і які у майбутньому будуть покладені у розробку оновленого навчально-методичного забезпечення для здобувачів вищої освіти Львівського державного університету внутрішніх справ.

Отже, одним з перших правил дотримання безпеки даних, які зберігаються в мережі Інтернет є видалення ряду акаунтів за умови, якщо користувач ними уже не користується. Такі акаунти часто пов'язані з ціннішими обліковими записами (через засоби синхронізації), які мають першочергове значення для користувача інформаційної мережі (додатка). Скорочення акаунтів дає можливість скоротити як кількість персональної інформації, так і зменшити кількість додаткових паролів та імен користувача.

Наступним правилом є використання спеціальних додатків, які допомагають користувачу мережі Інтернет упорядковувати паролі та імена. Такі додатки, як, наприклад, LastPass, 1Password дають

можливість користувачу управляти усіма його обліковими записами для входу до системи, згенерувати складні, захищені паролі, позбавивши при цьому необхідності користувача пам'ятати значну кількість паролів, чи використовувати єдиний пароль для входження до усіх додатків (on-line-сервісів).

Черговим правилом є використання двофакторної верифікації. Нині двофакторну верифікацію можна встановити для входу у більшість on-line-сервісів, у тому числі до облікових записів сервісів Google, Apple, Microsoft тощо. Це дає можливість у разі втрати (взлому) логіну і паролю убезпечити акаунт, оскільки зловмисники не зможуть увійти у нього (особливо з іншого пристрою) без додаткового ідентифікаційного коду, який приходить користувачу акаунта через SMS-повідомлення або через спеціальний додаток. Тобто зловмиснику необхідно у такому випадку мати фізичний доступ до гаджетів користувача.

Далі. Час від часу слід перевіряти активність облікового запису (у випадку, якщо додаток дозволяє її перевіряти). Це дозволяє переконатися у відсутності підозрілих дій з обліковими записами користувача. Якщо ж користувач виявив щось підозріле, то можна вийти з будь-яких сеансів (окрім поточного) та відмінити авторизацію облікового запису для будь-яких гаджетів, які не відомі користувачу.

Наступні рекомендації стосуються користувачів соціальних мереж. У таких мережах часто інші додатки та служби підключаються до акаунтів користувачів. І це нормально. Однак, слід звести такі під'єднання до мінімуму та видаляти або не дозволяти встановлюватися таким з'єднанням, якими користувач не користується з метою блокування будь-яких потенційних можливостей для використання облікових записів зловмисниками. Окрім цього, у таких соціальних мережах, наприклад, як у Facebook, є можливість отримання допомоги від друзів у випадку виникнення проблем з доступом до акаунту. Для цього слід обрати довірених осіб (до п'яти) через налаштування розділу «Безпека», яким будуть направлятися одноразові коди, які у подальшому можна використати для відновлення доступу до акаунту.

Не слід довіряти незрозумілим повідомленням. У випадку отримання сумнівного повідомлення за допомогою соціальних мереж чи електронної пошти, у якому міститься посилання сумнівного контексту (чи без нього), слід пам'ятати, що технології з отримання особистих даних і паролів активно розвиваються, стають доступнішими і хитрішими. Тому перед натисканням на таке посилання слід добре подумати.

Наступна рекомендація є стандартною вимогою щодо безпеки роботи з інформацією і стосується зміни паролів. Якщо навіть користувач використовує додатки, які дають можливість користувачу управляти усіма його обліковими записами та паролями для входу до системи (вище нами згадувані LastPass, 1Password), то у будь-якому випадку (особливо у підозрілій ситуації) слід постійно змінювати усі без винятку паролі.

Чергова рекомендація стосується програмного забезпечення, яке використовується користувачем. Необхідно пам'ятати, що застаріле програмне забезпечення є одним із вразливих місць персонального комп'ютера, а тому користувач має підтримувати в актуальному стані операційні системи, браузери тощо. Це не є складною проблемою, адже майже усі програмні продукти мають функцію автооновлення. Тому виконувати дану рекомендацію досить просто.

І на завершення кожному користувачу мережі Інтернет треба знати: усі облікові записи захищено надійно на стільки, наскільки захищено найслабкішу ланку передавання даних. Тому, час від часу слід переконуватися, що особисті персональні дані користувача відсутні у акаунтах соціальних мереж. Чим менше про користувача є даних у таких мережах тим краще. Також слід пам'ятати, що такі дані часто використовуються зловмисниками для створення портрету користувача, наприклад психологічного, з використанням сучасних технологій аналізу даних (Data Mining, Big Data).

Дотримання викладених вище нескладних правил роботи в інформаційно-телекомунікаційній мережі Інтернет дозволить будь-якому користувачу мінімізувати ризики втрати доступу як персональних так і інших даних, які зберігаються у мережі Інтернет.

Література:

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР. *База даних «Законодавство України» / ВР України*. URL: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/.

2. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *База даних «Законодавство України» / ВР України*. URL: http://zakon2.rada.gov.ua/laws/show/2297-17/.

3. Про інформацію : Закон України 2 жовтня 1992 р. № 2657-XII. *База даних «Законодавство України» / ВР України*. URL: http://zakon2.rada.gov.ua/laws/show/2657-12/.

4. Сеник В. В. Щодо дотримання прав громадян на захист персональних даних під час обробки інформаційних ресурсів Національною поліцією України. *Сучасний конституціоналізм: проблеми теорії та практики :* матеріали наукового семінару (23 червня 2017 року м. Львів) / упор. М. В. Ковалів. Львів: ЛьвДУВС, 2017. С. 241–243.

5. Сеник В. В., Кулешник Я. Ф., Магеровська Т. В. Проблеми захисту персональних даних у сучасних інформаційних системах. *Використання сучасних інформаційних технологій в діяльності Національної поліції України :* матеріали Всеукраїнського науково-практичного семінару (28 листопада 2019 року, м. Дніпро). Дніпро: ДДУВС. 2019. С. 66–68.

6. Сеник В. В., Рудий Т. В., Магеровська Т. В. Технології захисту інформації: методичні рекомендації для здобувачів вищої освіти юридичних та економічних спеціальностей. Львів, ЛьвДУВС, 2018. 92 с.

7. Сеник В. В., Рудий Т. В., Сеник С. В., Магеровська Т. В. Основи технологій захисту інформації в комп'ютерних системах : навч.-метод. посібник. Львів : ЛьвДУВС, 2019. 192 с.

Тулупов В. В.,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

Рязанцева І. М.,
начальник навчально-методичного відділу Харківського національного університету внутрішніх справ, кандидат юридичних наук

ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Високий темп розвитку інформаційних технологій навчання зумовлює: оновлення засобів матеріально-технічного забезпечення навчального процесу новими зразками техніки та інформаційними технологіями; оновлення кадрового потенціалу кафедр зі специфічними умовами навчання та взаємопроникнення інформаційних технологій та спеціальних знань в суміжні дисципліни, що викладаються; впровадження нових методик й прийомів навчання; комп'ютеризація та інформатизація навчального процесу; тісний зв'язок з передовими науково-технічними розробками в сфері інформаційних технологій та спеціальної техніки.

Розробка та впровадження компонентів інформаційних технологій для підготовки фахівців технічної ланки а саме фахівців з організації захисту інформації має суттєву прикладну компоненту наближення до проблематики діяльності підрозділів технічного захисту інформації у правоохоронних структурах. Найбільш у цьому сенсі має ефективна комплексна комп'ютеризація та тренажеризація професійної підготовки таких фахівців у навчальних закладах зі специфічними умовами навчання МВС України.

Слід виділити те що розробка однієї години високоефективної навчальної комп'ютерної програми, як показує вже наявний досвід, вимагає витрат багатьох людино-годин праці кваліфікованих програмістів і методистів. При цьому контроль якості навчаючих програм та ефективності тренажерної підготовки є справою складною, що потребує спеціальних знань, тестів, участі експертів тощо, також до цього варто додати констатацію неухильного зросту вартості апаратних і програмних засобів як існуючих навчаючих систем (тренажерів) так і інших інтерактивних засобів навчання.

Метою даної доповіді є виділення кола існуючих проблем щодо програмно-технічного забезпечення нормативних дисциплін кафедр зі специфічними умовами навчання у системі МВС України та шляхи їх подальшої реалізації на прикладі створення комп'ютерних навчаючих систем (комп'ютерних тренажерів) та впровадження їх у навчальний процес.

На теперішній час на ринку професійного навчання пропонуються різні тренажерні комплекси (комп'ютерні тренажери) та навчаючи системи для підготовки фахівців, професійна діяльність яких пов'язана не тільки з організації захисту інформації, а із використанням інформаційних технологій в освітньому процесі. Забезпечення ліцензіатів інструментальними засобами в повному обсязі неможливо

у зв'язку з їх великої вартістю, а існуючі на ринку засоби навчання за ціною сумірні, або дорожче реальних програмно-апаратних комплексів технічного захисту інформації .

Можливі підходи до розв'язання проблем. Розв'язання деяких вищезазначених проблем знайшли своє відображення у розробках кафедри Інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, де здійснюється підготовка фахівців за спеціальністю 125 – «Кібербезпека». Так, наприклад для забезпечення проведення практичних та лабораторних занять з дисциплін: «Метрологія та вимірювання», «Електроніка та схемотехніка», «Методи та засоби захисту інформації», «Цифрова обробка сигналів» розроблені та впроваджені комп'ютерні тренажери «Селективні мікровольтметри та вимірювачі напруги завад SMV- 8.5, SMV- 11» які призначені для отримання курсантами та студентами первинних практичних навичок роботи із даними приладами.

Тренажери являють собою спрощений інтерактивний аналог (симулятор) пристроїв SMV 8.5, SMV- 11 та мають наступні можливості: ознайомлення користувачів з призначенням пристрою; ознайомлення з технічними характеристиками й можливостями використання; ознайомлення з комплектацією пристрою; ознайомлення з органами управління пристроєм; демонстрація використання пристрою при виконанні учбово-тренувальних задач; безпосереднє виконання учбово-тренувальних задач для оволодіння навичками роботи з пристроєм та тестування користувачів.

Кафедрою також було розроблено та впроваджено у навчальний процес комп'ютерні тренажери а саме: «Виміри за допомогою селективного нановольтметру Unipan-233» та «Вимірювач шуму та вібрацій ВШВ-003-М2» з використанням мультимедійної платформи Adobe Flash та інших технологій.

На теперішній час у рамках дипломного проектування розробляються комп'ютерні тренажери для інших пристроїв з подальшим впровадженням їх у навчальний процес, наприклад пошуковий універсальний зонд-монітор СРМ-700 для виявлення передавачів, обстеження дротових ліній зв'язку, аналізу ІЧ-каналу.

Висновки. Впровадження таких розробок у навчальний процес дозволить у деякій мірі замінити традиційний науковий інструментарій засобами сучасних інформаційних технологій, шляхом виконання учбово-тренувальних задач на комп'ютерному тренажері, у зв'язку з обмеженістю таких приладів як на самих кафедрах зі специфічними умовами навчання, так і в практичних підрозділах.

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

ВИНИКНЕННЯ РОЗВІДУВАЛЬНОЇ (КРИМІНАЛЬНОЇ) АНАЛІТИКИ

Важливим та корисним є огляд історичного підґрунтя, «коріння» розвідки (intelligence) як продукту аналітичної діяльності та аналізу як процесу і як професії. Підвищення свого розуміння витоків розвідки та аналізу допомагає зрозуміти як і чому сформувалась у такому вигляді сучасна кримінальна розвідувальна аналітика. Це також покращує обізнаність про те, що розвідувальна аналітична практика постійно змінюється та розвивається, що для досягнення актуальності та корисності в практичному розумінні аналітика постійно потребує свіжого, гнучкого підходу, нових ідей, нових навичок, нових методик. Єдиною постійною умовою для процесу професійної розвідувальної (кримінальної) аналітики є те, що жодна з двох задач чи проектів ніколи не бувають абсолютно однаковими; кожне нове дослідження вимагає свіжого підходу.

Знання можуть потенційно прирівнюватися до влади. Концепція збору та використання інформації для підтримки прийняття рішень не є новою. Для того, щоб отримати перевагу перед супротивниками, необхідно обов'язково володіти найсучаснішою, точною інформацією щодо нього, його намірів та можливостей. Це правило застосовується в будь-якій галузі: політика, бізнес, військова стратегія, кримінальна розвідка тощо.

Крім того, це процес, який завжди і постійно розвивається у відповідь на зміни соціальних, культурних факторів, технологій, організаційних потреб та якісної зміни рівня аналітичної майстерності.

Історія знає чимало прикладів діяльності військових, релігійних та громадських лідерів, які активно проводили збір інформації для підтримки своїх рішень. Мабуть, найдавнішим визнаним текстом

на тему збору інформації та проведення на її основі розвідувальних дій є «Мистецтво війни», написане у V столітті до н.е. Сун Цзи, китайським воєначальником. Він був відомий своєю здатністю керувати військовими кампаніями, успіх яких багато в чому був наслідком ефективності дій зі збирання інформації та прийняття рішень на основі розвідки. Про якість цієї роботи свідчить те, що вона все ще залишається в друку і сьогодні та є важливою для військових та корпоративних стратегів та розвідників у всьому світі. З цих ранніх часів історії до порівняно недавнього часу загальною тенденцією було використання збирачів інформації для переважно військових цілей.

Більше того, в результаті цього процесу виникла методологія, яка в основному передбачала прямий контакт між збирачем інформації та замовником – особою, що приймає рішення.

Цей метод мав певні помітні особливості:

- логістика (відсутність реальної технології транспортування або зв'язку) створила велику затримку в часі між постановкою завдання збирачеві інформації, отриманням інформації та її доставкою "кінцевому користувачеві".
- використання збирачів інформації, які безпосередньо здійснювали відвідування окремих місць та проводили опитування про події особисто чи через посередників, гарантувало, що зібрана інформація буде обмежена їхніми почуттями та здатністю точно запам'ятовувати почуте і побачене. Таким чином, така інформація завжди була дуже суб'єктивною і схилялася до того, щоб ґрунтуватися не на фактах, а на думках.
- обсяг інформації, зібраної за витрат значної кількості часу та ресурсів, був надзвичайно малим.

Методи отримання інформації змінювалися дуже повільно протягом історії аж до кінця минулого століття. Масовий ріст технологій, який почався тоді і продовжується і сьогодні, призвів до масової зміни методів збирання інформації, що, в свою чергу, створило попит на нові підходи до аналізу та аналітики.

Цей процес розпочався наприкінці 19 століття з появою телеграфії та телефонії, що дозволило надсилатись повідомлення майже миттєво на усе більші відстані. Це усунуло проблему з ресурсом та часом, для переміщення інформації між джерелом та клієнтом. Ця зміна принесла із собою ряд переваг.

Так, «час відповіді» між клієнтом, який запитував інформацію та отримував результат, значно скоротився. Це очевидна перевага, оскільки значно кращою стала здатність клієнтів швидко реагувати і діяти на основі такої інформації. Крім того, цей розвиток також мав перевагу в тому, що час щоб «забути» або «втратити» інформацію значно знизився, тому якість інформації також покращилася. Також, відсутність потреби у фізичній передачі клієнтові інформації створило значну економію ресурсів – збирачі інформації змогли витрачати менше часу на передачу інформації, і, таким чином, більше часу вивільнилось на збір інформації.

Загальним результатом цієї зміни було і те, що ці переваги сформували нову проблему для клієнта. Накопичення інформації здійснювалось набагато швидше, ніж раніше, тому час реакції і прийняття рішень скорочувався. Крім того, сам контроль за процесом збору інформації став проблемою. Виникла потреба швидше формувати нові завданнях та розпорядженнях для збирачів інформації враховуючи їх покращені показники продуктивності.

Таким чином, якщо раніше процес включав передачу інформації між збирачем інформації та клієнтом, то нова система створила інформаційне «перевантаження», виникла нова проблема в тому, що клієнт просто не міг ефективно та швидко обробляти всю отриману інформацію, а потім реагувати на неї.

Таким чином для клієнта виникла необхідність швидкого тлумачення отриманої інформації та прийняття на її основі відповідних рішень. Це створило необхідність проміжного етапу між збирачем інформації та клієнтом, на якому основна частина інформації могла би бути записана, оцінена та досліджена для інтерпретації та вилучення змісту (сенсу) до того, як результат цього процесу буде переданий клієнту. Це було зародженням функції аналітика, і процес залишається по суті тим самим і до сьогодні.

Основна функція аналітика може бути розбита на трифазний процес таким чином:

- Зібрати інформацію, зрозуміти відповідність чи відношення кожної її частини до всіх інших.
- Розвивати цю інформацію об'єктивно, щоб прийти до розуміння цілого.
- Передавати це розуміння з іншими людьми і так використовувати розвідувальні аналітичні продукти для практичного використання.

Результатом розширення розмаїття, діапазону та доступності джерел інформації було те, що потреба у "аналітику" різко зростала. Простіше кажучи, по мірі того, наскільки більше інформації

передавалось до “центру” для прийняття рішень, керованих розвідувальною аналітикою, було виявлено, що все більше людей вимагають оцінювати інформацію.

Ця ситуація, що триває, має наслідки для сьогоднішніх аналітичних підрозділів та аналітичного персоналу. Чим більше інформації збирається, тим більше це допомагає аналізу та у підсумку – прийняттю вірного рішення. Однак це також збільшує подальше навантаження, що, в свою чергу, змушує збільшувати штат аналітиків і їх продуктивність або втрачати ефективність.

Література:

1. Criminal Intelligence. Manual for Analysts. UNITED NATIONS OFFICE ON DRUGS AND CRIME. – New York, 2011 – 95 p.

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

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

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ НОРМАТИВНО-ПРАВОВИХ ОСНОВ КІБЕРБЕЗПЕКИ

На сьогоднішній день перед Україною стоять значні виклики у сфері кібербезпеки. Значне проникнення інформаційних технологій у всі сфери життєдіяльності суспільства поруч із великими зручностями породжує і значні небезпеки. Як витоки інформації, так і несанкціоноване проникнення кіберзлочинців в інформаційні системи об’єктів критичної інфраструктури, можуть спричинити важкі наслідки, як економічні, так і такі, що створюють загрозу життю людей. Особливо яскраво такі небезпеки проявилися з початком російської агресії проти нашої держави, коли угруповання кіберзлочинців, керовані спецслужбами сусідньої держави, здійснюють напади на інформаційні мережі енергосистеми України та українських аеропортів [1, 2].

Однією з причин проблем, які виникають у сфері кібербезпеки в Україні, є недосконала нормативно-правова база та система державного управління.

На сьогоднішній день в Україні чинною є низка законів України та інших нормативних документів різних рівнів, що регулюють забезпечення кібербезпеки держави. Це, зокрема, Закони України «Про національну безпеку України» [3], «Про інформацію» [4], «Про захист інформації в інформаційно-телекомунікаційних системах» [5], «Про державну таємницю» [6], «Про Державну службу спеціального зв’язку та захисту інформації України» [7].

Також це такі нормативні документи, як Нормативні документи системи технічного захисту інформації (НД ТЗІ), зокрема, Типове положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-001-2000 [8] та Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-2005 [9].

Більшість із них і у тому числі Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації (НД ТЗІ) є застарілими. Комплексна система захисту інформації (КСЗІ), яку ці документи зобов’язують впроваджувати на об’єктах, де треба здійснювати захист інформації, вже морально застаріла та є неефективною.

Дуже важливим кроком було прийняття у 2017 році Закону України «Про основні засади забезпечення кібербезпеки України». Але цей Закон не поширюється на:

- відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;
- діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;
- соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять

інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

- комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем) [10].

У системі Національної поліції України було б раціональним створення організованої системи взаємодії та координування зусиль для протидії кіберзлочинності навіть з огляду на той факт, що статистика про скоєння кіберзлочинів розпорошена між різними силовими структурами і потребує використання наукових методів аналізу.

Зрештою, якщо протидія кіберзлочинам на об'єктах державної інфраструктури все ж регулюються чинним законодавством, то об'єкти приватного підпорядкування, де також є загрози від кіберзлочинців, випадають з його поля зору. А отже існує необхідність державного регулювання у сфері нормативно-правових основ кібербезпеки.

Тобто, завдання суб'єктів національної системи протидії кіберзлочинності не узгоджуються з базовими чинними законодавчими актами та системою забезпечення кібербезпеки у таких сегментах як органи державної влади та державного управління, економіки, приватного сектору тощо.

Вплив часового чинника на вищезгадані недоліки може призвести до непередбачуваних наслідків. Тому потрібно розробити та негайно імплементувати нову нормативно-правову базу з урахуванням інтеграційних процесів з Європейським союзом та розширення співпраці з НАТО.

Література:

1. Атака на енергомережі в Києві 2016 року: експерти знайшли зв'язок хакерів з РФ // Укрінформ від 13.06.2017. [Електронний ресурс]. URL: https://www.ukrinform.ua/rubric-technology/2246440-ataka-na-energomerezi-v-kievi-2016-roku-eksperti-znajsli-zvazok-hakeriv-z-rf.html(дата звернення: 04.12.2020).
2. Наталка Прудка Кібервійна проти України. Перші жертви і висновки // «Главком» від 8 квітня 2016 р. [Електронний ресурс]. URL: https://glavcom.ua/publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi-i-visnovki.html (дата звернення: 04.12.2020).
3. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII // Відомості Верховної Ради (ВВР), 2018, № 31, ст. 241.
4. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII // Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286.
6. Закон України«Про державну таємницю» від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України (ВВР), 1994, № 16, ст. 93.
7. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV // Відомості Верховної Ради України (ВВР), 2006, № 30, ст. 258.
8. Типове положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-001-2000 // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ 2000.
9. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-2005 // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ 2005.
10. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403.

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

РОЛЬ І МІСЦЕ ІНФОРМАЦІЙНИХ СИСТЕМ У ПОДАТКОВОМУ АДМІНІСТРУВАННІ

Пріоритетним напрямом розвитку податкової служби є підвищення економічної ефективності податкового адміністрування. Досягнення прийнятних результатів за даним напрямом неможливо без

використання потужного економічного ресурсу, яким є інформаційні технології. Організація роботи податкових органів неможлива без відповідної інформаційної підтримки.

Сьогодні необхідно продовжувати вдосконалення системи оподаткування та податкового адміністрування, створювати умови для податкового стимулювання громадян та ведення бізнесу, забезпечувати впровадження інноваційних технологій і процесів. Без впровадження комп'ютеризації та мереж неможливо якісне виконання завдань, що стоять перед податковою службою.

З цією метою в органах податкової служби створюється інформаційна система, яка призначена для автоматизації функцій всіх рівнів податкової служби щодо забезпечення збору податків та інших обов'язкових платежів до бюджету, проведення комплексного оперативного аналізу матеріалів з оподаткування, забезпечення органів управління та відповідних рівнів податкових служб достовірною інформацією.

В умовах непростої економічної ситуації податкові органи країни є важливим важелем державного управління, відповідальними за виконання дохідної частини державного бюджету, за яким стоїть добробут мільйонів громадян України.

Керівництво країни приділяє особливу увагу питанням інформатизації податкових органів, про що говорить той факт, що за рівнем оснащеності інформаційними технологіями податкова служба займає провідне місце серед інших державних структур.

Реалізація плану заходів щодо Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, спрямована на підтримку заходів щодо підвищення ефективності та раціональності податкової служби за допомогою впровадження сучасних стандартів [1]. Даний проект має наступні особливі компоненти інформатизації податкової діяльності: Компонент операційний розвиток має на меті вдосконалити та розвивати основні функції податкового адміністрування за допомогою реінжинірингу бізнес-процесів, впровадження автоматизованої системи управління ризиками, методології загального декларування, створення сучасного колл-центру та інших заходів (з метою підвищення податкової грамотності населення і роз'яснення податкового законодавства, у зв'язку з пропозиціями введенням загального декларування доходів зростає необхідність створення сучасного Call-центру податкових органів та розвитку електронних сервісів, створення центрів обробки даних податкових органів для обробки подаються декларацій).

Компонент розвитку інформаційно-технологічної інфраструктури спрямований на приведення всіх інформаційних систем у відповідність з єдиним технологічним підходом, на розвиток комплексної та інтегрованої системи податкового управління.

В останні роки зроблені суттєві кроки і досягнуті значні поліпшення у галузі податкової політики та податкового адміністрування. В рамках реформи зі Світовим Банком був вивчений кращий міжнародний досвід в частині розвитку кадрового потенціалу працівників податкової служби, їх мотивація. При реалізації всіх нововведень і інновацій орієнтуємося на передовий міжнародний досвід ОЕСР, ІОТА (ОЕСР – Організація економічного співробітництва і розвитку, ІОТА – Європейська організація співробітництва податкових адміністрацій).

Саме трудомістке з проведених заходів реформ це реінжиніринг процесів податкового адміністрування. Наприклад, для упорядкування адміністративного провадження розроблені блок-схеми по виявленню та притягненню правопорушника до адміністративної відповідальності. Дані блок-схеми наочно показують, що заходи накладення адміністративних штрафів ускладнені та громіздкі, що в деяких випадках призводить до корупційних проявів. У липні 2009 р року на засіданні Генеральної Асамблеї ІОТА було розглянуто питання про прийняття України до складу повноправних членів, що дозволило постійно бути в курсі всіх проведених реформ в частині податкового адміністрування в європейських країнах.

Ратифіковано Конвенцію про взаємну адміністративну допомогу в податкових справах, до якої приєдналися 103 держави, в тому числі 19 офшорних юрисдикцій. Конвенція передбачає обмін інформацією на взаємній основі між країнами-учасницями з метою протидії тіньовій економіці, відмиванню тіньових доходів, включаючи ухилення від сплат податків. Також ратифіковано Конвенцію про взаємну адміністративну допомогу в податкових справах (Страсбурзька конвенція 25 січня 1988 року, до конвенції приєдналися 103 держави, в тому числі 19 офшорних юрисдикцій).

Мета – обмін податковою інформацією з метою протидії тіньовій економіці, відмиванню тіньових доходів, включаючи ухилення від сплати податків. Створено правову основи для виконання положень

зазначеної угоди, внесено поправки в законодавство України, що передбачають впровадження механізмів та інструментів обміну інформацією в сфері оподаткування.

Всі заходи з побудови в Україні моделі податкової служби відповідно до міжнародних стандартів будуть впроваджуватися з урахуванням адаптації національного законодавства до вимог Європейського Союзу.

Відповідно до рейтингу Всесвітнього банку «Doing Business» за показником «Оподаткування», Україна знаходиться на 65 місці серед 189 країн [2].

Податкова політика завжди була важливим інструментом економічної політики держави. В умовах необхідності розвитку масового підприємництва та активізації інвестиційної діяльності, стоїть завдання побудови стабільної, передбачуваної та справедливої податкової системи. Пріоритетним напрямом в розвитку «електронного уряду» є необхідність розміщення всіх послуг в єдиній точці доступу, виводити послуги на портал «електронного уряду». Процес оптимізації форм податкової звітності проводиться паралельно з процесом розширення взаємодії з уповноваженими державними органами з обміну інформацією.

Пропонується запровадити контрольно-касові машини з SIM-картою, які в онлайн-режимі передають дані в податкові органи. Необхідна оптимізація чинних спеціальних податкових режимів з обов'язковим веденням податкового обліку доходів і витрат.

Існує ряд проблем, що негативно впливають на розвиток підприємництва. По-перше, це великий обсяг форм податкової звітності. Більшість «ненавмисних» податкових порушень відбуваються через громіздкість і велику трудомісткість податкової звітності, або неоднозначності тлумачення норм законодавства.

За чинним податковим законодавством для застосування Конвенції про уникнення подвійного оподаткування нерезидент буде зобов'язаний подати документ, який підтверджує резидентство, на паперовому носії з дипломатичної (консульської) легалізацією такого документа. У міжнародній практиці окремі країни перейшли на підтвердження резидентства в електронному вигляді шляхом розміщення на офіційних сайтах компетентних органів. (Грузія, Іспанія, Молдова, Чехія та ін.).

Пропонується для застосування міжнародних договорів про уникнення подвійного оподаткування, запровадити електронний документ, що підтверджує резидентство нерезидента.

Чинним податковим кодексом передбачено впровадження електронного аудиту при проведенні податкових або митних перевірок. Світова практика – електронний аудит при проведенні податкових або митних перевірок використовується в країнах ОЕСР і у країнах ЄС (Нідерланди, Португалія, Латвія, Естонія), що скорочує терміни проведення перевірок, підвищує їх результативність і прозорість.

Е-аудит дозволить підвищити результативність проведених перевірок і прозорість при проведенні. Однак впровадження Е-аудиту потребує доопрацювання інформаційних систем платників податків і тестування системи на добровільних засадах платників податків.

Значні обсяги інвестицій вкладено в розвиток інформаційних технологій, які в даний час активно використовуються. Держави ЄС переходять на підтвердження резидентства в електронному вигляді. Вони розміщують на офіційних сайтах уповноважених органів в електронному вигляді. Більше 75% платників податків використовують електронні форми звітності. Вжито заходів, спрямовані на поліпшення прозорості і підвищення ефективності управління роботою податкових органів, включаючи впровадження стандартів надання податкових послуг.

На сьогоднішній день податкове адміністрування вийшло на якісно новий етап розвитку, вже реалізовано низку реформ. Зокрема, внесені зміни до Податкового кодексу, який суттєво наближає податкову систему України до міжнародної практики, щодо несе інвестиційний потенціал, дозволяє побудувати прозорого систему податкового адміністрування.

Впровадження інформаційних систем у податкових органах, крім підвищення прозорості роботи, дозволило дисциплінувати платників податків в частині неправомірного завищення витрат. Всі вжиті заходи з упровадження інформаційних систем спрямовані на забезпечення прозорості податкової системи. Це збільшує можливості контролю для податкових органів і дає переваги платникам податків у становленні бізнесу.

Література:

1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII / Відомості Верховної Ради України. 2014. № 40. Ст. 2021.

2. DOING BUSINESS Оцінка Бізнес Регулювання. Всесвітній банк. URL. https://russian.doingbusiness.org/ru/rankings

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

СВІТОВИЙ ДОСВІД ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Поліцейські організації збирають і зберігають величезну кількість інформації. Традиційно ця інформація містилася на аркушах паперу, що зберігалися в картотеках. Сьогодні поліцейські організації трансформуються в епоху інформації. Більшість із них запровадили управлінські інформаційні системи (УІС) для запису, зберігання, доступу та аналізу даних про виклики громадян до служби, характер реакції поліції на ці виклики, зареєстровані злочини, арешти, дозволи на зброю, зупинки автотранспортних засобів, та багато інших типів даних. Деякі відомства підтримують централізований контроль за доступом до інформації, тоді як інші запровадили інтегровані системи управління, доступ до яких мають правоохоронці на будь-якому рівні (від патрульного до начальника). Цей "повний доступ" підхід дозволяє працівникам з різними потребами отримувати доступ до даних без необхідності чекати чи подавати офіційний запит. Деякі установи зберігають дані та отримують доступ до них в електронному вигляді, але не використовують їх як засіб для вдосконалення організації. Інші використовують дані як інструмент для вдосконалення управління та операцій. Хоча сьогодні більшість великих поліцейських установ значно покращили свою здатність збирати та зберігати великі обсяги даних, тільки деякі з них досягли значного прогресу у використанні даних, котрі вони збирають. Розвиток здатності використовувати дані для вдосконалення діяльності та управління представляє важливу проблему для поліцейських організацій сьогодні. Хоча сьогодні більшість великих поліцейських установ значно покращили свою здатність збирати та зберігати великі обсяги даних, мало хто досяг значного прогресу у використанні даних, які вони збирають. Системи автоматизованої диспетчеризації (САД) зараз широко використовуються багатьма відділами поліції. Системи САД надають пріоритет викликам на обслуговування, що надходять до центру зв'язку, "складаючи" менш термінові дзвінки, щоб співробітники поліції могли реагувати на ті дзвінки, що вимагають більш негайної уваги. Після того, як система САД визначить пріоритетом дзвінок, його можна транслювати офіцеру в патрульній машині через радіо або комп’ютер. САД дозволяє людям, які беруть участь у виклику та диспетчері, бути в курсі того, на які дзвінки відповідають, де знаходяться співробітники та як довго вони не були на розмові. Це зменшує ймовірність відправлення помилок і підвищує безпеку офіцерів. Системи САД також корисні для збору та зберігання даних. Після отримання дзвінка в комунікаційному центрі система класифікується системою САД.

У багатьох поліцейських установах США зараз у своїх патрульних автомобілях встановлені мобільні цифрові термінали (МЦТ) або комп’ютери (МК). МК мають ряд застосувань, не всі з яких доступні у всіх юрисдикціях. По-перше, вони дозволяють офіцеру отримувати "мовчазні депеші" через комп'ютер, а не через радіо, так що поліцейські сканери не можуть використовуватися для моніторингу зв'язку поліції. По-друге, співробітники можуть перевіряти реєстрації автотранспортних засобів, посвідчення водія та непогашені ордери безпосередньо, не чекаючи, поки диспетчер проведе комп'ютерну перевірку. По-третє, співробітники можуть вводити поліцейські звіти в комп’ютер, перебуваючи в полі, замість того, щоб повертатися до міліції достроково для оформлення документів. По-четверте, офіцери можуть надсилати електронне повідомлення іншим офіцерам, в тому числі тих, хто на той час не чергує. Нарешті, співробітники можуть іноді отримувати інформацію про арешти, злочинність та заклики до обслуговування з баз даних, які об’єднані між відомствами на місцевому, штатному або федеральному рівнях. Згідно з опитуванням з питань правоохоронної діяльності та адміністративної статистики (LEMAS) 1997 року, 78 відсотків великих муніципальних правоохоронних органів Сполучених Штатів використовують певний тип мобільного цифрового терміналу або комп'ютера.

Використання статистичних методів та методів географічного картографування для аналізу тенденцій злочинності, безладу, арештів та закликів до служби (надалі - аналіз злочинності) набуває

популярності у багатьох установах. Географічні інформаційні системи (ГІС) корисні для візуального планування випадків певних правопорушень у межах юрисдикції. Поєднуючи статистичні дані про злочинність, безладдя, арешти чи заклики до служби з описами земельних ділянок, аналітики злочинів можуть «намітити» ці райони в громаді з концентрацією певних проблем. Потім поліція може зосередити свої зусилля в цих відносно невеликих "гарячих точках". Карти, вироблені ГІС, є більш ніж вигадливою заміною старомодним "картам-шпилькам", які роками використовувала поліція. В ідеалі, вони повинні мати можливість відслідковувати тенденції злочинності (або тенденції до дзвінків чи розладів) у міру їх розвитку. Таким чином, якщо міліцейська операція в певному районі призводить до переміщення правопорушників до прилеглих районів, карти ГІС повинні відображати цей рух. Небагато агентств досягли цього ідеального стану ще через проблеми у зв'язку окремих баз даних та комп'ютерних систем. Як тільки ці проблеми будуть вирішені, картографування злочинів буде дедалі важливішим інструментом, який застосовується поліцією для аналізу та реагування на тенденції злочинності. Згідно з опитуванням LEMAS, 60 відсотків місцевих правоохоронних органів, що мають сто чи більше офіцерів, використовують комп'ютери для картографування злочинів. Інші інформаційні технології мають більш безпосереднє застосування для проведення розслідувань та відстеження правопорушників. Автоматизована система ідентифікації відбитків пальців (AFIS) зберігає зображення відбитків пальців у національній базі даних із понад 30 мільйонів карток відбитків пальців. AFIS дозволяє слідчим вирішувати кримінальні справи, яким кілька місяців, а то й кілька років. Оскільки інформаційні технології управління стали настільки цінними для поліцейських управлінь по всій країні, Міжнародна асоціація начальників поліції (IACP) створила Секцію управління інформацією про правоохоронні органи (LEIM) для створення довгострокових та короткотермінових цілей щодо використання комп'ютеризованих інформаційні системи в правоохоронних органах. Члени LEIM вважають, що різке збільшення використання комп'ютерів працівниками правоохоронних органів також збільшить потребу в комп'ютерному навчанні на всіх рівнях правоохоронних органів у майбутньому Поліцейські органи стикаються з низкою перешкод, намагаючись охопити інформаційну епоху. Знайти кваліфікованих та надійних фахівців з інформаційних технологій часто важко для поліцейських органів. Ті, хто має кваліфікацію, зазвичай можуть знайти набагато більш високооплачувані посади в приватному секторі. Аналіз інформації для оперативних цілей (наприклад, аналіз злочинності) – це крок важливіший, ніж просто збирати та зберігати її. Аналіз інформації для цілей управління – для підвищення підзвітності та покращення реагування організації – представляє набагато більш відповідальний крок. Обидва кроки необхідні для того, щоб поліцейські організації могли справді стати "навчальними організаціями".

Література:

1. https://law.jrank.org/pages/1671/Police-Organization-Management-Information-technologies-police.html#ixzz6eYF0uKDm

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

Міщенко А. С.,
заступник начальника Військового коледжу сержантського складу Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

ПРОГРАМНО-ТЕХНІЧНА СИСТЕМА ДЛЯ БЕЗКОНТАКТНОГО ВИЗНАЧЕННЯ ТЕМПЕРАТУРИ ПОРОХОВИХ ЗАРЯДІВ БОЄПРИПАСІВ

Стрімкий розвиток інформаційних технологій, широке застосування мікроконтролерів та комп′ютерних систем дозволяє в наш час вирішувати задачі, які раніше потребували довготривалих і ретельних вимірювань, що нерідко могли виконуватися лише в лабораторних умовах. Приклад успішного розв′язку важливої для артилерійських систем задачі на основі використання спеціалізованої програмно-технічної системи буде розглянуто в даній доповіді.

Аналіз збройних конфліктів сучасності та тенденцій розвитку сучасних артилерійських систем свідчить про те, що розвиток артилерійських комплексів головним чином спрямований на підвищення вогневої продуктивності, дальності та точності стрільби, зменшення уразливості від вогневих ударів артилерії противника [1].

Одним із основних підходів до покращення зазначених характеристик артилерійської системи є автоматизація процесу підготовки до виконання бойового завдання та обладнання артилерійських комплексів системами управління вогнем, навігаційними системами, датчиками, які точно та об'єктивно визначають балістичні та метеорологічні умови стрільби [1, 2].

Автоматизація артилерійських систем, на думку експертів [3], повинна відбуватися за допомогою приладів вимірювання стану ствола, температури метальних зарядів а також системи автоматичного обліку снарядів і зарядів. Артилерійські системи повинні бути оснащені індивідуальними засобами балістичної підготовки, інтегрованої до системи управління вогнем.

Балістична підготовка стрільби передбачає [4]: визначення відхилення початкової швидкості снарядів через знос каналу ствола, визначення різнобою гармат батареї відносно основної гармати, визначення сумарного відхилення початкової швидкості снарядів для основної гармати батареї, визначення температури зарядів, з метою введення поправки на її відхилення від нормальної, визначення балістичних характеристик боєприпасів, сортування та розподіл боєприпасів, організацію збереження боєприпасів за однакових температурних умов.

Визначення різнобою гармат та відхилення початкової швидкості із необхідною точністю можна забезпечити шляхом встановлення на кожну гармату балістичної станції [5], що дозволить автоматично надавати до системи управління вогнем виміряне значення початкової швидкості снаряду.

В той же час засоби вимірювання температури заряду, які використовуються на даний час в Збройних Силах не відповідають вимогам щодо точності та оперативності вимірювань. Методи вимірювання температури зарядів характеризуються наступними серединними помилками для метального заряду – 2-3ºС, реактивного заряду – 4-5ºС [6].

З метою забезпечення точного та оперативного визначення температури зарядів артилерійських боєприпасів, з одночасною можливістю автоматичного введення значення температури заряду до системи управління вогнем, пропонується визначати температуру заряду за зміною температури на поверхні гільзи.

Для визначення середньооб'ємної температури заряду даним методом необхідно двічі через проміжок часу $\Delta\tau$, якій відповідає умові (1), виміряти температуру поверхні гільзи в певній точці на поверхні заряду, потім за залежністю (2) визначити темп охолодження (нагрівання) системи m.

$$\Delta\tau \geq \frac{0,3l^2}{\alpha}, \tag{1}$$

де $\Delta\tau$ – проміжок часу між вимірюваннями;

l – довжина артилерійського заряду;

α – коефіцієнт температуропровідності пороху в заряді.

$$m = \frac{\ln t_{p1} - \ln t_{p2}}{\Delta\tau}, \tag{2}$$

де m – темп охолодження;

t – температура;

індекс p відповідає параметрам поверхні (гільзи), індекси 1 та 2 відносяться до першого та другого вимірювання відповідно.

При відомому значенні темпу охолодження m середньооб'ємна температура заряду визначатиметься за залежністю:

$$t_{z2} = \frac{(t_{p1} - t_{p2})\sum_{i=1}^{i=n} c_i\rho_i V_i(m+1)}{c_z\rho_z V_z(e^{-m\Delta\tau} - 1)} e^{-m\Delta\tau}, \tag{3}$$

де c_i – питома масова теплоємність матеріалу частини боєприпасу;

ρ_i – густина матеріалу частини боєприпасу;

V_i – об'єм частини боєприпасу

індекс z відповідає параметрам порохового заряду.

Для практичного використання безконтактного методу визначення температури заряду артилерійського боєприпасу розроблено наступний алгоритм (рис.1):

Крок 1: Підготовка до роботи вимірювального приладу та поверхні гільзи: перевірка зарядженості елементів живлення приладу, введення коефіцієнту випромінювання, відповідно до матеріалу поверхні гільзи очищення поверхні оболонки заряду від бруду та пилу.

Крок 2: Вимірювання значення температури поверхні T_1, початок вимірювання часу (отримання значення τ_1).

Крок 3: Після визначення проміжку часу між вимірюваннями $\Delta\tau$ і визначення τ_2, як $\tau_2 = \tau_1 + \Delta\tau$, вимірювання значення температури поверхні T_2 в момент часу τ_2.

Крок 4а: Якщо температура $T_1 = T_2$, тобто температура поверхні не змінюється, вважаючи процес стаціонарним приймаємо, що температура поверхні та заряду однакова $T_з = T_1 = T_2$, здійснюється перехід до кроку 6.

Крок 4б: Якщо температура $T_1 \neq T_2$, що свідчить про нестаціонарність процесу здійснюється перехід до кроку 5.

Крок 5: За залежністю (2) визначається темп охолодження (нагрівання) заряду за наявних умов.

Крок 6: За залежністю (3) визначається середньооб'ємна температура заряду в момент часу τ_2.

Крок 7 За таблицями стрільби артилерійської системи на основі отриманого в кроці 4а або 6 значення температури заряду визначається відповідна поправка на температуру заряду.

Крок 8 Отримана поправка передається до системи підготовки даних для стрільби.

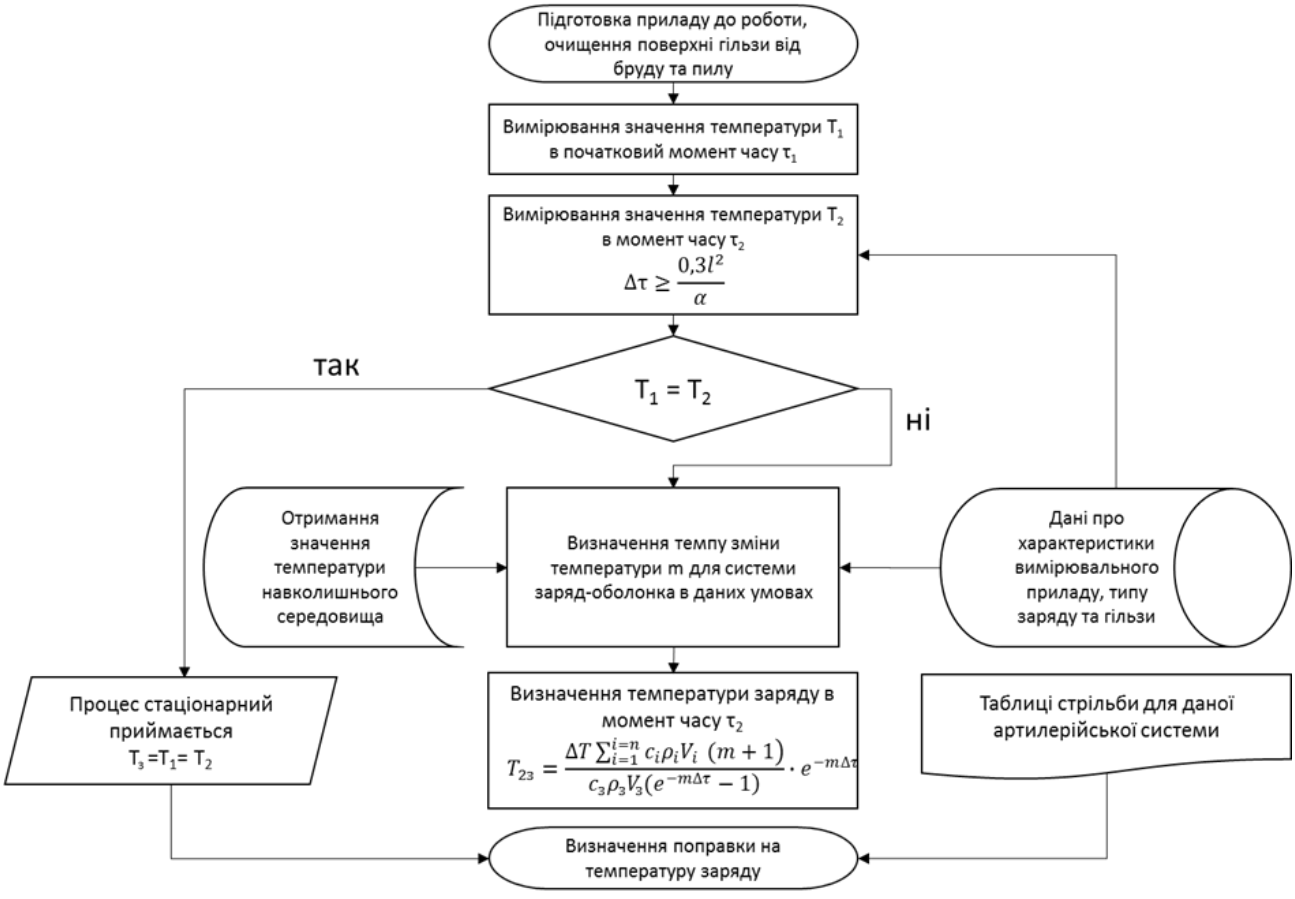


Рис 1. Блок-схема алгоритму визначення температури заряду артилерійського боєприпасу безконтактним методом та внесення відповідної поправки в данні для стрільби

Введення до системи управління вогнем такого способу дозволяє значно збільшити точність та оперативність визначення температури зарядів, крім того за умови застосування приладу із відповідним інтерфейсом надає можливість автоматичного введення виміряного значення температури зарядів до розрахунків.

Література:

1. М. І. Бєляєв, О. М. Толмачов Моніторинг стану самохідної артилерії сухопутних військ Збройних Сил України та визначення напрямків її розвитку / Системи озброєння і військова техніка. Сумський державний університет, Суми — 2015. — № 3(43) .
2. П. Є. Трофименко, Л.С. Демидко, Д.Л. Демидко Напрями удосконалення вітчизняних реактивних систем залпового вогню / Системи озброєння і військова техніка. Сумський державний університет, Суми — 2015 — № 1(41) – с. 75-78.
3. А. М. Кривошеєв Напрямки використання балістичної інформації провідними виробниками артилерійських систем / Системи озброєння і військова техніка. Сумський державний університет, Суми — 2009. — № 1(17) – с. 49-63.
4. Бойова робота вогневих підрозділів: навчальний посібник / О. П. Красюк, М. В. Бахмат, П Є. Трофименко та ін. – Львів: АСВ, 2012. – 280 с.
5. П. П. Ткачук Ю. І. Бударецький Ю. В. Щавінський В. В. Прокопенко. Вплив засобів автоматизації управління підрозділами і вогнем артилерії на ефективність її застосування/ Військово-технічний збірник – Львів, АСВ – 2015. – №12 – с.75-82
6. П. Є. Трофименко, В. І. Макеєв, А. Ф. Раскошний. Шляхи підвищення точності вимірювання температури зарядів у наземній артилерії / Системи озброєння і військова техніка. Сумський державний університет, Суми — 2011. — № 1(25) . — С. 58 — 60.

Кудінов В. А.,
професор кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ,
кандидат фізико-математичних наук, доцент

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЩОДО АНАЛІЗУ ДИНАМІКИ ЗАГАЛЬНОЇ КІЛЬКОСТІ ЗЛОЧИНІВ ПРОТИ ГРОМАДСЬКОЇ БЕЗПЕКИ ТА ПУБЛІЧНОГО ПОРЯДКУ В УКРАЇНІ ЗА 2013-2019 РОКИ

Національну поліцію України (далі – НПУ) було створено в 2015 році в межах реформування Міністерства внутрішніх справ [1; 2]. Одними з основних завдань НПУ є реалізація державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку. НПУ, відповідно до покладених на неї завдань, здійснює моніторинг оперативної обстановки в державі, вивчає, аналізує і узагальнює результати та ефективність поліцейської діяльності тощо.

Інформація про стан та структуру злочинності в Україні з 20 листопада 2012 року знаходиться в Єдиному реєстрі досудових розслідувань, держателем якого є Генеральна прокуратура України (з 02 січня 2020 року – Офіс Генерального прокурора) [3]. Реєстр утворений та ведеться відповідно до вимог Кримінального процесуального кодексу України з метою забезпечення: 1) реєстрації кримінальних правопорушень (проваджень) та обліку прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження; 2) оперативного контролю за додержанням законів під час проведення досудового розслідування; 3) аналізу стану та структури кримінальних правопорушень, вчинених у державі; 4) інформаційно-аналітичного забезпечення правоохоронних органів.

Аналіз оперативної обстановки в державі можливостями автоматизованої системи оперативного інформування МВС України у 2000-2012 роках наведено в роботі [4].

На підставі даних Єдиного реєстру досудових розслідувань проаналізуємо динаміку загальної кількості злочинів проти громадської безпеки та публічного порядку в Україні за 2013-2019 роки. Для цього будемо використовувати статистичні дані Єдиних звітів про кримінальні правопорушення в державі за 2013-2019 роки [5], а саме: загальні відомості про кількість зареєстрованих кримінальних правопорушень та результати їх досудового розслідування розділу 1, в якому таблиця 1.10 присвячена злочинам проти громадської безпеки, а таблиця 1.13 – злочинам проти громадського порядку та моральності. На нашу думку, слушною є позиція здобувача наукової лабораторії з проблем забезпечення публічної безпеки і порядку Національної академії внутрішніх справ (м. Київ, Україна) Крищенка А. Є., що на сучасному етапі розвитку законодавчого поля терміни «публічна безпека» і «публічний порядок» можна вважати рівнозначними поняттями з «громадська безпека» та «громадський порядок» [6].

Проведені нами дослідження представлено на рис. 1-4.

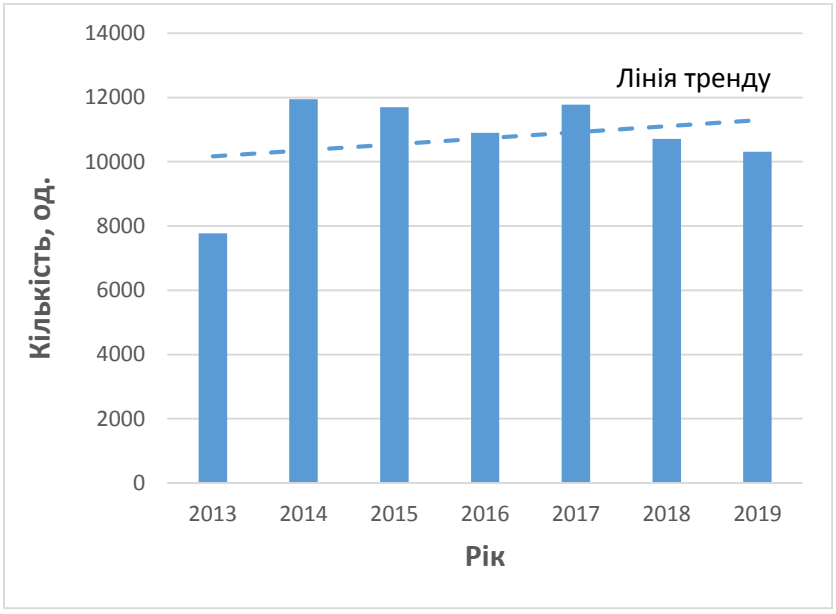


Рис. 1. Залежність загальної кількості злочинів проти громадської безпеки від року

Незважаючи на зменшення загальної кількості злочинів проти громадської безпеки після 2017 року, спостерігається, відповідно до лінії тренду, загальна тенденція щодо збільшення їх кількості протягом 2013-2019 років (рис. 1).

Необхідно відмітити, що до 01 липня 2020 року існувала така класифікація злочинів за тяжкістю: особливо тяжкі, тяжкі, середньої тяжкості, невеликої тяжкості. На рис. 2 представлені графіки залежності загальної кількості злочинів різних ступенів тяжкості проти громадської безпеки від року.

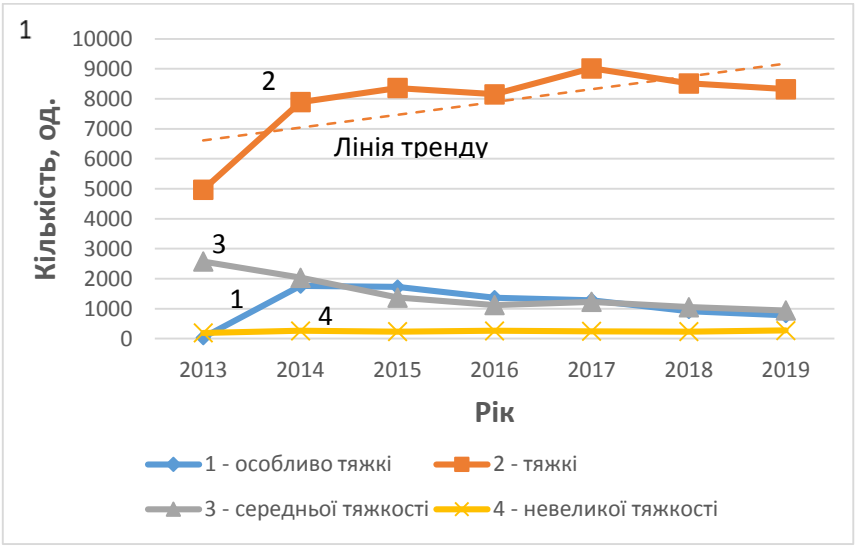


Рис. 2. Залежність загальної кількості злочинів різного ступеня тяжкості проти громадської безпеки від року

Їх аналіз дозволяє зробити такі висновки. Для особливо тяжких злочинів відмічається їх максимум в 2014 році, після якого спостерігається незначне їх зменшення протягом 2015-2019 років. Кількість тяжких злочинів значно перевищує кількість злочинів інших ступенів тяжкості (так, зокрема, в 2019 році – більше ніж в 8 разів). Крім того, відповідно до лінії тренду для тяжких злочинів спостерігається тенденція щодо їх збільшення протягом 2013-2019 років. Але для злочинів середньої тяжкості спостерігається, навпаки, тенденція щодо їх зменшення. Необхідно також відмітити, що кількість злочинів невеликої тяжкості залишається майже постійною.

