ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС І НАВЧАЛЬНОМУ ПРОЦЕСІ

Збірник наукових статей за матеріалами
доповідей учасників
Всеукраїнської науково-практичної конференції
23 грудня 2016 р.

Львів
2017

УДК 004
ББК 32.973
П 78

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол № 5 від 21.12.2016 р.)

РЕДАКЦІЙНА КОЛЕГІЯ

П 78 Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська /. – Львів: ЛьвДУВС, 2017. – 313 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками Ввеукраїнської науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі», що проводилася 23 грудня 2016 р. у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

УДК 004
ББК 32.973

РОЗДІЛ 1.
НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПОЛІЦІЇ

Деякі аспекти підготовки кадрів з попередження кіберзлочинності в Україні

Баляс А.В.,
курсант Одеського державного університету внутрішніх справ
Ісмайлов К.Ю.,
завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук

Державні правоохоронні установи у різних країнах світу утворюють спеціалізовані підрозділи, кількість яких постійно зростає, для збирання та аналізу «електронних» чи «комп'ютерних» доказів. Цю функцію також виконують численні спеціальні лабораторії судової експертизи. Зазначені обставини є одним із обґрунтувань формування спеціальних підрозділів по боротьбі зі злочинами, що вчиняються з використанням комп'ютерних технологій. Досвід багатьох країн свідчить, що комп'ютерні злочини мають розслідуватись лише тими підрозділами чи співробітниками правоохоронних органів, які мають спеціальні навички для ведення таких справ та пройшли відповідну підготовку. Це пов'язано з тим, що робота з комп'ютерним обладнанням вимагає спеціальних знань. Серйозні проблеми, які призводять до значних витрат, можуть виникнути, якщо справу з цією технікою матиме некваліфікована особа. На даний час це є актуальним питанням.

Ми живемо в епоху глобальної інформатизації, коли комп'ютерні та телекомунікаційні технології використовуються майже в

усіх сферах життєдіяльності людини та суспільства, роблячи життя більш комфортним і динамічним. У світі, зокрема в Україні, прискореними темпами розвивається мережа Інтернет. За останні п’ять років кількість регулярних користувачів серед населення нашої держави збільшилася майже втричі й нині становить понад 20 млн осіб (у світі цей показник уже сягнув 5,5 млрд) [1].

Проблематика попередження злочинності та підготовки кадрів у сфері інформаційних технологій і кіберебезпеки досить часто обговорюється фахівцями у сфері новітніх технологій, інформаційної безпеки та державного управління в журналах, на конференціях, круглих столах і засобах масової інформації. Деякі аспекти попередження кіберзлочинності вивчали та обговорювали у своїх статтях такі вчені як К. Бєляков, С. Битко, В. Бутузов, А. Волеводз, В. Голубєв, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Е. Рижков, Т. Тропіна, В. Хахановський та інші.

Статистика свідчить, що наша країна є одним з лідерів за кількістю кібератак у всьому світі. Україна виявилася у цієї сфері на четвертому місці після Росії, Тайваню і Німеччини.

Стосовно системи органів Національної поліції основними проблемними питаннями формування відомчої кіберінфраструктури є:

- відсутність чіткої стратегії створення і розвитку спеціалізованих підрозділів по боротьбі з кіберзлочинністю;
- розрізненість зусиль практичних і навчальних підрозділів з питань підготовки відповідних кадрів;
- відсутність резерву кандидатів для комплектування відповідних підрозділів і посад по лінії роботи;
- відсутність належного представництва провідних фахівців практичних підрозділів на спеціалізованих науково-практичних заходах;
- досить популістський підхід у питаннях організації співпраці основних суб'єктів боротьби з кіберзлочинністю;
- відсутність єдиного центру підготовки і перепідготовки кадрів для боротьби з кіберзлочинністю [2].

На даний час законодавством України також передбачені різні законопроекти з удосконаленню законодавства відповідно до цих злочинів.

У Проекті Концепції стратегії і тактики боротьби з комп'ютерною злочинністю в Україні зазначалося, що підготовка фахівців, які спеціалізуються на розкритті злочинів, що вчиняються з використанням комп'ютерних технологій, має здійснюватися за такою моделлю:

- у відомчих навчальних закладах правоохоронних органів (МВС, СБУ, Державній податковій адміністрації тощо) готуються спеціальні навчальні дисципліни за тематикою «Виявлення, профілактика та розкриття злочинів, що вчиняються з використанням комп'ютерних технологій»;
- у Національній академії внутрішніх справ України, в Національній академії служби безпеки України, в Академії державної податкової служби України (на факультеті податкової поліції) формуються на рівні магістратури спеціалізовані групи щодо підготовки викладачів для відомчих закладів освіти за проблематикою боротьби з кіберзлочинністю;
- в системі підвищення професійної підготовки та перепідготовки оперативного складу, слідчих та експертів проводяться спеціальні збори для навчання щодо виявлення, профілактики та розкриття комп'ютерних злочинів.

Підготовку, перепідготовку та підвищення кваліфікації кадрів для боротьби із злочинністю в сфері комп'ютерних технолог, на наше переконання, можливо здійснювати у спеціалізованому вищому навчальному закладі за умови виконання низки організаційних заходів.

1. Підготовку фахівців для боротьби із злочинністю у сфері комп'ютерних технологій треба здійснювати та базі відповідної вищої технічної освіти наданням другої вищої освіти юридичної (у відомчих навчальних закладах МВС України) за умови укладання відповідного контракту з такими фахівцями.
2. У перспективі у вищих навчальних закладів може бути створений факультет інформаційних технологій, до складу якого входило б кілька кафедр, зокрема: кафедра інформаційної безпеки, кафедра розкриття та розслідування кіберзлочинів. Крім того, слід передбачити відповідну науково-дослідну лабораторію для проведення наукових досліджень у цій сфері [3].

За умов реформування системи вищої освіти в Україні організація такої підготовки є складним завданням, виконанню якого повинне сприяти створення системи цільової підготовки і перепідготовки фахівців у сфері протидії кіберзлочинності.

Безумовно, в Україні за останні роки накопичено певний досвід протидії кіберзлочинності як у практичному, науковому і навчально-методичному плані.

Тому напевно необхідно розділити державне управління у сфері забезпечення кібербезпеки в країні на наступні напрями: по-перше загальну підготовку працівників правоохоронних органів, яка б включали загальні відомості про кібератаки, методи, способи та тактики проведення невідкладних слідчих та оперативних заходів з попередження та під час розслідування різноманітних злочинів (не тільки кіберзлочинів); по-друге, спеціалізовану підготовку працівників Департаменту кіберполіції України, яка повинна включати в себе комплекс заходів як у середині країни, а саме профільну підготовку з спеціалізації, а також підготовку під час участі у міжнародних тренінгах та семінарах.

1. Про надання інформації щодо проблемних питань міжнародного співробітництва у сфері боротьби з кіберзлочинністю [Електронний ресурс] : довідка Управління боротьби з кіберзлочинністю МВС України від 15 січ. 2013 р. № 37/135. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/index
2. Европейская Конвенция по киберпреступлениям от 23 листопада 2001 р. [Електронний ресурс]. – Режим доступу : http://www.eos.ru.
3. Україна – один з лідерів з кількості кібератак у світі [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua.
4. Орлов О. В. Державне управління підготовкою фахівців у сфері кібербезпеки / О. В. Орлов // Державне будівництво [Електронний ресурс]. – Режим доступу : http://kbuapa.kharkov.ua.

Захист WEB-порталів спеціалізованих інформаціних систем Національної поліції України

Бойчук Т.Я.,
курсант Львівського державного університету внутрішніх справ
Сеник В.В.,
завідувач кафедри інформатики Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Інформаційні впливи на держави, суспільства, людей сьогодні бувають ефективнішими за політичні, економічні або військові. Впровадження сучасних інформаційних технологій (ІТ), систем телекомунікацій, кількісна зміна масштабів інформаційних взаємодій призвели до якісної зміни у підходах до розв'язання існуючих проблем і виникнення нових, яких не існувало на попередніх стадіях розвитку інформаційного суспільства. Важливим напрямком підвищення ефективності функціонування спеціалізованих інформаційних систем Національної поліції (НП) є інтегрування з глобальною мережею Internet [2, с. 131]. У багатьох випадках завдяки, власне ступеню інтегрування, вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми інформаційних систем (ІС). По-друге, користувачам Internet забезпечується доступ до відкритої інформації ІС. Досить часто при розв'язанні обох задач використовується Web-сайт (Web-портал), який, крім того, відіграє представницьку роль ІС у мережі Internet.

Практичний досвід показує, що функціонування Web-порталу значною мірою впливає на ефективність функціонування всієї ІС. Основою Web-порталу є Web-сервер, який забезпечує доступ користувачів із мережі Internet до Web-сторінок порталу. Однак, в практиці зустрічаються випадки, коли безпека інформації зазнає негативних впливів. Такими випадками порушення безпеки інформації є:

- блокування інформації (дії, наслідком яких є припинення доступу до інформації);

- несанкціонований доступ (доступ до інформації, що здійснюється з порушенням установлених в ІС правил розмежування доступу);
- витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації (дія, внаслідок якої інформація в ІС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному або обмеженому обсязі);
- модифікування інформації (навмисні дії, які призводять до спотворення інформації, яка має оброблятися або зберігатися в ІС);
- порушення роботи ІС (дії або обставини, які призводять до спотворення процесу оброблення інформації) [4].

Тому, керівництво підрозділів НП під час створення Web-порталу та визначення операторів, вузли яких будуть використовуватися для під'єднання до мережі Internet, керуються законами України, іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації (ТЗІ), а також передовим досвідом стосовно розроблення новітніх методів і процесів захисту інформації.

Web-портал може бути розміщеним на власному сервері або на сервері, який є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації встановлений рівень захисту. Функціонування Web-порталу забезпечується ІС, за допомогою якої здійснюється актуалізування розміщених на Web-порталі інформаційних активів та керування доступом до них.

Для забезпечення захисту інформації (ЗІ) Web-порталу у цій ІС створюється комплексна система захисту інформації (КСЗІ), яка є сукупністю організаційно-правових і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують ЗІ. КСЗІ підлягає державній експертизі у порядку, передбаченому Положенням про державну експертизу в сфері ТЗІ [3, с.146].

Захист інформації на всіх етапах створення та експлуатування Web-порталу здійснюється відповідно до розробленого плану ЗІ.

До складу ІС, яка забезпечує функціонування Web-порталу входять:

- ОС, фізичне середовище, у якому ОС функціонує, середовище користувачів,
- оброблювана інформація, у тому числі й технологія її оброблення. [5, с.120].

Під час забезпечення ЗІ повинні бути враховані всі характеристики відзначених складових частин, які впливають на реалізацію політики інформаційної безпеки Web-порталу. У випадку, якщо Web-портал містить посилання на інформаційні ресурси іншого Web-порталу, умови функціонування останнього не повинні порушувати встановлену для даного Web-порталу політику безпеки.

Захист Web-порталу спеціалізованої інформаційної системи Національної поліції може здійснюватись із використанням наступних підсистем:

- підсистема криптографічного захисту;
- підсистема контролю цілісності;
- підсистема антивірусного захисту;
- підсистема аналізу захищеності;
- підсистема виявлення втручань;
- підсистема управління засобами захисту Web-порталу [1, с.241].

Не викликає сумніву, що чільною ознакою професійної придатності працівників НП усіх рівнів є вимога досконалого володіння інформаційними технологіями, вміння нагромаджувати, обробляти та аналізувати зростаючі потоки інформації, використовуючи для цього новітні технологічні засоби ІТ, прогресуючий розвиток яких, у свою чергу, спонукатиме до постійного вдосконалення навиків роботи з ними.

Уже сьогодні фактичним показником базового рівня володіння інформаційними технологіями стало вміння працювати з пакетами спеціалізованого програмного забезпечення, які надають широку гаму інструментів для завершеного циклу використання інформаційних продуктів у практичні діяльності. Нормальне функціонування Web-порталу, долученого до мережі Internet, практично неможливе, якщо не надавати належну увагу

проблемі забезпечення його інформаційної безпеки. Найефективніше ця проблема може бути вирішена шляхом застосування комплексного підходу до захисту інформаційних активів порталу від можливих інформаційних нападів. Для цього до складу комплексу засобів захисту порталу повинні входити підсистеми антивірусного захисту, виявлення втручань, контролю цілісності, криптографічного захисту, розмежування доступу, а також підсистема управління. При цьому кожна з підсистем повинна бути оснащена елементами власної безпеки.

1. Андреєв В. І. Основи інформаційної безпеки: підручник для студентів ВНЗ які навчаються за напрямом «Інформаційна безпека» / В. І. Андреєв, В. О Хорошко, В. С. Чередниченко, М. Є. Шелест; за ред. В. О. Хорошко. – К.: ДУІКТ, 2009. – Вид. 2-ге, доп. і переробл. – 293 с.
2. Захаров В. П. Проблеми інформаційного забезпечення правоохоронних структур: навчальний посібник / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2007. – 372 с.
3. Кулешник Я. Ф. Основні завдання захисту інформації в операційних системах / Я. Ф. Кулешник, Т. В. Рудий, І. В. Бичинюк, Д. М. Неспляк // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матеріали науково-практичної конференції (Львів, 24 грудня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 145–148.
4. Правопорушення, пов’язані з використанням комп’ютерних систем і мереж. Захист інформації в автоматизованих системах. Попередження комп’ютерних злочинів, особливості методики їх розслідування. [Електронний ресурс]. – Режим доступу: http://www.naiau.kiev.ua/books/Kriminal_inform/t_4.htm
5. Рудий Т. В. До питання технічного захисту інформації у підрозділах МВС / Т. В. Рудий, О. В. Омеляненко, Я. Ф. Кулешник, С. А. Гаранджа // Проблеми діяльності кримінальної міліції в умовах розбудови правової держави: матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (м. Львів, 12 березня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 115–120.

Роль приватного детектива у забезпеченні економічної безпеки підприємства

Верхівський В.О.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ

Приватним детективом вважається особа, яка отримала відповідну ліцензію, пройшла атестацію та виконує певні послуги в приватній розшуковій сфері. Інакше детектив займається детективною діяльністю у взаємодії з іншими структурними підрозділами підприємства, що дозволяє залучати для вирішення завдань забезпечення безпеки провідних фахівців з професіоналами в різних галузях економіки, у тому числі фінансистів, економістів, технологів, маркетологів, програмістів, юристів тощо [63]. Особливо визначальна роль у діяльності із запобігання та протидії внутрішнім і зовнішнім загрозам діяльності підприємства багато в чому залежить від ефективної роботи штатного підрозділу економічної безпеки – служби безпеки організації та діяльності приватного детектива. Йому має відводитися визначальне місце у структурі служби безпеки організації (рис. 1).

Рис. 1. Місце приватного детектива в організаційні структурі служби економічної безпеки організації

Завдання що будуть покладені на приватного детектива мають визначатися з урахуванням завдань, що покладаються на службу безпеки суб'єкта господарювання в цілому.

Основні напрями діяльності приватного детектива в системі економічної безпеки підприємства подано на рис. 2.

Рис. 2. Напрями діяльності приватного детектива в системі економічної безпеки підприємства

Під час здійснення своїх обов'язків приватним детективам відповідно до міжнародних нормативно-правових актів забороняється:

- приховувати від правоохоронних органів відомі їм факти про злочини або інформацію про підготовку до вчинення злочинів;
- видавати себе за співробітників правоохоронних органів;
- збирати відомості, пов'язані з особистим життям, політичними і релігійними переконаннями окремих осіб;
- здійснювати відео- та аудіозапис, фото- і кінозйомки в службових чи інших приміщеннях без письмової згоди на те відповідних посадових або приватних осіб;
- вдаватися до дій, які посягають на права і свободи громадян;

- здійснювати дії, що ставлять під загрозу життя, здоров'я, честь, гідність і майно громадян;
- фальсифікувати матеріали і вводити в оману клієнта;
- розголошувати зібрану інформацію, використовувати її у будь-яких цілях всупереч інтересам свого клієнта або в інтересах третіх осіб;
- передавати свою ліцензію для використання її іншими особами.

Використання у безпековій діяльності підприємства послуг приватного детектива зможе суттєво покращити її ефективність.

Організаційно-технічні засоби контролю швидкісного режиму на автошляхах країни

Вишня В.Б.,
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, доктор технічних наук, професор
Вишня О.В.,
старший оперуповноважений Управління захисту економіки Головного управління Національної поліції у Дніпропетровській області

Інтенсифікація дорожнього руху призводить до збільшення кількості правопорушень і порохно транспортних пригод (ДТП) на автошляхах. Навіть поверхневий аналіз причин правопорушень підтверджує, що серед причин ДТП перше місце впевнено утримує перевищення швидкості руху (порушення швидкісного режиму). Важливу роль v боротьбі з цим правопорушенням відіграє використання мобільних постів поліції, що здійснюють контроль швидкості руху в різних точках (пунктах) певного району. Мобільні пости розташовуються, як правило, у місцях, де встановлені обмеження швидкості руху, або небезпечних з огляду створення ДТП. Лише за умови, що ділянка обмеження швидкості є невеликою, дії мобільних постів визнаються ефективними.

Однак лише на одній трасі Дніпропетровськ-Павлоград є три ділянки з обмеженням швидкості в 40 км/год довжиною

відповідно 4,5; 3,9 і 2,5 км. Як правило, співробітники поліції контролюють швидкість руху механічних транспортних засобів відразу ж за дорожнім знаком чи на першій половині ділянки обмеження швидкості. Водії транспортних засобів, попереджені сигналами зустрічних автомобілів, скидають швидкість руху і проїздять контрольовану ділянку без порушень Однак як тільки автомобіль проїздить мобільний (пересувний) пост, водій, почуваючи безкарнісь, різко збільшує швидкість, долаючи частину ділянки обмеження, що залишилася, зі значно більшою швидкістю. Цю практику беруть на озброєння більшість водіїв, особливо швидкісних автомобілів.

Яким же чином можливо боротися з таким проявом порушень швидкісного режиму? Тут важливо проаналізувати як організаційні заходи, так і технічні засоби, що сприяють вирішенню поставленого завдання.

Уже на сьогодні для боротьби з такими порушеннями на великих ділянках обмеження швидкості виставляються, наприклад, два пости з деяким взаємо віддаленням. Однак водійська «солідарність» знижує ефект роботи спарених постів. Крім того, концентрація декількох постів на локальній ділянці траси «оголює» інші ділянки дороги.

Тому інтерес становить контроль протяжних ділянок за допомогою однієї мобільної бригади, оснащеної сучасними засобами контролю і передачі інформації.

Відомо, що інформація, передана по радіо на стаціонарний пункт про порушення швидкості руху тим чи іншим транспортним засобом, не може використовуватися для адміністративною покарання в силу відсутності об’єктивних доказів правопорушень. Тому пропонується оснастити мобільні пости передавальним комплектом (ПК) технічної системи контролю швидкісного режиму (рис. 1), до якого входять радар, цифрова відеокамера і радіомодем.

У свою чергу, на достатньому віддаленні від місця контролю мобільної бригади, наприклад на стаціонарному пункті чи у іншій мобільній бригаді поза зоною обмеження швидкості руху, встановлюється приймальний комплект (ПРК) системи (рис. 2), що містить радіомодем, відеомагнітофон і монітор. Оснащена такою системою мобільна бригада може працювати як у режимі

звичайного локального контролю швидкості руху транспортного засобу, що наближається, так і системного контролю автомобілів, що віддаляються (сучасний радар «Бар'єр-2» однаково добре працює стосовно об'єктів, що наближаються і віддаляються). Схему контролю швидкісного режиму подано на рис. 3.

Принцип роботи апаратури передавального комплекту І технічної системи передбачає, що контроль швидкісного режиму для автомобілів, які проїхали мобільний пост, здійснюється автоматично. У разі реєстрації факту перевищення швидкості руху вмикається камера, що записує автомобіль (модель, номер) і швидкість його руху. Вмикання радіомодема на передавання списаної інформації може здійснюватися автоматично після нормованої тривалості чи вручну співробітником поліції за звуковим сигналом завершення контролю. На приймальному боці повідомлення записується на відеомагнітофон із вказівкою часу приймання повідомлення. Отримана інформація може бути підставою для застосування санкцій до правопорушників.

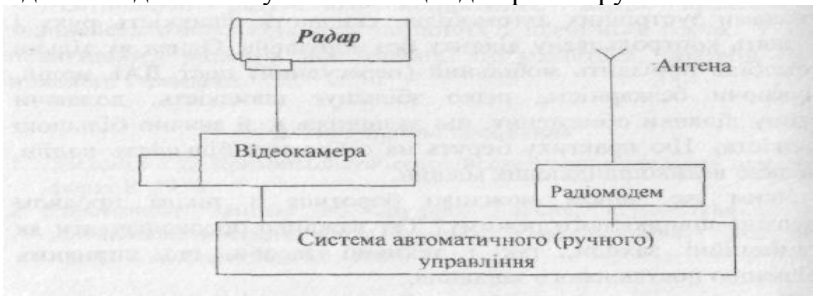


Рис. 1. Схема ПК системи контролю швидкісного режиму

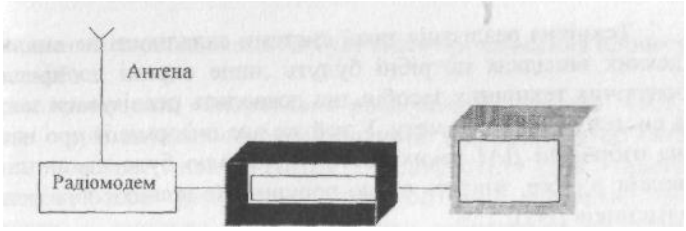


Рис. 2. Схема ПРК системи контролю швидкісного режиму

Технічна реалізація такої системи складності не викликає. У деяких випадках потрібні будуть лише окремі доопрацювання

існуючих технічних засобів, що дозволить реалізувати закладену в систему контролю мету. У той же час інформація про наявність на озброєнні підрозділів поліції таких систем контролю буде дисциплінувати водіїв, а отже, знизить число порушників швидкісного режиму й учасників ДТП.

Стаціонарний пункт

Мобільна бригада

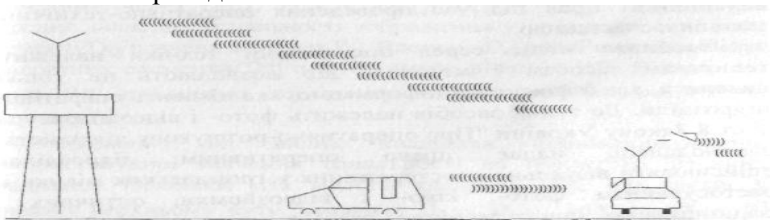


Рис. 3. Схема організації контролю швидкісного режиму автомобіля, що віддаляється.

Застосування автоматизованої системи документообігу в адміністративному судочинстві України

Гаврильців М.Т.,
доцент кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Медвідь Т.І.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ

На нинішньому цивілізаційного розвитку і переходу до інформаційного суспільства, ступінь розвитку інформаційних технологій стає безпосередньою умовою становлення активного і свідомого громадянина.

Сьогодні в Україні впроваджуються інформаційні технології в усіх сферах правотворчої, правозастосовної і правоохоронної діяльності. Розроблені потужні інформаційно-пошукові та операційні системи, які забезпечують оперативний доступ до інформації,

а відтак оптимізують діяльність державних та недержавних організацій, підприємств, бснків та інших структур, чия діяльність супроводжується значним обсягом створюваних, оброблюваних і збережених документів. Це, безумовно, сприяє зміцненню правової системи держави, захисту прав і основних свобод людини.

Формою залучення інформаційних технологій до роботи судової системи є розроблення та впровадження в судах автоматизованої системи документообігу, яка є основою електронного врядування і має значні переваги порівняно зі звичним, паперовим, документообігом. Зокрема, окрім підвищення культури діловодства, забезпечується економія коштів на тиражування та пересилання численних документів, що надзвичайно актуально за сучасних умов обмеженого фінансування.

Електронний документообіг, як високотехнологічний і прогресивний підхід, здатний суттєво підвищити ефективність роботи органів державної влади. Запровадження електронного документообігу в органах державної влади дозволяє підвищити ефективність функціонування всіх складових системи державного управління: прискорити рух документів, забезпечити своєчасність їх розгляду, скоротити терміни підготовки та прийняття управлінських рішень за допомогою автоматизації процесів колективного створення та використання документів, підвищити якість рішень завдяки наданню виконавцеві максимально повної бази документів, значно зменшити витрати на копіювання, передачу і збереження копій паперових документів, а отже й підвищити ефективність роботи як окремих державних службовців, так і конкретного органу державної влади [1].

Впровадження комп'ютерних систем діловодства в судах є надзвичайно важливим для підвищення ефективності їх роботи, а також прозорості, доступності для громадян та незаангажованості. Також застосування електронних систем зменшує паперовий документообіг і можливість помилки в судовому діловодстві [2, с. 59].

Ідея інформатизації всіх сфер суспільного життя, зокрема й судочинства, визначена в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [5], прийнятому з урахуванням Декларації ООН «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» [3].

Питання, що стосуються порядку функціонування автоматизованої системи документообігу в адміністративних судах, віднесені до компетенції зборів суддів згідно з вимогами Закону України «Про судоустрій і статус суддів» та «Положення про автоматизовану систему документообігу суду» [4].

Положення визначає порядок функціонування автоматизованої системи документообігу в судах загальної юрисдикції, яка забезпечує об'єктивний та неупереджений розподіл справ між суддями; надання фізичним та юридичним особам інформації про стан розгляду справ, в яких вони є учасниками процесу; централізоване зберігання текстів судових рішень та інших процесуальних документів; підготовку статистичних даних тощо [4].

Автоматизована система забезпечує автоматизацію технологічних процесів обробки інформації в суді: реєстрацію та розподіл вхідної кореспонденції, реєстрацію вихідної кореспонденції, а також внутрішніх документів суду; фіксування етапів проходження документів до їх передачі до електронного архіву, а також передачі судових справ з однієї судової інстанції до іншої.

Загальний рівень упровадження автоматизації документообігу та створення інформаційних документаційних систем, які автоматизують роботу судів, спрощують її, забезпечуючи сучасний рівень опрацювання інформації, у судовій системі України на сьогоднішній день визначається фахівцями як недостатній. Зокрема, функціонування автоматизованої системи документообігу, є незадовільний стан забезпечення комп'ютерною технікою, яка відповідає сучасним програмним вимогам. Відзначається, що переведення органів судової системи України до електронного документообігу ускладнюють такі фактори: брак кваліфікованих кадрів у галузі інформаційних технологій у державних установах, особливо в місцевих органах державної влади; недостатнє розуміння користувачами системи електронного документообігу в органах державної влади основних завдань, які має вирішувати електронний документообіг, та психологічна непідготовленість працівників до використання нових інформаційних технологій; низький рівень комп'ютерної грамотності суспільства, що ускладнює перехід до електронного документообігу у взаємодії між державними установами і громадянами [6].

Автоматизована система документообігу суду забезпечує: 1) об'єктивний та неупереджений розподіл справ між суддями; 2) надання фізичним і юридичним особам інформації про стан розгляду справ щодо них; 3) централізоване зберігання текстів судових рішень та інших процесуальних документів; 4) підготовку статистичних даних; 5) реєстрацію вхідної та вихідної кореспонденції й етапів її руху; 6) видачу копій судових рішень і виконавчих листів на підставі наявних у системі даних щодо судового рішення та реєстрації заяви особи, на користь якої воно ухвалене; 7) передачу справ до електронного архіву; 8) виконання інших функцій, необхідних для забезпечення нормальної діяльності судів і суддів [4].

З початку використання автоматизованої системи в судовій сфері спостерігається позитивна динаміка оперативності ефективного розгляду судових справ, а також отримання громадянами України поточної інформації стосовно стану розгляду своєї судової справи та копій потрібних процесуальних документів. Основними факторами вищезазначених позитивних результатів можна вважати те, що оперативна реєстрація вхідної і вихідної поштової та іншої кореспонденції (до якої належать позовні заяви, касаційні скарги, адміністративні справи й інші документи, які можуть подаватися до суду та бути предметом судового розгляду), нині вже відбувається в автоматизованому режимі. Таким чином, упровадження автоматизованої системи реєстрації кореспонденції дозволяє приблизно втричі зменшити час, необхідний для поточної реєстрації судових справ. Також під час застосування системи електронного документообігу значно зменшується обіг судових документів у паперовому форматі, що спрощує процес доступу громадян до потрібної інформації і робить суд відкритішим та доступнішим для населення. Крім того, автоматизована система документообігу має потужну систему контекстного пошуку, користуючись якою можна отримати потрібну інформацію за декілька хвилин. Отже, забезпечується процес оперативності, достовірності отримання громадянином у суді інформації щодо руху його судової справи.

Значною перевагою системи електронного суду є можливість складання статистичного звіту з використанням автоматизованої системи документообігу. Після впровадження в судову систему

електронних компонентів увесь процес підготовки окремого статистичного звіту набув нового змісту. Формування такого звіту здійснює лише один працівник [2, с. 68].

Технології, впроваджені в роботу адміністративного судочинства, мають відповідати сучасним вимогам. Окремі елементи електронного суду наявні в кожному суді. Це, наприклад, – система електронного діловодства, а також Єдиний реєстр судових рішень. Питання в тому, наскільки готові до електронного документообігу самі учасники процесу. Очевидно, що впровадження інформаційних технологій передбачає доступ до них обох сторін адміністративного судочинства.

Перспективи розвитку електронного документообігу в судових органах України слід спрямувати на вдосконалення технічних, прjграмних та інфjрмаційних засобів ведення судjвого документообігу України. З цією метою необхідно проводити систематичну роботу з підготовки та перепідготовки окремих спеціалістів, які ведуть діловодство в судовій сфері, а також здійснюють технічне забезпечення введення, передачі та зберігання електронних документів.

1. Джига Т. Вітчизняний та зарубіжний досвід запровадження в органах державної влади систем електронного документообігу: проблеми, переваги, рекомендації / Т. Джига // [Електронний ресурс]. – Режим доступу: http://old.niss.gov.ua.
2. Матвієнко О.В. Основи організації електронного документообігу: навч. посіб. / О.В. Матвієнко, М.Н. Цивін. – Київ: ЦУЛ, 2008. – 112с.
3. Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті: Декларація ООН від 12.12.2003 // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
4. Положення про автоматизовану систему документообігу суду: Затверджено рішенням Ради суддів України від 26.11.2010 № 30 // [Електронний ресурс]. – Режим доступу: http://court.gov.ua.
5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 // Відом. Верховної Ради України. – 2007. – № 12. – Ст.102.
6. Про реалізацію проекту щодо обміну електронними документами між судом та учасниками судового процесу: Наказ Державної судової адміністрації України від 31.05.2013 № 72 // [Електронний ресурс]. – Режим доступу: http://d

Покращення криптостійкості матричної Афінної системи шифрування даних

Грицюк Ю.І.,
професор кафедри програмного забезпечення інституту комп'ютерних наук та інформаційних технологій Національного університету «Львівська політехніка», доктор технічних наук, професор
Фірман Т.В.,
аспірант Національного лісотехнічного університету України
Лешкевич І.Ф.,
здобувач освітнього ступення «магістр» Національного університету «Львівська політехніка»

До класичних методів захисту інформації належить Афінна система підставлянь Цезаря і, як продовження, криптографічна система Лестера Хілла, в яких чітко виявлена спільність числових методів Афінних перетворень **[**2**]**. Однак, Афінна система **[**1**]**, будучи монограмним шифром простої заміни, є надзвичайно уразливою до атак, оскільки криптоаналітик шляхом частотного аналізу чи повного перебору може з'ясувати відповідність між двома будь-якими буквами початкового тексту і шифротексту. Водночас криптосистема Хілла, хоча і є поліграмним шифром, також вразлива до атак на основі відкритих текстів, позаяк у алгоритмі використовуються лінійні матричні операції. Для збільшення його криптостійкості в алгоритм шифрування потрібно додати будь-які нелінійні операції **[**3**]**.

Свого часу комбінування лінійних операцій шифру Хілла і нелінійних математичних перетворень привело до створення підстановно-перестановної мережі Фейстеля, в якій використовується ще й багатораундове виконання однотипних дій. Однак багато науковців свого часу пробували удосконалити Афінну криптосистему, особливо її матричний алгоритм, позаяк вона має ще багато прихованих можливостей. Тому розроблення надійної криптосистеми (де)шифрування інформації, яка б поєднувала матричні Афінні перетворення, а також багатораундові дії з різними ключами, є актуальним науковим завданням.

Алгебричний метод, який узагальнює Афінну систему підставлянь Цезаря, було сформульовано Лестером С. Хіллом для визначення *n*-грам **[**2**]**. Множина цілих чисел $\boldsymbol{Z}_m$, для якої визначені операції додавання, віднімання та множення за модулем *m*, є прикладом кільця *R*, тобто алгебричної системи пар елементів. У розглянутій нижче матричній Афінній криптосистемі використовуються такі матричні вирази для шифрування та дешифрування інформації:

$$\bar{\bar{K}} = \bar{\bar{A}} \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\oplus} \bar{B} \Rightarrow \bar{\bar{K}} = \left[\bar{K}_i = \left[k_{ij} = \sum_{l=1}^{n} a_{il} \underset{m}{\otimes} t_{lj} \underset{m}{\oplus} b_i,\ j = \overline{1,p} \right], i = \overline{1,n} \right]; \quad (1)$$

$$\bar{\bar{T}} = \bar{\bar{A}}' \underset{m}{\otimes} \bar{\bar{K}} \underset{m}{\oplus} \bar{B}' \Rightarrow \bar{\bar{T}} = \left[\bar{T}_i = \left[t_{ij} = \sum_{l=1}^{n} a'_{il} \underset{m}{\otimes} k_{lj} \underset{m}{\oplus} b'_i,\ j = \overline{1,p} \right], i = \overline{1,n} \right], \quad (2)$$

де: *m* – кількість символів алфавіту; $\bar{\bar{A}} = [\bar{A}_i = [a_{ij}, j = \overline{1,n}], i = \overline{1,n}]$ – матриця (ключ) шифрування, елементами якої є спеціально підібрані цілі числами з діапазону $1 \le a_{ij} < m$, а також НСД(a, m) = 1; $a = \det(\bar{\bar{A}}) \bmod m$ – визначник матриці $\bar{\bar{A}}$ за модулем *m*; $\bar{B} = [b_i, i = \overline{1,n}]$ – стовпець (ключ) коригування, елементами якого є цілі числами; $\bar{\bar{T}} = [t_{ij} = KodSym(s_{(i-1)\cdot p + j}), i = \overline{1,n}; j = \overline{1,p}]$ – матриця, елементами якої є числові коди символів вхідного повідомлення $\bar{S} = \{s_j, j = \overline{1, n \cdot p}\}$; $\bar{\bar{K}} = [\bar{K}_j = [k_{ij}, i = \overline{1,n}], j = \overline{1,p}]$ – матриця, елементами якої є коди символів зашифрованого повідомлення.

У виразах (1) і (2) символами $\underset{m}{\otimes}$ і $\underset{m}{\oplus}$ позначено відповідно множення та додавання елементів матриць за модулем *m*. Сучасне шифрування будь-якої вхідної інформації дає змогу використовувати розширену таблицю кодів ASCII, тобто значення елементів матриць $\bar{\bar{T}}$, $\bar{\bar{A}}$ і $\bar{B}$ можна встановлювати в межах [1;255], при цьому кількість символів алфавіту *m* становитиме 256.

Для отримання зворотної матриці дешифрування $\bar{\bar{A}}' = [\bar{A}'_i = [a'_{ij},\ j = \overline{1,n}],\ i = \overline{1,n}]$ та зворотного стовпця коригування $\bar{B}' = [b'_i, i = \overline{1,n}]$ потрібно виконати такі дії. Насамперед знаходимо обернену матрицю $\bar{\bar{A}}^{-1} = [\bar{A}_i^{-1} = [a_{ij}^{-1},\ j = \overline{1,n}],\ i = \overline{1,n}]$ до матриці $\bar{\bar{A}}$, елементами якої є дійсні числами. Розв'язавши лінійне рівняння

$a \cdot x + m \cdot y = 1$ за допомогою алгоритму Евкліда, знаходимо його корені x та y, внаслідок чого отримаємо $\det^{-1}(\bar{\bar{A}}) = x$. Тоді зворотне значення до визначника матриці $\bar{\bar{A}}$ становитиме $a' = \det^{-1}(\bar{\bar{A}}) \bmod m$. Звідси зворотну матрицю дешифрування знаходимо за таким виразом

$$\bar{\bar{A}}' = \bar{\bar{A}}^{-1} \underset{m}{\otimes} \det(\bar{\bar{A}}) \underset{m}{\otimes} a' \Rightarrow$$
$$\Rightarrow \bar{\bar{A}}' = [\bar{A}_i' = [a_{ij}' = (a_{ij}^{-1} \cdot \det(\bar{\bar{A}}) \cdot a') \bmod m,\ j = \overline{1,n}],\ i = \overline{1,n}] . \qquad (3)$$

Для перевірки правильності отримання значень зворотної матриці дешифрування використовуємо такий матричний вираз $\bar{\bar{A}} \underset{m}{\otimes} \bar{\bar{A}}' = \bar{\bar{E}}$, де $\bar{\bar{E}}$ – одинична матриця.

Щоб отримати зворотний стовпець коригування $\bar{B}'$, потрібно виконати такі матричні дії:

$$\bar{B}' = -\bar{\bar{A}}' \underset{m}{\otimes} \bar{B} \Rightarrow \bar{B}' = \left[b_i' = -\sum_{j=1}^{n} a_{ij}' \underset{m}{\otimes} b_j, i = \overline{1,n} \right]. \qquad (4)$$

У перетворенні (1), тобто при шифруванні вхідного повідомлення $\bar{\bar{T}}$, символи *n*-грами, яким відповідають числа *j*-го стовпця $\bar{T}_j$, замінюють на символи *n*-грами, що відповідають числовим значенням $(\bar{A}_i \times \bar{T}_j + b_i) \bmod m$, внаслідок чого отримуємо зашифроване повідомлення. При зворотному перетворенні (2), тобто дешифруванні повідомлення $\bar{\bar{K}}$, символи *n*-грами, яким відповідають числа *j*-го стовпця $\bar{K}_j$, замінюють на символи *n*-грами, що відповідають числовим значенням $(\bar{A}_i' \times \bar{K}_j + b_i') \bmod m$.

Якщо до матричного виразу (1), який дає змогу зашифрувати повідомлення $\bar{\bar{T}}$, застосувати *R*-раундову процедуру шифрування і кожного разу з новими ключами $\bar{\bar{A}}_r, \bar{B}_r$ ($r \in R$), то отримаємо багатораундову матричну Афінну криптосистему (де)шифрування інформації, аналогічну **[1]**. Водночас, процес дешифрування інформації за виразом (2) також повторюватиметься *R* разів. У цьому випадку узагальнені вирази для прямого та зворотного перетворення багатораундової матричної Афінної криптосистеми будуть мати такий вигляд:

$$\underline{\overline{\overline{K}} = \overline{\overline{A}}_R \underset{m}{\otimes} ... \left(\overline{\overline{A}}_2 \underset{m}{\otimes} \left(\overline{\overline{A}}_1 \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\oplus} \overline{B}_1 \right) \underset{m}{\oplus} \overline{B}_2 \right) ... \underset{m}{\oplus} \overline{B}_R}_{R \text{ раундів}}; \quad (5)$$

$$\underline{\overline{\overline{T}} = \overline{\overline{A}}'_1 \underset{m}{\otimes} ... \left(\overline{\overline{A}}'_{R-1} \underset{m}{\otimes} \left(\overline{\overline{A}}'_R \underset{m}{\otimes} \overline{\overline{K}} \underset{m}{\oplus} \overline{B}'_R \right) \underset{m}{\oplus} \overline{B}'_{R-1} \right) ... \underset{m}{\oplus} \overline{B}'_1}_{R \text{ раундів}}; \quad (6)$$

$$a_r = \det(\overline{\overline{A}}_r) \bmod m;\ a'_r = \det^{-1}(\overline{\overline{A}}_r) \bmod m;\ \det^{-1}(\overline{\overline{A}}_r) = x_r,\ r = \overline{1,R}; \quad (7)$$

$$\overline{\overline{A}}'_r = \overline{\overline{A}}_r^{-1} \underset{m}{\otimes} \det(\overline{\overline{A}}_r) \underset{m}{\oplus} a'_r;\ \overline{B}'_r = -\overline{\overline{A}}'_r \underset{m}{\otimes} \overline{B}_r,\ r = \overline{1,R}, \quad (8)$$

де: $\overline{\overline{A}}_r, \overline{\overline{A}}'_r, r \in R$ – матриці (ключі) (де)шифрування для *r*-го раунду; $a_r, a'_r, r \in R$ – визначники матриць $\overline{\overline{A}}_r$ та $\overline{\overline{A}}'_r$ за модулем *m* для *r*-го раунду дії алгоритму, при цьому НСД(a_r, *m*) = 1 та НСД(a'_r , *m*) = 1; $\overline{B}_r, \overline{B}'_r, r \in R$ – стовпці (ключі) коригування для *r*-го раунду дії алгоритму.

Поєднання матричних Афінних криптосистем з матричними перестановними алгоритмами **[**3**]** дає змогу створити багатораундову матричну Афінну перестановну криптосистему для перетворення інформації, які в загальному випадку можуть подаватися у вигляді процедур багатораундового (де)шифрування на основі таких матричних виразів:

$$\underline{\overline{\overline{K}}^{\text{п}}_{\text{рс}} = \overline{\overline{A}}_R \underset{m}{\otimes} ... \left(\overline{\overline{A}}_2 \underset{m}{\otimes} \left(\overline{\overline{A}}_1 \underset{m}{\otimes} \left(\overline{\overline{P}}^{\text{п}}_{\text{р}} \times \overline{\overline{T}} \times \overline{\overline{P}}^{\text{п}}_{\text{с}} \right) \underset{m}{\oplus} \overline{B}_1 \right) \underset{m}{\oplus} \overline{B}_2 \right) ... \underset{m}{\oplus} \overline{B}_R}_{R \text{ раундів}}; \quad (9)$$

$$\overline{\overline{T}}^{\text{п}}_{\text{ср}} = \overline{\overline{P}}'^{\text{п}}_{\text{р}} \times \left(\underbrace{\overline{\overline{A}}'_1 \underset{m}{\otimes} ... \left(\overline{\overline{A}}'_{R-1} \underset{m}{\otimes} \left(\overline{\overline{A}}'_R \underset{m}{\otimes} \overline{\overline{K}}^{\text{п}}_{\text{рс}} \underset{m}{\oplus} \overline{B}'_R \right) \underset{m}{\oplus} \overline{B}'_{R-1} \right) ... \underset{m}{\oplus} \overline{B}'_1}_{R \text{ раундів}} \times \overline{\overline{P}}'^{\text{п}}_{\text{с}} \right). \quad (10)$$

Можливі ще й такі матричні вирази для реалізації процедури багатораундового (де)шифрування інформації:

$$\overline{\overline{K}}^{\text{п}}_{\text{рс}} = \overline{\overline{P}}^{\text{п}}_{\text{р}} \times \underbrace{\overline{\overline{A}}_R \underset{m}{\otimes} ... \left(\overline{\overline{A}}_2 \underset{m}{\otimes} \left(\overline{\overline{A}}_1 \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\oplus} \overline{B}_1 \right) \underset{m}{\oplus} \overline{B}_2 \right) ... \underset{m}{\oplus} \overline{B}_R}_{R \text{ раундів}} \times \overline{\overline{P}}^{\text{п}}_{\text{с}}; \quad (11)$$

$$\underline{\overline{\overline{T}}^{\text{п}}_{\text{ср}} = \overline{\overline{A}}'_1 \underset{m}{\otimes} ... \left(\overline{\overline{A}}'_{R-1} \underset{m}{\otimes} \left(\overline{\overline{A}}'_R \underset{m}{\otimes} \left(\overline{\overline{P}}'^{\text{п}}_{\text{р}} \times \left(\overline{\overline{K}}^{\text{п}}_{\text{рс}} \times \overline{\overline{P}}'^{\text{п}}_{\text{с}} \right) \right) \underset{m}{\oplus} \overline{B}'_R \right) \underset{m}{\oplus} \overline{B}'_{R-1} \right) ... \underset{m}{\oplus} \overline{B}'_1}_{R \text{ раундів}}. \quad (12)$$

Криптоаналіз зашифрованої інформації за допомогою такої криптосистеми є надзвичайно важким **[**2**]**.