Незважаючи на локальне збільшення загальної кількості злочинів проти громадського порядку та моральності в 2017, 2018 роках у порівнянні з попередніми роками, спостерігається, відповідно до лінії тренду, загальна тенденція щодо зменшення їх кількості протягом 2013-2019 років (рис. 3).

Рис. 3. Залежність загальної кількості злочинів проти громадського порядку та моральності від року

Протягом 2013-2019 років відмічаються такі тенденції для злочинів різного ступеня тяжкості проти громадського порядку та моральності (рис. 4), а саме: 1) збільшення загальної кількості особливо тяжких та тяжких злочинів; 2) зменшення загальної кількості середньої та невеликої тяжкості злочинів (при цьому їх кількість майже однакова). Необхідно також відмітити, що в 2019 році загальна кількість тяжких злочинів проти громадського порядку та моральності перевищує в 17 разів загальну кількість особливо тяжких та в 1,3-1,5 рази загальну кількість невеликої та середньої тяжкості злочинів.

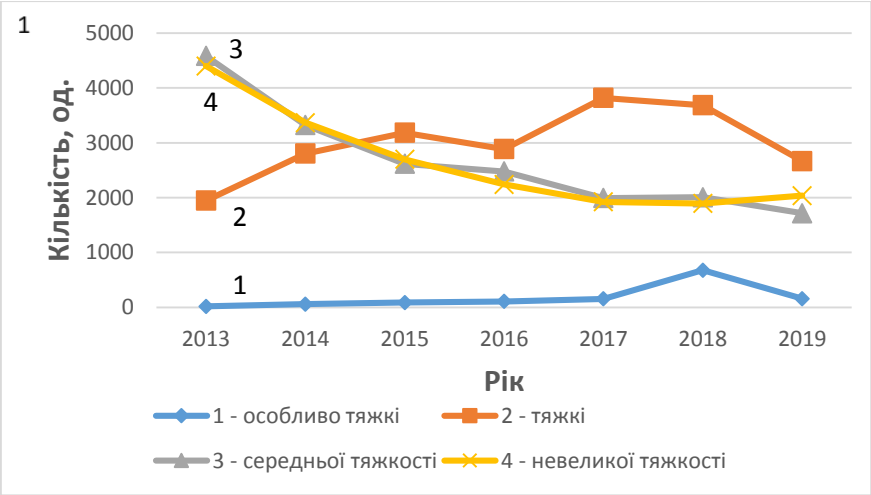


Рис. 4. Залежність загальної кількості злочинів різного ступеня тяжкості проти громадського порядку та моральності від року

Вважаємо, що органам Національної поліції України необхідно врахувати вище зазначені результати наукового дослідження для планування заходів щодо протидії злочинам проти громадської безпеки та публічного порядку.

Література:

1. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/580-19.
2. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877. *Верховна Рада України*: [сайт]. URL: http://zakon3.rada.gov.ua/laws/show/877-2015-%D0%BF.
3. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: Наказ ГПУ від 06 квіт. 2016 р. *Верховна Рада України*: [сайт]. URL: http://zakon2.rada.gov.ua/laws/show/z0680-16.
4. Кудінов В. А. Аналіз оперативної обстановки можливостями автоматизованої системи оперативного інформування МВС України. *Бюлетень з обміну досвідом роботи МВС України*. 2012. № 190. С. 28–33.

5. Статистична інформація за 2013-2019 роки. Офіс *Генерального прокурора*: [сайт]. URL: https://www.gp.gov.ua/ua/1stat

6. Крищенко А. Є. Особливості визначення терміна «публічна безпека і порядок». *Науковий вісник Національної академії внутрішніх справ*. 2017. № 1 (102). С. 206–214.

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

ВИКОРИСТАННЯ ВІТРУАЛЬНИХ ТЕХНОЛОГІЇ ТА ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ В ОСВІТНЬОМУ ПРОЦЕСІ

Інформаційні технології проникають в усі галузі діяльності людини, змінюють характер праці як у виробничій, так і у невиробничій сферах, підвищують рівень інформування широких верств населення, відкривають нові перспективи для підвищення ефективності освітнього процесу.

Останні дослідження показують, що обсяг ринку освітнього програмного забезпечення у 2018 році становить 2,3 млрд. доларів, а до 2025 року цей показник зросте вдвічі [6]. Це свідчить про активне впровадження і використання програмного забезпечення в усіх сферах освіти. У школах та університетах по всьому світу безліч технологій використовують для забезпечення інтерактивного навчання дітей та здобувачів вищої освіти.

До одних із перспективних освітніх сучасних інформаційних технології можна віднести віртуальні технології (VR) та технології доповненої реальності (AR), які здатні проектувати цифрову інформацію (зображення, відео, текст, графіку) поза екранами пристроїв та об'єднувати віртуальні об'єкти з реальним середовищем. Технології віртуальної реальності (Virtual Reality, VR) створені за допомогою комп'ютерних систем, забезпечують зорові, звукові та інші відчуття, за допомогою 360° картинки переносять людину в штучний світ, де навколишнє середовище повністю змінене. Віртуальна реальність імітує як вплив, так і реакції на вплив.

Доповнена реальність (Augmented Reality, AR) – це технологія, яка допомагає відслідковувати позицію та орієнтуватися в просторі за допомогою сенсорів та камери. Завдяки цьому можливо створити точну 3D-модель простору навколо пристрою, оновлювати її в реальному часі, визначати в ній положення, передавати ці дані всім додаткам та накладати поверх неї додаткові шари. Можливості цієї технології насправді унікальні: можна вимірювати відстані, вставляти різноманітні об'єкти та взаємодіяти з ними.

Технології віртуальної реальності є об'єктом дослідження багатьох вчених. Так використанню віртуальної реальності в різних сферах життєдіяльності людини присвячені праці С. В. Аксьонова "Компьютерное моделирование и виртуальная реальность" [1], А. В. Гощинського "Інноваційний розвиток мережевих організацій віртуального типу" [2], А. О. Петренко-Лисак "Соціальні детермінанти кіберв'ртуального простору" [3], А. А. Засєкін «Віртуальне спілкування як чинник особистісних змін студентської молоді», Ю. С. Лемешко «Синергетична модель управління проектами організації системи знань віртуального університету" [4].

Прикладом використання технології віртуальної і доповненої реальності в сфері освіти є створення віртуальних лабораторій. Віртуальні лабораторії - це змодельовані навчальні середовища, які дозволяють здобувачам освіти проводити лабораторні експерименти в Інтернеті та досліджувати концепції та теорії, не вступаючи у фізичну наукову лабораторію.

Використання віртуальних лабораторій в освітньому процесі допоможе здобувачам освіти:

- випробувати лабораторні методи та ознайомитись із передовим лабораторним обладнанням, яке в іншому випадку може бути недоступним;
- потренуватися, ознайомитись та впевнитись у роботі обладнання, перш ніж потрапити до справжньої лабораторії;
- надати нескінченну кількість часу для повторення та участі в експериментах;
- залучати до унікального, збагачуючого та захоплюючого досвіду, який має актуальність та застосування у реальному світі;
- візуально відчувати складні концепції, які в іншому випадку є занадто абстрактними або складними для вивчення на традиційному курсі;

Використання віртуальної лабораторії є безпечніші для занять, ніж реальні лабораторії та повністю виключає етичні питання, оскільки всі досліди, які розбирають та тестують користувачі є віртуальними.

Однією з таких лабораторій є *LABSTER* [8] – інтерактивний 3D-проект, розроблений у партнерстві з провідними університетами – MIT (Massachusetts Institute of Technology, Массачусетський технологічний інститут), Гарвардом і Стенфордом.

Також серед кращих проектів, які використовуються в світі, слід відзначити такі, як

Unimersiv [10] – це навчальна платформа для VR, яка щомісяця випускає навчальний контент. Вміст у програмі Unimersiv є більш індивідуалізованим та захоплюючим, і на даний момент доступними в програмі є три освітні враження. Unimersiv прагне створювати освітній контент на широкий спектр тем, що робить їх потенціал справді необмеженим.

Immersive VR Education *Lecture VR* [11] – це програма VR від Immersive VR Education, яка імітує лекційний зал у віртуальній реальності, додаючи при цьому спеціальні ефекти, які не можна використовувати в традиційних умовах класу. Лекції супроводжуються зображеннями, відео та захоплюючими враженнями, які покращують заняття. Ще одним головним надбанням цього типу навчання є те, що студенти та професори можуть віддалитися з будь-якої точки світу, що робить освіту більш доступною на глобальному рівні.

Програма Google Expeditions Pioneer Google [12] також вирує у сферу VR-освіти завдяки своїй захоплюючій програмі *Expeditions Pioneer*. Мета програми полягає в тому, щоб команди експедицій від Google відвідували школи по всьому світу та забезпечували все, що потрібно вчителям, щоб взяти своїх учнів у подорож куди завгодно; команда також допоможе викладачам у створенні та використанні цієї технології. Додаток працює таким чином, що здобувачі освіти та викладачі бачитимуть одне і те ж і будуть на одній сесії, але викладач зможе читати лекції та виділяти певні речі, які мають відношення до заняття.

zSpace [13] унікальний в освітній сфері у VR завдяки технології, яку вони використовують. zSpace вважає, що технологія VR не обов'язково повинна бути такою асоціальною та односторонньою, як кожен, хто одягає власну гарнітуру. zSpace має монітори, подібні до того, як працюють 3D-фільми, де група людей використовує окуляри, схожі за своїм відчуттям на 3D-окуляри; ці окуляри змушують вміст відриватися від екрана. Крім того, користувачі zSpace мають ручку, якою вони керують для стимулювання. Наразі zSpace пропонує контент для STEM-освіти та більш загального досвіду математики та науки.

Nearpod [14] використовує 360-градусні фотографії та відео в планах уроків, а також має щось подібне до PowerPoint, яке студенти можуть використовувати поряд із 360-градусними фото та відео. Існують також варіанти, щоб студенти відповідали на запитання, набираючи текст на своєму ноутбуці чи планшеті. Nearpod VR дає нам уявлення про те, як буде виглядати клас майбутнього, при цьому плани уроків будуть вдосконалені за допомогою технологій VR та AR, а студенти будуть більше залучені за допомогою цієї нової технології.

Як бачимо, використання віртуальної реальності відкриває багато нових можливостей в навчанні та освіті до основних переваг застосування AR/VR технологій можна віднести [5, 7]:

- наочність, використання 3D-графіки, дозволяє у віртуальній реальності дозволяє не тільки дати відомості про саме явище, а й продемонструвати його з будь-яким ступенем деталізації;
- залучення, віртуальна реальність дає змогу змінювати сценарії, впливати на хід експерименту або вирішувати завдання в ігровій і доступній для розуміння формі;
- фокусування, віртуальний світ, який оточить глядача з усіх боків на всі 360 градусів, дозволить цілком зосередитися на матеріалі і не відволікатися на зовнішніх подразників;
- безпека, управління надшвидкісним поїздом, техніка безпеки під час пожежі, кримінальна ситуація, у віртуальні реальності можна занурити користувача в будь-яку з цих ситуацій без найменших загроз для життя;
- результативність, вчені Мерілендського університету провели дослідження, під час якого запропонували двом групам людей запам’ятати розташування певних зображень. Під час експерименту одна з груп використовувала шоломи віртуальної реальності, друга – звичайні комп’ютери. При цьому група, яка вивчала зображення за допомогою VR-шоломів, показала результат на 10 % вищий, ніж учасники іншої групи [6].

Використання віртуальних технологій та технологій доповненої реальності – великий крок вперед в системі освіти. Ці технології корисні як для викладачів, так і для здобувачів освіти. Викладачі зможуть як ніколи привернути увагу своїх слухачів та залучити їх активніше до занять. Використання технологій VR та AR не тільки зробить навчання більш цікавим та захоплюючим для здобувачів освіти, але й збільшить можливість глибше вивчати предмети, візуалізувати та аналізувати.

Література:

1. Aksenova EA Metodologiya modelirovaniya tekhnologicheskikh ob "yektov pishchevykh proizvodstv. *XXI century: results of the past and problems of the present plus ": Periodical scientific publication*. Penza: Publishing house Penza. state. technol. Univ. 2016. No. 05 (33). - 144 p.
2. Гощинський А. В. Інноваційний розвиток мережевих організацій віртуального типу (на прикладі інформаційно-комунікаційного сектора економіки: автореф. дис. на здобуття наук. ступ. канд. екон. наук: 08.00.03. НАН України, Інт регіон. дослідж. Л., 2010. 20 с.
3. Петренко-Лисак А. О. Соціальні детермінанти кібервіртуального простору: дис. канд. соц. наук: 22.00.04. Київ, 2007. 192 с.
4. Ю. С. Лемешко «Синергетична модель управління проектами організації системи знань віртуального університету": автореф. дис. на здобуття наук. ступ. канд. тех. наук: 05.13.22 . Київ. 2015. 24 с.
5. Трач Ю. VR-технології як метод і засіб навчання. *Освітологічний дискурс*. 2017. № 3–4, С. 309–322. URL: http://nbuv.gov.ua/UJRN/osdys_2017_3-4_26. (дата звернення 10.12.2020).
6. Віртуальна та доповнена реальність: як нові технології надихають вчитися URL: https://osvitoria.media/opinions/virtualna-ta-dopovnena-realnist-yakoyu-mozhe-buty-suchasna-osvita/
7. Кухтюк В.О. Використання технології віртуальної реальності в освіті. *Актуальні питання сучасної інформатики.* 2017.(5). pp. 241-243.
8. Labster | 100+ virtual labs for universities and high schools. URL:https://www.labster.com/the-complete-guide-to-virtual-labs/
9. 9. Вовк Н., Шельвицька О. Використання методів штучного інтелекту для синтезу VR/AR технологій у навчанні. *Інформація, комунікація, суспільство 2019* : матеріали 8-ої Міжнародної наукової конференції ІКС-2019, 16-18 травня 2019. Львів : Видавництво Львівської політехніки, 2019. С. 55–56.
10. Unimersiv: VR Training // Virtual Reality Education URL: https://unimersiv.com/
11. Immersive VR Education | Learn through Experience | Home URL: URL: https://immersivevreducation.com/
12. Pioneer Expeditions - Off the beaten track and adventure ... URL: https://www.pioneerexpeditions.com/
13. zSpace: AR/VR Learning Experiences URL: https://zspace.com/
14. Nearpod: Make every lesson interactive URL: https://nearpod.com/

Лозинський О. Ю.,
професор кафедри енергетики і систем керування Національного університету «Львівська політехніка», доктор технічних наук, професор

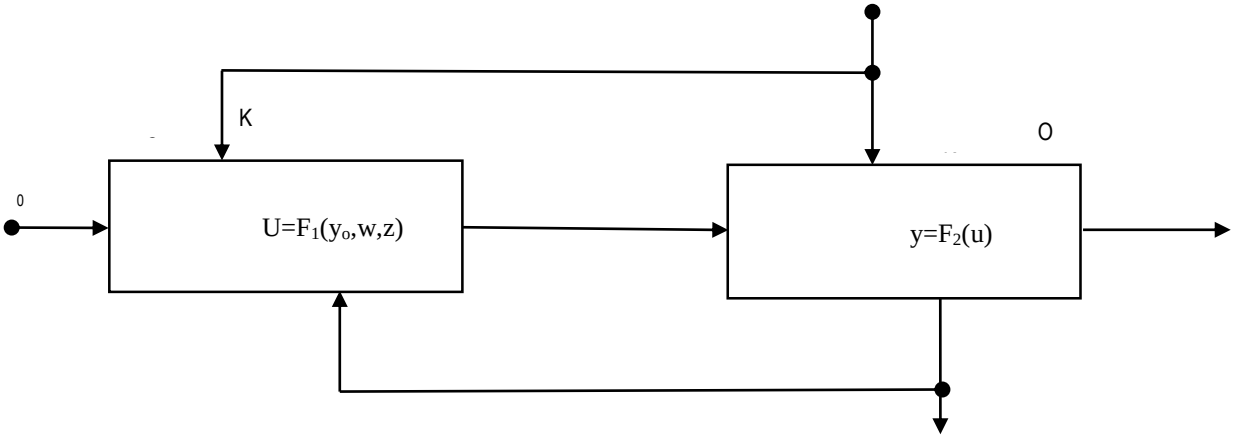
Лозинський А. О.,
директор інституту енергетики і систем керування Національного університету «Львівська політехніка», доктор технічних наук, професор

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

ПРО ДЕЯКІ АСПЕКТИ В ТЕОРІЇ КЕРУВАННЯ ДЕТЕРМІНОВАНИМИ І СТОХАСТИЧНИМИ ОБ'ЄКТАМИ

Зазначимо, що цей матеріал стосується насамперед теорії керування технологічними процесами в різних галузях людської діяльності. Тут не розглядаються автоматизовані системи управління, тому що за існуючими нормативними документами це – "людино-машинні системи, які призначені для збору і обробки інформації необхідної для оптимізації управління в різних сферах людської діяльності". Тобто така система збирає і переробляє інформацію для прийняття рішень на вищому рівні ієрархії, де про керування технологічним процесом може навіть і не згадуватися в класичному розумінні теорії керування.

В українській мові є можливість розрізняти терміни "управління", як прийняття стратегічних рішень і "керування", як формування керуючих впливів, зокрема в технічній системі. Замкнуту систему керування можна представити у вигляді такої типової функціональної схеми (рис. 1).



У цій схемі – КО-керуючий об'єкт, тобто система яка виробляє керуючий вплив; ОК – керований об'єкт, або об'єкт керування; y – вектор координат об'єкта керування; x – вимірювані координати, які характеризують стан об'єкта керування; y_o – вектор задаючих впливів; w – збурюючі впливи; u – керуючі впливи; z – сигнали зворотнього зв'язку; F_1 – функціональна залежність, яка характеризує формування керуючих впливів; F_2 – функціональна залежність, яка характеризує процеси в об'єкті керування.

Рис. 1. Функціональна схема замкнутої системи керування

Під керуванням розуміємо процес, який забезпечує необхідне при використанні за цільовим призначенням, протікання технологічного процесу перетворення енергії, речовин і інформації, або підтримання працездатності і безаварійності функціонування об'єкта шляхом збору і обробки інформації про стан об'єкта і зовнішнє середовище, а також напрацювань рішень щодо впливу на об'єкт і їх реалізацію, включаючи оптимізацію за цільовим призначенням. В цьому визначенні ми спеціально оминаємо самоорганізацію і самоналагодження системи. Ці принципи є предметом синергетики з однієї сторони і штучного інтелекту з іншої, які вивчають процеси самоорганізації у взаємодії з середовищем і тому охоплюють всі сучасні галузі знань про природу, в тому числі технічні і економічні.

У відкритих системах, які обмінюються із зовнішнім середовищем енергією, речовиною і інформацією виникають процеси стихійної самоорганізації, тобто процеси народження із фізичного хаосу деяких стійких впорядкованих структур, з новими властивостями. Необхідним фактором такої само організації в загальному випадку виступає наявність так званого «критика», який задає напрям процесу самоорганізації і на вищих ієрархічних рівнях цим «критиком» може бути таке філософське поняття, як Вищий Розум.

В античні часи, все що не вписувалося в звичні логічні заключення позначалося словами "випадок", "стихійність", "невизначеність" і вважалося, що то лише наслідок нашого незнання. За Дарвіном – випадковість це не відсутність закономірності, а лише непізнана закономірність схована від нас до певного часу. Зрозуміло, що під закономірністю він розумів все те що вписується в закони формальної логіки. "Випадковість – це витвір слабості (немочі) нашого розуму". Аналогічне визначення випадковості подав Франц Кафка : "Випадковість існує лише в нашому обмеженому сприйнятті. Вона є віддзеркалюванням меж нашого пізнання".

В такому разі "випадковість", "невизначеність", "стихійність" – це поняття якими ми моделюємо те, що не змогли пізнати на основі доступних нам уявлень. Згідно з твердженням Ейнштейна "Бог не гравець" і тому для Вищого Розуму все у Всесвіті є чітко детермінованим і має свої чіткі закони, які ми в силу відносності і абсолютності істини не пізнаємо ніколи. Поняття "випадку" в науці запровадили математична статистика і статистична фізика. Їхні постулати базуються на тому що "багато що в цьому світі є випадковим і зовсім не тому, що ми не знаємо додаткових умов, які перетворюють, допустимо, випадкове випадання "орла" на монеті, в необхідність – а це явище є випадковим за своєю природою".

Отже, у відповідності з базовими положеннями синергетики, її особливістю є стихійна самоорганізація, а суть виникаючих при цьому процесів, лежить у внутрішніх причинах – тобто причинний спосіб самоорганізації, а ті причини далеко не завжди є передбачуваними. Але при цьому в

теорії синергетичного керування спостерігається відхід від непередбачуваної поведінки системи, до направленого руху вздовж бажаних інваріантних видів – так званих аттракторів, до яких підлаштовуються всі змінні системи. А це вже спосіб направленої самоорганізації динамічних систем, яка забезпечується наявністю «критика».

Основною задачею теорії керування є задача переводу відповідної системи в якийсь визначений кінцевий стан незалежно від його попереднього стану. Але тут стає на перешкоді знаменита тріада – "нелінійність", "багатозвязність", "багато вимірність", яка викликає містичний жах в багатьох проектувальників і науковців. Ця тріада стала своєрідним методологічним бар'єром. На основі концепції, а вірніше "синергетичної" концепції керованої взаємодії енергії речовини і інформації в процесах різної природи, базується метод "аналітичного конструювання агрегованих регуляторів" – АКАР. Цей метод і принцип, який лежить в його основі дозволив подолати "прокляття розмірності" складних систем сформульоване Р.Беллманом, ба, навіть при такому принципі прекрасним стає теза "про благотворність високої розмірності". Але захоплюватися математичним "вбиранням" задач керування не варто, тому що можна прийти до тези, висловленої знову ж таки Ейнштейном - "Існує дивовижна можливість оволодіти предметом, не розуміючи суті справи". Тому математизація сучасної теорії автоматичного керування привела до того, що за захопленням математичною строгістю викладок ігноруються такі фундаментальні поняття як фізична суть і індивідуальна особливість керованого нелінійного об'єкта. За академіком Красовським А.А. – класичну теорію автоматичного регулювання створювали інженери для інженерів. Сучасну теорію автоматичного керування створюють в основному математики для інженерів, що також непогано, але коли на останньому етапі СТАК створюють математики для марематиків, то це вже розділ математики, який розвивається по своїх законах і рідко знаходить застосування в реальних системах керування. А це вже недобре з точки зору інженера і фізики процесів. Тому А.А. Красовським була поставлена проблема створення "фізичної теорії керування" – основним аспектом якої буде повернення витка спіралі від виключення фізичних властивостей об'єкта до їх включення. Крім того фізична суть пов'язана з такою властивістю об'єкта як лінійність, як індивідуальна, унікальна риса, а не лінійність, як типізація, основана на принципі суперпозиції занурення часткового явища в загальний опис, і тому пов'язана з математизованою стороною явища. Поєднання розвинутої аналітичної прикладної СТАК, як фундамента алгоритмічного забезпечення, з чисельними методами, як формою реалізації алгоритмів, ось де здавалося шлях рішення основної проблеми СТАК - оптимального керування у великому складними процесами. В той же час обчислювальний підхід в рішенні проблем СТАК за наявності такого потужного апарату оптимізації як еволюційні алгоритми створює у недосвідченого дослідника ілюзію простоти синтезу керуючих впливів та комп'ютерної всеохопленості будь-яких складних проблем і можливостей їх вирішення без розуміння суті процесів в системі. На жаль такий підхід може призвести до непередбачуваної поведінки реального об’єкту.

Сучасна теорія автоматичного керування повинна створюватися на умілому поєднанні "математики і фізики" досліджуваних систем. Тут потрібно привести кілька цитат видатних вчених, які підтверджують сказану тезу. Р. Нейман – видатний фізик – "якщо ми хочемо, щоб від науки було якась користь – ми повинні будувати догадки. Щоб наука не перетворилась в протоколи зроблених експериментів – ми повинні висовувати закони, які простираються на ще не звідані області".

Ісаак Ньютон – при вивченні наук приклади не менш повчальні ніж правила.

Дж. Максвелл – на благо людей з різним складом розуму наукова правда повинна представлятися в різних формах і повинна вважатися рівно науковою, чи вона представляється в формі і живих відтінках фізичної ілюстрації, чи в простоті і скупості символічних перетворень і виразів.

Представляючи цей матеріал, ми хотіли звернути увагу дослідників на необхідність всебічного підходу, включаючи філософські аспекти, до створення нових принципів і положень сучасної теорії автоматичного керування динамічними системами і технологічними процесами, які в них протікають.

Д'яков А. В.,
начальник науково-дослідного відділу (моделювання бойових дій) Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук

ПІДХОДИ ДО ПРОЕКТУВАННЯ ІМІТАЦІЙНИХ МОДЕЛЕЙ ЗБРОЙНОГО ПРОТИСТОЯННЯ ДЛЯ ПІДГОТОВКИ ВІЙСЬК

Існуючи тенденції математичного опису збройного протистояння передбачають математичний опис заснований на порівнянні бойових потенціалів, логіко-аналітичні методи, що характеризуються представленням реальних процесів і систем у вигляді явних функціональних залежностей (сценаріїв, етапів вирішальних правил), імітаційні, де описується апарат прийняття більш частих рішень з елементом ймовірності (ціль вражена/не уражена, виявлена/не виявлена) та інші.

В свою чергу, для процесів, що мають складний характер поведінки, якими є процеси збройної боротьби, при відсутності можливості математичної формалізації, яка забезпечує аналітичне рішення задачі, єдиними підходом до дослідження є використання методів імітаційного моделювання.

При проектуванні моделей збройного протистояння, підготовки системотехнічних та програмних рішень в першу чергу беруться до уваги цільова настанова моделювання, її функціональне призначення та місце моделі у системі прийняття рішення. При цьому, треба розуміти, що модель є лише інструментом діяльності посадових осіб штабу та командирів та не може забезпечувати відпрацювання єдиного вірного та всебічно обґрунтованого рішення за умови конкретної обстановки.

Модель є допоміжним інструментом підтримки процесу прийняття рішення та оцінки можливих альтернатив. Це обумовлено тим, що її математичний апарат і алгоритми охоплюють собою множину складних процесів, факторів і умов, які безпосередньо впливають результати моделювання. Частина з них задається кількісно, наприклад бойовий та чисельний склад конфліктуючих угрупувань, види та характеристики озброєння та військової техніки, ресурси, що виділяються фізико-географічні та метеорологічні умови та інші.

Інша частина вихідних даних за об'єктивними причинами неможливо представити у кількісному вимірюванні у наслідок того, що вони відносяться до когнітивної сфери людини. Саме тому, сьогодні при моделюванні бойових дій враховуються тільки формальні дані.

Врахування двостороннього характеру збройного протистояння зумовлює опис процесів протистояння двох антагоністичних систем, які вступають між собою не тільки в бойовий, але й в інтелектуальний конфлікт, що передбачається задумами дій сторін. Тому збройне протистояння розглядаються не тільки як збройне протиборство двох антагоністичних систем, але і як систем, що одночасно реалізують увесь свій інформаційний, морально-бойовий, психологічний та морально-технічний потенціал, який враховується у двох рішеннях конфліктуючих сторін.

Таким чином, такий підхід дозволяє створити біполярну модель, яка має у своєму складі два конкуруючих центра управління, що представляються відповідними моделями на декількох рівнях. У цьому випадку на перший план виходить не матеріальна складова бою, а прийняте рішення командиром та поставлені задачі військам.

Слід враховувати, що підсумки бойових дій необхідно розглядати крізь призму досягнення цілі та виконання поставлених бойових завдань своїми військами, незважаючи на те, що у даній структурі відтворена симетрія дій сторін, а противник розглядається як зовнішнє джерело випадкових та невигідних дій, що примушують до пошуку нових рішень, у відповідності до швидкоплинної обстановки.

В даній структурі бойові дії моделюються на трьох рівнях управління.

Перший рівень, забезпечує моделювання в інтересах прийняття рішення командуючим оперативного об'єднання.

Другий, охоплює процеси прийняття рішення і постановку завдань у тактичної ланці управління.

Третій рівень – це рівень виконавців поставлених завдань, тобто безпосередньо підпорядкованих підрозділів, де моделюється практична реалізація рішень двох вищих рівнів. За своєю суттю третій рівень представляє собою сукупність окремих моделей бойових дій різних видів і родів військ та є «фізичним» середовищем моделі, де відтворюється не просто збройний конфлікт, а сукупність усіх протиборств у всіх сферах їх прояву.

Необхідно зауважити, що для забезпечення гнучкості моделі, врахування проміжних результатів оперативно-тактичних розрахунків та вплив умов розвитку бойової обстановки передбачається втручання людини в процес моделювання за допомогою специфічних процедур. Завдяки цьому можливо враховувати нові данні, що виникають з розвитком обстановки, отримувати проміжні та кінцеві показники, змінювати умови моделювання, уточняти та оцінювати вплив різних факторів на попередній план. За цих умов процес моделювання програмується дискретно, по етапам та покроковою фіксацією стану та положення сили і засобів сторін.

На кожному з етапів забезпечується можливість уточнення даних та отримання різних варіантів дій.

Необхідно відмітити, що на сьогодні практично всі існуючі моделі мають ряд суттєвих недоліків:

- не враховують змін у сутності та змісті сучасного збройного протиборства;
- не «відчувають» усю різноманітність форм і способів оперативного і бойового застосування військ;
- не враховують неформальні вихідні дані, якими є військове мистецтво командирів, їх тактична «грамотність», бойовий дух та морально-психологічна підготовка особового складу;
- не відповідають на питання, що зробити, щоб отримати бажаний результат. Застосування сучасних моделей для складання найбільш раціонального плану потребує розгляду великої кількості альтернатив та підходить тільки для етапу завчасної підготовки до бойових дій.

Незважаючи на вказані недоліки, використання імітаційного моделювання при підготовці фахівців силових відомств дозволяє:

- забезпечити підвищення рівня навченості і злагодженості органів управління;
- проводити імітацію складної обстановки, аналізувати і оцінювати дії сторін за різними варіантами у найкоротші терміни;
- оперативно змінювати обстановку;
- зберігати відпрацьовані документи, результати навчань, проводити порівняльний аналіз декількох навчань;
- створювати експертні системи;
- здійснювати моделювання операцій (бойових дій) для перевірки нових теоретичних положень, організаційно-штатної структури військ (сил) і визначення форм і способів їх застосування.

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

Пукач П. Я.,
завідувач кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», доктор технічних наук, професор

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

РЕКОМЕНДАЦІЇ ЩОДО ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗА ФОРС-МАЖОРНИХ ОБСТАВИН

За оцінками експертів університетів США і Великобританії не буде повного повернення освітніх процесів до чистого очного навчання навіть після закінчення пандемії, а змішане навчання стане масовим явищем. Тому дослідження і узагальнення досвіду дистанційного і з мішаного навчання є актуальними. В [1] на базі досвіду, здобутого під час роботи зі студентами очної форми підготовки в доковідний період, описувались методичні та організаційні аспекти змішаного навчання інформатики як порівняно нового для України тренду в освіті [2]. Суть такого навчання полягає в поєднанні щодо студентів очної форми підготовки елементів очного, дистанційного і самостійного навчання з послідовним нарощенням частки останніх двох компонент [3]. Навчальний процес базувався на використанні електронних навчально-методичних комплексів, створених засобами

LMS Moodle, а також авторських електронних навчальних відеоресурсів, розташованих на відеохостингу YouTube.

У 90-х роках один із авторів проходив стажування в Альбертійському університеті (Канада) у лабораторії дистанційного навчання, де отримав певний досвід використання мультимедійних технологій на кшталт Authorware Professional компанії Macromedia (тепер Adobe) щодо створення навчального відеоконтенту, новітні аналоги яких в Україні стали затребуваними тільки через 10-20 років. За останні 10 років на базі програмного забезпечення Camtasia Studio були створені для базового курсу інформатики освітні відеоресурси для підтримки очного і дистанційного навчання студентів загальнотехнічних спеціальностей [4, 5]. Підхід виявився ефективним і як скоро з'ясувалось, гостро затребуваним. Отриманий досвід дав змогу швидко і без втрат якості навчання у березні 2020 року масово перейти від змішаного до чисто дистанційного навчання, від синхронного навчання до асинхронного, від викладання до тьюторингу, від звичної аудиторної до активної самостійної позааудиторної роботи студентів з електронними ресурсами з виробленням у них навичок самоосвіти і самоконтролю за часом, місцем, маршрутами та темпом навчання. Окрім позитивних моментів у впровадженні масового дистанційного навчання були виявлено низку негативних, що дало змогу зробити деякі попередні узагальнення і сформулювати наступні рекомендації як для МОН України, так і для закладів вищої освіти щодо організації впровадження масового дистанційного і змішаного навчання, які випливають з отриманого досвіду і які виносяться на обговорення.

Варто зменшити чисельність академічних груп до 20 осіб (півгруп – до 10). В умовах змішаного навчання, де частина занять відбувається аудиторно, це дасть змогу забезпечити соціальне дистанціювання. У випадку чистого дистанційного навчання це дасть змогу забезпечити більш якісну взаємодію суб'єктів навчального процесу (викладачів і студентів), оскільки навантаження на викладачів багатьох дисциплін в умовах дистанційного навчання зростає орієнтовно на 30-50% порівняно з очним навчанням, а це потребує перегляду відповідних виробничих норм і норм оплати праці. В усіх випадках, зокрема у випадку очного навчання, це дасть змогу покращити якість навчального процесу і наблизити його до міжнародних стандартів, що вестиме до визнання вітчизняних дипломів.

Впроваджуючи технології навчання на базі LMS Moodle, edX та інших технологій, які вважаються ефективними, зокрема, для великих закладів вищої освіти, варто передбачати сегментацію (розбиття на частини) відповідних віртуальних навчальних середовищ, оскільки одночасна робота в кожному з них більше 2000 студентів веде до «зависання».

Для організації самостійної роботи студентів, які не мають змоги в домашніх умовах користуватися інтернетом, сучасними ноутбуками і ліцензованим програмним забезпеченням, надати їм відкритий доступ для до комп'ютерних лабораторій у зручний час під наглядом виключно технічного персоналу, як це реалізовано у західних університетах незалежно від обставин.

Передбачити витрати щодо забезпечення викладачів необхідними сучасними індивідуальними комп'ютерними засобами для проведення дистанційного навчання шляхом здешевлення придбання ними нової комп'ютерної техніки, передачі їм безкоштовно чи на умовах оренди або лізингу університетських засобів, в гіршому випадку тих, які підлягають апгрейту тощо.

Передбачити витрати на придбання університетами потужних серверів для підтримки дистанційного навчання з розрахунку не менше двохпроцесорної системи з 4 Гб RAM і k*1 Тб HDD на одну тисячу активних користувачів, де k = 1, 2, ...

Ввести у штатний розпис посади адміністраторів навчальних середовищ як на рівні основних підрозділів (інститутів чи факультетів), так і на рівні кафедр, які цього потребують, з метою адміністрування мережі, навчання, надання допомоги та консультування викладачів і студентів щодо створення і використання засобів дистанційного навчання.

Розробити нормативні акти та інструкції щодо скасування зберігання підзвітних матеріалів, що стосуються навчального процесу, на паперових носіях. Дозволити зберігання звітів до лабораторних робіт, розрахунково-графічних робіт, контрольних робіт, курсових робіт, залікових та екзаменаційних робіт, робочих навчальних програм, журналів обліку успішності в електронному вигляді без зайвого дублювання для чого, наприклад, у НУ «Львівська політехніка» створюються копії віртуальних навчальних середовищ за попередні роки і забезпечується відповідний доступ до них.

Висновок. Наведені рекомендації були підготовані на запит одного із інститутів АПН України і будуть опубліковані з обґрунтуваннями у журналі наукових праць цього інституту. Їх можна взяти за основу підсумків і рішень конференції після обговорення, уточнення чи доповнення.

Література:

1. Глинський Я. М., Пелех Я.М, Камінський Б. Т. Змішане навчання інформатики: 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. С. 87-90.
2. Bonk C. J., Handbook of blended learning: Global perspectives, local designs. C. J. Bonk, C. R. Graham. San Francisco, CA: Pfeiffer, 2005. pp. 3–21. URL: http://goo.gl/0LwXKV.
3. Кухаренко В. М. та ін., Теорія та практика змішаного навчання. Харків, Україна: "Міськдрук", НТУ "ХПІ", 2016.
4. *YouTube-канал*. URL: https://www.YouTube.com/results?search_query= ярославглинський.
5. Глинський Я. М., Федасюк Д. В., Ряжська В. А. Розроблення і використання електронних відеоресурсів навчального призначення: *Інформаційні технології і засоби навчання*, т. 58, №2, с. 67–78, 2017. URL: https://journal.iitta.gov.ua/index.php/itlt/article/ view/1580.

Сеник С. В.,
викладач кафедри адміністративного права та адміністративного процесу Львівського державного університету внутрішніх справ, доктор філософії

ОСНОВНІ ЗАВДАННЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

У зв'язку зі створенням Національної поліції України та розмежуванням доступу до інформаційних ресурсів між МВС України та Національною поліцією виникла необхідність у зв'язку з тим, що відповідно до ст. 25 Закону України «Про Національну поліцію» [1] інформаційні ресурси єдиної інформаційної системи, в першу чергу Інтегрованої інформаційно-пошукової системи ОВС, належать МВС України, а поліція, у межах своєї інформаційно-аналітичної діяльності, формує та використовує бази (банки) даних, що входять до цієї системи. Окрім цього, законодавець надав право Національній поліції створювати власні бази даних, які потрібні для забезпечення повсякденної діяльності органів, підрозділів, закладів і установ поліції у галузі трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, що забезпечують виконання покладених на неї повноважень. Так виникла потреба в узгоджені використання інформаційних ресурсів між МВС України та Національною поліцією.

З метою вирішення цього питання у структурі Національної поліції створено відповідні підрозділи. Департамент організаційно-аналітичного забезпечення та оперативного реагування і Департамент інформаційно-аналітичної підтримки.

Департамент організаційно-аналітичного забезпечення та оперативного реагування забезпечує і виконує у межах власної компетенції завдання Національної поліції, пов'язані із координуванням, аналізуванням, плануванням, контролем, погодженням дій міжрегіональних, територіальних, відокремлених, інших органів і структурних підрозділів поліції з питань виконання державної політики у галузі забезпечення публічної безпеки та правопорядку, охорони й захисту прав і свобод людини, інтересів суспільства та держави, протидії злочинності.

Відповідно до положення [2] основними завданнями ДОАЗОР є:

- контроль оперативної обстановки у державі в цілому та регіонах зокрема;
- проведення аналізу й узагальнення результатів діяльності Національної поліції, її ефективності, вивчення умов і причин, які сприяють учиненню адміністративних правопорушень та кримінальних злочинів, ужиття необхідних заходів щодо їх усунення;
- підготовка для управлінського апарату МВС, Національної поліції України тощо інформаційних, аналітичних чи довідкових матеріалів стосовно питань реалізації політики держави у напрямі протидії злочинності, забезпечення порядку, публічної безпеки, охорони прав і свобод людини тощо;
- організація та контроль щодо проведення реагування на повідомлення та заяви громадян про кримінальні злочини, адміністративні правопорушення тощо;
- контроль та перевірка стану дотримання нормативно-правових актів та організаційно-розпорядчих документів, виконання яких контролюється Департаментом;

- узагальнення зведень оперативного характеру та інформаційно-аналітичних документів про кримінальні злочини, адміністративні правопорушення, інші події та обмін такими даними з іншими правоохоронними структурами;
- підготовка комплексних аналітичних матеріалів про оперативну ситуацію у державі, створення проектів управлінських рішень стосовно підвищення ефективності діяльності Національної поліції з питань боротьби зі злочинністю;
- контроль та перевірка дотримання порядку реєстрації та ведення поліцією єдиного обліку повідомлень і заяв про вчинені кримінальні злочини, адміністративні правопорушення й інші події;
- проведення аналізу обліково-реєстраційної роботи апарату Національної поліції, її органів і підрозділів, контроль виконавської дисципліни, а також проведення заходів щодо своєчасного виявлення негативних тенденцій у даному напрямі діяльності та їх усунення;
- забезпечення координації органів і підрозділів Національної поліції щодо геолокаційного відслідковування за місцезнаходженням обвинувачених, інших осіб, що підозрюються у вчинені злочину, які зобов'язані в установленому законом порядку носити електронні засоби контролю;
- здійснення у межах компетенції опрацювання проектів документів організаційно-розпорядчого, нормативного-правового характеру та з питань, які включають відомості, що містять державну таємницю;
- проведення безпосереднього контролю щодо виконання органами та підрозділами доручень від органів державної влади та від керівництва Національної поліції України;
- використання баз даних МВС, Національної поліції України для вирішення завдань, які покладені на ДОАЗОР.

Департамент інформаційно-аналітичної підтримки, який вживає заходи, що спрямовуються на інформаційне, інформаційно-аналітичне та інформаційно-телекомунікаційне забезпечення діяльності Національної поліції, а також на захист персональних даних, які опрацьовуються у структурних підрозділах, інших територіальних органах та підрозділах Національної поліції України.

До основних завдань Департаменту належать:

- організація інформаційної, інформаційно-аналітичної, інформаційно-телекомунікаційної та інформаційно-пошукової діяльності поліції;
- участь у реалізації державної політики у галузі інформатизації в межах компетенції Національної поліції;
- координація діяльності управлінь інформаційно-аналітичної підтримки (або окремо визначених посад з відповідними функціями) органів і підрозділів поліції головних управлінь Національної поліції України з питань інформатизації, формування баз (банків) даних, інформаційно-пошукової та інформаційно-аналітичної роботи, а також їх підтримання в актуальному стані, у тому числі координація проведення взаємозвірень між цими базами (банками) даних та відомостями Єдиного реєстру досудових розслідувань;
- організація заходів із дотримання вимог нормативно-правових актів щодо охорони програмного забезпечення під час його отримання, установлення, використання в органах та підрозділах поліції;
- забезпечення захисту інформації, що обробляється в інформаційно-телекомунікаційних системах ДІАП, у тому числі персональних даних та іншої інформації, вимоги до захисту якої встановлені законом;
- формування, координація та супроводження інформаційних підсистем інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» [2].

Нині, в межах подальшого удосконалення інформаційно-аналітичного забезпечення діяльності Національної поліції, МВС України прийнято низку нових нормативно-правових документів, які враховують загальнодержавні пріоритети у реалізації проектів взаємодії різних органів державної влади, з метою удосконалення порядку функціонування інформаційних систем організації доступу до них та ефективній протидії правопорушенням.

Література:

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. Про затвердження Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України : наказ Національної поліції України від 27 листопада 2015 р. № 126.

3. Департамент інформаційно-аналітичної підтримки Національної поліції України. URL: http://old.npu.gov.ua/mvs/control/main/uk/publish/article/1820541

Черняховський Б. В.,
старший слідчий в особливо важливих справах Головного слідчого управління Національної поліції України, ад'юнкт кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ

Юсупов В. В.,
професор кафедри криміналістичного забезпечення та судових експертиз Навчально-наукового інституту № 2 Національної академії внутрішніх справ, доктор юридичних наук, старший науковий співробітник

ОКРЕМІ АСПЕКТИ ЗБИРАННЯ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ

Стрімка інформатизація приватного та публічного сектору громадського життя є ключовою особливістю процесу державного розвитку. Тому більша частина організаційного та спеціалізованого функціоналу підприємств, установ та організацій реалізується за допомогою комп'ютерів, комп'ютерних систем чи комп'ютерних мереж, що забезпечило формування нового плацдарму у сфері стримування та протидії кримінальному елементу соціуму.

Боротьба зі злочинам у сфері використання комп'ютерних технологій вимагає активного впровадження та застосування комплексу новітніх способів, методів і засобів для фіксації злочинів як у традиційному (матеріальному) середовищі так і в нематеріальному (цифровому).

Окремі питання розслідування кіберзлочинів є предметом дослідження провідних науковців криміналістів, зокрема: П.Д. Біленчука, В.В. Бірюкова М.В. Салтевського, В.Г. Хахановського, С.С. Чернявського, О.І. Мотляха, Ю.Ю. Орлова та ін.

Аналіз офіційних статистичних даних кібератак та кіберінцидентів у яких наявний склад злочину визначений кримінальним законодавством України вказує, що найбільш розповсюдженими є факти несанкціонованого втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж (ст. 361 КК України). [2] Протягом одинадцяти місяців 2020 року було зареєстровано 1174 кримінальні правопорушення за указаною статтею. [3] За офіційною інформацією фахівців у сфері інформатизації та зв'язку, кібератаки, у тому числі, які підпадають під санкцію ст. 361 КК України реалізуються зловмисниками для порушення конфіденційності, цілісності або доступності державних інформаційних ресурсів (чи приватних), що зберігається, обробляється та циркулює в комп'ютерній/інформаційно-телекомунікаційній системі. З цією метою, як правило, використовують вразливості таких систем, тобто їх нездатність протистояти певній загрозі або сукупності загроз [4] .

Огляд результатів практики досудового розслідування злочинів за ст. 361 КК України вказує на значущість для формування доказової бази слідчого огляду та обшуку, ефективність яких прямо впливає на якість та повноту проведення судових експертних досліджень.

Так, при пошуку слідів незаконного доступу до апаратної частини комп'ютера, комп'ютерної мережі, вагоме значення надається традиційним слідам злочинних дій, які залишились на оточуючих предметах та поверхнях, що вимагає вивчення та аналізу обстановки місця події: місця можливого підключення до дротових ліній до приміщення, стану підключень у комутуючих шафах, цілісності дверних замків, наявності слідів рук, взуття (ніг), інших частин тіла, волосся, запахових слідів у місцях фізичного контакту злочинця з елементами обстановки тощо. Слід приділити увагу наявності таких слідів злочину як: сліди рук (папілярні візерунки), сліди взуття (ніг), які залишив зловмисник при здійсненні доступу до комп'ютерного обладнання, або ж сліди зламу замків, дверей, пломб на комутуючих шафах тощо. У слідчому огляді чи обшуку на підприємствах, в організаціях, установах важливо звернути увагу на паперові документи – журнали обліку роботи з комп'ютерним устаткуванням

(якщо такі ведуться), лістинги (роздруківок текстів комп'ютерних програм), технічна, технологічна та інша документація. Важливо перевірити можливу наявність підчисток, виправлень, додаткових записів, порядку нумерації сторінок, вкладишів, розпоряджень на виконання певних програмно-технічних робіт з комп'ютерним устаткуванням чи заміні програмного забезпечення, введення додаткової інформації не передбаченої технологічним процесом, відповідність форм запису такої інформації встановленим правилам тощо [5].

Ключову роль у розслідуванні несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж відіграє пошук доказів у нематеріальному (цифровому) середовищі. Особливість полягає в тому, що предметом даного злочину виступає інформація, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації та передається через комп'ютерні мережі чи мережі електрозв'язку. Зазначені умови формують запит на забезпечення належної тактичної та спеціальної підготовки слідчих для розслідування злочинів у сфері інформаційних цифрових технологій – кіберзлочинів.

Участь спеціаліста у сфері комп'ютерних технологій за відповідним напрямом, є одним із ключових, обов'язкових факторів який необхідно врахувати і забезпечити під час обшуку комп'ютерів, комп'ютерних систем/мереж, що забезпечують функціонування інформаційної системи [6]. Адже з програмно-технічної точки зору, елементи, які входять до складу комп'ютерної системи, при дослідженні на місці, потребують максимально обережного поводження з огляду на такі фактори як великий масив інформації в електронній формі, наявність права інтелектуальної власності на окрему частину інформації, до якої здійснюється доступ, наявність прихованих даних, доступ до яких базовий користувач комп'ютера не в змозі отримати та, що найбільш суттєво, ризики втрати інформації через необережні дії та можливий запрограмований автоматичний запуск алгоритму її знищення.

Вагомим у пошуку та фіксації цифрових (електронних) доказів є дотримання принципу Міжнародного кримінального суду «правило найкращого доказу» (англ. – best evidence rule), суть якого полягає в наданні привілейованого статусу саме оригіналу документа, порівняно з його копією чи відображенням. Дотримання такого принципу залежить від використання спеціальних знань під час збирання доказів в електронній (цифровій) формі, якими володіє спеціаліст. Дана умова убезпечить від ненавмисного видалення чи пошкодження електронних (цифрових) файлів, а також, уникнення випадків запрограмованого самознищення електронних (цифрових) файлів у разі введення невірного пароля.

З огляду на зазначене, під час пошуку цифрових (електронних) доказів слідчим, з урахуванням слідчої ситуації визначаються та узгоджуються головні завдання для залученого спеціаліста, які полягають в наступному:

- діагностика апаратних засобів (комп'ютери, ноутбуки, планшети, жорсткі диски, флеш-накопичувачі, картки пам'яті, мобільні пристрої тощо);
- визначення функціонального призначення, характеристик, алгоритму роботи й структурних особливостей, стану виявленого програмного системного й прикладного забезпечення;
- пошук, виявлення, аналіз та оцінка цифрових даних, виготовлених користувачем або створених прикладними програмами для організації інформаційних процесів у комп'ютерній системі;
- ідентифікація, електронних (цифрових) файлів/каталогів, їх ототожнення файлами/каталогами на інших носіях інформації.

Варто зазначити, що вилучені об'єкти (комп'ютерне обладнання, його складові) є потенційним джерелом доказів, а будь-які непрофесійні дії з ними в подальшому можуть бути підставою втрати або ж визнання доказів недопустимими.

Ураховуючи викладене, аргументованою є позиція щодо необхідності поглибленої спеціалізованої підготовки слідчих за напрямом розслідування кіберзлочинів, яка відповідає рівню викликів сьогодення та враховує перспективу подальшого розвитку інформаційно-технологічного сектору людської діяльності.

Література:

1. Борисова Л. В. Біленчук П. Д., Малій М. І. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. Міжвідомчий науково-методичний збірник «Криміналістика і судова експертиза». 2020. № 65. С. 230-239.

2. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14.

3. Офіційний сайт Національної поліції URL: https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html

4. Сальник С.В., Сторчак А.С., Крамський А.Є. Аналіз вразливостей та атак на державні інформаційні ресурси,що обробляються в інформаційно-телекомунікаційних системах. Системи обробки інформації. 2019. N 2(157). С. 121–128.

5. Старушкевич А. Організація огляду місця події. Аналіз криміналістично-значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації: Вісник прокуратури – № 12; ред.кол. М. К. Якимчук (голов. ред.) та ін. Київ: НАПУ, 2003. – с. 77-78.

6. Яковлєв О. В. Роль прокурора–процесуального керівника досудовим розслідуванням у призначенні судової експертизи та оцінці її результатів. Криміналістика і судова експертиза: міжвідомчий науково-методичний збірник Київського НДІ судових експертиз. 2019. № 64. С. 350-360.

Романов М. Ю.,
старший слідчий з ОВС Головного слідчого управління Національної поліції України, аспірант Національної академії внутрішніх справ

ЗАСТОСУВАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ (ПЕРЕПІДГОТОВЦІ) ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ ДІЗНАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасний етап трансформації правоохоронної системи України, характеризується великою кількістю пропозицій щодо оптимізації її функціонування. Одними із нещодавно створених підрозділів, в системі правоохоронних органів є органи дізнання.

На сьогоднішній день, враховуючи попередній досвід їх функціонування, а також пропозиції учених та практиків було запущено роботу відповідного інституту, проте, в подальшому, його функціонування потребуватиме вдосконалення.

Вже сьогодні, актуальними є питання підготовки нових, перепідготовки, для подальшої роботи вже діючих співробітників, а також підвищення кваліфікації дізнавачів Національної поліції України, що в умовах стрімких інформатизаційних та діджитал процесів характеризуються науковою популярністю та широтою дискусії навколо пропозицій, щодо оптимізації у даному напрямі.

Перш за все, слід зауважити, що українська наука, тлумачить поняття дізнання по різному, проте такий плюралізм дозволяє узагальнити сформульовані висновки та звернути увагу на необхідних для вдосконалення аспектах. Визначення поняття та сутності інституту дізнавача, дозволить більш точно та якісно, сформувати комплекс необхідних заходів, що необхідно спрямувати для його теоретичної та практичної підготовки із застосуванням інформаційних освітніх технологій.

Відповідно до наказу Міністерства внутрішніх справ України від 20 травня 2020 року № 405 «Про затвердження Положення про організацію діяльності підрозділів дізнання органів Національної поліції України», завданнями підрозділів дізнання Національної поліції України є: захист особи, суспільства та держави від кримінальних проступків; охорона прав, свобод та законних інтересів учасників кримінального провадження; забезпечення швидкого, повного та неупередженого розслідування кримінальних проступків, віднесених до підслідності органів Національної поліції України; забезпечення відшкодування фізичним і юридичним особам шкоди, заподіяної кримінальними проступками; виявлення причин і умов, які сприяють учиненню кримінальних проступків, і вжиття заходів щодо їх усунення [1].

Це дає підстави вважати, що дізнавачем у Національній поліції України є процесуальна особа, яка уповноважена на розслідування кримінальних проступків, віднесених до підслідності Національної поліції України виходячи із завдань кримінального провадження. Також, у зазначеному і полягає сутність функціонування інституту дізнавача котрий за наявності в нього процесуальних повноважень, у межах визначених законом обов'язків повинен проводити процесуальні дії та приймати процесуальні рішення з метою захисту прав і свобод людини і громадянина.

Поряд із цим, для виконання покладених на відповідних осіб повноважень, вітчизняна система освіти має забезпечити ефективну підготовку фахівців та створити дієву систему перекваліфікації

поліцейських кадрів для роботи в підрозділах дізнання, а також підвищення кваліфікації вже діючих дізнавачів Національної поліції України. Визначені завдання, перш за все та найбільш ефективно можуть бути вирішені за умови використання інформаційних технологій.

На думку ряду учених, інформаційними технологіями в освіті є комплекс навчальних і навчально-методичних матеріалів, технічних та інструментальних засобів, техніки навчального призначення, а також система наукових знань про форми і методи їх застосування для вдосконалення праці викладачів та студентів [2].

Питання застосування та розробки відповідних технологій, неодноразово ставали предметом наукових дискусій багатьох вітчизняних учених, що дає підстави стверджувати про актуальність та багатогранність зазначеної тематики.

Одним із ключових пріоритетів ЮНЕСКО у галузі освіти є допомога у виробленні стратегії і реалізації політики інформатизації освіти. У розробленому цією міжнародною організацією «Керівництві для вимірювальних інформаційних і комунікаційних технологій (ІКТ) в освіті» [3] виділено такі принципи з інформатизації країн світу: 1. Глобальні проблеми освіти, зокрема, завдання «Освіти для всіх» (ОДВ), особливо великі в країнах, що розвиваються. Тому розвиток методології показників ІКТ в освіті неминуче вимагає більшої уваги до основних політичних проблем у цих країнах. 2. Слід збалансовано застосовувати старі і нові технології. Передачі по радіо і телебаченню в ефірі та іншими способами, як і відео-технології, продовжують вважаються дієвими і ефективними засобами навчання поряд з інтерактивним комп'ютерним та пов’язаним з Інтернет віртуальним навчанням або дистанційною освітою в діалоговому режимі. 3. Рішення міжнародних завдань у галузі освіти до 2015 р. потребують великих капіталовкладень у навчальні заклади, де готують вчителів (UNESCO-UIS, 2006b). На думку експертів, основна проблема тут полягає в тому, що при звичайному очному навчанні це завдання не буде вирішене. Потреба у перегляді навчальних планів також вимагає постійного підвищення кваліфікації вчителів, і в цьому випадку підтримка ІКТ може зіграти основну роль. 4. Без дистанційного або віртуального типу навчання потреба у вищій освіті не може бути задоволена ні в розвинених країнах, ні в країнах, що розвиваються. 5. Без віртуальних класів, віртуальних лабораторій і т.п. не можуть бути задоволені потреби професійної підготовки. 6. Цілі в галузі освіти не можуть бути досягнуті без належної уваги до гендерних проблем.

Зазначене, додатково аргументує важливість та своєчасність окресленої автором проблематики, оскільки використання інформаційних технологій не тільки у навчанні, а й в практичній діяльності органів правопорядку, а навпроти – злочинцями, у злочинній діяльності, стало реалією сьогодення.

Одним із найбільш успішних, на нашу думку прикладів застосування інноваційних цифрових технологій у навчанні поліцейських загалом є досвід розробки та впровадження у використання фахівцями та науково-педагогічними працівниками Дніпропетровського державного університету внутрішніх справ інформаційно-технічної платформи, що покладена у основу проекту «Лінія-102».

Як підкреслюють розробники «В рамках проекту реалізовано повний замкнутий цикл відпрацювання навчальних фабул від отримання первинної інформації про правопорушення до винесення судом відповідного вироку. Безумовною перевагою проекту є його практична спрямованість. За сучасною методикою рольової гри курсанти, студенти та працівники Національної поліції України набувають практичних навичок, вивчають та поглиблюють теоретичний матеріал. Максимальна наочність та наближеність до реальних умов підвищує їх мотивацію до навчання здобувачів вищої освіти, сприяє підготовці мотивованого педагога із нестандартним творчим мисленням» [4].

Зазначене вище, публічно демонструє ефективність та виправданість застосування інноваційних цифрових технологій у практичному навчанні поліцейських. Окремим питанням у даному контексті постає застосування вже розробленого алгоритму навчання, до необхідних на сьогоднішній день процесів, відносно кандидатів на посади дізнавачів (з числа діючих співробітників, а також інших осіб) та діючих працівників підрозділів дізнання Національної поліції України (з метою підвищення їх кваліфікації).

На підставі проаналізованих матеріалів на нашу думку, серед найбільш ефективних та можливих засобів у контексті здійснення освітньої діяльності відносно діючих дізнавачів та кандидатів на відповідні посади є такі:

- можливість створення програмного забезпечення, що дозволить відпрацьовувати правильність та швидкість внесення інформації про кримінальні проступки до Єдиного реєстру досудових розслідувань;

- можливість створення інформаційних систем зі створення процесуальних документів у конкретному кримінальному провадженні, що дозволяють застосовувати вже внесену шаблонну інформацію, під час створення ланцюгів, відповідних документів (наприклад, після внесення у відповідну програму інформації, щодо посади дізнавача, його спеціального звання та інших необхідних даних, наприклад фабули про учинення кримінального проступку, зазначені дані, автоматично відображались би у будь-якому новоствореному процесуальному документі, у визначеному програмним забезпеченням місці (у відповідності до Кримінального процесуального кодексу України) з метою більш ефективного навчання дізнавачів, що дасть змогу наочно продемонструвати взаємопов'язаність різних процесуальних документів у одному кримінальному провадженні;
- необхідність інтеграції інформаційних програм «Moodle», «Microsoft Teams», «Zoom» та інших, у процес навчання, а зокрема, підвищення кваліфікації та перепідготовки діючих співробітників поліції для подальшого проходження ними служби у підрозділах дізнання;
- необхідність розробки інтерактивних цифрових навчальних практикумів зі складання процесуальних документів із передбаченням можливості використання відповідного забезпечення на мобільних платформах (Apple, Android);
- необхідність розробки та втілення у життя постійно діючих, інформаційно-довідкових порталів, що забезпечать можливість у режимі реального часу, будь-якому здобувачу вищої освіти, а у окремих випадках, діючому дізнавачу чи кандидату на посаду переглянути найбільш важливі для навчання/роботи довідкові матеріали чи у разі необхідності, терміново скачати бланк конкретного процесуального документу.

Література:

1. Наказ Міністерства внутрішніх справ України від 20 травня 2020 року № 405 «Про затвердження Положення про організацію діяльності підрозділів дізнання органів Національної поліції України» – [електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/laws/show/z0491-20#Text

2. Любович А. А. Сучасні інформаційні технології в освіті / А. А. Любович, 0. Г. Єсіна // Інформатика та інформаційні технології : студ. наук. конф., 20 квітня 2015 р. : матер. конф. — Одеса, ОНЕУ. — С. 118-120.

3. Guide to measuring in formation and communication technologies (ict) in education. – UNESCO-UIS, 2009. – 138р.[Електронний ресурс]. – Режим доступу: http://unesdoc.unesco.org/images/0018/001865/186547e.pdf

4. Рижков Е. В. Вдосконалення навчального процесу з урахуванням сучасних тенденцій інформатизації структурних підрозділів національної поліції / Е. В. Рижков // Використання сучасних інформаційних технологій в діяльності національної поліції України: матеріали всеукр. наук.-практ. семінару (24 листопада 2017 року, м. Дніпро). – Дніпро: ДДУВС, 2017. – С. 9-11.

Світличний В. А.,
доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФРАЗВУКОВОЇ НЕСМЕРТЕЛЬНОЇ ЗБРОЇ LRAD І "ШЕПІТ"

Постановка проблеми. Звукові частоти викликають в людях почуття страху і паніку, інші - зупиняють серце. Частота ж між 7 і 8 Гц взагалі надзвичайно небезпечна. Теоретично, такий, досить потужний, звук може розірвати всі внутрішні органи. 7 Гц - також середня частота альфа-ритмів мозку. Чи може такий інфразвук викликати епілептичні припадки, як вважають деякі дослідники - неясно. Експерименти дають суперечливі результати. Тому, незважаючи на цілком реальні результати, ця тема часто є приводом для інформаційних спекуляцій, фейків і інших малоприємних речей, (загуглить "коричнева нота", "частота смерті" і т. і.). Складно сказати точно, коли починається історія використання звуку в якості зброї. Бойові барабани відомі у багатьох народів, а з появою вогнепальної зброї аж до кінця 19-го століття гучний звук пострілу вважався його гідністю.

Виклад основного матеріалу. Якщо говорити про перших відомих спробах створити специфічне звукове зброя, то слід згадати відомий факт того, що в 1940 році німці задумали підкинути англійцям безліч

спеціальних копій грамплатівок з записами популярних виконавців, але з добавкою інфразвуку. План полягав у тому, щоб викликати у слухачів сум'яття, почуття страху і інші психічні розлади. Німецькі військові випустили з виду, що грамофони тих років практично не могли ці частоти відтворити. Однак тема виявилася затребуваною і перший реальних пристрій - інфразвукову зброю, створили саме німці підчас другої світової війни. Йдеться про акустичну гармату доктора Річарда Валлаушека, яка була випробувана у 1944-му році. Гармата Валлаушека не була доведена до серійного виробництва, але його ідеї знайшли продовження в США, де були розроблені так звані звукові прожектори.

Найбільш успішним, що серійно випускається і часто згадуються в ЗМІ зброєю цього типу є LRAD (англ. LongRangeAcousticDevice) – вузько спрямований, потужний акустичний випромінювач, розроблений компанією American Technology Corporationв 2000-му році. Пристрій був розроблений командою інженерів під керівництвом конструктора нелетальної зброї, відомого винахідника і керівника компанії ВуддиНорiса (ElwoodNorris).

Спочатку пристрій позиціонувалася як засіб розгону демонстрацій. Надалі його функціонал розширили і визнали ефективним в якості захисту від нападу терористів, піратів, допоміжний засіб при веденні бою в міських поселеннях і як засіб приборкання агресивно налаштованого натовпу.

У зброї, як зрозуміло з назви, застосовується ураження цілі силою звуку. Так робочий звуковий тиск (SPL) різних моделей LRAD на дистанції ураження становить від 136 до 162 дБ. В якості порівняння часто призводять SPL шуму від працюючих двигунів пасажирського лайнера, що становить 120 дБ, або SPL при якому пошкоджуються барабанні перетинки-130 дБ.

Діапазон робочих частот, які були обрані для вражаючого звукового сигналу, становить від 2,1 до 3,1 кГц. Найчастіше застосовується частота 2,5 кГц, при цьому гучномовець здатний створювати звуковий промінь від 30-60°, що дозволяє вибірково використовувати систему. Також LRAD можна застосовувати в якості банальних гучномовців, які використовуються для сповіщень. LRAD надає як психологічну, так і соматичну дію. Ураження пристроєм може викликати: відчуття страху, психоемоційну дестабілізацію мети, гострий біль у вухах, майже гарантоване пошкодження барабанної перетинки, дезорієнтацію, запаморочення, відчуття нудоти, аж до блювоти. У людей з лабільною психікою можуть розвитися панічні атаки.

Було розроблено кілька варіантів LRAD з різними маса-габаритними характеристиками, потужністю і дальністю ураження. Гуманні противники зброї стверджують, що потужні модифікації LRAD здатні пошкоджувати внутрішні органи. Ними також стверджується, що вплив LRAD може бути летальним.

Такі висновки робляться на основі досліджень, в яких проводилися досліди над тваринами. Але справа в тому, що в цих дослідженнях ефективно впливали на внутрішні органи хвилі поза чутного спектру. Наприклад, ультразвук високої інтенсивності (в діапазоні від 700 кГц до 3,6 МГц) викликав пошкодження кишечника і легенів у мишей. Також відомо, що після віброакустичної стимуляції у тварин виникали аритмії, тріпотіння передсердь і брадикардія.

За час свого існування LRAD був неодноразово застосований в поліцейських і військових (Ірак, Афганістан, Сирія) операціях, найбільш відомими користувачами є армія і поліція США, ФБР, американські приватні військові компанії, ВМФ Сінгапуру, Поліція Грузії, Берегова охорона В'єтнаму, Берегова охорона Японії , ВМС Сенегалу, Того і Кот-д'Івуара і ін. Одним з найвідоміших випадків успішного застосування LRAD є відбиття атаки сомалійських піратів на круїзний лайнер SeabournSpirit в 2005-му році. У 2007-му LRAD активно застосовувала грузинська поліція проти демонстрантів в Тбілісі. Останні відомі випадки використовування LRAD здійснила американська поліція у місті Рочестер, штат Нью-Йорк 12 та 16 вересня 2020 року під час протестів перед будинком мерії Рочестера.

З впливом інфразвуку пов'язано найбільше міфів, проте це не означає, що його не можна використовувати в якості зброї. Ефекти хвиль низької частоти головним чином психологічні. З інфразвуком пов'язують посилення емоцій і формування почуття страху.

Також відомо, що, згідно з дослідженнями NASA, коливання з частотою 19 Гц, джерелом яких є двигуни ракети, впливають на очні яблука і здатні викликати розлади зору у астронавтів, в тому числі формувати різного роду бачення.

Існує також думка, що інфразвук (так само як і ультразвук) здатний руйнівно впливати на внутрішні органи людини резонансними частотами. Ця гіпотеза була частково спростована вченими Американського інституту ультразвуку в медицині (AIUM).

Їх дослідження показали, що не зафіксовано доведених біологічних ефектів, пов'язаних з несфокусованого звуковим пучком з інтенсивністю нижче 100 мВт /см² SPTA або сфокусованими звуковими пучками нижче рівня інтенсивності 1 Вт / см² SPTA. Це стосується як інфразвуку з ультразвуком, так і чутного спектру.

На ефекті інфразвуку засновано сучасну російську нелетальну зброю, названу "Шепіт". Пристрій являє собою щит співробітника правоохоронних органів, з вмонтованим в нього випромінювачем інфразвукових коливань.

Пристрій був розроблений в 2014-му році і в 2015-му надійшов на озброєння поліції. Де проходила розробка пристрою невідомо, але ще 2015-му були опубліковані деякі його технічні характеристики. Так відомо, що "Шепіт" генерує звукові коливання від двох випромінювачів, які утворюють нелінійно-параметричну область інфразвукового впливу. Про частоту коливань не сказано, але відомо, що це інфразвук. Середня величина акустичного тиску, яке здатний створювати "Шепіт" на відстані 10 м, становить 120 дБ, час роботи пристрою від акумулятора досягає 50 хвилин, час безперервного випромінювання - 30 секунд, а інтервал між періодами впливу-15 секунд. Даних про бойовий і експериментальному застосуванні пристрою в відкритих джерелах немає.

Висновки. На відміну від поширених міфів звукова зброя не підриває голови. Зброя не налаштована на "частоту смерті" і не здатна викликати мимовільний акт дефекації. При цьому дослідження, які ведуться в цій галузі, як видно, привели до відчутних результатів. Деякі існуючі зразки вже випускаються серійно і масово використовуються поліцією і військовими. Таким чином, акустична зброя може бути віднесена до перспективних ефективних видів несмертельної зброї майбутнього.

Василенко О. В.,
професор кафедри правничої лінгвістики Національної академії внутрішніх справ,
кандидат педагогічних наук, доцент

ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ АСПЕКТИ ДИСТАНЦІЙНОГО НАВЧАННЯ МАЙБУТНІХ ФАХІВЦІВ

Перехід до інформаційного суспільства та пов’язані з цим економічні, політичні і соціальні зміни вимагають розширення доступу до освітньої і професійної підготовки всіх, хто цього потребує. З огляду на це, сучасне реформування освітньої системи відбувається за рахунок становлення і розвитку дистанційного навчання. Під дистанційним навчанням розуміють індивідуалізований процес набуття знань, умінь, навичок і способів пізнавальної діяльності фахівцем, який відбувається за опосередкованої взаємодії віддалених один від одного учасників навчального процесу у спеціалізованому середовищі, що функціонує на базі новітніх психолого-педагогічних та інформаційно-комунікативних технологій.

Як невід’ємна складова неперервної освіти дистанційне навчання дозволяє вирішувати завдання підготовки, перепідготовки, підвищення й удосконалення існуючої кваліфікації фахівців будь-якої галузі в системі вищої і післядипломної освіти. Дана форма навчання, окрім швидкого реагування на розвиток технологій і виклики швидкозмінного інформаційного суспільства, створює можливість і мотивує сучасного фахівця до постійного саморозвитку, самовдосконалення протягом всього життя.

Виділяють три інтегрованих фактори впливу на дистанційне навчання: технологічний, педагогічний і організаційний [4, с. 89]. Перший фактор пов’язаний з інформаційними технологіями, що використовуються для розробки, доставки, підтримки навчальних курсів і навчального процесу в цілому. Значення другого фактору визначається набором методів і прийомів, що використовуються в ході навчального процесу. Третій фактор, організаційний, характеризує специфіку організаційної структури дистанційного навчання. Ідеальна модель дистанційного навчання включає в себе інтегровану навчальну середу, з варіантним визначенням ролі різних компонентів – технологічних, педагогічних, організаційно-методичних.

Характерною особливістю дистанційного навчання є використання всіх видів інформаційних технологій, але переважно комп’ютерних і телекомунікаційних технологій, засобами яких є комп’ютери, комп’ютерні мережі, мультимедійні системи і т. ін. Нові електронні технології, доступні через глобальну мережу Інтернет, сприяють активному залученню студентів у навчальний процес, а також дозволяють управляти цим процесом, на відміну від більшості традиційних навчальних технологій [3].

При тому технічна реалізація дистанційного навчання по суті вторинна. Первинним у дистанційному навчанні є кваліфікація викладачів, якість навчально-методичних матеріалів і власне методика навчання [1]. Ефективність і успіх дистанційного навчання залежить від організації та методичної якості використовуваних матеріалів, а також того, наскільки враховані особливості подання інформації, рівня підготовки педагогів, що беруть участь в цьому процесі, і наскільки вони розуміють особливості надання та сприйняття інформації в рамках сучасних віртуальних комунікацій. Проте, методика дистанційного навчання не обмежується вирішенням питань «чому вчити і як вчити», а передбачає, перш за все, вирішення питання «як вчитися».

Тобто, основу освітнього процесу при дистанційному навчанні складає цілеспрямована і контрольована інтенсивна самостійна робота студента, який може вчитися у зручному для себе місці, за індивідуальним розкладом, маючи при собі комплект спеціальних засобів навчання і узгоджену можливість контакту з керівником та іншими студентами он-лайн або очно [2].

Виходячи з зазначеного, головним є організація навчальної роботи студентів із самодостатнім навчально-методичним забезпеченням незалежно від того, на яких носіях воно знаходиться – паперових, мультимедійних, або отримується у інтерактивному режимі з телекомунікаційної мережі. Відтоді можливість оптимізації навчання майбутніх фахівців на відстані пов'язана, насамперед, з активізацією самостійної роботи студентів, підвищенням її ефективності та якості.

Інформаційно-комунікативні технології дозволяють отримувати первинну інформацію не тільки від викладача, а й з допомогою інтерактивних навчальних програм, які допомагають учню при певному ступені компетентності засвоїти ту чи іншу дисципліну. Маючи необмежені можливості для отримання інформації, студент в процесі самостійної роботи може будь-коли звернутися за консультацією до різних навчально-пізнавальних джерел. Крім того, комп'ютер дозволяє постійно проводити різні форми самоконтролю, що підвищує мотивацію пізнавальної діяльності і творчий рівень навчання.

При дистанційному навчанні фахівців значно підвищується вимога до володіння студентами навичками навчальної роботи та роботи з джерелами інформації. За словами С. Сисоєвої, «вчитися ефективно за такою формою навчання можуть тільки люди з певними сформованими навичками самоосвіти і стійкою мотивацією щодо учіння» [2, с. 81]. До навичок та умінь, необхідних для планування і здійснення самостійного навчання студентів, відносяться наступні [1]:

- система знань, умінь, навичок що відображають міру інтелектуального розвитку особистості, або гностичні вміння: спеціальні знання, уміння, навички з конкретної дисципліни; вміння встановлювати внутрішні та міжпредметні зв'язки стосовно різних наукових понять, методів тощо; вміння аналізувати, синтезувати і узагальнювати факти і явища; гнучкість розумової діяльність, усвідомленість, стійкість і самостійність мислення; критичність, раціональність і темп мислення; увага, пам'ять, спостережливість і т. ін.
- узагальнені вміння працювати з основними джерелами інформації, а саме: характер орієнтування у різноманітних об'єктах інформації; психологічна готовність правильно оцінити функціональні можливості окремого чи сукупності джерел, вибрати доцільні засоби для пошуку і засвоєння інформації; культура сприйняття інформації з джерел; культура засвоєння інформації; вміння використовувати джерело інформації при самоконтролі та самооцінці якості навчання; темп читання тощо.
- організаційно-управлінські вміння, або вміння самоорганізації пізнавальної діяльності: вміння визначати і виконувати навчальні завдання, основні шляхи пошуку та засвоєння матеріалу; навички планування навчальної праці, розподілення зусиль і часу; уміння та навички самоконтролю, самоаналізу, самооцінки результатів навчальної діяльності; систематичність, послідовність у навчанні та ін.

Слід зауважити, що у системі дистанційної підготовки майбутніх фахівців суттєво змінюється роль і місце викладача у педагогічній взаємодії зі студентом: викладач виступає координатором, який не тільки організує і здійснює педагогічну взаємодію з тим, хто навчається, за допомогою інформаційних технологій, а й здійснює управління його навчально-пізнавальною діяльністю в індивідуальному режимі, його консультування і оцінювання навчальної діяльності [2]. Хоча роль викладача при цьому зводиться до управління навчальним процесом, але його вплив на пізнавальну діяльність студента не зменшується, а відповідальність збільшується. Перед викладачем стоїть завдання управління навчанням студентів шляхом формування мотивів діяльності, постановки

кінцевої та проміжних цілей, окреслення необхідної для досягнення цілей інформації і видів навчальної діяльності тощо.

Таким чином, у наш час дистанційна форма навчання стає все більш актуальною як для майбутніх фахівців, які здобувають вищу або додаткову освіту, так і для кваліфікованих фахівців, які хочуть удосконалити свої професійні знання і навички. Також необхідно розуміти, що дистанційне навчання являє собою не електронний варіант очного або заочного навчання, адаптуючи традиційні форми занять і паперові засоби навчання в телекомунікаційні. Дистанційне навчання покликане вирішувати специфічні завдання, що відносяться до розвитку творчої складової освіти та ускладнені для досягнення в звичайному навчанні.

Введення в навчальний процес технологій дистанційного навчання є надзвичайно важливим і допомагає вирішувати проблеми, такі як: оперативне використання новітніх знань; підвищення інформаційної забезпеченості навчального процесу; вільний доступ до спілкування з видатними вченими і досвідченими фахівцями певної галузі, підвищення мотивації та самоорганізації навчальної діяльності тих, хто навчається, тощо. Тому в сучасних умовах підготовки фахівців з використанням дистанційного навчання актуальним є, серед іншого, удосконалення змісту, методів, форм організації навчальної діяльності студентів, способів аналізу і корекції її результатів відповідно до нових дистанційних технологій.

Література:

1. Сериков Г. Н. Самообразование: Совершенствование подготовки студентов. Иркутск.: Изд-во Иркут. ун-та. 1991. 232 с.

2. Сисоєва С. О. Проблеми дистанційного навчання: педагогічний аспект. *Неперервна професійна освіта: теорія і практика: наук-метод журнал.* 2003. Вип. 3-4. С. 78-87.

3. Шуневич Б. Теоретичні основи дистанційного навчання: Навч. посібник. Львів: Видавництво Національного університету «Львівська політехніка», 2006. 244 с.

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

ІНФОРМАЦІЙНА КУЛЬТУРА У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ

Як відомо існують безліч факторів, що впливають на формування суспільної, групової та індивідуальної правосвідомість. Ці фактори являють собою систему, основними компонентами якої є різні соціальні сфери: економічна, правова, політична, моральна, інформаційна та ін. Безперечно, основою становлення інформаційного суспільства є розвиток інформаційної сфери та її інтеграція в інші сфери соціального життя.

Інформаційна сфера як елемент системи факторів, що впливають на правову свідомість в сучасних умовах, має визначальне значення у формуванні правосвідомості, особливо правоохоронця та поліцейського. Вплив інформаційної сфери на формування професійної правосвідомості правоохоронця виражається у впливі зовнішніх факторів та в умовах становлення самого інформаційного суспільства має мотиваційне спрямування.

Безперечно, що потрібно зважати на врахування принципу відповідності мінливих умов життя суспільства при організації процесу правового виховання правоохоронця, а також формувати його відносити та поведінку згідно загальноправовим принципам.

Здійснення в правоохоронній діяльності інформаційно-правового виховання, є засобом формування культури сприйняття інформації щодо правової дійсності, а також є деонтологічним процесом формування правосвідомості як продукту такого сприйняття за допомогою використання інформаційно-комунікаційних технологій.

Система факторів, що впливають на формування правосвідомості, а отже й внутрішнього імперативу, складається з підсистем, в якості яких виступають різні сфери суспільного життя: економічна, політична, правова, соціальна, наукова, релігійна та інші, в тому числі інформаційна, роль та вплив й значення, якої в сучасних умовах розвитку держави зростає.

Кожна з суспільних сфер складається з п'яти основних комплексів: нормативного, інституційного, комунікативного, функціонального, ідеологічного, що в свою чергу є наповненням інформаційної культури особи.

На правосвідомість правоохоронця впливають всі ці фактори, в тому числі зовнішні, що утворюють середовище діяльності даних органів, а також внутрішні, що відносяться до їх організації та функціонування.

Результатом функціонування системи таких факторів, що впливають на правосвідомість особи, є формування правосвідомості всіх суб'єктів права, у тому числі правоохоронців. Під формуванням професійної правосвідомості правоохоронця мається на увазі отримання і закріплення ними професійних знань, умінь, навичок, стереотипів правомірної поведінки, внутрішньої згоди (солідарності) з правовими принципами і нормами.

Становлення інформаційного суспільства - це процес, пов'язаний з посиленням в суспільстві ролі інформації та знань. Він заснований на інтеграції в усі сфери соціального життя інформаційно-комунікаційних технологій, що формують нову інформаційну інфраструктуру, розширюють можливості при оперуванні з інформаційними ресурсами, в результаті чого змінюється характер суспільних відносин і, як наслідок - суспільна свідомість (й безпосередньо професійна свідомість правоохоронця).

Основою цього процесу є розвиток інформаційної сфери, її проникнення в інші сфери життя суспільства. Тому, в таких інформаційних умовах істотно змінюється організація правоохоронної діяльності завдяки застосуванню нових засобів і способів збору, обробки, зберігання і використання інформації, що має значення для ефективного вирішення різних службових завдань та безпеки суспільства.

Вплив інформаційної сфери, яка постійно розвивається та є викликом сучасності (адже зараз не можливо уявити жодної сфери діяльності людини, де б не використовувалися певні інформаційні технології), на професійну правосвідомість правоохоронців виражається у впливі як зовнішніх інформаційних факторів (інформаційна сфера суспільства), так і внутрішніх (інформаційна сфера самих підрозділів, колективів, служб, органів), в тому числі пов'язаних з впровадженням в діяльність даних органів нових інформаційно-комунікаційних технологій.

При здійсненні правового виховання правоохоронців, а отже й впровадження інформаційної культури зокрема, доцільно дотримуватися принципу відповідності мінливих умов життя і розвитку суспільства, тобто враховувати соціальні зміни і використовувати нові досягнення, і в першу чергу в інформаційній сфері.

Даний принцип важливий не тільки в правовому вихованні та культурі, а й може бути представлений в якості загальноправового принципу, оскільки позитивне право повинно відображати реалії суспільного життя і змінюватися відповідно до відбуваються в суспільстві процесами.

Системно-правове виховання правоохоронної діяльності та самих правоохоронців - це робота, яка передбачає здійснення комплексу заходів, спрямованих на формування професійної правосвідомості особи з урахуванням системного впливу різних факторів, серед яких інформаційна культура займає одне з головних місць під час виховання та освоєння навиків роботи з інформаційними технологіями в своїй професійній діяльності.

Найважливішою частиною такої роботи є інформаційно-правове виховання, що передбачає формування установок на адекватне сприйняття фахівцями (поліцейськими) інформації про правову дійсність, її сортування, відбір і вироблення правильного та правового ставлення до неї на основі критичного мислення відповідно до існуючих в суспільстві правових і моральних цінностей, традицій, ідеалів, а також робота з формування умінь і навичок з пошуку, аналізу та використання правової інформації за допомогою сучасних інформаційних технологій, в тому числі із застосуванням інформаційно-комунікаційних засобів.

Література:

1. Бєляков К.І., Онупрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір. Монографія.: за заг. ред. К. І. Бєлякова. К.: КВІЦ, 2018. 169 с.

2. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: РНБО, Рішеня від 28.04.2014. Офіційний сайт ВРУ: URL: https://zakon.rada.gov.ua/laws/show/n0004525-14#Text (дата звернення: 01.09.2020).

3. Прудникова О.В. Філософія інформаційної культури: навч. посіб. Харків: право, 2017. 328 с.

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

Філімонов С. М.,
старший викладач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

ОПЕРАТИВНЕ УПРАВЛІННЯ ЕКСПЛУАТАЦІЄЮ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ В УМОВАХ НАВЧАЛЬНОГО ПРОЦЕСУ ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Оптимізувати процес експлуатації бойової техніки на протязі навчального процесу в Національній академії сухопутних військ і в такий спосіб зменшити витрати паливно-мастильних матеріалів, боєприпасів, імітаційної техніки та решти експлуатаційних матеріалів дозволить побудова динамічної інформаційної бази знань етапу «Використання за призначенням» системи експлуатації озброєння та військової техніки (ОВТ).

Для вирішення поставленої задачі оперативного управління експлуатацією ОВТ в умовах навчального процесу ВВНЗ необхідно розробити методичні, алгоритмічні та програмні засоби, які дозволять реалізувати комп'ютеризовану систему контролю й управління процесом експлуатації озброєння та військової техніки.

Вирішення задачі прийняття рішення у проблемно-орієнтованій автоматизованій системі контролю й управління процесом експлуатації ОВТ в умовах апріорної невизначеності обумовлює необхідність побудови:

- багатоагентної моделі системи зі схемою адаптивного пошуку;
- розробка модифікованого генетичного алгоритму;
- інтеграція алгоритмів генетичного та адаптивного пошуку – побудова гібридного алгоритму.

В якості загальної архітектури обрана модель анімата на основі навчання з підкріплення, розроблена в контексті дослідження адаптивної поведінки штучних агентів.

На практиці виконання вимог визначає експерт у лінгвістичній формі. Тому пропонується використати можливості апарата лінгвістичних змінних та нечітких множин та вводяться допоміжні лінгвістичні змінні, відповідно до задач управління ОВТ.

Пропонується варіант «зовнішньої» гібридизації. Гібридний алгоритм поєднує підходи адаптивного та генетичного пошуку в рамках єдиного оптимізаційного процесу.

Основна ідея гібридизації полягає в можливості обміну розв'язаннями, які отримані модифікованим генетичним та алгоритмом адаптивного пошуку окремо в ході пошукового процесу. Для генетичного алгоритму розв'язання, отримане від алгоритму адаптивного пошуку, служить додатковим генетичним матеріалом для генерації «якісних» індивідів.

Аналогічна ситуація для адаптивного пошуку, кращий індивід, отриманий в ході генетичного пошуку, може бути додатково покращена за рахунок застосування експертних правил, які закладені в механізмі адаптації.

Запропонований алгоритм може бути застосований в умовах здійснення паралельних обчислень, архітектура сучасних процесорів є багатоядерною, що в свою чергу дає можливість ведення паралельних та розподілених обчислень.

Таким чином, логіка гібридного алгоритму передбачає варіант, при якому здійснюється одночасний розрахунок рішень в модифікованому генетичному алгоритмі та алгоритмі адаптивного пошуку та обмін отриманими рішеннями в рамках однієї розрахункової ітерації гібридного алгоритму. Використання методів керування системами з вбудованими елементами штучного інтелекту в умовах невизначеності для управління процесом експлуатації ОВТ в вищому військовому закладі дозволяє побудувати індивідуальну траєкторію оптимального використання за призначенням військової техніки.

Гаврильців М. Т.,
доцент кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ кандидат юридичних наук, доцент

ПРАВОВІ ПРИНЦИПИ ОТРИМАННЯ ІНФОРМАЦІЇ ОРГАНАМИ ДЕРЖАВНОЇ ВЛАДИ В УКРАЇНІ

Правова регламентація формування єдиного інформаційного простору України повинна сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та засобів інформаційного виробництва в країні у процесі її руху до інформаційного суспільства. Відносини щодо отримання органами влади інформації є частиною відносин, що виникають із приводу доступу до інформації.

Дослідники проблематики галузі інформаційного права основними принципами доступу до інформації вважають: презумпцію доступності і відкритості інформації; достовірність і повноту інформації; своєчасність надання інформації; дотримання обмежень, встановлених законом; захист права на доступ до інформації; відповідальність за порушення права на доступ до інформації [1, с. 195].

Проаналізуємо ці принципи з огляду на можливість органами державної влади отримувати інформацію. По-перше, термін *«презумпція»* у цьому випадку не зовсім коректний, оскільки не має належного науково-теоретичного обґрунтування. По-друге, принцип доступності й відкритості інформації полягає в тому, що будь-яка інформація є відкритою і до неї має забезпечуватися доступ до того моменту, коли можливість отримати (ознайомитися з) таку інформацію не буде обмежена на законних підставах і у спосіб, передбачений законом. Так реалізується конституційне положення про винятковий характер обмеження права на інформацію.

Принцип *відкритості* обґрунтовують і вітчизняні дослідники, які зазначають, що «відкритий і безперешкодний доступ до суспільно значущої інформації гарантує ефективне управління і вільний розвиток суспільства, сприяє освіті громадян, стимулює прогрес і допомагає вирішенню складних економічних, наукових і соціальних проблем» [2, с. 5].

Однак, принцип *доступності й відкритості* інформації актуальний для доступу фізичних осіб до інформації і не поширюється на отримання органами державної влади відомостей, що належать фізичним і юридичним особам приватного права. Адже ключовим для регулювання таких відносин є передбаченість законом можливості органів державної влади отримати інформацію.

Достовірність і повнота інформації, яка надається органам державної влади, є актуальним принципом регулювання відповідних суспільних відносин. Науковці акцентують увагу на дотриманні достовірності та інших вимог до якості інформації: повнота, своєчасність, регулярність, комплексність [3, с. 23].

При отриманні органами державної влади інформації особливо важливими є використання принципів достовірності (вірогідності, об'єктивності, точності, правдивості) інформації. Вважаємо, достовірність (вірогідність, об'єктивність, точність, правдивість) інформації є необхідним елементом регулювання інформаційних відносин. Цей принцип полягає у відсутності спотворення змісту інформації і може бути підставою для накладення на органи державної влади додаткових повноважень у тих випадках, коли поширюється неправдива (недостовірна, необ'єктивна) інформація [4, с. 24-25].

Повнота отримання інформації означає, що органи державної влади отримують увесь обсяг інформації, яку вони потребують (запитують). Гарантією реалізації цього принципу є встановлення юридичної відповідальності за порушення прав чи обов'язків органів державної влади на отримання інформації.

Передумовою для належного врегулювання суспільних відносин із приводу отримання органами державної влади інформації є встановлення чітких термінів отримання інформації, котрі мають важливе значення при реалізації органами державної влади своїх повноважень. Потрібно виокремити такий принцип регулювання відповідних відносин, як своєчасність отримання органами державної влади інформації. Цей принцип передбачає отримання інформації чітко відповідно до термінів, передбачених законодавством або договором.

Загальний принцип регулювання відносин щодо доступу до інформації – *дотримання обмежень, встановлених законом*, варто детально проаналізувати для відносин, які предметом дослідження. Принцип обмеження доступу до інформації виключно на підставі закону стосується усієї

інформації (такої, що належить державі, і що є власністю приватних суб'єктів). Однак реалізація цього принципу відрізняється залежно від власника інформації. Для органів державної влади має бути не лише передбачене обмеження доступу до інформації, але й закріплено перелік категорій таких відомостей (як державна таємниця), визначено порядок поводження із такими відомостями, повноваження суб'єктів тощо [4, с. 25–26].

Особливі правові характеристики має *конфіденційна інформація про особу*. З урахуванням конституційного положення про те, що збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, формулюємо принцип: отримання органами державної влади інформації про особисте життя за згодою фізичної особи. Винятком із цього загального правила можуть бути випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Усім учасникам інформаційних відносин держава забезпечує рівні права і можливості отримання інформації, якщо тільки така інформація не є таємною. З урахуванням того, що крім таємної, існує й конфіденційна інформація як вид інформації з обмеженим доступом, слід сформулювати принцип рівності прав органів державної влади та інших учасників інформаційних відносин на отримання відкритої інформації. Стосовно інформації з обмеженим доступом, то для кожного органу державної влади законом мають передбачатися підстави для отримання конкретного виду таємної або конфіденційної інформації для виконання покладених на органи державної влади завдань [4, с. 26].

Важливим принципом регулювання відносин щодо отримання органом державної влади інформації має бути закріплення *юридичної відповідальності за порушення права* органу отримувати інформацію. Причому відповідні санкції мають враховувати шкоду, яка завдаватиметься інтересам держави, юридичних або фізичних осіб у зв'язку з невиконанням державної функції через ненадання інформації. Так, ненадання інформації правоохоронним органам при розслідуванні кримінальних справ може спричинити значні негативні наслідки для охоронюваних державою інтересів фізичних і юридичних осіб [4, с. 27].

З огляду на зазначене можемо сформулювати *спеціальні принципи* правового регулювання відносин щодо отримання органами державної влади України інформації, до яких віднесено: достовірність і повнота інформації, яка надається органам державної влади; своєчасність отримання органами державної влади інформації; отримання такими органами інформації про особисте юридичних осіб надавати інформацію органам державної влади на їх законний запит; погодження з власником інформації питання про передачу стороннім суб'єктам отриманих від нього цінних відомостей (об'єктів права інтелектуальної власності, інформацію з обмеженим доступом, недоторканість якої охороняється законом).

Література:

1. Бачило И. Л. Информационное право / И. Л. Бачило; [под ред. академика Б. Н. Топорнина]. СПб.: Юридический центр Пресс, 2005. *343 с.*
2. Громадяни у пошуках інформації: українські реалії / [упорядники: І. Підлуська, С. Горобчишина]. Київ: Агентство «Україна», 2005. 180 с.
3. Костецька Т. А. Право на інформацію в Україні / Т.А. Костецька ; НАН України; Інститут держави і права ім. В.М.Корецького. Київ: Вища школа права, 1998. 39 с.
4. Сопілко І. М. Методологічні засади виокремлення спеціальних принципів отримання інформації органами державної влади в Україні. Інформаційна безпека людини, суспільства, держави. 2012. № 1 (8). С. 23–28.

Махницкий О. В.,
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ

БЛОКЧЕЙН ЯК ІНСТРУМЕНТ КІБЕРБЕЗПЕКИ

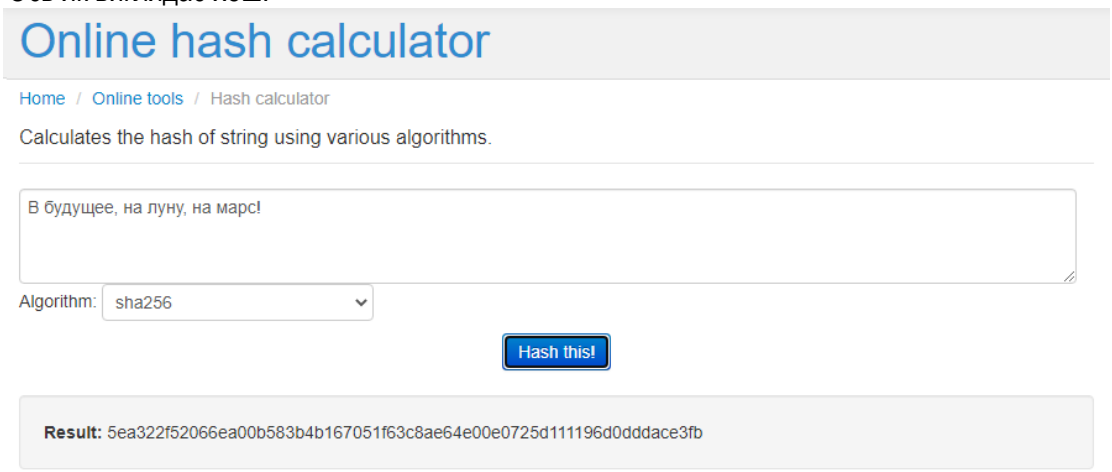
В ІТ-співтоваристві вже сформувалася стійка думка про те, що блокчейн може здорово допомогти людям з точки зору забезпечення безпеки даних. Можливість швидкого виявлення підробок,

стійкість до DDoS, високий рівень захищеності інформації роблять блокчейн вельми привабливою технологією. Далі розглянемо найбільш важливі елементи блокчейн-безпеки.

В основі блокчейна лежить обчислення з математичного алгоритму хешу від заданого набору даних. Ось деякі властивості і особливості хешу:

- Хеш – це певна кількість певної довжини;
- Хеш може бути отриманий в результаті перетворення даних в цифровий відбиток, тобто перетворити цілу енциклопедію в набір символів фіксованої довжини;
- Використовуються захищені алгоритми хешування, наприклад SHA256, SHA384 і SHA512;
- з обчисленого хешу важко або неможливо отримати вихідні дані, навіть знаючи алгоритми за якими формувався хеш;
- неможливо передбачити, як зміниться хеш при зміні вхідних даних;
- розбіжність хешу вказує на підробку даних при передачі.

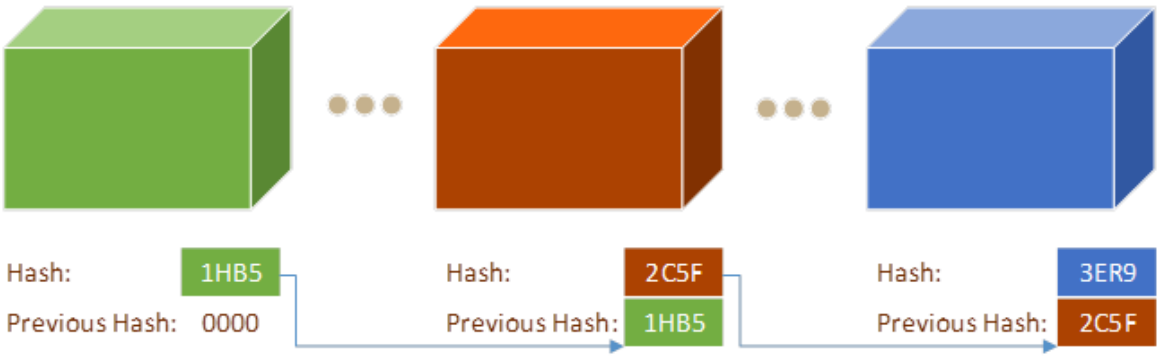
Ось як виглядає хеш.



Блоки даних.

У контексті структур даних блокчейн найбільш нагадує зв'язний список. Дані в блокчейне поділяються по контейнерах, що має назву блоками. Які вони мають особливості?

- На кожен блок даних посилається хеш, обчислений з вмісту цього блоку даних. Кожен блок даних містить також хеш від попереднього блоку даних.
- Існує журнал транзакцій, що відноситься до попередніх блокам даних.
- Якщо після передачі блоку даних обчислений хеш не збігається з еталонним, то це вказує на зміни в даних (підробку).
- Існує щохвилинна статистика створення блоку.
- Блоки даних з'єднуються разом в структуру пов'язаного списку. Хеш попереднього блоку додається в наступний блок і це формує зв'язок між блоками. При будь-якій зміні в попередніх блоках даних обчислених хеш не співпадатиме із зазначеним хешем в блоці даних, тому втручання в ланцюжок блоків неможливо.
- Гарант незмінності: дані хешу назавжди зберігаються в ланцюжку блоків і не можуть бути змінені.



У чому взагалі сенс блокчейн-безпеки, які сутності їй притаманні? Технологія дозволяє людям, які не довіряють один одному, ділитися цінними даними безпечним і захищеним способом. Завдяки їй досягається:

- блокування крадіжки особистих даних
- блокування підробки даних
- блокування DDoS - атак

Блокчейн перетворює цифрову ідентифікацію в реальність і допомагає захиститися від крадіжки ідентифікаційної інформації:

Цифрова ідентичність - це інформація, яка зберігається в цифровому форматі і сама по собі є повним ідентифікатором. Користувач, за запитом і з своєї згоди, ділиться цією інформацією з організацією. Зацікавлена організація звіряє отриманий хеш з публічним репозитарієм хешів, наприклад, Aadhaar. Якщо хеш збігається, то це говорить про те, що посвідчення використовується аутентифіцироватися особою. Дані видно не завжди і знаходяться в захищеному вигляді до моменту перевірки.

Є й інші важливі нюанси блокчейна. Назвемо найбільш цікаві з точки зору безпеки:

- користувач є повним власником своїх даних і сам вирішує, кому ці дані можна передати;
- діє концепція отримання підтвердження операції;
- дані про підтвердження зберігаються в блоках;
- інформація в блоках докладно описує кожну транзакцію, яка сталася між взаємодіючими сторонами.

Наприклад, перший запис про транзакції між користувачем і банком для відкриття рахунку, в якому користувач ділиться даними, необхідними для відкриття рахунку: особисті дані, унікальний ідентифікатор, фотографія, підтверджені адреси і т. д. Таким чином, квитанція про згоду буде містити всі відомості про ключові індикатори і зберігається в кожною організації, а також у блокчейні.

Якщо банк бажає передати дані третій стороні на законних підставах, він повинен передати їх за згодою користувача, який є власником ідентифікаційної інформації, і в квитанції про згоду буде транзакція від користувача, банку і третьої сторони. Але якщо банк намагається незаконно передати дані третій стороні без згоди користувача, який є єдиним власником, то вони будуть не валідними. Це покаже невідповідність в транзакціях, відсутність відповідного запису в квитанції згоди. І в подальшому це може бути виявлено при аудиті.

І ще однією важливою особливістю блокчейна є його захищеність від підробок:

- одержувачі і користувачі даних можуть перевірити джерело даних;
- блокчейн замінює секретність на прозорість, розподіляючи докази підписання документа з багатьма блокчейнами;
- практично неможливо маніпулювати даними;
- перевірка ідентичності без цифрового підпису - при цьому хеші вихідних файлів зберігаються в блокчейне, виконується перевірка інших копій файлів за допомогою алгоритму хешування і порівнюється результат з хешамі, що зберігаються в блокчейні;
- маніпуляції з даними будуть швидко виявлені, так як вихідний хеш існує на мільйонах вузлів.

Відзначимо також, що міністерство оборони США розглядає блокчейн-інфраструктуру KSI як потенційно придатну для захисту чутливих військових даних. А ще існує компанія під назвою Gem, яка допомагає використовувати блокчейн для безпечного обміну медичними даними між зацікавленими сторонами відповідно до вимог американської HIPPA.

Розглянемо ще одну перевагу – блокування DDoS-атак.

Розподілені атаки типу «відмова від обслуговування» (DDoS) – це проблема, яка за замовчуванням виключена в блокчейні. Давайте розглянемо це в контексті Ethereum і Hyperledger, обидві технології являють собою різні форми блокчейна – публічний і приватний блокчейн відповідно.

DDoS – це атаки, при яких на сервер приходить величезна кількість сміттєвих запитів, що значно збільшує час відповіді сервера для відповіді на нормальні запити. В контексті Ethereum за будь-який обслуговується запит повинна бути виплачена певна сума у вигляді GAS (найменша форма Ethereum). Такий підхід за своєю концепції виключає DDoS-атаки.

У Hyperledger, який являє собою окремий блокчейн, існує мережа, в якій всі учасники заздалегідь відомі, а нові учасники перевіряються сертифікують органами перед підключенням. Є незначні шанси на DDoS-атаку, але так як всі учасники вже відомі винуватця буде легко виявити.

Дуфенюк О. М.,
доцент кафедри кримінального процесу та криміналістики факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

МЕНТАЛЬНА КАРТА ЯК ІННОВАЦІЙНИЙ ІНСТРУМЕНТ РОЗВИТКУ МЕТАКОГНІТИВНИХ НАВИЧОК ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Заклади вищої освіти нового покоління покликані не тільки забезпечити майбутнього фахівця необхідними професійними знаннями та навичками, але й розвивати його потенціал, креативність, уміння бути гнучким та пристосовуватися до нових викликів сучасного життя. Одним із останніх освітніх трендів є впровадження ментальних карт як ефективного засобу розвитку метакогнітивних навичок здобувачів вищої освіти. Йдеться про здатність контролювати й регулювати свою когнітивну діяльність (поставити мету, спланувати свою діяльність, здійснити контроль і оцінити її ефективність) [1, с. 73]. Високий рівень навиків керування пізнавальними процесами в майбутньому дозволить фахівцю більш ефективно реалізовувати наступні процеси:

- працювати з великими масивами інформації;
- генерувати нові зв'язки, ідеї, асоціації;
- візуалізувати дані;
- відсіювати головне і другорядне, ранжувати об'єкти, вибудовувати ієрархії;
- дивитися на проблему з різних позицій, нових позицій;
- запам'ятовувати ключові питання заданої тематики;
- структурувати матеріал будь-якої тематики і будь-якої складності;
- логічно подавати аргументацію своєї позиції (вибудовувати лінію «за» або «проти»), переконувати опонента;
- креативно мислити та шукати інноваційні рішення проблем, що дозволить отримати значні соціально-економічні ефекти;
- критично оцінювати свою діяльність.

Сучасні дослідження у сфері когнітивної психології показують, що результативність розуміння тексту підвищується, якщо суб'єкт розуміння використовує не тільки різноманітні стратегії обробки інформації, а й метакогнітивні процеси, які розглядаються як один з обов'язкових чинників успішності пізнавальної діяльності. За словами А.Гриньківа, студенти з низьким рівнем розуміння тексту мають дефіцит метакогнітивних знань і використовують недостатнє число метакогнітивних стратегій. Вони мають обмежені знання про власні пізнавальні процеси, їх функціонування [2, с.41]. Натомість студенти з високим рівнем розуміння тексту порівняно зі студентами інших груп мають більше метакогнітивних знань, демонструють найбільш високий рівень метакогнітивної включеності в діяльність [2, с. 42]. Метакогніції є складними, багаторівневими, системними та організованими психічними процесами, які спрямовані на організацію, регуляцію та координацію первинних пізнавальних процесів. Відтак, на думку Ю. Адоньєвої, метакогнітивне навчання має бути обов'язковою складовою як системи вищої, так і післядипломної освіти [3, с. 13].

Широке використання ментальних карт в освітньому процесі дозволить досягнути значних успіхів у сфері опанування метакогнітивних навиків.

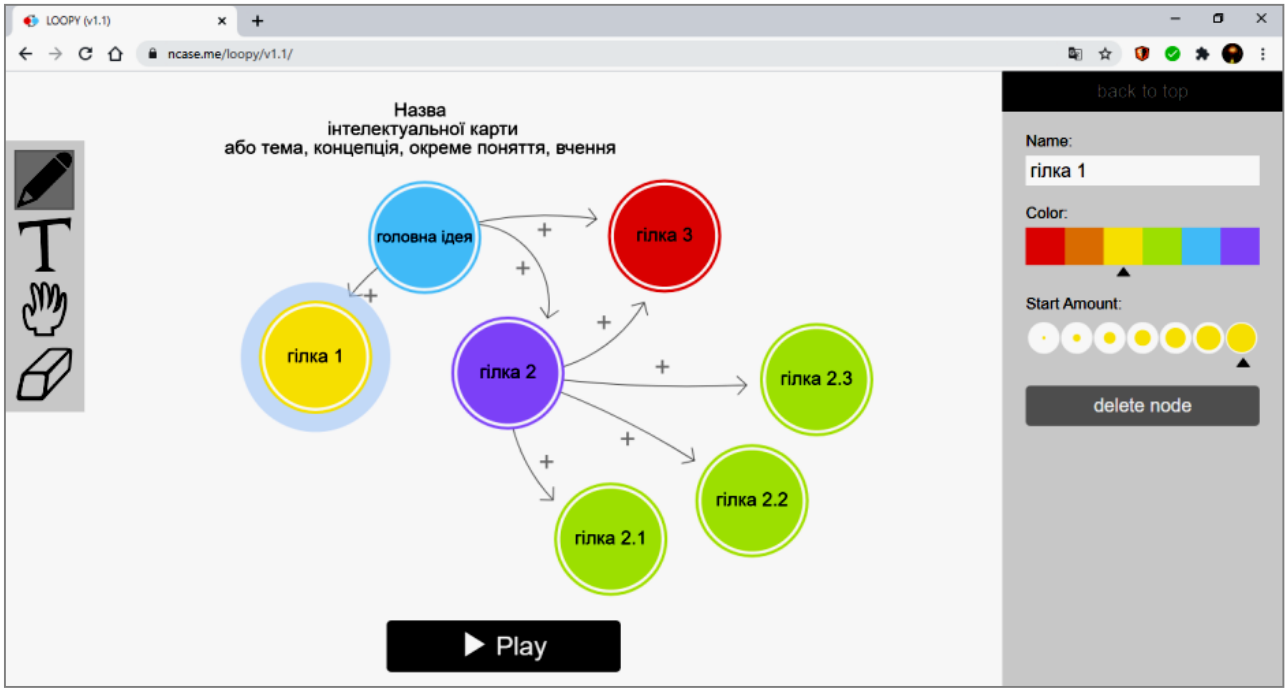
Ментальні карти (розумові карти, інтелектуальні карти) – це спосіб презентації інформації у схематичній формі, яка передбачає обрання умовного ядра (головної об'єднуючої ідеї, поняття, терміну) та розгалуження гілок (думки, тези, ідеї нижчого порядку), які в сукупності наочно презентують суттєві компоненти системи (теми, окремого вчення, концепції, правового інституту і т.д.) та їх зв'язки за допо–могою графічних засобів візуалізації (геометричні фігури, символи, кольори, точки, лінії, діаграми тощо).

Очевидно, що такі ментальні карти може готувати науково-педагогічний працівник, а потім в ході освітнього процесу їх презентувати для подачі теоретичного лекційного або іншого матеріалу. Однак більш ефективною вважається індивідуальна або групова робота здобувачів вищої освіти, коли вони власними зусиллями, опановуючи певний розділ, тему чи окремі поняття навчальної дисципліни, формують такі карти і при цьому навчаються не тільки на рівні професійному, але й на рівні метакогнітивному, особистісному. Позитивний ефект від такої роботи доведено «польовими» дослідженнями зарубіжних та українських вчених.

Зокрема, у даному контексті показовим є експеримент, проведений А. Мухлісіном (A. Muhlisin), який складався з трьох етапів та підсумкового опитування сорока студентів, які взяли участь в експерименті. Перший етап полягав у читанні текстів (студенти повинні були прочитати певний текстовий матеріал, отриманий з різних інформаційних / навчальних ресурсів). Другий етап полягав в інтелектуальному картуванні (студенти повинні були створити інтелектуальні карти за допомогою всіх доступних графічних засобів, схем, символів, кольорів, форм і т.д.). Третій етап передбачав обмін інформацією між студентами (студенти повинні були презентувати усій аудиторії свої ментальні карти).

Значну ефективність ментальних карт остаточно підтвердили результати постекспериментального опитування студентів, адже 92, 5 % респондентів позитивно оцінили таку модель навчання. Серед іншого, було звернуто увагу на наступні переваги занять з використанням засобів інтелектуального картування: така форма презентації навчального матеріалу допомагає мозку організувати, запам'ятати, порівняти об'єкти та встановити міжпредметні зв'язки; студенти демонструють більшу здатність дослідження певних питань як під час індивідуальної роботи, так і під час роботи в групах; заняття відбувається цікавіше, веселіше та зростає мотивація до навчання, оскільки при картуванні використовуються цікаві зображення, символи та кольори, а «неправильних» ментальних карт не існує (можна не боятися помилок); легше засвоїти матеріал, оскільки він має стислу форму записів, чітку логіку побудови, а тому легше запам'ятовувати дані; можна вдосконалити навики критичного мислення [4]. Схожі результати отримало дослідження думки українських студентів [5, с. 194].