Насамперед, атака грубої сили при такому алгоритмі є надзвичайно складною, позаяк матриця-ключ шифрування має розмір $n \times n$, а вектор-стовпець коригування – розміром n. Оскільки кожен вхід може мати одне з 255 значень, то це означає, що кількість матриць шифрування становитиме $255^{n \times n}$, а векторів коригування – 255^n. Однак, не всі матриці-ключі мають мультиплікативну інверсію, аналогічно як і стовпці коригування адитивну інверсію. Тому область існування ключів (матриці шифрування і стовпця коригування) все ж таки дещо зменшується.

Запропонований вище криптографічний алгоритм не зберігає статистику звичайного тексту. Неможливо провести аналіз частоти окремих блоків з двох або трьох букв, позаяк відбувається перестановка як рядків, так і стовпців числових кодів символів вхідного повідомлення. Аналіз частоти появи слів розміром m (а в нашому випадку m=256) не може спрацювати, але такого не буває, щоби вхідний текст мав таку велику кількість символів.

Отже, розроблена багатораундова матрична Афінна перестановна криптосистема забезпечують достатню стійкість до брутальних атак навіть за значний проміжок часу.

Висновки. Афінні матричні шифри, зокрема шифр Хілла, у базовому вигляді володіють численними недоліками, такими як вразливість до атак на основі відкритих текстів та низька криптостійкість загалом. Проведення багатораундового шифрування дає змогу підвищити криптостійкість та зменшити шанс вдалого підбору ключів зловмисником. Додавання певних нелінійних операцій (перестановок рядків та стовпців) дає змогу зробити шифр менш вразливим до атаки на основі відкритого тексту. Математично описано алгоритм (де)шифрування інформації за допомогою матричного перестановного алгоритму, яка дещо підвищує криптостійкість класичного алгоритму шифрування. Отже, отриманий у результаті алгоритм, порівняно з базовою версією, є значно більш надійним та захищеним.

1. Грицюк П.Ю., Грицюк Ю.І. Афінні перетворення у криптографічній системі Лестера Хілла // 66-а науково-технічна студентська конференція НЛТУ України. – Серція: Інформаційні технології : результати 66-ої СНТК, м. Львів, 13 листопада 2014 р. – Львів : НЛТУ України. **[**Електронний ресурс**]**. – Доступний з

http://it.nltu.edu.ua/index.php/kafedra/news/286-rezultaty-66-oi-snk-sektsiia-informatsiini-tekhnolohii
2. Красиленко В.Г., Грабовляк С.К. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень // Системи обробки інформації: зб. наук. праць. – Харків : Вид-во ХУПС ім. Івана Кожедуба. – 2012. – Вип. 3(101), т. 2. – С. 53-61.
3. Юзьків Ю.Т., Грицюк Ю.І. Спільність числових методів афінних перетворень у класичних криптосистемах // Захист інформації і безпека інформаційних систем : матер. І-ої Міжнар. наук.-техн. конф., м. Львів, 31 травня – 01 червня 2012 р. – Львів : Вид-во НУ «Львівська політехніка». – 2012. – С. 134-135.

Функціональна модель захисту конфіденційної інформації в організації

Грицюк Ю.І.,
професор кафедри програмного забезпечення інституту комп'ютерних наук та інформаційних технологій Національного університету «Львівська політехніка», доктор технічних наук, професор
Сівець О.О.,
здобувач освітнього ступення «магістр» Національного університету «Львівська політехніка»

Відомо [4], що головна мета впровадження системи захисту інформації (СЗІ) в організацію – досягнення максимальної ефективності захисту конфіденційної інформації за рахунок одночасного використання всіх необхідних ресурсів. Також відомо [2, 3], що впровадження сучасної СЗІ немає призводити до відчутних труднощів у роботі інформаційної системи організації, а створення самої СЗІ має бути економічно виправданим. Проте впроваджена СЗІ має забезпечувати захист важливих інформаційних ресурсів організації від усіх реальних загроз.

Множина функцій СЗІ. Один з підходів до побудови сучасної СЗІ ґрунтується на понятті функції захисту інформації [1]. Суть його полягає в тому, що процес функціонування СЗІ моделюється шляхом визначення в ній таких властивостей, завдяки яким вона відповідно реагує на події, які пов'язані із

забезпеченням безпеки інформації в організації. Кожній з таких подій ставиться у відповідність певна властивість СЗІ, яку називають функцією забезпечення захисту інформації $\tilde{S}^{\text{а}} = \{s_i^{\text{а}}, i = \overline{1, m^{\text{а}}}\}$.

Отже, основне завдання теорії та практики побудови сучасної СЗІ можна розуміти як формування та обґрунтування повної множини функцій захисту інформації $\tilde{S}^{\text{ф}} = \{s_i^{\text{ф}}, i = \overline{1, m^{\text{ф}}}\}$, яка має містити такі функції, щоби при їх реалізації СЗІ могла протидіяти всім потенційно можливим порушенням безпеки інформації, а також при організації та забезпеченні захисту інформації. Відомо [1], що множина функцій захисту $\tilde{S}^{\text{ф}}$ є об'єднанням двох інших множин $\tilde{S}^{\text{ф}} = \tilde{S}^{\text{а}} \cup \tilde{S}^{\text{с}}$, де: $\tilde{S}^{\text{а}} = \{s_i^{\text{а}}, i = \overline{1, m^{\text{а}}}\}$ – множини функцій забезпечення захисту інформації, реалізація яких створює передумови, необхідні для надійного її захисту; $\tilde{S}^{\text{с}} = \{s_i^{\text{с}}, i = \overline{1, m^{\text{с}}}\}$ – множина функцій управління механізмами захисту інформації, призначених для ефективної реалізації множини $\tilde{S}^{\text{а}}$.

Порушення інформаційної безпеки – це фактично виникнення та реалізація *дестабілізаційний чинник* (ДЧ). Тоді основним завданням СЗІ буде контроль над всіма можливими проявами ДЧ. Для будь-якої СЗІ завжди можна визначити такі умови її функціонування, при яких можуть виявитися які-небудь ДЧ. Якщо їх не буде, то не буде потреби в захисті інформації. Якщо ж ДЧ все-таки проявлять свої потенційні можливості, то треба уміти оцінювати реальну можливість їх прояву, виявляти і фіксувати факти їх прояву, прийняти заходи щодо запобігання їх дії на інформацію. Саме ці властивості [3] мають мати множини функцій забезпечення захисту інформації $\tilde{S}^{\text{а}} = \{s_i^{\text{а}}, i = \overline{1, m^{\text{а}}}\}$.

Незалежно від перерахованих можливостей функцій забезпечення захисту інформації $\tilde{S}^{\text{а}}$, в реальній СЗІ може виникати тільки така множина станів СЗІ $\tilde{Q}^{\text{а}} = \{q_j^{\text{а}}, j = \overline{1, n^{\text{а}}}\}$, де: $q_1^{\text{а}}$ – СЗІ повністю виконує свої завдання, тобто навіть за умови прояву будь-яких ДЧ запобігає їх негативну дію на інформацію, що захищається, або повністю ліквідовуються наслідки такої дії; $q_2^{\text{а}}$ – СЗІ не повністю виконує свої завдання, тобто не вдається

повністю запобігти негативним діям ДЧ на інформацію, проте ця дія швидко локалізується; $q_3^{\text{а}}$ – СЗІ не виконує жодного зі своїх завдань, тобто СЗІ порушена повністю, внаслідок чого негативна дія ДЧ на інформацію не тільки не ліквідована, але навіть не локалізована. Очевидно, що організація СЗІ полягає в досягненні першого стану $q_1^{\text{а}} \in \tilde{Q}^{\text{а}}$ і/або хоча б частково – другого $q_2^{\text{а}} \in \tilde{Q}^{\text{а}}$.

Визначення витрат на захист інформації. Для найбільш ефективного використання інформації в той чи інший період її життєвого циклу (ЖЦ), протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до неї, при якому ефект від її використання досягав би максимальної величини. Встановлення певних обмежень на доступ до інформації протягом деякого періоду її ЖЦ є одним із способів досягнення максимального ефекту від впровадження СЗІ.

Для вирішення цих завдань необхідно вибрати такий режим доступу до інформації, який би протягом періоду її активного ЖЦ забезпечував максимальний ефект від використання. Для визначення потенційних збитків від витоку інформації, упущених вигод від обмеженого її використання та необхідних витрат на захист інформації застосовується суб'єктивне оцінювання інформації експертами, що добре розуміють її цінність.

На підставі порівняння експертних оцінок окремих чинників (збитку, витрат і вигод) з урахуванням різних можливостей їх прояву обчислюється значення інтегрального показника вибраного режиму доступу до інформації за формулою

$$W(t) = U(t) \cdot p_t - V(t) \cdot q_t - Z(t),\ t = \overline{1,T},$$

де: T – тривалість ЖЦ конфіденційної інформації; потенційно можлива величина збитку $U(t)$ та величина вигод $V(t)$ при вільному використанні інформації в t-ий період її ЖЦ; ймовірність прояву потенційного збитку (p_t) і прояву упущених вигод (p_t) в t-ий період ЖЦ інформації; $Z(t)$ – величина необхідних витрат на захист інформації в t-ий період її ЖЦ.

Для наочної демонстрації залежності параметрів і характеристик конфіденційної інформації, що визначають умови їх захисту, може слугувати функціональна модель, наведена на рисунку. В цій моделі показано якісний взаємозв'язок таких параметрів СЗІ: їх цінність, необхідний рівень захисту, тривалість забезпечення конфіденційності.

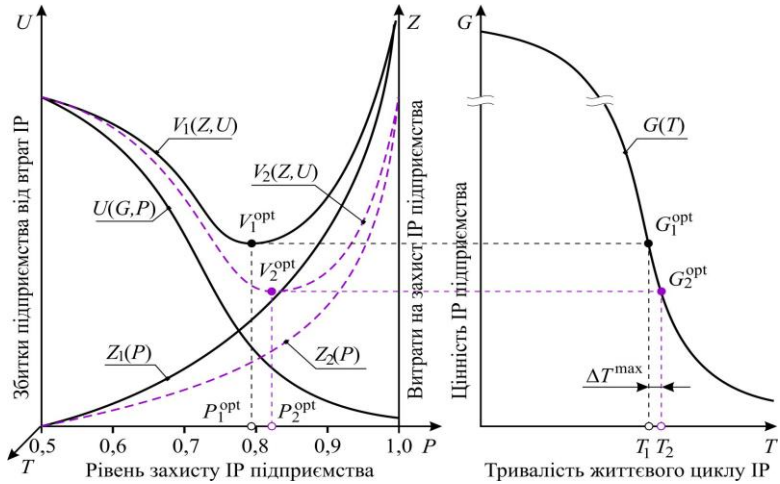


Рис. Функціональна модель оцінювання параметрів СЗІ

На рисунку введено такі позначення: G – цінність інформації – об'єкта конфіденційності (наприклад, науково-технічного звіту чи проектно-конструкторської документації); $G(T)$ – характеристика старіння інформації – зменшення цінності інформації з плином часу; P – рівень (ймовірність) забезпечення захисту інформації (практично $0{,}5 \le P < 1{,}0$, оскільки абсолютно надійний її захист неможливий); $Z_1(P)$ – допустимі витрати на захист інформації як функція від необхідного рівня її захисту. Ці витрати зростають при підвищенні вимог до рівня захисту інформації.

Прагнення досягти дуже високого рівня захисту інформації зазвичай призводить до різкого зростання витрат, які можуть перевищити цінність самої інформації, що захищається. Можливі втрати (збитки) власника інформації $U(G,P)$, понесені унаслідок неналежного рівня її захисту, є функцією від цінності самої інформації $G(T)$ та наявного рівня її захисту P. У нульовому наближенні ці втрати апроксимуються добутком цінності інформації $G(T)$ на ймовірність її витоку H, тобто $G(T)\cdot H$. Ймовірність витоку інформації знаходиться в зворотній залежності до досягнутого рівня її захисту, $H = (1 - P)$. При такому допущенні $U(G,P) = G(T)\cdot(1 - P)$.

З рисунку видно, що сума $Z_1(P) + U(G,P)$ визначає витрати $V(Z,U)$, пов'язані із забезпеченням конфіденційності інформації.

При цьому оптимальний рівень захисту інформації $V^{opt}(Z, U)$ відповідає мінімуму суми витрат на захист $Z_1(P)$ і можливих втрат $U(G,P)$ унаслідок неповноти захисту інформації. Прагнення перевищити його призведе до різкого зростання витрат $Z_1(P)$ на забезпечення захисту інформації; зниження ж рівня захисту призведе до збільшення можливих втрат $U(G,P)$ унаслідок недосконалості функціонування СЗІ.

Якщо прийняти, що $\Delta T = T_2 - T_1$ – часовий інтервал, впродовж якого конфіденційність інформації може бути економічно виправданою, то його максимальне значення становить $\Delta T^{max} = \Delta T(G(T), V^{opt}(Z, U))$. При цьому, як показано на рисунку, величина витрат на захист інформації $Z_1(P)$ в сумі з можливими збитками від її втрати $U(G,P)$ менша від вартості самої інформації $G(T)$ з урахуванням її знецінення. Для спрощення викладення матеріалу, нехтуємо залежністю $Z(P,T)$, тобто зростанням сумарних витрат на захист інформації з плином часу. Це можна легко побачити, подавши ліву частину рисунка в тривимірних координатах, а саме $PT0U$.

З викладеного вище матеріалу видно, що значення величини досягнутого рівня захисту інформації $Z(P)$ залежить як мінімум від двох параметрів: R_{pi} – використовуваних ресурсів (зокрема, матеріальних витрат на забезпечення захисту) і E_{pim} – ефективності механізму захисту інформації (використання цих ресурсів). Тому в рамках математичної моделі $Z(P) = f(R_{pi}, E_{pim})$ можлива така постановка оптимізаційної задачі.

Фактично E_{pim} – показник досконалості створеної та наявної СЗІ. При дещо якіснішому її проектуванні та практичній реалізації необхідної множини засобів і механізмів захисту, тобто максимально ефективному залученні всіх наявних ресурсів, один і той же рівень забезпечення захисту конфіденційної інформації можна досягнути при менших матеріальних витратах. На рисунку це переконливо демонструє крива $Z_2(P)$. При цьому відповідно оптимальний рівень захисту інформації P_2^{opt} може бути вищим порівняно з P_1^{opt}, а економічно виправдана тривалість ЖЦ інформації ΔT – більшою, тобто $T_2 = T_1 + \Delta T$.

Висновки. Наведено особливості побудови функціональної моделі захисту інформації в організації, описано множину

функцій захисту та множину можливих станів СЗІ. Виявлено, що для ефективного використання інформації в той чи інший період її життєвого циклу, протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до неї, при якому ефект від її використання досягав би максимальної величини.

1. Антонюк А.О. Теоретичні основи захисту інформації : конспект лекцій. – К. : Вид-во НТУУ «КПІ», 2003. – 233 с.
2. Грицюк Юрій, Сівець Ольга. Обґрунтування потреби захисту інформаційних ресурсів підприємства // Інформаційна безпека в сучасному суспільстві : матер. ІІ Міжнар. наук.-техн. конф., 24-25 листопада 2016, м. Львів, Україна. – Львів : Вид-во ЛДУ БЖД, 2016. – С. 41-43.
3. Грицюк П.Ю., Грицюк Ю.І. Побудова моделі функцій забезпечення захисту інформації // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації : матер. ІІ-ої Міжнар. наук.-практ. конф., 24-27 лютого 2016 року, с. Верхнє Студене, Україна. – К. : Вид-во Європейського ун-ту, 2016. – С. 55-58.
4. Егоров Ф.И., Тискина Е.О., Хорошко В.А. Задачи защиты информации // Захист інформації. – 2009. – № 1. – С. 5-12.

Деякі питання використання інформаційних можливостей мережі Internet під час протидії злочинам у сфері державних закупівель

Дараган В.В.,

доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук

Сфера державних закупівель в Україні є однією із найбільш уражених корупцією сфер економіки. Обов’язок протидіяти злочинам у цій сфері покладено на значну кількість правоохоронних органів, серед яких й підрозділи Національної поліції. В структурі Національної поліції обов’язок здійснення заходів щодо захисту бюджетних коштів від злочинних посягань, забезпечення правомірності застосування процедур закупівлі товарів,

робіт і послуг та цільового використання бюджетних коштів покладено на підрозділи Департаменту захисту економіки Національної поліції України (ДЗЕ НП).

Для якісного супроводження процесів державних закупівель, оперативному працівнику Департаменту захисту економіки Національної поліції, який відповідає за даний напрямок роботи, просто необхідно користуватися ресурсами глобальної мережі Internet.

Це зумовлено насамперед наступними чинниками:

- законодавство, яке регулює питання державних знаходиться в стадії становлення. У зв'язку з чим в ньому відбуваються постійні зміни та доповнення, які оперативно можна відстежити через мережу Internet.
- відкритий доступ до матеріалів журналістських розслідувань з приводу здійснення державних закупівель;
- оголошення про заплановані закупівлі та їх результати публікуються на електронному майданчику prozorro.gov.ua;
- вільний доступ до значної кількості інформації, необхідної для аналізу законності проведення певного тендеру;
- доступна вартість отримання такої інформації.

Глобальна мережа Internet є публічним ресурсом глобального масштабу та елементом сучасного інформаційного суспільства, яка включає в себе статистичну, адміністративну, правову, довідкову, енциклопедичну, аналітичну, комерційну, управлінську та соціологічну інформацію. Тому кількість інформації та ступінь її оновлення в мережі в загалом характеризують Internet як перспективне джерело інформації [6, с. 197].

У разі виникнення необхідності пошуку інформації щодо характеристики предмету закупівлі, його ціни, відомостей про учасників тендеру, замовників тощо, оперативному працівнику доцільно використовувати пошукові системи найбільш популярною у світі пошуковою системою є Google (69.24 %).

Розглянемо деякі ресурси мережі Internet та відомості, які в них можна отримати під час здійснення оперативного супроводження сфери державних закупівель:

3. *zakon.rada.gov.ua* – офіційний веб-сайт Верховної Ради України. *Інформація* – нормативно-правові акти з питань державних закупівель;

4. *prozorro.gov.ua* – електронна система публічних закупівель. Містить у вільному доступі інформацію про: заплановані закупівлі; тендери, які вже відбулися та які були відмінені; копії укладених договорів; тендерну документацію тощо. Під час пошуку зазначеної інформації оперативний працівник може здійснювати пошук за такими критеріями: ключове слово; CPV-код; за кодом Державного класифікатору продукції та послуг; за № закупівлі; за датою; за замовником; за регіоном; за статусом (подання пропозицій, аукціон, кваліфікація переможця, пропозиції розглянуті, торги відмінено, відмінена, завершена, перекваліфікація); за типом процедури. За кожною із процедур можна ознайомитися з коментарями учасників в яких може міститися оперативно значима інформація.
5. *usr.minjust.gov.ua* – єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань. Як правило через реєстр встановлюється інформація про директора, місце реєстрації, засновників тощо. Для пошуку інформації оперативному працівнику необхідно перейти на вкладку «Безкоштовний запит». Пошук здійснюється серед фізичних осіб-підприємців та юридичних осіб. Пошуку фізичної особи-підприємця здійснюється за індивідуальним податковим номером особи або за прізвищем та ініціалами особи. Пошук юридичної особи здійснюється за повним (або скороченим) найменуванням або кодом ЄДРПОУ.
6. *www.irc.gov.ua* – офіційний веб-сайт ДП «Інформаційно-ресурсний центр». Оперативний працівник має можливість ознайомитися з інформацією з Єдиного ліцензійного реєстру. Така інформація буде у нагоді коли до учасників тендеру висуваються певні кваліфікаційні вимоги або накуповується продукція (роботи або послуги), що є предметом ліцензійної діяльності. Пошук можна здійснювати через фізичних осіб-підприємців за індивідуальним податковим номером особи або за прізвищем та ініціалами особи та юридичних осіб – за повним (або скороченим) найменуванням або кодом ЄДРПОУ. Крім того, такий пошук можна здійснити за серією та номером ліцензії.
7. *www.reyestr.court.gov.ua* – Єдиний державний реєстр судових рішень. Використовуючи портал оперативний

працівник має можливість здійснити пошук судових рішень по ключових словах (наприклад: тендер, закупівля, будівництво тощо). Ознайомлення з такими рішеннями надасть можливість визначити способи вчинення злочинів у сфері закупівель, перелік документів, які можуть бути доказами по справі тощо. Пошук судових рішень здійснюється за: текстом судового рішення; регіоном суду; найменуванням суду; коду суду; ПІБ судді/головуючого; № справи; періодом надходження справи до суду; реєстраційним номером судового рішення; періодом ухвалення рішення; формою судочинства; формою судового рішення; статусу сторін судової справи.

8. *spending.gov.ua* – Єдиний веб-портал використання публічних коштів. Використовуючи портал оперативний працівник має можливість здійснити пошук розрахунків за державні кошти. Пошук транзакцій здійснюється за: розпорядником державних коштів (ЄДРПОУ); транзакцією; одержувачем (ЄДРПОУ). Можна зробити фільтрацію за регіоном або за періодом.

Звісно, даний список не може бути вичерпаний і може зростати залежно від поставленої перед оперативним співробітником мети.

Первинна інформація про предмети закупівлі їх кількість та ціну, а також відомості про учасників торгів є тією основою, за допомогою якої оперативний працівник ДЗЕ НП має можливість оцінювати оперативну обстановку, яка склалася в сфері закупівлі товарів, робіт і послуг за державні кошти.

Безперечно на основі такої інформації не можна робити певних висновків, щодо зловживань під час проведення закупівель, але в поєднанні даної інформації з інформацією отриманою оперативним шляхом, можна виділити ті процеси, які потребують найбільшої уваги з боку працівників ДЗЕ НП.

Таким чином, можна зробити висновок, що використання ресурсів глобальної мережі Internet в процесі протидії злочинам у сфері державних закупівель підвищує не тільки продуктивність праці й ефективність роботи оперативного працівника з виявлення, запобігання та розкриття злочинів, вчинених під час проведення закупівель, але й піднімають таку діяльність на якісно новий рівень.

Окремі аспекти удосконалення механізмів вирішення інформаційних спорів

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

Після революції гідності в Україні відзначається посилення залежності політичних процесів в від змісту інформаційних потоків, що відбувається на тлі постійного вдосконалення засобів масової інформації. Одночасно збільшилася кількість порушень інформаційних прав людини. У мережі Інтернет, що володіє широкими комунікаційними можливостями, розміщено безліч дифамаційних повідомлень, спостерігаються факти розголошення охоронюваних законом конфіденційних відомостей і інші форми порушення прав і свобод.

Ліквідація політичної цензури, що мало місце під час існування корумпованої влади, призвело до того, що серед засобів масової інформації та журналістів, у зв'язку з відсутність у суспільстві стійкої культури свободи вираження думок, виявилося чимало тих, хто не був готовий до відповідального використання конституційно закріплених прав і свобод. В результаті намітилася тенденція до різкого збільшення числа інформаційних спорів і пов'язаних з ними судових позовів до засобів масової інформації і звинувачень в адресу журналістів.

Сформована судова практика показала, що судовий розгляд питань, пов'язаних зі свободою слова, думки і масової інформації часом не дозволяє знайти справедливе рішення, оскільки встановлена законодавством відповідальність за інформаційні правопорушення далеко не завжди виявляється спів мірна вчиненого, як в частині провини, так і наслідків. Усвідомлюючи значущість незалежних засобів масової інформації, свободи думки та слова, які необхідні для країни в умовах асоціації України і Європейського Союзу, з метою вирішення найбільш складних інформаційних спорів, викликаних недотриманням редакціями засобів масової інформації, журналістами вимог законодавства, що пред'являються до висвітлення в засобах

масової інформації виникає необхідність розвитку механізму вирішення інформаційних спорів.

Незважаючи на те, що в Законі України «Про інформацію» створені юридичні передумови для того, щоб журналіст був захищений при виконанні своїх професійних обов'язків і сприймався як особа, що виконує громадський обов'язок, необхідно становлення такої практики розгляду інформаційних спорів, яка б ґрунтувалася на співвіднесенні порушеного приватного права і захищається журналістом публічного інтересу [1]. Це не відбувається відразу, а є тривалим процесом. Саме тому важливі такі механізми вирішення інформаційних спорів, які стимулюють формування свободи масової інформації та сприяють становленню журналістської спільноти як корпорації, що спирається на професійну етику та солідарність.

Існуючі сьогодні механізми судового вирішення інформаційних спорів потребують доповнення ефективними засобами позасудового врегулювання. Розвинена система позасудового розгляду інформаційних спорів повинна захищати інформаційні права громадян та сприяти формуванню єдиних професійно-етичних принципів функціонування засобів масової інформації.

Інформаційний спір представляє окрему категорію правових конфліктів, що виступає формою правомірної поведінки суб'єктів інформаційного права щодо захисту своїх суб'єктивних прав і законних інтересів, що випливають із адміністративних, цивільно-правових та інших правових відносин, пов'язаних з діяльністю засобів масової інформації і інформаційних відносин щодо пошуку, отримання, розповсюдження та виробництва масової інформації.

У даний час необхідно створення та реалізація юридичних механізмів використання позасудових засобів вирішення інформаційних спорів: наділення повноваженнями з регулювання даних правовідносин організацій, що застосовують позасудові механізми вирішення інформаційних спорів.

З урахуванням досвіду успішного функціонування подібних організацій і використання такого правового механізму в державах-членах Європейського Союзу зазначені організації повинні здійснювати повноваження щодо розгляду інформаційних спорів та володіти легітимною можливістю залучати тих чи інших суб'єктів зазначених спорів до юридичної відповідальності.

Оперативне і ефективне позасудове вирішення інформаційних спорів вимагає більш активного використання механізмів саморегулювання у межах галузі. У цих цілях є необхідність формування саморегулюючої організації засобів масової інформації, яка була б визнана з боку державних органів, суддівської та журналістської спільноти.

Існуючі законодавчі акти можуть бути застосовані для регулювання позасудових механізмів вирішення спорів в інформаційно-правовій сфері, але тим не менше вони не повністю відповідають необхідним для успішного функціонування такого інституту вимогам. Проект Закон України від 29.12.2015 за № 3665-1 (включено до порядку денного Верховної Ради України 1 листопада 2016 року) «Про медіацію «не передбачає механізмів захисту суспільного інтересу, який необхідно враховувати в інформаційно-правових конфліктах [2].

Закон України від 11 травня 2004 № 1701-IV «Про третейські суди» передбачає обов'язкове для підписання обома сторонами третейську угоду, в якій сторони погоджуються передати спір на вирішення третейського суду, тобто даний механізм вирішення спорів можливий у разі готовності обох сторін до участі, що позбавляє організацію позасудовою регулювання інформаційно-правових спорів можливості розгляду тих спорів, в яких одна з сторін не готова вдаватися до використання позасудових механізмів вирішення інформаційних спорів.

Діяльність з позасудового вирішення інформаційних спорів у сучасних нормативно-правових умов може бути заснована тільки на принципі добровільності. Ніякі примусові заходи не можуть застосовуватися для залучення сторін у позасудове вирішення інформаційних спорів.

Доцільно закріпити за суб'єктами інформаційних правовідносин права діяти на захист суспільних інтересів (взаємообумовлений інтерес суспільства і держави, сутнісні соціально-моральні установки і політико-правові правила розумної та справедливої організації суспільства, визнані державою і врегульовані правом). Інформаційно-правовий зміст діяльності суб'єктів позасудового вирішення інформаційних спорів зумовлює їх роль в якості представників невизначеного кола осіб при відстоюванні суспільних інтересів.

У цілях формування та удосконалення порядку регламентації використання позасудових механізмів вирішення інформаційних спорів пропонується внесення ряду змін до чинного законодавства. Доцільно доповнити положення Законів України від 2 жовтня 1992 року «Про інформацію», від 16 листопада 1992 року «Про друковані засоби масової інформації (пресу) в Україні», від 21 грудня 1993 року «Про телебачення і радіомовлення» нормами, які встановлюють порядок і випадки реалізації позасудових механізмів розв'язання спорів, що випливають з відносин, які формуються в процесі розповсюдження масової інформації. Зазначені положення повинні закріплювати правовий статус органів та організацій, до компетенції яких може бути віднесено вирішення інформаційних спорів.

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради. – 1992. – № 48. – Ст.650.
2. Про медіацію: проект Закону України 3665-1 від 29.12.2015. Офіційний портал Верховної Ради України. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57620

Щодо інформаційного забезпечення оперативно-розшукового супроводження доказування під час розслідування викрадань в АПК України

Єфімов В.В.,
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ,
кандидат юридичних наук, доцент

Важливе значення в забезпеченні економічної безпеки АПК відводиться органам Національної поліції. Проте реорганізація Міністерства внутрішніх справ, що проводиться упродовж останніх років, привела до ряду проблем, не кращим чином тих, що відбилися на забезпеченні однієї з функцій органів Національної поліції – захисту економіки, а саме протидії економічної злочинності.

Аналіз ситуації, що складається у сфері АПК, показує, що криміногенні чинники значною мірою визначають не лише його сьогоднішній стан, але і перспективи розвитку. Підтвердженням процесу активної криміналізації є кількість злочинів економічної спрямованості, що вчинюються в АПК, а також суми заподіяного матеріального збитку.

До недоліків інформаційної роботи, що негативно впливають на організацію оперативного обслуговування підприємств агропромислового комплексу (АПК) необхідно віднести: – недосконаліть структури справ, що стосуються оперативного обслуговування, занедбаності їхнього ведення оперативними підрозділами Національної поліції (НП); – відсутність яких-небудь документів на всіх рівнях, що встановлюють віднесення конкретних підприємств, установ і організацій до того чи іншого режиму оперативного обслуговування; – відсутність у функціональних обов'язках співробітників підрозділів захисту економіки (далі – ПЗЕ) організаційно-методичних вказівок на необхідність визначення рівня оперативного обслуговування об'єктів і галузей економіки.

Для забезпечення належного оперативного обслуговування підприємств АПК оперативний співробітник повинен глибоко вивчити криміногенну ситуацію, що склалася на конкретному об'єкті.

Для успішного інформаційного забезпечення оперативно-розшукового супроводження доказування під час розслідування викрадань в АПК України, оперативним працівникам необхідно поставити перед собою наступні завдання:

- сформувати уявлення про модель злочинної діяльності по привласненню або розтраті на підприємствах АПК;
- вивчати матеріали слідчої і судової практики з метою формування уявлення про помилки які були допущені оперативними працівниками на стадіях заведення і провадження за оперативно-розшуковими справами, і на стадії досудового розслідування;
- володіти алгоритмом дій з виявлення викрадань на підприємствах АПК на основі типових версій по цій категорії злочинів;
- досліджувати базу даних за допомогою статистичних методів аналізу з метою виявлення кореляційних взаємозв'язків між ознаками механізму злочинної діяльності

викрадачів на підприємствах АПК, і інтерпретувати отримані результати;

- знати перелік обставин, що підлягають встановленню і подальшому доказуванню обставин для відкриття кримінального провадження і рекомендації по виконанню перевірочних дій;
- мати в розпорядженні знання, пов'язані з виконанням окремих слідчих (розшукових), а також використанням різних форм спеціальних знань при розслідуванні викрадань на підприємствах АПК України.

Виявлення викрадань на підприємствах АПК пов'язане із здійсненням цілеспрямованої діяльності правоохоронних органів з пошуку ознак злочинної діяльності у відповідній сфері виробництва.

Викрадання на сільськогосподарських підприємствах, в переважній більшості, виявляються в результаті:

- здійснення цілеспрямованих оперативно-розшукових заходів по виявленню відповідних злочинів оперативними підрозділами;
- здійснення перевірочних заходів за заявами керівників або інших осіб підприємств АПК про вчинений злочин;
- здійснення перевірочних заходів за фактами наявності надлишок або недостачі товарно-матеріальних цінностей і грошових коштів у окремих матеріально-відповідальних осіб, що встановлено у рамках ревізійної діяльності на підприємстві;
- перевірки фактів затримання співробітниками патрульної поліції транспортних засобів, що перевозять майно без супровідних документів.

Вочевидь, що основна тяжкість роботи з виявлення замаскованих викрадань в АПК покладається, передусім, на оперативні підрозділи ЗЕ НП.

Спільне планування слідчим і оперативним співробітником розслідування по привласненню або розтраті на підприємствах АПК повинно бути підпорядковано ряду загальних і спеціальних вимог. До загальних вимог належить обов'язковість і конкретність планування, а також облік прямої залежності між складним

характером механізму злочинної діяльності викрадачів і складністю змістовної сторони планування розслідування привласнення або розтрати. В першу чергу розгорнутий і багаторівневий план потрібний у справах про групові викрадання і викрадання, що вчинені у великих розмірах.

Ще однією особливістю інформаційного забезпечення є специфіка формування фактичної бази версій. Висуненню версій у справах про викрадання найчастіше попередує не процесуальна діяльність слідчого, що проводиться у рамках первинних дій, а оперативно-розшукова робота підрозділів ЗЕ НП, або офіційні перевірки контролюючих або наглядових органів. Саме ці дані (оперативні і перевірочні) складають фактичну базу версій.

Специфічна риса процесу побудови версій в розслідуванні викрадань полягає в тому, що побудова версій відбувається до відкриття кримінального провадження. При цьому, якщо фактична база версій формується за допомогою оперативних даних підрозділів ЗЕ НП, то період часу, що відділяє етап висунення версій від етапу початку розслідування, як правило, значніший, ніж при офіційних перевірках матеріалів.

Деякі типові версії, що висуваються на самому початку розслідування викрадання, зберігають своє значення і на подальших етапах. Виявляючи ті або інші ознаки злочинів, слідчий підходить до їх оцінки з позицій основних типових версій.

Випадки, що зустрічаються серед типових ситуацій у справах про викрадання, особливо багатоепізодні, значно складніші, ніж при розслідуванні інших злочинів. Це обумовлює важливішу роль і у більшості універсальний, «наскрізний» характер типових версій, що дозволяє правоохоронним органам виконувати пошукові функції на всіх етапах оперативної і слідчої роботи.

Як підсумок, необхідно зазначити, що однією з умов ефективної діяльності щодо інформаційного забезпечення оперативно-розшукового супроводження доказування під час розслідування викрадань в АПК України є визначення і глибоке вивчення об'єктів злочинного посягання. Стосовно планування пошукових заходів існує проблема, пов'язана з недостатньою кількістю емпіричних досліджень, які дають матеріал для узагальнення характеристик особи злочинця. Це необхідно для визначення переліку осіб, які повинні перебувати на профілактичному обліку.

При встановленні такого переліку потрібно мати на увазі: вік (вікові групи) осіб, які вчиняли корисливі злочини; їх минулу та сьогоденну поведінку (наявність судимості, вид занять, зайнятість і характер зайнятості у вільний від роботи час); відносини в родині й у колективі тощо.

Відкритість інформації – одна з умов розвитку громадянського суспільства в Україні

Ковалів М.В.,
завідувач кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор
Собакарь А.О.,
завідувач кафедри тактико-спеціальної підготовки Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор

Угода про асоціацію України і Європейського Союзу передбачає гарантування реалізації вільного потоку інформації та ідей. Це є визнання принципу, що державні органи володіють інформацією в інтересах суспільства та від його імені. У зв'язку з цим при обмеженні доступу до інформації суспільні інтереси повинні головним критерієм для органів державної влади та місцевого самоврядування, їх посадових осіб, що володіють цією інформацією на законних підставах.

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

Принцип інформаційної відкритості закріплений у Законах України «Про Кабінет Міністрів України», «Про центральні органи виконавчої влади», «Про місцеве самоврядування в Україні», «Про доступ до публічної інформації» і інших нормативних актах [1-4].

Цей принцип виражається в доступності для громадян інформації, що становить суспільний інтерес або зачіпає особисті інтереси громадян; систематичному інформуванні громадян про передбачувані або прийняті рішеннях; здійсненні громадянами контролю за діяльністю державних органів, організацій і підприємств, громадських об'єднань, посадових осіб та прийнятими ними рішеннями, пов'язаними з дотриманням, охороною і захистом прав і законних інтересів громадян.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Важливим елементом громадянського суспільства є забезпечення державою можливості для громадян ознайомиться з тією інформацією, яка була підставою для прийняття органами влади того чи іншого рішення. В умовах формування суспільства, в якому інформація стає головною цінністю, неминуче повинна відбуватися переоцінка як прав, так і обов'язків органів влади та громадян в інформаційній сфері.

1. Про Кабінет Міністрів України: Закон України від 27.02.2014 № 794-VII // Відомості Верховної Ради. – 2014. – № 13. – Ст.222.
2. Про центральні органи виконавчої влади: Закон України від 17.03.2001 // Відомості Верховної Ради. – 2011. – № 38. – Ст.385.
3. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 № 280/97-ВР // Відомості Верховної Ради. – 1997. – № 24. – Ст.170.
4. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI // Відомості Верховної Ради. – 2011. – № 32. – Ст.314.

Роль інформаційних технологій в органах Національної поліції

Комісарчук Ю.А.,
доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Олійник Х.А.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ

У наші дні неможливо собі уявити ефективну роботу органів поліції з попередження, розкриття та розслідування злочинів без використання сучасних інформаційних технологій. Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських контор, юридичних офісів, і, звичайно ж, в оперативно-розшуковій, слідчій та експертній роботі органів поліції. Для цього застосовують не лише універсальне, але й спеціальне програмне забезпечення.

Темпи, з якими нові інформаційні технології зараз створюються та впроваджуються в практичну діяльність правоохоронних органів, настільки високі, що іноді навіть фахівці у галузі ІКТ, а тим більше, інші категорії користувачів не встигають оцінити масштаби й глибину всього, що відбувається. Проте кінцеві результати загальної роботи залежать від здатності кожного співробітника вирішувати завдання професійної інформаційної діяльності.

Проблемам використання інформаційних технологій в роботі органів поліції, а також підвищення рівня володіння цими технологіями випускниками ВНЗ системи МВС присвячені роботи зарубіжних і вітчизняних дослідників Х. А. Андріашина, С. Я. Казанцева, Г. В. Єпура, М. І. Ануфрієва, О. М. Бандурки, О. Н. Ярмиша, Ф. П. Васильєва, І. В. Горошка, М. П. Дубініна, О. М. Різника, Н.С. Павлюченка, В.Р. Женіла, В.А. Мінаева, А.Л. Полєжаєва, С. Бігуна та ін. Проте, як показує аналіз наукових робіт з даної проблематики, тему формування інформаційної компетентності та підвищення рівня володіння інформаційними технологіями випускниками вищих навчальних закладів системи МВС не можна назвати вичерпною. Недостатньо розробленою залишається методологія та методика підвищення інформаційної компетентності курсантів ВНЗ системи МВС за допомогою використання у навчальному процесі інформаційних технологій, які застосовуються в практичній роботі працівників поліції. Зокрема, недостатньо висвітленою є проблема опанування курсантами сучасного програмно-технічного забезпечення професійної діяльності працівників поліції.

Органи поліції у своїй роботі використовують інформацію, пов'язану не лише з відомостями про стан публічного порядку і рівня злочинності на певній території, але також і про самі органи та підрозділи, їх сили і засоби. Співробітники чергових частин, слідчі, працівники оперативних підрозділів карного розшуку, експерти-криміналісти, дільничні інспектора поліції, працівники паспортно-візових служб та інших підрозділів органів поліції у процесі своєї роботи накопичують величезні бази даних оперативно- довідкового і оперативно-розшукового призначення. У цих базах зазвичай міститься інформація, яка стосується обліково-реєстраційних даних громадян; правопорушень і кримінальних подій; правопорушників і злочинців; викрадених і вилучених речей, а також предметів антикваріату; власників автомототранспортних засобів; власників вогнепальної зброї; громадян, що знаходяться в розшуку та безвісті зниклих громадян, а також інша інформація, що підлягає зберіганню. Уся ця інформація необхідна для ефективної роботи різних підрозділів правоохоронних органів та своєчасного прийняття практичних заходів у боротьбі зі злочинністю та правопорушеннями [1].

Такі обсяги інформації вимагають не лише накопичення, але й аналітичного опрацювання, що полягає у спеціальному відборі, узагальненні й систематизації, інакше пошук необхідної інформації стане достатньо складним, а деколи навіть і неможливим. Проте це важко зробити без автоматизації всіх інформаційних процесів і використання автоматизованих інформаційних систем (АІС) та мереж. Тому збір, узагальнення, систематизація, обробка, передача, зберігання і видача по запитах усієї необхідної інформації сьогодні здійснюється з використанням сучасних інформаційних технологій. Визначимося з поняттями інформаційні технології і автоматизовані інформаційні системи.

Інформаційні технології – це система операцій з накопичення, зберігання, обробки та передачі інформації, які здійснюються за допомогою спеціальних каналах зв'язку з використанням комп'ютерної техніки [2].

Автоматизованими інформаційними системами (АІС) або банками даних називають сукупність структурованих певним чином баз даних, а також апаратно-програмних засобів, що дозволяють зберігати ці дані та маніпулювати ними [3].

Автоматизовані інформаційні системи, які правоохоронні органи використовують в своїй діяльності, за своїм призначенням діляться на:

- АІС, призначені для збору та обробки обліково-реєстраційної і статистичної інформації:
- АІС оперативного призначення;
- АІС, які використовують в слідчій роботі;
- АІС криміналістичного призначення;
- АІС, які використовуються в експертній діяльності;
- АІС управлінського призначення та інше.

З іншого боку ці автоматизовані інформаційні системи можна класифікувати за рівнем складності обробки інформації (технічної, обчислювальної, аналітичної, логічної), яка використовується, таким чином:

- Автоматизовані інформаційно-довідкові системи (АІДС).
- Автоматизовані інформаційно-пошукові системи (АІПС).
- Автоматизовані системи обробки даних (АСОД).
- Автоматизовані робочі місця (АРМ).
- Автоматизовані системи управління (АСУ).

Експертні системи (ЕС), експертно-консультуючі системи та системи підтримки ухвалення рішень.

АІДС (автоматизовані інформаційно-довідкові системи) дозволяють забезпечити користувача інформацією довідкового характеру. Працюючи в інтерактивному режимі, АІДС дозволяють вводити, систематизувати, зберігати та видавати відомості за запитом користувачів, при цьому, не роблячи ніяких складних перетворень даних.