Ментальні карти можна виготовити власноручно або за допомогою спеціальних ресурсів, які покликані забезпечити швидке та ефективне графічне кодування інформації, дозволяють сформувати певні шаблони, автоматично формують зв'язки, містять великі бібліотеки символів та інших інструментів для позначень. Зокрема до таких сервісів можна віднести Coogle (www.coggle.it), Freemind, Xmind (www.xmind.net), MindMeister (www.mindmeister.com), BubblUs (www.bubbl.us), MindMup 2 (www.mindmup.com), LOOPY (www.ncase.me/loopy/) (див. мал. 1), WiseMapping (www.wisemapping.com), Mind42 (www.mind42.com), iMindMap (www.imindmap.com) [5, с. 190–192].



Мал. 1. Приклад ментального картування з допомогою ресурсу LOOPY

Підсумуємо сказане. По-перше, розвиток метакогнітивних навичок здобувача вищої освіти є одним із пріоритетів сучасного освітнього процесу. По-друге, інтелектуальне картування є ефективним інструментом не тільки для вивчення конкретних навчальних дисциплін, але й для удосконалення навичок пізнавальної діяльності, які дозволять майбутньому фахівцеві бути креативним, здібним до аналітичного та критичного мислення, а також здатним реагувати на нові виклики в епоху стрімкого зростання обсягів інформації, що потребує обробки та вивчення.

Література:

1. Зошій І. В. Роль метакогнітивних здібностей у формуванні професійної компетентності юристів. *Science and Education a New Dimension. Pedagogy and Psychology*. V (54). Issue 126. 2017. С. 72–75. URL: https://seanewdim.com/uploads/3/4/5/1/34511564/i._v._zoshiy_role_of_metakohnityv_skills_in_forming_professional_competence_of_lawyers.pdf.
2. Гриньків А. Метакогнітивні дослідження в контексті освітніх інновацій. *Вища освіта України*. 2016. № 2. С. 37–43.
3. Адоньєва Ю. А. Метакогнітивне навчання майбутніх фахівців у вищих навчальних закладах: досвід та особливості впровадження. *Journal «ScienceRise: Pedagogical Education»*. 2017. № 6 (14). С. 10–13.
4. Muhlisin A. Analysis of students' response of the implementation of rms (reading, mind mapping, and sharing)learning model in philosophy of science. *USEJ.* 2018. 7 (1). P. 13–18. URL: http://journal.unnes.ac.id/sju/index.php/usej.
5. Романовський О., Гриньова В., Резван О. Ментальні карти як інноваційний спосіб організації інформації в навчальному процесі вищої школи. *Інформаційні технології і засоби навчання.* 2018. Том 64. № 2. С. 185–196.

Магеровська Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

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

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ У ХМАРНИХ СЕРВІСАХ

Для успішної організації інформаційної безпеки хмарної системи необхідно враховувати наступні елементи:

- підсистему, яка забезпечує надійне зберігання інформації у клієнта;
- підсистему яка організовує безпеку в мережі;
- підсистему забезпечення надійності віртуальних середовищ;
- підсистему, яка дозволяє організувати безпечну роботу в центрах оброблення даних.

Необхідно відзначити, що, як і в інших подібних системах призначених для захисту інформації, говорити про успішно організовану безпеку хмарної системи можна тільки тоді, коли робота всіх підсистем організовано на найвищому рівні.

Для детального вивчення питання дослідження безпеки у хмарах розглянемо кожну з перерахованих вище підсистем.

Підсистема, яка забезпечує надійне зберігання інформації у клієнта може бути схильна до таких загроз як Cross-site-scripting (XSS), Phishing, віруси, трояни. Це пояснюється тим, що користувачі змушені працювати з сервісом хмарних обчислень використовуючи інтернет-браузер. Для того щоб організувати безпеку інформації на цьому рівні необхідно на стороні клієнта дотримуватися виконання наявності наступних елементів:

- антивірусні пакети програм для захисту інформації;
- засоби, що дозволяють шифрувати дані на диску;
- персональний брандмауер, який буде знаходитися в ОС;
- інтернет-браузер, який правильно налаштований з точки зору безпечного підключення до мережі [1].

Підсистему, яка організовує безпеку в мережі необхідно організовувати таким чином, щоб дані, які знаходяться у публічній хмарі були в безпеці. Для цього необхідно використовувати спеціальний тунель віртуальної приватної мережі (VPN). Він надає можливість об'єднати клієнта і сервер з метою отримання публічних хмарних послуг. VPN-тунель дозволяє здійснювати безпечні з'єднання і, крім того, користувач має можливість використовувати єдине ім'я та пароль для входу до різних хмарних ресурсів. VPN-з'єднання використовує ресурси Інтернет, доступ до яких мають усі користувачі, для того щоб організувати процес передавання даних для публічних хмар. Описаний механізм можливо реалізувати

на практиці за допомогою режимів доступу із шифруванням з використанням двох ключів на базі протоколу Secure Sockets Layer.

Підсистема забезпечення надійності віртуальних середовищ залежить від безпеки механізмів віртуалізації. Якщо успішно реалізована атака на гіпервізор, то зловмисник може непомітно для систем захисту інформації, які функціонують у віртуальних машинах, здійснювати такі дії: копіювати та блокувати інформаційний потік даних, який йде на різні пристрої (HDD, принтер, USB); читати і редагувати інформацію на дисках віртуальних машин. Слід зазначити, що ці дії будуть можливі і при вимкнених машинах, без участі їх програмного забезпечення. Для того щоб вирішити описану проблему необхідно захистити гіпервізор. Для цього потрібно розмежувати права доступу до сервера віртуалізації, що можливо зробити шляхом своєчасної установки оновлень програмного забезпечення середовища віртуалізації, а також потрібно обмежити запуск програм.

Диск віртуальної машини знаходиться на SAN/NAS. У зв'язку з цим стає актуальним питання про захист інформаційних даних віртуальних машин шляхом обмеження доступу до дисків машин за допомогою сертифікованих засобів захисту інформації та спеціальних екранів, які здатні контролювати протоколи та інші елементи віртуальної інфраструктури. Якщо зловмисник отримає доступ до засобів адміністрування, то він буде мати можливість редагувати дані, знищувати, викрадати у всій мережі віртуальної інфраструктури. Щоб уникнути подібних випадків атак, необхідно захистити доступ до мережі адміністрування, серверів віртуальних машин, всіляких засобів управління інфраструктурою.

Віртуальні машини, які мають один фізичний сервер, мають можливість здійснювати обмін трафіком безпосередньо, не використовуючи при цьому мережеві комутатори. У цьому випадку використання міжмережевих екранів не буде особливо ефективним. Для успішного вирішення цієї проблеми необхідно удосконалити існуючі сертифіковані екрани і їх перенесення у віртуальне середовище. Окрім цього потрібно ще створити спеціалізовані засоби захисту інформації, які зможуть контролювати трафік усередині необхідного сервера. По мережі реплікації передаються сегменти їх оперативної пам'яті, тому, якщо зловмисники під час атаки перехоплять дані, то існує пряма загроза безпеці. А це означає, що мережу реплікації необхідно ізолювати від інших мереж і, крім того, використовувати сертифіковані VPN для каналу реплікації. Не потрібно розраховувати на тривіальність структури віртуальних машин, оскільки це може призвести до більших проблем з безпекою, а необхідно організувати процес управління віртуальними машинами, таким чином, щоб він був узгоджений з політикою безпеки організації.

Підсистема, яка дозволяє організувати безпечну роботу в центрах обробки даних (ЦОД), здатна забезпечити безвідмовну роботу системи на всіх її рівнях безпеки, надійності, доступності. Використання описаної технології надає можливість створювати резервні сховища інформації і при цьому не втрачати функціональність інформаційної системи.

Для кращого розуміння організації безпеки хмарних систем розглянемо структуру ЦОД. Центр даних являє собою кластер серверів, головна мета створення якого полягає в тому, щоб підвищувати ефективність безпеки в плані фізичного та мережевого захисту. Об'єктами захисту в ЦОД можна назвати наступні елементи: обладнання, приватна інформація, програмне забезпечення.

Підсистема ЦОТ в своєму складі має:

- відеоспостереження;
- пожежну сигналізацію;
- систему контролю для управління доступом;
- систему для створення резервного копіювання, відновлення інформації;
- систему для захисту безпеки даних ЦОД.

Основними компонентами, які необхідні для успішної побудови системи інформаційної безпеки ЦОД, є:

- централізована система для керівництва засобами захисту інформації;
- кошти, які допомагають запобігти вторгненню;
- засоби антивірусної безпеки;
- засоби для роботи з шифрування файлів;
- засоби міжмережевого екранування;
- засоби з обмеження доступу;
- засоби аналітики та управління подіями;

– кошти на проведення моніторингу з цілісності інформації і додатків.

Для ефективного забезпечення конфіденційності та надійності використання хмарних систем необхідно, перш за все, подбати про безпеку всіх учасників складових процесу передавання, зберігання інформації, починаючи від постачальника «хмарного» рішення, користувача та зв'язків, які їх пов'язують. Якщо говорити про поставлені завдання перед провайдером, то вони полягають у тому, щоб забезпечити недоторканність інформаційних даних третіми особами, як у фізичному, так і програмному сенсі. Для успішного вирішення подібних завдань користувач повинен вести у межах своєї території необхідну конфіденційну політику даних з метою виключення можливості з надання прав доступу до даних сторонніх осіб.

Якщо необхідно забезпечити цілісність даних, які використовуються через окремі хмарні додатки, то необхідно зробити необхідні дії, враховуючи сучасний інтерфейс баз даних, використовувати системи, які призначені для резервного копіювання, алгоритми для перевірки конфіденційності даних й інші рішення. Але крім всього перерахованого, також, необхідно враховувати інтеграцію кількох хмарних додатків від декількох постачальників.

Якщо порівнювати можливі ризики, що стосуються безпеки даних у відомих хмарних моделях і можливих альтернативних рішень питань безпеки, то в залежності від моделі SaaS, PaaS або IaaS, змінюється рівень контролю над безпекою та фізична інтерпретація рішення.

Розглянемо окремо питання забезпечення безпеки у кожній з відомих хмарних систем. У моделі SaaS додаток доступний через веб-браузер і запускається на хмарній інфраструктурі. У цьому випадку клієнт не має можливості управляти мережею, серверами, ОС і навіть деякими додатковими можливостями додатків, що використовуються. Виходячи з цього під час використанні моделі SaaS, головна відповідальність за забезпечення безпеки покладається тільки на постачальників і в зв'язку з цим користувач не має можливості керувати паролями.

Головним ризиком в моделі SaaS є те, що додатки розташовані у хмарі і можливе використання різних облікових записів для того, щоб отримати доступ до додатків. Компанії можуть вирішити описану проблему шляхом проведення уніфікації облікових записів для хмарних та локальних систем. Якщо користувач одноосібно контролюватиме вхід у додаток, то в свою чергу він отримає доступ до робочих станцій і хмарних сервісів. Даний підхід сприяє зменшенню кількості «підвислих» облікових записів, які можуть бути зламані після звільнення співробітників.

Використання моделі PaaS передбачає, що клієнт самостійно створює додаток на необхідних йому мовах програмування й інструментах, а потім розгортає його у хмарі. Аналогічно моделі SaaS, клієнти PaaS позбавлені можливості управління і контролю за інфраструктурою хмарних додатків: мережі, сервера, ОС, системи зберігання даних, але користувач має можливість розгортати додатки. Використовуючи модель PaaS, клієнти повинні дбати про безпеку додатків, управління API, мова йде про підтвердження входу в систему, авторизацію, проведення перевірки.

Головна проблема яка виникає під час використання PaaS – це шифрування даних. Відзначимо, що модель PaaS сама по собі безпечна, але виникає ризик пов'язаний з малою продуктивністю системи. Виникнення описаної проблеми, перш за все, пов'язано з тим, що під час здійснення обміну інформацією між провайдерами PaaS необхідно користуватися шифруванням. Але для цього потрібна відповідна потужність процесора. Крім того, відомо, що будь-яку дію передачі інформації користувачів необхідно здійснювати по зашифрованому каналу передачі даних.

У IaaS клієнти не можуть управляти хмарною інфраструктурою, але разом з тим вони мають доступ до контролю над ОС та розгортання додатків. У моделі, що розглядається існує декілька варіантів для забезпечення безпеки без всебічного захисту інфраструктури. З цього випливає те, що клієнти самі повинні організувати безпеку операційної системи, інформаційного контенту та додатків за рахунок API.

Виділимо основні елементи, захист яких повинен надати провайдер: безпосередній контроль за доступом до інфраструктури та стійкість архітектури, що використовується. Зі сторони користувача повинні бути захищені наступні об'єкти: міжмережеве екранування в межах інфраструктури, що використовується; захист ОС, інформаційних баз (доступ, стійкість, настройки безпеки); захист фінішних ланок додатків (антивірусний захист, контроль за входом в систему) [2].

Легко бачити, що значно більша частка для успішної організації захисту хмарних технологій лягає на плечі клієнтів, а що стосується провайдера, то він, швидше за все, надає стандартні

рекомендації, які необхідно виконувати для повноцінного захисту даних, ніж вирішує поставлені завдання перед користувачами.

Проведений аналіз літературних джерел з тематики даної роботи, показує, що науці відомо 7 основних напрямків атак на сервісні моделі SaaS, PaaS і IaaS:

- порушення конфінденцеальності під час використання хмарних технологій;
- порушення безпеки під час використання програмних інтерфейсів (API);
- порушення всередині компанії користувача;
- порушення цілісності систем віртуалізації;
- порушення правил аутентифікації, авторизації та аудиту, що тягне за собою втрату або витік інформації;
- порушення цілісності персональних даних, що надають доступ до необхідних сервісів;
- порушення стійкості внутрішньої інфраструктури системи [3].

Результатом спільної роботи організацій TCG і CSA, стосовно успішної організації безпеки хмарних систем на всіх її етапах роботи, стали сформовані рекомендації, які повинні бути враховані при укладенні договору між клієнтом і провайдером. Згідно рекомендаціям фахівців необхідно:

- використовувати технології шифрування для забезпечення збереження даних;
- захистити дані під час передавання, для цього потрібно використовувати надійні протоколи і алгоритми (наприклад TLS, IPsec і AES);
- організувати високий ступінь аутенфікації;
- ізолювати користувачів один від одного в тому плані, що дані і додатки одного клієнта повинні бути відокремлені від інших користувачів;
- провайдеру слідувати єдиній стратегії в нормативно-правовому аспекті;
- розробити документальні підтвердження на незаплановані події.

Виконання наданих порад дозволить вирішити безліч питань, пов'язаних з безпечним використанням хмар, надасть варіанти для виходу з форс-мажорних обставин, роз'яснить, як поводитися при зміні провайдера, який надає хмарні послуги, тощо.

Література:

1. Остапов С. Е. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
2. Битва за хмару: локальні дата-центри vs міжнародні хмарні провайдери [Електроний ресурс] – Режим доступу: https://nv.ua/ukr/techno/innovations/bitva-za-hmaru-lokalni-data-centri-vs-mizhnarodni-hmarni-provayderi-50065588.html
3. Mell Peter, Grance Thimothy. «The NIST Definition of Cloud Computing (Draft)» // Recommendations of the National Institute of Standards and Technology, Special Publication 800 – 145 (Draft), Вересень, 2017.

Синиціна Ю. П.,
доцент кафедри економічної та інформаційної безпеки Дніпропетровського Державного університету внутрішніх справ, кандидат технічних наук, доцент

АРТ-АТАК – ПРІОРИТЕТНИЙ НАПРЯМОК РОЗВИТКУ КІБЕРБЕЗПЕКИ

У вирішення питань ІБ залучаються топ-менеджери організацій, і для них гостро стоїть питання ефективності існуючої системи ІБ і використовуваних підходів. Керівництво задається питанням - а чи дійсно ті системи і заходи, які використовуються в компанії, зможуть захистити від реалізації найбільш значущих ризиків. Важливо, як вимірювати ефективність ІБ.

Актуальність даної теми очевидна, оскільки забезпечення безпеки роботи промислово стратегічних об’єктів є важливою складовою розвитку не лише окремо взятої структури, аі економіки країни в цілому. Окрему увагу варто приділити авторам-науковцям, в працях яких розглядалася дана тематика дослідження, а саме: М. М. Безкоровайный, А. Л. Татузов, Д. В. Дубов, О. Шаховал, І. Лозова, С. Гнатюк, С. В. Мельник, О. А. Баранов, В. П. Харченко та ін.

Новини про успішні цільових атаках APT-угруповань постійно миготять в ЗМІ, і під загрозою не тільки ті компанії, які згадуються в цих статтях, а й будь-яка інша. Не можна забувати і про масові атаки,

жертвами яких продовжують ставати великі компанії, які виплачують викупи за зашифровані дані. За результатами ретроспективного аналізу і розслідування інцидентів визначено, що багато компаній, які перейшли до практики виявлення кіберінцідентов, виявляють сліди зломів, що відбулися кілька місяців, а то й кілька років тому (в минулому році було виявлено угруповання TaskMasters, яка перебувала в інфраструктурі однією з жертв як мінімум 8 років). Це означає, що злочинці вже давно контролюють безліч організацій, але самі організації не помічають їх присутності, думаючи, що насправді захищені. При цьому часто виявляється, що в інфраструктурі таких компаній «живе» навіть не одна, а кілька угруповань. Підсумком планомірної роботи з компаніями стало те, що сьогодні вони почали дійсно цікавитися інформаційною безпекою, виявляти кіберінціденти у власній інфраструктурі, аналізувати дії хакерів, шукати відповіді на запитання про те, чи готова їхня інфраструктура до атак. Це, безумовно, позитивна тенденція. Але є і негативна. Злочинці все краще освоюються в кіберпросторі. Світ інформаційних технологій вже не можна назвати віртуальним: настільки тісно він пов'язаний з реальним.

Розслідуючи діяльність APT-угруповань, в цьому році було виявлено зростання числа APT-атак на різні галузі. Якщо в минулому році в поле зору потрапили 12 APT-угруповань, то в цьому році предметом досліджень стали вже 27 угруповань. Ця тенденція корелює з даними про постійне зростання числа унікальних кіберінцідентов з кварталу в квартал (в третьому кварталі 2019 року зафіксовано на 6% більше унікальних кіберінцідентов, ніж у другому)

Цілеспрямовані атаки в цьому році, що минає істотно переважають над масовими. Протягом року спостерігалося зростання цілеспрямованих атак: в третьому кварталі їх частка склала 65% (проти 59% у другому кварталі і 47% в першому). Організації рік за роком беруть на озброєння все більш ефективні методи захисту, тому масові атаки просто перестають працювати. Якщо ж говорити про націлених атаках, то ситуація інша: середня швидкість реакції компаній сегмента large enterprise на сучасні загрози - близько трьох років. Тобто з моменту усвідомлення необхідності покупки рішення щодо виявлення атак і протидії зловмисникам до його реального застосування в компаніях проходить близько трьох років, присвячених бюджетування, тендерів, пілотним впровадженням, закупівлю, впровадження, навчання та ін. При цьому зловмисники активно використовують новітні уразливості (в 2019 році APT-угруповання використовували в своїх атаках чотири уразливості нульового дня), діють дуже швидко, а головне - часто змінюють свій інструментарій і тактики. Наприклад, угруповання RTM протягом року використовувала три різні способи отримання інформації про контрольні серверах: через namecoin, через Tor, через bitcoin. Разом з тим в 2019 році маємо три різні версії Дроппер (установника основного модуля ВПО), одну версію завантажувача і три різних версій трояна. Інше угруповання, що працює в фінансовому секторі, Cobalt, з осені 2019 роки для кожної зараженої машини з контрольного сервера викачує закодований CobInt з унікальною хеш-сумою для кожного завантаження: таким чином зловмисники обходять детектування їх по хеш-сумам фінального шкідливого файлу. Одне з угруповань, що займаються крадіжкою даних, в 2019 році використовувала сім різних версій ВПО і чотири різні тактики для закріплення і обходу детектування в інфраструктурі. Таким чином, судячи з даних Експертної центру безпеки Positive Technologies (PT ESC), в 2019 році угруповання в середньому використовували по чотири різні варіанти ВПО і по п'ять тактик для закріплення в інфраструктурі. У той же час, 144 місяці - максимальний час, через яке стало відомо про дії APT-угруповання, і 17 місяців - середній час, що минув з моменту атаки до появи про неї публічної інформації. Таким чином, ключовими критеріями, за якими можна оцінювати сьогодні розстановку сил між зловмисниками і захисниками, є:

1. Використання новітніх технік атаки проти використання новітніх засобів захисту: тут в ряді випадків розбіг доходить до трьох років не на користь захисту.

2. Використання нових вразливостей проти середнього часу патч-менеджменту: співвідношення практично завжди виявляється на користь зловмисників, які адаптують новітні експлойти для своїх атак іноді протягом доби.

3. Вартість інструментів - вартість захисту. За нашою оцінкою, набір інструментів для проведення атаки, спрямованої на крадіжку грошей з банку, може коштувати від 55 тис. дол. США. Кібершпіонская кампанія обходиться на порядок дорожче, її мінімальний бюджет становить 500 тис. дол. США. Оцінку ж повної вартості захисту, включаючи вартість технічних засобів, витрати на вибудовування процесів і зарплату фахівців, виконати складно, так як все залежить від компанії і рівня її зрілості з точки зору ІБ.

Цілями APT-угруповань як і раніше є компанії, які володіють важливими даними і грошима. При цьому атакують не тільки великі компанії, а й підприємства середнього і малого бізнесу, перш за все для того, щоб використовувати їх як плацдарм для нападу на великий бізнес, а також для маскування своїх дій. Посилюється тренд атак на провайдерів послуг зв'язку, вендорів і постачальників послуг. При цьому іноді компанії навіть не підозрюють, що від цих організацій може виходити загроза. Як приклад випадок: один з постачальників вендінгових автоматів просив організувати віддалений канал доступу до автомата через інтернет. Автомат був підключений до корпоративної мережі і через неї був забезпечений доступ до інтернету для роботи автомата і його синхронізації з серверами керуючої компанії. В результаті внутрішні ресурси компанії піддалася атаці через цей канал зв'язку.

Отже, великі компанії при аналізі власних ризиків ІБ продовжать звертати увагу не тільки на вимоги регуляторів, а й на необхідність побудови практичної безпеки, спрямованої на мінімізацію значущих для себе бізнес-ризиків. Малий і середній бізнес, не завжди готовий вкладати чималі кошти в кібербезпека, залишатиметься під прицілом як масових кіберкампаній, так і цільових атак хакерських угруповань. З огляду на підвищення захищеності великих гравців хакерам доведеться вдаватися не тільки до витонченому фішингу та створення все більш досконалих зразків ВПО, але і до злому менш захищених компаній, щоб проводити через них атаки на цільові організації, в тому числі по налаштованим між ними довіреною каналах. Схеми кіберуслуг на продаж будуть розвиватися, набирати обертів і приймати нові форми. Зокрема, може придбати більшу популярність схема, коли одні зловмисники зламують інфраструктури компаній і проникають у внутрішню мережу, але не використовують такий доступ для своїх цілей, а продають або здають його в оренду іншим учасникам тіньового ринку (модель access as a service, «доступ як послуга»). Операторам шкідливого ПО (наприклад, шифрувальників) не треба буде думати, яким чином заразити системи компанії, вони просто заплатять певну ренту за доступ до вже зламаним мереж. Можна прогнозувати зростання числа інцидентів в секторі SMB, пов'язаних з BEC-шахрайством (business email compromise) - соціальною інженерією з використанням реальних акаунтів співробітників компаній, в тому числі керівництва. Загроза особливо актуальна для компаній, які регулярно здійснюють великі грошові перекази на адресу контрагентів, партнерів, оскільки зловмисники можуть - нібито від імені довіреної особи - просити уповноважених співробітників компанії-жертви оплатити рахунок за підставним реквізитами. Приклади подібних атак вже відомі.

Література:

1. https://www.tadviser.ru/
2. https://www.microsoft.com/uk-ua

Рижкова С. А.,
старший викладач кафедри адміністративного права, процесу та адміністративної діяльності
Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розгляд даної теми є досить актуальним, бо в епоху інформатизації суспільства потреба Національної поліції у вдосконалення рівня інформаційної безпеки дійсно виступає на перший план. Саме за допомогою підвищення уваги до такого роду безпеки поліція зможе ефективно протидіяти кіберзлочинності та знайти нові рішення проблем, які чітко пов’язані з інформаційною безпекою.

Інформаційна безпека – це стан захищеності системи обробки і зберігання даних при якій забезпечується конфіденційність певної інформації, яка має певне значення, тому захищається від використання та оприлюднення деяких персональних даних [1].

У ЗУ” Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” визначено, що інформаційна безпека захищає найважливіші інтереси не тільки суспільства, алей і держави, при якому запобігається нанесення шкоди певного роду інформації, яка реально може бути необхідною та потрібною у різних ситуаціях [2].

Безпека інформації Національної поліції має формуватися з урахуванням комплексного підходу до яких будуть застосовані системи захистів для відвернення чи припинення інформаційних атак, які

можуть спричини реальну загрозу у вигляді втрати важливої інформації, що може негативно вплинути на певні суспільні відносини, які не можуть бути здійсненні без інформаційних даних [3].

Однією з основних проблем є те, що кожного року інформаційні ресурси набувають нового прогресивного стану, тому й з тим самим й інтерес до конференційної інформації з боку кіберзлочинців зростає у великій прогресії, тому основним завданням поліції є не допустити втрату персональних даних, які так важливі для держави.

Основний портал поліції, який потребує захисту є інформаційний портал Національної поліції України відповідно до наказу МВС від 03.08.2017 № 676, "Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»", який зберігає в собі визначення щодо, серверів, додатків, шлюзових серверів, які потребують інформаційному захисту, бо можуть в собі містити інформацію з обмеженим доступом [4].

Інформація з обмеженим доступом – це інформація, яка містить в собі інформацію з обмеженим колом осіб і оприлюднення якої заборонено розпорядженнями або законодавчими актами. Відповідно до цього існує наказ МВС від 27.05.2016 № 432 "Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України" в цьому наказі наведено вичерпний перелік інформації з обмеженим доступом, який входить до сфери охорони Національної поліції України [5].

Звісно, що інформація, яка має обмежений доступ не в повному обсязі зберігається у паперовому вигляді. Існують документи, які потребують обміну між відомствами. Наприклад, Служба Безпеки України дає запит на інформацію, яка міститься у Міністерстві внутрішніх справ України. Звісно, що це регламентовано низкою наказів, які дозволяють обмінюватися інформацією, але чи повністю ця інформація захищена у значені інформаційної безпеки. Зрозуміло, що людина, яка працює з такою інформацією проходить певний відбір та огляд на психофізіологічний стан аби людина могла тримати інформацію при собі та не розповсюджувати її. Інше питання чи звісно в інформаційному просторі інформація захищена [6].

Якщо мова йде про захист інформації, то підключається Департамент кіберполіції, який за умови складнощів у зберіганні, обміні, захисті інформації зможе допомогти, якщо це необхідно. Кіберполіція (Департамент кіберполіції Національної поліції України із підпорядкованими підрозділами) – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та, відповідно до законодавства України, забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Даний підрозділ саме служить для того аби захистити інформацію з обмеженим досвідом накладаючи шифри, коди, блокування, антивіруси на програмне забезпечення Національної поліції, яке має важливе значення [7].

Отже, можна зробити висновок, що значення інформаційної безпеки в діяльності Національної поліції відіграє значну роль, бо захист інформації виступає важливою складовою у роботі поліції. Потрібно усвідомлювати, що вся інформація, яка захищається поліцією не повинна потрапити до рук кіберзлочинців або піддатися їх задумам у корисливих цілях. Тому методи та засоби, які застосовує поліція повинні робити все можливе для того аби робити захищеність даних бездоганною.

Література:

1. Основні поняття інформаційної безпеки //URL: https://sites.google.com/site/osnovuib/ (дата звернення 14.11.2020).
2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 06.02.2007 // URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 14.11.2020).
3. Деякі питання інформаційної безпеки діяльності територіальних органів поліції //URL: file:///C:/Users/%D0%9F%D0%B0%D0%B2%D0%B5%D0%BB/Downloads/SrjGk4gk4LmLNWQ-nZsDgWi-xrEqbbLk.pdf (дата звернення 14.11.2020).
4. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ 03.08.2017 № 676 //URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення 14.11.2020).
5. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України: Наказ //URL: https://zakon.rada.gov.ua/rada/show/v0432320-16#Text (дата звернення 14.11.2020).

6. Департамент внутрішньої безпеки //URL: https://mvs.gov.ua/ua/pages/Departament-vnutrishnoi-bezpeki.htm (дата звернення 14.11.2020).
7. Що таке кіберполіція? // URL: https://tribuna.pl.ua/news/shho-take-kiberpolitsiya/ (дата звернення 14.11.2020).

Хомин О. Й.,
професор кафедри соціальних дисциплін факультету №3 ІПФПНП Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

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

АЛГОРИТМІЧНЕ МОДЕЛЮВАННЯ ФАКТОРІВ ДЕМОГРАФІЧНОЇ БЕЗПЕКИ

Становлення факторів демографічної безпеки розпочинаємо з аналізу основних чинників і причин їх виникнення. Основні причини (чинники) поділяємо на дві категорії важливості – стимулятори та дестимулятори.

До стимуляторів відносимо: коефіцієнт приросту населення в ‰, очікувана тривалість життя при народженні, сумарний коефіцієнт народжуваності, брутто коефіцієнт відтворення, соціальні гарантії, охорона здоров'я, освіта та інші.

До дестимуляторів демографічної безпеки відносимо: коефіцієнт смертності в ‰, коефіцієнт дитячої смертності ‰, частка населення похилого віку, в загальній чисельності населення у %, коефіцієнт старіння, демографічне навантаження непрацездатного населення на працездатне у %, коефіцієнт міграційного приросту, скорочення, рівень корупції, тіньової економіки та злочинність.

Дослідження розпочинаємо з описового алгоритму, для кращого розуміння і пояснення складних процесів.

Оцінка ефективності моделювання словесним алгоритмом у вербальній формі. Алгоритм описує порядок дій, що необхідно впровадити для досягнення поставленої мети – мінімізації загроз демографічної безпеки. Такий алгоритм може бути ефективним оперуючи двома-трьома показниками, які ми можемо в описовій формі виразити, уявити та надати як рекомендації до простих характеристик демографічної безпеки. Наприклад, законодавче наказати людям «помирати у віці не нижче 85 років», заборонити виїжджати за межі країни та наказати народжувати дітей. Використовуючи статистичні дані, а саме чисельність жінок фертильного віку ми можемо розрахувати і можемо точно визначити через скільки десятиліть ми досягнемо 52 млн. населення. Але надто складні процеси у суспільстві, не дозволяють використовувати цей алгоритм.

Як бачимо словесний алгоритм є поверхневий і в нашому випадку кумедний, тому використовувати його в дослідженні недоцільно, оскільки показники народжуваності, смертності є набагато складнішими процесами в українському суспільстві;

Наступним етапом ми пропонуємо побудову алгоритму у вигляді рисунків, картин, що характеризують показники демографічної безпеки.

Як бачимо, ця модель алгоритму більш ефективно пояснює основні показники, що необхідні для демографічної безпеки населення. Але процеси, що відбуваються в державі та суспільстві залежить не тільки від наявності певних характеристик добробуту чи рівня життя населення. Так, аналізуючи довільно взятий з рисунка показник ми можемо сказати наскільки складні характеристики та залежності його від інших додаткових показників.

Процеси, які відбуваються в українському суспільстві показують, що основний показник (вік, стать) часто стає другорядним, або частиною іншого показника (рівень оплати праці). Наприклад якщо немає грошей – не купиш житло, не маєш роботи – не маєш грошей. Або не маєш достатнього рівня заробітної плати – недостатня кваліфікація (освіта).

Даним алгоритмом у зв'язку із складністю процесів у суспільстві та із викликами часу неможливо пояснити всі складні нюанси процесів демографічної безпеки;

Досліджуватимемо демографічні процеси за допомогою ієрархічної моделі. Ієрархічну модель ми наповнюємо кількісними і якісними показниками за допомогою котрих ми можемо контрасно виразити рівень демографічної безпеки. При складанні цього алгоритму слід пам'ятати, що людина

живе в суспільстві. І для забезпечення безпеки всіх верств населення (працівників, дітей та непрацюючих) держава повинна мати ресурс, який вона має отримувати від працюючого населення.

При вивченні цього алгоритму проводимо паралельні дослідження про ефективність діяльності особи у суспільстві, а точніше про коефіцієнт ефективності особи в державі. Також виникає необхідність формування менталітету людини.

Однак, як бачимо, для дослідження більш глибших і складних процесів у суспільстві ця модель є недостатньою.

Значно кращий підхід у дослідженні демографічної безпеки - у вигляді побудови алгоритмічних схем. Основною перевагою блок-схемного алгоритму є блок умов If (якщо). В результаті виконання чи невиконання умови на виході отримуємо логічну функцію так, або ні (запитання: Чи впливає на здоров'я якість продуктів харчування?). Отримуємо відповідь так, або ні, змінюючи коефіцієнт якості продуктів на вході функції. Звідси випливає інший алгоритм – які технології виготовлення продукції і якість сировини? Потрібно також брати до уваги якість води, повітря та інших екологічних показників.

Перевагою блок-схеми є те, що умови ми можемо ставити для будь якого показника, функцію якого потрібно відгулювати чи коректувати для досягнення позитивного результату.

Наступним кроком є дослідження демографічної безпеки реляційною моделлю. Вона найкраще представляє статистичні цифрові дані, що характеризують кількісні та якісні показники рівня життя, а відповідно демографічної безпеки.

Реляційну модель (таблиці із статистичними даними) легко перетворити в графічний матеріал. Недоліком є те, що не можна наочно показати складну комплексну функцію процесів у суспільстві та дати відповідь на питання які поставленні перед дослідником. Перевагою аналізу за допомогою реляційної моделі є те, що це дає можливість на її основі створити функцію користувача на алгоритмічній мові Visual Basic for Application (VBA). При цьому розрахунки формул можна виконувати та відображати в табличному процесорі EXCEL не тільки за допомогою вбудованих функцій, але і за допомогою функцій, запропонованих користувачем, тобто використовувати вже визначені формули демографічної безпеки як і виводити нові.

Враховуючи необхідність частого звернення до ручних підрахунків та великого масиву демографічної цифрової інформації проводимо автоматизацію системи розрахунків створюючи спеціальне, авторське програмне забезпечення на мові Visual Basic for Application.

При дослідженні характеристик та причин виникнення факторів демографічної безпеки, а особливо мінливих, автори використали п'ять штатних підходів до аналізу. В результаті досліджень, у зв'язку із складністю процесів та відсутності формул для оперативного розрахунку написано програмне забезпечення. Створене програмне забезпечення дозволяє проводити операції із значеннями в довільному порядку. Проводити розрахунки з вибіркою даних, усереднення по роках та інше.

Основною перевагою створеного програмного забезпечення є можливість моделювання прогнозу стану демографічної безпеки по роках з можливістю порівняння її з реальними даними. Так, наприклад, ми можемо використати дані з 1990 року і створити прогноз на 2010, та порівняти з реальним станом прогнозованої та реальної картини демографічної безпеки такої, яка вже відбулася.

Таким чином проводиться тестування створеного оригінального програмного забезпечення. Авторське програмне забезпечення дозволяє прогнозувати від будь якої точки років до довільної, наприклад до 2040 року. Як показала практика тестування програми, достовірність отриманих даних при порівнянні з реальними підтверджується даними минулих років. Ще одним важливим позитивним фактором та перевагою є відсутність людської суб'єктивності при оцінці та помилки при складних математичних підрахунків.

Луців І. І.,
аспірант кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У КОНТЕКСТІ НАДАННЯ ПУБЛІЧНИХ ПОСЛУГ

У даний час відбувається цифровізація всіх сфер діяльності людини. Сучасні інформаційні технології застосовуються в соціально-економічній та науковій діяльності, використовуються для

забезпечення потреб органів державної влади, юридичних і фізичних осіб, у наданні публічних послуг державними та комунальними організаціями. Їх роль полягає в отриманні відомостей про осіб, предмети, факти, події, явища та процеси на базі інформаційних систем і мереж, які здійснюють формування та обробку інформаційних ресурсів, видачу користувачеві документованої інформації передбаченою чинним законодавством у сфері надання адміністративних послуг.

Основою державного регулювання в галузі створення та використання інформаційних технологій і засобів забезпечення є формування та розвиток програмної, технічної частини, створення повноцінної інформаційної інфраструктури цифрового суспільства.

В Україні у контексті Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони реалізується багато програм, спрямованих на розвиток і широке застосування інформаційно-комунікаційних технологій в різних сферах діяльності суспільного життя, передусім у наданні публічних послуг [1]. Реалізація даних програм проходить на державному і місцевому рівні.

Проводиться широкомасштабна реалізація проектів по створенню цифрової інфраструктури державних органів з цілю забезпечення автоматизованого інформаційного обміну між ними на базі формування єдиного національного інформаційного простору, що охоплює усі сфери адміністративних (публічних) послуг, що надаються державними та комунальними організаціями. Відбувається приєднання до міжнародних інформаційних мереж.

Розробляються категорії інформаційних ресурсів, які мають державне значення, здійснюється їх державна реєстрація. Проводяться науково-дослідні роботи зі створення передових інформаційних технологій і програмного забезпечення, сучасних способів і методів захисту інформації в рамках відповідних державних програм. Однією з основних нормативних актів у даній сфері є Стратегії розвитку сфери інноваційної діяльності на період до 2030 року [2]. У стратегії розглянуто формування єдиного системного підходу держави до розвитку галузі інформаційних технологій. Реалізація даної стратегії дозволить закласти основи подальшої діяльності держави у галузі комплексного розвитку галузі інформатизації, у тому числі за рахунок взаємодії її учасників.

У даній стратегії під галуззю інформаційних технологій розуміється сукупність компаній, які здійснюють певні види діяльності, такі як:

- розробка тиражного програмного забезпечення;
- надання послуг в сфері інформаційних технологій, зокрема замовна розробка програмного забезпечення, проектування, впровадження та тестування інформаційних систем, консультування з питань інформатизації;
- розробка апаратно-програмних комплексів з високою доданою вартістю програмної частини;
- дистанційна обробка і надання інформації, в тому числі на сайтах в інформаційно-телекомунікаційній мережі Інтернет.

Відповідно до даної стратегії масштаб впливу галузі інформаційних технологій на державу значно перевершує галузеві ефекти. Розвиток інформаційних технологій є одним з важливих факторів, які сприяють вирішенню ключових завдань державної політики України. Зазначене знайшло відображення у Законі України «Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі» [3].

При реалізації заходів цієї стратегії має підтримуватися середній темп зростання галузі інформаційних технологій на рівні, що значно перевищує середній темп зростання валового внутрішнього продукту. Планується збільшити кількість високотехнологічних робочих місць в галузі інформаційних технологій до 2030 року, забезпечити зростання обсягу виробництва продукції та послуг у сфері інформаційних технологій.

У розглянутій стратегії одним з важливих напрямів відзначається повсюдний перехід на мобільні пристрої.

В Україні такий перехід продовжиться протягом всього терміну дії цієї стратегії. Серед інших тенденцій відзначається зростання користувальницького попиту на інтелектуальні пристрої та інтернет-сервіси з доступом до публічних послуг. Наголошується на необхідності збільшення державного замовлення, так, як глобалізація ринку інформаційних технологій і висока конкуренція між країнами впливає на розвиток робочих місць для фахівців і компаній інформаційної галузі.

Згідно з даними, характер розвитку інформаційної галузі обумовлюється сукупністю світових і локальних тенденцій. Серед них: упровадження засобів інформатизації в державне регулювання в надання публічних послуг. У найближчі роки збільшиться обсяг впровадження інформаційних технологій публічні послуги в соціально-економічній сфері, державному управління та бізнесі, що буде впливати на зростання продуктивності праці і якість життя населення.

Необхідно підвищувати ефективність технологічних, виробничих і управлінських процесів кожної галузі економіки за рахунок доступності на економічності надання публічних послуг.

Згідно з прогнозом темпів зростання ринку інформаційних технологій, певний потенціал має сегмент розробки програмних засобів для надання публічних послуг. Найближчим часом планується активне впровадження розробок в органах державної влади у даному секторі державної діяльності. Відповідно буде збільшуватися попит на інформаційні технології. Перспективними напрямами розвитку інформаційних технологій в сфері надання публічних послуг стануть: хмарні обчислення, мобільні додатки, інформаційна безпека.

Зміни у сфері інформаційних технологій відбуватимуться в бік збільшення частки послуг в електронній формі та частки ринку програмних засобів для даної сфери, що забезпечує необхідний рівень інформаційної безпеки, в тому числі за рахунок створення сучасних засобів реагування та попередження інформаційних загроз.

Література:

1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII / *Відомості Верховної Ради України*. 2014. № 40. Ст. 2021.
2. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року : Розпорядження Кабінету Міністрів України від 10.07.2019 р. № 526-р. Законодавство України. URL. https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text
3. Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі : Закон України від 03.11.2020 р. № 943-IX. Законодавство України. URL. https://zakon.rada.gov.ua/laws/show/943-IX#Text

Mikhalieva M.,
PhD, Hetman Petro Sahaidachnyi National Army Academy, Department of Electromechanics and Electronics

Shabatura Yu.,
professor, Hetman Petro Sahaidachnyi National Army Academy, Department of Electromechanics and Electronics

Atamanyuk V.,
PhD, Hetman Petro Sahaidachnyi National Army Academy, Department of Electromechanics and Electronics

Koziar O.,
Cadet, Hetman Petro Sahaidachnyi National Army Academy

Gavrylenkoенко V.,
Cadet, Hetman Petro Sahaidachnyi National Army Academy

NEW TECHNICAL METHOD OF TESTING FOR QUALITY OF ROCKET FUEL

In many areas of human activity, technical assessment of the risks that depend on the use of devices is relevant. The need to perform our research, educated in improving the methods and techniques of operational control of automated hardware used by multicomponent systems. In addition to long-term laboratory (with a methodological error of more than 60%) control methods, there are electric. Electrical methods, where the informative parameter is the specific conductivity, are used in portable devices - testers, where the informative parameter of measurement is the specific conductivity, which can not always be described in full warehouses.

The quality of jet fuel (composition according to brands) is another necessary control indicator that needs to be studied during the operation of military equipment. The electric method chosen by us, and the methods developed in the future allow to control its structure not in laboratory conditions.

The study is based on the analysis of modern methods of fuel control used by NATO countries, to create ways to determine the qualitative and quantitative composition of liquids, which due to the new electric method would quickly control the content of controlled substances in the liquid. This method is selective, express and simpler than the existing ones. The problem is solved by measuring the conductivity of the liquid by a capacitive transducer. This measurement differs in that the dependence of the active and reactive components of the conductivity of the solution of the reference sample on the frequency of the electromagnetic field in the range of 50Hz ÷ 100Hz.

Based on the obtained research results, scientific facts have been obtained that allow to develop improved National Standards on metrological testing methods in the Armed Forces of Ukraine, which are adapted and harmonized to NATO requirements. Tasks for implementing NATO standards in the activities of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, other components of the Defense Forces are defined by legislation (Law of Ukraine "On National Security of Ukraine") and strategic defense documents of Ukraine (National Security Strategy of Ukraine, Strategic Defense Bulletin, Military Doctrine of Ukraine).

The study of electrical parameters of liquids in an electromagnetic field of different frequencies and the study of new designs of primary transducers allows to obtain information about their composition in non-laboratory conditions in a short period of time. The developed methods consist in measuring the component of complex conductivity of liquid and comparing it with the laboratory established component of conductivity by simulation modeling. We studied the electrical properties of model fluids, which are close to the composition of technical fluids and are used in military equipment.

That is, the object of the study is the dependence of the complex conductivity - the admixture of a mixture of jet fuel in a different frequency electromagnetic field on the composition (quality).

As a result of studies of model mixtures, it was found that the graphical dependences of the reactive component on the field frequency corresponding to liquids without the presence of a controlled substance or with only a lower concentration than normalized, will be placed below or to the right relative to such dependence for standard solution. Graphical dependences corresponding to complex liquids with the content of the controlled substance of concentration higher than normalized are placed above the sample.

This means that the presence of ions of the element, even at low concentrations in the conditions of the same name of the electrode materials significantly increase the value of the component of the complex conductivity of the multicomponent aqueous mixture. On the basis of experimental results and the made conclusions the possibility of operative identification of the controlled substance is established: definition or control (more or less) of its concentration in difficult liquid mixes which are technical liquids.

The subject of the study is liquid fuel for jet engines, which must be controlled during operation. The simplicity of the design allows fast automated execution of mass analyzes for a wide range of controlled substances. The described methods using new designs of primary transducers make it possible to automate the express control of the composition of liquids and can be used in real working conditions.

The novelty of the proposed method and method is based on the use of new scientific facts in the field of dielectric research of high-resistance and low-resistance liquids. Based on the obtained results, the authors of the research plan to develop improved National Standards on Metrological Testing Methods of Technical Fluids in the Armed Forces of Ukraine, which are adapted and harmonized to NATO requirements.

Practical implementation. On the basis of scientific researches the method and methods of operative control of structure of technical multicomponent mix - liquid jet fuel based on dependence of value of active and reactive component of conductivity on signal frequency (imitation method) are offered.

This method allows to estimate the composition of the liquid for up to 2 seconds in non-laboratory conditions and to ensure uninterrupted operation of the equipment, which will be introduced in the new national standards. The implementation of NATO standards and their improvement with new developed methods ensures a systematic increase in the combat capability of troops, achieving interoperability with the forces and means of the world's leading countries, and enhances the efficiency of the use of state resources in the field of defense.

Our research is currently at the stage of testing the operation of models, components, transducers and elements of the measuring information system.

Література:

1. Mikhalieva M., Odosii L., Shabatura Y., Lunkova H., Hots N., Przystupa K., Atamaniuk V. Electrical Method for the Cyberphysical Control System of Non-Electrical Objects / M. Mikhalieva, L. Odosii, Y. Shabatura, H. Lunkova, N. Hots, K. Przystupa, V.Atamaniuk // Przeglad Electrotechniczny. – Vol 2019, No 11. – pp.200–203.

Орлов Р. Р.,
здобувач вищої освіти Харківського національного університету внутрішніх справ

Грищенко Д. О.,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ.

ОСНОВНІ АСПЕКТИ ФОРМУВАННЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ

В даний час актуальною темою для обговорення стає забезпечення інформаційної безпеки в вузі. Кількість загроз постійно зростає, що призводить до необхідності зміни методів і способів забезпечення навчального процесу. Неможливо в системі вищої професійної освіти обійтися без застосування інформаційних технологій, які використовуються, як в самому освітньому процесі, зберіганні інформації, так і для передачі інформації від викладача до студента. Необхідно відзначити, що останнім часом в вузах розвинена система інтернет-тестування, а також повсюдно впроваджуються і використовуються сучасні дистанційні технології навчання студентів заочників. Будь-яке втручання в інформаційну систему може привести до небажаних наслідків, які позначаться на якості освітнього процесу в цілому. З точки зору забезпечення інформаційної безпеки, вуз відрізняється рядом таких особливостей, як:

- величезний потік інформації, що циркулює в інформаційному середовищі;
- великі території, які займає вуз;
- велике скупчення людей, більшість з яких студенти - молоді люди у віці від 18 до 23 років, а з точки зору захисту інформації саме ця категорія людей є найбільш вразливою;
- наявність в інформаційному середовищі різних напрацювань в області наукової діяльності, що представляють собою інтелектуальну власність і т. д.

Перераховані вище особливості призводять до неконтрольованого зростання кількості вразливостей, збільшення числа загроз з боку зовнішніх і внутрішніх зловмисників і, відповідно, важко передбачуваним потенційним матеріальним, фінансовим, моральних та інших видів втрат.

Особливу увагу необхідно приділити організації дистанційного навчання. На сьогоднішній день існує ряд загроз і ризиків, боротьба з якими сприятиме не тільки ефективному забезпеченню інформаційної безпеки, але і організації якісного та конкурентоспроможного процесу в дистанційному навчанні. На думку спеціалістів можна виділити наступні типові загрози нормальному функціонуванню системи електронного навчання:

- неавторизований доступ до цифрового контенту, включаючи фізичний доступ до серверів;
- порушення цілісності і неадекватність навчальних ресурсів (часто електронні навчальні посібники, поряд з ресурсами Інтернету, є основними джерелами навчальної інформації для студента);
- порушення безпеки процедур тестування і електронних іспитів (проблеми ідентифікації студентів, списування, плагіату та адекватного функціонування системи оцінювання знань);
- порушення нормального функціонування служб і сервісів навчального закладу [3].

Звідси можна виділити основні сервіси безпеки, які повинні застосовуватися для побудови повноцінної системи захисту інформаційного середовища і організації дистанційної освіти:

- конфіденційність;
- аутентифікація;
- цілісність;
- неможливість відмови;
- контроль доступу;
- доступність.

Дані сервіси реалізуються механізмами безпеки, а саме алгоритмами симетричного, асиметричного шифрування та хеш-функціями.

Другим важливим питанням є забезпечення безпеки деякої інформаційної системи, до якої необхідно запобігти небажаному доступ або налаштувати тимчасової доступ з чітким зазначенням періодів.

В даному випадку слід керуватися сервісами безпеки, які умовно можна розбити на дві лінії захисту:

- перша лінія, так звана «сторожова», спрямована на запобігання атак (різні міжмережеві екрани);
- друга лінія складається з різноманітних внутрішніх моніторів, контролюючих доступ і аналізують діяльність користувачів вже допущених в захищену інформаційне середовище користувачів.

При використанні даних сервісів і механізмів існує момент, коли аутентифікація за допомогою пароля або загального секрету захищає двох або більше учасників взаємодіючих в захищається інформаційному середовищі від порушників, але не захищає від порушення здійснюваного один перед одним (як варіант порушення - використання чужих наукових праць). У цій ситуації необхідно застосувати більш дієвий спосіб, ніж аутентифікація на основі загального секрету. Як варіант вирішення даної проблеми можна запропонувати використання електронно-цифрового підпису.

Дана підпис повинна володіти обов'язковими властивостями такими як:

- ЕЦП повинна використовувати унікальну інформацію відправника;
- ЕЦП повинна залежати від повідомлення, яке вона запевняє;
- ЦП повинна легко генеруватися і перевірятися.

Значне збільшення за останні роки застосовуються інформаційних технологій в діяльності вузу і, як наслідок, розширення інформаційного простору повинні істотно розширити методи і способи, що регулюють питання інформаційної безпеки. Оптимальним вирішенням питання при створенні захищеного інформаційного середовища ВНЗ і організації дистанційної освіти є використання засвідчувальних центрів, що забезпечують за допомогою електронно-цифрового підпису і захищених каналів зв'язку вирішення завдань щодо забезпечення належного рівня безпеки.

Таращук І. В.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

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

МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»

Існуюча інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – ІПНП) призначена для інформаційно-аналітичного забезпечення діяльності Національної поліції України, наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до єдиної інформаційної системи МВС (далі – ЕІС МВС), забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу та електронної взаємодії з МВС, першими органами державної влади. Однак існуюча сьогодні система не цілком задовольняє зрослі вимоги щодо оперативності, надійності й захищеності. Тому виникає актуальне завдання модернізації системи ШНП, яке досліджується в цій доповіді .

Метою модернізації (побудови) системи ІПНП є створення високонадійної, сучасної програмно-технічної інфраструктури поліції, що сприятиме захисту конституційних прав і свобод громадян та інтересів держави, суттєвому недосконаленню інформаційного забезпечення поліції інформаційній взаємодії правоохоронних та інших державних органів у сфері боротьби зі злочинністю, що забезпечить:

- підвищення:
  1. Надійності та ефективності;
  2. Повноти й достовірності обліку інформації, утвореної у процесі діяльності поліції;
  3. Оперативності інформаційної взаємодії між центральним та регіональними органами поліції;

- формування інформаційних ресурсів ЕІС МВСВ;
- надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС та інших органів державної влади у випадках, не визначених законодавством;
- генерацію інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції, суб'єктів системи ІІПНП з іншими органами державної влади, органами правопорядку іноземним держав, міжнародними організаціями;
- надання пошукових та аналітичних сервісів для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та других органів державної влади в межах службової діяльності відповідно до рівня доступу повноважень за запит або регламентом;
- упровадження оброблення біометричних даних для можливості проведення портретної (ідентифікації осіб, формування та використання дактилоскопічної інформації, в тому числі ДНК-профілів;
- використання програмних компонентів геоінформаційніх систем для візуалізації інформації у відеоелектронних карт, автоматичної зміни збережений образу об'єкта залежних від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;
- автоматизацію процесів управління силами та засоби поліції;
- запровадження електронного документообігу в органах (підрозділах) полці, обмін електронними документами з МВС та іншими органами державної влади;
- захист інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП;
- зниження витрат на експлуатацію та підтримку системи за рахунок уніфікації та спрощення використання її складових [2].

У доповіді розглянуто структуру системи ІПНП та основні вимоги до її функціонування.

Система ІПНП відповідно до Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» повинною включать: центральний ПТК; Автоматизовані робочі місці; телекомунікаційну мережу доступу та комплексну систему захисту інформації з підтвердженою відповідністю.

Центральний ПТК ШЕП повинен включати територіально рознесені основний (ЦОД-1) та резервний центри обробки даних (ЦОД-2).

Автоматизовані робочі місця користувачів - робочі місця поліцейських та інших працівників поліції, обладнані комп'ютерною технікою, в тому числі планшетними комп'ютерами, що підключені до телекомунікаційної мережі доступу системи ІПНП призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП [3, с. 347].

Телекомунікаційна мережа доступу сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації в телекомунікаційній мережі (Єдина цифрова відомча телекомунікаційна мережа Міністерства внутрішніх справ України, канали передачі даних) використовуються засоби технічного та криптографічного захисту інформації з підтвердженою.

Система ІПНІП повинна забезпечити підвищення ефективності діяльності персоналу підрозділів за рахунок:

- оперативності, достовірності, повноти, доступності та багатоваріантності автоматизованого обліку, оброблення, накопичення, передавання та подання облікової, оперативно-розшукової та довідкової інформації;
- постійного автоматизованого контролю за виконанням службових обов'язків користувачами системи.

Література

1. Про Національну програму інформатизації: Закон України від 04 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 181.

2. Сазонець О. М. Інформаційні системи і технології в управлінні зовнішньоекономічною діяльністю [текст] : навч. посіб. / О. М. Сазонець. – К. : Центр учбової літератури, 2014. – 256 с.

3. Сучасні інформаційні системи і технології: конспект лекцій / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова, В. В. Карасюка. – Х.: Нац. юрид. ун-т ім. Ярослава Мудрого, 2014. – 347 с.