АІПС (автоматизовані інформаційно-пошукові системи) дають можливість відбирати і виводити інформацію за умовами, які задаються в запитах.

АСОД (автоматизовані системи обробки даних) – це системи, які дозволяють вирішувати завдання, що мають чітку структуру за наявності вхідних даних, алгоритмів та стандартних процедур обробки. Такі системи використовуються для автоматизації повсякденних дій управлінського персоналу, які часто повторюються.

АРМ (автоматизовані робочі місця) – це основне середовище інформаційно-технічної автоматизації професійної діяльності співробітника ОВС. Вони є індивідуальним комплексом технічних засобів та програмного забезпечення, який дозволяє максимально автоматизувати роботу фахівців конкретного підрозділу. АРМ в основному складається з персонального комп'ютера, принтера, сканера, ксерокса, графічного пристрою та інших технічних засобів, а також пакетів прикладних програм загального призначення (текстових процесорів, електронних таблиць, графічних програм) і спеціального програмного забезпечення. Існує три типи АРМ: індивідуального користування, групового користування та користування в мережі. Співробітникові, що працює на АРМ, не потрібні доскональні знання в області інформатики (ОС, прикладне програмне забезпечення), його головним завданням є уміння розбиратися у своїй предметній області.

АСУ (автоматизовані системи управління) є комплексами технічних та програмних засобів, за допомогою яких можна автоматизувати управління різними об’єктами. Забезпечення керівництва інформацією є основною функцією АСУ. Зазвичай АСУ є сукупністю різних автоматизованих робочих місць, які пов'язані між собою.

ЕС (експертні системи) – це спеціальні програми, які в процесі рішення проблемних ситуацій здатні частково замінювати фахівця- експерта. Вони ґрунтуються на алгоритмах штучного інтелекту і використовують інформацію, отриману від фахівців в конкретній галузі. Такі системи, спираючись на спеціалізовану базу даних і використовуючи певний набір правил та механізмів виведення інформації на основі наявних фактів, дозволяють розпізнавати ситуації, ставити діагнози, пропонувати вирішення проблем і давати рекомендації по вибору дій [4].

1. Информатика и математика для юристов : учеб. пособие для вузов / под ред. проф. Х. А. Андриашина и проф. С. Я. Казанцева. – М. : ЮНИТИ, Закон и право, 2011. – 463 с. 2. Основы автоматизации управления в органах внутренних дел : учебник / под ред. В. А. Минаева, А. П
2. Информационные технологии управления в органах внутренних дел : учебник / Ф. П. Васильєв, И. В. Горошко, М. П. Дубінін, В. Р. Женіло и др.
3. Теорія управління органами внутрішніх справ : підручник / за ред. канд. юрид. наук Ю. Ф. Кравченка. – К. : Національна академія внутрішніх справ України, 2009. – 702 с.
4. Снегірьова Т. Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС.

Роль інформаційно-пошукових систем в підрозділах Національної поліції України

Коміссарчук Ю.А.,
доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Matioc I.B.,
курсант Львівського державного університету
внутрішніх справ

Сучасний рівень розвитку суспільства характеризується стрімким зростанням потоків і обсягів інформації, ускладненням

механізмів управління соціальними процесами та явищами. Сьогоднішню діяльність підрозділів Національної поліції України важко уявити без використання інформаційних технологій та інформаційного забезпечення, накопичення та систематизації інформації в базах даних.

Закон України «Про інформацію» містить визначення інформації, згідно з яким інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. В цьому ж законі визначені основні види інформації – це: 1) інформація про фізичну особу; 2) інформація довідково-енциклопедичного характеру; 3) інформація про стан довкілля (екологічна інформація); 4) інформація про товар (роботу, послугу); 5) науково-технічна інформація; 6) податкова інформація; 7) правова інформація; 8) статистична інформація; 9) соціологічна інформація; 10) інші види інформації [1].

Інформація, яка здобувається і використовується співробітниками підрозділів Національної поліції України, повинна бути упорядкованою, бо інакше потрібні відомості знайти важко чи просто неможливо. Саме тому в діяльність підрозділів Національної поліції України (далі– НП України) було впроваджено автоматизовані інформаційні системи (АІС), які стали опорою не тільки в адміністративній діяльності міліції, а й в боротьбі зі злочинністю. АІС надали змогу співробітникам інформаційних служб систематизувати об’єм інформації, з якою необхідно працювати органам внутрішніх справ, та можливість постійно поповнювати її новою та вилучати застарілу інформацію [2, 232]. Такий принцип діяльності АІС дає можливість оперативно надавати запитувану інформацію співробітникам підрозділів НП України й здійснювати їх головну мету – ефективність боротьби зі злочинцями та правопорушниками.

Система інформаційного забезпечення НП України – це сукупність взаємопов’язаних та взаємодіючих організаційних елементів та технічних засобів, яка здійснює інформаційне забезпечення НП України.

Формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення НП України, здійснюється згідно з такими принципами:

- нормативно-правової забезпеченості;

- фактичності даних;
- функціонального призначення (інформаційні підсистеми оперативно-розшукового, оперативно-довідкового, організаційно-управлінського призначення, інформаційні підсистеми кримінальної статистики, спеціалізовані інформаційні підсистеми);
- доцільності впровадження та експлуатації;
- нарощення та розвитку.

Інформаційна підсистема – це один чи декілька банків даних певних обліків, поєднаних відповідною технологією обміну інформацією.

Інформаційна система – це система обробки даних засобами накопичення, зберігання, оновлення та їх пошуку і відображення.

Інформаційні підсистеми як складові частини системи інформаційного забезпечення, призначені для збору, накопичення, зберігання та обробки інформації певних напрямків обліків і орієнтовані на використання в діяльності багатьох служб, мають загальновідомчий характер і відносяться до загальновідомчих інформаційних підсистем.

Структурна побудова інформаційних підсистем НП України поєднує принципи територіально-розподіленої та централізованої топології і організована у вигляді ієрархічної моделі з трьох рівнів. Належність інформаційної підсистеми до певного рівня визначається принципами територіальності, специфіки використання та обсягом інформації, яка обробляється.

Необхідно також відмітити, що зазначена система містить у собі наступні бази даних:

1. «Факт» (відомості щодо злочинів (правопорушень), подій, які загрожують особистій чи громадській безпеці, надзвичайних подій, викладених у заявах (повідомленнях, рапортах) та зареєстрованих у черговій частині).
2. «Злочин» (відомості щодо зареєстрованих злочинів (особливо тяжкі, тяжкі, середньої тяжкості), учинених на території обслуговування, у тому числі за матеріалами яких заведено ОРС).
3. «Контур» – електронні фотографії, опис зовнішності та особливих прикмет.
4. «Доставлені» (доставлені до НП України особи).

5. «Розшук» – відомості щодо оголошених у державний, міждержавний, міжнародний розшук.
6. «Особа» – відомості стосовно осіб, які вчинили правопорушення та щодо яких здійснюється профілактична робота працівниками НП України.
7. «Адміністративне правопорушення» – відомості щодо зареєстрованих в НП України адміністративних правопорушень.
8. «Корупційне правопорушення» – відомості щодо зареєстрованих корупційних правопорушень.
9. «Мігрант» – відомості щодо осіб, які порушили законодавство України про правовий статус іноземців та осіб без громадянства, виявлених працівниками НП України.
10. «Угон» – відомості щодо транспортних засобів (автомобілів, мотоциклів та мопедів), які розшукуються, а також виявлених безгосподарних, у тому числі викрадені та втрачені державні номерні знаки транспортних засобів.
11. «Річ» – відомості щодо речей, викрадених, вилучених з ознаками підробки, заборонених або обмежених в обороті у громадян і службових осіб, безгосподарних, що знайдено або вилучено із камер схову вокзалів, портів, аеропортів, та зданих до НП України.
12. «Втрачені документи» – відомості щодо документів (бланків документів) викрадених, утрачених, вилучених (з ознаками підробки) у громадян і службових осіб, паспортів померлих громадян України не зданих до НП України, паспортів осіб які знаходяться в розшуку, та які мають індивідуальні заводські (фабричні) номери і знаходяться у державному обігу.
13. «Кримінальна зброя» – відомості щодо зброї викраденої, утраченої, знайденої, зданої до НП України, вилученої працівниками НП України із числа тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей.
14. «Зареєстрована зброя» – відомості щодо зброї, що має індивідуальні заводські (фабричні) номери, перебуває у

користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано відповідно до законодавства дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується підрозділами дозвільної системи НП України.

15. «Електронний рапорт» – відомості, які було отримано/виявлено працівниками ОВС у процесі виконання ними своїх службових обов'язків або під час проведення гласних оперативно-розшукових заходів від громадян і посадових осіб (без розкриття джерела інформації і тільки відкритого характеру) [4].

Також у підрозділах Національної поліції України функціонує оперативно-довідкова картотека, яка призначена ля обробки інформації про судимості осіб. Включає обліки оперативно-довідкової картотеки та дактилоскопічні обліки ДІТ та НДЕКЦ МВС України і забезпечує:

- ведення автоматизованого обліку та видачу у встановленому порядку ОВС, СБУ, Прокуратурі, судам та іншим правоохоронним органам інформації про осіб, які скоїли злочини на території України, були заарештовані, засуджені, затримані за бродяжництво, зникли від слідства та суду;
- ідентифікацію осіб які приховують свої біографічні дані від правоохоронних органів;
- пошук злочинців по слідах, виявлених на місці злочину.

До складу ОДК входять також підсистеми «Мігрант» та «Рубін-2002»:

Підсистема «Мігрант» – веде облік осіб, затриманих за порушення законодавства України про державний кордон та про правовий статус іноземця.

Підсистема «Рубін-2002» – дозволяє реалізувати технології віддаленого оперативного доступу до банків даних з метою введення інформації і перевірки вимог на судимості [4].

1. Закон України «Про інформацію» від 02.10.1992р. [Ел. ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1906-15
2. Кормич Б.А. Інформаційне право: підручник. – Харків: БУРУН і К., 2011р. – 334с.

3. Ковальов М. В. Проблеми інформаційного забезпечення діяльності практичних підрозділів ОВС та впровадження інформаційних технологій в навчальний процес / М.В. Ковальов. – Л., 2004. – 201
4. Про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: положення від 16 травня 2016 р. № 460 // Наказ Міністерства внутрішніх справ. – 2016. – № 436.

Особливості інформаційного забезпечення органів Національної поліції та шляхи його оптимізації

Коміссарчук Ю.А.,
доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Олійник Б.А.,
курсант Львівського державного університету
внутрішніх справ

Сучасний етап розвитку суспільства і становлення України як суверенної держави характеризується нечуваним зростанням ролі управління, ускладненням і розширенням його завдань у всіх сферах людської діяльності, які з успіхом розв'язуються на засадах нового інформаційно-методичного забезпечення. Високо кваліфіковане, раціонально збалансоване та організоване управління на базі сучасного інформаційного забезпечення у зовнішній і внутрішній політиці держави та системі державного господарювання, зокрема, в правоохоронній діяльності, організації боротьби зі злочинністю та профілактиці правопорушень виступає нині надійною запорукою успіху, законності, прогресу та правопорядку.

Основними завданнями функціонування системи інформаційного забезпечення ОВС вважаються:

- забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами поліції для розкриття;
- забезпечення динамічної та ефективної інформаційної взаємодії усіх галузевих служб поліції України, інших

правоохоронних органів та державних установ; забезпечення захисту інформації. Органи поліції користуються й іншим інформаційним забезпеченням. За доступністю його можна поділити на відкрите і закрите забезпечення. Відкрите – це забезпечення зовнішнього загального користування, наприклад, обласні адресно-довідкові картотеки (адресні бюро), а закрите – обмеженого користування, наприклад, оперативно-довідкова картотека джерел інформації, призначене тільки для певної категорії працівників, допущених до оперативно-розшукової діяльності. Окремі служби МВС створюють свої специфічні інформаційні системи, які забезпечують функціональну діяльність структури. Такі системи мають Головне управління пожежної охорони, Державна служба охорони, Медичне управління і деякі інші;

- розслідування, попередження злочинів і розшуку злочинців; збір, обробка та узагальнення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної, і контрольної-інформації для оцінки ситуації та прийняття обгрунтованих оптимальних рішень на всіх рівнях діяльності органів поліції.

Таким чином, ми бачимо, що інформаційне забезпечення органів поліції являє собою органічну єдність роботи щодо визначення змісту, обсягів, якості інформації, необхідної для здійснення управління, а також заходів щодо раціональної організації процесів збирання, систематизації, накопичення та обробки цієї інформації шляхом застосування різноманітних методів, методик і технічних засобів [3, с. 161].

Управління органами внутрішніх справ як у зовнішньому, так і внутрішньому напрямку грунтується на власній інформаційній системі, елементами якої є:

- зосередження у відповідних інформаційних масивах (банках даних) відомостей, необхідних для здійснення основних функцій органів поліції і управління структурними підрозділами системи національної поліції України;
- джерела отримання цих відомостей і схеми потоків інформації;
- засоби обліку, зберігання і переробки інформації;

- канали зв'язку і передачі інформації, персонал суб'єкта і об'єкта управління, що забезпечує діяльність інформаційної системи.

Головна мета інформаційної системи полягає в тому, щоб на підставі зібраних початкових даних отримати похідну, підсумкову інформацію, яка буде складати основу для підготовки управлінських рішень у системі органів поліції [2, с. 35].

Інформація, необхідна для здійснення управління органами, накопичується, обробляється і зберігається в єдиному інформаційному масиві (банку даних).

Система інформаційного забезпечення являє собою сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання та забезпечення загальновизначених та обов'язкових вимог: нормативно-правової бази, організаційно-кадрового забезпечення інформаційних підрозділів, навчання та перепідготовки кадрів; комп'ютерних, програмних, телекомунікаційних засобів та технологій; матеріально-технічного та фінансового забезпечення.

Основною метою системи інформаційного забезпечення органів внутрішніх справ України є всебічна інформаційна підтримка діяльності ОВС у боротьбі зі злочинністю на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів. Формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення ОВС, здійснюється згідно з такими принципами: функціонального призначення. Нормативно-правової забезпеченості; фактичності даних; доцільності впровадження та експлуатації; нарощення та розвитку [1, с. 173].

Інформаційні підсистеми як складові частини системи інформаційного забезпечення, призначені для збору, накопичення, зберігання та обробки інформації певних напрямків обліків і орієнтовані на використання в діяльності багатьох служб, мають загальновідомчий характер і належать до загальновідомчих інформаційних систем.

Належність інформаційної підсистеми до певного рівня визначається принципами територіальності, специфіки використання та обсягом інформації, яка обробляється. Перший рівень – центральний, інтегрує інформаційні підсистеми ОВС загальновідомчого значення та галузевих служб МВС України. На

центральному рівні інтегрується інформація, що використовується при аналізі, плануванні, прийнятті рішень та проведенні в межах України оперативно-розшукових, слідчих та інших спеціальних заходів по боротьбі зі злочинністю. До складу інформаційних обліків першого рівня входять:

- банки кримінологічної інформації про надзвичайні події, нерозкриті тяжкі та резонансні злочини, викрадені, загублені та вилучені предмети, знаряддя скоєння злочинів, речові докази, осіб таких категорій: особливо-небезпечних рецидивістів; гастролерів; оголошених у розшук; організаторів і членів злочинних угруповань, кілерів; засуджених за злочини, пов'язані з наркотиками, торгівців наркотичними речовинами, схильних до вчинення злочинів, які посягають на інтереси держави; безвісти зниклих; невпізнаних трупів та невідомих хворих;
- банк оперативно-довідкової інформації, що містить дані алфавітного та дактилоскопічного обліків раніше засуджених осіб;
- банк статистичної інформації, що містить дані про стан злочинності та результати боротьби з нею;
- банк спеціальної інформації;
- банк паспортної реєстрації громадян;
- банк з інформацією про зареєстрований автотранспорт;
- банк з інформацією про зареєстровану вогнепальну зброю;
- банки даних адміністративно-управлінського призначення;
- банки даних спеціалізованого призначення галузевих служб;
- банки даних архівів та спеціальних фондів [5, с. 8].

Стрімкий розвиток інформаційних технологій у світовому просторі призвів до активного їхнього використання у боротьбі зі злочинністю. Основними тенденціями розвитку інформаційних систем у правоохоронній сфері є: удосконалення форм та методів управління системами інформаційного забезпечення; централізація та інтеграція комп'ютерних банків даних; впровадження новітніх інформаційних технологій для ведення кримінологічних та криміналістичних обліків; широке використання ефективних комп'ютерних мереж; застосування спеціалізованих засобів захисту інформації; налагодження ефективного обміну кримінологічною інформацією на міждержавному рівні [4, с. 32].

1. Про інформацію: Закон України від 02 жовтня 1992р. № 48, ст.651, станом на 06 квітня 2000 р. № 27, ст. 213.
2. Бабаскін В.В., Жалгунова С.А. Проблемні питання інформаційного забезпечення діяльності ОВС // Науковий вісник ЮА МВС. – 2014. – № 3. – С.32-38.
3. Бандурка О.М. Управління в органах внутрішніх справ України: Підручник. – Харків, 2009. –780 с.
4. Державне управління: Навч. посіб. / Мельник А.Ф., Оболенський О.Ю., Васіна А.Ю., Гордієнко Л.Ю.; За ред. А.Ф. Мельник. – К.: Знання-Прес, 2013. – 343 с.
5. Інформаційні підсистеми ОВС України. – http://www. naiau.kiev.ua/biblio/books/Kriminal inform/tema 3/htm.

До питання застосування гласних заходів пошукового характеру щодо виявлення та отримання інформації

Кондратюк О.В.,
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Будь-яку гласну пошукову діяльність в поєднанні із негласними методами роботи оперативних підрозділів щодо виявлення інформації протиправного характеру можна віднести до оперативно-розшукової діяльності відповідно до визначення поняття оперативно-розшукової діяльності.

На основі аналізу прав підрозділів, які здійснюють оперативно-розшукову діяльність, передбачених ст. 8 Закону «Про ОРД», ми виділили гласні заходи пошукової діяльності, а саме:

- опитування осіб за їх згодою, використання їх добровільної допомоги (*безпосередній пошук носіїв інформації*);
- порушення в установленому законом порядку питання про проведення перевірок фінансово-господарської діяльності підприємств, установ, організацій незалежно від форми власності та осіб, які займаються підприємниць-

кою діяльністю або іншими видами господарської діяльності індивідуально, та прийняття участі в їх проведенні (*безпосередній пошук ознак протиправної діяльності*);

- ознайомлення з документами та даними, що характеризують діяльність підприємств, установ та організацій, із правом вивчати їх, виготовляти копії з таких документів (*безпосередній пошук як джерел інформації, так і ознак протиправної діяльності*);
- відвідування жилих та інших приміщень за згодою їх власників або мешканців для з'ясування обставин злочину, що готується, а також збір відомостей про протиправну діяльність осіб, щодо яких провадиться перевірка (*безпосередній пошук як джерел інформації, так і ознак протиправної діяльності*);
- отримування від юридичних чи фізичних осіб безкоштовно або за винагороду інформації про злочини, що готуються або вчинені, та про загрозу безпеці суспільства і держави (*безпосередній пошук як джерел інформації, так і ознак протиправної діяльності*);
- використання за згодою адміністрації службових приміщень, транспортних засобів та іншого майна підприємств, установ, організацій, а так само за згодою осіб – житла, інших приміщень, транспортних засобів і майна, які їм належать (*можна використовувати як спосіб виявлення осіб, схильних до протиправної діяльності, створюючи різні, до прикладу, пастки чи інші умови реалізації злочинного наміру*);
- створення і застосування автоматизованих інформаційних систем (*для накопичення та аналізу інформації з метою виявлення суб´єктів протиправної діяльності*);
- звернення у межах своїх повноважень із запитами до правоохоронних органів інших держав та міжнародних правоохоронних організацій (*отримання неочевидної інформації*).

Вкотре наголошуємо, що перелічені гласні заходи пошукової діяльності обумовлені правами оперативного підрозділу як суб'єкта оперативно-розшукової діяльності. А якщо такий

підрозділ не здійснює на даний час в конкретному випадку оперативно-розшукову діяльність, які ж є правові підстави застосування зазначених заходів, адже право не являється підставою, але наявність підстави обумовлює виникнення права. Крім того, статтею 7 Закону чітко визначено обов´язком підрозділів, які здійснюють оперативно-розшукову діяльність, зобов´язання вживати заходів щодо попередження, своєчасного виявлення і припинення злочинів та викриття причин і умов, які сприяють вчинення злочинів, а також здійснювати профілактику правопорушень.

Зрозумілим і логічними є те, що для того, щоб знайти, необхідно шукати, а латентна злочинність, на жаль, нам не вказує місця, де треба шукати. Відтак, під так звані заходи із відпрацювання чи загальної профілактики підпадає той масив можливих джерел і носіїв інформації, який здатен охопити оперативний підрозділ. Звичайно, що застосування згаданих заходів не повинно носити тотальний характер, супроводжуватися порушенням чи необґрунтованим обмеженням прав громадян, безпідставними втручаннями в господарські процеси підприємств, адміністративну діяльність установ та організацій тощо. З іншої сторони, спостерігаючи відношення суспільства до правоохоронних органів, необхідно очікувати супротив, але якщо особа чи суб´єкт господарської діяльності «чисті перед законом», відповідно їм немає чого боятися, крім того обов´язком громадян є сприяння правоохоронним органам у виконанні покладених на них функцій, що прямо прописано в ст.11 Закону. На жаль, сьогодні суспільство добре пам´ятає про обов´язки правоохоронних органів, в той же час далеко не всі громадяни пам´ятають та знають про свої обов´язки перед тим же суспільством і правоохоронними органами зокрема.

Аналіз нормативно-правового забезпечення оперативно-розшукової діяльності Національної поліції дозволяє нам констатувати, що реалізація завдань оперативно-розшукової діяльності, по суті, відбувається шляхом застосування заходів оперативного пошуку (негласної роботи) та оперативно-розшукових заходів із використанням оперативних та оперативно-технічних засобів. На відміну від оперативно-розшукових заходів, застосування яких проводиться лише за заведеними оперативно-розшуковими справами, з метою виконання завдань оперативно-розшукової

діяльності оперативні підрозділи Національної поліції можуть здійснювати оперативний пошук. В теорії оперативно-розшукової діяльності та відомчих нормативно-правових актах під оперативним пошуком розуміють комплекс заходів, що не порушує прав і свобод громадян, здійснюється оперативним підрозділом з метою виявлення, запобігання та припинення злочинів, профілактики протиправної діяльності. Пошукова діяльність оперативних підрозділів частково урегульовується відомчими нормативно-правовими актами із грифом секретності. Ними ж визначено перелік і зміст пошукових заходів. В тексті Закону взагалі не згадується оперативний пошук, який, до речі, є однією із форм оперативно-розшукової діяльності, а тим більше не прописані в тексті Закону конкретні заходи із його реалізації з метою виконання завдань оперативно-розшукової діяльності. Якщо оперативній розробці, як формі оперативно-розшукової діяльності, що здійснюється після заведення оперативно-розшукової справи шляхом застосування оперативно-розшукових заходів і носить негласний (таємний) характер, в Законі визначено місце, то поняттю, змісту та заходам оперативного пошуку, які, переважно мають гласний (відкритий) характер, такого місця не знайшлося. А це, на нашу думку, і призводить до виникнення конфліктних ситуацій між громадянами та оперативними підрозділами, на зразок: «Що ви тут робите, чому ви нами цікавитеся, це політичне переслідування?!». Крім того, якщо оперативна розробка полягає у встановленні, накопиченні, фіксації фактичних даних про діяння осіб, стосовно яких є дані про участь у протиправній діяльності, то основним завданням оперативного пошуку є саме процес безпосереднього чи опосередкованого виявлення, відшукання даних про участь такої особи у протиправній діяльності, а відтак заходи і зміст такої діяльності однозначно повинні визначатися положеннями Закону «Про оперативно-розшукову діяльність».

Вплив структурної організації спеціального програмного забезпечення автоматизованих інформаційних систем МВС України на його стійкість функціонування

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

Автоматизовані інформаційні системи (далі – АІС) МВС України є системами реального часу, відмовлення чи відступ від заданих обмежень яких може викликати серйозні наслідки. Залежність цих АІС від програмних засобів породжує необхідність надання застосовуваним у них програмним засобам заданих властивостей якості при виконанні критичною системою основної своєї цільової функції.

Необхідність ретельного дослідження якості саме спеціального програмного забезпечення (далі – СПЗ) в АІС МВС України обумовлена тим, що програмне забезпечення несе більше функціональне навантаження при вирішенні завдань управління, ніж технічні засоби. Крім того, відомо, що витрати на розробку СПЗ мають тенденцію до збільшення і складають 50-80 % витрат на розробку АІС в цілому. Тому якість СПЗ в значній мірі визначає якість системи в цілому.

Предметом дослідження даної роботи є стійкість функціонування та здатність до відновлення СПЗ АІС МВС України і вплив на них його структурної організації. Стійкість функціонування СПЗ – це спроможність СПЗ підтримувати заданий рівень виконання у випадках внутрішніх помилок. Здатність до відновлення СПЗ – це спроможність СПЗ відновлювати свій рівень виконання і відновлювати дані, що були зіпсовані безпосередньо у разі відмови.

Структурна організація СПЗ в загальному випадку залежить від наступних факторів: обраної методології проектування; процесу реального світу, для управління яким створюється автоматизована інформаційна система; використовуваних в системі управління стандартних технічних і програмних засобів.

Запропонована в роботі методологія структурного проектування СПЗ АІС МВС України добре враховує умову гнучкості СПЗ (модульність, структурність, здатність до переміщення програм). Для СПЗ припустимими структурами є: підсистеми-комплекси задач, інтерфейси задач, ядра-підпрограми, структури структурного програмування.

Стійкість функціонування та здатність до відновлення структури СПЗ АІС МВС України досягається на всіх етапах розробки наступними прийомами: 1) реалізацією модульно-ієрархічного принципу побудови завершеного СПЗ і введенням ієрархічного контролю виконання програми; 2) введенням програмних засобів підвищення стійкості функціонування технічних засобів; 3) введенням програмних засобів підвищення вірогідності даних при функціонуванні програми.

Модульно-ієрархічний принцип побудови програми дозволяє реалізувати ланцюги зворотних зв'язків з боку модулів нижчих рівнів. Під прямим зв'язком розуміється запуск (передача управління) підлеглого модуля модулем вищого рівня. Під зворотним зв'язком – надання модулю вищого рівня повідомлень, що ідентифікує результати роботи запущеного модуля. Повідомлення аналізується на вищестоящому рівні, на підставі чого приймається рішення або про продовження подальшого функціонування, або про передачу повідомлень на більш високий рівень. Глибина зворотного зв'язку (число шарів, охоплених зв'язком) дозволяє забезпечити ієрархічний контроль результатів виконання програми і залежить від наявних ресурсів, вимог до надійності АІС та ін. Кожний модуль залежно від виду реалізованої функції (обчислення, логічний аналіз тощо) має містити відповідні засоби самоконтролю виконання.

При ініціації модуля використовуються програмні засоби контролю вхідних параметрів, при завершенні роботи – засоби контролю результатів обробки даних. Модуль направляє головному модулю задачі повідомлення про результат завершення своєї роботи за допомогою обумовлених ідентифікаторів – кодів завершення. Головний модуль задачі аналізує результати роботи підлеглих модулів за допомогою кодів завершення, наданих йому модулями. У випадку позитивних результатів самоперевірки модулем вихідних параметрів головний модуль задачі може дати

дозвіл про надсилання вихідних даних в область глобальних змінних. У випадку, якщо в результаті аналізу коду завершення головний модуль задачі не знаходить позитивного рішення про продовження подальшої роботи, управління і повідомлення про відмову модуля передається головній організуючій задачі. Виклик кожного модуля повинен мати стандартну перемінну – код повернення, аналіз якого дозволяє модулю, що викликав, оцінити ступінь виконання функції. Контроль здійснюється в наступній ієрархічній структурі: стандартна операційна система – головна задача – функціональні задачі – структури. Всі рівні, крім головної задачі, охоплені зворотними зв'язками.

Таким чином, реалізація модульно-ієрархічного принципу побудови завершеного спеціального програмного забезпечення АІС МВС України і введення ієрархічного контролю виконання програми, а також введення програмних засобів підвищення стійкості функціонування технічних засобів, підвищення вірогідності даних при функціонуванні програми дозволяють підвищити стійкість функціонування та здатність до відновлення структури СПЗ на всіх етапах його розробки.

Захист інформаційного суверенітету як важлива складова політичної функції держави

Кузенко У.І.,
здобувач кафедри теорії та історії держави і права, конституційного та міжнародного права Львівського державного університету внутрішніх справ

У сучасному світі створюється єдина глобальна комунікаційна система. У цьому процесі беруть участь держави, міжнародні інформаційні агенції, транснаціональні медійні корпорації, неурядові правозахисні організації тощо.

Сьогодні ми стаємо свідками того, що сучасні інформаційні технології проникають у всі сфери суспільного життя, спричиняють не тільки нові можливості, але й певні загрози. Внаслідок виникнення, накопичення, використання та розповсюдження великої кількості інформації у світі та її властивості поширюватись

майже миттєво на значні відстані постає питання про визначення інформаційного простору та його співвідношення з територією держави, державною безпекою, державним суверенітетом.

Новітніми інформаційними технологіями створюється інформаційний простір, у якому практично відсутні державні кордони, однак безконтрольність розповсюдження інформації, так само як і обмеження до її доступу, може завдавати значної шкоди державним та суспільним інтересам. У зв'язку з цим виникає питання щодо окреслення меж розповсюдження, збирання, використання, зберігання та доступу до інформації на території держави та серед її громадян, що, у свою чергу, ставить проблему юридичного характеру щодо визначення таких категорій, як інформаційний простір, інформаційний суверенітет та інформаційна безпека держави [3, с. 367].

Те, що відбувається в глобальному інформаційному середовищі, набуває дедалі більшого значення для соціокультурного життя. Отже, на сьогодні інформаційний простір активно формується й держава прагне встановити контроль лімітування кордонів і позначити власну територію у глобалізованому середовищі.

Суверенітет (нім. souverdnitdt, франц. souverainete – верховна влада, похідні від латин. super – над) у юридичній науці визначається як найважливіша азнака держави у вигляді її повної самостійності, тобто верховенства внутрішньої політики та незалежності в зовнішній.

В усі часи суверенітет держав обмежувався багатьма факторами. У нинішньому світі виникає необхідність переосмислення та переоцінка поняття «суверенітет». При цьому все більше простежується тенденція відмови від частини національного суверенітету на користь наднаціональних і світових спільнот, міжнародних організацій. Найголовніше в суверенітеті – право війни та миру – знаходиться під світовим контролем.

Збереження територіальної цілісності та громадського спокою в країні сьогодні не може бути забезпечено виключно військовим захистом суверенітету. Виникли такі форми нападу на державу, як обмеження потоків інформації через міжнародну інформаційну мережу, дезінформація, створення інформаційного хаосу. Виникає проблема забезпечення інформаційного суверенітету. Зараз він захищається головним чином національним

законодавством, міжнародні угоди в цій галузі практично відсутні. Проти інформаційного суверенітету держав спрямовується політика транснаціональних корпорацій. Глобальний інформаційний простір як якісно нове середовище функціонування й розвитку міжнародних відносин, органічно втілює економічні, політичні, соціальні й культурні процеси, а самі інформаційні технології стають значною змістовною характеристикою цих процесів, створюють принципово нові умови функціонування та розвитку інформаційних ресурсів. Саме цим обумовлюється важливість вирішення Україною проблем подолання негативних тенденцій і створення у правовому та організаційному плані логічно завершеної системи управління, формування, розвитку, використання, захисту інформаційних ресурсів [1, с. 106].

Закон України «Про національну програму інформатизації» визначає інформаційний суверенітет держави як здатність держави контролювати і регулювати потоки інформації з-за кордонів держави з метою дотримання законів України, прав і свобод громадян, гарантування національної безпеки. В інший спосіб розкриває поняття інформаційного суверенітету Закон України «Про інформацію» та Закон України «Про науково-технічну інформацію», якими передбачається, що основою інформаційного суверенітету є національні інформаційні ресурси. Найбільш вичерпним є визначення інформаційного суверенітету, що пропонується у науковій літературі: «це виключне право України відповідно до Конституції та законодавства України, нормам міжнародного права самостійно й незалежно, з дотриманням балансу інтересів особи, суспільства та держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню й зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови задля його інтеграції у світовий інформаційний простір і гарантувати інформаційну безпеку держави» [4, с. 535].

Проблеми забезпечення інформаційного суверенітету виникли як проблеми нового інформаційного суспільства, що набувають дедалі більшої актуальності, та щораз більш насущними стають питання, пов’язані з необхідністю конкретизації уявлень

про інформаційний суверенітет, уточнення його характеристик для отримання практичної відповіді на питання про методики й засоби його збереження та вдосконалення.

Розвиток України як правової демократичної держави неможливий без переходу й розвитку інформаційно відкритого суспільства, що передбачає виникнення нових форм інформаційної взаємодії державної влади із суспільством. Насамперед, державна влада має здійснювати відкриту і чесну інформаційну взаємодію з громадськістю через засоби масової комунікації.

Специфічною ознакою глобалізаційних процесів в умовах розвитку інформаційного суспільства є втрата контролю з боку політичних інститутів держави над змістом інформаційного простору. Це явище має як позитивні наслідки, зокрема — відкритість національних інформаційних систем, так і негативні, оскільки призводить до суттєвих проблем у проведенні цілеспрямованої державної інформаційної політики. Саме тому більшість розвинутих країн на найвищому державному рівні приділяють серйозну увагу творенню і розвитку національного інформаційного простору [2, с. 56, 58].

Останнім часом цілеспрямованим поширенням інформації за кордон активно займаються соціальні медіа, наприклад, група «Інформаційний спротив». Група веде планову спрямовану політику викриття (спростування) неправдивої інформації про події в Україні, про стосунки України і Росії. Підготовлені експертами аргументовані матеріали перекладаються різними мовами (англійською, німецькою, французькою, чеською, болгарською та ін.) і поширюються інформаційними каналами світових ЗМІ.

Причиною відсутності докорінних змін у позиціонуванні образу України в світовому інформаційному просторі є наступні фактори: недостатність чіткої координації між органами влади; змістові та методичні недоліки в інформаційно-роз'яснювальній роботі, яка проводилась у цьому зв'язку українськими органами державної влади; недостатня увага до визначення цільової аудиторії, на яку, перш за все, мав би бути здійснений інформаційний вплив при проведенні конкретного заходу; спроби безпосереднього руйнування існуючих негативних стереотипів щодо ідентифікації «образу» України виключно шляхом їхнього спростування, а не послідовною, систематичною й цілеспрямованою роботою щодо поступового їх заміщення новим позитивним [5].

Серед основних чинників, які перешкоджають Україні створити достатньо потужний імідж у світі та на достатньому рівні представляти українську тематику в інформаційному просторі інших держав можна назвати: недостатній рівень інтегрованості України у світовий інформаційний простір внаслідок слабкого розвитку необхідної для цього матеріально-технічної бази; брак фахових спеціалістів, особливо у державних органах влади, з міжнародної інформації та PR-технологій; недостатня увага центральних органів влади до проблеми забезпечення позитивного міжнародного іміджу України [2, с. 62].

Таким чином, у сучасних умовах Українська держава потребує цілеспрямованої інформаційної політики, яка б, з одного боку, забезпечувала потреби кожної людини в інформації, надаючи їй усебічний і гармонійний розвиток, а з іншого – слугувала б ефективним інструментом захисту національної безпеки та територіальної цілісності України. Розробка та впровадження такої інформаційної політики повинні стати першочерговим завданням діяльності центральних органів влади та виступати невід'ємною складовою стратегії соціально-економічного розвитку та програми соціально-економічних реформ в Україні.

1. Герасимова О.А. Забезпечення державного інформаційного суверенітету як функція державної мови / О.А. Герасимова // Теорія та практика державного управління. – 2009. – Вип. 4. – С. 103–110.
2. Інформаційна складова державної політики та управління: монографія / С.Г. Соловйов, та ін.; заг. ред. Н.В. Грицяк; Нац. акад. держ. упр. при Президентові України, Каф. інформ. політики та електрон. урядування. – К.: К.І.С., 2015. – 320 с.
3. Новікова Н.А. Інформаційний простір як основа інформаційної функції сучасної держави / Н.А. Новікова // Актуальні проблеми держави і права. – 2011. – Вип. 61. – С. 365–373.
4. Олійник О.В. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної України / О.В. Олійник, О.В. Соснін, Л.Є. Шиманський // Держава і право: Збірник наукових праць. – Вип. 13. – С. 534–541.
5. Чупрій Л.В. Створення позитивного іміджу України у світі / Чупрій Л.В. [Електронний ресурс]. – Режим доступу: http://oprosdim.com/index.php.html.

Нормативно-правове забезпечення у сфері боротьби із кіберзлочинністю в Україні

Магеровська Т.В.,
доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент
Беркій Х.Л.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ

У XXI ст. людство не може уявити свого життя без інформаційних технологій (далі – ІТ), які заполонили майже всі сфери життєдіяльності. Як свідчить статистика, українці все більше користуються благами інформаційної ери та намагаються використовувати всі можливості, що стали доступними внаслідок науково-технічної революції. Не зважаючи на переваги, які отримало людство в результаті технічного прогресу, використання ІТ викликало появу нового виду злочинів, які загально можна окреслити як кіберзлочини.

У літературі вживається як поняття «кіберзлочинність», так і «комп'ютерна злочинність». Ці два терміни дуже близькі один одному, але, на думку науковців, не є синонімами. Поняття «кібезлочинність» є ширшим, ніж поняття «комп'ютерна злочинність», і більш точно відображає природу злочинності в інформаційному просторі.

Поняття «комп'ютерна злочинність» вперше з'явилося в американській науковій та юридичній літературі на початку 60-х років минулого століття [1]. «Комп'ютерна злочинність» – це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних. За останні 10-15 років сформувалося поняття «кіберзлочинність» – під якою розуміють злочинність в традиційному сенсі цього слова, але яка має місце в мережі Інтернет [3, с. 338].

Чинна вітчизняна нормативно-правова база у сфері боротьби проти кіберзлочинності є недосконалою і лише частково задовольняє потреби сьогодення. В Україні діє низка законів України та інших нормативно-правових актів в цій сфері, але, на жаль, вони

недостатньо охоплюють всі ключові елементи, що стосуються злочинності в інформаційному просторі, та не здатні повною мірою забезпечити кібербезпеку держави.

Слід зазначити, що в законодавстві України використовується чимало термінів, які не узгоджені між собою. Так у законі України «Про основи національної безпеки України» згадуються поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», однак ні в цьому нормативно-правовому актів, ні в інших не надається визначення цих термінів. У «Доктрині інформаційної безпеки України» згадуються «комп'ютерна злочинність», «комп'ютерний тероризм» та «кібератаки», але знову ж таки без жодного пояснення їх значення. Отже, як бачимо, законодавець використовує чимало термінів, що стосуються кібезлочинності, але не розкриває їх. Водночас це є значною прогалиною в законодавстві, оскільки виникають дискусії щодо правильного розуміння значення цих понять.

У 2005 році Україна ратифікувала Конвенцію «Про кіберзлочинність» від 23 листопада 2001 року, яка відповідно до ст. 9 Конституції України є частиною національного законодавства. Конвенція також не надає конкретного визначення поняття «кіберзлочинність», але окреслює коло суспільно небезпечних діянь, що мають статус кіберзлочинів. До них належать: незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання у дані, втручання у систему, зловживання пристроями, підробка та шахрайство пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав [4].

Повертаючись до України, слід зазначити, що деякі кроки щодо захисту від кіберзагроз робить і наша країна. Затверджено закони України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо. В розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України (далі – КК України) передбачено кримінальну відповідальність за суспільно небезпечні діяння у сфері ІТ. Водночас науковці та правники наголошують, що в

цього розділі необхідно передбачити відповідальність й за інші суспільно небезпечні діяння, які вчиняються з використанням мережі Інтернет та комп'ютерів.

У грудні 2011 року в Україні було створено Департамент по боротьбі з кіберзлочинністю МВС України (зараз Департамент Кіберполіції). Специфіка роботи в Кіберполіції полягає в тому, що працівники повинні володіти не лише нормативно-правовою базою, але й мати глибокі знання в сфері ІТ.

Що стосується підзаконних нормативно-правових актів, то про актуальність цієї проблеми наголошується в Указах Президента України: «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891, «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000, «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001.

Проте сучасний стан нормативно-правової бази щодо запобігання та протидії кіберзлочинності в цілому можна охарактеризувати як недосконалий через безсистемність та відсутність термінологічної визначеності в базових поняттях. Українське законодавство у сфері захисту інформації, на думку Ю. Омельченка, вимагає дуже серйозного доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», – зазначив експерт [2].

Отже, як зауважує М.О. Довбиш, кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Тому сьогодні особливо важливо вдосконалити наявні заходи боротьби з кіберзлочинність та розробити нові, які здатні ефективно забезпечити кібезбезпеку не лише окремої держави, а й всієї міжнародної спільноти. Одним із таких заходів є визнання на законодавчому рівні необхідності боротьби зі злочинністю в інформаційному просторі та закріплення в нормативно-правових актах як національного, так і міжнародного рівня основних напрямків такої боротьби.

1. Алієв М.М. Проблема кіберзлочинності та шляхи її подолання в сучасному інформаційному суспільстві // М.М. Алієв. [Електронний ресурс]. – Режим доступу: http://vuzlib.com.ua/ articles/ book/12123Proble ma_k%D1%96berzloch innost%D1% 96_t/1.html1.
2. Кіберзлочинність в Україні. [Електронний ресурс]. – Режим доступу: https://www.science-community.org/uk/node/16132\.
3. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби / Н.В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо-поліграфічний центр «Київський університет», 2009. – Вип. 19. – С. 338-342.
4. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки // О.О. Тихомиров [Електронний ресурс]. – Режим доступу: http://tihoma-law.at.ua/publ/kibernetichna_bezpeka/ protidija_kiberzlochinnosti_jak_skladova_derzhavnogo_zabezpechennja_informacijnoji_bezpeki/2-1-0-13.

Конфлікти у сфері інформаційно-аналітичного забезпечення ОРД

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

Оперативно-розшукова діяльність – як система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, спрямованих на захист громадян, суспільства і держави від злочинних посягань, а також як функціональна структура, що складається із суб'єктів ОРД, об'єктів ОРД, заходів, засобів і методів ОРД, – визначають конфліктну сутність цієї діяльності. Термін «конфлікт» походить від латинського слова «*konflictus*» (зіткнення), що означає зіткнення протилежних інтересів, поглядів; гостра суперечка; крайнє загострення суперечностей, що призводить до ускладнень чи гострої боротьби [1].

Важливою складовою ОРД є інформаційно-аналітична робота, яка визначається як передбачена законами України та врегульована відомчими нормативно-правовими актами система заходів, спрямованих на збір, обробку, систематизацію, узагальнення,

аналіз, зберігання та використання інформації, у тому числі обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах досудового слідства, безпеки громадян, суспільства і держави.

Уникнути конфліктів в інформаційно-аналітичній роботі в ОРД та їхніх наслідків, часом негативних, досить складно, тому й постає потреба вивчення їх сутності, причин, меж, динаміки, досвіду вирішення, прогнозування та запобігання. Зважаючи на те, що інформаційний конфлікт є не чим іншим, як формою соціального конфлікту, джерела конфліктів в інформаційно-аналітичній роботі необхідно шукати в соціальних конфліктах.

До головних причин, що викликають конфлікти в інформаційній сфері, науковці відносять прагнення до отримання певної свободи в інформаційному («віртуальному») просторі без урахування розбіжностей індивідуальної і суспільної моралі, життєвих цінностей, протиріччя між очікуваннями, практичними намірами і вчинками осіб, нерозуміння людьми своїх дій по відношенню один до одного, усілякі непорозуміння, логічні помилки та семантичні труднощі в процесі комунікації, недоліки і «неякісність» інформації тощо [2, с. 83–84].

Завдяки своєму міжгалузевому характеру, інформаційні конфлікти, як правило, пов’язані з різними галузями законодавства – адміністративним, цивільним, трудовим, сімейним, фінансовим, кримінальним, кримінально-процесуальним чи виправно-трудовим правом.

За правовими нормами інформаційні конфлікти можуть мати як забороняючий, так і зобов’язуючий чи уповноважуючий характер.

За територіальними ознаками, інформаційні конфлікти можуть носити внутрішньогруповий, внутрішньодержавний або міжнародний характер.

Зважаючи на те, що діяльність правоохоронних органів не застрахована від помилок, некомпетентності, відсутності спеціальних знань та навичок, перевищення службових повноважень та зловживань, можуть виникнути інформаційно-правові конфлікти не тільки між особою (фізичною чи юридичною) та правоохоронними органами, а й між окремими правоохоронними та правозастосовними органами, наприклад, між органами адвокатури та

слідства, між органами прокуратури та адвокатури, між структурними підрозділами окремого правоохоронного органу тощо.

У визначенні меж конфлікту виділяють три аспекти: просторовий, часовий та внутрішньосистемний.

Просторові межі визначають територію, на якій відбувається конфлікт. Вони можуть бути як мінімальними, так і глобальними.

Часові межі інформаційного конфлікту визначають його тривалість у часі (початок, розвиток, загасання та закінчення), що має значення для кваліфікації дій учасників конфлікту та вирішення питання про юридичну відповідальність.

Внутрішньосистемні межі визначаються тим, що практично будь-який конфлікт відбувається у певній обумовленій системі, будь-то сім'я, група співробітників, держава тощо. Конфлікт між сторонами, що входять до однієї системи, може бути більш глибоким, широким або частковим, обмеженим.

За соціологічною класифікацією суб'єкти інформаційного конфлікту поділяються на три рівні: індивіди, соціальні групи, держави (народи). Із правових позицій виділяються дві групи суб'єктів: фізичні і юридичні особи.

Саме на зазначених етапах та їх межах, як правило, виникають проблеми правового регулювання завдяки їх можливої невизначеності, що є характерною особливістю конфліктів в інформаційній сфері.

Розвиток конфліктної ситуації до фази порушення норм чинного законодавства чи міжнародно-правових актів, призводить до вчинення протиправних суспільно небезпечних діянь (дій або бездіяльності) – правопорушення, як крайньої форми інформаційного конфлікту, подальшого проведення передбачених законом процесуальних дій і притягнення винних до юридичної відповідальності.

Сутність інформаційного конфлікту полягає в тому, що це найбільш гострий спосіб розв'язання протиріч в інтересах, цілях, поглядах, що виникають в інформаційній сфері та в процесі соціальної комунікації, протидії суб'єктів інформаційних відносин, порушенні їх прав та обов'язків, у процесі обігу та захисту інформаційних ресурсів, як правило, супроводжується використанням інформаційних технологій та виходить за межі моралі, соціальних правил і правових норм, створюючи протиправну ситуацію – інформаційне правопорушення [3, с. 45].

Ми вважаємо, що у сфері інформаційно-аналітичного забезпечення ОРД виділяються три основних аспекти конфліктів:

- нормативно-правові (юридичні помилки, колізії правових норм, породжені в процесі нормотворення недосконалістю текстів законодавчих актів щодо регулювання інформаційних відносин та юридичної техніки їх застосування). Інформаційні нормативно-правові конфлікти виникають через суперечливість норм права та складають окремий різновид інформаційних конфліктів – конфліктні ситуації, в яких безпосередні учасники взагалі відсутні, а сам конфлікт відбувається на рівні нормативних визначень, викликаних недосконалістю текстів законодавчих актів щодо регулювання інформаційних відносин та юридичної техніки їх застосування [3, с. 41];
- організаційно-управлінські протиріччя. Невідповідність здійснюваних аналітичних досліджень, форм і методів оперативної роботи вимогам сьогодення та їх неадекватність сучасним суспільним відносинам, розвитку злочинних угруповань та їх проникненню в соціально-економічні й адміністративно-правові сфери діяльності зумовлює необхідність подальшого реформування інформаційно-аналітичної роботи в оперативних підрозділах. Національна поліція потребує створення на базі єдиного інформаційного поля підрозділів поліції із залученням інформаційних ресурсів інших органів державної влади та управління повного розвідувально-аналітичного циклу з метою ефективної обробки здобутої оперативним шляхом інформації, удосконалення якості наявних та отримання нових знань, необхідних для прийняття оптимальних управлінських рішень;
- конфлікти на організаційно-тактичному рівні отримання та використання інформаційно-аналітичної інформації. В інформаційному конфлікті оперативно-розшуковим заходам оперативних підрозділів протиставляються відповідні контрзаходи злочинців, їх підсобників та заінтересованих осіб. Це визначає необхідність збирання оперативними підрозділами максимальної інформації про об’єкт оперативної розробки і одночасно захисту себе від аналогічних дій у відповідь. Для подолання інформаційного конфлікту

оперативним підрозділам необхідно: забезпечувати конспіративність, розподіляти інформацію між виконавцями для збереження загального змісту інформації від можливого витоку, використовувати лише надійні канали зв'язку, запобігати можливості «зняття» інформації сторонніми особами за допомогою технічних засобів, використовувати технічні засоби збирання інформації та аналітичної розвідки, здійснювати заходи для дезінформації противника, перевіряти будь-яку інформацію, що надходить, проводити контррозвідувальні заходи з приводу можливих витоків інформації через корумпованих посадових осіб тощо [4, с. 399].

1. Словник іншомовних слів [Електронний ресурс]. – Режим доступу: http://eslovo.com.ua/slovnyk_inshomovnyk_sliv/page/ konflikt.9535/.
2. Боер В. М. Информационное право: учеб. пособие / В. М. Боер, О. Г. Павельева. – Ч. 1: ГУАП. – СПб., 2006. – 116 с.
3. Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 38–46.
4. Міжнародна поліцейська енциклопедія : у 10 т. / відп. ред. В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. – К. : Атіка, 2010. – Т. VI. Оперативно-розшукова діяльність поліції (міліції). – 1128 с.

Застосування сучасних інформаційних технологій у розвитку місцевого самоврядування

Мойсеєнко І.П.,
професор кафедри фінансів та обліку
Львівського державного університету внутрішніх справ,
доктор економічних наук, професор
Мойсеєнко І.В.,
аспірант кафедри теоретичної та прикладної економіки
Львівського торговельно-економічного університету

Впровадження європейського досвіду застосування сучасних технологій управління *Smart Grid*, заснованих на технічному

регулювання у сфері стандартизації «розумних міст та розумних спільнот» (*Smart Cities & Smart Communities)* з широким використанням новітніх інформаційних та комунікаційних технологій, на думку експертів, дасть можливість підтримувати адміністративно-територіальним утворенням динамічний баланс попиту й пропозиції, покращувати використання активів, підвищувати якість електроенергії та стійкість енергосистем до несанкціонованих зовнішніх впливів й стихійних лих і, зрештою, дасть поштовх розвитку нових видів продукції і послуг, а також формуванню нових ринків. Одним із головних довгострокових напрямів є створення економіко-правового середовища територіальних громад, що функціонує на основі єдиних норм, правил та стандартів в єдиному європейському економічному просторі.

Вирішальну роль в узгодженні, уточненні та формуванні майбутньої інноваційної моделі розвитку територіальних спільнот, адаптованої до функціональної еталонної архітектури розумної інтелектуальної мережі (*Smart Grid),* відіграє організація й виконання робіт з міжнародної, регіональної та національної стандартизації щодо продукції, процесів та послуг, зокрема систем, їхньої сумісності, правил, процедур, функцій та методів побудови. Міжнародні стандарти забезпечують підтримку формування політики держави у практичних рішеннях, які базуються на забезпеченні довіри до технічних характеристик та вимог техніки безпеки, а також сприяння в забезпеченні виконання зобов'язань для реалізації цілей сталого розвитку.

Особлива роль у виробленні єдиної технічної політики та загальних технічних принципів розвитку територіальних спільнот з метою *забезпечення процесів уніфікації, функціональної сумісності, взаємозамінності та надійності комунальних мереж, у тому числі енергетики, водних ресурсів, транспорту, поводження з відходами, ІКТ,* які забезпечують життєдіяльність територіальних громад і зосереджені на технічних аспектах в умовах глобальної відповідальності, в ЄС відведена співпраці міжнародних організацій, таких як Міжнародна організація зі стандартизації – *ISO* (*International Organization for Standartization*), Міжнародна електротехнічна комісія – *IEC (International Electrotechnical Commission*), Міжнародний Союз електрозв'язку – *ITU (International Telecommunication Union*), європейські організації із стандартизації, такі як – Європейський

комітет зі стандартизації – *CEN* (*European Committee for Standardization*), Європейський комітет зі стандартизації в електротехніці – *CENELEC* (*Comité Européen de Normalisation Électrotechnique*) та Європейський інститут із стандартизації в сфері телекомунікацій – *ETSI* (*European Telecommunications Standards Institute),* а також національні органи стандартизації – *NSB (National Standards Body*), технічні комітети стандартизації – *TC (Technical committees) та* розробників стандартів організацій – *SDOs (Standards Developing Organizations*)[1].

Міжнародна організація зі стандартизації (ISO), метою діяльності якої є ратифікація розроблених спільними зусиллями делегатів від різних країн стандартів, через свої технічні комітети стандартизації (*TC ISO*) сприяє розвитку стандартизації у світовому масштабі для полегшення міжнародного товарообміну та взаємодопомоги, а також для розширення співробітництва в галузі інтелектуальної, наукової, технічної та економічної діяльності. В *ISO* нині розроблено понад 21000 міжнародних стандартів, які включені в загальний каталог стандартів і ідентифікуються як за галузевими ознаками Міжнародного класифікатора стандартів – ***ICS (International Classification for Standards)***, так і за допомогою назв технічних комітетів стандартизації (*TC)* та ключових слів.

У рамках *ISO* з метою вироблення та реалізації цілісних міжсекторальних підходів та прийняття інтегрованих рішень для забезпечення сталого розвитку в *Smart community* в березні 2012 р. створено **Технічний комітет стандартизації – *ISO/TC 268* «Сталий розвиток в громадах»** *(Sustainable development in communities),* в структурі якого функціонує підкомітет *ISO/TC 268/SC 1* «Інтелектуальні громадські інфраструктури» (*Smart community infrastructures*) та робочі групи – *WG 1* «Системи управління» (*Management Systems*) і *WG 2* «Міські індикатори» (*City Indicators*).

Для забезпечення реалізації цілісних підходів в забезпеченні сталого розвитку *Smart community ISO TC 268* тісно взаємодіє з іншими технічними та проектними комітетами стандартизації *ISO*

1 New global platform to help cities become sustainable and smart [Електронний ресурс]. – Режим доступу : http://www.iso.org/iso/ru/news.htm?refid=Ref2042

щодо розробки стандартів, зокрема з: проектним комітетом – *ISO/TC 242* «Управління електроенергією» (*Energy Management*), технічними комітетами – *ISO/TC 224* «Послуги, що пов'язані з експлуатацією систем постачання питної води та систем відведення стічних вод. Критерії якості послуг та показники якості» (*Service activities relating to drinking water supply systems and wastewater systems – Quality criteria of the service and performance indicators*), *ISO/TC 204* «Автоматизовані транспортні системи» (*Intelligent transport systems*) та іншими.

Стандартизація сталого розвитку в спільнотах *ISO/TC 268* передбачає розроблення та оприлюднення стандартів серії *ISO/PRF 37101* як у вигляді проектів технічних доповідей (наприклад, ISO/DTR 37 121), так і у вигляді нових пропозицій щодо формування вимог до систем управління (*ISO/NP 37 122*) для різних видів *Smart community*.

Реалізація єдиної технічної політики для підтримки належної роботи інфраструктури щодо забезпечення уніфікації, функціональної сумісності, взаємозамінності та надійності комунальних мереж вимагає розробки та гармонізації необхідних стандартів на міжнародному рівні, які полегшать сумісність, відкритість нових учасників ринку, забезпечуючи безпеку та демонструючи можливості в боротьбі з кіберзлочинністю та тероризмом «*розумних міст та громад*» – *SC&C* (*Smart cities and communities*).

На даний момент у нормативній базі України не існує такого терміну, як «*розумна громада*», «*розумна спільнота*» або його україномовного аналогу. Для встановлення на державному рівні мінімально необхідних вимог та принципів побудови інтелектуальної інфраструктури «*розумних громад*» доцільно при розробці регламентної бази[2] розглянути можливість запровадження відповідних дефініцій. Це є важливим етапом, оскільки спектр питань, який необхідно охопити для ефективного розвитку територіальних громад, є доволі широким: формування технічних вимог до окремих компонентів «*розумних мереж*» (*Smart Grid)*,

2 Про технічні регламенти та оцінку відповідності : закон України від 15.01. 2015 р. № 124-VIII184 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/124-19

регламенти та протоколи взаємодії компонентів, електромагнітна сумісність, кібербезпека тощо.

Варто зазначити, що на даному етапі в міжнародній практиці не існує універсальної моделі розвитку «*розумних спільнот*» та чіткої ідентифікації поняття «*розумна громада*». Існує безліч визначень розумної громади, однак концептуально-архітектурний опис такої моделі позиціонується з декількома дефініціями в залежності від значень слова «розумний»: розумне місто (*Smart City*), розумне середовище (*Smart Environments*), розумні транспортні системи (*Intelligent Transportation System*), розумне виробництво (*Smart Manufacturing*), розумні будинки (*Smart Houses*), цифрове місто (*Digital City*) тощо. Ці поняття беруть свій початок з 1993 року з визначення вченими Каліфорнійського технологічного інституту «*розумної спільноти*» як спільноти, яка використовує інформаційні технології в межах свого регіону для фундаментального розвитку[3]. Водночас у працях науковців «*розумні громади*» досліджуються як з точки зору системного підходу якісного життя в співтоваристві, так і в залежності від економічних екологічних та етнографічних підходів.

У праці Дамера Р. та Кочіа А. на основі системного підходу здійснено аналіз наукових публікацій та висловлювань експертів за 20-річний період щодо визначення моделі «*розумних громад*» і виокремлено категорію, що визначає поняття «*розумна спільнота*» (*Smart Communities)*[4] як географічний район, в якому інноваційні технології у сфері інформаційно-комунікаційних технологій (*ІКТ)*, логістики, виробництва електроенергії тощо повинні створювати переваги для громадян з погляду їх включення до участі в наступному:

- оптимізації споживання енергії за рахунок енергоефективності та відновлювальних джерел енергії;

3 In Ajmer as a Smart City; an Assessment of Challenges and Responsibilities Dr.Ajay Kumar Sharma1 , Mrs. Rohini Yadawar2 International Journal of Interdisciplinary Research in Science Society and Culture(IJIRSSC), 2015 [Електронний ресурс]. – Режим доступу : http://ijirssc.in/pdf/1451536461.pdf

4 Smart City and Digital City: Twenty Years of Terminology Evolution R.P. Dameri and A. Cocchia [Електронний ресурс]. – Режим доступу : http://www.cersi.it/itais2013/pdf/119.pdf; Smart City How to Create Public and Economic Value with High Technology in Urban Space R.P. Dameri, C. Rosenthal-Sabroux [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books?id

- поліпшенні якості навколишнього середовища в міському просторі, зменшуючи викиди CO2 та кількість шкідливих відходів;
- підвищення якості життя громадян через забезпечення кращих державних та приватних послуг, таких як місцевий громадський транспорт.

Дослідник П. Хол, аналізуючи еволюцію інтелектуальної турбулентності творчих громад, дійшов висновку, що місто, яке контролює та інтегрує критичну інфраструктуру, в тому числі дороги, мости, тунелі, колії, метрополітени, аеропорти, морські порти, комунікації, водопостачання, електрику, великі будівлі може краще оптимізувати свої ресурси, планувати свої профілактичні заходи з технічного обслуговування і контролювати захист важливих об'єктів[5].

Підсумовуючи напрацювання сучасної науки та технічні аспекти у сфері дослідження «*розумних громад*», у червні 2015 р. на 63-му засіданні *Ради з технічного управління ISO* затверджене робоче визначення «*розумного міста*» (*Smart Cities)*[6] за такими ознаками:

- спільні інтереси у вирішенні питань життєдіяльності міста;
- фундаментальне поліпшення взаємодії в процесі реалізації інтересів у різних сферах міських мереж на основі використання інтегрованих технологій;
- соціальна взаємодія (мешканців, відвідувачів, підприємств) щодо отримання якісних послуг та рівня життя для тих, хто пов'язаний з містом.

Концептуальні засади та стратегії розвитку *Smart Cities* вимагають цілісного підходу у виробленні складного механізму взаємодії всіх зацікавлених сторін для економічного зростання територіальних громад з урахуванням таких викликів, як зміна клімату, швидке зростання чисельності населення, а також політичної та економічної нестабільності.

5 Creative cities and economic development. Urban Studies, 37(4), 633–649 [Електронний ресурс]. – Режим доступу : http://usj.sagepub.com/content/37/4/639.extract

6 Технічна резолюція правління 68/2015 [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/ga/second/68/second_res.shtml

Існуючі нині концептуальні підходи до побудови *Smart Cities* суттєво відрізняються в залежності від обраної стратегії. Так, наприклад, в Амстердамі основна увага у формуванні сталого розвитку спільноти приділяється посиленню екологічної стійкості, застосування новітніх технологій для скорочення шкідливих викидів в атмосферу, ефективнішого використання енергії. В інших містах вживаються заходи для перетворення широкого діапазону міських функцій в «*розумні*», використовуючи повсюдно поширені «*розумні технології*» у всіх аспектах життя спільнот. Прикладами такої стратегії можуть служити проекти «Місто електронної інтеграції» (*u-місто*) в Республіці Корея і Deutsche Telekom «*T-місто*» в Німеччині. Проект «*Розумний Сеул*» здійснюється з метою перетворення системи управління містом в більш «*розумну організаційну структуру*» для підвищення якості життя громад[7].

У різних містах ставляться різні пріоритетні цілі й завдання, але для них всіх характерні три найважливіші риси *Smart Cities.* Перша – наявність захищеної інфраструктури *ІКТ* для наступних поколінь, яка відіграє першорядне значення для успішного надання нових послуг в *Smart Cities*. Друга – в місті повинна бути створена чітко вибудувана й інтегрована система управління на основі дотримання єдиних стандартів. Третя – в *Smart Cities* повинні бути «*розумні*» користувачі. Основу *Smart Cities* становить відкрита для всіх єдина мережа користувачів «*розумних пристроїв*», сформована на основі єдиних стандартів, норм та правил.

В ЄС сформовано бачення майбутнього сталого міського та територіального розвитку з розвитку інтелектуальних мереж *(Smart Systems/IoT*) і сталого розвитку розумних міст та розумних спільнот – *SC & C* (*Smart Cities & Smart Communities),* яке зосереджене на виробленні єдиних підходів до стандартизації «*Інтернету речей*» – *IoT* (*Internet of Things)* та *SC & C.* Ця ініціатива спрямована на підтримку міст у скороченні викидів парникових газів на 40 % за рахунок стійкого виробництва та споживання енергії до 2020 року. Кожна країна, виходячи з

[7] Умные города Наблюдение за технологиями Новости МСЭ № 5 2013 Електронний ресурс]. – Режим доступу : https://itunews.itu.int/Ru/Note.aspx?Note=4232

власного стратегічного бачення сталого розвитку «*розумних громад*», формує свою інституційну платформу.

Головним завданням майбутнього є забезпечення єдності ідеології та управління науково-технічними процесами з урахуванням тенденцій глобальної зміни клімату та орієнтацією на світову модель перебудови електроенергетичного ринку з метою формування вітчизняної інтелектуальної електричної мережі, яка визначена в Європі через «*Платформу європейських розумних мереж електропостачання*» (*Smart Grid European Technology Platform*)[7].

Системні напрями створення моделі «*зеленої економіки*» виключно за рахунок відновлювальних джерел енергії передбачають розробку науково обґрунтованих заходів, які визначатимуть зміни у рамках сучасної екстенсивної парадигми економіки в Україні. Такі підходи вимагають *формування єдиної системи, заснованої на міжнародному механізмі співпраці, для* проведення наукових досліджень з основних питань збалансованого розвитку на регіональному, національному та місцевому рівнях та визначення формувача управління для реалізації світоглядної парадигми збалансованого розвитку.

Використання державних інформаційних реєстрів у юридичній практиці

Неспляк Д.М.,
доцент кафедри інформатики Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук
Дякун З.-В. П.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ
Магеровський Д.В.,
здобувач освітнього ступення «магістр»
Національного університету «Львівська політехніка»

Державні реєстри – це систематизовані бази даних про різні об’єкти, суб’єкти та їх правовий, економічний, природний чи

соціальний статус, процес створення та функціонування яких впроваджено на підставі відповідних нормативно-правових актів та держателем яких є уповноважені органи державної влади або спеціально створені ними державні підприємства [1].

Державні реєстри відіграють надзвичайно важливу роль в сучасному суспільстві. З одного боку, за допомогою реєстрів уповноважені органи державної влади можуть зберігати і систематизувати дані про об'єкти, суб'єкти та їх статус (правовий, економічний тощо), а з іншого, – реєстри є «знаряддям», за допомогою якого можна швидко отримати необхідні дані у певній сфері.

Розглянемо більш детально державні реєстри України.

Єдиний державний реєстр судових рішень – це систематизована база даних судових рішень всіх судів загальної юрисдикції України.

Відповідно до ЗУ Про доступ до судових рішень: Єдиний державний реєстр судових рішень – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень [2].

Реєстр судових рішень є відкритим для пересічних громадян, тобто, будь-яка бажаюча особа, може ознайомитись із необхідним судовим рішенням. Адміністратором Єдиного державного реєстру судових рішень України є Державне підприємство «Інформаційні судові системи».

Єдиний державний реєстр досудових розслідувань (Далі – ЄДРДР) – створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюються збирання, зберігання, захист, облік, пошук, узагальнення даних, зазначених у положенні, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру, з дотриманням вимог кримінального процесуального законодавства та законодавства, яким врегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом [3].

Тобто, ЄДРДР – це база даних, яка містить відомості, необхідні для проведення досудового розслідування.

Держателем ЄДРДР є Генеральна прокуратура України. Держатель ЄДРДР виконує функцію адміністратора реєстру. Реєстраторами ЄДРДР є прокурори, керівники прокуратур; керівники

органів досудового розслідування. Користувачами ЄДРДР є прокурори, керівники прокуратур; керівники органів досудового розслідування; слідчі органів поліції, безпеки і т. д.

Із вищезазначеного випливає, що ЄДРДР є закритою базою даних, доступ до якої мають лише уповноважені особи. За незаконне втручання у роботу ЄДРДР настає кримінальна відповідальність, передбачена ст. 361, ст. 362 Кримінального кодексу України.

Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань – це база даних, що містить відомості про юридичних осіб, фізичних осіб – підприємців та громадські формування, що не є юридичними особами.

Зазначений реєстр є відкритим і загальнодоступним для пересічних громадян. Адміністратором реєстру є державне підприємство «Національні інформаційні системи».

Єдиний державний реєстр нормативно-правових актів (далі – ЄДРНПА) – це автоматизована база даних, яка містить нормативно-правові акти (закони, підзаконні акти), видані уповноваженими державними органами і посадовими особами.

Користувачем ЄДРНПА може бути будь-яка фізична чи юридична особа, у якої виникла необхідність отримати інформацію, що міститься в реєстрі. Проте, щоб отримати необхідну інформацію з ЄДРНПА, потрібно звернутись із запитом до адміністратора ЄДРНПА. Адміністратором реєстру є державне підприємство «Інформаційний центр» Міністерства юстиції України.

Єдиний державний реєстр виконавчих проваджень – це база даних, за допомогою якої здійснюється зберігання, облік, пошук, надання даних про виконавчі дії.

Доступ до зазначеного реєстру мають сторони виконавчого провадження, у якому вони беруть участь. Адміністратором реєстру є державне підприємство «Інформаційний центр» Міністерства юстиції України.

Підсумовуючи викладене, можна сказати, що державні реєстри – це систематизовані бази даних про об’єкти, суб’єкти та їх статус, що функціонують на підставі нормативно-правових актів, та держателями яких є уповноважені державні органи або державні підприємства.

Реєстри допомагають пришвидшити та полегшити роботу уповноважених органів та посадових осіб, пересічних громадян (якщо реєстр загальнодоступний). Тобто, реєстри виконують надзвичайно важливу функцію у суспільстві – значною мірою полегшують роботу звичайних людей, які користуються ними, оскільки при наявності великої кількості неавтоматизованих і несистематизованих даних, ними неможливо було б користуватись.

1. Когут Н. Д., Організаційно-правова роль державних та інших реєстрів в забезпеченні безпеки суспільного ладу та прав людини/Н. Д. Когут - Інформація і право, 2016 р., № 2(17).
2. «Про доступ до судових рішень» : Закон України від 22.12.2005 р. // [Електронний ресурс]/Режим доступу: http://zakon5.rada.gov.ua/laws/show/3262-15
3. «Про порядок ведення Єдиного реєстру досудових розслідувань» : Положення від 06.04.2016 р. // [Електронний ресурс]/Режим доступу: http://zakon5.rada.gov.ua/laws/show/z0680-16/conv/page

Єдина цифрова платіжна система як засіб зміцнення економічної безпеки Держави

Пурій Р.П.,
аспірант Львівського торговельно-економічного університету

У світовій фінансовій сфері є одна обставина непереборної сили. Сучасні гроші і грошово-банківська система до якої ми звикли, еволюціонують у *цифрові платіжні системи* – системи безготівкових розрахунків.

Загальносвітовий тренд у банківській сфері – скорочення готівкового обігу, що веде до закриття пунктів касового обслуговування клієнтів. Зокрема в 2013 році тільки в Європі закрилось більше семи сотень банківських філіалів. З дещо інших причин, але в Україні стрімко скорочується не тільки кількість філіалів банків але і самі банки. Банки, що залишаються на ринку «оцифровуються», а Уряд рік від року скорочує суми, дозволені для готівкових розрахунків.

Світовий тренд трансформації грошово-платіжної системи паперових грошей в цифрову платіжну систему 100% електронних грошей не омине і Україну. Це питання 5-10 років і нам не варто ігнорувати цей факт. Чи готові ми, українське суспільство, жити в системі стовідсоткових електронних грошей? Які вигоди і ризики нашому добробуту несе ця система? Що краще для нас, народу України, залишити все під контролем нечистих на руку приватних банкірів чи взяти систему під свій конторолль, а може просто чекати падіння системи і на виживання під її обломками.

Якщо ми за контроль над ***системою,*** то нам залишається тільки підштовхнути розвал існуючої системи (наприклад, ігнорувати приватні банки) і контролювати трансформацію старого в нове.

Провідні світові економісти вважають правильною систему 100% електронних грошей, цифровий банкінг, з демерреджем в 4%. (демерредж – це від'ємний відсоток на депозит, тобто, в реалі, це мінус чотири відсотки річних на ваші кошти, що обертаються в банку). Насправді це пастка і глобальна афера банкірів, що несе загрозу економічному суверенітету всім громадянам цивілізованого світу.

На думку автора «правильним напрямком» розвитку суспільства є встановлення соціал-капіталістичного (різновид солідаризму) суспільного ладу. Соцкап передбачає, зокрема, ***суспільну (народну) власність*** на банківську систему. Нам потрібно інтенсивніше працювати над консолідацією громадянського суспільства довкола ідеї контролю за банківською системою країни через володіння нею.

Якщо народ України є носієм влади, то як суверен має природне право контролювати емісію грошей і грошовий обіг в економіці країни.

Що конкретно ми хочемо? Щоб у державі був єдиний, державний цифровий банк і щоб він належав народові. «Мої гроші в нашому банку»!

Що це таке?

Єдина цифрова платіжна система (ЄЦПС) – найбільш досконала система ***консолідації*** і управління універсальним ресурсом – грошима як ***суспільним благом***.

Чому система має бути єдиною?

Консолідація платіжного засобу в одному цифровому банку спрощує управління і автоматизацію всіх фінансових процесів,

ліквідовує можливість фінансових махінацій з грошима шляхом перекидання їх з банку в банк і оготівковування. Стає неможливим переведення клієнтами коштів з банку в банк, пов'язаною з міграцією клієнтів, що призводить до банкрутства банківської установи і втрати клієнтами своїх заощаджень. Закривається тема міжбанківської конкуренції і, знову ж таки, банкрутства банку.

Саме завдяки цим можливостям ЄЦПС має стати потужним і надійним засобом зміцнення економічної безпеки грошово-банківської системи зокрема і Держави загалом.

Єдина система дає можливість спрощувати управління економікою Держави, здешевлює управлінські процеси. Всі гроші в одному банку – це блискавичні розрахунки. Гроші не виходять за межі банку, завжди доступні і завжди на місці. Змінюються тільки їх тимчасові власники. Це дає можливість для максимальної автоматизації облікової, фіскальної, статистичної функції цієї системи.

Образно кажучи, єдина цифрова, автоматична, платіжна система нагадує нам земну атмосферу, де всі дихають одним повітрям і воно належить всім і нікому одночасно. Інший образ – вода в басейні. Кожному співвласнику води належить якась кількість у літровому еквіваленті і люди обмінюються, продаючи і купуючи, але ніхто воду з басейну для цього не вичерпує і кількість води в басейні не зменшується.

Цифровий банк. Саме цифрові технології дозволяють автоматизувати багато процесів в обліку, статистиці і розрахунках. Перехід на 100% електроні гроші ліквідовує проблему, пов'язану з обслуговуванням готівкового обігу: виготовлення нових купюр, захисту купюр від підробок, зберігання і транспортування паперових грошей, охорону транспортування і зберігання.***Рівень безпеки банківських операцій, що може забезпечити ЄЦПС безпрецидентний***. Йде в історію система банкоматів і платіжних терміналів. А ще вирішується проблема нелегальної торгівлі, хабарництва і корупції.

Повна автоматизація банківської системи. Сучасні цифрові технології, застосовані в Є. Автоматизованій П.С., дозволяють охопити всю грошову масу держави, а також всю товарну масу і послуги, заявлені на національному ринку. «Заявлені» означає оцифровані і введені в реєстр торгівельних мереж як в рітейлі так і в віртуальних магазинах. Саме через облік і регулювання

доступної покупцям грошової маси можна регулювати стабільність купівельної спроможності українського ринку і, автоматично, національної грошової одиниці. В процеси регулювання включається ***вартість кредитних грошей,*** розмір ставки кінцевого, ***плаваючого податку на споживання*** (а це трансформоване ПДВ), а також регулювання добової доступності коштів, що направляються на споживання.

Фіскальна функція ЄЦПС. Цифрова система банківництва дозволяє автоматизувати збір податків (усуває людський фактор, а з ним корупцію і зловживання), але для цього слід кардинально змінити підходи до фіскальної політики. Щоб бізнес перейшов на цифрові технології Уряду слід забути про податки на прибуток бізнесу і доходи громадян, а зайнятись оподаткуванням споживання. Цей податок піддається автоматизації і чудово зніматиметься в рітейлі (підігнаний під систему ПДВ). Але це, наразі, інша тема. Електронна платіжна система дає можливість ***ввести податок на споживання (покупки).*** «Багаті платять більше» – ця ідея спрацьовує як в системі кредитування так і при оподаткуванні покупок.

Автоматизація платіжної системи звільняє велику кількість робочої сили, що має мігрувати в реальний сектор економіки. Система також усуває людський фактор з банківської сфери, а це усуває можливості шахрайства і чисельних зловживань.

Прозорість. Банківська платіжна система Держави повинна стояти на платформі електронних грошей і цифрових технологій. Сучасні технічні можливості дозволяють вибудувати ***прозору систему банківництва,*** гідну сучасного розумінню демократії. Така банківсько-платіжна система – основа соціальної справедливості. ЄЦПС вирівнює людей у правах і можливостях.

Гроші громадян зберігаються на їхніх персональних рахунках у банку ***без відсотків і демерреджу.***

Стає неможливим обвал банку через бажання громадян зняти кошти з банку в панічному порядку.

Банк видає кредити як бізнесу – так і громадянам, згідно з ринковою кон'юнктурою, що, по суті, ***є оподаткуванням за використування суспільного блага –*** грошей.

Через процентні ставки стає можливим регулювати економічний розвиток регіонів. Очевидно, що людські ресурси потягнуться в регіони з дешевшими кредитами на бізнес і споживання.

Система також дає можливість автоматично балансувати товарну масу з грошовою. Для забезпечення «чистоти експерименту» необхідно вивести іноземні валюти з обігу на території держави і використання її, як засіб накопичення. Іноземна валюта може ходити тільки у цифровій версії. Ввіз паперових грошових знаків інших держав на територію України забороняється.

Загалом ЄЦПС вирішує проблему інфляції/дефляції, хабарництва, корупції, нелегального бізнесу, тощо.

Система дозволяє регулювати купівельну спроможність грошей через банківський процент і контроль щоденного споживання як вцілому, так і по галузях. Це, повторююсь, за допомогою ***плаваючого податку на споживання.***

ЄЦПС дає можливі рівномірно розміщувати продуктивні сили на всій території країни і тонко керувати процесами розвитку економіки, інфраструктури і соціального забезпечення.

Гібрид соціалістичної ідеї про державну власність на банківську систему і можливості керованої ринкової економіки в сфері реального сектора – це цивілізаційний вихід з економічного тупика.

ЄЦПС – цемент національної економіки, а здорова економіка запорука розвитку здорової нації. Спільний банк – ЄЦПС, буде об'єднувати всіх громадян. Це і чудова система пенсійного забезпечення. Система вирішує проблему інвестицій.

Висновки

Країна, яка першою перейде на нову систему економічного мислення і першою замінить існуючу економічну модель засновану на лихварському підході до банківництва і приватній власності на банки, отримає очевидні переваги в своєму розвитку на довгу перспективу. Першому завжди важко, але воно цього варте.

Емісія грошей і грошово-банківська система в інформаційному демократичному суспільстві рівних можливостей повинні вийти з під контролю приватних осіб.

Гроші – суспільна цінність (суспільне благо), що по своєму природньому задуму і еволюційному шляху повинні спрощувати економічні стосунки між громадянами.

Народ, і тільки він, як суверен і носій влади в Державі має священне право володіти грошово-банківською системою і контролювати емісію грошей.

Оскільки, в системі соціал-капілалізму головна функція Уряду, на чолі з Прем'єр-міністром, є забезпечення стабільності купівельної спроможності національної валюти – ЄЦПС є інструментом автоматизації цього процесу.

ЄЦПС – цемент національної економіки, а здорова економіка запорука розвитку здорової нації. Спільний банк – ЄЦПС, буде об'єднувати всіх громадян. Це і чудова система пенсійного забезпечення. Система вирішує проблему інвестицій

Саме громадянин України є головним вигодонабувачем від впровадження цієї системи

Шляхи покращення інформаційного забезпечення патрульної поліції України

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

Більше року виповнилось з початку роботи Патрульної поліції в Україні. Зараз в усіх обласних центрах та інших великих містах держави працюють українські копи.

Великі надії покладались і покладаються керівництвом держави та Міністерства внутрішніх справ, всього суспільства, на цю передову, першу реформовану частину правоохоронної системи України. Подальші реформи Міністерства внутрішніх справ спираються на досвід реформування Патрульної поліції.

В цій доповіді ми будемо намагатись проаналізувати інформаційну складову забезпечення діяльності Патрульної поліції України, виявити проблеми та вади систем обміну інформацією, проаналізувати ефективність інформаційних потоків.

На заняття курсантів Дніпропетровського державного університету внутрішніх справ з дисципліни «Застосування комп'ютерних технологій в Національній поліції» запрошуються практичні

працівники підрозділів Національної поліції м. Дніпра, в тому числі патрульні поліцейські. Окрім того викладачі кафедри завітали у місця базування служби «102», диспетчерів патрульної поліції та поспілкувались з поліцейськими, які там працюють. В результаті взаємного обміну інформацією і з'ясувались ті проблемні питання інформаційного забезпечення діяльності патрульної поліції, які потребують вирішення.

Для інформаційного забезпечення патрульної поліції використовується програмний комплекс «Цунамі», який можна розділити на дві основні складові – організаційно-контролюючу та інформаційно-пошукову.

Спочатку проаналізуємо організаційно-контролюючу частину програмного комплексу «Цунамі». Патрульна поліція виконує функції підрозділу швидкого реагування у боротьбі з кримінальними та адміністративними правопорушеннями, вона повинна якнайшвидше прибувати на місце події. Час реагування на подію, як правило, складається з трьох етапів:

- приймання повідомлення у Call центрі (служба «102»);
- обробка диспетчером інформації за карткою «102» та складання завдання для найближчого вільного патруля;
- прийом завдання, прибуття на місце та реагування поліцейськими на подію.

Як показують дослідження у м. Дніпро найбільш проблемною ділянкою у цьому ланцюжку є служба «102». Оператори часто не якісно та повільно збирають первинні відомості щодо події. Це пояснюється відсутність мотивації працівників Call центру, посади яких комплектуються за остаточним принципом, та як правило, з поліцейських, посади яких скорочені.

Окрім того програмне забезпечення Call центру «Цунамі» розроблено для цифрових телефонних станцій, відсутність якої в Управлінні поліції м. Дніпра ГУНП в Дніпропетровській області обмежує можливості оболонки «102» щодо он-лайн інформації про заявника та швидкості оформлення картки «102». Заповнена картка надсилається диспетчеру та черговому відділу поліції за місцем відбування події для занесення у спеціальні обліки.

Диспетчер виконує функції організаційно-інформаційного супроводження діяльності патрульної поліції і є дуже важливим елементом ефективності роботи. Як на нашу думку, необхідно

розширювати інформаційну підтримку патрулів з боку диспетчерів, яким тільки два місяці тому надали доступ до Інтегрованої інформаційно-пошукової системи Національної поліції України.

Можливо необхідні помічники диспетчерів для більш швидкого збирання інформації стосовно встановлених учасників та місця (адреси) відбування зареєстрованої події для подальшого надання патрульному екіпажу цієї інформації ще до його прибуття за цією адресою. Це може значно впливати на тактику поводження патрульних під час реагування на подію, підвищують ефективність їхніх дій та можливо збереже їх життя та здоров'я. Такі експерименти проводяться у Патрульній поліції м. Києва, де на допомогу диспетчеру надаються найбільш підготовлені патрульні поліцейські, що дуже позитивно впливає на швидкість та правильність надання завдань патрулям не за принципом найкоротшої відстані на карті, а за принципом найшвидшого прибуття на місце події. Виникає можливість закріплення за одним патрулем декілька незначних подій у одному районі почергово, що значно оптимізує використання наявних патрулів та пришвидшує час реагування на резонансні події.

Найбільше нарікань, з боку патрульних поліцейських, на мобільну частину комплексу «Цунамі», яка встановлена на планшетах патрульних.

В усіх містах України де працюють патрульні поліції, система «Цунамі» доволі часто дає збій під час реєстрації нової зміни патрульних, яка проходить одночасно у всіх містах і сервера, які фізично розташовані у місті Київ та обслуговують всю Україну, не витримують цього великого потоку одночасної інформації.

Але основні скарги на роботу «Цунамі» у патрульних поліції Дніпра викликає постійно виникаюча відсутність зв'язку з мобільним оператором «Київстар», за допомогою стільникових мереж якого здійснюється обмін між мобільними та стаціонарними частинами комплексу. Це викликано перевантаженістю стільникових мереж оператора «Київстар» у м. Дніпро. Окрім того як вхідна так і вихідна інформація шифрується для захисту засобами мобільного оператора, що призводить до збільшення об'єму інформаційних потоків. Як вихід, пропонується надання переваги (пріоритету) сім-карткам «Київстару», які встановлені в планшети з «Цунамі».

Часто виникали збої на планшетах патрульних під час оформлення звіту про виконані завдання, після яких зникала введена інформація. На теперішній момент проблема зі зникненням введеної інформації вирішена. Але виникає питання вдосконалення системи (ЦУНАМІ) при складанні звіту шляхом реалізації функції «Голосового набору», яка вже давно реалізована в ОС Андроїд.

Патрульні поліцейські піднімали питання нормативно-правової підтримки їхньої діяльності в системі «ЦУНАМІ», яка була частково реалізована розробником і зараз є можливість доступу до необхідних для роботи законодавчих та нормативних актів.

У патрульних поліцейських міста Дніпро виникли проблеми з роботою вбудованого у «ЦУНАМІ» GPS-навігатора, який доволі часто працює дуже некоректно. Для встановлення місцезнаходження адреси події, у наданому диспетчером завданні, вони дуже часто використовують особисті гаджети.

Зазначені проблеми організаційно-контролюючого характеру в роботі мобільної частини комплексу «ЦУНАМІ» у свої більшості пов'язані з технічною підтримкою мобільного оператора «Київстар». Але це доволі часто зводить нанівець можливості вкрай необхідної інформаційно-технічної підтримки патрульних поліцейських, що реалізована в комплексі «ЦУНАМІ». Дане питання можна вирішити тільки на рівні міністерства.

Деякі проблеми виникають і у інформаційно-пошуковій частини комплексу «ЦУНАМІ». В першу чергу патрульні поліцейські скаржаться, як вони кажуть, на «напівпусті» бази даних Інтегрованої інформаційно-пошукової системи Національної поліції України стосовно осіб, речей та транспортних засобів, що знаходяться у розшуку. Достатньо часто, коли запит по «ЦУНАМІ» не дає релузьтату, але «шосте відчуття» поліцейського підказує, що це не так, вони звертаються до диспетчера або працівників Національної поліції, які мають доступ до ІІПС зі стаціонарних робочих місць і отримують позитивні запроси на осіб, які мали багато «стосунків» з правоохоронними підрозділами. Небагато допомагають патрульним і інформаційні обліки власників авто-, мототранспорту, які викладені у неповному обсязі.

Достатньо часто у патрульних поліцейських виникає необхідність наявності фото осіб, які неодноразово попадали в поле зору

правоохоронців, але інформація по яким не міститься в Інтегрованій інформаційно-пошуковій системі Національної поліції. Фототеки даного континенту осіб розміщені у районних відділеннях поліції.

Відсутність можливості розміщення фото потенційних правопорушників, а точніше тих, які не були спіймані «на гарячому», у системі «ЦУНАМІ», замінюється обліком фото, та іншої необхідної службової інформації за допомогою оболонки «Viber» на особистих смартфонах поліцейських. Використання незахищених оболонок може призвести та вже призводило до витоку службової інформації. Тому виникає необхідність розміщення такої фототеки на захищеній мобільній частині комплексу «ЦУНАМІ».