Сидор В. В.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

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

ДО ПИТАННЯ ЗАСТОСУВАННЯ СТ. 361 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ У КОНТЕКСТІ ДІЯЛЬНОСТІ ХАКТИВІСТІВ

Упродовж останніх років спостерігається вплив волонтерських та громадських структур у допомозі державним структурам у різних напрямах забезпечення безпеки держави. Особливо ця допомога була помітною у перші роки конфлікту на Донбасі. Не стала виключенням і кібербезпека. Зокрема, українські хакери проводили взломування інформаційно-телекомунікаційних систем терористів та їх російських кураторів; отримували доступ до їх поштових скриньок; відслідковували акаунти у соціальних мережах та мережі Інтернет, за допомогою яких терористичні угрупування вели агітаційну діяльність та збір коштів; надавали допомогу у ідентифікації осіб, які брали участь у збройному протистоянні проти операції об'єднаних сил тощо.

Незважаючи на те, що такі дії здійснюються в інтересах забезпечення кібербезпеки держави (що публічно декларується), потрібно констатувати, що відповідно до чинного законодавства все це є порушенням українського законодавства.

Проблема неоднозначності українського законодавства щодо діяльності у кіберпросторі проявилась в історії навколо флешмобу «Ukrainian Cyber Alliance» (UCA) (під хештегом #F*ckResponsibleDisclosure[1] який відбувся восени 2017 року [1]. На думку організаторів його мета – «громадська акція для підвищення рівня IT-гігієни» (однак за сутністю флешмоб став формою краудсорсингового пентесту державних інформаційних систем). У межах акції було знайдено уразливості у комп'ютерних системах понад десяти центральних органів виконавчої влади (у тому числі – правоохоронних органів, обласних рад, інших об'єктів, які можна віднести до критичної інфраструктури держави). Деякі зі структур звернулися до поліції із заявою щодо незаконного втручання у локальну комп'ютерну мережу.

Необхідно визнати, що відповідно до чинного законодавства дії UCA порушують ст. 361 Кримінального Кодексу України (ККУ): «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» [2]. За своєю сутністю дана стаття трактує будь-яке втручання (в т. ч. те, яке не нанесло шкоди автоматизованій системі чи комп'ютерній мережі) як злочин, оскільки внаслідок дій UCA відбувся витік інформації. Таким чином формулювання вказаної статті ККУ практично унеможливлює діяльність пентестерів за умови, якщо таке тестування заздалегідь не погоджене з об'єктом атаки.

Одним із допустимих варіантів вирішення цієї проблеми є уточнення ст. 361 з врахуванням формулювання ст. 111 ККУ «Державна зрада», в якій зазначено, що «звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання». Тобто йдеться про форму попередження органів державної влади, про дії, які можуть бути трактовані як злочин у відповідності до положень ст. 361 ККУ.

Крім того необхідно визнати, що діяльність UCA та інших хактивістів, очевидно частково підпадає під формулювання «негласна перевірка готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів», що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [3] покладено на Службу безпеки України (СБУ). При цьому ст. 361 ККУ підвідомча Національній поліції, відтак дії таких хактивістів повинні узгоджуватися з Національною поліцією та СБУ.

[1] Responsible Disclosure – форма пошуку уразливостей інформаційних систем, за якою першою про її наявність повідомляється власник системи (для того, щоб він міг її виправити) і лише з певним часовим проміжком про цю уразливість повідомляють громадськості. Концепція «Full disclosure» не передбачає паузи для інформування власника системи.

Тут треба зазначити, що негласна перевірка є складовою оперативно-розшукової діяльності (ОРД), яка у Законі України «Про оперативно-розшукову діяльність» [4] визначена як «система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів», а, відповідно до законодавства, СБУ та Національна поліція є суб'єктами проведення ОРД. Звідси випливає трудність пошуку механізму співпраці між хактивістами, СБУ та Національною поліцією.

Таким чином флешмоб UCA проявив описану проблему й обумовив необхідність пошуку її вирішення, одним з яких є уточнення положень ст. 361 ККУ з метою створення чіткого механізму який би вивів дії таких хактивістів з під дії ККУ.

Література:

1. F*ck responsible disclosure. Привет от очень злых хакеров. URL: https://petrimazepa.com/disclosure.html
2. Кримінальний Кодекс України від 5 квітня 2001 року № 2341-III. *База даних* «*Законодавство України*» / *ВР України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14/print
3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *База даних* «*Законодавство України*» / *ВР України.* URL: http://zakon.rada.gov.ua/laws/show/2163-19
4. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. № 2135-XII. *База даних* «*Законодавство України*» / *ВР України*. URL: http://zakon3.rada.gov.ua/laws/show/2135-12/

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

Гецко Ю. М.,
здобувач вищої освіти центру післядипломної освіти, заочного та дистанційного навчання Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИ ЯК АСПЕКТ ІНФОРМАЦІЙНИХ ВІДНОСИН

Ми живемо в епоху інформаційного суспільства, яка характеризується, зокрема, тим, що крім природного середовища проживання людини існує інформаційне середовище проживання, роль і значення якої зростає з розвитком засобів масових комунікацій. Це середовище надає на людину активний вплив: на формування та функціонування особистості, на духовний, інтелектуальний і психічний розвиток, стан психічного здоров'я.

Можна виділити найбільш небезпечні особливості сучасного інформаційного середовища: зміна пріоритетів у подачі інформаційних новин; суперечливість інформації про реальну обстановку та негативні наслідки; збільшення обсягів збудливою інформації; виникнення інформаційних війн. Сьогодні людина сприймає навколишнє соціальне середовище, спираючись на побачене по телевізору або прочитане в Інтернеті – і гостро постає проблема здатності людини адекватно оцінити отриману інформацію.

Засоби масової інформації пропонують іноді негативні моделі поведінки, а особа сприймає ці способи поведінки. Інформаційно-психологічна безпека особи – це стан захищеності особи і можливостей її розвитку, що забезпечує її цілісність як активного соціального суб'єкта в умовах інформаційної взаємодії з навколишнім середовищем. Вона залежить від особистісних якостей індивіда та від моральних, соціальних і правових умов в суспільстві.

В якості основної загрози інформаційно-психологічної безпеки виділяють масове поширення психологічних маніпуляцій, сутністю яких є приховане психологічне примушення. Інформаційна безпека особи і держави – це безпека соціальних систем або, в разі розгляду соціально-політичної та інформаційно-психологічної складових безпеки – безпека системи соціальних, політичних, інформаційно-психологічних відносин суспільства.

Інформаційна безпека особи і держави є для соціальної системи головною умовою інтенсивного розвитку та прогресу. Політичні можливості держав визначають сьогодні не тільки силові, а й інформаційні фактори.

Російська Федерація агресивно поширює і впроваджує, нав'язує духовні, ідейні цінності іншим державам; гальмує, трансформує і підриває духовно-естетичні засади. Цілеспрямованим інформаційним впливом можна управляти станом і поведінкою не тільки окремо взятої людини, а й колективом людей.

У науковий обіг вводиться поняття інформаційної експансії і інформаційної війни, тобто нанесення противнику збитків шляхом масового інформаційного впливу. Масштабність і потужність впливу інформаційних чинників за допомогою комунікаційних технологій на психіку людей висуває забезпечення інформаційно-психологічної безпеки в сучасних умовах на рівень загальнонаціональної проблеми.

У 2017 році була прийнята нова Доктрина інформаційної безпеки України, положення якої відповідають актуальним тенденціям у цій галузі і рівню інформаційних відносин [1].

У Доктрині інформаційної безпеки дається визначення: інформаційна безпека України – стан захищеності особи, суспільства і держави від внутрішніх і зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини та громадянина, гідні якість і рівень життя громадян, суверенітет, територіальна цілісність і сталий соціально-економічний розвиток України, оборона і безпека держави.

На сучасному етапі розширюються масштаби використання спеціальними службами Росії засобів надання інформаційно-психологічного впливу, спрямованого на дестабілізацію внутрішньополітичної та соціальної ситуації в різних регіонах світу і приводить до підриву суверенітету та порушення територіальної цілісності інших держав.

Наростає інформаційний вплив на населення України, в першу чергу на молодь, з метою розмивання традиційних духовно-моральних цінностей. Стан інформаційної безпеки в галузі освіти характеризується недостатнім кадровим забезпеченням, компетентним в інформаційній безпеці, низькою поінформованістю громадян в питаннях забезпечення особистої інформаційної безпеки.

Стратегічними цілями забезпечення інформаційної безпеки у сфері державної та громадської безпеки є захист суверенітету, підтримку політичної та соціальної стабільності, територіальної цілісності України, забезпечення основних прав і свобод людини та громадянина, захист критичної інформаційної інфраструктури.

Серед важливих завдань Доктрини інформаційної безпеки виділяються: забезпечення захищеності громадян від інформаційних загроз, у тому числі за рахунок формування культури особистої інформаційної безпеки; дотримання балансу між потребою громадян у вільному обміні інформацією і обмеженнями, пов'язаними з необхідністю забезпечення національної безпеки, у тому числі в інформаційній сфері; нейтралізація інформаційно-психологічного впливу, спрямованого на підрив історичних основ і патріотичних традицій, пов'язаних із захистом України; протидія використанню інформаційних технологій для пропаганди ідеології сепаратизму, політичної та соціальної стабільності, насильницької зміни конституційного ладу.

Держава серйозно займається проблемами інформаційної безпеки на законодавчому та на виконавчому рівнях. Це заходи щодо обмеження доступу до небезпечної інформації.

На найвищому рівні йдеться про те, що від підтримки інформаційно-психологічної безпеки особи залежить майбутнє країни, державна стабільність. Але без повсюдної підтримки на рівні навчальних закладів, на рівні сім'ї така робота не буде достатньо результативною. Особливо вразливою частиною інтернет-аудиторії є психологічно і соціально незрілі особи, в першу чергу діти та підлітки. Сьогодні говорять про Інтернет як про п'яту влади, причому для підліткової аудиторії, на відміну від дорослої, ця влада може стати абсолютною.

Коли інформація сприймається підсвідомістю, вона не обробляється, а відкладається в голові у тому вигляді, в якому була отримана. Підсвідомість не аналізує дані, але в певних ситуаціях направляє нашу поведінку згідно з тією інформацією, яка зберігається. Адже одна з головних задач пропаганди – переконати всіх, що її не існує. Безконтрольне використання Інтернет-ресурсів підлітком може змінити його в найкоротші терміни до невпізнання. Розвивати інформаційну культуру, навчати правилам Інтернет-безпеки потрібно починати з батьків, оскільки без їх підтримки всі шкільні та університетські заходи будуть малоефективними. Переважна більшість батьків не знають, чим займається в Інтернеті їх дитина.

На нашу думку, таке ставлення батьків – наслідок довіри старшого покоління до сучасних технічних пристроїв, нерозуміння того, що якщо дитина знає розташування клавіш і вміє інсталювати

операційну систему, то це зовсім не означає, що дитина вміє адекватно сприймати, обробляти і оцінювати одержувану інформацію. Це все одно, що вважати: моя дитина вміє користуватися кульковою ручкою – значить, пише без помилок. Головним завданням є ознайомлення молоді та представників старшого покоління, з технологіями реклами, з сучасними маніпулятивними технологіями такими, як нейролінгвістичне програмування, прийоми «чорного піару», «чорної риторики», щоб могли ефективно захищатися.

Заклад вищої освіти стає одним з основних суб'єктів забезпечення інформаційно-психологічної безпеки здобувачів вищої освіти майбутніх фахівців і громадян. Ця мета повинна бути досягнута шляхом формування та розвитку культури інформаційної безпеки.

Безпека людини у інформаційному просторі забезпечується, насамперед, його інформаційною культурою. Для профілактики та подолання явищ деструктивного впливу на психіку з боку інформаційного середовища необхідно вносити зміни у систему сімейного виховання, навчання в школі та вишу.

Необхідно формувати інформаційну толерантність (стійкість до впливів) у дітей і підлітків шляхом розвитку соціальної компетентності, впевненості у собі, здібностей прояви власної волі і вміння сформувати та відстоювати власну думку.

Література:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL. https://zakon.rada.gov.ua/laws/show/47/2017#Text

Морозова В. Ю.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Гіденко Є.С.,
викладач кафедри тактико-спеціальної підготовки Дніпропетровського державного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РОБОТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Сучасний стан розвитку суспільства характеризується підвищенням ролі інформаційних технологій у життєдіяльності окремої людини, суспільства і держави. На сьогоднішній день, ефективність роботи правоохоронних органів, боротьба зі злочинністю яких є основною функцією, залежить не лише від професіоналізму та освіченості працівників відповідного органу, а й від технічного та інформаційного оснащення. Без сумніву, інформаційне забезпечення правоохоронної діяльності відкриває нові можливості для попередження злочинності та сприяють ефективному і об'єктивному дослідженню усіх обставин злочину.

Зарубіжний досвід поліцейської діяльності в особливих умовах і збройних конфліктів, і антитерористичних операцій показав, що одним з найважливіших і конкретних видів оперативної підтримки є інформаційне забезпечення [3, с. 3]. На сьогоднішній день, ефективність роботи правоохоронних органів, боротьба зі злочинністю яких є основною функцією, залежить не лише від професіоналізму та освіченості працівників відповідного органу, а й від технічного та інформаційного оснащення. Варто зазначити, що інформаційне забезпечення органів поліції – це система методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань.

У період реформування усієї системи державних органів неможливо уявити якісну та своєчасну роботу підрозділу Національної поліції без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Так, зокрема, у практичній діяльності органів Національної поліції широко запроваджується обчислювальна техніка, створюються локальні мережі, автоматизовані робочі місця, які обладнані сучасними потужними персональними комп'ютерами та базами даних. Все це, у свою чергу, дозволяє полегшити роботу працівників, звільняючи їх від виконання однотипних завдань, які безпосередньо не стосуються їхньої основної функції. Окрім того,

використання інформаційних технологій дає можливість одночасному вивченню значного об'єму фактів, які стосуються відповідного завдання, яке стоїть перед державним службовцем.

Сучасними інформаційними технологіями, перш за все, є методи, виробничі процеси та програмно-технічні засоби, інтегровані з метою з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів.

Доцільно виокремити наступні види сучасних інформаційних технологій:

- інформаційна технологія опрацювання даних;
- інформаційна технологія керування;
- інформаційна технологія підтримки прийняття рішень;
- інформаційна технологія експертних систем [1, с. 396–397].

У зв'язку з масштабністю та складністю обробки інформації, що надходить до правоохоронних органів постало питання про необхідність застосування принципово нової технології збору та систематизації цієї інформації на основі прогресивних методів та засобів інформаційно-обчислювальної техніки. Інформація, яка здобувається і в подальшому використовується співробітниками правоохоронних органів, повинна бути систематизована. Так, у діяльність відповідних органів було доцільно запровадити автоматизовані інформаційні системи, які стали важливим інструментом для співробітників правоохоронних органів не лише для виконання своїх завдань, а й для боротьби зі злочинністю в цілому. Дані системи дали можливість не лише систематизувати та упорядкувати великий об'єм інформації, а також оновлювати та доповнювати її новими відомостями, необхідними для виконання службових завдань [2, с. 322].

Окрім того, здобуття знань на навичок з інформатики та обчислювальної техніки, інформаційного забезпечення професійної діяльності повинно бути одним з пріоритетних напрямів освітнього процесу.

Підсумовуючи, варто наголосити на тому, актуальність запровадження інформаційних технологій зростає у зв'язку з інтенсивним використанням комп'ютерної техніки в діяльність правоохоронних органів. Цей процес впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення працівників національної поліції, а також впровадження автоматизованих систем пошук інформації про будь-які об'єкти (особи, об'єкти, події) сприяє науковій і організаційній роботі, оптимізує збір, зберігання, систематизацію та аналіз доказів. Так звана інтеграція інформаційних технологій в діяльність органів Національної поліції України дає можливість модернізувати механізми управління та належного функціонування правоохоронних органів, а саме: своєчасно отримувати доступ до певної інформації, необхідної для виконання поставлених завдань, використовувати досягнення науково-технічної думки для оптимізації слідчих дій.

Література:

1. Варенко В. М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с.

2. Плішкін В. М. Теорія управління органами внутрішніх справ: [підручник] / В. М. Плішкін. – [за ред. Ю. Ф. Кравченка]. – К. : Національна академія внутрішніх справ України, 1999. – 702 с.

3. Узлов Д. Ю., Струков В. М. Про новий підхід до взаємодії поліції з населенням на основі сучасних інформаційних технологій // «Сучасні проблеми правового, економічного та соціального розвитку держави» : тези доп. V Міжнародної науково-практичної конференції (м. Харків, 18 листопада 2016 року) / МВС України, Харківський національний університет внутрішніх справ. – Харків, 2016. – 472 с.

Чуб А. В.,
здобувач кафедри адміністративного та господарського права Запорізького національного університету, кандидат юридичних наук

ПРАВОВІ АСПЕКТИ УЧАСТІ ОСІБ В ПРИЙНЯТТІ УПРАВЛІНСЬКИХ РІШЕНЬ У ФОРМІ ЕЛЕКТРОННИХ КОНСУЛЬТАЦІЙ З ГРОМАДСЬКІСТЮ

В Україні як демократичній державі суспільство відіграє важливу роль у формуванні внутрішньої та зовнішньої політики. Дахова І. І. зазначає, що демократія не може бути правлінням народу в

буквальному розумінні. Народовладдя передбачає створення умов для управління всіма справами суспільства не тільки від імені народу і не тільки в інтересах народу, а й здійснення цього управління самим народом [1, с. 106]. Одним з проявів цього є громадські консультації.

Автори посібника «Наші права: участь громадян в управлінні державними справами» виокремлюють такі форми проведення консультацій з громадськістю: 1) публічне громадське обговорення; 2) вивчення громадської думки. Публічне громадське обговорення на їх думку відбувається у таких формах: конференції, семінари, форуми, громадські слухання, засідання за «круглими столами», збори, зустрічі з громадськістю, робота громадських приймалень, теле- або радіодебати, дискусії, діалоги, інтерв'ю, підготовка інших матеріалів в засоби масової інформації, Інтернет-конференції, телефонні "гарячі лінії", інтерактивне спілкування в інших формах. Вивчення громадської думки реалізується через: проведення соціологічних досліджень (анкетування, контент-аналіз інформаційних матеріалів, фокус-групи), проведення експрес-аналізу коментарів, відгуків, інтерв'ю, інших матеріалів у пресі, на радіо та телебаченні для визначення позицій різних соціальних груп; запровадження спеціальних рубрик у друкованих та електронних засобах масової інформації, опрацювання та узагальнення висловлених у зверненнях громадян зауважень і пропозицій, проведення аналізу цільової інформації, що надходить до спеціальних скриньок [3, с. 21].

Однією з можливостей реалізації права особи на участь у прийнятті управлінських рішень є електронні консультації з громадськістю, які за законодавством є безпосередньою формою, на відміну від опосередкованої форми – вивчення громадської думки.

Протягом І кварталу 2020 р. 71 орган виконавчої влади у рамках консультацій з громадськістю провів 805 заходів. На обговорення виносились 786 питань, що мають суспільно важливе значення, у т. ч. 396 проектів нормативно-правових актів: міністерства провели 260 консультацій, інші центральні органи виконавчої влади – 100, обласні держадміністрації – 445 [8]. Це свідчить про високий рівень затребуваності громадянським суспільством цієї форми участі громадян у прийнятті управлінських рішень.

Консультації з громадськістю проводяться з метою залучення громадян до участі в управлінні державними справами, надання можливості для їх вільного доступу до інформації про діяльність органів виконавчої влади, а також забезпечення гласності, відкритості та прозорості діяльності зазначених органів. Зазначений спосіб участі громадян в управлінні державними справами передбачений постановою Кабінету Міністрів України від 3.10.2010 №996 «Про забезпечення участі громадськості у формуванні та реалізації державної політики» [5]. Порядком визначаються основні вимоги до організації і проведення органами виконавчої влади консультацій з громадськістю з питань формування та реалізації державної політики.

С. В. Злобін, С. О. Майданевич, Н. В. Окша та Д. В. Войтенко зазначають, що консультації з громадськістю проводяться не тільки для цілей зазначених у постанові Кабінету Міністрів України від 3.10.2010 №996, а також з метою: 1) сприяння системному діалогу органів виконавчої влади і громадськості; 2) підвищення якості підготовки та прийняття рішень з важливих питань державного і суспільного життя з урахуванням думки громадськості; 3) створення умов для участі громадян у розробленні проектів рішень влади з питань, що є важливими для суспільства; 4) врахування прав, інтересів та знань всіх зацікавлених сторін. Консультації з громадськістю надають можливість громадянам впливати на зміст рішень, що ухвалюються органами влади [3, с. 22].

П. 12 постанови Кабінету Міністрів України від 3.10.2010 №996 визначає коло питань з яких в обов'язковому порядку проводяться консультації з громадськістю у формі електронних консультацій з громадськістю щодо проектів нормативно-правових актів, які: 1) стосуються конституційних прав, свобод та обов'язків громадян; 2) стосуються життєвих інтересів громадян, у тому числі впливають на стан навколишнього природного середовища; 3) передбачають провадження регуляторної діяльності у певній сфері; 4) визначають стратегічні цілі, пріоритети і завдання у відповідній сфері державного управління; 5) стосуються інтересів територіальних громад, здійснення повноважень місцевого самоврядування, делегованих органам виконавчої влади відповідними радами; 6) визначають порядок надання адміністративних послуг; 7) стосуються правового статусу громадських об'єднань, їх фінансування та діяльності; 8) передбачають надання пільг чи встановлення обмежень для суб'єктів господарювання та інститутів громадянського суспільства; 9) стосуються присвоєння юридичним особам та об'єктам права власності, які за ними закріплені, об'єктам права власності, які належать

фізичним особам, імен (псевдонімів) фізичних осіб, ювілейних та святкових дат, назв і дат історичних подій; 10) стосуються витрачання бюджетних коштів (звіти головних розпорядників бюджетних коштів за минулий рік) [5]. Водночас Міністерство юстиції України наголошує на тому, що на обговорення виносяться не лише проекти нормативно-правових актів, а й проблемні питання державної політики для обговорення варіантів їх вирішення (політичні документи) [6].

Строк проведення таких консультацій з громадськістю визначається органом виконавчої влади і повинен становити не менш як 15 календарних днів. Електронні консультації з громадськістю проводяться у підрубриці «Електронні консультації з громадськістю» рубрики «Консультації з громадськістю» офіційного веб-сайту органу виконавчої влади, а також на урядовому веб-сайті «Громадянське суспільство і влада» [5; 7].

Під час проведення електронних консультацій з громадськістю орган виконавчої влади оприлюднює на своєму офіційному веб-сайті та на урядовому веб-сайті «Громадянське суспільство і влада» інформаційне повідомлення про проведення електронних консультацій, текст проекту акта, винесеного на обговорення. В інформаційному повідомленні про проведення електронних консультацій з громадськістю зазначаються: 1) найменування органу виконавчої влади, який проводить електронні консультації з громадськістю; 2) назва проекту акта або стислий зміст пропозиції щодо реалізації державної політики у відповідній сфері державного і суспільного життя, винесеної на обговорення; 3) соціальні групи населення та заінтересовані сторони, на які поширюватиметься дія рішення, яке планується прийняти за результатами електронних консультацій з громадськістю; 4) можливі наслідки проведення в життя рішення для різних соціальних груп населення та заінтересованих сторін; 5) електронна адреса, строк і форма подання пропозицій та зауважень; 7) прізвище, ім'я відповідальної особи органу виконавчої влади; 8) строк і спосіб оприлюднення результатів обговорення. Пропозиції та зауваження учасників електронних консультацій з громадськістю подаються в письмовій формі на електронну адресу, зазначену в інформаційному повідомленні про проведення електронних консультацій з громадськістю, а також за допомогою спеціальних сервісів урядового веб-сайту «Громадянське суспільство і влада» та офіційних веб-сайтів органів виконавчої влади за їх наявності [5].

Згідно з аналітичними даними Єдиного веб-порталу органів виконавчої влади України за 2018 р., е-консультації є найпоширенішим методом консультування міністерств, інших центральних органів виконавчої влади та місцевих органів виконавчої влади. Більше 50 % питань, винесених на консультації з громадськістю, становлять проекти нормативно-правових актів. Найактивніше виносять питання на публічні консультації Міністерство освіти та науки України, Фонд Державного майна України та Київська міська державна адміністрація. Станом на 2018 рік Міністерствами України було проведено заходів з публічних консультацій у кількості 503, центральними органами виконавчої влади – 417, Обласними держадміністраціями – 738 [2].

За результатами публічного громадського обговорення, електронних консультацій з громадськістю органи виконавчої влади готують звіт, в якому зазначається: 1) найменування органу виконавчої влади, який проводив обговорення; 2) зміст питання або назва проекту акта, що виносилися на обговорення; 3) інформація про осіб, що взяли участь в обговоренні; 4) інформація про пропозиції, що надійшли до органу виконавчої влади за результатами обговорення, із зазначенням автора кожної пропозиції; 5) інформація про врахування пропозицій та зауважень громадськості з обов'язковим обґрунтуванням прийнятого рішення та причин неврахування пропозицій та зауважень; 6) інформація про рішення, прийняті за результатами обговорення [5].

Згідно п. 21 Постанови Кабінету Міністрів України від 3.10.2010 №996 звіт про результати публічного громадського обговорення та електронних консультацій з громадськістю орган виконавчої влади в обов'язковому порядку доводить до відома громадськості шляхом оприлюднення на своєму офіційному веб-сайті, урядовому веб-сайті «Громадянське суспільство і влада» (у разі проведення електронних консультацій з громадськістю на зазначеному веб-сайті) та в інший прийнятний спосіб не пізніше ніж через два тижні після прийняття рішень за результатами обговорення [5]. Так наприклад, Міністерством цифрової трансформації України на 2020 рік було заплановано проведення 14 електронних громадських консультацій [4]. Міністерство юстиції України на своєму сайті у розділі «Звіти про результати електронних консультацій з громадськістю» розміщує відповідні звіти. Кількість таких звітів дуже велика. а у 2020 році Міністерство юстиції України на своєму сайті розмістило 28 звітів про результати публічного громадського обговорення проектів нормативно-правових актів, а Міністерство

внутрішніх справ України – 16 звітів. Усі зауваження та пропозиції до питань, що виносяться на консультацію розміщуються у таблицях відображених на сайтах зазначених міністерств.

Водночас аналіз звіті органів публічної влади щодо проведення електронних громадських консультацій виявив низьку активність громадян та громадських організацій щодо участі у цих заходах. Процедура проведення громадських слухань дає можливість органам влади і громадянам досягти більшої взаємодовіри, уникнути непорозумінь, а також прийняти обґрунтоване рішення, що буде з розумінням сприйматися та виконуватися. Результати проведення консультацій з громадськістю не є обов'язковими при прийнятті остаточного рішення органом виконавчої влади і мають лише консультативний характер. Перевагами проведення електронних консультацій із громадськістю є низька вартість проведення такого заходу, можливість оперативно отримати та опрацювати інформацію. Тому, пропонуємо активно поширювати інформацію серед населення щодо їх можливостей участі в прийнятті управлінських рішень органами публічної влади у формі електронних громадських консультацій.

Література:

1. Дахова І. І. Участь громадян в управлінні державними справами. Форум права. 2014. №3. С. 102–109. URL: http://dspace.nlu.edu.ua/bitstream/123456789/12352/1/Dahova_102-109.pdf
2. Е-консультації, як елемент публічних консультацій. Практичне дослідження. / С. Лобойко, О. Гречко, О. Медведенко, Й. Томкова, А. Ємельянова, К. Літвінова. Київ. 2018. https://cid.center/wp-content/uploads/2019/0297.pdf
3. Наші права: участь громадян в управлінні державними справами С.В. Злобін, С.О. Майданевич, Н.В. Окша, Д.В. Войтенко; Заг. ред. Н. К. Дніпренко. Вінниця: ТОВ "Консоль", 2006. 64 с.
4. Орієнтовний план проведення консультацій з громадськістю Міністерством цифрової трансформації України на 2020 р. : затверджено Наказом Міністерством цифрової трансформації України від 26.12.2019 №31. https://thedigital.gov.ua
5. Про забезпечення участі громадськості у формуванні та реалізації державної політики: постановою Кабінету Міністрів України від 3 листопада 2010 р. № 996. Урядовий кур'єр від 11.11.2010.№ 211, № 194 від 24.10.2012
6. Рекомендації щодо змісту інформації, що оприлюднюється в рубриці «Консультації з громадськістю». URL: https://minjust.gov.ua/m/str_50623
7. Щодо проведення електронних консультацій з громадськістю на сайті "Громадянське суспільство і влада": Наказ Міністерства Юстиції України від 13.04.2009 № 324/7. URL: ttps://zakon.rada.gov.ua/laws/show/v324_323-09#Text
8. Як проводились консультації з громадськістю у І кварталі 2020 року. https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/rubrik_konsult/zvit-2020-konsul-1.pdf

Балдін С. П.,
здобувач освітнього ступеня бакалавр ФУЕБ Львівського державного університету внутрішніх справ

Балуєва С. І.,
здобувач освітнього ступеня бакалавр ФУЕБ Львівського державного університету внутрішніх справ

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

ЦИФРОВІЗАЦІЯ: ПОЗИТИВНІ І НЕГАТИВНІ ВПЛИВИ

Розвиток інформаційного суспільства стимулює формування економічної системи інформаційного типу – цифрової економіки. Цифрова економіка – це економіка, заснована на даних, мобільності, хмарних сервісах і новітніх інформаційних технологіях. Цифрова економіка продукує трансформаційні процеси економічних відносин у цифровий формат. Як тренд розвитку світової економіки і суспільства цифровізація (цифрова трансформація) впливає на різні сфери суспільства і від ступеня її впливу залежить місце кожної країни у світовому співтоваристві.

Цифровізація є безумовним драйвером сучасного суспільства, усіх його складових і дає багато переваг для зростання економіки. Розглядається як аксіома, що інвестиції в цифровий актив значно

прибутковіші, ніж у нецифровий, а сектори, пов'язані з цифровими технологіями, показують більший приріст робочої сили, ніж світова економіка в цілому. Тому і вплив цифровізації, і ставлення до неї є неоднозначним [1].

Цифровізація надає низку переваг для розвитку економіки. Технології, інтелектуальні програми та інші інновації у цифровій економіці можуть підвищити якість послуг, що надаються, і допомогти вирішити проблеми в різних областях, включно з охороною здоров'я, сільським господарством, державним управлінням, податками, транспортом, освітою, екологією та ін. [2].

Цифровізація всіх аспектів життя обумовлена, перш за все, її можливими позитивними проявами та наслідками на всіх рівнях:

- економічний і соціальний ефект від цифрових технологій для бізнесу та суспільства;
- підвищення якості життя;
- зростання продуктивності всієї суспільної праці;
- виникнення нових моделей і форм бізнесу;
- підвищення прозорості економічних операцій і забезпечення можливості їх моніторингу;
- забезпечення доступності і просування товарів і послуг як державних, так і комерційних;
- поява людинозамінних керуючих систем [2].

Технологічні переваги, обумовлені цифровізацією:

- спільне використання інформації і відсутність конкуренції у споживанні знань та інформації;
- акумулювання великих обсягів даних, здійснення їх автоматичного оброблення та аналізу;
- синхронізація потоків інформації, можливість точкового розподілу даних у рамках усього бізнесу і, як наслідок, можливість відстеження великої кількості ланцюжків між постачальниками і споживачами, проведення інтелектуальної та точкової аналітики;
- оволодіння новими технологіями на прикладному рівні;
- перехід від паперових документів до електронних [3].

До головних проблем і перешкод на шляху впровадження та розвитку цифрової економіки в Україні слід віднести:

- не досить розвинуту інфраструктуру;
- низьку технологічну освіченість, територіальну цифрову нерівність, незначну частку інновацій у цифрову економіку;
- застарілість техніки в державних структурах;
- відсутність стандартизації цілих інформаційних систем, які б гарантували інформаційну безпеку як на індивідуальному рівні, так і на рівні надання інформаційних послуг державою;
- непропорційну структуру ринку ІТ, неузгодженість стратегічного підходу до формування політик у напрямі гармонізації цифрових ринків з ЄС [4].

Для української економіки тренди цифровізації пов'язані з серйозними викликами, оскільки питання формування цифрової економіки стають для України питаннями її національної безпеки і конкурентоспроможності на світовому ринку (зовнішні виклики), а також питаннями рівня і якості життя населення України (внутрішні виклики). Відставання України за темпами і масштабами цифровізації від країн сусідів може призвести до того, що Україна опиниться на узбіччі науково-технічного прогресу, що, своєю чергою, зумовить:

- роль України у світовій економіці буде наздоганяюча;
- забезпечення національної безпеки буде поставлене під питання;
- Україна буде позбавлена перспектив інноваційного розвитку, що істотно знизить конкурентоспроможність як окремих вітчизняних компаній, так і всієї української економіки на світовому ринку [4].

В Україні на державному рівні визнається необхідність формування цифрової економіки, а цифрові технології розглядаються в якості одного з ключових драйверів сталого розвитку.

Особливість українського цифрового розвитку полягає в тому, що індивідуальні користувачі і бізнес значно випереджають державу і промисловість. Український малий і середній бізнес уже використовують ІКТ і здебільшого цифрові методи просування своїх послуг, тоді як держава і велика промисловість в Україні кардинально відстають [3].

Роль держави у впровадженні цифрової економіки розглядають як подвійну:

- як регулятора, що запроваджує норми, принципи та основи співіснування елементів цифрової економіки, здійснює технологічні зміни, що сприяють закріпленню цифрових відносин між суспільством та владою;
- держава може використовувати Internet та інформаційні технології безпосередньо під час надання своїх послуг в он-лайн-торгівлі, електронному врядуванні.

Відставання від розвинутих країн пояснюється:

- особливістю економічної моделі, в якій значне місце посідає агропромисловий комплекс;
- надто повільними темпами впровадження цифрових технологій;
- необхідністю подолання відставання в розвитку науково-технічної бази, порівняно з постіндустріальними країнами [4].

Література:

1. Четвертая промышленная революция. Целевые ориентиры развития промышленных технологий и инноваций. Информационный документ. – Всемирный экономический форум. Електронний ресурс]. URL: http://www3.weforum.org/docs/WEF_%D0%A7%D0%B5%D1%82%D0%B2%D0%B5%D1%80%D1%82%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F%20%D1%80%D0%B5%D0%B2%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D1%8F.pdf.
2. OECD Digital Economy Outlook 2017. – OECD. Електронний ресурс]. URL: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/9317011e.pdf.
3. Цифрова економіка як новітній вектор реконструкції традиційної економіки. Електронний ресурс]. URL: http://inneco.org/index.php/innecoua/article/view/305/367
4. Цифрова економіка: тренди, ризики та соціальні детермінанти. [Електронний ресурс]. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf

Апетик А. М.,
аспірантка кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

ОСОБЛИВОСТІ ФОРМУВАННЯ ТА РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ

При розгляді питань формування інформаційного простору України, були виділені наступні три підходи до осмислення поняття «інформаційний простір»:

- геополітичний підхід, розглядає під інформаційним простором віртуальну інформаційно-комунікаційну територію, що належить державі, яка виступає специфічним державним ресурсом і повинна захищатися від впливу факторів зовнішнього середовища;
- метафоричний підхід визначає інформаційний простір як простір певних інформаційних взаємодій;
- соціальний підхід передбачає розгляд інформаційного простору, як сфери відносин між людьми та спільнотами з приводу інформації.

Слід зазначити, що фахівцями у галузі інформаційних досліджень, виділені кілька напрямів аналізу інформаційного простору. У рамках одного з них інформаційний простір представлено у вигляді сукупності п'яти об'єктів: образ, знак, концепт, текст, документ. У рамках іншого напряму пропонується розгляд інформаційного простору у вигляді гіпертекстової структури, яка виступає зосередженням різноманітних образів, знаків, концептів, текстів, документів, взаємопов'язаних всілякими переходами.

Ще одна версія осмислення інформаційного простору викладена в Стратегії розвитку інформаційного суспільства в Україні яка передбачає формування та розвиток єдиного інформаційного простору України і відповідних державних інформаційних ресурсів [1]. На думку авторів концепції, Україна може виступити в ролі носія специфічної моделі цивілізаційного розвитку, яка багато в чому коректує російський еталон.

Особливостями обраного шляху України до інформаційного суспільства виступають:

- історична спадкоємність;
- національна ідентичність;
- відновлення моральної свідомості;
- утворення єдиної духовного простору країни.

Однією з проблем інформаційних відносин, виступає глобалізація інформаційного простору, так як багатьох хвилює той факт, що кордони інформаційних просторів, стають все більш і більш умовними.

Прихильники інформаційної глобалізації вказують, що поява глобального інформаційного простору означає наближення епохи економіки, яка буде характеризуватися:

- стиранням географічних кордонів ринків збуту;
- появою розподілених мережевих трудових ресурсів;
- кардинальним зближенням виробництва та споживання;
- відкриттям нових ринків у новій сфері інтелектуального споживання.

Розглядаючи проблеми глобалізації інформаційного простору, виділимо технологічний і політичний аспекти.

Технологічний аспект повинен бути реалізований за допомогою створення на всій території України адекватної інформаційно-комунікаційної інфраструктури. Вирішення проблеми глобалізації інформаційного простору, за допомогою технологічного аспекту передбачає:

- реорганізацію утворюючих систему підприємств зв'язку;
- забезпечення рівномірного розвитку територій шляхом реалізації механізму «універсальні послуги»;
- розвиток конкуренції;
- створення законодавчої та нормативно-правової бази для впровадження в Україні загальноприйнятих на світовому ринку, у світовій практиці принципів взаємодії операторів;
- формування ефективних галузевих ринків;
- перехід на загальноприйняті в світі методи тарифного регулювання загальноприйнятих послуг електричного зв'язку, розробка концепції підтримки національного виробництва у галузі інформаційних комунікацій;
- державну підтримку прискореного широкомасштабного поширення термінального обладнання для роботи в Інтернеті (особливо для шкіл, вишів, бібліотек, об'єктів соціальної інфраструктури, зв'язку, домашнього користування).

Політичний аспект проблеми глобалізації проявляється в тому, що високий ступінь інформатизації суспільства і зростаюча роль нових інформаційних технологій є показниками переходу до нового типу суспільства – інформаційного, відповідно, новим чинникам взаємодії в політико-інформаційній сфері.

Якщо раніше питання забезпечення політичної безпеки можна було вирішити шляхом обмеження доступу до інформаційних ресурсів, то сьогодні необхідно враховувати відкритість інформаційного простору та безперервну появу нових джерел інформації та способів їх функціонування.

Здатність держави забезпечити достатні інформаційні ресурси та інформаційні потоки для підтримки своєї життєдіяльності та життєздатності, сталого розвитку, функціонування та протидії інформаційним ризикам і загрозам, негативному інформаційному впливу, обумовлює можливість збереження суверенітету, цілісності кордонів держави.

Обмін інформацією та ідеями сприяють формуванню основи для взаєморозуміння та розмивання стереотипів. Розглядаючи інформаційні ресурси як інструмент в забезпеченні політичної безпеки, необхідно:

- за допомогою телебачення, мережі Інтернет, розробити образ громадянина, який прагне до активної життєвої позиції, мислячого інноваційними категоріями інформаційного суспільства, що складається в Україні;
- створити спеціалізовані експертні групи при органах влади України, у віданні яких знаходилися б політологічні дослідження, спрямовані на вивчення тенденцій у галузі інформаційних впливів і направлення інформаційних потоків.

Важливо при спробі контролю інформаційних потоків і застосування інформаційних ресурсів з метою вирішення питань забезпечення політичної безпеки дотримуватися конституційних прав і свободи людини та громадянина, основні принципи правової держави та громадянського суспільства.

Література:

1. 1. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL. https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

Баран М. В.,
аспірант кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

ЕЛЕКТРОННІ ТОРГИ В АСПЕКТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Трансформаційні процеси, що відбуваються в економіці України у контексті реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, визначаються необхідністю подолання спаду в економіці, обумовленого пандемією короновірусу. Реалізація даних завдань актуалізує постановку питання про активізацію факторів, які у дослідженнях проблем економічного зростання пов'язують із здійсненням структурних та інституційних перетворень в економіці.

У ряду даних факторів відзначається роль підвищення частки продукції, виробленої в галузях з високим ступенем переробки (доданої вартості) в структурі внутрішнього валового продукту, конкурентоспроможності продукції на внутрішньому та зовнішньому ринках, збільшення частки продукції переробних галузей в українському експорті.

Масштабність поставлених завдань визначає значення універсальних чинників зростання, що характеризують рівень технологічного розвитку галузей переробки. В умовах формування інформаційного суспільства це розробка та впровадження інновацій, які пов'язані з цінностями та інститутами постіндустріального розвитку.

Сучасний етап розвитку економіки характеризується активним впровадженням Інтернет-технологій. Сучасна система електронних торгів прийшла на зміну традиційним фінансовим аукціонам, що проводилися між різними фірмами і компаніями. Електронні торги вважаються найбільш перспективною формою проведення торгів, однак на практиці виникає ряд проблем при застосуванні.

Реалії нових форм комунікації виробників і споживачів продукції, що виходять за рамки внутрішніх ринків і охоплюють взаємодію продавців і покупців у міжнародній системі економічних цифрових зв'язків, визначають актуальність наукового аналізу сутності електронних торгів, механізмів управління та регулювання цих процесів, оцінки невизначеності та ризиків, що виникають у ході проведення.

Дослідження економічної сутності електронних торгів вимагає, перш за все, визначення цифрової економіки. Цифрова економіка це система господарських зв'язків і відносин, що виникають у виробничій діяльності суспільства, пов'язаних з особливими формами зберігання, використання та передачі інформації господарюючими суб'єктами для досягнення економічних цілей.

Як зазначається в програмних документах Кабінету Міністрів України, ключовим фактором функціонування господарської діяльності у такій економіці є дані в цифровій формі, що сприяють формуванню інформаційного простору з урахуванням потреб громадян і суспільства в отриманні якісних та достовірних відомостей, розвитку інформаційної інфраструктури України, створення та застосування інформаційно-комунікаційних технологій, формування нової технологічної основи для соціальної та економічної сфери.

Рівень освоєння основних принципів і елементів цифрової економіки в Україні у даний час є недостатнім. Це істотно знижує можливості для розвитку національної економіки.

Рівень просування економіки у цьому напрямі може бути оцінений за показником індексу мережевої готовності, запропонованого в доповіді «Глобальні інформаційні технології» на Всесвітньому економічному форумі. Згідно з цим індексом Україна посідає 43-е місце, істотно відстаючи від розвинених країн. З точки зору економічних і інноваційних результатів використання цифрових технологій, Україна займає 78-е місце з великим відставанням від країн-лідерів.

Серед причин відставання відзначається фактична непідготовленість нормативно-правового регулювання поширення цифрових технологій в країні, низький рівень інфраструктурного забезпечення, несприятливі умови ведення підприємницької діяльності у сфері інновацій, внаслідок чого бізнес-структури не використовують у діяльності ресурси цифрових комунікаційних систем.

Оцінка ролі та значення інформатизації економіки та суспільства знайшла відображення в ряді програмних документів, прийнятих Кабінетом Міністрів України.

Цілі, напрями та рівні інформатизації економіки, були конкретизовані в Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її

реалізації та Стратегії розвитку сфери інноваційної діяльності на період до 2030 року, затвердженої розпорядженням Кабінету Міністрів України [1; 2].

У даних документах сформульовані завдання з просування інформаційних технологій в економіці та соціальній сфері, використанні в діяльності підприємств різних форм власності.

Формування основних інститутів цифрової господарської системи має здійснюватися на різних рівнях у тісній взаємодії, надавати сприятливий вплив на життя громадян і суспільства. Слід зазначити роль інформаційних платформ і технологій, які сприяють формуванню компетенцій для розвитку ринків і галузей економіки.

Ще одним структурним елементом є інституційне середовище, що створює умови для розвитку платформ і технологій, ефективної взаємодії суб'єктів ринків у галузях економіки, представлене правовими регуляторами, інфраструктурою інформаційних комунікацій, кадровим забезпеченням і інформаційною безпекою.

Провідну роль в цифровому облаштуванні економічних відносин відіграють розробка, впровадження та освоєння платформ і технологій. Слід підкреслити значення регуляторів інституційного середовища і її провідників, тобто компетентних фахівців, на яких покладено відповідальність за безпечне застосування.

Вищесказане дозволяє уточнити цілі та завдання формування цифрових комунікацій в окремому сегменті відтворювального циклу – товарообмін, просторі комунікацій, що реалізуються при укладанні ринкових угод з приводу купівлі-продажу потенційних і реальних благ та послуг. По-перше, розвиток законодавства з метою реалізації нормативного регулювання електронних торгів, підготовка кадрів для організації, проведення та контролю порядку протікання торгів відповідно до вимог законодавства, створення та вдосконалення технологій використання інформаційних ресурсів. По-друге, створення основних елементів інформаційної інфраструктури та безпеки для здійснення електронних торгів.

У наукових дослідженнях проблем організації та проведення електронних торгів, реалізованих у працях економістів, основна увага приділена механізмам застосування цифрових технологій у взаємодії державних структур та приватних фірм при організації та проведенні державних закупівель.

Пріоритет даної сфери відбиває рівень поширення цифрових технологій у національній економіці. А між тим, як зазначалося раніше, необхідно їх подальше просування. Представляє інтерес досвід, накопичений під час проведення державних закупівель у формі електронних торгів. У публікаціях з даної тематики позитивно оцінюється практика проведення торгів на базі електронних майданчиків, що функціонують у даний час в економіці.

Узагальнення досвіду функціонування даних майданчиків дозволяє сформулювати важливі аспекти діяльності, які можуть мати значення для здійснення електронних торгів для більш широкого кола учасників, які виходять за рамки взаємодії державних установ і підприємств приватного сектора економіки.

У даному контексті слід говорити, по-перше, про використання даних електронних майданчиків та створення нових платформ для проведення електронних торгів, у тому числі за участю домогосподарств як покупців продукції і замовників у виробництві благ.

По-друге, можливості застосування механізму електронних аукціонів при укладенні контрактів між приватними товаровиробниками. По-третє, необхідність використання інструментарію планування торгів і важливості розробки інструментів синхронізації процедур планування, укладання контрактів і контролю їх виконання з процесами розробки та впровадження бізнес-процесів на електронних торговельних майданчиках.

Необхідне подальше підвищення ролі контролю Антимонопольного комітету України в реалізації цінової політики фірм при проведенні електронних торгів.

Література:

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

2. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року : Розпорядження Кабінету Міністрів України від 10.07.2019 р. № 526-р. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text

Тур Т. О.,
аспірант кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНЕ І ПРОГРАМНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ СУДІВ ЗАГАЛЬНОЇ ЮРИСДИКЦІЇ

Створення умов для нормального функціонування судової влади, зміцнення самостійності судів і незалежність суддів визначає зміст забезпечувальної діяльності судів. Забезпечувальна діяльність судів визначає набір вимог забезпечення умов, що визначають незалежність і самостійність правосуддя в країні. Інформаційне та програмно-технічні забезпечення діяльності судів загальної юрисдикції це сукупність методів і прийомів фінансового, інформаційного, кадрового, матеріально-технічного забезпечення, які спрямовані на створення умов здійснення правосуддя в країні.

Ефективність функціонування судової влади здійснюється на основі створення оптимальних умов для її діяльності, які включають: наявність законодавчої бази; укомплектованість професійними та кваліфікованими кадрами; оснащеність комп'ютерною та іншою оргтехнікою; інші необхідні умови відповідного забезпечення діяльності судів.

Затвердження Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки, сприяло підвищенню якості здійснення правосуддя та вдосконалення судового захисту прав і законних інтересів громадян, установ і організацій [1].

Ключовими заходами Стратегії є: будівництво, реконструкція та придбання будівель судів; інформатизація судової системи, впровадження сучасних інформаційних технологій в діяльність судів; оснащення приміщень судів технічними засобами та системами забезпечення безпеки (понад 100 будівель судів загальної юрисдикції оснащені технічними засобами та системами захисту).

Інформатизація та впровадження автоматизованих систем у діяльність судів загальної юрисдикції дозволить значно знизити порушення процесуальних строків розгляду справ і суперечок, скоротити кількість незавершених справ, підвищити якість і ефективність роботи апаратів судів.

Постанова Кабінету Міністрів України «Про визначення механізму впровадження Плану дій щодо реалізації положень Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки», включає комплекс заходів щодо розвитку інформаційно-комунікаційних технологій у Верховному Суді України та судах загальної юрисдикції [2].

У Стратегії наголошується на необхідності створення інформаційно-телекомунікаційної інфраструктури єдиного інформаційного простору Верховного Суду України та судів загальної юрисдикції, органів суддівського співтовариства, системи Державної судової адміністрації України, для вдосконалення та розвитку інформаційно-комунікаційних технологій.

Впровадження автоматизованих систем у діяльність судів загальної юрисдикції сприятиме розвитку інформаційно-комунікаційних технологій, на основі: розвитку і створення комплексу сканування і зберігання електронних образів судових документів; проведення робіт з переведення судових архівів в електронний вигляд; створення умов для електронного судочинства, що передбачає спрощення процедур подачі у суд позовних заяв, скарг в електронному вигляді, отримання копій документів і ознайомлення з матеріалами справи; створення технічних умов для забезпечення взаємодії судів загальної юрисдикції з інформаційними системами Генеральної прокуратури України, МВС України, Міністерства юстиції України, Державної пенітенціарної служби України та інших відомств в електронному вигляді, забезпечить зручний і швидкий доступ до інформації та підвищить якість і ефективність роботи апаратів суден.

Перераховані вище заходи сприятимуть забезпеченню зручного та швидкого доступу до інформації та підвищення якості і ефективності роботи апаратів судів.

Передбачається оснастити: - системами відео протоколювання ходу судових засідань 250 будівель судів загальної юрисдикції; системами аудіо протоколювання ходу судових засідань 600 залів судових засідань судів загальної юрисдикції; комплектами відео конференції зв'язку 95 відсотків судів загальної юрисдикції.

Сучасний етап соціально-економічного розвитку країни ставить перед судовою системою нові завдання, до числа яких відносяться: підвищення якості та доступності правосуддя; підвищення

авторитету судової влади; удосконалення видів судочинства, законодавчих гарантій на отримання громадянами повної та достовірної інформації про діяльність судів; розробка кримінально-правової концепції держави з метою упорядкування змін, що вносяться до кримінального та кримінального процесуального законодавства України; зміцнення кадрового складу судової системи та гарантій статусу суддів; оптимізація та нормативне визначення норм службового навантаження суддів.

Відзначимо, що зменшення службового навантаження неможливо без визначення оптимальних термінів розгляду справ, вдосконалення порядку повідомлення осіб, які беруть участь у справі, у тому числі з використанням інформаційних технологій, подальшого розвитку спрощених форм судочинства, розширення інститутів досудового та позасудового врегулювання спорів, скорочення категорій цивільних справ, за якими складаються мотивовані судові рішення.

На з'їзді суддів велику увагу представники суддівського корпусу приділили питанням фінансування судів і в зв'язку з цим було прийнято рішення про оптимізацію суддівського навантаження. Високе навантаження позначається на якості роботи суддів і може привести до порушень прав громадян та інтересів держави. Робоча група готує нормативний акт щодо норм службового навантаження суддів і працівників апаратів судів. У даний час представниками Верховного суду України та Національною академією правових наук ведеться робота з визначення норм службової навантаження.

Хотілося відзначити, що розвиток інформаційного і програмно-технічного забезпечення діяльності судів загальної юрисдикції буде сприяти скороченню порушень процесуальних строків розгляду справ і суперечок, скорочення кількості незавершених справ і забезпечить зручний і швидкий доступ до інформації, що послужить основою для підвищення якості та ефективності роботи апаратів судів.

Література:

1. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки: Указ Президента України від 20.05.2015 р. № 276/2015. URL. https://zakon.rada.gov.ua/laws/show/276/2015#Text
2. Про визначення механізму впровадження Плану дій щодо реалізації положень Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки: Розпорядження Кабінету Міністрів України від 19.08.2015 р. № 864-р. URL. https://www.kmu.gov.ua/npas/248443925

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

Хорошаєв В. Р.,
здобувач вищої освіти факультету управління та економічної безпеки Львівського державного університету внутрішніх справ

АНАЛІЗ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В ЕКОНОМІЦІ ТА БІЗНЕСІ

Останнім часом інформаційні технології стали частиною нашого життя у всіх його сферах. Існування будь-якого підприємства чи державної фінансової структури, сьогодні, важко уявити без використання сучасних інформаційних технологій, які значно підвищують ефективність процесів, дозволяють досліджувати та взаємопов'язувати складові ділянки діяльності організацій між собою.

У науково-технічній літературі інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування [1].

Інформаційні технології в економіці створюються з метою: оптимізації внутрішньої діяльності; підвищення ефективності у взаємодії з іншими органами державної влади, громадянами, підприємствами, установами, організаціями, економії часу та коштів.

Використовують інформаційні технологій і у своїй діяльності органи, які здійснюють фінансування соціального забезпечення громадян України, а саме: органи Пенсійного фонду України, соціального захисту населення, та казначейської служби.

Основними завданнями інформаційно-аналітичного забезпечення діяльності установ Пенсійного фонду України є підвищення та аналіз ефективності функціонування системи пенсійного забезпечення стосовно: надання пенсій та всіх видів соціальних допомог; контролю за правильністю призначення та виплати пенсій, допомог і компенсаційних виплат; контролю за наданням пільг; моніторингу соціальних процесів, аналізу рівня бідності та прогнозування рівня життя соціально вразливих верств населення; інформаційного обслуговування.

Система збирання, обробки та ведення інформації Пенсійного фонду складається з інформаційно-технологічних підсистем [2, 3]:

- автоматизованої системи персоніфікованого обліку внесків (СПОВ);
- автоматизованої системи обробки пенсійної документації на базі комп'ютерних технологій (АСОПД);
- системи призначення та виплати пенсій деяким категоріям громадян;
- автоматизованої системи обліку сплати страхових внесків і центрального сховища обліку сплати страхових внесків (АРМ ОССВ);
- системи реєстрації вхідної та вихідної кореспонденції (АСЕДО).

В перспективі, у сфері пенсійного забезпечення передбачається запровадження електронних пенсійних справ, створення реєстру електронних пенсійних справ та систем їх технічної підтримки, комплексної системи захисту інформації. Планується залучення для обслуговування громадян банків, відділень поштового зв'язку, об'єднаних громад з подальшим розширенням мережі таких пунктів обслуговування [4].

Використання автоматизованих систем органами Державної казначейської служби забезпечує створення єдиного інформаційного простору, що охоплює всі ділянки та всіх учасників бюджетної сфери, зокрема і сферу бюджетного фінансування соціального забезпечення.

Автоматизована казначейська система обліку доходів та видатків бюджетів усіх рівнів являє собою комплекс, у якому взаємодіють декілька систем [5]:

- база даних Єдиної платформи системи обслуговування бюджетів (АС «Є-Казна»);
- база даних централізованого сховища інформації (АС «Є-Звіт»);
- база даних системи подання електронної звітності розпорядниками та одержувачами бюджетних коштів і державними цільовими фондами (АС «Є-Звітність»).

У кожну із систем закладені функції виходячи зі специфіки діяльності казначейства, до яких відносяться: відкриття рахунків розпорядникам і одержувачам бюджетних коштів і їхнє обслуговування, складання звітності про розподіл і використання бюджетних коштів; відкриття рахунків для збору доходів державного і місцевого бюджетів у розрізі видів доходів та територій , їхнє обслуговування відповідно до діючого законодавства і складання звітності про виконання бюджетів усіх рівнів по доходах; введення мережі розпорядників бюджетних коштів, починаючи від головних розпорядників і закінчуючи одержувачами; контроль за цільовим використанням бюджетних коштів; ведення бухгалтерського обліку [6, 7].

Наприклад, АС «Є-Звітність» надає можливість [6]: заповнити в електронному вигляді затверджені форми фінансової звітності, перевірити, підписати ЕЦП кожну форму фінансової звітності та подати до органу Казначейства за місцем обслуговування; на підставі даних бухгалтерського обліку, що формуються в інформаційній системі Казначейства, скласти бюджетну звітність за формами та з дотриманням вимог, перевірити її, заповнити форми розкриття елементів бюджетної звітності, підписати ЕЦП кожну форму бюджетної звітності та подати до органу Казначейства за місцем обслуговування. Автоматичне формування бюджетної звітності зменшить затрати робочого часу на заповнення форм звітності [7, 8].

Казначейська система обслуговування бюджетів вдосконалюється, її функціональні можливості розширюються, вживаються заходи щодо стандартизації та оптимізації передових інформаційних технологій, спрямованих на модернізацію та уніфікацію казначейських процедур і забезпечення підвищення ефективності, прозорості та доступності інформації у сфері державних та місцевих фінансів.

До основними завданнями використання інформаційних технологій в бізнесі можна віднести: ефективна підтримка оперативної діяльності; ведення обліку, контроль; організація документообігу,

підготовка документів (бухгалтерські документи – рахунки, акти, накладні; комерційні пропозиції; договори тощо); швидке формування звітів про стан справ в компанії за будь-який період часу; підвищення ефективності використання робочого часу та продуктивності співробітників завдяки звільненню їх від рутинних робочих операцій; мінімізація помилок та впливу «людського фактору» на найважливіші бізнес процеси підприємства; підвищення якості обслуговування клієнтів та роботи з партнерами; безпечне зберігання інформації.

Серед програм *електронного документообігу лідером є система M.E.Doc.* «M.E.Doc» (*My Electronic Document*) українське програмне забезпечення для подання звітності до контролюючих органів та обміну юридично значущими первинними документами між контрагентами в електронному вигляді. У 2018 році програмою користувалася переважна більшість компаній в України. Програма має як готові рішення для основних потреб користувачів, так і додаткові модулі:

- рішення M.E.Doc.Держава – подача всіх видів звітності в усі контролюючі органи, реєстрація податкових накладних в Єдиному реєстрі податкових накладних та обмін ними з контрагентами. Модуль «Звітність» у M.E.Doc.Держава дозволяє миттєво подавати звітність в електронному вигляді в усі контролюючі органи: Державну фіскальну службу, Державний службу статистики, Пенсійний фонд України, Державний центр зайнятості, ФСС з ТВП.
- рішення M.E.Doc.Бізнес – обмін первинними бухгалтерськими документами з контрагентами;
- модуль M.E.Doc.Акциз та ТТН – для роботи з системою електронного адміністрування реалізації палива та поводження з товарно-транспортними накладними;
- модуль M.E.Doc.Зарплата — розрахунок і нарахування заробітної плати співробітникам, облік і управління персоналом;
- модуль M.E.Doc.Корпорація — консолідація звітності підприємств з розгалуженою структурою.

Ефективними та дієвими в організаційної системи інформаційного забезпечення підприємства є системи, які інтегровані з технологією оперативного управління бізнес-процесами. На ринку IT-технологій існує великій вибір BPM-систем. BPM (business process management, управління бізнес-процесами) - концепція процесного управління організацією, яка розглядає бізнес-процеси як особливі ресурси підприємства, безперервно адаптуються до постійних змін; основні принципи даної концепції - зрозумілість і прозорість бізнес-процесів. Досягається це за рахунок їх моделювання з використанням формальних нотацій, використання програмного забезпечення для симуляції, моніторингу, моделювання та аналізу бізнес-процесів, динамічного перестроювання моделей бізнес-процесів силами персоналу і засобами програмних систем [9].

Система – це Bonita BPM – потужна відкрита система управління бізнес процесами для підприємств середнього і малого бізнесу. Продукт легко інтегрується в існуючі інформаційні системи незалежно від рівня складності й критичності проекту. Bonita BPM дозволяє автоматично генерувати повністю незалежні BPM-додатки, які можна перенести в робоче оточення користувача, а також розширити можливості програмного забезпечення [10, 11].

Oracle BPM – повнофункціональний інструмент для створення, виконання та оптимізації бізнес-процесів. Oracle BPM стоїть між потребами функціональних фахівців і реалізацією цих вимог у вигляді комплексних інформаційних систем, дозволяючи автоматизувати й оптимізувати бізнес-процеси організації з точки зору IT реалізації.

IBM Blueworks Live – інтуїтивно зрозумілий хмарний інструмент для моделювання бізнес-процесів, дає можливість створювати макети, документувати й виводити висновки згідно зі стандартом BPMN 2.0 [14].

Провівши аналіз використання інформаційних технологій в економіці та бізнесі можна стверджувати, що інформаційні технології перетворилася на один з найважливіших компонентів сучасної ринкової інфраструктури. Розвиток інформаційних технологій та систем значно скорочують час на збір і обробку інформації, відбувається перехід від ієрархічних до сітьових структур управління, інтеграції способів досліджень, домінування інформаційних комунікацій. Усе це вказує на формування нових економічних відносин, побудованих на знаннях та інформації.

Бізнес, який працює на основі сучасних інформаційно-комунікаційних технологій, це ефективний та конкурентоспроможний бізнес, який буде готовий до Євроінтеграційних процесів та виходу на міжнародні ринки.

Література:

1. Шевчук І. Б. Теоретичні аспекти розвитку і застосування інформаційних технологій в економіці та управлінні: мезо- та мікрорівень [Електронний ресурс] URL: http://www.sworld.com.ua/simpoz2/82.pdf.
2. Балаженко О.Г Павлова К.В Інформаційні системи пенсійного фонду України. *Економіка та управління підприємствами*. 2017. Випуск 4-1 (43). С. 113-116.
3. Пенсійний фонд України: офіційний веб- сайт. URL: www.pfu.gov.ua (дата звернення: 25.11.2020).
4. Розпорядження Кабінету Міністрів України від 14.09.2016 № 672-р «Про схвалення Стратегії модернізації та розвитку Пенсійного фонду України на період до 2020 року» URL: http://zakon5.rada.gov.ua/laws/show/ru/672-2016-%D1%80 (дата звернення: 27.11.2020).
5. Юрій С. М. Теоретичні питання інформаційної модернізації казначейського обслуговування бюджетів. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки*. 2019. Вип. 1. С. 196–204.
6. Скорик О. О. Інформаційні технології системи казначейського обслуговування: сучасний стан та перспективи їх удосконалення. *Електронне видання «Державне управління: удосконалення та розвиток»*. URL: http://www.dy.nayka.com.ua/pdf/12_2018/28.pdf.
7. ДКСУ про запровадження АС «Є-Звітність». *«Бухгалтер» для працівників бюджетної сфери*. URL: https://buhgalter. com.ua/news/ zvitnist/dksupro-zaprovadzhennya-as-ye-zvitnist/ (дата звернення: 27.11.2020).
8. Автоматизація інформаційна система державного казначейства України. URL: http://constantine-mf.blogspot.com/2010/01/blog-post.html.
9. Що таке CRM-система, ERP-система, управління бізнес-процесами (BPM) URL: Access mode: https://crm-onebox.com/ua/what-is-crm-erp-bpm/
10. Струтинська І. Інформаційні технології організації бізнесу – імператив інноваційного розвитку бізнес-структур економіка та управління національним господарством. *Галицький економічний вісник*. 2018, № 2 (55). С. 40-50
11. Meta-Digital Accounting in the Context of Cloud Computing / Alexandru Tugui, : Encyclopedia of Information Science and Technology, Third Edition, 2015.
12. Кіт, Л.З. Еволюція мережевої економіки. *Вісник Хмельницького національного університету. Економічні науки*. 2014. № 3, Т. 2. С. 187 – 194.
13. Бурик З. М., Огірко О. І. Інформаційні технології забезпечення сталого розвитку в контексті формування нової науково-технічної парадигми. *Інтернетнаука.* 2017. № 1 (2). С. 24–28.
14. Четверта промислова революція: як до неї готуватися URL: https://nubip.edu.ua/node/23076

Прусак М. А.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

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

КІБЕРТЕРОРИЗМ – ВАЖЛИВА ЗАГРОЗА СЬОГОДЕННЯ

Тероризм став однією з важливих загроз цивілізованому суспільству. Терористи намагаються залякати людей та привернути цим до себе увагу. І вони щоразу знаходять нові засоби терору. Інформаційні технології відіграють все більш важливу роль в житті суспільства. Немає такої галузі, де в наш час не використовувалися б інформаційні технології. Тому не дивно, що виникло таке явище, як кібертероризм.

Термін «кібертероризм» був запропонований у середині 1980-х років старшим науковим співробітником американського Інституту безпеки і розвідки (анг. – Institute for Security and Intelligence) Баррі Колліном, який досліджував тенденції переходу тероризму від фізичного до віртуального [1, с. 104].

Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. не дає чіткого визначення «кібертероризму». У цій Конвенції іде мова про такі види комп'ютерних злочинів: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями з метою вчинення комп'ютерних злочинів. Також визначено, що засобами вчинення комп'ютерних злочинів є: комп'ютерна система, комп'ютерні дані, послуги інформаційно-комп'ютерних технологій та дані про рух інформації [2]. Україна ратифікувала цю конвенцію у 2005 р.

Закон України «Про боротьбу з тероризмом» дає визначення поняття «технологічний тероризм», де у переліку засобів вчинення кримінального правопорушення вказано застосування комп'ютерних систем та комунікаційних мереж з терористичною метою, що становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [3].

Закон України «Про національну безпеку України» визначає таке поняття, як «Стратегія кібербезпеки України – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [4]. За повідомленням «Укрінформ» фахівці Національного координаційного центру кібербезпеки при РНБО розпочали розробку Стратегії кібербезпеки України [5].

Проте, на даний час чинний Кримінальний кодекс України не містить понять кіберзлочинність та кібертероризм, лише окремим розділом XVI Кримінального кодексу України визначено злочини у сфері використання електронно-обчислювальних машин (ком'ютерів), систем та комп'ютерних мереж чи мереж електрозв'язку [6].

Визначення кібертероризму можна знайти у дослідженнях багатьох вчених, у міжнародно-правових документах та проектах конвенцій. Але у більшості таких визначень іде мова лише про один аспект інформаційної безпеки, пов'язаний із засобами оброблення інформації [7]. У той же час ціллю кібертерористів все частіше стають критично важливі галузі діяльності суспільства, такі як оборона, національна безпека, енергетика, транспорт, зв'язок, водопостачання, фінансова й банківська системи. Є багато прикладів кібератак, що можна вважати реальним тероризмом. Особливо загострилась ця небезпека із початком російської агресії проти України. Наприклад, в кінці 2015 року сталися кібернапади на чотири обленерго, в результаті чого були знеструмлені помешкання сотень тисяч українців. Важко уявити наслідки кібератаки на аеропорт «Бориспіль» у січні 2016 року, якби в його мережах вчасно не виявили вірусне програмне забезпечення, здатне управляти літаками – атакована комп'ютерна мережа відповідала саме за управління повітряним рухом аеропорту [8].

Тому зараз дуже важливо законодавчо визначити поняття кібертероризму й встановити сурову кримінальну відповідальність за вчинення актів кібертероризму, які можуть бути скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокацій військового конфлікту та спрямовані на підрив національних інтересів й національної безпеки.

Висновок: є нагальна необхідність дати чітке законодавче визначення поняття «кібертероризм» з врахуванням усіх його проявів та цілей, створити єдину нормативну базу, яка б закріплювала механізм захисту суспільства від такого виду злочинів. І, зокрема, необхідно внести зміни в Кримінальний кодекс України, які б передбачали кримінальну відповідальність за кібертероризм.

Література:

1. Марків С. Історико-правовий аспект кібертероризму. // Актуальні проблеми правознавства. Випуск 2 (10). 2017 р. С. 103-106.
2. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. URL: http://zakon2.rada.gov.ua/laws/show/994_575/page *(дата звернення: 30.11.2020).*
3. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. [Електронний ресурс]. URL: http://zakon0.rada.gov.ua/laws/show/638-15/page2 (дата звернення: 30.11.2020).
4. Про національну безпеку України: Закон України від 21.06.2018 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355 *(дата звернення: 30.11.2020).*
5. У РНБО почали розробляти стратегію кібербезпеки України // Укрінформ від 1 грудня 2020 р. [Електронний ресурс]. URL: https://www.ukrinform.ua/rubric-polytics/3105556-u-rnbo-pocali-rozroblati-strategiu-kiberbezpeki-ukraini.html *(дата звернення: 01.12.2020).*
6. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131.
7. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс] / О. В. Кубишкін. URL: http://pravolib.pp.ua/informatsionnyiy-terrorizm-15103.html (дата звернення: 30.11.2020).
8. Наталка Прудка Кібервійна проти України. Перші жертви і висновки // «Главком» від 8 квітня 2016 р. [Електронний ресурс]. URL: https://glavcom.ua/ publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi -i-visnovki.html *(дата звернення: 30.11.2020).*

Форос Г.В.,
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Івасько Т.,
здобувач вищої освіти Одеського державного університету внутрішніх справ

Баранець М.В.,
здобувач вищої освіти Одеського державного університету внутрішніх справ

МЕТОДИ ТА ФОРМИ ВЗАЄМОДІЇ ПРАВООХОРОННИХ ОРГАНІВ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

З теоретичної точки зору, на національному рівні взаємодія правоохоронних органів поділяється на такі види: координація діяльності правоохоронних органів; співпраця органу досудового розслідування та оперативних підрозділів; взаємодія прокурора із органами досудового розслідування; взаємодія слідчого (органів дізнання) з експертами, фахівцями у відповідних галузях знань (наукове забезпечення); взаємодія слідчого з іншими міжнародними та громадськими організаціями [1].

Суб'єктів такої міжнародної взаємодії можна класифікувати на два «блоки»: державні органи та приватні структури. До першого блоку входять Генеральна прокуратура, МВС України, регіональні та місцеві органи прокуратури, Державна служба зв'язку та захисту інформації України та СБУ, в частині діяльності Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки держави.

До приватних структур входять юридичні та фізичні особи, які професійно займаються протидією торгівлі людьми та громадські організації.

Взаємодія правоохоронних органів на національному рівні являє собою перший алгоритм дій. По-перше, усна заява особи про кримінальне правопорушення заноситься уповноваженими працівниками до протоколу усної заяви про кримінальне правопорушення. Далі, слідчий, відповідно до ст. 60 КПК України повинен повідомити про реєстрацію такої заяви у ЄРДР та про початок досудового розслідування.

За результатом початку досудового розслідування разом з оперативними підрозділами складається план проведення слідчих (розшукових) дій.

У рамках досудового розслідування слідчий відповідно до ст. 40 КПК України направляє доручення начальникові підрозділу боротьби зі злочинами, пов'язаними з торгівлею людьми.

За необхідності, слідчий, прокурор підготовлює клопотання про проведення негласних (слідчих) розшукових дій та направляє доручення про їх проведення оперативним підрозділам, яке за результатом складання має гриф «таємно» та зберігається в режимно-секретному органі.

На наступних етапах слідчий слідчий готує клопотання про проведення інших слідчих (розшукових дій), про застосування запобіжних заходів або ж винесення повідомлення про підозру, погодивши їх з прокурором.

В деяких випадках, внаслідок попереднього збирання оперативної інформації, оперативні підрозділи потребують отримати таку інформацію з інших юрисдикцій, зокрема інших держав, що здійснюється в наступних формах:

1) міжнародно-правової допомоги, а саме проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою шляхом надання відповіді на запит про надання правової допомоги у кримінальному провадженні;

2) обміну відомостями оперативно-розшукового характеру, реагування на повідомлення та запити правоохоронних органів іноземних держав шляхом співробітництва центрального бюро Інтерполу в Україні з Генеральним секретаріатом Інтерполу та правоохоронними органами зарубіжних держав під час здійснення діяльності, пов'язаної із попередженням, розкриттям та розслідуванням злочинів, які мають транснаціональний характер або виходять за межі України.

За загальним правилом, встановленим ст. 545 КПК України, зносини з питань правової допомоги у кримінальному провадженні здійснюються через центральні органи України, а саме: Генеральну прокуратуру України (під час досудового розслідування) та Міністерство юстиції України (під час судового провадження).

Порядок направлення запитів українськими компетентними органами чітко визначено ст.ст. 548 та 551 КПК України. Суд, прокурор або слідчий за погодженням з прокурором надсилає до уповноваженого (центрального) органу України запит про міжнародну правову допомогу у кримінальному провадженні, яке він здійснює.

Зміст та форма запиту про міжнародну правову допомогу повинні відповідати загальним вимогам, встановленим ст. 552 КПК України, а також міжнародному договору України, що застосовується у конкретному випадку. Загальний опис фабули має бути простим і стислим, але достатнім з юридичної точки зору для отримання допомоги [2].

Відомості, які містяться в матеріалах, отриманих у результаті виконання дій, передбачених у запиті про міжнародне співробітництво, органами іноземної держави та за процедурою, передбаченою законодавством запитуваної держави, не потребують легалізації і визнаються судом допустимими, якщо під час їх отримання не було порушено засади справедливого судочинства, права людини і основоположні свободи.

Співробітництво органів Національної поліції України з правоохоронними органами іноземних держав із питань обміну відомостями оперативно-розшукового характеру з метою запобігання транснаціональним злочинам та їх розкриття, а також реагування на повідомлення та запити правоохоронних органів іноземних держав здійснюється також з Управлінням міжнародних зв'язків та Робочий апарат Укрбюро Інтерполу.

Порядок направлення запитів до Укрбюро Інтерполу, їх типову форму й зміст регламентує Інструкція про порядок використання правоохоронними органами можливостей Національного центрального бюро Інтерполу в Україні у попередженні, розкритті та розслідуванні кримінальних правопорушень [3].

У межах міжнародного розшуку правоохоронні органи України мають можливість ініціювати проведення розшукових заходів на території однієї, декількох або всіх держав-учасниць Інтерполу, ініціювати публікацію міжнародного повідомлення Інтерполу, розмістити в банках даних Генерального секретаріату Інтерполу інформацію щодо розшукуваних або інших осіб, у том числі громадян України, які не перебувають у розшуку, але є членами організованої злочинної групи або схильні до вчинення тяжких злочинів, зокрема тих, що пов'язані з торгівлею людьми на території різних держав.

Отже, ефективне розслідування торгівлі людьми не можливе без організації взаємодії слідчих з іншими підрозділами органів Національної поліції України, зокрема підрозділами боротьби зі злочинами, пов'язаними з торгівлею людьми Національної поліції України. Взаємодія слідчих з оперативними підрозділами повинна здійснюватися у відповідності з вимогами державного законодавства України та міжнародних договорів.

Література:

1. Біленчук П. Д., Борисова Л. В., Паніотов Є. К. Взаємодія правоохоронних органів України та країн світу при розслідуванні електронних високотехнологічних транснаціональних злочинів. Право і безпека. 2003. 4(1). С. 54-59.

2. Методичні рекомендації щодо виконання вимог міжнародних договорів та КПК України про міжнародну правову допомогу при проведенні процесуальних дій у кримінальному провадженні, схвалені протоколом засідання науково-методичної ради 20.04.2017 № 3.

3. Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів, затверджена спільним наказом № 3/1/2/5/2/2 Міністерства внутрішніх справ, Генеральної прокуратури, Служби безпеки, Державного комітету у справах охорони державного кордону, Державної митної служби, Державної податкової адміністрації від 09.01.1997. Офіційний вісник України. 1997.

Маслова К. В.,
здобувач вищої освіти Одеського державного університету внутрішніх справ

Мельнікова О. О.,
викладач кафедри кібербезпеки та інформаційного забезпечення факультету підготовки фахівців для підрозділів кримінальної поліції Одеського державного університету внутрішніх справ,
кандидат юридичних наук

КІБЕРБУЛІНГ: ВИЯВЛЕННЯ ТА СПОСОБИ ЗАХИСТУ

Перед тим, як перейти до розгляду питання кібербулінгу, здійснемо порівняння булінгу та кібербулінгу. Відмінність кібербулінгу від реального зумовлюється особливостями Інтернет-середовища: анонімністю, можливістю фальшувати ідентичність, мати величезну аудиторію одночасно, здатність тероризувати жертву будь-де та будь-коли.

Кібербулінг – переслідування повідомленнями, що містять образи, агресію, залякування, хуліганство за допомогою багатьох Інтернет-сервісів.

Кібербулінг – дуже розпоширений вид злочинності в Інтернеті.

Кубербулінг розповсюджений не тільки в школах, ліцеях, а також у закладах вищої освіти.

Часто в реальному житті кібербулінг набирає вкрай жорстоких форм з виявами імпульсивності та агресії (наприклад, масові побиття, катування, які записують на відео і знаходяться у вільному доступі в мережі Інтернет). Головними героями таких відеороликів є діти-булери віком 11–18 років.

Існують цілі співтовариства, які можна сказати «полюють» на обраних жертв. Часто вони використовують методи злому, щоб отримати пароль до особистих даних користувача, а потім перетворюють цю людину в жертву. Такі переслідування доводять людей до депресії та серйозних проблем з психікою.

Прийнято виділяти два провідних фактори, за якими можна виділити жертву кібербулінгу:

- множинний стрес (погане самопочуття, низький соціальний статус, погані стосунки з однолітками);
- стигматизація (расові та фізичні особливості людини).

Кібербулінг має декілька виявів, жоден з яких не можна ігнорувати:

- погрозливі й образливі текстові повідомлення;
- розповсюдження (спам) відео та фото порнографічного змісту;
- троллінг (погрозливі, грубі повідомлення в соціальних мережах, чатах чи онлайн-іграх); – демонстративне видалення зі спільнот у соцмережах, з онлайн-ігор;
- створення груп ненависті до конкретної дитини;
- пропозиція проголосувати за чи проти когось в образливому опитуванні;
- провокування підлітків до самогубства чи понівечення себе (групи смерті типу «Синій кит»);
- створення підробних сторінок у соцмережах, викрадення даних для формування онлайн-клону;
- надсилання фотографій з відвертим зображенням (здебільшого дорослі надсилають дітям);
- пропозиції до дітей надсилати їхні особисті фотографії відвертого характеру та заклик до сексуальних розмов чи листування за допомогою месенджерів.

Визначення поняття кібербулінгу як протиправного діяння та встановлення відповідальності за його вияви (форми) в Україні на сучасному етапі в науковій та законодавчій сферах не сформульовано. Однак деякі його вияви є вкрай небезпечними та можуть призвести, як різновид булінгу, до тяжких наслідків, пов'язаних зі шкодою для здоров'я та життя осіб.

Основні поради задля захисту від кібербулінгу:

- намагайтесь обмежувати час користування Інтернетом;
- застосовуйте технічні засоби безпеки для захисту від інформаційних загроз (користуйтеся спеціальними безпечними пошуковими системами);
- формуйте комунікативну культуру; зважайте, що спілкування в Інтернеті, як і в реальному житті, має бути відповідальним, воно може мати певні наслідки і для самого підлітка, і для людей, з якими він спілкується в Інтернеті; не варто створювати вигадані образи, негативно реагувати на кожне повідомлення провокативного характеру. Слід знати, що анонімна свобода в Інтернеті умовна. Адже коли дії в Інтернеті спричиняють реальну шкоду або кримінальну відповідальність,

правоохоронні органи можуть довідатись інформацію з профілів, встановити координати комп'ютерів, з яких людина відправляла повідомлення тощо.

- обмежуйте доступ до персональної інформації у соцмережах;
  - створіть надійний пароль, який зберігайте у таємниці;
  - обмежуйте доступ до свого профілю;
  - не розміщуйте власну адресу і телефон у профілі;
  - помірковано обирайте друзів;
  - обмежуйте доступ до особистих фотографій;
  - не розміщуйте номерів платіжних карток;
  - не відповідайте під дією сильних емоцій;
  - остерігайтесь віртуальних співрозмовників.

Питання кібербулінгу в сучасному інформаційному просторі є дуже актуальним, адже значна кількість дітей та молоді потерпають від психологічного та соціального насильства. Дійте стосовно рекомендацій захисту від кібербулерів.

Література:

1. Грінченко М. С. Кібербулінг як чинник розвитку девіацій у процесі соціалізації молоді: Збірник наукових праць Херсонського державного університету. Педагогічні науки. – 2016. – Вип. 69(3). – С. 31–35.

2. Миронюк Т. В., Запорожець А. К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія: Юридичний часопис Національної академії внутрішніх справ № 2. К.: НАВСУ, 2018. С. 275-284.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html

Старик-Блудова А. Ю.,
здобувач вищої освіти юридичного факультету
Дніпропетровського державного університету внутрішніх справ

Станіна О. Д.,
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук

КІБЕРЗЛОЧИННІСТЬ ТА ШЛЯХИ БОРОТЬБИ З НЕЮ

На початку 80-х, коли був зареєстрований перший випадок комп'ютерного вірусу, розробка шкідливих програм сприймалася спеціалістами, як жартівливе змагання. Але на зараз це явище приймає жахливі масштаби: з'являються цілі організації, призвані створювати загрозу в інформаційному середовищі. Разом з поширенням у світі комп'ютерів та мережі «Інтернет» з'явився і новий вид злочинності – «кіберзлочинність». Під кіберзлочинністю тут і далі будемо розуміти злочинність, якій притаманне розповсюдження у «всесвітньому павутинні». В сучасному світі майже всі підприємства та фірми використовують інформаційні технології, а отже, знаходяться в зоні ризику.

Шахрайство, розповсюдження вірусів, поширення шкідливої інформації (від простої вигадки до матеріалів порнографічного змісту), продаж заборонених речовин та предметів – це далеко на весь перелік речей, якими займаються кіберзлочинці. Так, згідно з даними сайту Cybersecurity Ventures [1], такими темпами до 2025 року кіберзлочинність буде коштувати людству майже 10,5 трильйонів доларів збитків. Крім того, самі користувачі не відрізняються усвідомленістю в сфері кіберзахисту. Як зазначає компанія Varonis Systems [2], 21% всіх файлів з мільярда переглянутих дослідниками є повністю відкритим для будь-кого, а у 41% компаній більше 1000 конфіденційних файлів доступні для публічного перегляду.

І не зважаючи на низький рівень захисту особистої та конфіденційної інформації, сьогоднішня кіберзлочинність має багато засобів досягти своєї мети, і тому все більш актуальним стає питання протидії та запобіганню шахрайству зловмисниками. Так, за словами міністра МВС А.Авакова, за останні 5 років кількість кіберзлочинності в України збільшилася у 2,5 разів. Боротьба зі злочинністю в мережі Інтернет – це питання не тільки особисте, але й державне і, навіть, світове.

Згідно статистиці МВС України, за останні роки найбільш вразливими до кібератак виявилися наступні галузі: охорона здоров'я, виробництво, фінансові послуги, уряд і транспорт, електронна комерція тощо. Основними схемами шахрайства в Інтернеті за статистикою правоохоронних органів є наступні [3]:

- купівля-продаж товарів і послуг шляхом отримання передоплати;
- створення віртуальних фінансових пірамід у кіберпросторі, таких як МММ-2011 чи SWB;
- прийом інвестицій, довірчого управління фінансовими активами, представлення інших фінансових послуг в мережі Інтернет;
- розіграш подарунків, в тому числі з використанням платних телефонних номерів чи коротких повідомлень;
- розміщення оголошень з пропозицією прибуткової роботи вдома з обов'язковим попереднім грошовим внеском тощо.

Тобто в більшості випадків злочинці грають на довірі людей, а отримавши неправомірну вигоду, зникають, залишаючи після себе мінімум «слідів», що дуже ускладнює роботу поліцейських.

Слід зазначити, що згідно з офіційними опублікованими даними МВС [3], кіберполіції частіше за все вдається викривати розповсюджувачів порнографії, дрібних шахраїв, які крадуть пенсії з електронних карток та так званих «закладчиків» – людей, які розповсюджують наркотичні речовини на території певних договірних точках, де потім їх забирають замовники. Невеликий відсоток розкритих кіберзлочинів можна пояснити декількома факторами. По-перше, варто зауважити новітність такого виду злочинності, а отже, – і невеликий досвід розкриття злочинних інтернет-ланцюгів. По-друге, досить нечисленний колектив людей, які займаються кібербезпекою. Прикладом слугує Департамент кіберполіції Національної поліції України, у якому працює приблизно 400 чоловік. Спеціалісти даного відділу постійно розробляють нові методи захисту, моніторингу та розкриття злочинних інтернет-організацій, що сприяють зменшенню кількості незаконних діянь.

Крім того, слід зазначити, що питання кібербезпеки неможливо вирішити лише зусиллями кіберполіції, адже це насамперед низка заходів в різних сферах діяльності: правовій, технічній, організаційній, міжнародній, навчальній тощо. Так, правову сферу можна вважати першочерговою, адже без наявності відповідного чіткого законодавства неможливо запобігти кіберзлочинності. Також боротьба в мережі Інтернет потребує особливих механізмів, інструментів та технічних засобів. Не маючи правильно створеної організаційної структури, не можна чекати на комплексне вирішення питань, пов’язаних з кіберзлочинністю. Важливою є міжнародна співпраця, яка дозволяє вивчати та користуватися всесвітнім досвітом. І наприкінці, виділимо значимість навчання користувачів щодо запобігання інтернет-шахрайства. Адже, як було зазначено вище, велика кількість кіберзлочинів виникає не через відсутність засобів захисту, а через необізнаність та зайву довірливість користувачів.

Підсумовуючи написане, можна зробити висновок , що на сьогодні кіберполіція в Україні не в змозі на відповідному рівні протидіяти кіберзлочинності, і це має зрозумілі першопричини. Виправити цю ситуацію можливо тільки за допомогою досить суттєвих змін, які включають в себе низку заходів в правовій, технічній, організаційній, навчальній та міжнародній сферах діяльності. Такі масштабні зміни потребують великої кількості часу та грошей. Але, при наявності відповідної зацікавленості, є сенс крок за кроком йти до поставленої мети. Так, наприклад, щоб посприяти розвитку кіберполіції, можна «збільшити» кількість працівників за рахунок хакерів, які готові стати на шлях виправлення. Це може добре відобразиться на запобіганні злочинності і укріпленні систем захисту України – завдяки синергії знань та вмінь поліцейських і тих людей, які скоювали правопорушення і на протязі довгих років уникали покарання.

Література:

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, (дата звернення: 04.12.2020)

2. Global data risk report from the varonis data lab, URL: https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf, (дата звернення: 04.12.2020)

3. МВД Украины объявило войну киберпреступности, URL: https://ain.ua/2013/06/21/mvd-ukrainy-obyavilo-vojnu-kiberprestupnosti/, (дата звернення: 04.12.2020).

Москаленко Д. Ю.,
здобувач вищої освіти юридичного факультету
Дніпропетровського державного університету внутрішніх справ

Станіна О. Д.,
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук

ІСТОРІЯ РОЗВИТКУ ТА СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Досягнення в галузі інформаційних технологій створили дивовижні можливості для працівників правоохоронних органів на місцевому, регіональному та державному рівнях. Сучасні можливості збору, класифікації та обміну даними забезпечують різноманітність практичних знань. Це є важливим кроком на шляху досягнення ефективного запобігання злочинності.

Основи інформаційного забезпечення правоохоронних органів України сформувалися на початку 70-х років минулого сторіччя. У цей період був створений Республіканський науково-дослідний інформаційний центр з мережею філіалів у всіх регіонах країни. Характерним для побудови тогочасних інформаційних систем було те, що обробка інформації здійснювалася централізовано, тим самим ускладнюючи або унеможливлюючи прямий доступ працівників правоохоронних органів до бази даних.

Подальше зростання рівня злочинності в Україні призвело до вдосконалення існуючих та створення принципово нових підходів у діяльності органів внутрішніх справ. У сфері інформаційного забезпечення пріоритетним завданням було створення єдиної інтегрованої інформаційної мережі, яка містила б усю накопичену і нову інформацію оперативно-розшукового призначення. За основу була взята система «АРМОР» (Автоматизоване Робоче Місце Оперативника), яка в даний час є інтегрованою інформаційно-пошуковою системою органів внутрішніх справ України (ІІПС). Вона являє собою сукупність організаційно-розпорядчих, програмно-технічних та інформаційно-телекомунікаційних засобів, за допомогою яких здійснюється формування та ведення довідково-інформаційних, оперативно-розшукових обліків та забезпечується авторизований доступ до інформаційних ресурсів ІІПС. [1]

Наступним кроком в розвитку інформаційного забезпечення стало формування Департаменту інформаційної підтримки та координації поліції (ДІПКП) «102» Національної поліції України [1]. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розробленні проектів нормативно-правових актів МВС з питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також обробки персональних даних в органах і підрозділах поліції.

Отримані за допомогою інформаційних систем звіти з місця події, записи судових рішень, списки відомих злочинців та підозрюваних – це важливе джерело даних, яке надає точну, повну та своєчасну інформацію для співробітників правоохоронної діяльності. Але використання такої бази має певні вимоги.

Так, серед нагальних проблем у сфері інформаційного забезпечення правоохоронних органів науковці виділяють наступні:

- недосконаліть правового регулювання сфери інформаційного забезпечення правоохоронних органів;
- невідповідність інформаційних систем актуальним потребам правоохоронців та відсутність дієвої інтегрованої інформаційної системи;
- неналежне технічне оснащення підрозділів правоохоронних органів, особливо низових;
- низьку якість кадрових ресурсів, тобто відсутність належного рівня інформаційної підготовки професійного спрямування як у майбутніх правоохоронців, так і в діючих працівників тощо.

Особливу увагу слід приділити питанню організаційно-кадрового потенціалу. Адже, по-перше, існує проблема підготовки працівників, які в повинні мірі мають володіти знаннями, вміннями та навичками застосування інформаційних технологій. В той час як основна частина кадрового складу правоохоронних органів має юридичну освіту, набуття технічних навичок повинно бути враховано ще при підготовці майбутніх фахівців у вищих навчальних закладах [1].

По-друге, важливе значення має службова підготовка працівників правоохоронних органів. Так, за умов активного розвитку інформаційних технологій працівники інформаційних підрозділів та інших служб в галузі комп'ютерних технологій повинні постійно підвищувати кваліфікацію з інформаційної культури, комп'ютерної підготовки та інформаційної безпеки [2].

Інформаційна підготовка майбутніх та діючих працівників правоохоронних органів повинна бути спрямована на формування інформаційної культури за допомогою освоєння спеціалізованих курсів інформатики та набуття навичок застосування інформаційних технологій у професійній діяльності. Рівень ефективності інформаційної підготовки кадрів для правоохоронних органів повинен підвищуватися за рахунок впровадження інтерактивних методик і технологій навчання, організації комп'ютерних лабораторій, забезпечення навчально-наукової та практичної співпраці з підрозділами правоохоронних органів та розвитку науково-дослідної роботи [3].

Сьогоднішні досягнення в області інформаційних технологій дозволяють практично будь-кому переглядати та ділитися даними; це суттєвий прорив, але він вимагає вирішення ряду нових проблем, серед яких не останнє місце займає технічне оснащення звичайного поліцейського та рівень його компетенцій, знань та вмінь.

Література:

1. Беляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Монографія. К. : КВІЦ, 2008, 576 с.
2. Катеринчук І. П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України [Електронний ресурс] / І. П. Катеринчук // Форум права. 2011. № 2. С. 376–380. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2011- 2/11kippou.pdf
3. Бочковий О.В. Ігнорування інформаційно-технічного прогресу органами досудового розслідування в Україні: хронічна риса чи тимчасове явище? / О. В. Бочковий // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2016. Вип. 3. – С. 223-231.

Рвачов О. М.,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

Ковтун В. О.,
здобувач вищої освіти Харківського національного університету внутрішніх справ

ЩОДО НЕОБХІДНОСТІ СТВОРЕННЯ БАЗИ ДАНИХ ГРАФІЧНИХ МАТЕРІАЛІВ ЩОДО НАСИЛЬСТВА ЗА УЧАСТІ ДІТЕЙ

Під терміном «насильство» прийнято розуміти будь-які умисні дії однієї особи по відношенню до іншої, якщо ці дії порушують права й свободи людини, наносять їй фізичну, моральну чи психічну шкоду [1].

За характером вчинюваних дій насильство по відношенню до людини поділяють на: фізичне; психологічне; сексуальне; економічне [2]. Цей перелік видів насилля не є вичерпним: у ньому наведені найхарактерніші види насилля.

До *фізичного насильства* найчастіше відносять штовхання, запотиличники, копняки, нанесення побоїв, жбурляння різними предметами, примусове закриття в приміщенні, спроба вбивства, катування шляхом умисного завдання болю, страждань, позбавлення жертви їжі, води тощо.

Прояви *психічного насильства* варіюються від глузування, образ, пліток, наклепів до жорстокого приниження людської гідності, злісного висміювання та колективної ізоляції, бойкоту, ігнорування.

Коли говорять про *економічне насилля*, то до нього відносять фінансовий контроль, обмеження, заборону працювати і вчитися, свідоме руйнування та пошкодження майна, що належіть певній особі.

До *сексуального насильства* відносять вульгарну поведінку або жести непристойного характеру, мацання статевих органів, примушення до публічного оголення та відверті сексуальні домагання, зґвалтування [3, с. 307].

Причини насильства зазвичай приховані. Ними можуть бути: стрес на роботі; пияцтво; вживання наркотиків; запальний характер; виховна мета; образа; патологічні ревнощі; модель поведінки, засвоєна

у батьківській сім'ї; занижена або завищена самооцінка; нереалізовані мрії та бажання з дитинства; власне самоствердження через інших людей; потреба у визнанні; психічні відхилення та захворювання; різні релігійні та політичні погляди; хронічний алкоголізм, наркоманія [4].

Місце вчинення насильства може знаходитись:

1) на приватній території чи в приміщенні (наприклад, на земельній ділянці, у будинку, квартирі чи кімнаті в гуртожитку, а також у транспортному засобі);

2) у громадських місцях (наприклад, у приміщенні та на території закладів охорони здоров'я, навчальних закладів; на дитячих майданчиках; у приміщенні та на території спортивних, фізкультурно-оздоровчих споруд і закладів фізичної культури та спорту, у під'їздах житлових будинків, у підземних переходах, у транспорті загального користування, що використовується для перевезення пасажирів, тощо).

Насильство можуть вчиняти: 1) дорослі по відношенню до інших дорослих; 2) дорослі по відношенню до дітей; 3) діти по відношенню до інших дітей; 4) діти по відношенню до дорослих. Також насильство може відбуватися у присутності дітей.

Особи, яким стало відомо про вчинення насильства, у тому числі домашнього, зокрема, якщо постраждалими особами стали або можуть стати діти, мають можливість невідкладно повідомити про це: працівників Національної поліції України, наприклад, зателефонувавши до «служби 102» на відповідний короткий номер; представників районних, районних державних адміністрацій у містах Києві та Севастополі; виконавчі органи сільських, селищних, міських, районних у містах (у разі їх створення) рад; представників цілодобового Кол-центру з питань запобігання та протидії домашньому насильству, насильству за ознакою статі та насильству стосовно дітей, який працює на базі державної установи «Урядовий контактний центр» за номером телефону «1547» [5].

Кінець XX століття ознаменувався інтенсивним розвитком і впровадженням у всі сфери життя суспільства досягнень науки та техніки, а особливо інформатики. Це проявилося в інтенсивному вдосконаленні засобів обчислювальної техніки та техніки зв'язку, у появі нових і в подальшому розвитку існуючих інформаційних технологій, а також в реалізації прикладних інформаційних систем [6, с. 11-12].

Але, як свідчить практика, використання дітьми та дорослими сучасних інформаційних технологій і засобів комунікації несе не тільки поліпшення і полегшення, але і створює певні ризики і загрози [7], а також призводить до появи нових способів вчинення правопорушень.

Через появу та поширення компактних і мініатюрних засобів фотографування та відеозапису, обладнання ними мобільних персональних телекомунікаційний пристроїв (телефонів та смартфонів), персональних комп'ютерів (вебкамери), транспортних засобів (відеореєстратори) усе більше випадків безпосереднього вчинення насильства або його наслідки (синці, рани на тілі тощо) фіксуються на фото- та відео.

Факти насильства або його наслідки можуть фіксувати кривдники, співучасники, випадкові свідки, правоохоронці або потерпілі від насильства. Також вони можуть випадково потрапляти в кут огляду відеокамер систем охоронного спостереження, автомобільних відеореєстраторів чи під час прямої відеотрансляцій в інтернет.

Також доволі часто за допомогою засобів фото- та відеозапису фіксують факти неналежного виконання батьківських обов'язків батьками або особами, які їх замінюють, наприклад, розміщення дорослим у присутності дитини «закладок» із наркотичними речовинами, вживання дорослим наркотичних речовин «на очах у дитини» тощо.

На жаль, певну частину таких графічних матеріалів (фотографій та відеозаписів), на яких зафіксовано факт насильства чи його наслідки, замість того, щоб передати їх напряму до правоохоронних органів з метою вжиття ними заходів щодо встановлення та притягнення винних у насильстві осіб до відповідальності, відновлення та захисту прав потерпілих, розміщують та поширюють у соціальних мережах, інтернет-месенджерах, ЗМІ тощо. Доволі часто ці графічні матеріали викликають у громадян обурення. Вони вимагають від правоохоронної системи країни чи певної території, де було поширено графічні матеріали, якнайшвидшого звітування щодо надання допомоги потерпілим і притягнення винних у протиправних діях до відповідальності.

Правоохоронні органи постійно моніторять інформаційний простір, тому в разі виявлення фотографій і відеозаписів із зафіксованими на них фактами насильства чи його наслідками, особливо по відношенню чи за участі дітей, одразу вживають заходів щодо встановлення кола осіб, по

відношенню до яких та за участі яких було вчинено насильство, місця вчинення насильства та коли його було вчинено.

Непоодинокі випадки, коли в інформаційному просторі певної країни або декількох країн починають поширюватися інтернет-користувачами графічні матеріали, щодо подій які сталися в інших країнах та/або в минулі роки без зазначення інформації, де та коли було зафіксовано людей, зображених на цих фотографіях чи відеозаписах. Правоохоронці, яких залучають до аналізу виявлених графічних матеріалів, витрачають свій робочий час, щоб встановити, що події, зафіксовані на повторно оприлюднених графічних матеріалах, сталися в інших країнах і в минулі роки, а потерпілі та кривдники вже відомі правоохоронцям.

Щоб зробити роботу правоохоронних органів більш ефективною, підвищити рівень захисту прав і свобод дітей, пропонується розглянути пропозицію: **створення бази даних графічних матеріалів щодо насильства за участі дітей.**

До бази необхідно додавати всі виявлені фото та відеофайли, які були поширені громадянами в мережі Інтернет, на яких зафіксовано факти насильства над дітьми.

Кожна включена до бази фотографія та відеозапис повинні бути описані (що саме зафіксовано у графічному файлі) – кількість учасників, їх стать, вік, час доби, пора року, місце зйомки, тип насильства, фрази учасників на відеозаписі тощо.

У базі пропонується зберігати інформація про дату, країну, назву населеного пункту, де відбулася подія, дані осіб, які вчинили протиправні дії, та потерпілих, перелік вжитих правоохоронними органами заходів реагування тощо.

У разі виявлення в мережі Інтернет фактів поширення графічних файлів з насильством над дітьми, правоохоронець здійснює пошук у базі даних за ключовими словами та перевіряє, чи міститься в ній інформація про випадок, що міг статися в попередній період. У разі виявлення в базі ідентичних файлів формується короткий звіт про місце та учасників події для заспокоєння громадськості.

За рахунок використання бази економиться час реакції працівників правоохоронних органів на виявлені повідомлення у ЗМІ та соціальних мережах, які набули резонансу на теперішній час, але ці події відбулися в попередні місяці та роки чи взагалі сталися в інших країнах. Без потреби не залучаються працівники правоохоронних органів для перевірки фактів, зафіксованих та поширених у ЗМІ, соціальних мережах графічних матеріалів, виявленні причетних осіб тощо.

Література:

1. Не мовчи, захисти себе // Безоплатна правова допомога / Координаційний центр з надання правової допомоги : сайт. 11.11.2019. URL: https://www.legalaid.gov.ua/novyny/ne-movchy-zahysty-sebe/ (дата звернення: 10.12.2020).
2. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 № 2229-VIII // БД «Законодавство України» / ВР України : вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2229-19 (дата звернення: 10.12.2020).
3. Шуміло О. О. Щодо визначення видів насильства серед учнівської молоді. *Трибуна докторанта, аспіранта і здобувача*. 2014. Випуск 27. С. 301-310. URL: http://dspace.nlu.edu.ua/bitstream/123456789/7334/1/SHumilo_301_310.pdf.
4. Причини агресії в сім'ї. Лекція 1 // EdEra : сайт. URL: https://nonviolence.ed-era.com/violence-causes (дата звернення: 10.12.2020).
5. Плеханов В. Р., Рвачов О. М., Макаренко П. В. Оперативне реагування на випадки домашнього насильства за допомогою Telegram чат-боту МВС України «#ДійПротиНасильства» // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 179-184. URL: http://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/52.pdf.
6. Советов Б. Я., Яковлев С. А. Моделирование систем : учебник для академического бакалавриата. 7-е изд. Москва : Издательство Юрайт, 2019. 343 с.
7. Зуб Л. В., Рвачов О. М. Сучасні загрози сімейній онлайн безпеці: класифікація та профілактика виникнення // Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 149-154. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/45.pdf.

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

Королько С. В.,
старший викладач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

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

ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ДЛЯ МАГНІТОГІДРОДИНАМІЧНОЇ ТЕХНОЛОГІЇ ОЧИЩЕННЯ РІДИН

Серед глобальних проблем сьогодення проблема забезпечення багатьох регіонів нашої планети прісною водою, придатною для споживання є однією із найважливіших. В основі функціонування багатьох систем очищення водних розчинів від домішок та шкідливих речовин лежать хімічні або фізико-хімічні методи очищення, які потребують розхідних матеріалів, різного роду фільтрів і мембран, а також джерел електричної енергії, без яких дані системи не можуть працювати. Крім цього, для контролю концентраційної складової необхідно постійно проводити багато лабораторних досліджень з використанням хімічних речовин-реагентів. В обох випадках такі аналізи потребують наявності спеціалізованого обладнання і витратних матеріалів.

У доповіді пропонується обговорити новий підхід до взаємно-інтегрованого вирішення як задачі очищення водних розчинів від іонів солей та формування певного складу багатокомпонентних рідин, так і задачі оперативного контролю кількісного і якісного складу цих розчинів.

Автономна магнітогідродинамічна (МГД) система складається із спеціально запроектованої конструкції, в якій розміщено систему каналів, вхідні та вихідні патрубки з давачами контролю, серію спеціально встановлених постійних магнітів та систему розподілу вихідного потоку на канали. При цьому система не вимагає жодних джерел зовнішньої енергії, витрат сировини чи матеріалів.

Принцип роботи МГД системи очищення базується на взаємодії частинок забруднень, що мають нескомпенсований електричний заряд з магнітним полем. Під час руху з потоком води в поперечному магнітному полі на ці частинки діє сила Лоренца. Її величина пропорційна швидкості руху частинки, величині її заряду та індукції магнітного поля. Дія сили Лоренца спричиняє зміну траєкторії руху частинок забруднень, причому, під дією даної сили відбувається перерозподіл концентрацій іонів забруднень. Біля протилежних сторін каналу системи утворюються зони підвищених концентрацій зарядів, що призводить до виникнення поперечного електричного поля. Позитивно заряджені іони солей (катіони) та негативно заряджені іони (аніони) будуть концентруватись на протилежних сторонах каналу. На периферії в середньому каналі буде утворюватись водний розчин з меншою концентрацією іонів, тобто більш-чистішою водою.

Однією з актуальних задач розвитку екологічної, хімічної, енергетичної та інших галузей промислового комплексу України є автоматизація та контроль багатьох фізичних процесів на різних технологічних рівнях. Вимірювання фізичних величин та стан будь-якої системи загалом можна проводити за допомогою сучасних пристроїв інформаційно-вимірювальної техніки. У зв'язку з тим, для вивчення ефективної роботи МГД системи та реалізації даної технології є необхідність використання ЕОМ, що дає можливість визначати миттєві значення перехідних процесів, вимірювати електричні та гідромеханічні величини з високою швидкодією. Універсальним пристроєм для введення, обробки та виведення результатів є мікроконтролер, який поєднує в собі функції процесора, запам'ятовувального та периферійного пристроїв. В якості обчислювальної платформи для практичної реалізації цифрових вимірювань змінних фізичних величин в системі використано мікроконтролерну системну плату Arduino Uno з мікроконтролерним модулем MEGA-2560, що містить у собі аналого-цифровий перетворювач і здатна проводити вимірювання багатьох фізичних величин в реальному режимі часу.

Програмно-технічні аспекти для магнітогідродинамічної технології очищення рідин основані на введенні гранично допустимих параметрів роботи і функціонування МГД системи безпосередньо в програмний комплекс Ардуіно. При запиті з боку системного (host) комп'ютера модуль передає у нього

дані по стандартному інтерфейсу RS-485 і забезпечує узгодження сигналів. В програмі є можливість встановлювати час початку і кінця вимірювання величини сигналу, кількість виміряних точок за секунду, час тривалості паузи у вимірюванні, частоту вимірювань та тривалість імпульсів. При цьому максимальне амплітудне значення вхідної напруги може досягти 3,3 або 5,0 вольт. Програма дозволяє легко візуалізувати результати вимірювань з використанням масштабних коефіцієнтів і координатної сітки. Можна виділяти будь-яку область даних всередині блоку для їх редагування і аналізу. Також у програмі є багато інших інструментів, які дозволяють автоматизувати процеси вимірювання та управління.

Окремим блоком контролю концентраційної складової в системі імітансного контролю вихідної концентрації речовин та продуктів очищення слугувало джерело змінної напруги з регулюванням діапазонів частот в широких межах. Для автоматичного контролю ефективної площі потоку водних розчинів використано лінійне переміщення ширини каналу за допомогою спеціальних індикаторів переміщення. Швидкість потоку рідини визначалась за допомогою витратомірів.

На підставі отриманих експериментальних даних для встановлення граничних умов та параметрів роботи МГД системи використано серію датчиків вимірювання швидкості вхідного та вихідних потоків води, величину різниці потенціалів під час магнітної сепарації іонів, положення зміни ефективного перерізу каналу на периферії, геометричних розмірів та форми цих каналів, величини магнітної індукції в місцях розташування постійних магнітів, вимірювання інтегрованих концентрацій розчинів солей, ємності водних розчинів під час їх накопичення в відповідні посудини, визначення коефіцієнта сумарного ступеня демінералізації води.

Магнітогідродинамічна технологія очищення проводилась з використанням модельного розчину мідного купоросу відомої концентрації 1,077 г/л. В результаті отримані три розчини з концентраціями: 0,941 г/л, 0,996 г/л, 1,099 г/л. Метод визначення концентрацій – титриметричний. Фіксована температура становила 23 ˚С. Генерована напруга склала в максимумі 1,62 В. Для визначення концентрації іонів в розчині застосовано як титрометричний так і імітансний електричний методи аналізу концентрацій вихідних іонів та продуктів сепарації. Дослідження включали також визначення вмісту іонів кальцію, магнію і заліза, а також хлоридів, сульфатів та гідрокарбонатів. Змінюючи швидкість подачі забрудненої води, зміну ефективного перерізу густини потоку розчину, визначали концентрацію іонів до і після очищення. В результаті досліджень вдалось встановити окремі залежності параметрів роботи МГД системи та зробити відповідні висновки.

Отримані експериментальні дані показують, що МГД технологія дійсно призводить до зміни концентрацій розчинених речовин, а імітансний метод показує високу чутливість концентрацій речовин в двох діапазонах зміни частот тестового сигналу – в межах від 100 Гц до 1 МГц. Виконані в роботі дослідження створюють науково-обгрунтовану основу для практичної реалізації і застосування магнітогідродинамічної технології очищення води. Здатність установок призначених для здійснення технології генерування електричної енергії створює можливість реалізації замкненої саморегульованої системи, яка при використанні інтелектуальних цифрових засобів стає повністю автономною.

Таким чином здійснена експериментальна перевірка функціонування усіх компонентів запропонованої автономної програмно-технічної системи керованого очищення і контролю складу води. В подальших дослідженнях планується здійснити теоретичні і експериментальні пошуки оптимальних режимів функціонування розробленої системи.

Нестєров В. Д.,
здобувач вищої освіти Донецького юридичного інституту МВС України

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Високий розвиток інформаційних технологій, технічних засобів та систем, їх активне впровадження в усі сфери нашого життя, нестабільний стан інформаційного захисту створили передумови виникнення нового різновиду злочинів – злочинів, пов'язаних з використанням високих технологій.

За реаліями сьогодення комп'ютер, не підключений до мережі Інтернет вважається анахронізмом, а комунікаційний модуль Wi-Fi можна знайти в телевізорі, телефоні, холодильнику,

гідромасажному боксі, лампі освітлення тощо. Усе більше особистої, корпоративної та державної інформації зберігається за хмарними технологіями та на віддалених хостингах, обчислювальні операції переносяться з персональних систем в обчислювальні кластери, на віртуальні сервери, в хмарні технології. Науково-технічний прогрес, крім позитивних досягнень, має шкідливі наслідки. Різноманіття телекомунікаційних ресурсів є благодатним полем для появи нових витончених способів злочинної діяльності. Злочинів у сфері високих телекомунікаційних технологій стає дедалі більше, методи і засоби вчинення кіберзлочинів стають дедалі технологічними [1, с. 192].

В злочинах такого виду комп'ютерні засоби або інформація, яка в них зберігається, виступають безпосередньо об'єктами злочинного зазіхання або ж стали засобами здійснення злочину.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами [2].

Глобальність і транскордонність комп'ютерних і телекомунікаційних мереж створює ситуації, коли злочинець, перебуваючи на одному континенті, вчиняє злочин на другому, а наслідки правопорушення настають на третьому. Зазначені події відбуваються в кіберпросторі.

Але все одно внаслідок вчинення кіберзлочинів утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди. Ефективність розслідуванню та розкриттю кіберзлочинів багато в чому залежить від своєчасного виявлення слідів злочинних дій правопорушника. Ці сліди утворюються в результаті неправомірного впливу на електронний пристрій, автоматизовану систему чи програму. Для того, щоб ми змогли ці сліди перетворити на докази. Нам потрібно їх знайти, виявити та зафіксувати відповідно до законодавства [1, с. 193].