Аналіз зазначених проблем з інформаційним забезпеченням патрульної поліції України та окреслені авторами можливі шляхи вирішення деяких з них, окреслюють напрями вдосконалення існуючого інформаційного комплексу «ЦУНАМІ». Посилення інформаційної підтримки патрульних поліцейських неодмінно буде впливати на якість виконаної ними роботи та поширення позитивного іміджу працівників правоохоронних структур.

Аудит безпеки спеціалізованих інформаційних систем

Руда О.І.,
доцент кафедри економіки та економічної безпеки
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент;
Хміль Ю.Й.,
старший лаборант кафедри інформатики
Львівського державного університету внутрішніх справ
Протиняк Д.А.,
студентка Львівського державного університету
внутрішніх справ

Впроваджуючи інформаційну стратегію при розробленні інформаційних систем (ІС) спеціального призначення вважаємо

за необхідне звернути увагу на теорію та практику інформаційного аудиту, який дає можливість отримати цілісну та об'єктивну картину стану всієї ІС та її окремих елементів, локалізувати притаманні проблеми з метою створення ефективної і оптимальної програми розвитку забезпечення інформаційної безпеки.

В умовах впровадження технології систем з відкритою архітектурою, які вирізняється складною взаємодією ІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (мобільність) питання захисту інформації (ЗІ) набуває все більшої ваги.

На даний момент ще не сформовано усталеного визначення аудиту інформаційної безпеки (ІБ). У подальшому ми пропонуємо під поняттям аудиту ІБ розуміти системний процес вивчення об'єктивних якісних і кількісних оцінок заходів безпеки, процесів доступу, використання інформації, інформаційних ресурсів та потоків, їх зв'язку з персоналом відповідно до визначених критеріїв та показників ІБ, вимог міжнародних стандартів, чинного законодавства України, відомчих нормативно-правових актів.

Результати аудиту ІБ надають керівництву об'єктивну інформацію про стан захищеності ІС. Однак, як показує практика, керівництво і особовий склад найчастіше розуміють суть даного сервісу по-різному.

З огляду на згадані обставини керівництву підрозділів Національної поліції України необхідно взяти до уваги проблеми ІБ у спеціалізованих ІС, ймовірність виникнення яких є обов'язковою у процесі функціонування довільної ІС. Єдиним правильним, з пункту бачення захищеності ІС, рішенням у такій ситуації є аудит ІБ, який проведуть фахівці у галузі ІБ.

Основними цілями проведення робіт з аудиту ІБ є: ідентифікування загроз та виявлення імовірних каналів несанкціонованого витоку інформації у ІС; розроблення політики безпеки [1] та супровідних документів; інвентаризування інформаційних активів ІС та їх подальше категоріювання; розроблення та запровадження системи менеджменту ІБ; забезпечення відповідності прийнятих технічних рішень вимогам чинного законодавства та галузевих норм [2]; незалежне оцінювання поточного стану захищеності інформаційної структури ІС та мінімізування збитків від інцидентів безпеки.

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

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

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

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності ІС з точки зору зловмисника, що володіє високою кваліфікацією в області сучасних інформаційних технологій (ІТ). Найчастіше послугу активного аудиту іменують інструментальним аналізом захищеності ІС, щоб виокремити цей вид аудиту від інших.

Суть активного аудиту полягає у тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи захисту зовнішнього периметру корпоративної мережі спеціалізованої ІС.

При здійсненні даного виду аудиту на систему захисту зовнішнього периметру корпоративної мережі спеціалізованої ІС моделюється якомога більша кількість мережевих атак, які може здійснити зловмисник. При цьому аудитор штучно ставиться саме у такі умови, в яких працює зловмисник, – йому надається мінімум інформації, тільки та, яку можна отримати з відкритих джерел.

Активний аудит умовно можна поділити на два види – «зовнішній» і «внутрішній». При «зовнішньому» активному аудиті фахівці моделюють атаки на зовнішній периметр корпоративної мережі і окремі вузли спеціалізованої ІС «зовнішнього»

зловмисника. У даному випадку проводяться такі процедури: визначення доступних з зовнішніх мереж IP-адрес корпоративної мережі спеціалізованої ІС; сканування даних адрес з метою визначення працюючих сервісів, а також призначення відсканованих хостів; визначення версій сервісів сканованих хостів; вивчення трафіку до хостів корпоративної мережі; збір інформації про систему безпеки ІС з відкритих джерел; аналіз отриманих даних з метою реалізування загроз.

Однак, всупереч поширеним уявленням, загрози зовнішньому периметру мереж не є найбільш критичними для безпеки інформаційних активів ІС. Інсайдерські загрози (загрози, які виходять від своїх же працівників) є на порядок вищими, ніж загрози зовнішні.

«Внутрішній» активний аудит за складом робіт аналогічний до «зовнішнього» і проводиться з використанням спеціальних програмних засобів моделювання загроз від «внутрішнього» зловмисника.

З огляду на специфіку функціонування спеціалізованих ІС у ході активного аудиту необхідно виконувати ряд додаткових досліджень, безпосередньо пов'язаних з оцінюванням стану системи безпеки, зокрема – проведення спеціалізованих досліджень. Це пов’язано з використанням спеціалізованого програмного забезпечення (ПЗ) призначеного для розв’язання спеціальних завдань. Подібне ПЗ унікальне, тому готових засобів і технологій для аналізу їх захищеності не існує.

Експертний аудит можна умовно подати як порівняння стану системи захисту ІС з «ідеальним» описом. Ключовий етап експертного аудиту – аналіз системи захисту ІС, топології корпоративної мережі та технології оброблення інформації, у ході якого виявляються недоліки існуючої системи захисту, які знижують рівень захищеності ІС [3]. За результатами робіт даного етапу пропонуються зміни в існуючій ІС і технології оброблення інформації, спрямовані на усунення виявлених недоліків.

Наступний етап – аналіз інформаційних потоків. На даному етапі визначається критичність інформаційних потоків у ІС та використовуються методи забезпечення ІБ, що відображають рівень захищеності інформаційного потоку.

На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент ІС, які

беруть участь у найбільш важливих процесах трансмісії, зберігання та оброблення даних. Застосування аналізу рівня критичності інформаційних потоків дає можливість реалізувати систему захисту, яка відповідає принципу розумної достатності.

Особлива увага на етапі аналізу інформаційних потоків надається визначенню повноважень і відповідальності конкретних осіб за забезпечення ІБ різних ділянок ІС. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності декларованим цілям і заходам ІБ.

Аудит на відповідність стандартам. При проведенні даного виду аудиту стан системи захисту ІС порівнюється з прийнятим абстрактним описом, який подається у міжнародних стандартах.

Забезпечення ІБ у спеціалізованих ІС – це комплексний процес, що вимагає чіткої організації і дисципліни. Він повинен починатися з визначення ролей і розподілу відповідальності серед посадових осіб, які відповідальні за ІБ. Тому, перший пункт аудиторського обстеження починається, власне, з отримання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. У зв'язку з цим аудитору потрібна документація, що стосується схеми організаційної структури ІС.

Організаційно-правова структура аудиту системи ІБ у ІС формується відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для менеджменту інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційною безпекою.

Офіційний звіт, підготований у результаті проведення даного виду аудиту, включає наступну інформацію: ступінь відповідності ІС обраним стандартам; ступінь відповідності власним внутрішнім вимогам в області ІБ; кількість і категорії отриманих невідповідностей і зауважень; настанови з побудови або модифікування системи ІБ, що дозволяють привести її у відповідність з даним стандартом; докладне посилання на основні документи, включаючи політику інформаційної безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і нормативні документи, які запроваджені у ІС.

Спеціалізовані ІС, які обробляють інформацію з обмеженим доступом, відомості, що становлять державну таємницю, відповідно до чинного законодавства обов’язково підлягають атестуванню за участю органу уповноваженого Кабінетом Міністрів України [4].

Висновки. Аудит безпеки ІС спеціального призначення дозволяє правильно організувати процес захисту інформаційних активів і управління ризиками для цих активів.

Міжнародні стандарти визначають базовий, необхідний набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики. Використання цих стандартів визначає різні набори вимог безпеки в залежності від необхідного рівня захищеності ІС, її приналежності та призначення.

1. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.
2. Рудий Т.В. Управління безпекою в інформаційних системах МВС / Т.В. Рудий, Я.Ф. Кулешник, І.М. Ганич, І.В Бичинюк / Науковий вісник Львівського державного університету внутрішніх справ, №1(47), – Львів. 2011. – С. 382-392.
3. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк. – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.

4. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник, А.Т. Рудий / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. –Львів: ЛДУВС. 2010, – с.90-97.

Захист спеціалізованих комп'ютерних мереж підрозділів Національної поліції України на основі адаптивного підходу

Рудий Т.В.,
професор кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Кулешник Я.Ф.,
доцент кафедри інформатики,
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Піцюра І.С.,
заступник директора Львівського державного коледжу харчової і переробної промисловості НУХТ

Порушення у системі захисту інформаційних активів спеціалізованих комп'ютерних мереж (СКМ) Національної поліції України можуть ставити під загрозу функціонування інформаційних систем (ІС) та успішне виконання оперативних завдань. Ефективність системи захисту СКМ залежить від прийняття виважених рішень які підтримують і адаптують систему захисту інформації до постійно змінюваних умов функціонування мережевого оточення.

Під поняттям спеціалізованої комп'ютерної мережі, у межах даної публікації, будемо розуміти частину ІС у якій забезпечується взаємодія між значною кількістю незалежних компонент, які, у свою чергу, можуть розглядатися як окремі локальні комп'ютерні мережі. СКМ притаманні такі характеристики: територіальна роззосередженість; високий ступінь гетерогенності; використання глобальних зв'язків [1].

Зважаючи на те, що СКМ за колом розв'язуваних задач, складу, архітектурі є системою неоднорідною, тому і система захисту інформації (ЗІ) повинна бути неоднорідною. Неоднорідність системи ЗІ полягає у наявності різних об'єктів захисту і, як наслідок, різних вимог до ЗІ у кожній незалежній складовій. Це є наслідком того, що окремій незалежній складовій СКМ притаманні тільки її критичні інформаційні активи, програмно-апаратні засоби оброблення інформації, моделі загроз і різні політики інформаційної безпеки (ПІБ).

Беручи за основу таке розуміння СКМ забезпечення ЗІ є особливою проблемою. Це обумовлено такими чинниками:

- рівень необхідного захисту від несанкціонованого доступу (НСД) для різних користувачів у різних компонентах СКМ може змінюватися у широкому діапазоні;
- наявність механізмів і засобів ЗІ потенційно вплине на продуктивність функціонування усієї ІС.

Аналіз літературних джерел надає широкий спектр різноманітних методів захисту ІС, які знижують ризики втрати інформаційних активів. Тому, важливим етапом реалізування захисту ІС є вибір ефективного методу захисту конкретної СКМ. Для побудови захищеної СКМ потрібні засоби, які не лише виявляють і блокують атаки, але і попереджують останні.

Автори пропонують використати адаптивний підхід до захисту периметру та інформаційних активів СКМ, який дає можливість контролювати практично усі загрози і своєчасно реагувати на них високоефективним способом, що дозволяє не лише усунути уразливості, які можуть призвести до реалізування загрози, але і аналізувати умови, які призводять до їх виникнення.

Метою даної публікації є обґрунтування ефективності систем ЗІ на основі оцінювання рівня загроз із врахуванням цілей дій зловмисників та аналізу ризиків загроз безпеці інформаційних активів, що забезпечується за допомогою засобів адаптивного управління безпекою СКМ на основі випереджуючої реакції системи ЗІ на реалізування імовірних атак.

При розгляді питань ЗІ в СКМ завжди говорять про наявність деяких бажаних станів усієї ІС. Ці бажані стани описують захищеність ІС. Особливістю поняття захищеність є його тісний зв'язок з поняттям загроза (те, що може бути причиною виведення ІС із захищеного стану).

Отже, виокремимо три компоненти, які безпосередньо пов'язані з порушенням безпеки СКМ: загроза – зовнішнє, відносно СКМ, джерело порушення властивості захищеності; об'єкт атаки – частина СКМ, на яку спрямована загроза; канал дії – середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує усі компоненти, є політика інформаційної безпеки – якісний (або якісно-кількісний) вираз властивостей захищеності СКМ [2]. Опис ПІБ повинен включати або враховувати властивості загроз, об'єкта атаки та каналу реалізування атаки.

Для СКМ існує своя типова архітектура, структурні компоненти якої розв’язують свої специфічні задачі. У загальному випадку архітектура СКМ включає чотири рівні:

- рівень прикладного програмного забезпечення (ППЗ) – рівень взаємодії з користувачем;
- рівень системи управління базами даних (СУБД) та Web-сервери – рівень збереження і оброблення даних у СКМ;
- рівень операційної системи (ОС) – рівень обслуговування СУБД і ППЗ;
- мережевий рівень – рівень взаємодії вузлів СКМ.

Зловмисник має у своєму розпорядженні широкий спектр можливостей порушення інформаційної безпеки (ІБ) СКМ. Ці можливості можуть бути реалізовані на всіх перерахованих вище рівнях СКМ. Найбільш видовищним проявом порушення безпеки СКМ та ІС державної установи є блокування або модифікування вмісту Web-порталу цієї установи.

Розглянемо етапи здійснення атаки на СКМ (рис. 1).

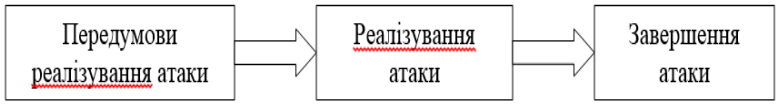


Рис. 1. Етапи реалізування атаки на СКМ

Атакою на СКМ вважається довільна дія, виконувана зловмисником для спроби реалізування загрози шляхом використовування уразливостей. Під уразливістю СКМ розуміється нездатність системи ЗІ протистояти реалізуванню певної загрози або сукупності загроз.

Уразливими є практично всі компоненти СКМ. Серед них відзначимо: мережеві протоколи і пристрої, які формують мережеве оточення; операційні системи; СУБД і Web-сервери.

Отже, саме забезпечення відсутності уразливостей повинно бути покладено в основу формалізування вимог щодо засобів ЗІ.

Перший, підготовчий етап полягає у пошуку зловмисником передумов для здійснення тієї або іншої атаки. На даному етапі зловмисник шукає уразливості в системі захисту. Використовування цих уразливостей здійснюється на другому, основному етапі реалізування атаки. На третій, завершальній стадії, зловмисник завершує атаку і прагне приховати сліди вторгнення. У принципі, перший і третій етапи можуть бути атаками.

У більшості випадків для розв'язання існуючих проблем у системі ЗІ використовуються часткові підходи. Зазвичай, вони обумовлені, перш за все, поточним рівнем доступних ресурсів. До того ж адміністратори безпеки схильні адекватно реагувати тільки на ті ризики ІБ, які їм зрозумілі. Фактично таких ризиків може бути істотно більше. Тільки суворий поточний контроль захищеності СКМ і адаптивний підхід, який забезпечує єдину ПІБ стосовно усієї ІС, дозволяють істотно знизити ризики ІБ.

Такий підхід до системи ЗІ у СКМ прийнято називати моделлю адаптивної мережевої безпеки (Adaptive Network Security Model, ANSM), який здатний контролювати практично усі загрози і своєчасно реагувати на них високоефективним способом, що забезпечує не тільки усунення уразливостей, які можуть привести до реалізування загроз, але і виявлення умов, які обумовлюють появу уразливостей.

Адаптивна компонента моделі ANSM відповідає за модифікування процесу аналізу захищеності, надаючи йому найновішу інформацію про нові загрози. Механізм взаємодії систем аналізу захищеності і виявлення атак моделі ANSM подано на рис. 2.

Слід відзначити, що пропонована модель не відкидає уже використовувані механізми захисту, а розширює їх функціональність за рахунок нових інформаційних технологій (ІТ). Для того, щоб привести систему ЗІ у відповідність до сучасних вимог, необхідно доповнити наявні рішення трьома новими компонентами, які відповідають за аналіз захищеності, виявлення атак і управління інцидентами.

Рис. 2. Взаємодія систем аналізу захищеності і виявлення атак моделі ANSM

Адаптивний підхід до ЗІ дозволяє виявляти, контролювати ризики ІБ і реагувати на них у режимі реального часу, використовуючи правильно спроектовані і добре керовані процеси і засоби. Адаптивні системи захисту орієнтовані на активне протистояння загрозам безпеці. Реалізування такого підходу потребує запровадження системи менеджменту інцидентами інформаційної безпеки (СМІБ), розроблення ПІБ, використання традиційних засобів ЗІ, постійного аудиту ІБ та моніторингу стану системи ЗІ, що має дозволити оперативно реагувати на ризики безпеки [3].

Адаптивна система ЗІ складається з трьох основних елементів:

- технології аналізу захищеності;
- технології виявлення атак;
- технології управління інцидентами ІБ.

Технології аналізу захищеності – це технології пошуку вразливих місць у мережевому оточенні. СКМ складається із з'єднань, вузлів, хостів, робочих станцій (WS), ОС, СУБД і ППЗ. Усі вони потребують як оцінки ефективності їх захисту, так і виявлення невідомих уразливостей. Технології аналізу захищеності є дійовим методом, який дозволяє реалізувати ПІБ у СКМ перш, ніж здійсниться спроба її порушення ззовні або з середини.

Технології аналізу захищеності, за технічним реалізуванням, полягають у виконанні серії тестів з виявлення уразливостей. Ці тести є аналогічними до тих, що використовуються зловмисниками при здійсненні атак на СКМ.

У СКМ доводиться регулярно перевіряти, наскільки реалізовані або використовувані механізми ЗІ відповідають

положенням прийнятої ПІБ. Така задача періодично виникає при зміні і оновленні компонент мережевого оточення, масштабування СКМ, зміні конфігурації ОС тощо. Проте адміністратори безпеки не мають досить часу на проведення подібних перевірок для всіх вузлів СКМ. Тому, використання сканерів безпеки значно полегшить аналіз захищеності використовуваних механізмів забезпечення ЗІ у СКМ.

Засоби аналізу захищеності працюють на першому етапі здійснення атаки. Виявляючи і своєчасно усуваючи уразливості, вони, таким чином, запобігають самій можливості реалізування атаки, що дозволяє знизити витрати на експлуатування засобів ЗІ. Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів, ОС, СУБД і Web-додатків, ППЗ.

Технології виявлення атак є процесом оцінювання підозрілих дій, які відбуваються в СКМ. Виявлення атак реалізується за допомогою аналізу журналів реєстрації ОС і додатків, а також мережевого трафіку у реальному часі. Компоненти виявлення атак, які розміщені на вузлах або сегментах СКМ оцінюють різні події та уразливості.

Технології управління інцидентами ІБ – процес виявлення, аналізу та зменшення ризиків інформаційної безпеки. Завдання управління інцидентами включає в себе створення набору заходів (засобів контролю), які дозволяють знизити рівень ризиків до допустимої величини.

Негативні наслідки широкого кола загроз (починаючи від атак хакерів і закінчуючи діями інсайдерів, які використовують свої знання і права доступу до даних СКМ для своєї вигоди) можна зменшити, використовуючи підхід до управління інцидентами інформаційної безпеки, описаний у новому міжнародному стандарті ISO/IEC 27035:2011 [4].

Стандарт ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки» надає практичні рекомендації з виявлення, реєстрування і оцінювання випадків порушення ІБ і реалізування загроз.

Він допоможе реагувати на інциденти ІБ, зокрема, вводити відповідні інструменти контролю для їхнього запобігання, а також відновлення, і, таким чином, набувати досвіду та покращувати загальний підхід.

Інтегрування СМІБ дає ряд переваг:

- підвищення загального рівня ІБ;
- зменшення негативних наслідків реалізування загроз;
- посилення акценту на попередження інцидентів ІБ;
- призначення пріоритетів і збору даних;
- внесок в обґрунтування рішень щодо бюджету та ресурсів;
- поліпшення якості оцінювання та управління інцидентами ІБ;
- надання додаткової інформації для розроблення ПІБ та супутньої документації.

Організація процесу управління інцидентами ІБ дозволить виявити і мінімізувати інформаційні ризики, а також: гарантувати ЗІ в агресивному динамічному середовищі ризиків; оптимізувати витрати на реалізування системи ЗІ; забезпечить визначеність у тому, наскільки потрібно захищати інформаційні активи; забезпечить визначеність у тому, як краще досягти прийнятного рівня ІБ, і який рівень можна вважати прийнятним; керівництво зможе приймати правильні стратегічні рішення, беручи до уваги інформацію про актуальні ризики; інтегрування функцій безпеки в усі аспекти управління ІС [5].

Висновки. Розв'язання проблем безпеки СКМ вимагає застосування адаптивного механізму, що працює у режимі реального часу і володіє високою чутливістю до змін в інформаційній інфраструктурі. Ефективність функціонування СКМ залежить від прийняття обґрунтованих рішень з захисту, які адаптовуються до постійно змінюваних умов мережевого оточення.

Адаптивний підхід до безпеки СКМ дає можливість пристосовуватися до зовнішніх змін середовища функціонування компенсовуючи небажані впливи, дозволяючи системі оптимізувати свою роботу відповідно до встановлених критеріїв, і, навіть, змінити ціль функціонування, якщо цього вимагають нові умови.

---

1. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.

2. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.
3. Герасимчук О.І. Комплексні системи санкціонованого доступу: навч. посіб. / О.І. Герасимчук, В.Б. Дудикевич, В.А. Ромака. – Львів: Видавництво Львівської політехніки, 2010. – 212 с.
4. Електронний ресурс - http:www.iso.org
5. Рудий Т.В. Система управління інформаційною безпекою в інформаційних системах підрозділів МВС на засадах політики безпеки / Т.В. Рудий, О.І. Зачек, О.В. Захарова / Боротьба з Інтернет-злочинністю. Матеріали міжнародної науково-практичної конференції (м. Донецьк, 12-13 червня 2013 року). – Донецьк: Донецький юридичний інститут, 2013. – С. 228-231.

Використання міжнародних стандартів у системі захисту інформаційних систем підрозділів Національної поліції України

Рудий Т.В.,
професор кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Сеник С.В.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ справ
Ізьо М.І.,
студентка Львівського державного університету
внутрішніх справ

В умовах сучасної повномасштабної інформаційної і кібервійни, яка ведеться проти нашої країни, забезпечення безпеки інформаційних систем (ІС) підрозділів Національної поліції (НП) України має стати державним завданням. Особливої уваги вимагає захист критичних активів, а також централізованих баз даних.

Порушення безпеки ІС може істотно ускладнити виконання завдань оперативними підрозділами, тому проблема створення ефективної системи захисту інформації (ЗІ) набуває дуже важливого значення. Автори вважають, що така система ЗІ повинна бути, у першу чергу, комплексною і адаптивною.

З розвитком інформаційних технологій (ІТ) і систем ЗІ виникла необхідність уніфікувати вимоги до їх проектування та забезпечити достатній рівень стандартизації. Одним з найважливіших підсумків цієї роботи є адаптування міжнародного стандарту серії ISO/IEC 27000.

Проблемам створення і функціонування систем ЗІ присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування систем ЗІ є суттєві недоліки, які знижують ефективність їх функціонування. Необхідно обґрунтувати розроблення організаційно-правових засад ЗІ, які визначать стратегію, тактику системи ЗІ, а також враховує динаміку зміни загроз інформаційним активам ІС.

Однак, у законодавстві України немає посилань на міжнародні стандарти, які надають більш широкий спектр послуг та профілів захищеності.

Дотримання принципів стандартів серії ISO 27000 забезпечує керування і контроль доступом, розроблення та обслуговування апаратно-програмних комплексів, керування безперервністю інформаційних процесів. Відповідність вимогам стандартів серії ISO 27000 і дотримання національних правових норм з інформаційної безпеки є запорукою створення ефективної системи ЗІ.

Мета даної публікації полягає у тому, щоб окреслити організаційно-правову структуру системи ЗІ у ІС підрозділів НП України. Разом з тим, відзначимо, що це є всього лише однин з аспектів стратегії системи управління інформаційними технологіями у підрозділах НП України.

Правову основу ЗІ у ІС підрозділів НП України становлять: Конституція України; Закони України; акти Президента України та Кабінету Міністрів України; нормативно-правові акти Служби безпеки України; Державної служби спеціального зв'язку та

захисту інформації України, інших державних органів; міжнародні угоди України, згода на обов'язковість яких надана Верховною Радою України. Видано низку відомчих актів Державною службою спеціального зв'язку та захисту інформації України (ДССЗТЗІ) – циркулярних листів, тлумачень, методик тощо, які є обов'язковими для усіх державних органів, підприємств, установ, організацій під час здійснення ними функцій щодо забезпечення захисту службової інформації, перш за все – державної таємниці.

Регулятивно-правову основу забезпечення ЗІ у ІС підрозділів НП України становлять: Конституція України; Концепція національної безпеки України; Закони України «Про інформацію», «Про науково-технічну інформацію», «Про державну таємницю», «Про національний архівний фонд та архівні установи», «Про зв'язок», «Про видавничу справу», «Про доступ до публічної інформації», «Про захист персональних даних».

В Україні розроблено серію нормативних документів системи технічного захисту інформації, основним з яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу». Цей документ використовується при проектуванні та створенні комплексних систем захисту інформації (КСЗІ) державних інформаційних ресурсів, а також систем, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої визначено законом.

Однак, довільна використовувана при проектуванні КСЗІ методологія повинна бути сумісною з основними сучасними стандартами на системи управління, такими як ISO/IEC серії 27000.

Тому, організаційно-правова структура системи ЗІ в ІС підрозділів НП України повинна формуватися відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002: 2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004: 2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки;

ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційною безпекою [1, 2, 3, 4, 5].

У світовій практиці паралельно з розвитком ТСЗІ розвивався напрямок стандартизації у частині менеджменту інформаційної безпеки. Результатом стало затвердження міжнародного стандарту ISO/IEC 27001:2005, а пізніше ISO/IEC 27001:2013. Впровадження системи менеджменту інформаційною безпекою (СМІБ). Стандарт дозволяє правильно організувати процес захисту інформаційних активів і управління ризиками для цих активів. Для контролю якості процесу менеджменту інформаційної безпеки було запроваджено інститут сертифікування. Сертифікат має міжнародний статус.

Неможливо обійти увагою новий стандарт ISO/IEC 27035: 2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки» [6], який надає практичні рекомендації з виявлення, реєстрування і оцінювання випадків порушення інформаційної безпеки.

Він допоможе реагувати на інциденти інформаційної безпеки, зокрема, вводити відповідні інструменти контролю для їхнього запобігання та відновлення у випадку реалізування загроз, покращувати загальний підхід до проектування технічних систем захисту інформації.

Інтегрування системи управління інцидентами інформаційної безпеки у КСЗІ дає ряд переваг:

- підвищення загального рівня інформаційної безпеки;
- зменшення негативних наслідків реалізування загроз;
- посилення акценту на попередження інцидентів інформаційної безпеки;
- призначення пріоритетів і збору даних;
- внесок в обґрунтування рішень щодо формування бюджету та ресурсів;
- надання додаткової інформації для розроблення політики інформаційної безпеки та супутньої документації.

В Україні тільки перша версія ISO/IEC 27001:2005 частково отримала статус державного стандарту. Питання його практично-

го застосування залишається актуальним. Стандарт з урахуванням галузевих особливостей є обов'язковим у банківській сфері – СОУ Н НБУ 65.1 СУІБ 1.0: 2010.

Отже, замовник своїми силами або із залученням підрядників розробляє технічне завдання (ТЗ) на КСЗІ, погоджує його з ДССЗТЗІ, а потім, на підставі ТЗ проектує, реалізовує КСЗІ за допомогою сукупності організаційних, програмно-апаратних та інженерних засобів і вводить в дослідну експлуатацію. Далі, на підставі отриманої заявки ДССЗТЗІ визначає компанію-ліцензіата, яка виступає організатором державної експертизи КСЗІ. Організатор експертизи, володіє штатом кваліфікованих експертів, розробляє програму та методику експертних випробувань, проводить їх і подає результати своєї роботи у вигляді проекту експертного висновку на розгляд експертної ради з питань технічного захисту інформації ДССЗТЗІ. У разі позитивного рішення КСЗІ отримує атестат відповідності вимогам системи технічного захисту інформації (ТЗІ).

Наявна правова колізія, коли міжнародні стандарти ISO/IEC серії 27000 в Україні не адаптовані, а критерії захищеності 1999 року є давно застарілими (технології ЗІ, на відміну від чинного законодавства, інтенсивно розвивалися) має тенденцію до загострення за найгіршим сценарієм.

Існуючій системі проектування КСЗІ притаманний і ряд інших недоліків. Так, для ІС з різною архітектурою, різними вимогами щодо забезпечення ЗІ, що ґрунтуються, в тому числі, і на різних категоріях доступу до інформації, існують стандартні функціональні профілі захищеності, тобто деякі фіксовані набори послуг безпеки. У той же час, розробник КСЗІ при формуванні ТЗ самостійно визначає об'єкти захисту, на які ці послуги поширюються. Експерти з ДССЗТЗІ, в процесі узгодження ТЗ, перевіряють специфікації послуг, однак складно визначити рівень адекватності висунутих вимог до умов функціонування існуючих ІС.

Наступний етап контролю за відповідністю ТЗ створеній КСЗІ – експертиза. Зазвичай, експертиза полягає лише у перевірці якості реалізації заявлених послуг безпеки в ІС та комплектність документації на КСЗІ. Практично ніколи експертами якість впровадженої КСЗІ не перевіряється тестуванням на несанкціонований доступ (НСД) до активів ІС. По-перше, цього не вимагає

нормативно-правова база, а по-друге для проведення таких робіт потрібен високий фаховий рівень експертів [7].

Недостатнє бюджетне фінансування при закупівлі відповідних програмно-технічних засобів захисту накладає поважні обмеження на технічну складову КСЗІ в ІС підрозділів НП України.

Фахівці можуть розробити та запровадити ідеальний варіант КСЗІ, відповідні служби та експерти виконають усі необхідні експертизи та заходи з атестування, а відсутність кваліфікованих фахівців зведе нанівець усі попередні зусилля. Для забезпечення якісного функціонування КСЗІ необхідно терміново переглянути посадові оклади працівникам Служби захисту інформації, щоб залучити потрібних фахівців.

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих загроз щодо порушення роботи ІС, тобто загроз, які підвищують уразливість інформації, призводять до її витоку, випадкового або навмисного компрометування, знищення. Розглядаючи загальні принципи ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС має у своїй основі використання організаційних та програмно-апаратних засобів ЗІ. Такі засоби повинні забезпечувати ідентифікування та автентифікування користувачів, розподіл повноважень доступу до активів ІС, реєстрацію та облік спроб несанкціонованого доступу [8].

Висновки. На підставі проведеного аналізу автори вважають, що існуюча нормативно-правова база, яка крім іншого не окреслює вимог до розроблення політики інформаційної безпеки та оцінювання ризиків в ІС, повинна бути істотно доповненою. Для цього необхідно або адаптувати стандарти ISO/IEC серії 27000, що дасть можливість легально брати участь у державному або приватному сертифікуванні систем ЗІ, або – розроблення власних, якісно нових стандартів безпеки для державних силових структур.

Міжнародні стандарти ISO/IEC серії 27000 на відміну від нормативних документів в Україні, об’єктом захисту передбачають процес оброблення, доступу та збереження інформації, а не КСЗІ.

1. Міжнародний стандарт ISO/IEC 27001 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

2. Міжнародний стандарт ISO/IEC 27002 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
3. Міжнародний стандарт ISO/IEC 27003-27004 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
4. Міжнародний стандарт ISO/IEC 27005 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
5. Міжнародний стандарт ISO/IEC 27006 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
6. Міжнародний стандарт ISO/IEC 27035 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
7. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (12 березня 2010 р.). – Львів: Львівський державний університет внутрішніх справ, 2010. – С. 90-97.
8. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.

Опрацювання зображень для виявлення і попередження злочинності

Смичок В.Д.,
начальник відділу аерологічних спостережень Львівського регіонального центру з гідрометеорології ДСНС, кандидат технічних наук, доцент
Хомин О.Й.,
професор кафедри соціальних дисциплін Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

Анотація. В публікації проведено оглядове дослідження технічних систем і способів виявлення і розпізнавання зображень. Основну увагу акцентовано на розпізнавання подій по просторово-часовій і смисловій структурі у режимі реального часу [1]. В

основу публікації покладені сучасні програмні і технічні засоби розпізнавання, які використовують математичні алгоритми штучного інтелекту (AI).

Проблеми розпізнавання образу людини, предмета при попередженні злочинності.

При проведенні оперативно-пошукових заходів Національна поліція не завжди має можливість отримати якісне зображення порушника. Часто трапляється так, що найнебезпечніший правопорушник є людиною досвідченою, а навіть такою, що знає методи технічного відеоспостереження, розташування камер спостережень та їх технічні характеристики і можливості. При цьому, досвідчені порушники, як провило, при скоєнні злочину закривають лице. В такій ситуації слідчим важко проводити пошук злочинця лише по деяких зовнішніх ознаках (рис.1.а.б.).

Однак, як бачимо із кадрів, що наведені на рис.1. в оперативній обстановці, що склалася злочин «добре підготовлений». Про це свідчить поведінка злочинців. Вони знають про те, що камери відеоспостереження в безпосередній близькості відсутні, тому більш якісні кадри їх зовнішності за допомогою зумів отримати не вдасться. Тому для працівників поліції вкрай необхідно оперувати іншими характеристиками розпізнавання, використовуючи комп'ютерне моделювання, розпізнавання образів засобами AI.

Хоча розпізнавання по поведінці не мають доказової бази для слідчих, але вони можуть суттєво звузити коло підозрюваних та вказати на особливості характеру та поведінки злочинців.

Рис.1.а.б. Документальні кадри з камер спостереження підготовки злочину.

Структура програми підготовки персоналу, для засобів розпізнавання.

Основною складовою структури програмного забезпечення є «База даних дій особи». В статті, для прикладу, розглядаємо базу даних, що складається з відео-файлів, що включає шість видів людських дій. А саме: ходьба, біг підтюпцем, біг-ривок, швидкий біг, бокс, розмахування рукою, виконаних в декілька разів (25-ма) особами в чотирьох різних сценаріях:

S1 – на вулиці,

S2 – на відкритому повітрі з масштабом варіації,

S3 – на відкритому повітрі в різному одязі;

S4 – в приміщенні.

В даному прикладі база даних містить 2391 різних послідовностей дій. Всі послідовності були записані на однорідному фоні за допомогою статичної камери з частотою 25 кадрів/сек. Послідовності з субдескретизації використовувались з просторовою роздільною здатністю у 160x120 пікселів. Запис тривав в середньому від однієї до чотирьох секунд.

У наших експериментах з програмою – ICPR'04 [2, 3] використовуються всі послідовності дії осіб, які брали участь в експериментах. Ми розглядаємо три групи, до яких відносимо 1). 8 осіб, яких вчили певних дій (класифікатори); 2). 8 осіб, у яких були певні навички виконувати потрібні дії; 3). 9 осіб, яких проводили тестування-випробування програмного забезпечення. Учасники – класифікатори пройшли навчання під час навчального набору в той час як набір перевірки був використаний для оптимізації параметрів кожного методу. Результати розпізнавання були отримані під час проведення тестування-випробування програмного забезпечення.

Область розпізнавання дій людини тісно пов'язана з іншими напрямки досліджень. Представлене нами відео дозволяє проаналізувати рух людини враховуючи лише їй притаманні ознаки як її ходьба, так і особливості її поведінки. При проведені розслідування підходи до розпізнавання дій людини, також її мотивації і поведінка, як правило, аналізуються і обговорюються в обмеженому колі. Дані про особу аналізують, також аналізується і бачення її поведінки. Останні викристалізовуються на основі оперативної інформації та літератури.

Поставлена авторами мета статті обмежується баченням аналізу розпізнавання дій осіб на основі декількох підходів. Так, нами розглядаються питання розпізнавання на різних рівнях, що ілюструється рис. 2.

Рис.2. Спрощена загальна структура методики програмного розпізнавання

Вхід відео зображення розбивається на безліч функцій, які приймають вигляд індивідуальних кадрів. До розрахунку беруться руки, які розглядають ізольовано. Так, на приклад, беруть співвідношення рук, людська рука, напрямки руху для класифікації команд, управління рухом, жест, зовнішній вигляд. Методичний підхід, використовує особливості зображення для моделювання.

Для прикладу, зовнішній вигляд людської руки порівнюється з її параметрами, взятими, з особливостями зображення відео входу.

Також приділяється увага на дослідженням сегментації виявлення активності частин тіла та визнання їх діяльності.

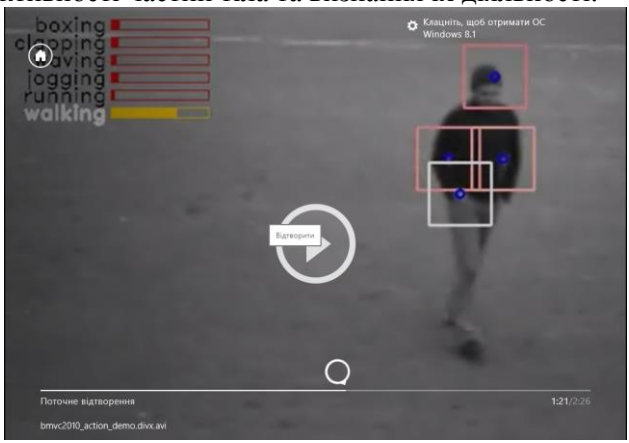


Рис. 3. Програми визначила його як пішохода, що має виражну жестикуляціюцію (у %) з навиками боксера

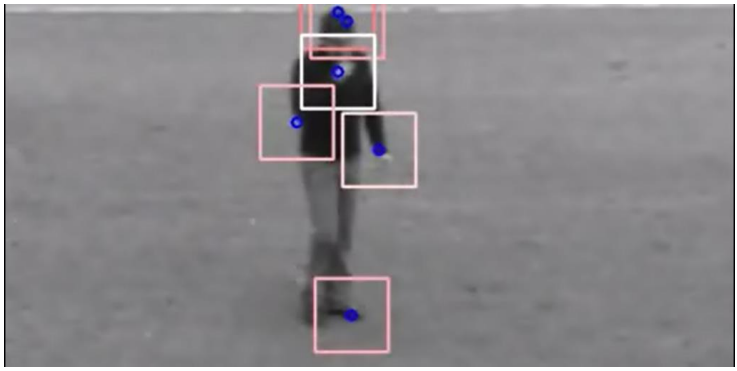


Рис.4. Приклад розпізнавання неякісних кадрів програмою bmvc2010_action_demo.divx

Програма визначила сегментацію, виявила активності частин тіла та визначила рід їх діяльності (рис.4). Це дозволяє визначити причетність даної особи до скоєння злочину.

Висновок. Відповідно до поставлених завдань авторами проводились дослідження оптимізації систем розпізнавання по поведінці людини, виключаючи при цьому особливості розпізнавання лиця людини. В результаті проведеного аналізу декількох програмних пакетів, які використовуються поліцейськими підрозділами зарубіжних країн, для попередження і виявлення злочинності, автори дослідження, розглядають просторово-часові структури алгоритмів розпізнавання. Згідно яких розпізнавання вектора руху людини відбувається алгоритмами штучного інтелекту, що реалізуються за допомогою декількох пакетів програмного забезпечення з використанням – A.I. Tech: People Tracking, Multiple People Tracking, People detection and tracking multiple cameras, Real-time Action Reco –gnition by Spatiotemporal Semantic and Structural Forests та ін.

1. Хомин О.Й. Міжнародний досвід забезпечення безпеки населення в сфері контролю за застосуванням вогнепальної зброї» // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі. Збірник наукових статей за матеріалами доповідей учасників науково-практичної конференції 17 грудня 2015 р. – Львів: Льв.ДУВС, 2015. – 243 с.,С. 186-190.

2. «Recognizing Human Actions: A Local SVM Approach», Christian Schuldt, Ivan Laptev and Barbara Caputo; in Proc. ICPR'04, Cambridge, UK.
3. «Local Descriptors for Spatio-Temporal Recognition», Ivan Laptev and Tony Lindeberg; ECCV Workshop «Spatial Coherence for Visual Motion Analysis».

Шляхи підвищення ефективності захисту комерційної таємниці як об'єкту економічної безпеки підприємства

Субота І.І.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ

Діяльності підприємств здійснюється в умовах існування великої кількості загроз. Їх можна поділити на три групи:

- фізичні та моральні впливи особистого спрямування (спрямовані проти конкретної особистості);
- негативні дії, спрямовані на завдання шкоди майну, включаючи загрози зменшення активів підприємства (організації) і втрати ним (нею) фінансової незалежності;
- негативний вплив на інформаційне середовище суб'єкта господарювання.

Серед них мають й місце загрози пов'язанні з втратою підприємством комерційної таємниці, що у кінцевому випадку це обертається для нього великими збитками.

Різноманітне їх походження зумовлює необхідність побудови комплексних систем захисту бізнесу, які б включали заходи організаційного, правового, економічного, ідеологічного, соціального характеру та ін. Функціонування цих систем забезпечується через діяльність як спеціалізованих підрозділів безпеки, так і всіх інших підрозділів і працівників підприємства. Ефективність таких систем значною мірою залежатиме від уміння персоналу кожної комерційної структури розпізнавати загрози їхній діяльності, активно протистояти їм, забезпечувати грамотну і безпечну поведінку в умовах реалізації таких загроз.

Захист комерційної таємниці як інформаційної складової економічної безпеки можна здійснювати шляхом реалізація заходів з розробки та охорони. Алгоритм такої діяльності наведено рис. 1.

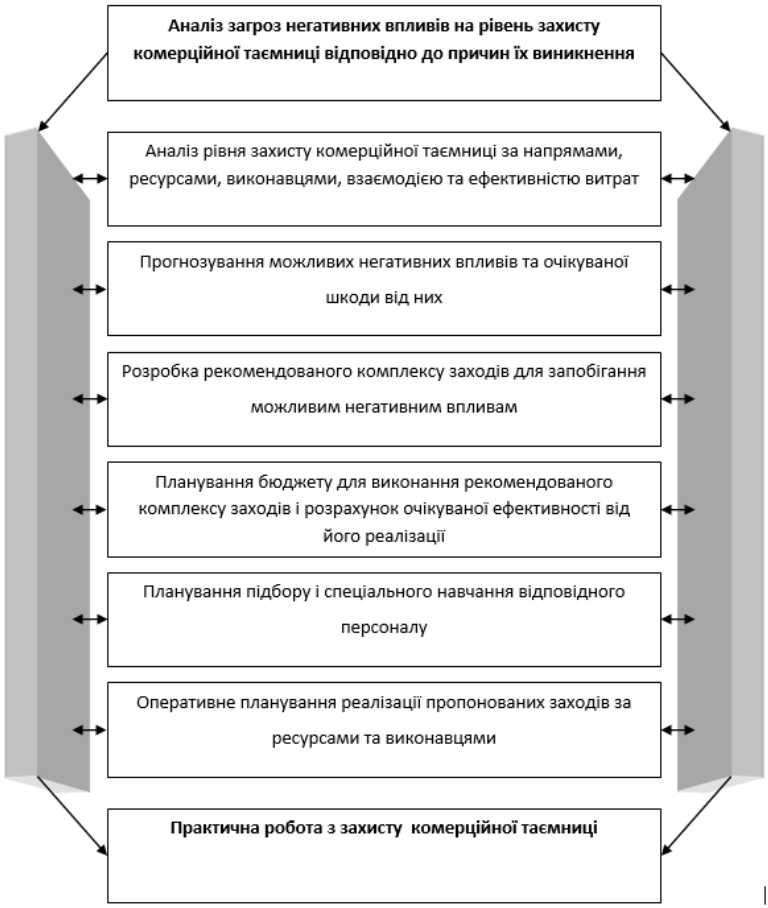


Рис.1. Принципова загальна схема посилення захисту комерційної таємниці

На кожному підприємстві при створенні системи захисту інформації необхідно правильно організувати:

- облік і охорону деяких видів матеріалів і готових виробів (особливо дослідних зразків)

- порядок діловодства з документами, що містять підприємницьку таємницю (правила циркуляції, обліку, зберігання, знищення і ін.)
- контроль за засобами копіювання і розмноження документів
- захист комерційної інформації в засобах зв'язку і обчислювальної техніки
- охорону території підприємства і його основних будівель і споруд
- контроль за відвідинами даного підприємства сторонніми особами.