Доцільним є розглянути дві групи типових слідів, пов'язаних з комп'ютерними злочинами, а саме – матеріальні та інформаційні.

Так, до матеріальних слідів можна віднести:

- сліди, що залишаються на засобах комп'ютерної техніки (сліди пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо);
- сліди, що залишаються на робочому місці злочинця, а саме рукописні записи, що пов'язані з безпосередньою злочинною діяльністю;
- сліди, що залишаються на засобах захисту інформації (спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера, пристроях упізнання користувача).

До інформаційних слідів належать:

- сліди, що вказують на зміни у заданій файловій структурі;
- сліди мережевої активності;
- сліди здійснення віддаленого доступу.

Зазначені дії вимагають застосування спеціальних знань як в процесуальній, так і не процесуальній формі.

Поняття «спеціальні знання» тлумачать як наукові, технічні або інші з позицій кримінального процесуального закону неюридичні знання, отримані внаслідок спеціальної підготовки та практики суб'єктом, процесуальний статус якого визначається як експерт або прирівнюється до спеціаліста [3, с. 27].

Сутність експертизи полягає в тому, що експерт самостійно на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо досліджує надані йому об'єкти, явища й процеси з метою надання висновку з питань, що є або будуть предметом судового розгляду.

Питання призначення та проведення експертиз регулюються Законом України «Про судову експертизу» [4], Інструкцією про призначення та проведення судових експертиз та експертних досліджень [5], а також науково-методичними рекомендаціями з питань підготовки матеріалів та призначення судових експертиз» [6].

Комп'ютерно-технічна експертиза – це дослідження технічних властивостей цифрового обладнання (комп'ютерів, накопичувачів інформації, мобільних телефонів тощо) та програмного забезпечення з метою отримання фактичних даних, що відносяться до обставин скоєного злочину або предмету цивільного позову. Експертиза дозволяє виявити істотні ознаки злочину (інциденту) і створити цілісну доказову базу шляхом дослідження інформації [7].

У залежності від мети дослідження в рамках комп'ютерно-технічної експертизи виділяють: технічну експертизу комп'ютерів та їх комплектуючих і експертизу програмного забезпечення [8, с. 3].

Завданнями, що вирішуються в рамках проведення комп'ютерно-технічної експертизи є:

- встановлення виду (типу, марки), властивостей апаратного засобу, а також його технічних і функціональних характеристик;
- встановлення фактичного стану і справності апаратного засобу;
- виявлення і дослідження функціональних властивостей, а також налаштувань програмного забезпечення, часу його інсталяції;
- виявлення потрібної інформації, встановлення її властивостей та виду відображення в комп'ютерній системі;
- відновлення видаленої та зашифрованої інформації на різного виду носіях;
- виявлення ознак діяльності шкідливого програмного забезпечення;
- виявлення слідів активності в мережі Інтернет, змісту електронного листування, історії обміну повідомленнями у програмах для спілкування та інше [7].

Доцільно виділити такі етапи організації процесу комп'ютерно-технічної експертизи:

1. Отримання дозволу про призначення експертизи – ці дії вважаються законними у разі отримання ухвали слідчого судді. Судова експертиза може бути організована за особистою ініціативою учасників судочинства, наприклад, позивачем, відповідачем, обвинуваченим, потерпілим, адвокатом, або за клопотанням прокурора чи слідчого за погодженням із прокурором. Після схвалення запиту складається список питань, на які фахівець повинен дати розгорнуту відповідь у строки, відповідні ухвалі.

2. Направлення комп'ютерної техніки і програмних продуктів до вказаного в ухвалі слідчого судді експертного центру.

3. Безпосереднє проведення досліджень і надання відповідей на поставлені питання визначені у Наказі Міністерства юстиції України.

4. Отримання висновку експерта. За неможливості дати висновок експерт зобов'язаний скласти пояснювальну записку, в якій повинен надати роз'яснення причин відмови від експертизи, до найбільш поширених. можна віднести непридатність матеріалів і об'єктів досліджень; недостатність кваліфікованих кадрів; відсутність сучасних технологій, що не дозволяє дати відповідь на завдання експертизи [9, с. 185].

Таким чином, можна зазначити, що судова комп'ютерно-технічна експертиза вирішує широке коло питань, дозволяє отримати нові фактичних дані, які є важливими доказами для притягнення до відповідальності винних у вчиненні кіберзлочинів. Цей вид експертизи постійно розвивається шляхом створення нових і вдосконалення наявних методик дослідження, використання сучасного обладнання, програмного забезпечення.

Використання спеціальних знань при розслідуванні кіберзлочинів має велике значення для розкриття та попередження їх у майбутньому. Слід зауважити, що при будь-яких діях, пов'язаних з розслідуванням злочинів у сфері використання комп'ютерних технологій, особливо – вилучення інформації та комп'ютерного обладнання, з метою недопущення помилок, є доцільним залучення фахівця у галузі інформаційних технологій.

Література:

1. Вадим Коршенко. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National Law Journal,* 2017. С. 192 – 194. URL: file:///C:/Users/User/Downloads/5aUExaNedUw0w3RvChG7g3kV17pvRho.pdf (дата звернення 11.12.2020).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Дата оновлення 24.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.12.2020).
3. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст]: навчально-методичний посібник. Одеса: 2020. 112 с.
4. Про судову експертизу : Закон України від 25 лютого 1994 року № 4038-XII. Дата оновлення 03.07.2020. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення 11.12.2020).
5. Інструкція про призначення та проведення судових експертиз та експертних досліджень : затв. наказом Міністерства юстиції України від 08.10.98 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 11.12.2020).

6. Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказом Міністерства юстиції України від 08.10.98 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 11.12.2020).

7. Експертна спеціальність 10.9 «Дослідження комп'ютерної техніки та програмних продуктів». URL: https://dndekc.mvs.gov.ua/%D0%B5%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%BD%D0%B0-%D1%81%D0%BF%D0%B5%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C-10-9-%D0%B4%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD/#:~:text=%D0%9A%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%2D%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B0%20%D0%B5%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%B8%D0%B7%D0%B0%20%E2%80%93,%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D1%83%20%D0%B0%D0%B1%D0%BE%20%D0%BF%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%D1%83%20%D1%86%D0%B8%D0%B2%D1%96%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D0%BE%D0%B7%D0%BE%D0%B2%D1%83 (дата звернення 11.12.2020).

8. Дубинський О. Ю. Судова експертиза як форма застосування спеціальних знань при розслідуванні злочинів, вчинених з використанням комп'ютерних технологій. URL: http://eir.nuos.edu.ua/xmlui/bitstream/handle/123456789/2292/Dubinskyi.PDF?sequence=1&isAllowed=y (дата звернення 10.12.2020).

9. Яцик Т. П., Кисла К. О., Пушкарьова Т. М. Кіберзлочинність в Україні: аналіз дієвості способів розслідування кіберзлочинів і напрями їх вдосконалення. *Юридичний науковий електронний журнал*, 2019. № 1. С. 184-186. URL: http://www.lsej.org.ua/1_2019/51.pdf. (дата звернення 11.12.2020).

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

Микієвич Л. М.,
здобувач вищої освіти юридичного факультету
Львівського національного університету імені Івана Франка

ТЛУМАЧЕННЯ І ЗАСТОСУВАННЯ НОРМ В ІНФОРМАЦІЙНІЙ СФЕРІ

Про інформаційне право, як про самостійну науку і галузь права юридичної науки почали говорити порівняно недавно, приблизно 60-70-х роках 20 століття. Так єдиного розуміння і думки також не було сформовано, а термінологія, яку ми зараз відносимо до інформаційного права не було точно визначено, і відповідно в літературі того часу можна зустріти різні визначення, що відносяться нерідко до одного і того ж явища.

Більшість у своєму розумінні інформаційного права зводилася тільки, як називали в той самий же час до комп'ютерного права або до правової кібернетики. Розвиток юридичної науки породило не один десяток самостійних галузей права, які раніше були в складі традиційних і усталених галузях права.

Поява інформаційного права для юридичної науки потребувало додаткових обґрунтувань та роз'яснень. Інформаційне право в цьому відношенні не є винятком. Більш того, саме інформаційне право зараховується до розряду галузей права, новизна яких викликає чимало сумнівів і суперечок з приводу їх самостійного існування.

Для точного і одноманітного застосування на практиці норм інформаційного права до тієї чи іншої інформаційної ситуації необхідно, перш за все, щоб використовувати ту чи іншу норму правильно і точно усвідомити сенс і зміст норми.

Так само як і інші норми, норма інформаційного права виражена в джерелах даної галузі – законах і підзаконних актах, в яких відбивається зміст інформаційно-правових норм, їх цілі, спрямованість, суть, взаємозв'язок з іншими нормами тощо.

У зв'язку з цим для з'ясування конкретної інформаційної норми потрібне вивчення самого закону, в якому ця норма міститься, його аналіз, дослідження структури, регулятивних можливостей, з метою подальшого застосування на практиці.

До тлумачення закону чи інших актів інформаційного характеру доводиться вдаватися в процесі їх застосування до конкретних інформаційних ситуацій, при вирішенні правових завдань в ході правового регулювання інформаційних відносин.

Тлумаченню може підлягати будь-яке джерело інформаційного права: закон або інший акт інформаційної спрямованості, що встановлює інформаційно-правові приписи, правила поведінки суб'єктів інформаційних правовідносин.

Офіційне тлумачення законів в даній сфері – це тлумачення уповноваженими на те державними органами і посадовими особами. Цей вид тлумачення закріплюється в законодавчому порядку і підлягає неухильному і безперечному виконанні.

З правозастосовної практики, офіційне тлумачення буває легальним і судовим. Легальне тлумачення законів в інформаційній сфері дається уповноваженим на те державним органом і є обов'язковим для застосування до конкретних ситуацій.

Практиці відомі факти тлумачення норм інформаційного законодавства та іншими державними органами. Однак самостійним видом тлумачення законів в інформаційній сфері є в першу чергу судове тлумачення, оскільки рішення або вирок суду щодо вирішення інформаційного спору (випадку) набуває владні обриси і навіть якусь законодавчу силу і в цьому сенсі не може порівнюватися з тлумаченням норм інформаційного законодавства міністерствами і відомствами .

Найбільш поширеним видом тлумачення законів інформаційної спрямованості сьогодні є наукове тлумачення, що базується на наукових дослідженнях, розробках і публікаціях у сфері інформаційного права та інформаційної техніки.

Тлумачення зазначених законів, що здійснюється в монографіях, коментарях, навчальних посібниках з інформаційного права, відіграє велику роль для вдосконалення чинного інформаційного законодавства, раціоналізації роботи інформаційних агентств, ЗМІ, центральних органів виконавчої влади, і зміцнення законності і правопорядку в інформаційній сфері.

Цей вид тлумачення законів - неофіційний і в цьому сенсі він не має обов'язкового юридичного значення для застосовують норми інформаційного права для державних органів і посадових осіб, які в ході своєї правозастосовної діяльності, безумовно, повинні знати останні досягнення науки і думки вчених, оприлюднені через друк, але в процесі своєї інформаційно-правової діяльності зобов'язані в першу чергу спиратися на закони та інші акти, обов'язкові для виконання всіма.

Наукове тлумачення зазначених законів можуть давати не тільки вчені-юристи та воно може відображатися не тільки в наукових джерелах, книгах і т.д., а здійснюватися прокурорами, адвокатами, журналістами, експертами в їх статтях, виступах і ін. Якщо подібне тлумачення носить науковий характер, засноване на достовірному аналізі норм права, фактів, то воно теж може розглядатися як наукове і використовуватися в ході застосування норм інформаційного права.

Норми, що містяться в Конституції України, є предметом інформаційного права становлять основу даної галузі, так як регламентовані в Основному законі країни, хоча і не є вичерпними. Конституція України встановлює принцип пріоритетності прав на недоторканність приватного життя, особисту і сімейну таємницю, захист своєї честі і гідності [1]. Також на таємницю особистих вкладів і заощаджень, листування, телефонних переговорів, поштових, телеграфних та інших повідомлень. Обмеження цього права допускаються тільки у випадках і в порядку, прямо встановлених законом.

Конституції України гарантує свободу слова і творчості. Також і інші норми інформаційної сфери, які містяться в Основному законі. Крім норм Конституції за весь час становлення національного законодавства було прийнято чимало нормативних актів у інформаційній сфері, зокрема Закон України «Про інформацію» [2].

Саме застосування норм інформаційного права виступає як специфічна дія, як реалізація його норм, положень, статей; воно характеризує здійснення тих приписів і правил, які встановлює інформаційне законодавство.

Завданням застосування норм інформаційного права є в першу чергу повна реалізація законів, актів, положень інформаційного характеру в точній відповідності з їх змістом і сенсом, без найменшого відступу від закону.

Іншими словами, застосування норм інформаційного права – це перш за все форма їх реалізації, під якою в теорії права розуміється як втілення розпоряджень юридичних норм у життя шляхом правомірної поведінки суб'єктів суспільних відносин (державних органів, посадових осіб, громадських організацій громадян).

Потрібно відзначити, що реалізація норм інформаційного права завжди пов'язана з правомірною поведінкою учасників інформаційних правовідносин, тобто такою поведінкою, яка не передбачає

здійснення правопорушень в інформаційній сфері, причому це правомірна поведінка може виступати як у формі активних дій (дії автора з метою опублікувати свою роботу), так і у формі бездіяльності (відсутність перешкоджання з боку автора поширенню інформації про свою роботу).

Література:

1. Конституція України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України «Про інформацію» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Козопас М. В.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

Магеровська Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

ОГЛЯД ІСНУЮЧИХ ВИДІВ ХМАРНИХ ПОСЛУГ І МОДЕЛЕЙ ХМАРНОГО РОЗМІЩЕННЯ

Сучасні тенденції розвитку IT-індустрії дозволяють перейти від традиційних методів оброблення інформації до більш прогресивних. Одним із таких методів є перенесення обчислень у хмарні структури провайдера – постачальника хмарних послуг. *Обчислення в хмарі* – це способи надання споживачеві через Інтернет ресурсів у вигляді послуг, що базуються на сукупності різних технологій. При цьому кошти підтримки цих послуг приховані від споживача, а самі ресурси оплачуються ним у міру їх використання. Хмарні обчислення дозволяють не ускладнювати інформаційну інфраструктуру споживача хмарних послуг завдяки використанню об'єднаних у віртуальну інфраструктуру ресурсів постачальника.

Хмарна інформаційна система складається з хмарного клієнта і хмарного сервера. Під *хмарним клієнтом* розуміються засоби обчислювальної техніки, що входять до складу інформаційної системи, побудованої з використанням технологій хмарних обчислень, за допомогою яких здійснюється отримання однієї або декількох хмарних послуг. *Хмарний сервер* – розподілена обчислювальна мережа, що обробляє запити споживачів хмарних послуг. Хмарний сервер може мати у своєму складі мережеве обладнання, сервери оброблення даних, операційну систему (ОС), мережеві сховища, засоби управління базами даних, прикладні програми, мережеві служби тощо.

На віртуальному сервері, що знаходиться в «хмарі» постачальника, під управлінням різних операційних систем може одночасно функціонувати безліч додатків споживачів хмарних послуг. Віртуальний поділ ресурсів дозволяє створювати мережеві домени, що надають послуги різним споживачам з оброблення конфіденційної інформації.

Під час використання моделі доступу «хмарні обчислення» інформаційні сервіси надаються так, що технології, які їх забезпечують, стають практично «невидимими» для споживача. А оскільки це дозволяє відокремити інформаційні сервіси від інформаційної інфраструктури, що забезпечують їх роботу, хмарні обчислення можуть бути частиною стратегії по підвищенню динамічності роботи сучасних установ.

Поява першої технології, близької до сучасного розуміння терміну «cloud computing», приписується компанії Salesforce.com, заснованої у 1999 році [1]. Саме тоді і з'явилася перша пропозиція нового виду – «Програмне забезпечення як сервіс» ("Software as a Service", "SaaS"). Перше бізнес-рішення під назвою «Amazon Web Services» було запущене у 2005 році компанією Amazon.com, яка активно займалася модернізацією своїх центрів оброблення даних (ЦОД). Найхарактерніший приклад використання додатків хмарних обчислень сьогодні – служба Google Docs, що дозволяє працювати з офісними документами через браузер споживача.

Існує безліч видів хмарних послуг і моделей хмарного розміщення. Компанія споживача хмарних послуг має розуміти різницю між наявними типами хмарних середовищ і визначити, які з них найкращим чином відповідають її бізнес-процесам.

Розрізняють декілька моделей хмарного розміщення. *Приватна хмара* (private cloud) – інфраструктура, призначена для використання однією організацією, що включає декілька споживачів (наприклад, підрозділів однієї організації), а також клієнтами даної організації. Приватна хмара може перебувати у власності, управлінні та експлуатації як даної організації, так і третьої сторони, і вона може фізично існувати як всередині, так і поза юрисдикцією власника [2].

Під час використання приватної хмари знижується час очікування надання ресурсів для співробітників компанії споживача хмарних послуг, хмарне середовище сприяє ефективному розподілу ресурсів всередині організації, допомагає динамічно розподілити навантаження між фізичними системами ЦОД, відстежувати реальне споживання ресурсів всередині компанії.

Наступним варіантом розгортання є *публічна хмара* – це система, підготовлена постачальником хмарних послуг для відкритого використання декількома компаніями. Хмара існує тільки на території хмарного постачальника, на відміну від приватної хмари, яка може розгортатися і в межах інформаційної системи споживача хмарних послуг.

Гібридна хмара – спільне використання двох перерахованих вище моделей розгортання. Така модель являє собою композицію з двох або більше різних інфраструктур хмар, що мають унікальні об'єкти, але пов'язані між собою технологіями, які дозволяють переносити дані або програми між компонентами.

Використання технологій приватної, публічної і гібридної хмари дозволяє користувачам хмарних обчислень скористатися обчислювальними потужностями і сховищами даних, які за допомогою певних технологій віртуалізації та високого рівня абстракції надаються їм як послуги.

Найнижчий рівень і найбільш проста модель розгортання хмарних сервісів дозволяє замовнику взяти в оренду тільки підтримуючу інфраструктуру, яка називається IaaS. Це, по суті, просто порожній склад. Приклади IaaS: IBM Softlayer, Hetzner Cloud, Amazon EC2.

Більш складна модель розгортання хмарних обчислень охоплює рівень платформи інформаційної системи і отримала назва PaaS. Цей рівень включає в себе не тільки інфраструктуру, але і деякі сервісні служби, наприклад операційні системи й їх обслуговування. Приклади PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry.

SaaS – модель розгортання хмарних сервісів, що характеризується найбільш повним наданням послуг замовникові, передбачає використання додатків із хмари для роботи на локальному комп'ютері замовника. Багато SaaS додатків є заміною традиційного програмного забезпечення і формою перенесення його в хмарне середовище.

Таким чином, для споживача хмарних послуг відкриваються широкі можливості, що дозволяють знизити вимоги до обчислювальної потужності власної інформаційної системи, а будь-кому, як завгодно слабкому обчислювальному пристрою отримати потенціал найсучаснішого і дорогого устаткування.

Література:

1. Історія хмарних обчислень. [Електроний ресурс] – Режим доступу: https://nachasi.com/2017/09/26/istoriya-hmarnyh-obchyslen/

2. Що таке хмарні сервіси і чому вони так стрімко розвиваються. [Електроний ресурс] – Режим доступу: https://businessviews.com.ua/ru/tech/id/hmari-dlja-biznesu-2003/

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

Бродик А. Р.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

ОСОБЛИВОСТІ ДЕЯКИХ ПЛАТФОРМ ДЛЯ ПРОВЕДЕННЯ ВІДЕОКОНФЕРЕНЦІЙ ТА ВЕБІНАРІВ

Платформи конференцій та вебінарів пропонують аналогічні функції і можливості, але володіють декількома важливими відмінностями.

Конференції – це спільні заходи, в ході яких всі учасники можуть демонструвати вміст екрану, включати передачу відео і звуку і бачити список присутніх.

Вебінари організовані таким чином, щоб організатор і вибрані доповідачі могли транслювати відео, звук і демонструвати вміст екрану. Учасники вебінарів володіють тільки правами перегляду. Вони можуть взаємодіяти за допомогою функції «Питання і відповіді», спілкуватися в чаті і брати участь в опитуваннях. Організатор також може включати звук учасників. Розглянемо деякі переваги та недоліки використання найбільш вживаних відеоплатформ.

Відеоплатформа Skype (www: skype.com). Skype – фактично першопроходець в цьому напрямку. Його реліз відбувся в 2003 році. Це не перший інструмент для організації відеозв'язку, але за рахунок простоти реєстрації він швидко завоював популярність, і вже в 2009 році кількість облікових записів в Skype переступило за півмільярда.

Мабуть, його можна назвати піонером масової побутової відеозв'язку. Сервіс функціонує через клієнт, який скачується і встановлюється на цілий перелік платформ. Доступна і веб-версія.

Переваги. З плюсів – можливість дзвонити на стаціонарні і мобільні номери по всьому світу, правда, не безкоштовно. При цьому навіть в Росії можна підставляти в CALLER ID номер свого мобільного телефону. У деяких країнах доступні вхідні дзвінки на Skype з мобільних через спеціальний номер.

Недоліки. Skype частіше застосовується для невеликих нарад або індивідуальних консультацій. Велика конференція на Skype – рідкість.

Skype не дозволяє безперервно спілкуватися більше чотирьох годин. Крім того, обсяг групових відеодзвінків обмежений 100 годинами на місяць (10 годинами в день) – це ліміти безпеки, встановлені розробниками.

Інструмент часто критикують за те, що він гірше реагує на проблеми з мережею, ніж той же Google Hangouts або Zoom. Крім того, мобільний клієнт досить вимогливий до ресурсів пристрою.

Варто зазначити, що у Microsoft є Skype for Business - самостійний продукт в сімействі Skype, що володіє великим функціоналом. До наради в Skype for Business можна підключитися за допомогою звичайного Skype, але можна використовувати веб-клієнт в браузері. У Skype for Business доступна функція публічного показу зборів, яка дозволяє демонструвати те, що відбувається аудиторії до 10 тис. чоловік.

Відеоплатформа Zoom. Zoom зараз найчастіше згадується в новинах і анонсах заходів. Але популярність він отримав не тільки завдяки загальній ситуації. У минулому році Gartner включив Zoom в список лідерів конференц-рішень.

Зараз Zoom став стандартом де-факто для проведення невеликих вебінарів і дискусій де відзначається лавиноподібне зростання користувачів, в тому числі за рахунок сегмента освіти, який практично повністю пішов на on-line рішення.

Цей же інструмент використовують на більших заходах для організації взаємодії слухачів з доповідачами після виступу або в перервах між ними (наприклад, Zoom використовувався в такому ключі в рамках перекладеної на днях в он-лайн-форматі Moscow Python Conf ++ 2020).

Zoom – це ідеальне програмне забезпечення для веб-зустрічей для користувачів, які хочуть просто та ефективно віддалено з'єднуватися з клієнтами. Він також має підтримку ОС Chrome та Linux для підвищення гнучкості та безпечного шифрування шару сокета (SSL) для забезпечення безпечної комунікації.

Усі можливості Zoom включають:

- обмін екраном з настільних ПК, планшетів або мобільних пристроїв;
- дошка для дошки;
- HD відео та голос;
- необмежена кількість зустрічей на місяць;
- шифрування захищеного сокетного шару (SSL);
- чат та повідомлення (приватні та групові);
- планування з розширеннями Chrome;
- варіант запису зустрічей;
- можливість приєднатися до зустрічі по телефону;
- миттєві або заплановані зустрічі;
- он-лайн-підтримка;
- кімнати прориву.

Можливості прориву дозволяють розділити зустрічі на цілих 50 окремих сесій.

Існує також безкоштовна версія Zoom, але можливості її обмежені. Конференції, які мають багато учасників, не можуть перевищувати 40 хвилин. Для таких розширених функцій, як управління користувачами, сумісність, індивідуальні ідентифікаційні зустрічі для окремих учасників, підтримка телефону та керовані домени, ви повинні підписатися на один із своїх преміальних планів.

Учасники. Кількість дозволених учасників на зустріч буде залежати від обраного вами плану. Є можливість додавати більше учасників з кожним планом, крім безкоштовної версії.

Переваги. Zoom орієнтований на порівняно великі зустрічі. Є функції «підняття руки» і різні інструменти організатора, що дозволяють управляти спілкуванням по відео. Важливо також, що захід можна записати як в локальну систему, так і в хмару.

На платних тарифах у Zoom є API для реалізації додаткових функцій. В цілому у інструменту багато опцій, і є можливість платити тільки за використовувані функції. У списку можна знайти навіть звітність і взаємодія з Outlook або Lync. Є окремі пакети для організаторів вебінарів на певну аудиторію. Оплачує цей тариф тільки організатор - учасники підключаються безкоштовно.

Недоліки. Вони умовні. Наприклад, конференція не може тривати більше 24 годин. Інші обмеження залежать від обраного тарифного плану.

Безкоштовно в Zoom можна проводити відеозустрічі до 100 чоловік тривалістю не більше 40 хвилин. На спілкування один на один ліміти часу не поширюються.

Порівняльна характеристика платформ відеозв'язку Zoom та Skype.

	Zoom	**Skype**
Вартість	Безкоштовно - $ 19,99 / міс. +	Безкоштовно - 12,50 дол. / Міс. На кожного користувача
Основні характеристики		
Підтримувані пристрої	Android, iPhone / iPad, Mac, веб-бази, Linux, Windows	Windows, Android, iPhone / iPad, Mac, Веб-версія, Windows mobile
Підтримка	Онлайн-підтримка	Підтримка на вимогу
Учасники	До 100 учасників	До 250 учасників
Підтримувані інтеграції	Google Drive, Pardot, Dropbox, Eloqua, HubSpot, Infusionsoft та багато іншого	Agile CRM, Slack, Microsoft Systems, Grasshopper та багато іншого
Особливості конференцій	HD-відео, HD-голос, обмін екраном, дошка	Групові відеодзвінки, інструменти співпраці, обмін екраном
Веб-функції	Чати в режимі реального часу та приватні роботи, засоби презентації, можливості запису та відтворення	Чати в режимі реального часу, обмін файлами, обмін відео повідомленнями
Мови, що підтримуються	Англійська	Англійська
Призначений для	Малий, середній та великий бізнес	Малий, середній та великий бізнес
Помітні клієнти	Delta, Match.com, Sonos, Pandora, Slack, GoDaddy	VerbalizeIt, Advansys, AIRDEX, Diverse Learners

Трансляції Youtube. На тлі інших описаних майданчиків YouTube виділяється своєю орієнтацією на трансляцію відеопотоку без взаємодії зі спікером. Єдина можливість задати питання - написати його в коментарях і сподіватися, що спікер туди загляне.

Трансляція доступна не для будь-якого облікового запису – лише для тих, хто підтвердив номер телефону.

При всіх обмеженнях спілкування YouTube-трансляції підкуповують своєю простотою. Відео можна транслювати з веб-камери комп'ютера або з мобільного пристрою з програми. YouTube Live підтримує відео у форматах HD, однак через зростання трафіку в період пандемії сервіс ввів примусове обмеження до SD.

Крім згаданих платформ можливі ще й такі:

Відеоплатформа Microsoft Teams. Команди Microsoft розроблені для бездоганної ефективності та співпраці. Він інтегрується з такими додатками Office, як Word та SharePoint, а його дизайн та інфраструктура роблять його винятково інтерактивним. Компанія також дозволила інтегрувати Skype для бізнесу в команди Microsoft.

Ця програма була розроблена як відповідь на зростаючу кількість інструментів співпраці, таких як Slack, які домінували на ринку за останні кілька років. **Microsoft Teams** – це загальнодоступний інструмент чату для робочого місця, але його можливість проведення відеоконференцій настільки ж переконлива і потужна. Користувачі можуть запускати відеоконференції безпосередньо зі своїх чатів.

Усі можливості Microsoft Teams включають:

- веб-версія Word, Excel та PowerPoint;
- зберігання та обмін файлами;
- до 300 користувачів;
- цілодобова підтримка телефону та Інтернету.

Одна з найновіших функцій, що входять до команд Microsoft, дозволяє користувачам запрошувати гостей, які не входять у Azure Active Directory свого підприємства. Крім того, мобільна версія Microsoft Teams підтримує голосову пошту на Android та iOS.

Відеоплатформа Skype для бізнесу. У комплекті з Microsoft Office 365 Skype для бізнесу, ймовірно, вже знайомий багатьом користувачам. Ділова версія піднімає безкоштовні, стандартні можливості платформи на наступний рівень.

Усі можливості Skype для бізнесу включають:

- необмежені зустрічі;
- обмін екраном;
- миттєві повідомлення в будь-який час;
- жорстка безпека;
- конференції з до 250 учасників.

Skype також може легко інтегруватися з такими програмами Microsoft Office, як Word, Excel, PowerPoint, OneNote та Outlook.

Додавши корпоративний пакет, керівники нарад можуть приймати до 250 учасників через безпечне з'єднання. Оновлення до Online Plan 2 додає HD відео та аудіодзвінки, поштову скриньку об'ємом 50 ГБ та зберігання файлів до 1 ТБ та технічну підтримку мобільних пристроїв.

Хоча інтеграція існує для команд Microsoft, жодні дані не свідчать про те, що Microsoft планує припинити використання Skype для бізнесу на користь свого нового продукту.

Деякі поради щодо пошуку свого ідеального програмного забезпечення для відеоконференцій.

Під час вибору платформи слід враховувати можливості бюджету та потреб:

- багато планів відеоконференцій дешевше, якщо ви платите щороку замість місяця на місяць;
- деякі плани стягуватимуться з кожного користувача. Переконайтеся, що ви знаєте, скільки дозволено на план, і перевірте, чи можете ви додавати користувачів за потребою;
- якщо програмне забезпечення для відеоконференцій, яке вас цікавить, не пропонує безкоштовного плану або безкоштовної пробної версії, виберіть демонстраційну версію, щоб ви могли побачити її, перш ніж взяти на себе зобов'язання придбати.

Вибравши програмну платформу для відеоконференцій, потрібно буде оцінити, як вона впишеться у середовище вашої кімнати для нарад.

Циганський А.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

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

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ХМАРНИХ СХОВИЩ

Хмарні сховища даних зараз дуже популярні. Головне їхнє призначення – це збереження і доступ до інформації з будь якого пристрою у будь який час і можливість ділитися цією інформацією, документами, фотографіями та довільними файлами з іншими людьми. До того ж хмарні технології надають додаткові корисні сервіси для користувачів, наприклад створення та робота з документами в режимі online, сумісний доступ та інше.

Розглянемо деякі особливості використання хмарних сховищ.

Хмарні сховища як заміна накопичувачів. Для аналізу розглянемо декілька можливостей хмарних сховищ, а саме: One Drive від фірми Microsoft, хмарний диски від пошукової системи Google, сховище Mega та Dropbox.

Перший параметр для дослідження – це кількість безкоштовного хмарного простору.

Необхідно відзначити особливість сховища Google, а саме, можливість підключення до нашої хмари багато різних застосувань, наприклад конвертор файлів pdf та аудіо чи відео редактори, а також можливість програмування на деяких мовах програмування.

Беззаперечно, за розмірами безкоштовного дискового простору переваги мають сховище Mega та Google Drive.

	MicrosoftOne Drive	Google Drive	Сховище Mega	Сховище Drobox
				
Безкоштовний об’єм пам’яті (GB)	5	15	50	2
Можливість додаткового розширення	-	+	-	-
Створення офісних документів	+	+	-	-
Редагування офісних документі	+	Свої редактори	-	+

Переваги та недоліки деяких хмарних сховищ. OneDrive

Переваги: Сервіс OneDrive відмінно працює з пристроями Windows, тому що він вбудований в цю операційну систему, встановлену на персональних комп'ютерах, планшетах і смартфонах. Можливість відкрити збережені в OneDrive файли за допомогою інших додатків компанії Microsoft, таких як Word або Photos. Так як OneDrive тісно пов'язаний з Microsoft Office, це хороший вибір для тих, хто часто користується програмами Office.

Недоліки: Якщо всі ваші пристрої не працюють в операційній системі Windows, сервіс OneDrive перестає бути таким вже привабливим. Існують додатки для інших пристроїв, але абсолютно ясно, що OneDrive призначений саме для пристроїв на Windows. Для того щоб користуватися OneDrive, доведеться відкрити свій обліковий запис Microsoft, яка дасть доступ до Outlook, Xbox Live та інших сервісів Microsoft, незалежно від того, хочете ви цього чи ні. Microsoft дотримується більш суворої політики щодо файлів, які ви завантажуєте в OneDrive, ніж будь-який інший сервіс хмарного зберігання даних. Тут не можна зберігати файли що зображують будь-який вид наготи, підбурюють до прояву расизму або пропагують його і таке інше.

Важко сказати, наскільки завзято Microsoft буде дотримуватися цих обмеження, але вони, тим не менш, є частиною «Умов надання послуг», з якими ви погоджуєтеся при реєстрації.

Dropbox

Переваги: Найсильнішим сервісу є те, що він однаково добре працює на Windows і Mac, Android і iOS. Сервіс спроектований настільки простим і елегантним, що будь-якому буде легко навчитися працювати з ним. Десктопні програми легко працюють з файловою системою вашого комп'ютера.

Недоліки: На думку автора, дизайн сайту Dropbox – найслабший з усіх сервісів хмарного зберігання даних. Він простий і зрозумілий, але ви не можете управляти тим, як відображаються файли. Однак у вас є набагато більше можливостей ділитися файлами на сайті, що майже компенсує такий примітивний дизайн.

Google Drive

Переваги: Якщо у вас вже є обліковий запис Google, для установки Google Drive знадобиться мало зусиль. Якщо ви користуєтеся поштою Gmail, ви можете зберігати вкладені в листи файли в Google Drive безпосередньо, всього лише в кілька кліків.

Недоліки: У Google Drive немає можливості автоматично завантажувати фотографії з вашого смартфона прямо в сервіс. Замість цього у Google є функція Auto Backup в мобільному додатку Google+, яке відправляє ваші фотографії в профіль Google+.

MEGA для Windows

Основні переваги: Ви зможете зберігати об'ємні файли на сторонньому диску. Обсяг безкоштовної пам'яті становить 50 Гб. Програма автоматично синхронізує дані ваших комп'ютерів і хмарного сховища, дозволяє синхронізувати будь-яку теку на ПК з текою в сховищі. Сховище може бути доступним тільки для вас, навіть, якщо за одним ПК працюють кілька користувачів. Окрім цього, всі файли зашифровано, а хмарне сховище захищено від незаконного втручання.

Основні недоліки: Використання програми потребує реєстрації на офіційному сайті mega.nz. Якщо ви забажаєте використати додаткові переваги програми та більший обсяг пам'яті, потрібно буде оформити платну підписку.

Згоба М. І.,
здобувачка вищої освіти Національного університету «Львівська політехніка»

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

ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ПРОГНОЗУВАННЯ ПОПИТУ НА ПАСАЖИРСЬКІ ПЕРЕВЕЗЕННЯ ТАКСІ

Вступ. Останнім часом нейронні мережі набирають неабиякої популярності, позаяк їх широко застосовують для розв'язання різних задач з багатьох предметних областей знань, наприклад, туризму, комерції, маркетингу та інші. Проте, для вирішення завдань прогнозування попиту на товари чи послуги за допомогою машинного навчання не знайшли широкого застосування у повсякденній роботі, наприклад, відповідних сервісів пасажирських перевезень. Для того, щоб нейронна мережа давала хороші прогнози, необхідно обробити значний набір вхідних даних [4]. Тренування мережі по суті означає вибір однієї моделі з множини дозволених моделей (або, в баєсовій системі – визначення розподілу над множиною дозволених моделей), що зводить витрати на її навчання до мінімуму. Щоб вирішити цю проблему якнайшвидше, застосовують розпаралелювання процедури навчання мережі з використанням графічних процесорів [2].

Для проведення дослідження у цій роботі взято за основу час, за який нейронна мережа проходить одну епоху (англ. *epoch*) тренування. Швидкість процедури навчання нейронної мережі залежить, насамперед, від обраного алгоритму її тренування та архітектури програмної системи, кількості наборів даних для її тренування та їхнього обсягу, комплектації апаратного забезпечення та його потужності. Дослідження виконано для двох різних конфігурацій апаратного забезпечення, аби показати користь від паралелізації нейронної мережі залежно від розміру вхідних даних у наборі та їхньої кількості [8].

Результати дослідження та їх обговорення. Найважливішим завданням будь-якої компанії та водія таксі є мінімізація тривалості очікування нових замовлень та відстані до клієнтів на момент їх надходження. Зараз водіям необхідно самостійно вирішувати, де чекати пасажирів, так щоб вони могли їх швидко забрати. Природно, що вони ніколи не можуть достовірно знати, у якому місці будуть майбутні пасажири, однак досвідчені водії можуть робити здогадки та прогнози на підставі своїх знань. Система відправки таксі ефективно допомагає клієнтам та водіям скоротити тривалість очікування як замовлення, так і самого таксі. Проте водії однаково не мають достатньої інформації про те, де чекати, щоб швидко приїхати до нового пасажира. А оператор таксі-центру може організувати та надіслати необхідну кількість водіїв до району, виходячи з історичних даних.

Дані для тренування. Для тренування нейронної мережі у роботі використовується набір вхідних даних, що містить 4,5 млн. поїздок таксі компанії Uber в межах Нью-Йорка за період з квітня по

жовтень 2014 року. Набір вхідних даних взято з відкритих джерел [3]. Для більшої точності передбачень зібрано та додано до набору даних погодинні метеорологічні дані за цей самий період, а саме температуру повітря та наявність семи видів атмосферних явищ.

Сформований нами набір вхідних даних для тренування нейронної мережі має такі атрибути: день, місяць і рік поїздки, широта та довгота початкової точки поїздки, температура повітря, наявність легкого, середнього та сильного дощу, наявність туману, серпанку, легкого снігу [7]. Широта та довгота початкової точки поїздки – це атрибути, які нейронна мережа повинна передбачати для визначення місцезнаходження пасажира у заданий час та наявну погоду [2, 6].

Багатошаровий перцептрон. Для передбачення місцезнаходження наступного пасажира використано *багатошаровий персептрон* (англ. *Multilayer Perceptron*) як один з видів нейронних мереж (рис. 1). Оскільки це різновид мережі прямого зв'язку з одним або декількома рівнями внутрішніх шарів між вхідним і вихідним шарами, то вхідний сигнал у такій мережі поширюється в одному напрямку, від шару до шару. Вихідні одиниці представляють гіперплощину в просторі шаблонів введення. Мережа складається з *M* шарів, кожен з яких містить $J_m, m = \overline{1, M}$ вузлів. Ваги від (*m*–1)-го шару до *m*-го шару позначаються w^{m-1}. Функція зміщення [1], виходу та активації *i*-го нейрона в *m*-му шарі, відповідно, позначається як $\theta_i^{(m)}$, $\theta_i^{(m)}$ та $\phi_i^{(m)}(\cdot)$.

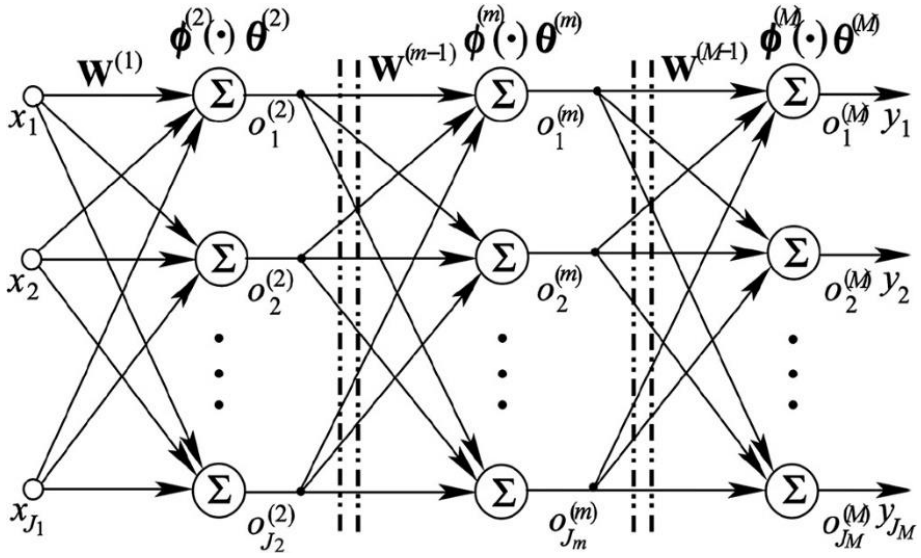


Рис. 1. Архітектура багатошарового персептрону

Багатошарові персептрони успішно застосовують для вирішення різноманітних завдань та мають такі особливості визнання. Кожна нейронна мережа має нелінійну функцію активації. Окрім шарів входу та виходу, такого типу нейронна мережа має декілька прихованих шарів.

Стохастичний градієнтний спуск. Найпоширенішою технікою для обчислення та оновлення ваг мережі є *стохастичний градієнтний спуск* SGD (англ. *Stochastic gradient descent*). SGD виконує такі кроки ітеративно. Спочатку обчислюється крок передачі вперед. Вхідні вибірки обробляються шар за шаром, поки не буде отримано прогноз після останнього шару. На наступному кроці, зворотному розповсюдженні, ваги оновлюються на підставі обчисленої різниці (градієнтів) між прогнозованими та позначеними результатами. Ці кроки виконуються ітеративно для всіх міні-пакетів (англ. *mini-batch*) у наборі даних. Як тільки всі міні-пакети опрацьовано, то одна епоха завершується. Це означає, що весь набір вхідних даних передавався вперед і назад через DNN тільки один раз. Процес можна продовжувати протягом наступних епох. SGD прагне мінімізувати функцію втрати, знаходячи ваги, які б у кращому випадку відповідали цілому набору даних. Отже, SGD виконує функцію апроксимації для всієї навчальної процедури [5].

Останнім часом набуває популярності використання оптимізатора типу SGD Adam. Він використовує квадратичні градієнти для масштабування швидкості процедури навчання, та імпульс, використовуючи ковзну середню градієнта замість самого градієнта. Метод використовує оцінки першого та другого моментів градієнта, щоб адаптувати швидкість процедури навчання для кожної ваги нейронної мережі. Adam добре підходить для вирішення проблем машинного навчання з великими

наборами даних, а також з глибокими багатошаровими нейронними мережами, частково завдяки хорошому коефіцієнту пам'яті.

Функції втрати (англ. *Loss function*) описує, наскільки далеко знаходиться мережа від здійснення ідеальних прогнозів для заданих даних. Результатом роботи функції втрати є відносне значення [6]. Якщо прогнози покращуються, то значення функції втрати зменшується. Вибір типу функції для нейронної мережі значною мірою залежить від проблеми, яку потрібно вирішити. Для прогнозування попиту на пасажирські перевезення таксі як функцію втрати найчастіше використовують *середньоквадратичну помилку* MSE (англ. *Mean Square Error*). Визначають яку суму квадратів відстаней між цільовою змінною та передбаченими значеннями, поділених на їх кількість, а саме

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(v_i y_i - y^p)^2, \qquad (1)$$

де: n – кількість нейронів у схованому шарі; v_i – вага синапсу j-го нейрона схованого шару до вихідного нейрона; y_i – вихідне значення j-го нейрона схованого шару (цільова змінна); y^p – поріг вихідного нейрона (передбачене значення).

Тренування нейронної мережі на графічному процесорі. Для будь-якої нейронної мережі стадія її навчання є найбільш ресурсомістким завданням. Якщо нейронна мережа має приблизно 10, 100 або навіть 100 000 параметрів, то звичайний комп'ютер однаково зможе впоратися з цим за лічені хвилини, чи десятки хвилин. Проте, якщо нейронна мережа має понад 10 мільярдів параметрів, тоді для її навчання, використовуючи традиційний підхід, були б потрібні місяці.

Глибока нейронна мережа DNN (англ. *Deep Neu Ral Network*) – це штучна нейронна мережа з декількома прихованими шарами. Подібно до звичайних нейронних мереж, глибокі нейронні мережі можуть моделювати складні нелінійні відносини між елементами. Під час навчання глибокої нейронної мережі отримувана модель намагається подати об'єкт у вигляді комбінації простих примітивів (наприклад, у задачі розпізнавання осіб такими примітивами можуть бути частини обличчя: ніс, очі, рот і т.д.). Додаткові шари дають змогу будувати абстракції все більш високих рівнів, що і дає можливість будувати моделі для розпізнавання складних об'єктів реального світу.

Навчання глибинних нейронних мереж можна здійснити за допомогою звичайного алгоритму зворотного поширення помилки. Існує велика кількість модифікацій такого алгоритму, в яких використовують декілька правил налаштування ваг. Наприклад, для навчання вагових коефіцієнтів $\omega_{ij}(t)$ можна використати алгоритм стохастичного градієнтного спуску:

$$\omega_{ij}(t+1) = \omega_{ij}(t) + \eta\frac{\partial C}{\partial \omega_{ij}},\ j = \overline{1,m};\ i = \overline{1,n}, \qquad (2)$$

де: η – стала для регулювання величини поточного кроку; C – функція втрат. Вибір функції втрат може бути обумовлений класом завдання машинного навчання (з учителем, без учителя, з підкріпленням) і функцією активації. До двох головних проблем глибоких нейронних мереж належать ті ж проблеми, що виникають і при навчанні звичайних нейронних мереж: тривалість навчання та перенавчання.

Через простоту реалізації та хорошу збіжність для реалізації процедури навчання глибоких нейронних мереж часто використовують метод зворотного поширення помилки і градієнтний спуск. Однак, при навчанні глибоких структур мережі виникає декілька проблем, які особливо важливі при оптимізації функцій втрат у просторі великої розмірності: кількість обчислювальних елементів, початкові умови для ваг мережі, а також константа регулювання величини кроку.

Глибинні нейронні мережі можна навчати значно швидше, виконуючи для цього всі операції одночасно, а не одну за одною. Цього можна досягти, застосовуючи графічний процесор, наприклад, GPU (англ. *Graphics Processing Unit*) – спеціалізований процесор із виділеною пам'яттю, який, зазвичай, виконує операції з плаваючою комою, необхідні для рендерингу графіки. Сучасні графічні процесори дуже ефективно обробляють та відображують комп'ютерну графіку завдяки спеціалізованій конвеєрній архітектурі, вони набагато ефективніші під час оброблення графічної інформації, ніж типовий центральний процесор. Також графічні процесори оптимізовані для навчання моделей штучного інтелекту та проведення глибокого навчання, оскільки вони можуть обробляти декілька обчислень одночасно.

Паралелізація даних в нейронних мережах. Ефективне навчання нейронних мереж є важливою частиною глибокого їх навчання. Зі збільшенням обсягу навчальних наборів даних й

складності моделі мережі пропорційно зростає обчислювальна потужність процесора та потреба в пам'яті комп'ютера. Пришвидшення процедури навчання сприяє підвищенню якості моделі, даючи можливість здійснити навчання нейронних мереж на значно більших наборах даних [8].

Паралельне навчання глибинних нейронних мереж має істотні переваги перед серійним навчанням. Нерідкі випадки, коли великі моделі нейронних мереж не можуть поміститися в пам'яті одного графічного процесора. Навчання різних частин моделі на різних графічних процесорах – це простий спосіб подолати обмеження пам'яті графічних процесорів. Водночас, застосування паралельних навчальних стратегій приводять до дещо швидшого навчання, розподіляючи перекриваючі обчислення між різними вузлами. Використання обчислень, зв'язку та перекриття введення/виведення даних сприяє кращому використанню обчислювальних ресурсів і, як наслідок, значно швидшій конвергенції при навчанні моделі мережі [4].

***Обговорення результатів дослідження*.** Дослідження здійснено на центральному процесорі, одному графічному процесорі NVIDIA Tesla K80 та на двох таких процесорах відповідно. Тренування мережі проведено на двох різних розмірах вхідних даних batch_size = 16 та batch_size = 2048. Результатом дослідження є порівняння часу для однієї епохи тренування. Дані, наведені на рис. 2,*а*, показують порівняння тривалості процедури навчання нейронної мережі для однієї епохи на одному центральному процесорі, одному та двох графічних процесорах, використовуючи для цього mini-batch розміром 16 проб. Це порівняння представлене на осі *X*. Вісь *Y* представляє функцію втрати – середньоквадратична помилка. Дослідження на одному графічному процесорі (червона лінія) пришвидшує тренування на центральному процесорі (чорна лінія) у 1.0715 разів. Таке невелике пришвидшення процедури навчання пояснюється малим розміром набору даних, що розпаралелюються (розмір mini-batch) та значними витратами часу для передачі даних між графічним і центральним процесором, який керує процедурою тренуванням.

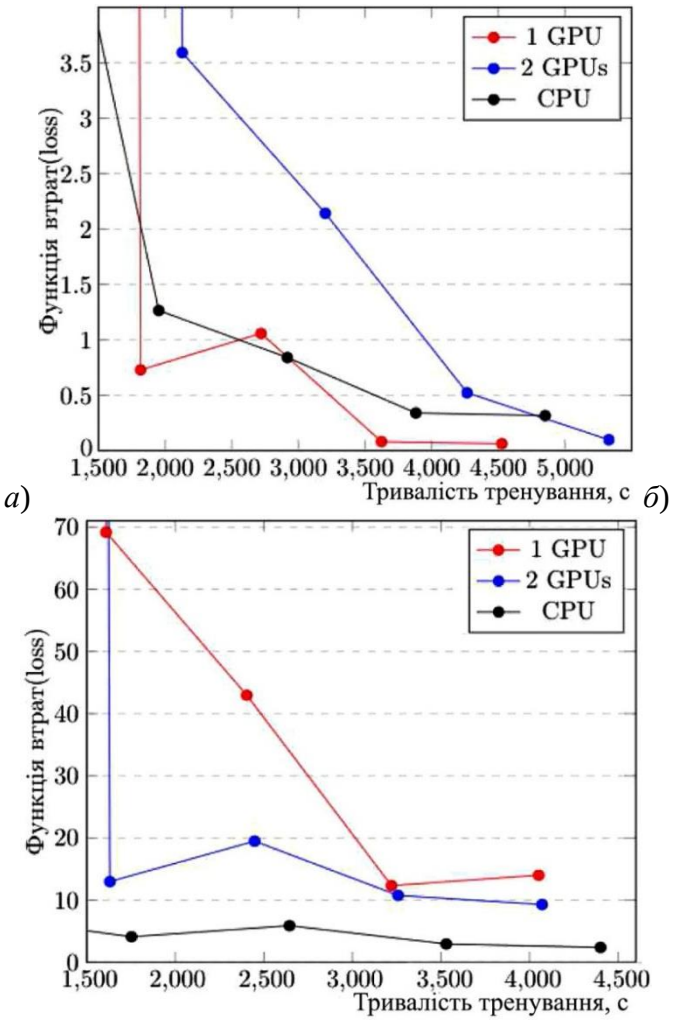


Рис. 2. Залежність тривалості процедури навчання від кількості використаних ресурсів: а) mini-batch = 16; б) mini-batch = 2048

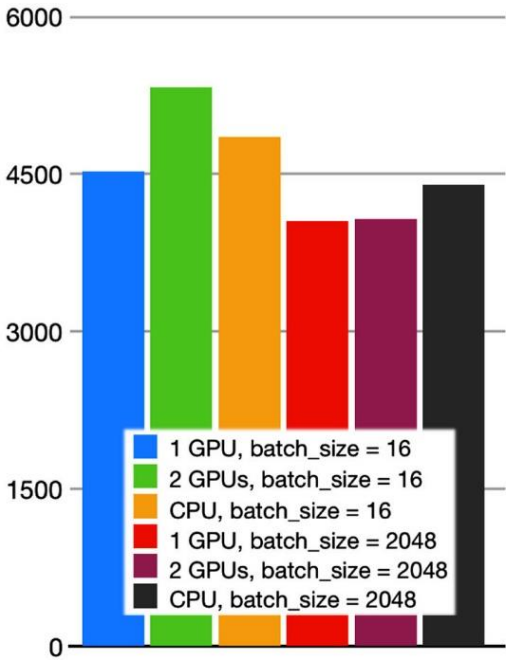


Рис. 3. Залежність тривалості процедури навчання від кількості використаних ресурсів

Тренування на двох графічних процесорах (синя лінія) погіршує тривалість процедури навчання мережі порівняно з тренуванням на одному графічному або центральному процесорі. Такий результат пояснюється високими витратами часу для синхронізації градієнтів спуску між двома графічними процесорами перед кожним оновленням параметрів мережі (після кожної batch-ітерації). Ці витрати для синхронізації не перекриваються ефектом від паралелізації обчислень, оскільки розмір вхідних даних, що розпаралелюються (розмір mini-batch), є занадто малим. Отже, при використанні mini-batch розміру 16 проб найоптимальнішим є тренування обраної конфігурації нейронної мережі для передбачення попиту на пасажирські перевезення таксі тільки на одному графічному процесорі.

Дані, наведені на рис. 3, показують результат порівняння тривалості процедури навчання нейронної мережі для однієї епохи на одному центральному процесорі, одному та двох графічних процесорах, використовуючи mini-batch розміром 2048 проб. Розмір вхідних даних, що розпаралелюються, mini-batch розмір, є у 128 разів більший за розмір вхідних даних, використаний для отримання результатів з рис. 2,*б*. Тренування нейронної мережі на одному (червона лінія) та двох (синя лінія) графічних процесорах є у 1.0861 та 1.0811 відповідно разів швидше, ніж тренування на одному центральному процесорі (чорна лінія). Порівняно з результатами для mini-batch розміру 16 проб, тренування на двох графічних процесорах відбувається значно швидше, ніж на одному центральному процесорі. Проте, немає пришвидшення між тренуванням мережі на одному та двох графічних процесорах, оскільки користь від паралелізації проведення обчислень на двох графічних процесорах компенсується витратами на синхронізацію між цими процесорами під тривалість тренування.

Інформація, наведена на рис. 3, також показує залежність тривалості процедури навчання нейронної мережі для однієї епохи між усіма використаними у цій роботі апаратними конфігураціями комп'ютерної техніки. Тренування на одному графічному процесорі з використанням mini-batch розміру 2048 проб було найменшим, водночас як аналогічне тренування на двох графічних процесорах розміру 16 проб було найбільшим. Різниця між тривалістю тренування нейронної мережі для однієї епохи знаходиться в межах сотень секунд для обраних апаратних конфігурацій та вибраної архітектури нейронної мережі.

Висновки. З'ясовано, що для мінімізації тривалості очікування нових замовлень та відстані до клієнтів на момент їх надходження, а саме для вирішення проблеми прогнозування попиту на пасажирські перевезення таксі, доцільно використовувати засоби машинного навчання. Встановлено, щоб досягти великої точності у прогнозуванні попиту на пасажирські перевезення таксі, нами опрацьовано великий набір вхідних даних, а саме 4,5 млн поїздок таксі. Для зменшення тривалості процесу тренування нейронної мережі застосовано розпаралелювання процедури її навчання з використанням графічних процесорів. Визначено, що пришвидшення процедури навчання нейронної мережі залежить від багатьох чинників: її архітектури, гіперпараметрів тренування, конфігурації апаратного забезпечення та методу паралелізації виконання розрахунків.