Питання щодо інформаційного забезпечення в системі МВС України

Фірман І.В.,
головний фахівець Департаменту формування політики щодо підконтрольних Міністрові органів влади та моніторингу

Сучасний стан застосування інформаційних технологій та наявності великої кількості інформаційних потоків у різних сферах діяльності, зумовлює правоохоронні органи інтенсивно впроваджувати нові інформаційні системи, орієнтовані на системно-інформаційний аналіз.

Забезпечення на сучасному етапі безперебійної та сталої життєдіяльності держави, її виконавчих органів в умовах стрімкого зростання інформаційних потоків, накопичення і збереження надвеликих обсягів інформації в базах даних, суттєве збільшення інформаційного навантаження на системи опрацювання і систематизації інформації, обміну інформацією між підконтрольними службами і департаментами міністру, потребує якісно підготовлених служб і фахівців, спроможних забезпечувати замовників необхідною та актуальною інформацією. Необхідними і достатніми умовами, щодо формування належного інформаційного забезпечення системи МВС для виконання покладених на неї обов'язків, є створення системи правових, організаційно-техніч-

них та соціально-економічних заходів на основі чинного законодавства України, а саме Конституція України, Цивільного кодексу, законів України «Про інформацію», «Про мови», «Про державну таємницю», «Про науково-технічну інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про захист інформації в автоматизованих системах», «Про зв'язок», «Про національний архівний фонд і архівні установи» та інші.

На жаль, в державі, дослідженням питань інформаційного забезпечення діяльності, для вирішення комплексних завдань, поставлених перед МВС України в цілому, не приділялося достатньої уваги. Існуючі державні служби, як правило «замикалися» у межах своїх повноважень, діяли обособлено.

У зв'язку з реформуванням МВС України, постала потреба вдосконалення системи інформаційного обміну та забезпечення інформацією підконтрольні Міністрові органи влади та моніторингу. Зокрема, дуже важливим є інтегрування баз даних Національної поліції, Державної прикордонної служби України, Державної служби України з надзвичайних ситуацій, Державної міграційної служби України, Національної гвардії України.

Серед низки завдань системи інформаційного забезпечення є здійснення інформаційної підтримки правоохоронних органів у розкритті та попередженні злочинів, установленні й розшуку злочинців, а також надання статистики, аналітичної та довідкової інформації.

Інформаційно-технічне забезпечення і середовище будь якої служби вкрай неоднорідне. Воно відображає, як регіональну, так і галузеву специфіку, накопичену технічну базу і стан науково-технічного потенціалу. Все це визначає кількісні та якісні характеристики, ступінь їх впливу і участі у міжгалузевому обміні знаннями, інформацією, можливостями реалізації інноваційних стратегій та інформаційного обслуговування.

Інформаційне забезпечення, як поняття, визначається комплексом накопиченої інформації з різних інформаційних потоків, їх вірогідністю, що впливає на вибір ефективних і оптимальних варіантів дій. За результатом системно-інформаційного аналізу приймаються управлінські рішення.

Таким чином, в умовах реформування всієї системи державних органів в Україні та формування оновленої системи правоохоронних органів, необхідність змін відношення до сутності

інформаційного забезпечення Міністерства внутрішніх справ, є ефективним способом забезпечення боротьби зі злочинністю, захистом прав і свобод громадян, а також суспільства в цілому.

Сучасні реалії та загрози інформаційній безпеці в діяльності юридичної особи

Хитра О. Л.,
доцент кафедри адміністративного права та адміністративного процесу Львівського державного університету внутрішніх справ, кандидат юридичних наук

Створення ефективної системи інформаційної безпеки юридичної особи є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією.

Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарата.

Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності.

Фахівці встановлюють, в середньому, наступне співвідношення зовнішніх і внутрішніх загроз: 82% загроз створюються співробітниками фірми або за їх прямої або опосередкованої участі; 17% загроз виникає ззовні – зовнішні загрози; 1% загроз створюється випадковими особами [1].

Основними загрозами інформації є її розголошення, витік і несанкціонований доступ до її джерел.

З урахуванням викладеного залишається розглянути питання, які умови сприяють неправомірному оволодінню конфіденційною інформацією. В літературі вказуються наступні умови:

- розголошення (зайва балакучість співробітників) – 32%;
- відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14%;

- несанкціонований доступ шляхом підкупу і схиляння до співробітництва з боку конкурентів і злочинних угруповань – 24%;
- традиційний обмін виробничим досвідом – 12%;
- безконтрольне використання інформаційних систем – 10%;
- наявність передумов виникнення серед співробітників конфліктних ситуацій – 8% [1].

Розголошення комерційних секретів, мабуть, найбільш розповсюджена дія юридичної особи (джерела), що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витратах зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічних засобів.

Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать:

- ділові зустрічі, наради, переговори та інші форми спілкування;
- обмін офіційними діловими, науковими і технічними документами засобами передачі офіційної інформації (пошта, телефон, телеграф, факс тощо.)

Неформальними каналами поширення інформації є:

- особисте спілкування (зустрічі, переписка, телефонні переговори тощо.);
- виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи;
- засоби масової інформації (преса, інтерв'ю, радіо, телебачення тощо).

Як правило, причиною розголошення конфіденційної інформації є:

- слабке знання (або незнання) вимог захисту конфіденційної інформації;
- помилковість дій персоналу через низьку виробничу кваліфікацію;
- відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій;

- злісне, навмисне невиконання вимог захисту комерційної таємниці.

Наведена нижче таблиця дає уявлення про фактори, що сприяють розголошенню комерційних секретів [1].

№	ФАКТОРИ	%
1.	Зайва балакучість співробітників	32
2.	Прагнення співробітників заробляти гроші будь-якими способами і за будь-яку ціну	24
3.	Відсутність на фірмі служби безпеки	14
4.	«Радянські» звички співробітників фірми ділитися один з одним (тобто традиційний обмін досвідом)	12
5.	Безконтрольне використання інформаційних систем	10
6.	Наявність передумов для виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів.	8

Витік інформації загалом можна розглядати як неправомірний вихід конфіденційної інформації за межі організації або кола осіб, яким ця інформація була довірена.

Витік інформації за своєю суттю завжди припускає протиправне (таємне або явне, усвідомлене або випадкове) оволодіння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

Причини витоку інформації полягають, як правило, у недосконалості норм щодо збереження комерційних секретів, порушенні цих норм, а також відступі від правил поводження з відповідними документами, технічними засобами, зразками продукції та іншими матеріалами, що містять конфіденційну інформацію.

Умови включають різні фактори і обставини, що складаються в процесі наукової, виробничої, рекламної, видавничої, звітної, інформаційної та іншої діяльності юридичної особи і створюють передумови для витоку комерційних секретів. До таких факторів і обставин можуть, наприклад, відноситися:

- недостатнє знання працівниками підприємства правил захисту комерційної таємниці і нерозуміння (або непорозуміння) необхідності їх ретельного дотримання;

- використання не атестованих технічних засобів обробки конфіденційної інформації;
- слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та інженерно-технічними заходами;
- плинність кадрів, у тому числі які володіють інформацією, що становить комерційну таємницю.

Таким чином, значна частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникають через недбалість керівників підприємств та їхніх співробітників.

Несанкціонований доступ (НД) можна визначити як сукупність прийомів і порядок дій з метою одержання (добування) охоронюваних даних протиправним шляхом.

До таких способів відносяться:

1. Таємне спостереження.
2. Підкуп службовця конкуруючої фірми або особи, що займається її постачанням.
3. Використання агента для одержання інформації.
4. Перехоплення телеграфних повідомлень.
5. Підслуховування телефонних переговорів.
6. Крадіжки креслень, зразків, документів тощо.
7. Шпигунство і вимагання.

До інших способів несанкціонованого доступу до інформації, які не порушують норм закону, але знаходяться на грані такої ситуації, можна віднести:

- Співбесіди про найм на роботу зі службовцями конкуруючих фірм (хоча опитувач зовсім не має наміру приймати дану людини на роботу).
- Так звані «помилкові» переговори з фірмою-конкурентом щодо придбання ліцензії, створення спільного підприємства, підписання партнерської угоди.
- Найм на роботу службовця конкуруючої фірми для одержання необхідної інформації.
- Працевлаштування «свого» працівника на підприємство-конкурента.

У закордонних матеріалах наводяться окремі показники співвідношення способів несанкціонованого доступу, зокрема:

№	Спосіб НД	%
1.	Підкуп, шантаж, переманювання службовців, впровадження агентів	43
2.	Підслуховування телефонних розмов	5
3.	Крадіжка документів	10
4.	Проникнення в ПЕОМ	18
5.	Знімання інформації з каналів зв'язку	24

Аналіз наведених даних показує, що значна частина дій (2, 4, 5) реалізуються в кримінальній практиці за допомогою використання тих або інших технічних засобів і складають загалом 47% від загального їхнього числа. Це зайвий раз підтверджує небезпеку технічних способів добування інформації в практиці здійснення підприємницької діяльності [2].

Таким чином, створення системи інформаційної безпеки юридичної особи є масштабною роботою, яка вимагає серйозних зусиль. Тому фахівці радять, насамперед, найбільш точно визначити загрози, які існують для інформаційної безпеки підприємства, і не вживати додаткових заходів забезпечення безпеки, якщо це реально не відобразиться на підвищенні росту його діяльності.

1. Об'єднання професіоналів конкурентної розвідки Росії // Офіційний сайт. Режим доступу: www.rscip.ru
2. Антирейдерский союз предпринимателей Украины Консультационный центр «Корпоративная безопасность предприятия (фирмы)» – «Коммерческая тайна. Секрет Полишинеля или тайна за семью печатями. (зарубежный опыт)» – Курс лекций – Библиотека Антирейдера. – Режим доступу: file:///C:/Users/Acer/Downloads/Nzlubp_2011_7_57.pdf.

Алгоритм процесу оцінювання рівня економічної безпеки підприємства

Чередніченко А.О.,

здобувач освітнього ступення «магістр»

Львівського державного університету внутрішніх справ

Для оцінювання стану та визначення рівня економічної безпеки виникає необхідність у розробці відповідного алгоритму.

Його основний зміст наведено на рис.

Першим етапом є затвердження підприємством методичних рекомендацій щодо оцінювання рівня економічної безпеки. На цьому ж етапі визначається відповідальна за оцінювання особа з відділу економічної безпеки і встановлюється механізм залучення окремих осіб з інших підрозділів підприємства (бухгалтерії, юридичного відділу, відділу кадрів, виробничих підрозділів).

На другому етапі відбувається збирання інформації, необхідної для розрахунку показників, що характеризують кожну складову економічної безпеки підприємства.

Джерелами інформації повинні слугувати: нормативні акти, первинні та зведені документи підприємства, матеріали ревізій, аудиту, перевірок податкової служби, відомості про контрагентів, матеріали маркетингових досліджень тощо. Аналіз зібраної інформації проводиться на третьому етапі та включає обробку даних, отриманих з різних джерел, перевірку наявності усієї необхідної інформації, порівняння показників. На наступному етапі визначаються кількісні та якісні показники, які систематизовано за кожною складовою економічної безпеки підприємства. Далі здійснюється визначення комплексного показника рівня економічної безпеки, який розраховується за допомогою сумування рівнів усіх складових, помножених на коефіцієнт їхньої вагомості.

Якщо максимального рівня економічної безпеки не досягнуто, тоді необхідно встановити відхилення за кожною складовою, а також виявити чинники внутрішнього та зовнішнього середовищ, які негативно вплинули на зниження рівня. Після оцінки відхилень відділ економічної безпеки підприємства розробляє конкретні дії та надає рекомендації щодо підвищення рівня економічної безпеки.

У процесі розроблення і реалізації цих заходів необхідно здійснювати аналіз їхньої оптимальності для підприємства. Після закінчення кожного етапу працівник відділу економічної безпеки складає звіт про отримані результати проведеної роботи та подає його попередньо визначеним особам. Тому, якщо реалізовані заходи не принесли позитивного результату, тоді, враховуючи зауваження, отримані в результаті опрацювання звітів, та надані

рекомендації, необхідно розробити подальші дії для встановлення причин відхилення від максимального рівня економічної безпеки.

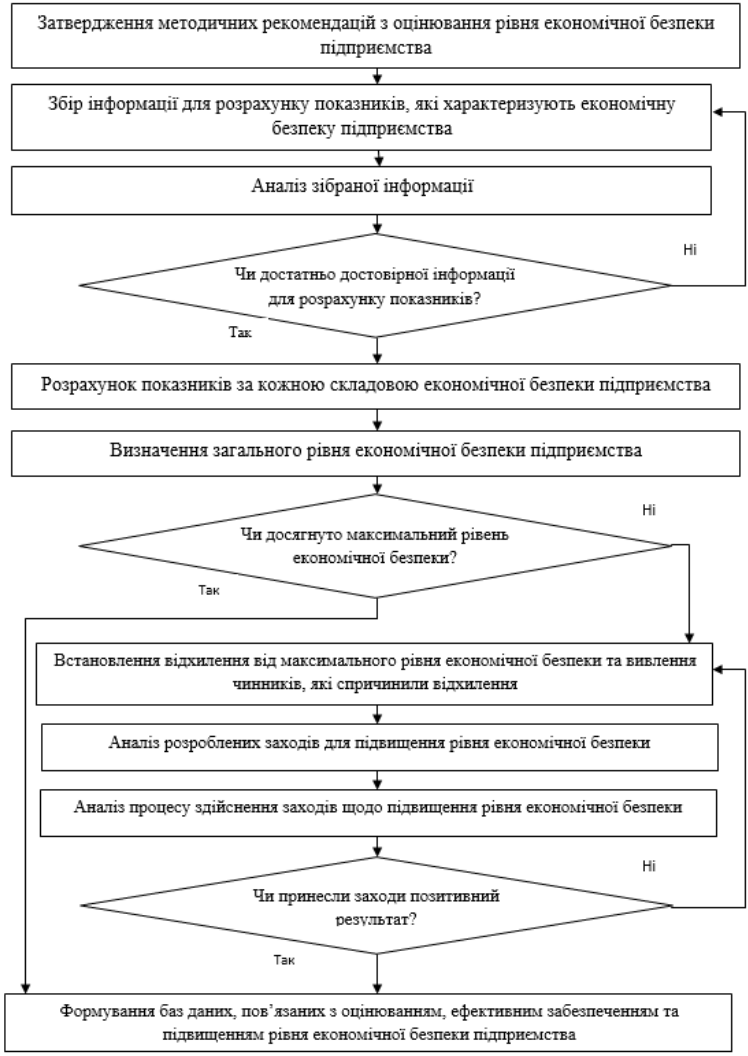


Рис. Алгоритм процесу оцінювання рівня економічної безпеки підприємства

Дотримуючись запропонованих етапів алгоритму оцінювання рівня економічної безпеки підприємства, можна оперативно встановити причину її низького рівня та розробити конкретні дії щодо її зміцнення.

Інформація як важливий чинник адміністративно-правового забезпечення безпеки суб'єктів господарювання

Чистоклетов Л.Г.,
професор кафедри адміністративно-правових дисциплін,
Львівського державного університету внутрішніх справ,
доктор юридичних наук, професор
Шишко В.Й.,
старший викладач кафедри інформатики Львівського
державного університету внутрішніх справ

На сьогодні інформація у сфері адміністративно-правового забезпечення безпеки суб'єктів господарювання набуває особливої актуальності, що підтверджується інтенсивним насиченням всіх сфер її життєдіяльності інформаційними продуктами та комп'ютерно-телекомунікаційними технологіями. Виходячи з цього, можна стверджувати, що цим тенденціям повинні слідувати усі ієрархічні рівні управління як державою в цілому, так і окремими суб'єктами господарювання. Ефективна та якісна система інформаційно-аналітичного забезпечення в сфері адміністративно-правового забезпечення безпеки господарювання є невід'ємною складовою професійного функціонування її системи управління. Впровадження та всебічне використання сучасних інформаційних технологій в управлінській діяльності забезпечує інформаційно-аналітичну підтримку прийняття стратегічних управлінських рішень на всіх рівнях, супроводжує інформаційну підтримку фінансово-економічного розвитку суб'єктів господарювання, забезпечує інформаційні потреби топ менеджерів, створює умови для формування позитивної громадсь-кої думки щодо їх діяльності, а також послуг, які ними надаються.

Слід зазначити, що обсяги інформації у світі постійно зростають. Якщо ще в 80-х роках XX ст. її обсяги кожні десять років подвоювалися, то на сучасному етапі вони подвоюються щороку. Все це спонукало людство широко застосовувати технічні засоби для збирання, обробки та зберігання інформації, а канали зв'язку — для її передачі [1, с. 16].

Інформаційний вплив на державу, суспільство, громадянина зараз є ефективнішим, ніж політичний, економічний і навіть військовий. Інформація стає реальною, майже фізично відчутною силою [2].

Відображаючи реальну дійсність, інформація інтегрується в усі напрямки діяльності держави, суспільства, громадянина. З появою нових інформаційних технологій, основою яких є впровадження засобів обчислювальної техніки, зв'язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, громадських організації та громадян. Від її якості та достовірності, оперативності одержання залежать численні рішення, що приймаються на різних рівнях – від глави держави до громадянина [3, с. 31].

Термін «інформація» не має точного й однозначного визначення, як і ряд інших, наприклад, «час», який людство багатогранно використовує для обліку, нормування, планування тощо. У перекладі з латинської мови «інформація» (informatio) – інформування, повідомлення про будь-що, про будь-який факт, явище тощо, роз'яснення чого-небудь [4]. А взагалі інформація – це сукупність різноманітних знань, сигналів, відомостей про фактичні та інші процеси і явища, що їх певна система сприймає (збирає, зберігає, обробляє) від навколишнього середовища (вхідна інформація), видає в навколишнє середовище – систему (вихідна інформація) або зберігає її в собі (внутрішня інформація) і використовує для визначених цілей, в тому числі і для менеджменту [1, с. 63].

Поняття інформації неодноразово змінювалось, його межі то розширювалися, то звужувалися. Спочатку під цим словом розуміли «уявлення», «поняття», згодом – «відомості», «передачу повідомлень». Вперше термін «інформація» знайшов своє відображення у математичній теорії інформатики і теорії передачі даних каналами зв'язку Клода Шеннона (1948), у якій він під

«інформацією» розумів усі види повідомлень. К. Шеннон разом з У.Уівером запропонували імовірні методи для визначення кількості інформації, що передається. Однак такі методи описують лише знакову структуру інформації, не торкаючись її змісту [3, с. 55].

Після того, як Н. Вінер запропонував «інформаційне бачення» кібернетики як науки про управління в живих організмах та технічних системах, під інформацією почали розуміти вже не будь-які відомості, а лише ті, які є новими та корисними для прийняття такого рішення, що забезпечить досягнення мети управління. Інші відомості не вважались інформацією.

У свою чергу Л.М. Беккер, як і Н. Вінер, підкреслює у цьому понятті ознаку впорядкованості і зазначає: «інформація може бути охарактеризована як збереження і відновлення її носієм упорядкованості станів і її джерела, яке впливає на цього носія» [5, с. 44].

Узагальнюючи думки різних вчених, М. Демкова та М. Фігель виділяють дві концепції інформації. Прихильники першої концепції зробили спробу співвіднести інформацію з поняттям «відображення», розкриваючи у той же час необхідність єдності відображення й взаємодії як діалектичної єдності полярних категорій. Друга концепція інформації, на думку багатьох вчених, є більш плідним підходом до вирішення проблеми інформації, – «різноманітна» концентрація інформації. Також підкреслюється, що «інформація існує там, де є розмаїття, неоднорідність. Інформація «виявляється» тоді, коли хоча б два «елементи» у сукупності різняться, і вона «зникає», якщо об’єкти «склеюються», «ототожнюються» [3, с. 72].

Інформаційно-аналітичне забезпечення є базою, на якій будується безпека суб’єктів господарювання. З цієї точки зору А.О. Дєгтяр розглядає інформацію як певну сукупність різних повідомлень, зведень, даних про відповідні предмети, явища, процеси, відносини, які будучи зібраними, систематизованими і перетвореними на придатну для використання форму, відіграють у процесі прийняття й реалізації управлінських рішень виняткову роль [6, с. 91].

Серед ознак, які характеризують інформацію в управлінських структурах як наукову категорію, виділено відому самостійність даних; можливість їхнього багаторазового використання, збереження у передавача чи отримувача, придатність до оброблення,

інтеграції та ущільнення за рахунок вилучення дублюючої, надлишкової інформації; припустимість математичного аналізу; системність і комунікативність. Крім наведених, ознаками інформації як джерела державно-управлінських рішень слід вважати:

- нематеріальний характер (самостійність відносно носія, тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона зафіксована);
- суб‘єктивний характер (інформація виникає в результаті діяльності суб‘єкта, який наділений свідомістю, тобто вона є результатом інтелектуальної діяльності);
- кількісна визначеність;
- здатність до відтворення, копіювання, збереження і накопичення.

Інформацію, яка використовується в управлінні інформаційно-аналітичним забезпеченням безпеки суб’єктів господарювання, можна класифікувати за різними напрямками та ознаками. На підставі результатів систематизації поглядів різних вчених, можна запропонувати поділ інформації на:

- вхідну і вихідну;
- внутрішню і зовнішню;
- офіційну і неофіційну;
- загальну і галузеву;
- горизонтальну і вертикальну;
- інформацію про минуле, сьогодення й майбутнє;
- інформацію, призначену для керівника суб’єкта управління та для інших посадових осіб;
- усну, електронну, подану на паперових носіях;
- універсальну та спеціалізовану.

Інформація для прийняття управлінських рішень має відповідати критеріям актуальності, своєчасності, повноти, цінності, точності, доступності, адекватності для прийняття відповідних управлінських рішень.

Таким чином, саме інформаційно-аналітичні системи адміністративно-правового забезпечення суб’єктів господарювання можуть бути основою для формування їх інформаційних ресурсів як системи. Для цього потрібне вирішення складних організа-

ційно-технічних питань, пов'язаних із забезпеченням скоординованого формування та ведення інформаційних ресурсів всієї діяльності господарюючих суб'єктів.

1. Твердохліб М. Г. Інформаційне забезпечення менеджменту: Навч. посібник / М.Г. Твердохліб. — [Вид. 2-ге, доп. та перероб.]. — К.: КНЕУ, 2006. — 224 с.
2. Черешкин Д.С. Оружие, которое может быть опаснее ядерного / Д.С. Черешкин // Независимая газета. – 2007. – № 123.
3. Демкова М. Інформація як основа інформаційного суспільства: визначення поняття та правове регулювання / М. Демкова, М. Фігель // Інформаційне Суспільство. Шлях України. – К. : Фонд «Інформаційне суспільство України», 2004. – 422 с.
4. Юридична енциклопедія: В 6 т. // Редкол.: Ю.С.Шемшученко (голова редкол.) та ін. – К. : Укр. енцикл., 1998. – С. 717.
5. Беккер Л.М. Воспитание и основы его моделирования / Л.М. Беккер. – М. – 286 с.
6. Дєгтяр А.О. Державно-управлінські рішення: інформаційно-аналітичне та організаційне забезпечення: [Моногр.] / А.О. Дєгтяр. – Х.: Вид-во ХарРІ НАДУ «Магістр». – 2006. – 224 с.

Кіберзлочинність у фінансовій сфері України

Шаєвська Ю.В.,
курсант Одеського державного університету внутрішніх справ
Ісмайлов К.Ю.,
завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук

Останнім часом проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів та постійно зростають. Серед найбільш вразливих до кіберзлочинів сфер суспільного життя відноситься фінансовий сектор економіки, а саме – банки та їх послуги [1].

Кіберзлочинність – це п'ятий за розмірами вид економічної злочинності в України після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю.

За результатами опитування на кіберзлочинність припадає 23% випадків шахрайства у світі і 17% в Україні (рис.1).

Рис. 1

З статичних даних ми бачимо, що у відсотновому співвідношенні рівень кіберзлочинності у світі вищий ніж в Україні. Це явище пояснюється тим, що фінансова сфера, яка досить часто потопає від кібератак, в Україні менш розвинена ніж у всьому світі, тому звідси й нищі показники. І це зовсім не з причин якісної організації протидія кіберзлочинцям.

Розглянемо причини розповсюдження кіберзлочинності:

- по-перше, зазначена сфера злочинна діяльності є дуже прибутковою та стає в один ряд з такими незаконними сферами діяльності, як незаконний обіг наркотиків, зброї та торгівля людьми;
- по-друге, фінансові установи скривають від правоохоронних органів більшість фактів кібератак на свої установи, піклуючись про свою репутацію серед клієнтів;
- по-третє, за умови незначних фінансових втрат, фінансові установи не проводять навіть внутрішніх розслідувань з огляду на те, що людські, фінансові та інші затрати на таке їх проведення значно перевищують втрати;
- по-четверте, злочини скоїться у віртуальному середовищі, тобто є дуже латентними.

Так, за оцінками експертів, в останні місяці тільки в м. Києві фіксується до двадцяти випадків крадіжки грошей через клієнт-банк в місяць. Суми становлять від 20 тис. до 40 млн. грн. Однак

подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам не вигідний галас навколо того, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків [2].

На сьогодні кіберзлочинність – це реальна глобальна загроза, яка може походити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних видів економічних злочинів.

Серед усіх сфер суспільного життя найбільш вразливою до шахрайства є фінансово-кредитна сфера, особливо у міжнародних економічних відносин.

Останнім часом найбільшого поширення набули такі види злочинів як кіберзлочинність в фінансово-банківській сфері, шахрайство з використанням платіжних карток та їх реквізитами, крадіжки коштів з банківських рахунків, «відмивання» грошей, заволодіння конфіденційною комп'ютерною інформацією про клієнтів тощо.

Кібернетична злочинність все більше посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. Чинниками, які сприяють зростанню кіберзлочинів є розвиток та удосконалення ІТ-технологій, значна географія для скоєння злочинів, недостатня теоретична та практична підготовка працівників органів внутрішніх структур та недосконаліть вітчизняного законодавства [3].

Так, в опитуванні представлені погляди представників понад 13 різних галузей. Фінансові послуги, роздрібна торгівля, виробництво споживчих товарів, промислове виробництво та професійні послуги представляють понад половину (63%) від загальної кількості учасників в Україні та світі. Кожен другий респондент, що працює у секторі фінансових послуг, енергетики та гірничо-видобувної промисловості за останні 12 місяців зіштовхнувся із випадками кіберзлочинів (рис.2) [4].

Дослідження проблем боротьби з кіберзлочинністю показали, що використання тільки технічного захисту інформації не має значного успіху.

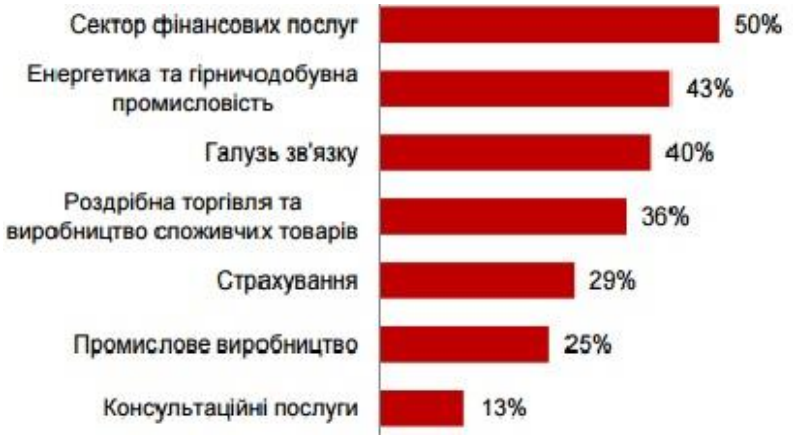


Рис.2

Кіберзлочинність є порівняно новою небезпекою для суспільства, але, на відміну від традиційних крадіжок і шахрайства, вона удосконалюється разом з технологіями, що ускладнює її виявлення та протидію, що унеможливлює складення єдиної методики та тактики розслідування зазначених злочинів.

За офіційними даними, більшість респондентів, які зіткнулися з економічною кіберзлочинність злочинністю за останні 12 місяців, оцінюють збитки до 5 млн. доларів США.

Найдорожчими для організацій виявилася маніпуляції з фінансовою звітністю (рис. 3)

Рис. 3

Кібернетична злочинність все більше посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв.

Наведемо кількість шахрайських операцій із використанням платіжних карток, емітованих українськими банками в 2010 – 2015 роках у вигляді діаграми (рис. 4)

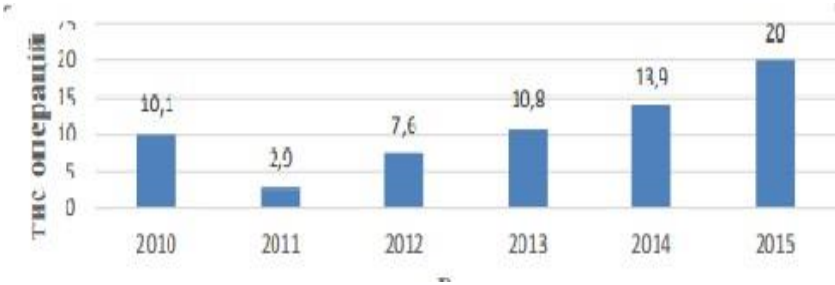


Рис. 4

Основні висновки щодо стану кіберзлочинності в Україні:

- кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні;
- кожен третій респондент (37%) вважає, що ризик кіберзлочинності підвищився за останні 12 місяців;
- понад 25% організацій не мають відповідних політик та механізмів реагування на кіберзлочини;
- 46% опитаних не проходили навчання в області кібербезпеки протягом останніх 12 місяців;
- 58% респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингу відвідування соціальних мереж.

В Україні способами протидії кіберзлочинності можуть виступати: вдосконалення норм і прав боротьби з кіберзлочинністю, чітке розмежування компетенції та функцій правоохоронних органів. Також одним із способів протидії кіберзлочинності може бути покращення практичного досвіду працівників підрозділів кіберполіції України, поліпшення методичного забезпечення розслідування кіберзлочинів, налагодження співпраці зі службою безпеки банків та підприємств, судовою системою.

1. Чекотовська О. Правове регулювання кіберзлочинності. – [Електронний ресурс] / Ольга Чекотовська. – Режим доступу: http://ukrjustice.com.ua.
2. Кіберзлочинність в Україні. – [Електроннийресурс] – Режим доступу: http://www.science-community.org
3. Некрасов В. Экономическая правда / Всеволод Некрасов. Легкие деньги: Украина превращается в Мекку для киберпреступников . – Киев : Летопись, 2016. – Т. 2 : Д–Й. – С.34.
4. Дуброва Н.П., Сучасгтц стан фінансової системи України в глобалізаційному процесі // Фінансове право - 2015р. – №1(9) - с.114-115.
5. Коротких Я.В. Економічна безпека в умовах глобалізації // «Розвиток фінансової системи України». – 2016р. – с.211-212.

Розділ 2.
ПРОБЛЕМИ ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА ПРОГРАМНО-ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПОЛІЦІЇ

Забезпечення захисту конфіденційної інформації при використанні засобів зв'язку в діяльності органів Національної поліції

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

При проведенні правоохоронними органами, в тому числі органами Національної поліції заходів спрямованих на протидію злочинності, не завжди виникає можливість передати або отримати оперативну інформацію відкритими засобами (каналами) зв'язку, а сучасні шифрувальні засоби своїм виглядом можуть демаскувати їх в очах оточуючих, серед яких може бути і зацікавлена особа. У деяких ситуаціях виникає необхідність виходити на зв'язок з будь-яких засобів зв'язку, і як наслідок з'являються сумніви щодо конфіденційності проведених телефонних розмов, що спричиняє труднощі у роботі або й більш серйозні наслідки пов'язані з витоком конфіденційної інформації [1].

Сучасні інформаційні технології інтенсивно впроваджуються в усі сфери життя і діяльності суспільства, до такої міри, що національна безпека держави починає бути залежною від забезпечення інформаційної безпеки.

Володіння інформацією в різних формах її прояву є важливою перевагою. З цієї причини проблема її захисту від втрат різними способами є досить актуальною [2, с. 481].

Одним з основних джерел загроз інформаційної безпеки є використання пристроїв технічної розвідки, тому питання аналізу джерел витоку інформації по технічних каналах, та методи їх захисту є назрілою задачею. До таких каналів можна віднести існуючі технічні засоби передачі інформації та допоміжні технічні засоби й системи (мережа електроживлення, пожежна сигналізація, заземлення, металеві труби систем опалення, водопостачання й інші струмопровідні металоконструкції), що проходять через приміщення контрольованої зони, і виходять за її межі й доступ до яких отримати не складно.

Так, конфіденційна інформація дуже часто передається по телефонних комунікаціях, що пов'язано з оперативністю і зручністю використання цього виду зв'язку. Використання для передачі інформації засобів стільникового зв'язку, комп'ютерних мереж, Інтернету, апаратів дротового зв'язку наразі залишаються незмінними атрибутами правоохоронних органів. Слід відзначити, що такі засоби зв'язку відносяться до розряду найменш захищених. І справа не лише в можливості несанкціонованого прослуховування телефонних розмов у режимі реального часу, їхнього запису чи ретрансляції, а й у використанні абонентської телефонної лінії (АТЛ) для встановлення телефонних закладок, прослухуванні приміщень у режимі покладеної телефонної трубки, а також використання мережі автоматичних телефонних станцій (АТС) для живлення засобів технічної розвідки чи передачі по них інформації за межі контрольованих приміщень.

Тому методи запобігання та протидії поширенню конфіденційної інформації каналами зв'язку можна класифікувати наступним чином:

- обмеження фізичного доступу до каналів телефонного зв'язку;
- встановлення запобіжних засобів протидії витоку мовної інформації (технічні засоби просторового зашумлення, пристрої віброакустичного захисту, технічні засоби ультразвукового захисту, засоби створення електромагнітних маскуючих перешкод);

- контроль та виявлення несанкціонованих під'єднань до АТЛ, яка перебуває у робочому стані;
- усунення чи виведення з ладу встановлених телефонних закладок;
- впровадження криптографічних методів захисту конфіденційної інформації, що передається засобами комунікації;
- розробка нових та вдосконаленні існуючих засобів та способів захисту інформації.

Одними із найдосконаліших способів захисту даних, що передається каналами зв'язку, є використання криптографічних алгоритмів шифрування мовної інформації. Такий спосіб буде вимагати від абонентів, що спілкуються, наявності однакових пристроїв кодування-декодування сигналу – скремблерів, які забезпечують повну конфіденційність переговорів [3].

Скремблювання, як відомо, оборотне перетворення цифрового потоку без зміни швидкості передачі з метою отримання властивостей випадкової послідовності [4].

Наприклад, дві найбільші телефонні компанії «Vodafone» і «Cellnet Securicor's (O2)» створили розгалужені мережі цифрових мобільних телефонів, підключених до глобальної системи мобільних комунікацій (ГСМ), що охоплює 40 країн. Кожен цифровий мобільний телефонний апарат забезпечений власним «обертовим» кодом, що зашифровує кожну окрему розмову.

Кодування розмови відбувається за допомогою мікро-ЕОМ, вмонтованої в слухавку, і як наслідок мовний (аналоговий) сигнал перетворюється у цифровий, котрий передається по мережі. Мова в цьому випадку піддається частотній інверсії. В свою чергу звуковий сигнал, займаючи ту ж саму частоту лінії зв'язку, стає нерозбірливим для несанкціонованого абонента [5]. Кодування відбувається щоразу по-новому, тому важко розшифровується.

Скремблерування також підвищує надійність синхронізації пристроїв, підключених до лінії зв'язку (забезпечує надійне виділення тактової частоти безпосередньо з прийнятого сигналу), і зменшує рівень перешкод, випромінюваних на сусідні лінії багатожильного кабелю [4].

Ще одним способом захисту мовної інформації є новація компанії T-Systems, яка пропонує мобільний додаток Mobile Encryption App який можна легко встановити на будь-який

смартфон. Додаток генерує індивідуальний ключ кожен раз, коли він використовується кодуючи розмову або повідомлення. Телефонні дзвінки здійснюються через IP (Internet Protocol) з пропускною здатністю 4,8 кбіт/с.

IP-телефонія є одним із пріоритетних напрямків розвитку телефонного зв'язку. З кожним роком кількість абонентів, які використовують IP-телефонію для проведення голосових переговорів VoIP (Voice Internet Protocal), збільшується. Це пов'язано, насамперед, з меншою вартістю передачі даних за допомогою мережі Інтернет.

Але IP-телефонія має ряд значних відмінностей від телефонної мережі загального користування, які роблять її особливо вразливою до зовнішнього втручання і утруднюють застосування існуючих підходів до захисту голосової інформації в мережі Інтернет.

На відміну від класичної телефонії, де використовується комутація каналів, IP-телефонія базується на мережевих протоколах з комутацією пакетів. У процесі передачі даних по IP-мережі вони проходять через певну кількість недостатньо захищених серверів, до того ж з'єднаних між собою незахищеними каналами. Одночасно IP-телефонія певним чином відрізняється і від звичайної передачі даних IP-мережами. Це пов'язано з необхідністю виконання аналого-цифрових перетворень даних в реальному часі. Зважаючи на необхідність дотримання вимог щодо якості зв'язку, такі перетворення, включаючи стискання, шифрування та ін., повинні відбуватися за мінімально короткий час. Існуючі системи IP-телефонії реалізують недостатньо високий рівень захисту інформації та використовують відносно нестійкі криптографічні алгоритми або алгоритми, надійність і якість яких не доведена.

Важливим питанням залишається розповсюдження ключів. Але на даному етапі, при відсутності нормативно закріпленої структури обміну відкритих ключів, найкращий рівень конфіденційності можливий при умові безпечного постачання ключів обом сторонам при використанні симетричного алгоритму шифрування.

Таким чином, захист інформації в VoIP потребує проведення подальших досліджень, у тому числі удосконалення вже існуючих систем шляхом використання додаткових засобів захисту, які б дозволили підвищити надійність існуючих методів шифрування, або розроблення нових методів та схем захисту з урахуванням потреб сьогодення [6].

Провівши аналіз існуючих методів та пристроїв кодування аналогової інформації і враховуючи специфіку роботи оперативних підрозділів органів Національної поліції, завданням яких є боротьба зі злочинністю, нами розроблено шифрувальний пристрій для шифрування розмов по стаціонарному телефонному апарату та телефонну гарнітуру для шифрування розмов по стільниковому телефоні.

Поставлена задача вирішується наступним чином. В аналогово-цифровому перетворювачі відбувається перетворення аудіосигналу, прийнятого з мікрофона телефонного апарату чи гарнітури, в цифрову форму, який дальше шифрується в шифраторі, після чого перетворюється з цифрової форми в аналогову в цифро-аналоговому перетворювачі і надходить на штекер, який підключається до телефонного апарата (стаціонарного чи мобільного). Вхідний сигнал з аудіовиходу телефону через штекер надходить на вхід аналогово-цифрового перетворювача телефонного каналу, в цифровій формі дешифрується в дешифраторі, перетворюється в аналоговий у цифро-аналоговому перетворювачі і поступає на телефон слухавки чи стільникової гарнітури. Обидва канали шифрувального пристрою працюють без змін фізичних параметрів лінії зв'язку.

Використання шифрувального пристрою дозволяє проводити конфіденційні телефонні переговори, використовуючи довільні існуючі телефонні апарати і лінії зв'язку без використання можливостей IP-телефонії, що сприяє зменшенню ризиків втрати інформації.

При роботі з шифрувальним пристроєм виявити додаткове шифрування практично неможливо через те, що шифрування і дешифрування відбувається на кінцевих стадіях формування аудіосигналу і ніякі електричні, фізичні і цифрові параметри ліній зв'язку при цьому не змінюються. Єдиним джерелом інформації про те, що телефонна розмова відбувається, є з'єднання між абонентами, але її зміст зашифрований і ніяким чином не зрозумілий. Обов'яз-ковою умовою для роботи з шифрувальною гарнітурою та шифрувальним телефонним апаратом є ідентичність комплектів шифрувального пристрою і ключів шифрування абонентів на лінії зв'язку [7, 8].

Таким чином, запропонований принципово новий спосіб захисту аудіо інформації. Простий у користуванні, та зручний шифрувальний пристрій у будь який момент може слугувати

надійним спецзасобом в роботі органів Національної поліції та інших підрозділів які ведуть боротьбу зі злочинністю, а інформацію отриману в такий спосіб можна використати в оперативній роботі не переживаючи про її витік.

1. Дмитрик Ю.І. Використання пристрою шифрування аудіоінформації в оперативній роботі // Науковий вісник Львівського державного університету внутрішніх справ. 1’2009. Спеціальний випуск / Ю.І. Дмитрик, В.Д. Смичок. – Львів: ЛьвДУВС, 2009. – С. 78–87
2. Зачек О.І. Розробка гарнітури для шифрування розмов по стільниковому телефону / Діяльність підрозділів кримінальної міліції: сучасний стан та перспективи вдосконалення // Матеріали міжнародної науково-практичної конференції (12 квітня 2013 р.) / О.І. Зачек, Ю.І. Дмитрик – Львів: ЛьвДУВС, 2013. – С. 481–485
3. Цибуляк Б.З. Захист інформації від витоку каналами телефонного зв’язку [Ел. ресурс]. – Режим доступу: http://ubgd.lviv.ua/moodle/
4. Скремблер [Ел. ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/
5. Економічна безпека підприємства [Електронний ресурс]. – Режим доступу: http://subject.com.ua/economic/safety/54.html
6. Литвинов В.В. Сучасний стан захисту інформації в ір-телефонії // Математичні машини і системи / В.В. Литвинов, В.В. Казимир, Є.В. Риндич. – 2009, № 2. – С. 76-84
7. Патент України на корисну модель № 71446 «Шифрувальна телефонна гарнітура», виданий згідно заявки №u201200477 від 16.01.12 р.
8. Патент України на корисну модель № 82310 «Шифрувальний телефонний апарат», виданий згідно заявки №u201302307 від 21.02.13 р.

Політика якості щодо діяльності криміналістичних лабораторій Республіки Польща

Дуфенюк О.М.,

доцент кафедри криміналістики, судової медицини та психіатрії Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Актуальність окресленої тематики обумовлена кількома чинниками. По-перше, прагнення гармонізувати українське законодавство з європейськими стандартами, підвищити ефективність

функціонування правоохоронних органів, модернізувати матеріальне та організаційно-технічне забезпечення мотивують до пошуку позитивного досвіду провадження реформ у цих сферах, зокрема в Польщі. По-друге, важливість обговорення стандартів якості інноваційного забезпечення криміналістичних лабораторій викликана тим, що висновок експерта у кримінальному провадженні як і в українському, так і в польському кримінальному процесі, має особливе значення, хоча у відповідних процесуальних кодексах двох країн такої норми немає.

Такий кшталт вищевказаного джерела доказу обумовлений необхідністю застосувати спеціальні знання, що по суті означає, що тільки експерт, який володіє такими знаннями, дає спеціалізовану оцінку фактам, подіям, об'єктам та явищам, і з допомогою певних технологій отримує такі дані, які неможливо отримати в жодний інший спосіб жодному іншому учаснику кримінального провадження. На цьому ґрунтується власне ситуація, згідно з якою у практиці польського кримінального судочинства висновок експерта часом трактується як «коронний доказ», що означає, що у разі якихось сумнівів щодо справи чи вини обвинуваченого суд чи прокурори перекладають тягар відповідальності за прийняте процесуальне рішення на експерта [1, с. 26]. Більше того, у деяких країнах така ситуація не просто допустима, а навпаки – вітається. Наприклад, у шведській системі права окремі експерти мають на стільки широку компетенцію (аж до участі у складі суду, який розглядає приймає рішення у справі), що дає підстави правникам називати їх «суддями фактів» [2, с. 58].

Отже, забезпечення максимальної якості компетенції польських експертів-криміналістів, за словами М. Грегоровіч реалізується з допомогою двох механізмів:

- внутрішній, який пов'язаний із процесом здобуття працівниками криміналістичних лабораторій повноважень надавати самостійно висновки;
- зовнішній, який стосується підтвердження рівня формулювання висновків лабораторіями на підставі міжнародних стандартів [3, с. 23].

Слушно зазначають польські фахівці, для того щоб видати висновок експерта у багатьох галузях криміналістики, потрібно

володіти новітніми апаратними комплексами та опанувати дослідницькі методики. До прикладу для проведення ДНК експертизи необхідна наявність такого обладнання лабораторії, що має високий рівень захисту від контамінації (випадкової зміни, забруднення дослідницького біологічного матеріалу), відповідає сучасним вимогам та має доступ до загальної системи бази ДНК. Схожа ситуація з хімічними, токсикологічними, дактилоскопічними, механоскопійними, трасологічними та іншими криміналістичними дослідженнями. Сучасна наука і техніка впроваджує сучасне обладнання, що збільшує можливості дослідження, а разом з тим і можливості доказування у судовому провадженні [4, с.47]. Саме тому питання якості технічної оснащеності криміналістичних лабораторій потребує особливої уваги.

З огляду на сказане, Центральна Криміналістична Лабораторія Поліції Республіки Польща *(Centralny Laboratorium Kryminalistyczny Policji*) (далі – ЦКЛП) оформила основні засади політики якості у вигляді окремого документу, який фактично відіграє роль своєрідної конституції, методологічної основи функціонування системи криміналістичних лабораторій [5]. При цьому ЦКЛП гарантує, що результати виконаних установою досліджень є ретельними, придатними для використання і відповідають світовим стандартам якості. Реалізація покладених на лабораторію завдань досягається завдяки цілій низці заходів:

- проведення досліджень ефективним способом, що ґрунтується на професійній практиці, згідно з затвердженими методами досліджень, найновіші досягнення науки і техніки;
- підтримка постійної співпраці з центрами та науковими організаціями з метою обміну досвідом та поширення результатів наукових досліджень;
- впровадження системи управління відповідно до норм EN ISO 900 і EN ISO/ IEC 17025;
- зростання якості надаваних послуг шляхом піднесення кваліфікації персоналу;
- дотримання вимог норм права та акредитаційної і сертифікаційної установи;
- забезпечення відповідного технічного обладнання та інфраструктури, що дозволяє досягнути високої якості послуг;

- забезпечення незалежності, безсторонності і довіри до досліджень, що проводяться на всіх рівнях функціонування Інституту;
- підтримання постійної співпраці з замовниками послуг з метою визначення їх очікувань та вимог;
- ефективне використання шансів, які створює Європейський Дослідницький Простір (*Europejska Przestrzeń Badawcza*) та Державна Програма Досліджень (*Krajowy Program Badań*) [5].

ЦКЛП постійно вимагає від свої експертів систематичного підвищення кваліфікації шляхом участі у різних навчальних курсах та міжнародних програмах обміну досвідом, стажуваннях, спеціалізованих семінарах, які організовуються загальноєвропейськими правоохоронними інституціями, а також окремими державами Європейського Союзу (*Bundeskriminalamt* в Німеччині, *Forensic Science Service* в Англії, *Institut National de Police Scientifique* у Франції, *Netherlands Forensic Institute* в Голандії) [4, с. 51]. За таких умов польські експерти-криміналісти можуть проводити свої дослідження, враховуючи останні досягнення науки і техніки. Триває також активна робота щодо співпраці та входження Польщі до систем ЄвроЕкперт (*EuroExpert*), Європейської академії судових наук (*European Akadamy of Forensic Sciens*), Європейської мережі інститутів судових наук (*European Network of Forensic Sciens Institutes*) у межах яких існує взаємне міждержавне визнання кваліфікації судових експертів, акретидації та сертифікації лабораторій.

Підсумовуючи, звернемо увагу на те, що Україна також зацікавлена в гармонізації стандартів якості проведення судових експертиз. З метою швидкого і водночас ефективного виконання своїх функцій вітчизняні експертні установи потребують періодичного оновлення технічного обладнання, впровадження нових методик дослідження, стимулювання наукових розвідок, спрямованих на розширення дослідницьких можливостей та підвищення якості експертиз. Важливо не залишитись на узбіччі європейської і взагалі світової науки, яка є інтелектуальною зброєю проти злочинності.

---

1. Całkiewicz M. Wykorzystanie opinii biegłego w polskim procesie karnym / M. Całkiewicz // Problemy kryminalistyki. – 259 (styczeń–marzec). – 2008. – S. 26–36.

2. Girdwoyń P. Opinia biegłego w sprawach karnych w europejskim systemie prawnym / P. Girdwoyń. – Warszawa: Wydawnictwo: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, 2011. – 182 s.
3. Hrehorowicz M. Opinia biegłego w sprawach karnych gospodarczych i jej ocena sądowa / M. Hrehorowicz. – Poznań: Wydawnictwo Poznańskie, 2013. – 388 s.
4. Pękała M., Marciniak E. Pojęcie jakości we współczesnej technice kryminalistycznej / M.Pękała, E. Marciniak // Problemy kryminalistyki. – 260 (kwiecień–czerwiec). – 2008. – S. 45–54.
5. Centralne Laboratorium Kryminalistyczne Policji. Polityka Jakości [Електронний ресурс]. – Режим доступу: http://clk.policja.pl/clk/system-jakosci/polityka-jakosci/66054, Polityka -Jakosci. html.

Імітаційне моделювання пішоходних потоків в проектах створення об'єктів з масовим перебуванням людей

Зачко О.Б.,
професор кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності,
доктор технічних наук, доцент
Головатий Р.Р.,
ад'юнкт кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності

Імітаційне моделювання руху людей в будівлях та спорудах з масовим перебуванням людей набирає підвищену актуальність через проблеми з забезпеченням безпеки на об'єктах даного типу. Посилені переміщення потоків відвідувачів відбуваються на об'єктах з масовим перебуванням людей (ОМПЛ), зокрема на спортивно-видовищних спорудах, аеропортах, вокзалах, торгово-розважальних-центрах, об'єктах підвищеної небезпеки, тощо. Сучасні програмні засоби імітаційного моделювання, зокрема продукт AnyLogic [1], дозволяють формалізувати можливі переміщення відвідувачів ОМПЛ в моделі пішохідних потоків ще на

стадії планування проекту. Це дозволяє зберегти час та підвищити якість опрацювання безпекових характеристик будівлі та споруди під час ініціації проектів та програм створення об'єктів даного типу.

Імітаційна модель досліджуваної споруди та її поведінки в умовах нормального функціонування та у разі виникнення надзвичайних ситуацій – це формальний опис її логічної структури. Кожний окремий елемент нашої системи підлягає імітаційному опису, та у загальному вигляді надає показники ймовірності певної величини: зокрема пропускної здатності споруди, кількісті людей на певну площину, можливість виникнення паніки серед відвідувачів будівлі, тощо. Моделювання пішохідних потоків – як елемент безпекоорієнтованого проектування, що разом з дослідженням бізнес-процесів ОМПЛ, системи координації сил та засобів реагування на надзвичайні ситуації, інформаційного середовища [2], транспортних потоків прилеглої території ОМПЛ, тощо – утворюють систему управління безпекою в проектах створення споруд з масовим перебуванням людей.

На рисунку 1 графічно зображено модель імітаційного моделювання життєвого циклу проекту створення торгово-розважального центру (згідно класифікаційних ознак – складова ОМПЛ). Споруда зображена з врахуванням сектору крамниць, сектору охорони та сектору відпочинку. Сектор продуктових магазинів для розрахунку пропускної здатності ОМПЛ не враховувався.

У моделі, крім параметрів будівлі, нами задані статичні дані: кількість працівників, охорони, допоміжній персонал, відвідувачі, робочий транспорт, які корелюються у незначних статистичних межах. Увімкнувши нашу систему (написана на мові програмування Java) – ми отримаємо показники, які дозволять сформувати уявлення про безпечне функціонування ОМПЛ. Це час прибуття відвідувачів, час доставки товарів, час замовлення, наявність вузьких зон в разі виникнення потреби евакуації – тощо. Ідентифікатор заповненості секторів – дозволяє вчасно зреагувати на можливе перенаповнення відвідувачами певних зон та внести корективи на стадії планування проекту.

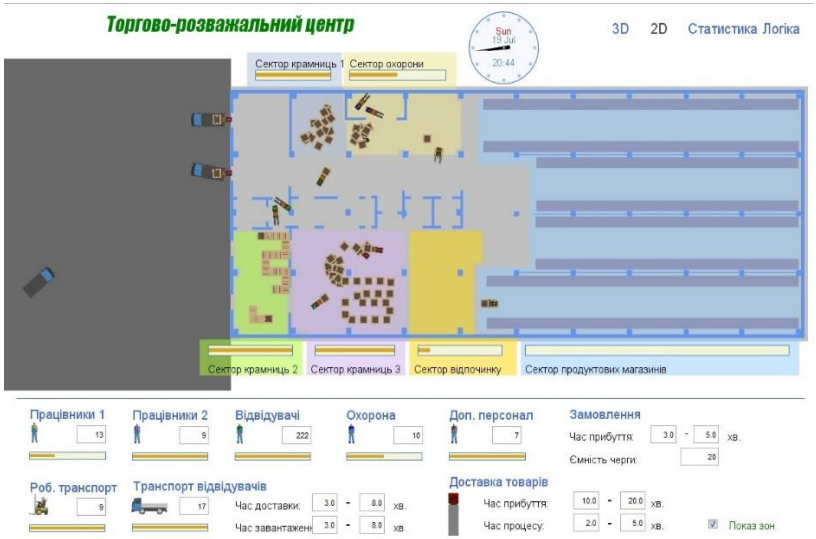


Рис. 1. Імітаційна модель життєвого циклу проекту створення ОМПЛ

На рис. 2 зображена динамічна модель імітаційного середовища життєвого циклу ОМПЛ, яка випливає з інтелектуальних розрахунків, показаних на рис.1.

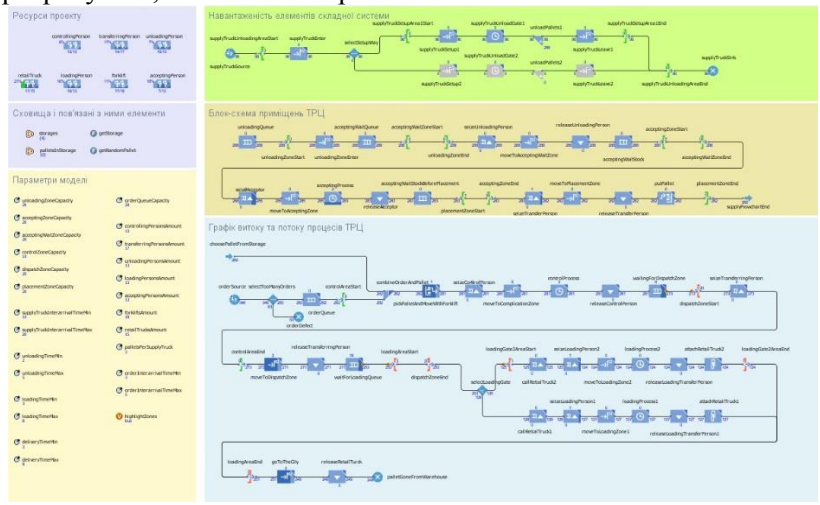


Рис. 2. Динамічна модель імітаційного середовища життєвого циклу ОМПЛ

Динамічна модель дає змогу візуально ознайомитися з параметрами, заданими для розрахунку безпечної експлуатації нашої споруди та включити свої редагування та правки. Робочий екран моделі складається з наступних складових: ресурси проекту, сховища та пов'язані з ними елементи, параметри моделі, навантаженість елементів системи, блок-схема приміщення ТРЦ, графік витоку та потоку процесів ТРЦ.

Розроблення імітаційної та динамічної моделей проектів створення об'єктів з масовим перебуванням людей дозволяють підвищити надійність функціонування системи на стадії планування проекту. Це дозволить зберегти фінансові ресурси, а найголовніше – життя та здоров'я громадян при проектуванні споруди та її безпекових характеристик.

1. Зачко, О.Б. Методологічний базис безпеко-орієнтованого управління проектами розвитку складних систем / О.Б. Зачко // Управління розвитком складних систем. – К.: вид-во КНУБА. –2015. – Вип. 23(1). – С. 51-55.
2. Зачко О.Б. Інтелектуальне моделювання параметрів продукту інфраструктурного проекту (на прикладі аеропорту «Львів») / О.Б. Зачко // Східно-Європейський журнал передових технологій. –2013. – № 1/10(61). С. 92-94.

Прилади для виявлення наркотичних речовин

Зачек О.І.,
доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Козаченко В.В.,
курсант Львівського державного університету
внутрішніх справ

Значним сегментом злочинної діяльності є незаконний наркобізнес. Злочинців в цьому бізнесі приваблюють надприбутки та постійне зростання доходів, оскільки наркозалежні особи постійно потребують все більшої кількості наркотичних засобів. На обліку в Україні перебувають сто тисяч наркоманів і це лише

вершина айсберга, оскільки кількість неврахованих наркоманів є невідомою. Наркоманія в Україні збільшується на 8% за рік – тенденція, одна з найвищих у світі. 70% наркоманів – молодь до 25 років. Жіноча наркоманія в Україні в процентному співвідношенні – найвища в Європі. Наркоманія в Україні впливає (і в майбутньому цей вплив багаторазово зросте) на негативну демографічну ситуацію [1].

Загалом головним постачальником наркотиків у межах України правоохоронні органи визнають іноземні злочинні організації. Через своє стратегічне географічне положення Україна є важливим шляхопроводом для різних форм контрабанди. Контрабандисти постійно удосконалюють форми, методи та спрямованість своєї злочинної діяльності. Для транспортування наркотиків зазвичай використовують такі транспортні засоби:

- рейсові автобуси і легкові автомобілі, в яких наркотики перевозять у пасажирському салоні або серед речей багажу в багажному відсіку автобуса, у салоні автомобіля на задньому сидінні під чохлом (наркотики використовують як набивку сидіння), у запасному колесі, у дверцятах, бамперах, бензобаку, закріплені до днища;
- пасажирські поїзди (міжнародного сполучення), де наркотики перевозяться серед особистих речей багажу або як нічийне майно із використанням особливостей конструкції пасажирських вагонів: технологічних порожнин, рундуків для вугілля, міжстельового простору над вбиральнями та тамбурами вагонів, рундуків під сидіннями, радіаторів опалення, «третього поверху» полиць, сміттєзбірників, люків над електрощитами, акумуляторних ящиків, ніш для котлів опалення та умивальників, вентиляційних люків тощо [2].

Для максимально ефективного виявлення контрабанди наркотичних засобів і психотропних речовин необхідно застосовувати технічні прилади виявлення наркотичних засобів у схованках та інших місцях (іонсканери, рентгенівська апаратура, електронні щупи).

Митні органи багатьох країн почали використовувати засоби технічного контролю, створені за допомогою сучасних наукових

досягнень. В основі технології новітнього обладнання – спектрометрія іонної рухливості. Прилади використовуються для експрес-виявлення слідових кількостей наркотичних або вибухових речовин. Наприклад, настільний детектор для виявлення слідів вибухових та наркотичних речовин «IONSCAN» здатен лише за декілька секунд виявити та ідентифікувати більше 40 видів наркотиків та вибухових речовин [3].

Існує два основних принципи роботи технічних засобів для пошуку та виявлення наркотиків. Перший принцип використовує рентгенівський контроль і базується на здатності наркотичних речовин (як і інших органічних речовин) не поглинати, а відбивати, розсіювати рентгенівські промені. Другий принцип базується на аерозольній дисперсії наркотиків (полягає в наявності мікрочастин речовини в повітряному середовищі упаковки), коли виділяється гранично мала доза речовини і її характеристики порівнюються із закладеними в пам'яті ЕОМ параметрами відомих наркотичних речовин [4].

Існує велика кількість технічних засобів, які базуються на цих принципах. Розглянемо деякі з них.

Технічний прилад NDS-2000 є портативним детектором наркотичних речовин. Він використовується для виявлення широкого спектра наркотичних речовин. Має свої особливості: невелика вага пристрою (5.5 кг з акумулятором) та простота застосування NDS-2000 є важливими для використання в роботі правоохоронних органів; може живитися від акумулятора, електромережі та автомобільного прикурювача; виявляє надзвичайно малі сліди кокаїну, героїну, ТНС, метамфетаміну, а також інших наркотиків. Принцип роботи базується на газовому хроматографі та детекторі поверхневої іонізації. Відбір проб здійснюється за допомогою серветок або за допомогою спеціального електричного повітрозбірника, потім проба переноситься на сітчастий екран та вставляється в прилад. Протягом кількох секунд здійснюється аналіз та видається результат на рідкокристалічному індикаторі. Виявлення наркотику супроводжується світловою та звуковою індикацією [5].

SABRE 5000 – портативний детектор слідів наркотичних речовин. Переваги моделі наступні: компактний і легкий, містить три режими: детектор (виявляє вибухові, наркотичні та бойові

хімічні речовини), швидке очищення приладу після виявлення небезпечних речовин; автоматична діагностика роботи систем. Нові характеристики у співвідношенні з відмінним дизайном і надійністю попередніх моделей (SABRE 4000) роблять новий аналізатор придатним для захисту об'єктів життєзабезпечення, портів, кордонів. SABRE 5000, в основі якого лежить технологія спектрометрії іонної рухомості, запрограмований на виявлення та розпізнання протягом 20 секунд більше 40 небезпечних речовин. Прилад має такі особливості: час виконання аналізу 10 секунд, не більше 20 секунд; тип сигналу тривоги звуковий одночасно з візуалізацією ідентифікованих речовин; вага 3.2 кг разом з акумулятором; діапазон робочих температур від 0° до 40°С [6].

Рис. 1. Детектор наркотичних речовин NDS-2000

Рис. 2. Детектор слідів вибухових, наркотичних та отруйних речовин SABRE 5000

Детектор контрабанди Buster K910B використовує гамма-випромінювання низької інтенсивності для швидкого сканування транспортних засобів і житлових приміщень з метою виявлення прихованої контрабанди. Прилад надсилає потік гамма-випромінювання всередину досліджуваного об’єкта і реагує на потік випромінювання, що відбивається. На дисплей видаються покази, що залежать від густини та структури об’єкта. Buster K910B реагує на місця, де можуть бути заховані наркотики, зброя і тому подібне.

Рис. 3. Детектор контрабанди Buster K910B

Buster K910B має такі характеристики: швидкість сканування 0.25 секунд; термін служби батареї 6-12 місяців; вага 700-900 г. На світовому ринку Buster K910B займає провідні позиції, використовується вже більше як 25 років, ним користуються правоохоронні органи, митні та прикордонні служби більше 60 країн [7].

Детектор для ідентифікації твердих та рідких хімічних речовин HazmatID Ranger є інфрачервоним фур'є-спектрометром (Фур'є-ІЧ). Система використовує неруйнівну технологію аналізу твердих матеріалів, порошків, пастоподібних мас, гелів і рідин. Аналіз виконується шляхом доторкання до речовини кінчиком алмазного давача автоматичного розпізнавання. Можливість швидкої та точної ідентифікації більше чим 32 000 хімічних субстанцій, а саме: білі порошки, наркотики і похідні речовини для їх виготовлення, зброя масового ураження, вибухові речовини, пестициди, звичайні й токсичні промислові хімікати та

інше. Має такі особливості: вага – 2.94 кг.; діапазон робочої температури від -7°С до +50°С; джерело живлення від внутрішньої батареї, від мережі; час роботи батареї складає більше трьох годин [8].

Рис. 4. Детектор для ідентифікації твердих та рідких хімічних речовин HazmatID Ranger

В останній час розробляються комплекси для виявлення наркотичних речовин, які дозволяють дистанційно забирати проби повітря за допомогою дронів та роботизованих транспортних засобів з метою виявлення наявності слідів наркотиків для викриття нарколабораторій [9, с. 398-408].

Проаналізувавши розглянуті вище технічні засоби, які використовують різні принципи виявлення наркотичних речовин, можна прийти до висновку, що вибір таких приладів для використання обумовлюється конкретними обставинами роботи правоохоронних органів та завданнями, які постають перед ними. Якщо ж порівняти їх технічні параметри, то можна прийти до наступних висновків. Застосування Buster K910B на відмінну від приладу NDS-2000 є зручнішим, що зумовлює його компактність та легкість. Його вага (700-900 г.) майже у 7 разів є меншою ніж у NDS-2000 (5.5 кг.) Також перевага Buster є у його миттєвому аналізі об’єкта на наявність в ньому наркотичних речовин (0.25 секунд) на відмінно від SABRE 5000 (10 секунд), NDS-2000 (до 40 секунд). Технічний пристрій HazmatID Ranger є кращим у

використанні під час сильної спеки, адже його діапазон роботи до +55°С. Так само і у період морозу HazmatID Ranger лідирує, його робочий діапазон при мінусовій температурі складає -7°С, тоді як SABRE 5000 може функціонувати лише від 0°С, а технічний пристрій NDS-2000 взагалі лише при плюсовій +5°С.

1. Наркоманія в Україні. – [Електронний ресурс]. – Режим доступу: http://narconon.kiev.ua/narcukr_uk.
2. Практика розгляду судами справ про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів. – [Електронний ресурс]. – Режим доступу: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/179F1409F1D9B89AC2257B7C0044C93B.
3. IONSCAN 400B. – [Електронний ресурс]. – Режим доступу: http://www.versiya.com/smiths-detection/security-checkpoint-solutions/ionscan-400b.html.
4. Спеціальні технічні засоби митного контролю, структура та застосування. – [Електронний ресурс]. – Режим доступу: www.center.km.ua/metcab/plans/files/Z000180.doc.
5. Портативный детектор наркотических веществ NDS-2000. – Інтернет-магазин 9 мм. – [Електронний ресурс]. – Режим доступу: http://9mm.com.ua/spectehnika-bezopasnoati/poiskovaja - spectehnika/antiterror/nds-2000.html.
6. Портативный детектор следов взрывчатых и наркотических веществ, боевых и промышленных отравляющих химических веществ. – [Електронний ресурс]. – Режим доступу: http://www.versiya.com/smiths-detection/explosives-narcotics-etection/sabre5000.html.
7. Денситометр (измеритель плотности и детектор контрабанды) Buster K910B. – Криминалистическое и антитеррористическое оборудование «Экспертные системы». – [Електронний ресурс]. – Режим доступу: http://es-trade.kiev.ua/ru/catalog_anti-terror_and_security/view/315212/Buster_K910B/info/.
8. Ручной прибор для идентификации твердых и жидких химических веществ. – [Електронний ресурс]. – Режим доступу: http://www.versiya.com/smiths-detection/chemical-identification/hazmatid-ranger.html.
9. Kosiński Jerzy, Jewartowski Błażej, Szmigielski Radoslaw, Duszyńska Anna. Kołowy autonomiczny namierzacz i analizator «KANIA» // Теорія та практика правоохоронної діяльності: Тези доповідей учасників Міжнародної науково-практичної конференції 11 листопада 2016р. – Львів: ЛьвДУВС, 2016. – С. 398-408.

Оптоелектронна система визначення аберацій та пропускної здатності оптичних засобів військового призначення

Когут Р.Л.,
курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Якість лінзових оптичних систем, у т.ч. військового призначення, визначається параметрами, найважливішими з яких є аберації та пропускна здатність. Через аберації зображення втрачають чіткість і не точно відповідають зображуваним об'єктам. Найпоширенішими абераціями є хроматична, сферична, кома, дисторсія, астигматизм. Оптичні системи зазвичай мають одночасно кілька різних типів аберацій. Також при проходженні променя крізь оптичну систему, знижується його світлова енергія – зменшується яскравість та контраст, що пов'язане з відбиванням і поглинанням (за наявними даними 1 см скла поглинає приблизно 12% світла і, за відсутності спеціального покриття, вібиває 46% падаючого світла).

Для виявлення аберацій та пропускної здатності оптичних систем сконструйовано оптоелектронну систему, що складається з трьох лазерів з різними кольорами свічення (для аналізу хроматичної аберції) потужністю 1 мкВт кожен, приймача оптичного випромінювання – двовимірної ПЗЗ-матриці з відповідною електронікою до неї та досліджуваної оптичної системи, які розміщені на оптичній лаві і при дослідженні крім зміни віддалі між ними можуть переміщуватися у взаємопаралельних площинах, перпендикулярних головній оптичній осі досліджуваної оптичної системи, щоб лазерний промінь можна було пропускати крізь досліджувану оптичну системи паралельно її головній оптичній осі, та промінь можна запускати під певним кутом до головної оптичної осі досліджуваної оптичної системи (для аналізу коми). ПЗЗ-матриця через USB-порт приєднується до комп'ютера для аналізу сигналограм та побудови за ними графіків створених спотворень сигналу досліджуваною оптичною системою.

Початкові дослідження для перевірки оптоелектронної системи проведені на багатолінзових оптичних системах цивільного призначення – біноклях для мисливства з 8- та 10-кратним збільшенням.

Основні напрямки профілактики злочинів проти статевої свободи та статевої недоторканості

Кожина К.П.,
студентка Одеського державного університету внутрішніх справ
Цільмак О.М.,
професор кафедри криміналістики, судової медицини та психіатрії Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

На сьогодні найбільш резонансними злочинами, які піднімають хвилю громадського оббурювання, є злочини проти статевої свободи та статевої недоторканості особи. Такі злочинні діяння посягають на найвищі соціальні цінності, а саме на життя і здоров'я, честь і гідність, недоторканність і безпеку людини (ст. 3 Конституції України) [2].

Основним безпосереднім об'єктом статевих злочинів є суспільні відносини, що забезпечують статеву свободу та статеву недоторканість особи. В кримінально-правовій літературі статева свобода визначається як право особи самостійно обирати собі партнера для статевих зносин і не допускати у сфері таких зносин будь-якого примусу. Отже, статева недоторканість – це право людини на не вторгнення в його статеве життя без його згоди.

Виходячи з вищесказаного, злочини проти статевої свободи та статевої недоторканості особи являють собою саме ті злочини, які передбачені розділом IV Кримінального кодексу України (далі – КК України). До них віднесені: зґвалтування (ст. 152 КК України), насильницьке задоволення статевої пристрасті неприродним способом (ст. 153 КК України), примушування до вступу в статевий зв'язок (ст. 154 КК України), статеві зносини з особою, яка не досягла статевої зрілості (ст. 155 КК України), розбещення неповнолітніх (ст. 156 КК України) [3, ст. 152-156].

Таким чином, прослідкувавши офіційні статистичні показники, можемо зробити висновок, що в останні роки майже не спостерігаються зміни в динаміці статевих злочинів. Відповідно до офіційних статистичних даних Генеральної прокуратури

України, спостерігаємо наступну тенденцію розвитку злочинів проти статевої свободи та статевої недоторканості: в 2013 р. вчинено 1114 злочинів; в 2014 р. – 893 злочинів, в 2015 р. – 776 злочинів, станом на жовтень 2016 р. – вчинено 882 злочини. Ці показники свідчать передусім не про низький рівень вчинюваних злочинів, а про високу латентність злочинів проти статевої свободи та статевої недоторканості особи, де частка прихованих складає майже до 90 % [4].

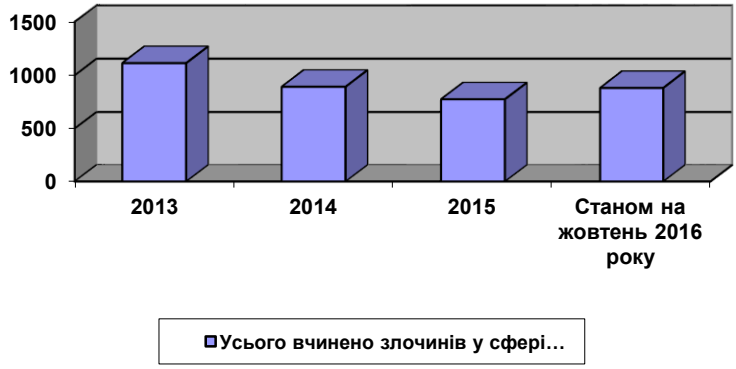


Рис. 1.

Статеві злочини по-різному представлені в структурі зареєстрованої злочинності (наприклад, за даними Департаменту інформаційних технологій МВС України 81,1 % в структурі статевих злочинів разом складають згвалтування та задоволення статевої пристрасті неприродним способом). Ці злочини є найбільш поширеними в структурі злочинів, пов'язаних із сексуальним насильством. За ними слідує розбещення неповнолітніх – 14,1 %, а злочини, передбачені ст. 155 КК України (статеві зносини з особою, яка не досягла статевої зрілості) та ст. 154 КК України (примушування до вступу в статевий зв'язок) зустрічаються досить рідко і разом становлять 3,2 % [5].

Дослідження науковців-кримінологів свідчать про те, що більшість статевих правопорушень вчиняються у стані наркотичного, алкогольного та іншого сп'яніння. Тому ми вважаємо доцільним звернути увагу на злочини, які коються частіше в порівнянні з іншими злочинами в категорії злочинів проти статевої свободи та статевої недоторканості особи.

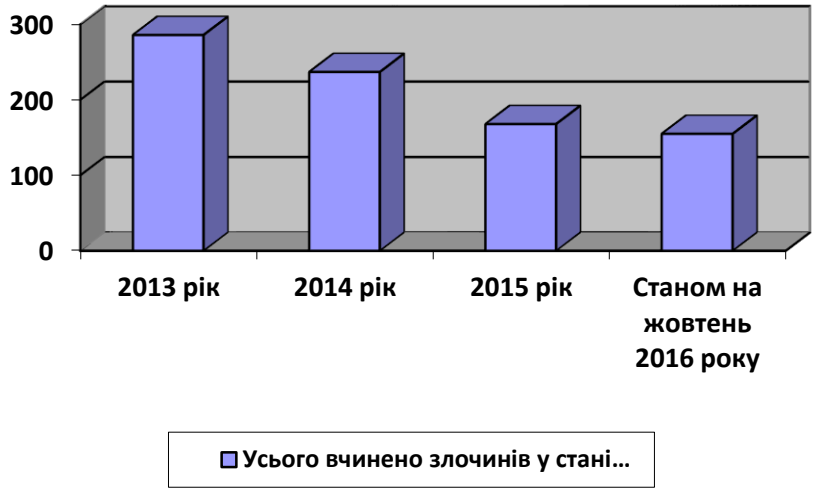


Рис. 2.

Отже, відповідно до статистичних показників Генеральної прокуратури України було зареєстровано така кількість злочинів, вчинених у стані алкогольного сп'яніння у звітному періоді за січень – грудень 2013 р. 286. За ступенем тяжкості: особливо тяжкі – 75 злочинів; тяжкі – 92; злочини середньої тяжкості – 119; злочини невеликої тяжкості – 0. За видами правопорушень проти статевої свободи та статевої недоторканості особи: зґвалтування (ст. 152 КК України) – 163; насильницьке задоволення статевої пристрасті неприродним способом (ст. 153 КК України) – 80; примушування до вступу в статевий зв'язок (ст. 154 КК України) - 0; статеві зносини з особою, яка не досягла статевої зрілості (ст. 155 КК України) – 12; розбещення неповнолітніх (ст. 156 КК України) – 31.

У стані алкогольного сп'яніння в звітному періоді за січень – грудень 2014 р. було зареєстровано злочинів – 237; За ступенем тяжкості: за вчинення особливо тяжких злочинів – 69; за вчинення тяжких злочинів – 83; за вчинення злочинів середньої тяжкості – 84; за злочини невеликої тяжкості – 1. За видами правопорушень: зґвалтування (ст. 152 КК України) – 122; насильницьке задоволення статевої пристрасті неприродним способом (ст. 153 КК України) – 80; примушування до вступу в статевий

зв’язок (ст. 154 КК України) – 1; статеві зносини з особою, яка не досягла статевої зрілості (ст. 155 КК України) – 8; розбещення неповнолітніх (ст. 156 КК України) – 26.

У стані алкогольного сп'яніння в звітному періоді за січень – грудень 2015 р. було зареєстровано злочинів – 168; За ступенем тяжкості: за вчинення особливо тяжких злочинів - 50; за вчинення тяжких злочинів – 52; за вчинення злочинів середньої тяжкості – 66; за злочини невеликої тяжкості – 0. За видами правопорушень: зґвалтування (ст. 152 КК України) – 87; насильницьке задоволення статевої пристрасті неприродним способом (ст. 153 КК України) – 59; примушування до вступу в статевий зв’язок (ст. 154 КК України) – 0; статеві зносини з особою, яка не досягла статевої зрілості (ст. 155 КК України) – 2; розбещення неповнолітніх (ст. 156 КК України) – 20.

У стані алкогольного сп'яніння в звітному періоді за січень – жовтень 2016 р. було зареєстровано злочинів – 155; За ступенем тяжкості: за вчинення особливо тяжких злочинів – 30; за вчинення тяжких злочинів 64; за вчинення злочинів середньої тяжкості – 61; за злочини невеликої тяжкості – 0. За видами правопорушень: зґвалтування (ст. 152 КК України) – 82; насильницьке задоволення статевої пристрасті неприродним способом (ст.153 КК України) – 48; примушування до вступу в статевий зв’язок (ст. 154 КК України) – 0; статеві зносини з особою, яка не досягла статевої зрілості (ст. 155 КК України) – 0; розбещення неповнолітніх (ст. 156 КК України) – 25 [4].

Отже, можна констатувати, що у загальному обсягу (за 2013–2016 рр.) кількість таких тяжких кримінальних правопорушень, як злочини проти статевої свободи та статевої недоторканості, мають певну стабільність та серйозні несприятливі тенденції до їх розвитку. Враховуючи вищезазначене, можна стверджувати, що означені несприятливі тенденції динаміки даних кримінальних правопорушень триватимуть на тлі посилення соціально-економічної кризи у країні.

Виходячи з вищезазначеного можна констатувати, що злочини сексуального характеру, вчинені в алкогольному сп’янінні набувають масовий характер, висока шкідливість яких очевидна. Тому, насамперед, необхідно вжити ряд дій превентивного характеру. Протидія злочинам проти статевої свободи та статевої

недоторканості особи повинна проводитися в комплексі попереджувальних заходів.

На загально-соціальному рівні в державі необхідно створити умови для формування духовних, культурних та моральних цінностей суспільства. Також необхідно проводити широку просвітницьку діяльність серед молоді в сфері статевих відносин, планування сім'ї, зміцнення родинних зв'язків та сім'ї як основного соціального інституту суспільства.

На державному рівні сприяти вирішенню житлових проблем, зайнятості молоді та організації дозвілля, боротьбі з дитячою бездоглядністю та безпритульністю; зміцненню матеріально-технічної бази місць дозвілля і вирішення інших питань використання вільного часу; забезпеченню рівного доступу усіх членів суспільства до освіти і культурних цінностей; наданню широкої психологічної допомоги населенню; здійсненню програми щодо захисту жертв насильства і надання їм медико-психологічної допомоги; запровадити обмеження і заборону пропаганди насильства і порнографії. Також повинна ефективно проводитися боротьба з проституцією, алкоголізмом, наркоманією і токсикоманією [1, с. 27-29].

Покращити взаємодію правоохоронних органів з освітніми установами у напрямках розробки програм правового та статевого виховання, проведення тематичних занять, залучення фахівців психологів та медиків є спеціально-кримінологічним попереджувальним заходом протидії статевим злочинам.

Також необхідно вжити ряд превентивних заходів щодо забезпечення індивідуальної профілактики статевих злочинів. А саме:

- застосування заходів медичного характеру. (Наприклад, слід обов'язково проводити комплексну медико-психіатричну експертизу за всіма різновидами статевих злочинів, результати якої необхідно враховувати як при призначенні покарання так і для організації лікування особи);
- здійснення виховної роботи серед населення та молоді;
- проведення в навчальних закладах різного рівня лекцій-бесід правового виховання, в яких роз'яснювати, як не стати жертвою статевого злочину, наголошувати на обов'язковості повідомлення правоохоронних органів у випадку, коли злочин був вчинений.

Вжиття профілактичних заходів будуть дієвими якщо спиратимуться на великомасштабні заходи соціально-економічного, культурно-виховного, ідеологічного характеру.

1. Голіна В.В. Попередження злочинності. Конспект лекції. – Х.: 1994, с. 27— 29.
2. [Конституція України: закон України від 28 червня 1996 р. № 254/96 // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141]
3. [Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131]
4. Статичні показники Генеральної прокуратури України [електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ ua/stst2011.html
5. Стан та структура злочинності в Україні. Статистика Департаменту інформаційних технологій МВС України [Електронний ресурс]. – Режим доступу : http://sfs.gov.ua/diyalnist-/pokazniki-roboti/ dosudove-slidstvo/

Інформаційні технології в судовій практиці

Костюк О.Є.,
здобувач освітнього ступення «магістр»
Львівського державного університету внутрішніх справ
Магеровська Т.В.,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук, доцент

Упровадження інформаційних технологій у судовій системі − це не відповідь моді, а необхідність і вимога сучасності, це один зі шляхів прозорої діяльності суду та забезпечення доступності і підвищення оперативності українського судочинства, саме ці технології здійснюють забезпечення громадян і організації достовірною судовою інформацією.

У умовах проведення судової реформи особливого значення набуває вдосконалення якості судочинства, розширення доступу громадян до правосуддя і забезпечення гласності розгляду справ судами, у тому числі шляхом створення та ефективного застосування сучасних інформаційних технологій та систем.

Варто зазначити, що майбутній вступ України до ЄС неможливий без впровадження міжнародних стандартів обміну правовою інформацією (включаючи судову) в електронному вигляді через Інтернет.

У зв'язку зі змінами соціально-економічної ситуації в Україні, зростанням злочинності, збільшенням і якісною зміною змісту цивільних справ, розширенням можливостей оскарження у суді неправомірних дій посадових осіб навантаження на органи судової влади зростає з кожним роком.

За відсутності в більшості судів першої інстанції сучасних комп'ютерних технологій судова практика характеризується серйозними порушеннями процесуальних термінів розгляду справ і заяв. Майже половина позовів про поновлення на роботі, щодо житлових спорів, про позбавлення батьківських прав тощо не розглядаються судами вчасно. Повільність судів при розгляді кримінальних справ призводить до збільшення термінів утримання обвинувачуваних під арештом.

Інформатизація судової діяльності – систематизований процес створення сприятливих умов для доступу до інформації, використовуваної в судочинстві, її зберігання, обробки і передачі в електронній формі на основі ресурсів і послуг судових інформаційних систем з метою підвищення ефективності і прозорості українського правосуддя.

Судові інформаційні системи являють собою сукупність баз даних, що забезпечують обробку технологій і програмно-технічних засобів, що застосовуються у своїй діяльності судові органи [1].

Судова інформація визначається як цілеспрямований процес мінімізації ентропії(невизначеності) щодо можливої, дозволеної і забороненої поведінки суб'єктів суспільних відносин у сфері процесуальної і позапроцесуальної діяльності суддів загальної юрисдикції [2].

Політика інформатизації судової системи повинна базуватися на таких базових принципах державної інформаційної політики:

1. Принцип рівності інтересів – політика рівною мірою враховує інтереси всіх учасників інформаційної діяльності незалежно від їх положення в суспільстві (єдині для всіх «правила гри»).

2. Принцип відкритості політики – всі основні заходи судової політики в інформаційній сфері відкрито обговорюються фахівцями і їх думка враховується.
3. Принцип системності передбачає декомпозицію системи на складові частини (компоненти), які дають можливість їх автономної розробки і впровадження при забезпеченні єдності технічної політики.
4. Принцип соціальної орієнтації, основні заходи судової політики повинні бути спрямовані на забезпечення соціальних інтересів громадян України.

Побудова автоматизованої судової системи в Україні має здійснюватися відповідно до таких вимог:

- комплексне організаційне і методичне забезпечення процесів створення, впровадження та експлуатації засобів інформатизації в судах;
- уніфікація базових комп'ютерних засобів, засобів зв'язку і передачі даних в межах відповідних функціональних підсистем;
- попередній підбір кадрів та навчання персоналу судів комп'ютерним технологіям [4].

Серед найбільш важливих систем, що впроваджуються в більшості судів світу, є наступні:

- система електронного діловодства;
- система аудіо- та відеозапису і протоколювання;
- відеоконференцсистема;
- система анонімного допиту свідка;
- система публікації записів або трансляції судових засідань на Інтернет-порталі.

Аналіз досвіду багатьох країн засвідчує, що спостерігаються тенденції розробки та впровадження єдиних інформаційних систем в межах країни для забезпечення скоординованої роботи судів, правоохоронних та правозахисних органів.

На даний час в Україні працюють розрізнені технічні системи для автоматизації роботи в судах, які відповідають світовому рівню, але немає єдиної концепції і єдиного технологічного середовища, які б забезпечили ефективну та скоординовану роботу судів, правоохоронних та правозахисних органів. Таким чином,

потрібна невідкладна розробка та впровадження національної програми по комплексній модернізації технологічної бази судів та правоохоронних органів України [3].

Зробивши всебічний аналіз практики з інформатизації судів можна зробити висновок, що в умовах відсутності єдиного державного проекту, належного фінансування, недостатність забезпечення обчислювальною технікою, велика частка застарілих комп'ютерів ускладнюють впровадження сучасних інформаційних технологій.