Література:

1. Du, K.-L., & Swamy, M.N.s. (2014). Multilayer Perceptrons: Architecture and Error Backpropagation. Neural Networks and Statistical Learning, pp. 83–126. https://doi.org/10.1007/978-1-4471-5571-3_4
2. Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2016). Region-Based Convolutional Networks for Accurate Object Detection and Segmentation. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(1), 142–158. https://doi.org/10.1109/TPAMI.2015.2437384
3. Jun Xu, Rouhollah Rahmatizadeh, Ladislau Bölöni, & Damla Turgut. (2018). Real-Time Prediction of Taxi Demand Using Recurrent Neural Networks. IEEE Transaction on Intelligent transport system, 19(8), 2572–2581. https://doi.org/10.1109/TITS.2017.2755684
4. Kennedy, R. K., Khoshgoftaar, T. M., Villanustre, F., & Humphrey, T. (2019). A parallel and distributed stochastic gradient descent implementation using commodity clusters. Journal of Big Data, 6(1), 16. https://doi.org/10.1186/s40537-019-0179-2
5. Li, J., Nicolae, B., Wozniak, J., & Bosilca, G. (2019). Understanding scalability and fine-grain parallelism of synchronous data parallel training. IEEE/ACM Workshop – Machine Learning in High Performance Computing Environments (MLHPC) IEEE, pp. 1–8. https://doi.org/10.1109/MLHPC49564.2019.00006
6. Ren, S., He, K., Girshick, R., & Sun, J. (2017). Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(6), 1137–1149. https://doi.org/10.1109/TPAMI.2016.2577031
7. Simonyan, K., & Zisserman, A. (2014). Very Deep Convolutional Networks for Large–Scale Image Recognition. CoRR, abs/1409.1556. https://doi.org/10.1.1.740.6937
8. Zghoba, M. I., & Hrytsiuk, Yu. I. (2020). Neural network training for forecasting the demand for passenger transportation by taxi using graphics processors. Ukrainian Journal of Information Technology, 2(1), 29–36. https://doi.org/10.23939/ujit2020.02.029

Феній Н. С.,
здобувач вищої освіти Національного університету «Львівська політехніка»

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

КЛАСИФІКАЦІЯ ТЕКСТОВИХ НОВИН З ІНТЕРНЕТ-САЙТІВ МЕТОДАМИ НЕЙРОННОЇ МЕРЕЖІ

Вступ. Класифікація текстової інформації, що знаходиться на різних інтернет-сайтах, – одне з основних завдань відповідних інтернет-сервісів щодо організації текстових даних, а також подальшого її зберігання у відповідних БД. Для вирішення такого завдання все частіше використовують методи інтелектуального аналізу текстів – Text Mining [1, 5], найчастіше – методами нейронних мереж [2, 3]. Їхня робота зводиться до встановлення прихованих закономірностей у аналізованих текстах та її класифікації. Завдання ускладнюється ще й тим, що безліч викладеної інформації на інтернет-сайтах є політематичною, тобто належить одночасно до декількох категорій. Водночас, більшість відомих на сьогодні методів класифікації такої інформації не враховують цієї особливості, позаяк орієнтовані на знаходження певних класів, а також не можуть в послідовному режимі класифікувати вхідні текстові дані, що є їхнім істотним недоліком.

Отже, на даний момент практично відсутні ефективні методи, що обробляють та здійснюють класифікацію політематичних текстових даних. Саме тому для багатьох дослідників актуальним завданням є розроблення таких методів Text Mining, які вирішували би окреслені вище проблеми.

Результати дослідження та їх обговорення. Поряд із значним зростанням кількості політематичних текстових новин виникає потреба автоматичного оброблення їхнього вмісту – проведення аналізу, здійснення класифікації, зберігання, реферування та інше. Для вирішення цих завдань використовують відповідне ПЗ та ефективні методи оброблення текстової інформації для великої кількості вхідних даних. Дослідження багатьох науковців [4, 7] показали, що наявні методи оброблення текстової інформації придатні для малих за обсягом даних і скеровані на вузьку тематику. Тому це не влаштовує багатьох замовників такої інформації з декількома тематиками водночас, наприклад, політематичної стрічки новин.

Завдання класифікації політематичних текстових даних. Розглянемо основні завдання класифікації політематичних текстових новин. Під класифікацією текстових даних розуміють процес віднесення масиву повнотекстових даних, які отримують після аналізу і пошуку їхньої внутрішньої тематичної структури, з наявністю у ньому апріорної інформації, тобто при наявності наперед визначеного рубрикатора і множини документів-зразків. За такої класифікації документи, зв'язані між собою, прагнуть бути релевантними одним і тим самим запитам, тобто нерелевантні запиту документи відокремлені від релевантних.

Завдання класифікації політематичних текстових даних у загальному вигляді можна сформулювати так: задано множину текстів природною мовою – масив політематичних текстових даних. Будемо вважати, що існує множина тематичних груп класів $\boldsymbol{C} = \{c_j,\ j = \overline{1, N_C}\}$, на які можна поділити масив даних, заданий в умові. Тоді, згідно з певним критерієм якості поділу даних, завдання їхньої класифікації полягає у знаходженні оптимальної скінченної множини класів $\boldsymbol{C}$, яка є невідомою.

Зазвичай, за вхідні дані приймаємо не самі тексти інформації природною мовою, а їхнє векторне подання $\vec{\boldsymbol{D}} = \{\vec{d}_j,\ j = \overline{1, N_D}\}$, які характеризують смисловий зміст текстових даних. Ознаки таких даних автоматично формуються відповідно до обраного способу подання текстової інформації й, найчастіше, є одинарними словами. Ознаки даних об'єднують в спільну множину $\boldsymbol{P} = \{p_l, l = \overline{1, N_P}\}$, а розмірністю вектору ознак кожного набору даних є N_P.

Для зниження обсягу вхідних даних, що є поширеною практикою поділу текстових даних, часто використовують метод головних компонент, внаслідок чого відбувається спрощення векторного подання $\vec{\boldsymbol{D}}$ за рахунок синонімів і омонімів. Базуючись на статичній інформації про множину текстових даних, таке спрощення тягне за собою значні обчислювальні витрати при великих обсягах вхідних даних.

Процес класифікації текстової інформації базується на аналізі тематичної схожості даних, визначення якої ґрунтується на припущенні, що геометрична близькість векторного подання $\vec{\boldsymbol{D}}$ в просторі ознак даних всього їхнього масиву означає дійсну схожість предметних областей таких даних.

Оцінка тематичної схожості даних ґрунтується на обчисленні деякої міри схожості $Sim(\vec{d}_i, \vec{d}_j)$. Часто використовуваними ступенями схожості між векторним поданням текстових даних у просторі їхніх ознак є міра, яка визначає значення косинуса між двома векторними поданнями [6]:

$$Sim(\vec{d}_i, \vec{d}_j) = \cos\left(\angle(\vec{d}_i, \vec{d}_j)\right) = \frac{\sum_{k=1}^{N_P} d_{ki} \cdot d_{kj}}{\sqrt{\sum_{k=1}^{N_P} d_{ki}^2} \cdot \sqrt{\sum_{k=1}^{N_P} d_{kj}^2}}$$

і ступеня близькості, що ґрунтується на вимірюванні відстані між векторними поданнями даних у багатовимірному просторі їхніх ознак:

$$Sim(\vec{d}_i, \vec{d}_j) = 1 - \left(\sum_{k=1}^{N_P} \left| d_{ik} - d_{jk} \right|^{v} \right)^{1/r},$$

де v і r – типів відстаней – параметри, які визначає користувач. Окремі випадки типів відстаней автоматичної класифікації текстових даних є достатньо розповсюдженими: евклідова відстань $(v = 2,\ r = 1/2)$, квадрат евклідової відстані $(v = 2,\ r = 1)$, манхеттенська відстань $(v = 1,\ r = 1)$.

Нейромережеві методи класифікації текстової інформації. На сьогодні навчання "з учителем" нейронної мережі є найбільш поширеною й очевидною парадигмою. В такому навчанні учителю відома інформація про зовнішнє середовище, яке задають у вигляді послідовності або пакету вхідних векторів x, а також "правильна реакція" на ці сигнали, яку подають у вигляді навчального сигналу d. Природним є те, що реакція ненавченої нейронної мережі y відрізняється від правильної реакції вчителя, внаслідок чого виникає помилка $e = d - y$. Тому, під час навчання штучної нейронної мережі необхідно налаштувати її параметри так, щоб деяка скалярна функція $E(e)$ (критерій якості) досягла свого мінімального значення. Якщо мережа повторює реакцію учителя, то можемо зробити висновок про те, що вона є навченою. Оскільки інформація про зовнішнє середовище зазвичай має

нестаціонарний характер, то для забезпечення неперервного навчання використовують ті чи інші рекурентні процедури.

Також достатньо широко розповсюджена технологія змішаного навчання, коли частину параметрів налаштовують за допомогою вчителя, а решта або їхню частину налаштовують шляхом самонавчання. В основі алгоритмів знаходяться певні правила навчання, що тісно пов'язані із наведеними парадигмами. Визначено п'ять основних правил: навчання на підставі корекції за помилкою, навчання за Больцманом чи за Хеббом, навчання пам'яті та конкурентне навчання [7].

За допомогою ймовірнісної нейронної мережі (PNN), введеної Д. Ф. Шпехтом [2, 3], можна достатньо ефективно вирішувати завдання класифікації текстових даних. В основі принципу навчання знаходиться метод "нейрони в точках даних", через що він є достатньо швидким у роботі та простим у реалізації. Існують також модифікації PNN, які призначені для оброблення текстової інформації, а відрізняються між собою наявністю елементів конкуренції у процесі навчання та можливістю корекції рецепторних полів. Але коли обсяги даних, над якими проводиться аналіз, надто великий, а вектори ознак мають достатньо велику розмірність, то завдання класифікації значно ускладнюється. Це пояснюється тим, що у всіх нейронних мережах, які навчаються за принципом "нейрони в точках даних", кількість нейронів першого прихованого шару визначається кількістю векторів-образів навчальної вибірки *N*. Через це значно знижується швидкодія алгоритму і потреби виділити місце для зберігання всіх даних, які використовують у процесі навчання. Для того, щоб зменшити вплив цього недоліку, у роботі [2] було запропоновано покращену ймовірнісну нейронну мережу (EPNN), де перший прихований шар поданий не образами, а прототипами класів, отриманими за допомогою звичайного *k*-середнього (HCM) у пакетному режимі. Оскільки у завданнях класифікації кількість можливих класів *m* зазвичай значно менше обсягу навчальної вибірки *N*, то нейронна мережа EPNN набагато краще пристосована для вирішення прикладних завдань, ніж мережа PNN.

Як і всі відомі методи, мережа EPNN має свої недоліки: можливість навчання є тільки у пакетному режимі; навчальна вибірка має бути задана наперед; чіткий результат класифікації отримують тоді, коли при обробленні текстової інформації аналізований текст за різними рівнями належності може належати відразу декільком класам, що перетинаються.

Особливості реалізації архітектури ПЗ. Для реалізації ПЗ було обрано клієнт-серверну архітектуру [7]. Вона є обчислювальною моделлю для розроблення комп'ютеризованих систем. Ця модель базується на розподілі функцій між двома типами незалежних і автономними процесами: сервер і клієнт. Клієнтом є будь-який процес, який вимагає конкретного запиту послуги з серверного процесу. Сервер – це процес, який надає запитані послуги клієнту. Процеси клієнта і сервера можуть перебувати на одному комп'ютері або на різних комп'ютерах, пов'язаних між собою локальною чи глобальною мережею.

Коли клієнтські та серверні процеси знаходяться на двох або більше незалежних комп'ютерах у мережі, то сервер може надавати послуги для більш ніж одного клієнта. Окрім цього, клієнт може запитувати послуги з декількох серверів у мережі без урахування їхнього розташування або фізичних характеристик комп'ютера, в якому знаходиться серверний процес. Мережа зв'язує сервер і клієнт разом, забезпечуючи середовище, через яке клієнти і сервер спілкуються між собою. Наведений нижче рис. 1 показує основну комп'ютерну модель клієнта-сервера.

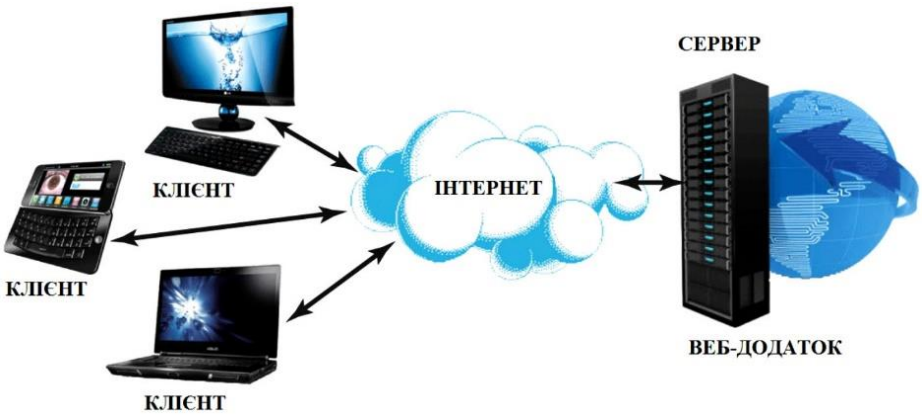


Рис. 1. Клієнт-серверна архітектурна модель роботи ПЗ

Такий тип архітектури має низку переваг серед інших моделей роботи ПЗ [7], а саме: забезпечення кращим обміном даних. Зазвичай, всі дані зберігаються в базі даних, тому стають доступні тільки авторизованим клієнтам. Дана властивість також захищає від несанкціонованого доступу до функцій серверу користувачам без доступу; ресурси спільні для різних платформ. Архітектура клієнт-сервер дає змогу додавати до ПЗ довільну кількість клієнтських частин на різних платформах: телефон, веб-додаток, комп'ютерний застосунок. При цьому не потрібно змінювати логіку роботи сервера і бази даних. Це економить як час роботи, так і додає певні гнучкості при розробленні ПЗ; легке обслуговування та краща безпека. Клієнт-серверна архітектура є розподіленою моделлю і тому її достатньо легко замінити, оновити та імпровізувати цю архітектуру. Знову ж таки, оскільки сервери мають кращий і ефективний контроль над ресурсами, безпека, яка забезпечується цією архітектурою, також є достатньо жорсткою. Водночас, архітектура веб-додатків в поєднані бібліотеки React.js і сервера майже ніколи не є завершеною, тому здебільшого є дуже складною для реалізації та супроводу. Прийнято використовувати додаткові бібліотеку React-Redux, схема роботи якої зображена на рис. 2.

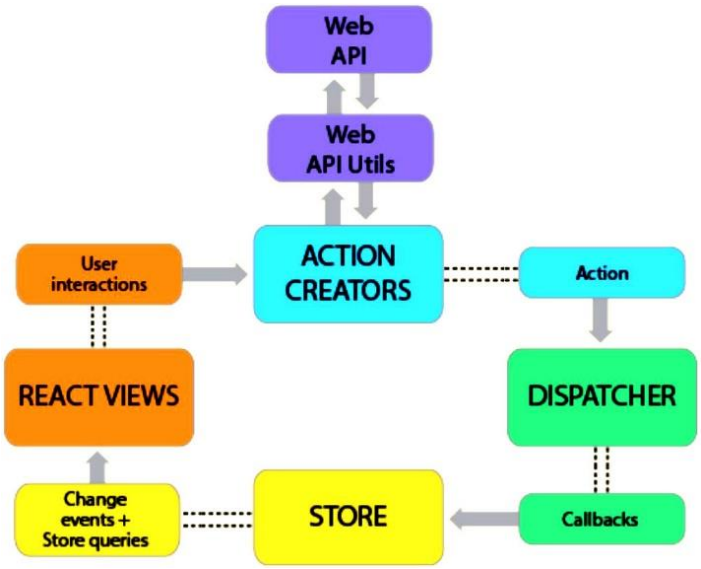


Рис. 2. Алгоритм роботи повноцінного React Native додатку

Для зручної передачі даних між елементами управління та екранами програмного продукту, бібліотека React-Redux забезпечує загальне сховище даних "Store", де програма зазвичай зберігає дані й доступається до них з будь-якого місця. Це сховище прослуховує події від "Dispatcher'а", зміни від якого будуть змінюватися в "Store" та відразу оновлюватися на елементах подання даних "View". Actions – помічники, які передають дані в "Dispatcher", а саме – назву події та дані, які необхідно обробити. Самі "View" містять елементи управління, при взаємодії користувача з якими відбувається подія і "Dispatcher" відправляє "вказівки", що робити з даними в Store. Action Creators – функції, які саме створюють дані події, тому вони можуть не тільки маніпулювати даними, але й робити зовнішні API виклики на сервери та обробляти інформацію звідти. Такий тип клієнт-серверної архітектури роботи ПЗ називають Flux (гнучким) і є не менш популярним, ніж MVC. Сервер програмної системи будується за принципами REST (англ. *Representational State Transfer*). Оскільки дані передаються без застосування додаткових шарів, тому REST вважається менш ресурсозатратним, ніж SOAP або XML-RPC, позаяк не треба "парсити" запит, щоб зрозуміти, що він повинен зробити, і не треба переводити дані з одного формату в інший. Кожна одиниця інформації однозначно визначається глобальним ідентифікатором, таким як URL. Кожна URL водночас має строго заданий формат. Для позначення цього, які дії сервер має виконати над даними за необхідним посиланням, використовують операції CRUD (англ. *Create, Read, Update, Delete*).

За зв'язок з базою даних відповідає бібліотека mongoose, вона представляє ODM (англ. *Object Data Modelling*) – бібліотеку і працює подібно до інструментів ORM. Вона забезпечує пряме, базоване на схемі, рішення, містить вбудоване приведення до типів, валідацію, створення запитів. Для ознайомлення із функціональними характеристиками веб-додатку розроблено відповідну діаграму

прецедентів (рис. 3). Для подання статичної складової фізичної архітектури системи реалізації веб-додатку розроблено діаграму розгортання [7, рис. 5]. На діаграмі зображено 4 частини веб-додатку, які містять клієнтську, дві серверні частини та частину бази даних. Для правильного розподілу ресурсів та коштів частина веб-додатку, яка здійснює складні обчислення, розміщена окремо та викликається тільки за потреби. Доступ до бази даних здійснюється з серверної частини веб-додатку середовища Node.js. Як систему управління базами даних було обрано нереляційну документо-орієнтовану базу даних MongoDB. СУБД займає нішу між швидкими і масштабованими системами, що оперують даними у форматі ключ-значення, і реляційними СКБД, функціональними і зручними у формуванні запитів.
Зберігання документів в базі даних відбувається у форматі JSON, що робить її гнучкою та дає змогу зберігати великі обсяги даних. Зазвичай, нереляційні бази даних не потребують цього ж обсягу підготовчих дій, які часто необхідні для реляційних баз, що значно пришвидшує розроблення ПЗ. В цьому можна побачити велику перевагу її використання для створення програмного продукту порівняно з реляційними базами даних. Модель фізичної моделі бази даних веб-сервісу створено за допомогою онлайн веб-додатку Lucidchart [7, рис. 6]. Веб-додаток реалізовано за допомогою системи інтегрованого розроблення Intellij Idea згідно з спроектованою архітектурою роботи ПЗ, зображеної на діаграмах, наведених у роботі [7].

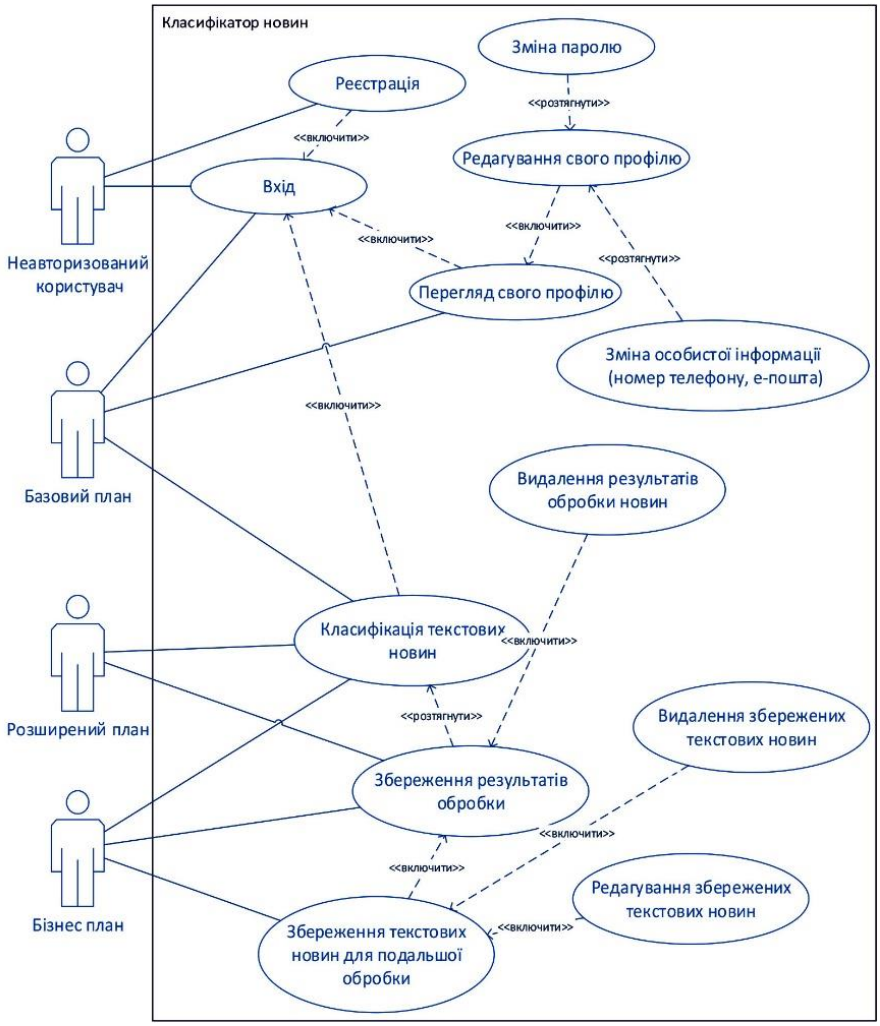


Рис. 3. Діаграма прецедентів длярозроблюваного веб-додатку

Висновки. Розроблено веб-додаток, за допомогою якого можна здійснювати класифікацію політематичних текстових новин в режимі онлайн, їх зберігати й редагувати, а також ставити їх у чергу для подальшого оброблення. Визначено метод для класифікації політематичних текстових новин, який може працювати в режимі онлайн та на вхід послідовно отримувати множину текстових даних. Спроектовано клієнт-серверну архітектуру веб-додатку для послідовної класифікації текстових новин в режимі онлайн та запропоновано набір додаткових функції, які дають змогу зберігати, обробляти та переглядати текстову інформацію, отриману внаслідок роботи веб-додатку або необхідної для його роботи.

Література:

1. Abdessalem, W. K. B., & Amdouni, S. (2011). E-recruiting support system based on Text Mining methods. International Journal of Knowledge and Learning, 7(3), 220–232. https://doi.org/10.1504/IJKL.2011.044542
2. Ciarelli, P. M., & Oliveira, E. (2009). An enhanced probobalistic neural network approach applied to text classification. Lecture Notes on Computer Science, 5856, 661–668. Berlin-Heidelberg: Springer-Verlag.
3. Jonsson, H., Nugues, P., Bach, C., & Gunnarsson, J. (2010). Text Mining of personal communication. In 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN), (pp. 1–5). New York, NY: IEEE. https://doi.org/10.1109/ICIN.2010.5640938
4. Lan, M., Tan, C. L., Su, J., & Lu, Y. (2009). Supervised and traditional term weighting methods for automatic text categorization. IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(4), 721–735. https://doi.org/10.1109/TPAMI.2008.110
5. Lee, S., Baker, J., Song, J., Wetherbe, J. C. (2010). An empirical comparison of four Text Mining methods. In 43rd Hawaii International Conference on System Sciences (HICSS), (pp. 1–10). https://doi.org/10.1109/HICSS.2010.48
6. Song, F., Liu, S., & Yang, J. (2005). A comparative study on text representation schemes in text categorization. Pattern Analysis and Applications, 8(1-2), 199–209. https://doi.org/10.1007/s10044-005-0256-3
7. Fenii, N. S., & Hrytsiuk, Yu. I. (2020). Automation of the process of classification of text news from internet sites by neural network methods. Scientific Bulletin of UNFU, 30(4), 123–133. https://doi.org/10.36930/40300421

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

Коляда Д. В.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ДИСТАНЦІЙНОГО НАВЧАННЯ НА КАРАНТИНІ

Всіх нас застала глобальна проблема пандемії. Все суспільство вимушене звикати до нових реаліїв життя.

Ключові слова: дистанційне навчання, проблеми, викладачі, студенти, інформаційні-технології.

*Проблема:*поява пандемії змусила школи, вищі навчальні заклади та інші заклади освіти перейти на новий для нас спосіб навчання-дистанційне. Дистанційне навчання має свої плюси та мінуси. Такий вид навчання спричиняє деякі труднощі як для курсантів та студентів ,так і для викладачів.

Основна цінність дистанційного навчання (звісно, крім можливості навчання на відстані) це навчання у своєму темпі за своєю індивідуальною програмою. Але реально жоден відомий авторам ресурс такої можливості не надає. Основні причини цього: немає навчальних ресурсів, які повноцінно змістовно наповнені, якісно структуровані і потенційно можуть забезпечити формування змісту необхідної програми навчання на замовлення; немає середовища, яке дозволяє ефективно формувати й адмініструвати індивідуальні програми навчання одночасно для багатьох курсантів та студентів; не існує системи (організаційно, технологічно, нормативно), яка забезпечує розроблення, оновлення й адміністрування відповідних навчальних ресурсів і адміністрування самого процесу індивідуального дистанційного навчання одночасно великої кількості курсантів та студентів; немає системи підготовки тьюторів (викладачів) дистанційного навчання [1].

Основний матеріал: Як визначено в наказі Міністерства освіти і науки України від 25.04.2013 № 466 “Про затвердження Положення про дистанційне навчання”, зареєстрованого в Міністерстві юстиції України 30 квітня 2013 р. за № 703/23235, дистанційне навчання — це індивідуалізований процес набуття знань, умінь, навичок і способів пізнавальної діяльності людини, який відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників навчального процесу у спеціалізованому середовищі, яке функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій.

Дистанційна форма навчання передбачає доступ до інтернету, технічне забезпечення (комп’ютер, планшет, смартфон тощо) в усіх учасників освітнього процесу.

Дистанційне навчання це та тема яка важлива як для дітей, так і для викладачів.

Проблема з якою ми стикаємось відразу після переходу на такий вид навчання це навчити викладачів, які до дистанційного навчання не користувалися в роботі електронними засобами. В цьому випадку ми маємо використати експрес-навчання. Сьогодні весь світ перебуває в умовах необхідності працювати по-іншому. Не варто тиснути на викладача, якщо в нього щось не виходить. Важливі підтримка й допомога. Занадто високі вимоги до «віртуального ідеального» вчителя або учня, а також відсутність чіткої нормативно-правової бази в умовах існування багатьох інших освітніх проблем щодо впровадження дистанційного навчання не сприяють ефективному вирішенню проблеми [2].

Для курсантів та студентів та викладачів невід'ємною частиною є комунікація. Це основний компонент освітнього процесу. Від рівня комунікації залежить ефективність навчання. Тому ще однією проблемою для викладача на дистанційному навчанні це забезпечити потрібний рівень комунікації з учнем, а також постає питання про стимулювання до навчання. Тому що, основна мета комунікації це забезпечити заохочення до навчання.

Дистанційне навчання базується на принципі гнучкості місця, часу, темпу та траєкторії навчання, і використати ці переваги. Можливість впливати на деякі аспекти свого навчання підвищує внутрішню мотивацію курсантів та студентів, тож варто дати їм вибір у тому, які завдання виконувати (наприклад, 3 з 5 запропонованих), у якому порядку, за яким розкладом (у межах навчального тижня). Самостійна відповідальність за власну навчальну траєкторію формується поступово, тому варто нарощувати автономність у процесі навчання [3].

На квітень-жовтень 2020 року за опитуванням 73% викладачів вважають, що не всі студенти виходять на зв'язок – роблять запропоновані завдання, беруть участь в онлайн-заходах тощо.

Також половина бачать проблемою відсутність попереднього досвіду організації дистанційного навчання. 14,4% вказали, що проблемою є відсутність потрібної техніки вдома, 5% – відсутність потрібної техніки в навчальному закладі, а 2,3% – відсутність необхідної техніки в курсантів та студентів.

Висновок: Отже ми можемо окреслити такі шляхи розв'язання проблем. Стратегічний шлях, яким ми йдемо, це:

- створення чітко структурованого банку навчальних елементів, з яких можна формувати конкретну індивідуальну програму навчання;
- створення середовища адміністрування навчальних елементів і формування індивідуальних програм (ресурсів) дистанційного навчання;
- створення середовища дистанційного навчання, яке поєднано з банком навчальних елементів, і підтримує індивідуальний формат навчання за індивідуальними програмами;
- створення соціальної мережі, яка забезпечує розроблення, оновлення й адміністрування відповідних навчальних ресурсів і адміністрування самого процесу індивідуального дистанційного навчання;
- підготовка тьюторів-викладачів безпосередньо на роботі.

Література:

1. Міністерство охорони здоров'я. Організація дистанційного навчання. Методичні рекомендації [Електронний ресурс] / Охорони Здоров'я Міністерство – Режим доступу до ресурсу: https://mon.gov.ua/storage/app/media/zagalna%20serednya/metodichni%20recomendazii/2020/metodichni%20recomendazii-dustanciyna%20osvita-2020.pdf.

2. Дослідження стану реалізації дистанційного навчання в Україні [Електронний ресурс]. – 13. – Режим доступу до ресурсу: https://nus.org.ua/news/najbilsha-problema-shho-uchni-ne-vyhodyat-na-zv-yazok-doslidzhennya-dystantsijnogo-navchannya-v-ukrayini/.

3. Богачков Ю. М. ДИСТАНЦІЙНЕ НАВЧАННЯ – МОЖЛИВОСТІ І ПРОБЛЕМИ [Електронний ресурс] / Ю. М. Богачков, П. С. Ухань, Ю. Л. Новіков – Режим доступу до ресурсу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=komp_2011_2_9.

Кашперський О. С.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

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

СОЦІАЛЬНІ МЕРЕЖІ ТА ЇХ РОЛЬ У РОБОТІ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У наш час, кожна людина позиціонує себе як інформаційно-забезпеченою, іншими словами як активний користувач мережі "Інтерент". Він міцно увійшов у наше повсякденне життя. Ми активно користуємося Інтернетом вдома, на роботі, з розвитком нових технологій Інтернет перекочував в наші мобільні телефони і смартфони. Що дало нам можливість практично весь час перебувати on-line. Поява Інтернету радикально змінила форми, зміст, механізми, функції соціальних комунікацій. З розвитком Інтернету, з'явилася можливість використовувати всі його досягнення в різних його проявах. Одним з таких проявів стали соціальні мережі, які набули на сьогодні статусу невід'ємного атрибуту нашого життя. Представити сучасну людину без соціальних мереж просто неможливо. Перш за все, пропонуємо визначити, що саме таке соціальні мережі?

Соціальна мережа – це мережа людей, які зустрічаються в Інтернеті для спілкування, розміщуючи інформацію та зображення, залишаючи коментарі чи надсилаючи повідомлення. Учасники можуть розширити свої особисті та ділові контакти, зв'язавшись з іншими на веб-сайтах соціальних мереж та в додатках [1].

Через що, люди зв'язуються між собою? Бажання людей поділитися власним досвідом, своїми емоціями або просто поспілкуватися з людьми - це і є причина використання соціальних мереж людьми, як засобу зв'язку. Це бажання ділитися і спілкуватися, зумовлене взаємозалежністю. Люди залежать один від одного для схвалення, визнання та соціалізації. Взаємозалежність може базуватися на: дружбі, спорідненості, спільних інтересах, фінансовому обміні, або спільним переконанням [2].

Ви можете задатися питанням, до чого тут робота працівників Національної поліції України? А все дуже просто та прозоро. Як відомо, те що з'явилося в інтернеті, назавжди залишається в ньому, опубліковані фото з закріпленою за ним геолокацією, відправлене повідомлення, або закріплене повідомлення на оформленні власної сторінки, з метою донести власні думки усім, хто на неї заходить. Тому можна сказати, що особиста сторінка у соціальній мережі - це свого роду особиста справа, яку люди самі собі створюють. Завдяки якій можна: відслідкувати перебування власника сторінки, по фото та закріпленою за ним геолокацією, також є можливість дізнатися про коло спілкування, через друзів у додатку, ще є можливість дізнатися про вподобання особи переглянувши її публікації. Проаналізувавши все вище перелічене, ми дійсно знаходимо щось спільне, між особистою сторінкою та особистою справою особи.

Тому з ціллю пошуку можливих правопорушників, шахраїв, безвісти зниклих осіб, використовуючи мережу "Інтеренет" в Україні було створено спеціальний підрозділ, кіберполіція, який займається з вище перерахованими завданнями.

Отже, можна дійти висновку, що соціальні мережі відіграють досить значну роль у отриманні поліцейськими оперативної інформації та інформації під час досудового розслідування, що допомагає їм у виконанні своїх службових обов'язків.

Література:

1. Електронна стаття "Що таке соціальні мережі?(види,класифікація,безпека...) URL: https://futurenow.com.ua/shho-take-sotsialni-merezhi-vydy-klasyfikatsiya-bezpeka/

2. Електронна стаття "Соціальні мережі: різні аспекти впливу на людину" URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_berkiy_Social_networks_and_there_involves/

Мартинець І. В.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Синиціна Ю. П.,
доцент кафедри економічної та інформаційної безпеки
Дніпропетровського Державного університету внутрішніх справ, кандидат технічних наук, доцент

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СУЧАСНОМУ СУСПІЛЬСТВІ

На даний момент, інформаційна сфера обслуговує практично всі аспекти суспільного життя, наприклад: політику, науку, економіку, культуру і тощо. Інформаційна безпека - це стан захищеності систем обробки, зберігання даних, інформації від випадкових або навмисних дій, які можуть завдати шкоду суб'єктам інформаційних відносин при якому забезпечено конфіденційність, доступність і цілісність інформації.

Вагомі внески у досліджені проблема інформаційної безпеки у сучасному суспільстві внесені Я. І. Чмир, І. Р. Боднар, Р. В. Грищук, К. В. Молодецька-Гринчук та ін. Питанням ролі і місця проблема інформаційної безпеки у суспільстві приділено увагу в роботах А. В. Войціховський,С. В. Бєлай та Д. М. Корнієнко. Втім, за кожним стриманим кроком наукового пошуку відкриваються ще більші горизонти безмежного пізнання дійсності [1, 2].

На сьогодні інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни та суспільства. Зазначене обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, істотним зростанням впливу інформаційної сфери на життя нашого суспільства [3].

Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну та телекомунікації (рис. 1). Масштабний доступ до інформаційних ресурсів, призвели до глобалізації інформаційного простору. Таким чином це спричинило появу негативних наслідків, які пов'язані з інформаційною безпекою держави, перенесення конфліктів між провідними державами світу, розвитку кіберзлочинності та впливу на засоби масової комунікації.

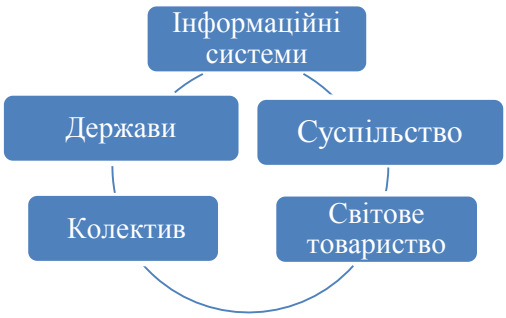


Рис. 1. Об'єкти інформаційної безпеки

До основних негативних наслідків глобалізації інформаційного простору можна віднести: появу нових видів інформаційних загроз; втрата національних форм культури; сплеск транснаціональної злочинності; злочинності в інформаційному (кіберпросторі) (рис. 2).

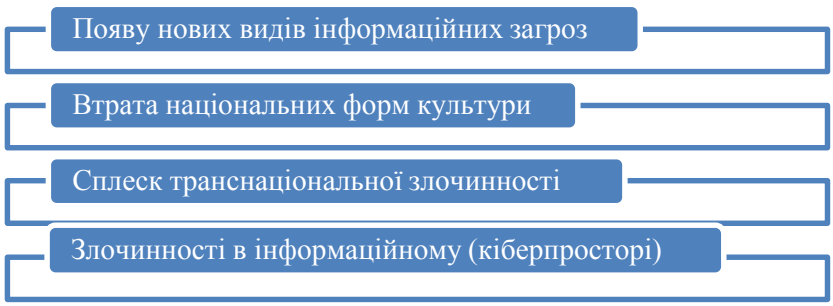


Рис. 2. Негативні наслідки глобалізації інформаційного простору

Постійне джерело інформаційних загроз корениться і в неврегульованих міжнародних відносинах, міжнародній конкуренції і зіткненні національних інтересів, у войовничості націй,відмінності життєво важливих цілей і інтересів держав.

До основних джерел інформаційних загроз відносяться: загрози обумовлені діями суб'єкта; загрози обумовлені технічними засобами; стихійні джерела (рис. 3).

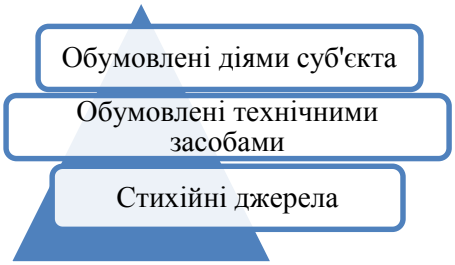


Рис. 3. Джерела інформаційних загроз

У XXI ст. перебудувати міждержавні відносини не вдалося. Локальні війни, міжнародний терор, сепаратистські рухи починалися і супроводжуються інформаційними війнами. В підривну інформаційну діяльність проти інших держав сьогодні включено безліч спецслужб, які володіють величезними матеріальними людськими ресурсами. А це означає, що інформаційна безпека є об'єктом не тільки внутрішньої, але й міжнародної політики. Це боротьба за культуру і взаємну повагу прав і обов'язків у міжнародних відносинах [4].

Отже,с цим треба бути обережно і виділяти час на інформаційну безпеку, так як є загроза розголошення інформації, яка становить державну таємницю, вплив засобів масової інформації на свідомість людини та суспільства. Треба зрозуміти властивість, сутність інформаційної небезпеки ішляхів її запобігання.

Література:

1. Аспекти публічного правління Том 6 № 9 2018/Чмир Я.І. / Проблеми забезпечення інформаційної безпеки в системі публічного управління - С.16

2. Механізм регулювання економіки, 2014, № 1 /І.Р.Боднар / Інформаційна безпека як основа національної безпеки - С.68

3. Сучасний захист інформації №1(33), 2018 / Р. В. Грищук, К. В. Молодецька-Гринчук/ Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах - С.43

4. Вісник Харківського національного університету ім. В.Н.Каразіна. Серія «ПРАВО». Вип. 29, 2020 / Войціховський А. В. / Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід) – С. 281

5. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. / Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпекиС.408

6. Аспекти публічного правління Том 6 № 9 2018/Проблеми забезпечення інформаційної безпеки в системі публічного управління - С.17

7. Політологічний вісник/ Інформаційна безпека України: загрози, зумовлені цивілізаційним вибором європейських цінностей / Дзьобань, О.П. Данильян, О. Г. – С. 63.

Чечель А. О.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

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

ПОШУК ЗНИКЛИХ ДІТЕЙ ЯК ОДИН ІЗ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення національної безпеки є досить актуальною проблемою, адже у зв'язку зі стрімким процесом реформування та бурхливим розвитком інноваційних технологій інформаційні ресурси, до

яких надано доступ лише державним службовцям, знаходяться у відкритому доступі, що негативно впливає на збереження важливої інформації, яка у подальшому використовується не за призначенням та взагалі втрачає свою цінність в роботі правоохоронних органів.

Досить важливу роль у всіх сферах життєдіяльності займають інформаційні технології. Важко уявити сучасне повсякдення без комп'ютерів, смартфонів, телевізорів, тощо. Інноваційні технології не лише урізноманітнили життя людей, але й набагато полегшили їх роботу.

Міністерство внутрішніх справ України не є виключенням з переліку сфер, де інформаційні технології є необхідними для забезпечення ефективної роботи всієї правоохоронної структури. Як зазначалося вище, інформаційні технології перш за все пов'язані з національною безпекою, адже колообіг інформації та даних, які використовуються правоохоронними органами кожного дня має великий об'єм та закритий доступ.

Сьогодні поліції користується низкою інформаційних систем (базами даних), в яких накопляється, обробляється та зберігається інформація.

В правоохоронній системі діє цілий комплекс науково-технічних, довідково-інформаційних, технологічних та нормативних заходів, які мають на меті забезпечити повсякденну роботу всієї правоохоронної системи.

Слід зауважити, що бази даних використовуються поліцією перш за все задля боротьби зі злочинністю. Але не лише пошук та виявлення злочинців входить до завдань поліції. Одним з таких завдань є надання допомоги особам, які цього потребують.

Також, не всі бази даних використовуються задля виявлення злочинців. Досить розповсюдженою проблемою є пошук дітей. В правоохоронній структурі також функціонує інформаційна система «Пошук дітей», яка розшукує дітей в межах від 1000–3000 метрів [1].

Очевидно, що кількість дітей, які зникали почала зростати, та постало питання про необхідність вдосконалення роботи вищезазначеної бази даних. З огляду на таку проблему, уповноважені представники «Київстар» і Національної поліції України підписали Меморандум про співпрацю, у рамках якого впроваджується спільна соціальна послуга «Пошук дітей».

Завдяки даній співпраці за 2019-2020 роки Національній поліції вдалося розшукати 485 дітей. Специфіка роботи даної послуги полягає в тому, «Київстар» отримує від поліції запит на SMS-розсилку, що містить інформацію про зниклу дитину та місце, де її бачили востаннє, після чого дану розсилку «Київстар» розповсюджує такі повідомлення на номери абонентів, які могли бути свідками зникнення, адже вони користувалися послугами зв'язку (телефонували, писали SMS або користувалися мобільним інтернетом) у радіусі 1–3 км від місця події. [2]. У повідомленні міститься посилання на сайт Міністерства внутрішніх справ України, де знаходиться фотокартка зниклої дитини та її особливі прикмети.

На нашу думку, це досить позитивна співпраця між ПрАТ «Київстар» та представниками Національної поліції України, але слід зауважити, що не всі особи користуються послугами ПрАТ «Київстар», окрім даного тарифу є також ПрАТ «ВФ Україна» та ТОВ «ЛАЙФСЕЛЛ», тобто така співпраця повинна бути з усіма операторами мобільного зв'язку.

Слід зауважити, що окрім пошуку дітей Україна зацікавлена в запровадженні проекту «PROJECT LIFESAVER», який надає працівникам поліції багато переваг у пошуку осіб з когнітивними розладами, які схильні до небезпечного для життя поведінки. Даний проект запроваджений та вже досить ефективно діє в США. [3, с.229]. Особливістю даного проекту є те, що дана програма поєднує в собі найсучасніші технологічні та інформаційні методи визначення та пошуку місцезнаходження таких осіб. Крім того, пошук осіб, які страждають на вищевказані захворювання скоротився з днів та годин до хвилин.

Очевидно, що вищевказаний проект також необхідний задля запровадження в Україні, адже в нашій країні також існує великий відсоток осіб, які страждають когнітивними розладами, тому задля допомоги таким особам та їх близьким родичам необхідно реалізувати проект «PROJECT LIFESAVER».

У підсумку варто зазначити, що завдяки впровадженню такої співпраці з усіма операторами мобільного зв'язку,а не лише з ПрАТ «Київстар», вдасться не лише збільшити відсоток можливості знайдення дитини, але й залучити якомога більше населення до допомоги правоохоронним органам.

Також, досить важливим є впровадження проекту «PROJECT LIFESAVER», який орієнтований на пошук осіб з когнітивними розладами та іншими психічними захворюваннями, що також є однією з проблем, з якими стикаються правоохоронці кожного дня.

Література:

1. Аналітично-пошукові функції сучасних інформаційних систем. Можливості використання результатів аналізу в розкритті та розслідуванні злочинів URL:https://pravo.studio/osnovyi-kriminalistiki/analitichno-poshukovi-funktsijisuchasnih_html (дата звернення: 09.11.2020).
2. Пошук дітей. ПрАТ «Київстар».: веб-сайт. URL: https://kyivstar.ua/uk/about/responsibility/kidsearch (дата звернення: 09.11.2020).
3. Рижкова С. А. Рижков Е. В. Використання досвіду проекту «PROJECT LIFESAVER» у пошуковій роботі Національної поліції // Міжнародна та національна безпека: теоретичні і прикладні аспекти: Матеріали IV Міжнародної науково-практичної конференції (ДДУВС, 13.03.2020). с.229-231. (дата звернення: 09.11.2020).

Романенко П. П.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Черкас О. В.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

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

ПОПЕРЕДЖЕННЯ НАРКОМАНІЇ НА ОСНОВІ КОНТЕНТ-АНАЛІЗУ У МЕРЕЖІ ІНТЕРНЕТ

Проблема наркотрафіку в інтернеті на сьогодні є актуальною та мало дослідженою. У новому тисячолітті інформаційна революція, яка відкрила людям нові можливості у сфері отримання та обробки інформації та викликала глобалізацію людства, стала однією з головних причин виникнення інтернет злочинності, також і у сфері розповсюдження наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів. Тому вивчення цього питання з метою профілактики та протидії розповсюдженню наркотиків є досить важливим.

Зараз в мережі інтернет функціонує безліч сайтів на яких розміщується реклама з продажу наркотичних препаратів невідомого походження та дозування, формули та рецепти їх виготовлення, які перебувають у відкритому доступі. Реклама сайтів та електронних адрес розповсюджувачів цих речовин знаходиться на кожному боці, тому придбати собі дозу не є великою проблемою навіть для звичайного підлітка. Для збуту своїх товарів наркодилери використовують різні соціальні мережі, найпопулярнішою з яких є програма для обміну миттєвими текстовими повідомленнями – Telegram. Цю програму використовують через анонімність повідомлень. Розробники схеми збуту наркотиків застосовують алгоритм шифрування, через який при спробі зламати цю соцмережу, ані інформацію про них та ні саме листування правоохоронці отримати не зможуть. За інформацією з груп в Telegram оплата відбувається через термінали iBox в біткойнах, а це є найбезпечнішим шляхом оплати, адже неможливо ідентифікувати наркодилерів. І це є головною проблемою у розслідуванні таких злочинів [1].

В Україні наркоторгівля через мережу інтернет набирає небачених обертів. Дилери використовують так звану схему «закладок», це коли наркоторгівці наймають особу, яка ховає дозу у будь-якому місці міста та відправляє фото з місцезнаходженням препарату. Таким чином контакт відбувається через спеціальний протокол обміну повідомленнями, який шифрує листування, а не особисто між продавцем та покупцем.

Поки кількість смертей від наркозалежності невпинно збільшується, правоохоронці лише розводять руками, адже для відстеження наркоторгівців в інтернеті необхідне відповідне матеріально-технічне забезпечення, якого наразі немає. Тому, щоб допомогти поліцейським, у Харківському національному університеті внутрішніх справ курсантами було створено чат-бот-програму, яка відстежує злочинців у популярному серед наркодилерів месенджері Telegram. За допомогою програми вони формують базу даних, аналізують сторінки та передають інформацію правоохоронцям. У ній будь-який користувач може поскаржитися на підозрілі сторінки онлайн-магазинів, відправити фото з намальованими на стіні лінками та зазначити геолокацію цих місць. За два тижні роботи, до чату приєдналися майже шість із половиною тисяч користувачів. Розробники кажуть: що більше надходитиме

скарг на сторінки магазинів із продажу наркотиків, то швидше вони блокуватимуться. А це завдасть неабияких збитків наркоторговцям [2].

Для протидії кіберзлочинності, зокрема й розповсюдженню наркотиків мережею інтернет в Україні діє закон «Про основні засади забезпечення кібербезпеки в Україні» від 05.10.2017 року, який визначає правові основи забезпечення захисту інтересів людини і громадянина, суспільства та держави [3]. Також в Україні від 01.07.2006 діє міжнародна Конвенція про кіберзлочинність, у якій розглядається механізм про міжнародну співпрацю в розслідуванні даних злочинів. А саме, за її умовами країни мають надати повноваження правоохоронним органам щодо здійснення перехоплення інформації та вилучення комп'ютерних даних [4].

Отже, підсумовуючи сказане можна зробити висновок, що збут наркотиків з використанням сучасних інформаційних технологій є серйозною проблемою яка набирає оборотів. Для її вирішення потрібно докласти багато зусиль у створенні нових підрозділів кіберполіції, удосконаленні матеріально-технічного забезпечення та методів боротьби з наркотрафіком.Я вважаю, що для зменшення кількості сайтів з продажу нарктотичних засобів, психотропних речовин їх аналогів та прекурсорів потрібно запровадити моніторинг розповсюдження цих препаратів у всіх школах та ЗВО України, адже вживання наркотиків є найбільш розповсюдженим серед молоді. Це допоможе значно зменшити кількість наркозелижних у нашій країні.

Література:

1. Ступник Я. В., Когут М. Г. Протидія наркозлочинності в мережі Інтернет: виклики сьогодення // Науковий вісник Ужгородського національного університету. Серія Право., Випуск 22. 2014. - С. 226-230.
2. У Харкові студенти створили чат-бота для боротьби з он-лайн-наркоторговцями – як він працює? // Веб-сайт : URL: https://www.5.ua (дата звернення 17.11.2020.)
3. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними : Закон України від 05.10.2017 № 2163-VIII.
4. Конвенція про кіберзлочинність. Рада Європи; Міжнародний документ від 23.11.2001. – Режим доступу : http:// zakon2.rada.gov.ua/laws/show/994_575.

Лукащук Ю. А.,
Аспірант Національного університету «Львівська політехніка»

Лукащук Д. А.,
магістр прикладної математики

ХМАРНІ СЕРВІСИ ДЛЯ ОНЛАЙН НАВЧАННЯ

Нові економічні та соціальні реалії життя суспільства вимагають формування нових ключових компетентностей особистості – професійних, соціальних та інформаційних. В інформаційному суспільстві зростає потреба формування інноваційних професійних компетентностей студентів. Для сучасної освіти характерним є пошук нових можливостей, пов'язаних з поєднанням традиційних форм навчання з використанням сучасних наукових розробок та напрацювань у галузі інформаційних технологій з урахуванням запитів суспільства, збільшення вимог до якості підготовки фахівців та інтеграції у міжнародний освітній простір. Зокрема затребуваними є такі освітні системи, які передбачають відкритість матеріалів для коментування, редагування в необхідних випадках та адаптації під конкретного користувача. Запровадження інформаційно-комунікаційних технологій в систему освіти веде до появи нових методів, організаційних форм та засобів навчання, інтенсифікацію всіх рівнів освітнього процесу, підвищення його результативності, розвиток творчого потенціалу студентів, формування їх інформаційної культури та медіаграмотності, здатності до критичного та водночас творчого мислення. У контексті інноваційного розвитку освіти на основі інформаційно-комунікаційних технологій значні перспективи має навчання за дистанційною формою.

Концепція хмарної технології передбачає можливість самостійного створення, наповнення та редагування контенту користувачем. При цьому контент зберігається на сервері компанії-розробника, а

не на комп'ютері користувача. Прикладом одного з найбільш успішних впроваджень хмарних технологій є Вікіпедія.

Використання хмарних технологій в освіті є новим явищем. Застосування цих інноваційних форм і сервісів сприяє інтенсифікації процесу навчання, підвищенню рівня фахової підготовки здобувачів вищої освіти, економії фінансових, матеріальних і кадрових ресурсів. А в умовах пандемічних загроз – уникнення ризику масових заражень.

Назагал хмарні технології узагальнюють такі поняття:

- - контент створює користувач;
- - контент зберігається на віддаленому сервері;
- - відкритий доступ до матеріалів великої кількості користувачів. При цьому право втручання у контент, його перегляд та редагування надається власником контенту (розмежування прав доступу).

На сьогодні кількість хмарних технологій є велика та постійно зростає. Зокрема корпорація Google запропонувала освітянам безкоштовний пакет хмарних сервісів Google Apps for Education (зараз G Suite for Education), який відразу підключили близько 80 тисяч викладачів і студентів США, а згодом їх кількість зросла до 70 мільйонів користувачів у всьому світі.

До найбільш використовуваних хмарних технологій відносять:

Google Диск застосовують для збереження матеріалів онлайн. Це можуть бути документи, конспекти, презентації, підручники, розробки. На Google Диску можна розмістити навчальні матеріали, плани уроків, презентації.

YouTube застосовують для розміщення відеоматеріалів. Це і розважальні відео, і освітні відео та канали. Цей сервіс дозволяє створити власні колекції навчальних відеофільмів. Педагоги знімають і викладають на YouTube власні відеоуроки.

Blogger застосовується для створення і ведення персональних блогів. Блог використовується для публікації новин, які відображаються у хронологічному порядку за датою додавання. Окрім власних блогів на загальні теми, поширення набули спеціалізовані тематичні блоги, які містять наукові дослідження з певного напрямку з можливістю коментування.

Google Forms застосовують з метою отримання зворотного зв’язку. З його допомогою можна створювати онлайн-опитування, тести, інтернет-вікторини, веб-квести тощо. Аналогічний сервіс Microsoft Forms пропонується у складі пакету Office 365. Істотною перевагою цих сервісів є автоматична перевірка результатів, завдяки чому респонденти отримують інформацію про наслідки своєї діяльності одразу після проходження тестів.

Google Сайти застосовується для презентації власних проектів та створення своїх електронних посібників, сайтів класу, школи, дозволяє додавати текст, зображення і відео, а також об'єкти, що зберігаються на Google Диску: документи, презентації, форми, таблиці, діаграми. Для його обслуговування не потрібне знання програмування.

Microsoft Sway – це презентації онлайн. Використовується для презентації проектів або створення портфоліо [1].

Таким чином використання хмарних технологій та сервісів в освітньому процесі сприяє інтеграції знань та інформації з цифрових технологій, забезпечує доступ до навчання онлайн, доступ до світових масивів інформації, що, зрештою, веде до формування особистості з конкурентноздатними фаховими (професійними) знаннями, навичками та якостями.

Література:

1. Хмарні технології в освіті. URL: https://sites.google.com/view/cloudinedu/%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0?authuser=0 (дата звернення: 11.12.2020).

ЗМІСТ

Наукове видання

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

19 грудня 2020 року

Опубліковано в авторській редакції

Формат 60×84/8. Умовн. друк арк. 16,4.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.