1. Інформаційні системи судових органів. [Електронний ресурс]. – Режим доступу: http://allref.com.ua/uk/skachaty/informaciiyni_sistemi_sudovih_organiv
2. Маргарян А. Р. Институты судебной власти в информационно-правовом пространстве / А. Р. Маргарян // Право. – 2007. – № 18. – С. 68.
3. Радуцький О., Вільшун О. Інформаційні технології в судах. – Юридичний журнал, 04(106) 2011// РАДУЦЬКИЙ О., ВІЛЬШУН О. [Електронний ресурс]. – Режим доступу: http://www.srs.kiev.ua/index.php?id=224&Itemid=6&lang=ru&option=com_content&view=article
4. Туркіна І. «Ефективність державного управління».– Збірник наукових праць. – 2011. – Вип. 29

Програмне забезпечення системи апаратних обчислювальних платформ для уніфікованого управління наявними програмними ресурсами

Крошний І.М.,
доцент кафедри інформаційних технологій
Національного лісотехнічного університету України,
кандидат технічних наук, доцент
Шиба П.В.,
здобувач освітнього ступення «магістр»
Національного лісотехнічного університету України

Система складається з двох важливих частин: відправника (низькорівнева програмна плата) і приймача (програмне забезпечення високого рівня, адаптоване для роботи з платою). Система

забезпечить ефективний спосіб зв'язку і обміну даних між пристроями. Для цієї мети, розроблюється програмна бібліотека для потоку даних, яка буде ефективною під час їх обробки.

З точки зору низькорівневого програмування, ефективно буде використовувати фіксований стеко-орієнтований підхід для роботи з пам'яттю і обробки даних відправника.

Внутрішні алгоритми обробки операцій управління пам'яттю для підвищення продуктивності в конкретних ситуаціях є частиної загального програмного інтерфейсу.

На стороні приймача, ми повинні замінити поточні операції виділення/звільнення пам’яті. Стандартна реалізація цих операцій ефективна для розподілу великих обсягів даних, які не актуальні ддя низькорівневих операцій (дані менше 128 байт).

Практичне застосування

Сучасні системи використовують багато різних видів зовнішніх датчиків. Крім того, існує безліч систем реального часу, які відправляють багато даних досить малого розміру.

Для прикладу, можна підключити до плати датчик руху та відео камеру і, таким чином, отримати базову систему моніторингу, яка буде працювати тільки тоді коли в певній області буде виявлено рух.

Для систем реального часу, нам потрібно позбавитися від непотрібних даних і додаткових операцій. Це ефективний підхід, який використовується для медичних пристроїв, де важлива продуктивність.

Наприклад, сучасний кардіодефібрилятор має додаткові опції, такі як моніторинг ЕКГ. Отримані дані повинні бути дуже точні і швидко оброблювані.

Апаратна частина

Для ефективної роботи системи було обрано плату Arduino Nano.

Плата Arduino складається з мікроконтролера Atmel AVR, а також елементів обв’язки для програмування та інтеграції з

іншими пристроями. На багатьох платах наявний лінійний стабілізатор напруги +5В або +3,3В. Тактування здійснюється на частоті 16 або 8 МГц кварцовим резонатором. У мікроконтролер записаний завантажувач (bootloader), тому зовнішній програматор не потрібен.

На концептуальному рівні усі плати програмуються через RS-232 (послідовне з'єднання), але реалізація даного способу різниться від версії до версії. Новіші плати програмуються через USB, що можливо завдяки мікросхемі конвертера USB-to-Serial FTDI FT232R. У деяких варіантах, таких як Arduino Mini або неофіційній Boarduino, для програмування потрібно підключити до контролера окрему плату USB-to-Serial або кабель.

Програмне забезпечення

Інтегроване середовище розробки Arduino це багатоплатформовий додаток на Java, що включає в себе редактор коду, компілятор і модуль передачі прошивки в плату. Строго кажучи, це C++, доповнений деякими бібліотеками. Програми обробляються за допомогою препроцесора, а потім компілюється за допомогою AVR-GCC.

Реалізація на програмному рівні

Ідея полягає в компенсації основної проблеми malloc і інших поточних стандартних операцій з пам'яттю. Також можна скласти, для кожного окремого випадку, уніфіковані можливості такі як: 1) збір статистичної інформації про профілі використання пам'яті: 2) застосувати механізмів блокування, щоб пам'ять, виділена для блоків, була обмежена в рамках конкретного буферу. 3) ефективно звільняти пам'ять в однопотокових середовищах.

Кожен алокатор повертає такий блок:

```
struct block {
void *ptr;
size_t length;};
```

Запит на виділення пам'яті виглядатиме так:

```
auto myMemBlock = allocator.allocate(42);
```

В основному, система, на низькому рівні, буде використовувати стеко-оріентований розподіл пам'яті. Компіляція програмної бібліотеки буде здійснюватися для плати та для прикладного програмного забезпечення окремо. Загальний програмий інтерфейст зводиться до наступних функцій:

- static constexpr unsigned alignment; – поточне вирівнювання байт
- static constexpr realSize(size_t); – реальний розмір виділеного блоку
- block ps_allocate(size_t); – виділення пам'яті з вказаним розміром
- block ps_allocateAll(); - виділення всієї доступної пам'яті
- bool ps_expand(block&, size_t delta); – збільшення поточного блоку
- void ps_reallocate(block&, size_t); – виділення блоку пам'яті, з поточного
- void deallocate(block); – звільнення блоку
- void deallocateAll(); – звільнення всієї доступної пам'яті.

Розроблена система дозволить отримати ефективний засіб управління пам'яттю апаратної плати, що дозволить розширювати її функціональність залежно від наявних давачів та інших компонентів. З іншого боку, прикладне програмне забезпечення матиме змогу доступу до даних, отриманих через апаратну плату в найбільш ефективний спосіб, що зменшить затрати на їх обробку та інтерпретацію.

1. Berger, E. D.; Zorn, B. G.; McKinley, K. S. (June 2001). «Composing High-Performance Memory Allocators». Proceedings of the ACM SIGPLAN 2001 conference on Programming language design and implementation (PDF). pp. 114–124. CiteSeerX 10.1.1.1.2112Freely accessible. doi:10.1145/378795.378821. ISBN 1-58113-414-2.
2. Berger, E. D.; Zorn, B. G.; McKinley, K. S. (November 2002). «Reconsidering Custom Memory Allocation». Proceedings of the 17th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (PDF). pp. 1–12. CiteSeerX 10.1.1.119.5298Freely accessible. doi:10.1145/582419.582421. ISBN 1-58113-471-1.
3. http://www.drdobbs.com/policy-based-memory-allocation/184402039
4. Simple Memory Allocation Algorithms (originally published on OSDEV Community)
5. Wilson, P. R.; Johnstone, M. S.; Neely, M.; Boles, D. (1995). «Dynamic storage allocation: A survey and critical review». Memory Management. Lecture Notes in Computer Science. 986. pp. 1–116. CiteSeerX 10.1.1.47.275Freely accessible. doi:10.1007/3-540-60368-9_19. ISBN 978-3-540-60368-9.

Проблеми нормативно–правового забезпечення застосування поліграфа в Україні

Кунтій А.І.,
доцент кафедри кримінального процесу Львівського державного університету внутрішніх справ, кандидат юридичних наук
Марчук С.О.,
курсант Львівського державного університету внутрішніх справ

Серед методів, що використовуються у розслідуванні кримінальних правопорушень, мають місце методи, котрі не дістали достатнього визнання та поширення, котрі не можна віднести до загальновідомих і впровадження у практику. Одним із таких є використання поліграфа і на сьогодні постає необхідність вдосконалення правової норми його застосування.

Поліграф (грецькою poli – багато, graphos – пишу) – багатоканальний психофізіологічний пристрій, призначе¬ний для реєстрації та запису у реальному часі показників емоційного напруження, що виникає у відповідь на інформацію у вигляді слів, словосполучень, малюнків, фотокарток [1, с. 8].

Вченими вироблено різні підходи до визначення місця і ролі цього технічного забезпечення, але єдиного системно концептуального бачення стосовно нормативно–правової регламентації поліграфа не вироблено і до сьогодні. Над даною проблемою працювали такі вчені як С.Д. Гусарєв, В.В. Чернєй, О.І Мотлях, Т.Р. Морозова, В.В. Топчін, А.В. Мовчан, І.В. Басиста, І.М. Охріменко, І.В. Кубарєв та інші.

В Україні на законодавчому рівні не закріплено використання поліграфа у процесі розслідування, проте були спроби доповнити Кримінальний процесуальний кодекс України, ініціатором такого доповнення був народний депутат Г.Г. Москаль, котрий вніс на розгляд Верховної Ради України законопроект від 12 березня 2013 р. № 2521 «Про доповнення Кримінального процесуального кодексу України положеннями, щодо використання поліграфа (детектора брехні)» [2]. У проекті запропоновано окреслити загальні вимоги до проведення перевірки на поліграфі у кримінальному провадженні, а також встановити необхідність її проведення експертами державних спеціалізованих установ. Повторною

спробою узаконення поліграфа у Кримінальному процесуальному кодексі України, була законодавча ініціатива народних депутатів України: О.С. Барни, Т.З. Юрика, М.В. Люшняка, О.В. Ревеги від 10 грудня 2015 р. N 3611 «Про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні)» [3]. Проте як і попередня поправка не була прийнята адже під час проходження поліграфа людина відповідає на питання «так» або «ні», а отже вона може завчити відповіді на запитання, що знімає «ефект раптовості».

У Міністерстві внутрішніх справ використання поліграфа регламентується Наказом від 28 липня 2004 р. за №842, яким затверджено «Інструкцію щодо застосування комп'ютерних поліграфів у роботі з персоналом органів внутрішніх справ України» [4]. Дана інструкція не передбачає обов'язкового проходження працівниками поліграфічних перевірок, не містить чітких критеріїв відповідності результатів обстежень кваліфікаційним вимогам щодо окремих категорій персоналу. Використання поліграфа у Державній фіскальній службі регламентує наказ Міністерством доходів та зборів України від 02 серпня 2013 р. № 329, «Про використання поліграфів у діяльності Міністерства доходів і зборів України та його територіальних органів» [5]. У Міністерстві оборони використання поліграфа регламентує наказ від14 квітня 2015 р. № 164 «Про затвердження Інструкції про порядок організації та проведення опитування персоналу з використанням поліграфа у Міністерстві оборони України та Збройних Силах України» [6]. Даний наказ був прийнятий у зв'язку з корупцією і державною зрадою чиновників Міністерства оборони України, так і завдяки йому можна буде зменшити роздутий штат міністерства і звільнити тих людей, які не придатні для розбудови обороноздатності країни.

Таким чином, ми вважаємо доцільним, доповнити Кримінальний процесуальний кодекс України статтями, які регламентуватимуть використання слідчим, прокурором поліграфа ще на стадії досудового розслідування, що дасть змогу оптимізувати процес розслідування кримінального провадження, тим самим збільшити ефективність роботи органу досудового розслідування та прокурора.

---

1. Морозова Т.Р. Використання комп'ютерних поліграфів у кадровій роботі органів і підрозділів внутрішніх справ України: навч.-метод.

посіб. / Т.Р. Морозова, І.О. Моцонелідзе, Д.З. Моцонелідзе; за ред. Красюка І.П. – К.: Атіка, 2006. – 120 с.
2. Про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні): Законопроект від 12 березня 2013 р. № 2521 [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46058.
3. Про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні): Законодавча ініціатива народних депутатів України О.С. Барни, Т.З. Юрика, М.В. Люшняка, О.В Ревеги, від 10.12.2015 р. N 3611 [Елекронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua /pls/zweb2/webproc4_1?pf3511=57349.
4. Інструкція щодо застосування комп'ютерних поліграфів у роботі з персоналом органів внутрішніх справ України: Наказ МВС України від 28.07.2004 р. №842 [Електронний ресурс] – Режим доступу: http://zakon5.rada.gov.ua/laws/show/z1373–04.
5. Про використання поліграфів у діяльності Міністерства доходів і зборів України та його територіальних органів: Наказ Міністерством доходів та зборів України від 02.08.2013 р. № 329 [Елекронний ресурс] – Режим доступу: http://zakon3.rada. gov.ua/laws/show/z1748-13.
6. Про затвердження Інструкції про порядок організації та проведення опитування персоналу з використанням поліграфа у Міністерстві оборони України та Збройних Силах України: Наказ МО України від 14.04.2015 р. № 164 [Елекронний ресурс] – Режим доступу:

Програмне забезпечення біометричної аутентифікації за відбитком пальця

Мельник Р.А.,
професор кафедри програмного забезпечення
Національного університету «Львівська політехніка»,
доктор технічних наук, професор
Красниця Т.О.,
здобувач освітнього ступення «магістр»
Національного університету «Львівська політехніка»

Процес верифікації (порівнянням «один до одного», або «один до багатьох») відбитків пальців є доволі простим, але часоємким, якщо розміри БД зареєстрованих шаблонів є значними.

Тому підвищення швидкодії алгоритмів опрацювання відбитків є актуальним.

Програмна система. Вхідними даними є зображення відбитка пальця, взяте із спеціального сканера. Програмне забезпечення для пошуку і обробки зображень відбитків пальців розроблене на мові C#. Основними блоками є модулі знаходження особливих точок та пошуку подібних у базі даних відбитків пальців.

В загальному робота системи буде складатися з наступних кроків (рис.1):

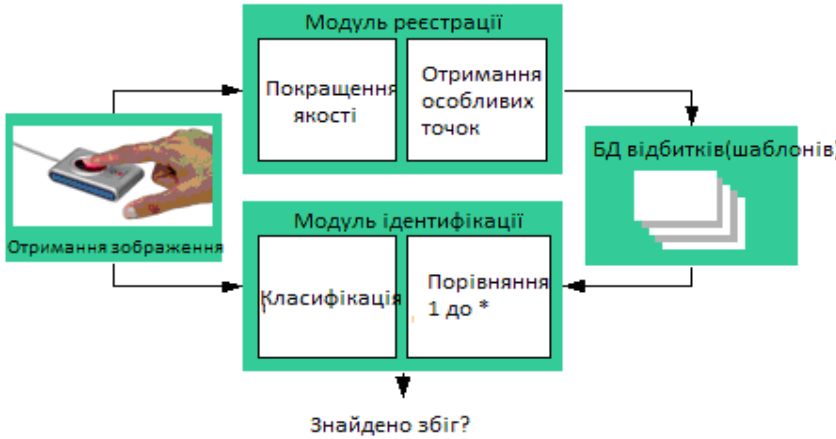


Рис.1. Загальна схема роботи системи

1) отримання вхідного зображення відбитка пальця та покращення його якості;
2) виділення унікальних характеристик, створення шаблону та занесення його в БД для подальшої ідентифікації;
3) пошук схожого шаблону відповідно до ознак.

Скелетизація зображення. Видалення максимального числа пікселів зображення без зміни форми його об'єкту називається скелетонізацією. Іншими словами, після побудови скелетону він повинен допомагати розпізнати саме зображення. Виділяють наступні властивості скелетону: лінії найтонші можливі; всі відрізки зв'язані між собою; каркас розташований в центрі об'єкту спостереження. Приклад зображення букви та його скелетона наведено на рис.2.

Рис. 2. Приклад скелетона

Розглянемо процес побудови скелетону з допомогою алгоритму [1-4}, достатньо простому і формалізованому. Алгоритм працює з бінарними зображеннями. Суть алгоритм полягає в ітераційному скануванні матриці пікселів зображення вікном позицій та поступовій заміні чорних пікселів на білі. Вікно алгоритму має розміри 3×3 або 4×4 позицій. Розглянемо версію алгоритму для вікна сканування розмірами 3×3. Тоді всі пікселі у вікні пронумеровані від p_1 до p_9, як це показано на рис.3.

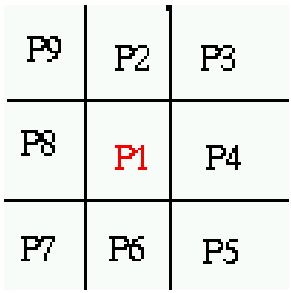


Рис. 3. Нумерація пікселів у вікні сканування

При скануванні рішення про заміну кольору приймається щодо пікселя p_1 (в центрі вікна). Для отримання відповіді на питання чи піксель p_1 темного кольору залишати в скелетоні чи його колір поміняти на білий необхідно обчислити дві функції:

B(p1) = кількість ненульових сусідів для p1 та A(p1) = кількість пар {0,1} в послідовності p2, p3, p4, p5, p6, p7, p8, p9, p2.

Більш яскравим прикладом застосування скелетонів є опрацювання відбитків пальців. Скелетоном усувають надлишкову інформацію та полегшують доступ до особливих точок, які є предметом дослідження та порівняння. На рис. 4 наведено приклад відбитка пальця та його скелетона.

Рис. 4. Відбиток пальця та його скелетони

На скелетоні присутні особливі точки, а саме: розгалуження та початки (кінці) ліній. Розгалуження – це точки, в яких сходять три і більше ліній. Для букв «Y» та «X» особливі точки продемонстровано на рис. 5.

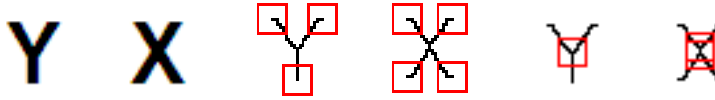


Рис. 5. Особливі точки: кінці ліній та розгалуження

Застосуємо до скелетона відбитку пальця алгоритм знаходження розгалужень та кінців ліній. Отримаємо зображення, на яких квадратами обведені позицій розгалужень (рис. 6*а*) та кінців ліній (рис. 6*б*). На другому скелетоні алгоритмом фіксується також неінформативні початки (кінці) ліній. Вони, зазвичай, не використовуються для формування ознак на розпізнавання.

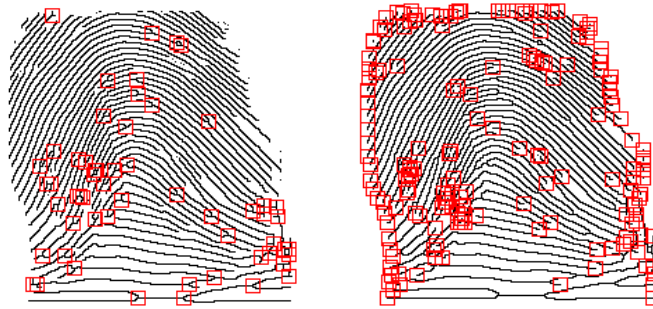


Рис. 6. Знаходження точок розгалужень та кінців ліній

При розбиваванні зображення на різну кількість клітинок отримаємо в них кількість особливих точок (рис, 7).

Рис.7. Сітки з різним кроком

Точність ознаки збільшується при збільшенні кількості клітинок.

Процес ідентифікації відбитка відбувається у Web API. Зображення відбитка зберігається на стороні клієнта, а в базі даних – його шаблон, Це дозволило зменшити розміри бази шаблонів відбитків.

Пошук відбитків. Клієнт-програма з допомогою HTTP протоколу подає запит на сервер, який заносить шаблони відбитків в базу даних, Тобто всі процеси ідентифікації, верифікації відбуваються на стороні сервера. Приклади результатів пошуку і цільові функції представлені на рис. 8.

Рис.8. Результати пошуку вдбитків

Висновок. Розроблено експериментальну програмну систему розпізнавання відбитків пальців. Система передбачає проведення експериментів для дослідження алгоритмів знаходження особливих точок, класифікації шаблонів та пошуку їх в базі даних.

1. Khalid Saeed, Marek Tabędzki, Mariusz Rybnik, Marcin Adamski, 2010. K3M: A universal algorithm for image skeletonization and a review of thinning techniques International. Journal of Applied Mathematics and Computer Science, vol. 20.
2. Danielle Azar, Godfried Toussain, 1997. Hilditch's algorithm for skeletonization, thttp://cgm.cs.mcgill.ca/~godfried/teaching/
3. projects97/azar/skeleton.html
4. Gabriella Sanniti di Baja, Edouard Thiel, 1996. Skeletonization algorithm running on path-based distance maps. Image and Vision Computing vol.14, 47–57.
5. P. Morrison , Ju Jia Zou, 2005. An effective skeletonization method based on adaptive selection of contour points. Proceedings of International Conference on Information Technology and Applications vol.1, 644 – 649.

Аналіз та візуалізація даних на графах

Поберейко Б.П.,
завідувач кафедри автоматизації та комп'ютерно-інтегрованих технологій Національного лісотехнічного університету України, доктор технічних наук, професор
Куклінов А.П.,
здобувач освітнього ступення «магістр» Національного лісотехнічного університет України

В рамках клієнтської сторони розроблено програмну бібліотеку, що здатна візуалізовувати дані у вигляді графа. Бібліотеки такого роду дозволяють без особливих перешкод отримувати дані у зручному для користувача представлені, а саме у вигляді графа.

На сьогоднішній день в основі мережі Інтернет лежать великі об’єми електронного контенту. Декілька років тому, основною проблемою при роботі в мережі було відсутність підходу, який би дозволив без проблем для людини, сприймати великі об’єми

інформації. Наприклад будь-який інформаційний ресурс, що містить статті можна подати у вигляді об'єктів. При цьому посилання на інші статті чи ресурси можуть виступити у вигляді зв'язків. Згідно такого принципу, з'являється можливість представити статті інформаційного ресурсу у вигляді вершин графа, а посилання на інші статті у вигляді ребер. Представлення, та графічне подання соціальних зв'язків між людьми, що взаємодіють між собою, прийнято називати «Соціальний граф». Даний підхід не обмежується лише у поданому прикладі. Його можна застосувати і в багатьох інших галузях. Для прикладу можна навести граф соціальних відносин між людьми, зв'язки між частками будь-якого тіла, посилання між ресурсами у мережі чи звичайний зв'язок декількох комп'ютерів між собою.

При побудові великих систем, що являють собою механізм для соціальної взаємодії між людьми, необхідно покласти в основу деякі принципи. В таких системах, користувач зазвичай повинен здійснювати взаємодію лише з тими людьми, які підпорядковуються категорії спільних інтересів. Завдяки цьому, виникне змога отримання визнання між користувачами, та налагодження нових соціальних зв'язків.

В останні декілька років поряд з визначенням «соціальний граф», виникло поняття «граф інтересів». Даний граф здатний описувати систему, яка складається з користувачів, інтересів, та зв'язків між ними. Якщо в соціальному графі прийнято брати до уваги лише один тип зв'язку, а саме «користувач-користувач», то в графі інтересів визначають такі зв'язки: «користувач-користувач», «користувач-інтерес», «інтерес-інтерес». Граф інтересів утворює нову область в абстракції даних та виглядає соціальний граф, третім виміром якого є шар що визначає сукупність вузлів у вигляді інтересів.

Оскільки на сьогоднішній день є широко розвиненим поняття соціальних зв'язків в мережі, виникає потреба візуалізації даних. Дана потреба пояснюється бажанням людини бачити сукупність даних на площині. Зокрема дану потребу можна пояснити і тим, що користувачу не достатньо отримувати результат у вигляді звичайного текстового виводу. Іншою вагомою причиною використання підходу для візуалізації даних є те, що аналіз користувачем інформації яка представлена у вигляді сукупності

графічних об’єктів відбувається швидше, ніж аналіз великих об’ємів текстової інформації. Процес та результати візуалізації повинні бути як можна простіші, та зрозуміліші для користувача.

Іноді необхідно надати користувачу візуальне зображення графа так, щоб можна було побачити його повноцінну структуру. Це можна застосувати у багатьох прикладах, таких як: представлення класових діаграм, соціального графа, трейдових та даних іншого роду.

Рис.1. Графічне зображення графа

Ідея оптимізації графічного подання графу полягає у зміні представлення зовнішнього вигляду ребра. Це може допомогти у подальшому об’єднанні сукупності ребр в так звані «скрутки», якщо виникне така потреба.

Наприклад, нам необхідно з’єднати дві вершини (*P0 та P4*) ребром, при умові, що початкова та кінцева вершини сполучені за допомогою інших вершин та ребер. У такому випадку нам необхідно буде знайти найкоротший шлях до цільової вершини. При проходженні шляху, потрібно запам’ятовувати пройдені вершини, а саме першу вершину яка йде після початкової і останню вершину за якою слідує цільова вершина.

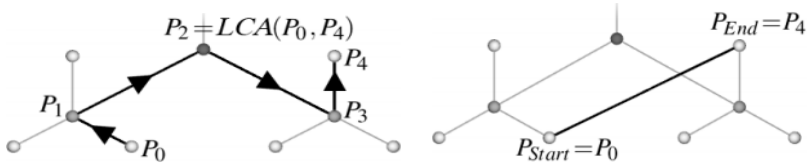


Рис.2. Етапи побудови ребра між вершинами

Останнім кроком є проведення кривої через отримані точки. В більшості випадків, для досягнення даної цілі прийнято використовувати сплайни. Сплайн являє собою набір кривих, що проходять через задані точки. Оскільки при малюванні кривої в JavaScript потрібно зазначати дві або одну контрольні точки, з'являється можливість використати в якості цих точок координати вершини P1 та P3.

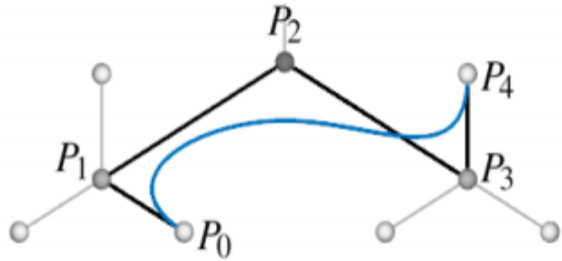


Рис.3. З'єднання вершин кривою

В якості інструменту, для реалізації поставленого завдання була взята мова JavaScript. Дана мова програмування дозволяє без зайвих проблем відображати графічні об'єкти в браузері користувача.

Компонентом, що служить основою для побудови графічних елементів, являється об'єкт Document Object Model який носить назву SVG. Даний компонент базується на векторній графіці. Основними перевагами SVG є: масштабування без втрати якості, кожен графічний об'єкт є елементом DOM що дозволяє з легкістю оперувати ними за допомогою JavaScript, при зміні окремих частин дерева елементів не потрібне повне перемалювання компонента-обгортки.

На рисунку 4 наведене результат візуалізації графа. Даний графічний результат було отримано за допомогою тестових даних у форматі JSON. Розміщення вершин соціального графу відбувається зверху вниз. При отриманні масиву об'єктів, клієнтський скрипт визначає взаємозв'язки між користувачами, які представлені вкладеними об'єктами.

Розміщення вершин соціального графу відбувається рівномірно, а також рівновіддалено один від одної. Така методика дозволить побудувати легке для користувацького сприйняття зображення.

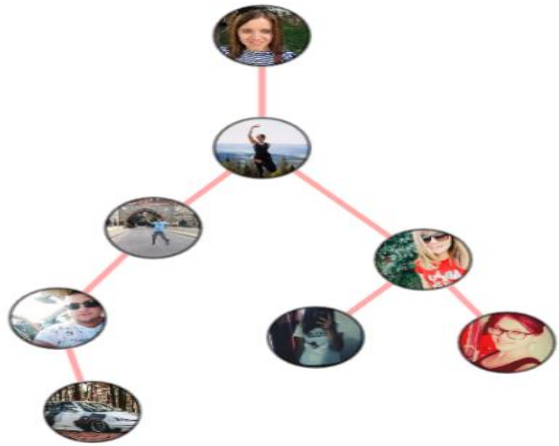


Рис.4. Візуалізація графа

Оскільки візуалізація вершин відбувається через створення окремих DOM елементів, була створена можливість зміни позиції вершин шляхом їх перетягування. Даний процес відбувається шляхом фіксування вершини лівою клавішею миші та подальша зміна позиції курсору миші.

Виконання побудови зв'язку між двома вершинами у вигляді кривої, зображено на рисунку 5. В даному випадку крива має дві контрольні точки, що знаходяться нижче від вершин. Це дозволяє вигнути криву під необхідним кутом. У випадку, якщо бібліотека не мала би даної можливості, ребро з'єднало дві вершини і являло би собою звичайну пряму. На перший погляд це не є проблемою. Але якщо б початкова вершина була би з'єднана з іншими більшою кількістю ребер, малюнок став би складним для сприйняття користувачем.

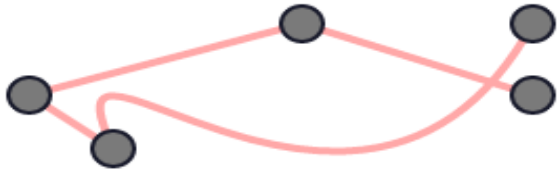


Рис.5. Побудова ребра у вигляді кривої

Візуалізація – потужний інструмент донесення думок і ідей до кінцевого споживача, помічник для сприйняття та аналізу даних. При вмілому застосуванні візуалізація даних дозволяє зробити матеріал вражаючим, не нудним і таким, що запам'ятовується.

1. Mohammed J. Zaki Data mining and analysis / Zaki J. Mohammed, 112 (2014).
2. Wagner Meira Jr. Fundamental Concepts and Algorithms / Jr. Meira Wagner, 120 (2014).
3. Ian H. Witten, Eibe Frank Practical Machine Learning Tools and Techniques, Second Edition / Witten H. Ian, Frank Eibe, 351 (2005).
4. Дэвид Флэнаган – JavaScript. Подробное руководство (JavaScript. The Definitive Guide).
5. Коржинский С.Н. Настольная книга Web-мастера: эффективное применение HTML, CSS и Javascript. – М.:Издательский торговый дом «Кнорус», 2000. – 320с.

Використання апарату вищої математики у задачах мікроекономіки

Саницька А.О.,
викладач Львівського інституту економіки і туризму
Ташак М.С.,
викладач Національного університету «Львівська політехніка»

Теорія виробництва досліджує зв’язок між задіяними у виробництві ресурсами, що взаємодіють між собою у виробничому процесі, та результатом цієї взаємодії – продуктом. Цей зв’язок між затратами та випуском продукції називають виробничою функцією.

Ефективним є виробництво, яке дає змогу випустити заданий фізичний розмір високоякісної продукції за допомогою мінімального обсягу введених ресурсів. Постає проблема: як може фірма виробляти продукцію з мінімальними витратами?

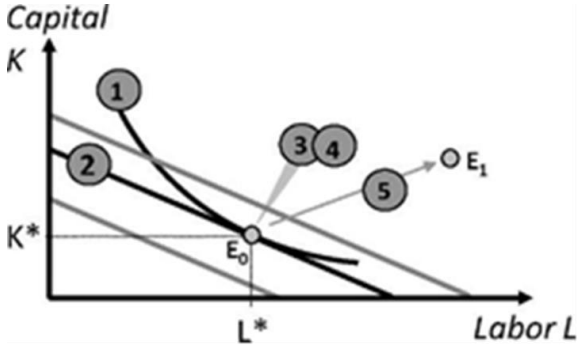
Відомо, що зв’язок між задіяними у виробничому процесі ресурсами та обсягом випуску описується виробничою функцією. Для спрощення припустимо, що фірма використовує для виробництва два ресурси: працю (L) і капітал (K). Виробнича функція

показує взаємозв'язок між затратами праці та капіталу і обсягом вупуску продукції.

Питання знаходження оптимуму може бути вирішене:

- за допомогою ізоквант – кривих, що показують різні комбінації ресурсів, що забезпечують однаковий випуск продукції. (Проблема 1);
- за допомогою ізокост – ліній, що відображають всі можливі поєднання двох ресурсів, які предбачають однакові витрати виробництва. (Проблема 2);
- знаходження аналітично комбінації ресурсів праці та капіталу, що забезпечують мінімальні витрати фірми. (Проблема 3);
- знаходження графічно найнижчої ізокости, що є дотичною до ізокванти для даного виробництва. (Проблема 4);
- знаходження комбінації змінних ресурсів, що мінімізують виробничу функцію, якщо ціни, технології і виробництво змінюються. (Проблема 5).

Графічно огляд проблем (цифри позначають проблеми) має наступний вигляд:



Проблема 1: виробнича функція і ізокванти

Фірма використовує для виробництва два ресурси: працю (*L*) і капітал (*K*).

1. Задано значення: $Z_1 = (2;8)$, $Z_2 = (3; 12)$, $Z_3 = (8;2)$ *і* $Z_4 = (12;3)$ (перше число – кількість праці, друге - кількість капіталу). Знайти для кожної комбінації змінних обсяг випуску продукції *x*. Визначити аналітично рівняння відповідних ізоквант. Намалювати комбінації змінних Z_1,

Z_2, Z_3 *і* Z_4 і відповідні ізокванти (праця - на осі абсцис, капітал - на осі ординат).

2. Обчислити граничну продуктивність обох ресурсів в точках Z_1, Z_2, Z_3 *і* Z_4 . Дати інтерпретацію знайденої граничної продуктивності з точки зору економіки.
3. Обчислити нахил ізоквант в точках Z_1, Z_2, Z_3 *і* Z_4 . Як називається абсолютна величина цього нахилу в економіці?
4. Яке відношення існує між граничною продуктивністю та граничною нормою технологічного заміщення в одній точці? Підтвердити це співвідношення для точок Z_1, Z_2, Z_3 *і* Z_4.
5. Як зміниться ізокванта, коли гранична продуктивність праці підвищується за рахунок подальшої освіти. Який буде ефект цієї зміни на ізокванті для $x = 6$?
6. Як зміниться ізокванта, коли гранична продуктивність капіталу підвищується за рахунок технологічних інновацій. Який буде ефект цієї зміни на ізокванті для $x = 6$?

Розв'язання.

1. Виробнича функція має вигляд: $x(L,K) = L^{0,5}K^{0,5}$

Обсяг випуску продукції у заданих точках $x(2;8) = 2^{\frac{1}{2}} \cdot 8^{\frac{1}{2}} = 4$ становить:

$$x(3;12) = 3^{0,5} \cdot 12^{0,5} = 6,$$

$$x(8;2) = 8^{0,5} \cdot 2^{0,5} = 4,$$

$$x(12;3) = 12^{0,5} \cdot 3^{0,5} = 6.$$

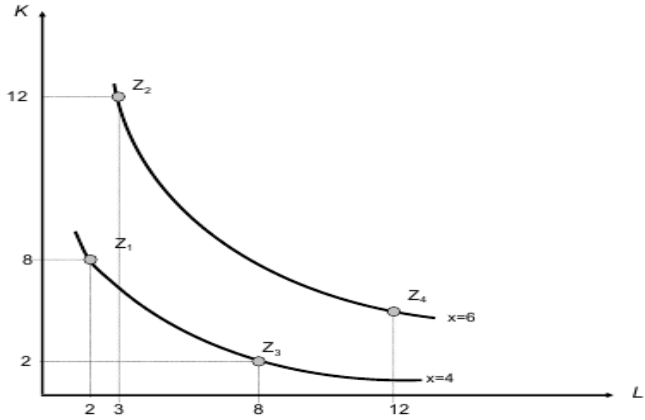
Знайдемо рівняння ізокванти:

$$x(L,K) = L^{0,5}K^{0,5}$$

$$x^2 = L \cdot K \quad \Rightarrow \quad K = \frac{x^2}{L}.$$

$$x = 4 \qquad K = \frac{16}{L},$$

$$x = 6 \qquad K = \frac{36}{L}.$$



2. Гранична продуктивність ресурсу дорівнює першій похідній від виробничої функції по відношенню до цього ресурсу в даній точці:

$$\frac{\partial x(L,K)}{\partial L} = \frac{1}{2} L^{\frac{-1}{2}} K^{\frac{1}{2}} = \frac{1}{2} \frac{K^{\frac{1}{2}}}{L^{\frac{1}{2}}};$$

$$\frac{\partial x(L,K)}{\partial K} = \frac{1}{2} L^{\frac{1}{2}} K^{\frac{-1}{2}} = \frac{1}{2} \frac{L^{\frac{1}{2}}}{K^{\frac{1}{2}}}.$$

Гранична продуктивність ресурсу (Marginal Product, MP) показує на скільки збільшиться обсяг продукції, якщо кількість ресурсу збільшити на одиницю (за умови незмінності другого ресурсу).

Гранична продуктивність праці у заданих точках:

$$\frac{\partial x(L,K)}{\partial L}(2;8) = 1, \qquad \frac{\partial x(L,K)}{\partial L}(3;12) = 1,$$

$$\frac{\partial x(L,K)}{\partial L}(8;2) = \frac{1}{4}, \qquad \frac{\partial x(L,K)}{\partial L}(12;3) = \frac{1}{4}.$$

Гранична продуктивність капіталу у заданих точках:

$$\frac{\partial x(L,K)}{\partial K}(2;8) = \frac{1}{4}, \qquad \frac{\partial x(L,K)}{\partial K}(3;12) = \frac{1}{4},$$

$$\frac{\partial x(L,K)}{\partial K}(8;2)=1,\quad \frac{\partial x(L,K)}{\partial K}(12;3)=1.$$

Отже, у точці (2,8) гранична продуктивність праці дорівнює 1. Якщо даний ресурс збільшити на 1 одиницю, обсяг продукції збільшується на одну одиницю.

3. Розрахуємо нахил ізоквант в точках Z_1 і Z_3 (x=4):

$$\frac{\partial K}{\partial L}=-\frac{16}{L^2};\qquad \frac{\partial K}{\partial L}(2;8)=-4;$$

Для Z_2 *і* Z_4 (x=6):

$$\frac{\partial K}{\partial L}=-\frac{36}{L^2};\qquad \frac{\partial K}{\partial L}(3;12)=-\frac{36}{9}=-4;$$

$$\frac{\partial K}{\partial L}(12;3)=-\frac{36}{144}=-\frac{1}{4}.$$

Абсолютна величина нахилу – це гранична норма технологічного заміщення (MRTS) – показує, на скільки одиниць капіталу повинно використовуватися більше для підтримки незмінного обсягу випуску продукції, якщо кількість праці зменшується на одну одиницю.

Проблема 2

Фірма використовує два взаємозамінних ресурси – працю (L) і капітал (K). Годинна ставка заробітної плати w=4, ціна одиниці фізичного капіталу q=1(придбання та експлуатаційні витрати, процентні платежі). Обчислити рівняння ізоквант для рівня витрат C=16, C=24 (аналітично та графічно). Обчислити нахил ізокост. Як зміниться ізокоста при зростанні капіталу та зменшенні кількості трудових ресурсів?

Розв'язання.

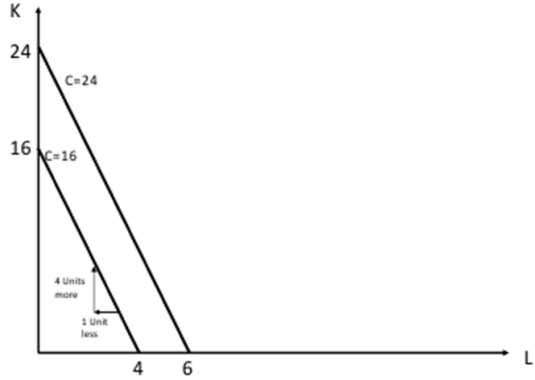
Ізокости – це лінії, що відображають всі можливі комбінації ресурсів, які передбачають однакові витрати виробництва.

$$wL+qK=C\ \Rightarrow\ K=-\frac{w}{q}L+\frac{C}{q}.$$

Якщо C=16, то $4L+K=16,\ K=-4L+16$. Точки перетину з осями координат: L=0, K=16; K=0, L=4.

Якщо C=24, то $4L+K=24,\ K=-4L+24$. Точки перетину з осями координат: L=0, K=24; K=0, L=6.

Графік ізокости має вигляд:



Знайдемо нахил ізокости :

$$K = -\frac{w}{q}L + \frac{C}{q}; \quad \frac{\partial K}{\partial L} = -\frac{w}{q}.$$

Для C=16 $K = -4L + 16, \ \frac{\partial K}{\partial L} = -4.$

Для C=24 $K = -4L + 24, \ \frac{\partial K}{\partial L} = -4.$

Гранична норма заміщення ринку MRMS

$$MRMS = \left|\frac{\partial K}{\partial L}\right| = \left|-\frac{w}{q}\right| = \frac{w}{q}.$$

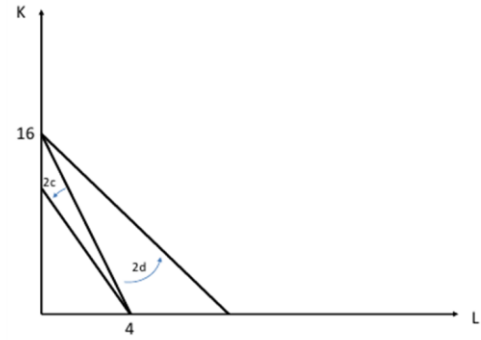
Якщо $K = -4L + 16, \ MRMS = |-4| = 4.$

Для $K = -4L + 24, \ MRMS = |-4| = 4.$

MRMS дорівнює абсолютному значенню нахилу відповідної ізокости.

MRMS показує, на скільки одиниць одного ресурсу буде використано більше, якщо іншого ресурсу використовуватиметься на одну одиницю менше для збереження незмінної ціни.

Якщо зростає ціна капіталу (C=16), то змінюються точки перетину на осі та нахил: відбувається обертання ізокости проти годинникової стрілки. Якщо знижується вартість трудових ресурсів (C=16), то змінюються точки перетину на осі та нахил: відбувається обертання проти годинникової стрілки



Проблема 3

Задана виробнича функція

$$x(L,K) = L^{0,5}K^{0,5}.$$

Ціна трудових ресурсів w=4, ціна капіталу q=1. Використовуючи метод Лагранжа знайти комбінації ресурсів праці та капіталу, що забезпечують мінімальні витрати фірми. Обчислити для рівня виробництва x=4 і x=6.

Сформулюємо задачу умовної максимізації – мінімізувати витрати ресурсів

$$\min_{L,K} C = \min_{L,K}(wL + qK) \text{ при умові } L^{0,5}K^{0,5} = x.$$

Запишемо функцію Лагранжа: $LF = (wL + qK) + \lambda(x - L^{0,5}K^{0,5})$

Знайдемо частинні похідні функції і прирівняємо їх до нуля.

$$\frac{\partial LF}{\partial L} = w - \lambda\frac{K^{0,5}}{2L^{0,5}} = 0, \qquad \frac{\partial LF}{\partial K} = q - \lambda\frac{L^{0,5}}{2K^{0,5}} = 0,$$

$$\frac{\partial LF}{\partial \lambda} = x - L^{0,5}K^{0,5} = 0,$$

Розв'язуємо перше і друге рівняння відносно λ:

$$\lambda = 2w\frac{L^{0,5}}{K^{0,5}}, \quad \lambda = 2q\frac{K^{0,5}}{L^{0,5}}.$$

Тоді $2w\frac{L^{0,5}}{K^{0,5}} = 2q\frac{K^{0,5}}{L^{0,5}} \quad \Rightarrow \quad L = \frac{q}{w}K.$

Підставляємо в третє рівняння вартість мінімального внеску капіталу і знаходимо К:

$$x-(\frac{q}{w}K)^{0,5}K^{0,5}=0,\quad K=x\left(\frac{w}{q}\right)^{0,5}.$$

Вартість мінімальної факторної комбінації для x=4:

$$L^*=x\left(\frac{q}{w}\right)^{0,5}=4\left(\frac{1}{4}\right)^{0,5}=2,\qquad K^*=x\left(\frac{w}{q}\right)^{0,5}=4\cdot 2=8.$$

Для x=6:

$$L^*=x\left(\frac{q}{w}\right)^{0,5}=6\left(\frac{1}{4}\right)^{0,5}=3,\qquad K^*=x\left(\frac{w}{q}\right)^{0,5}=6\cdot 2=12.$$

Знайдемо значення функції витрат, підставляючи знайдені оптимальні значення ресурсів:

$$C(x)=wL+qK=wx\left(\frac{q}{w}\right)^{0,5}+qx\left(\frac{w}{q}\right)^{0,5}=x(wq)^{0,5}+x(wq)^{0,5}=2x(wq)^{0,5}.$$

Для конкретної виробничої кількості:

$$C(x)=2x(wq)^{0,5}\quad\Rightarrow\quad C(4)=2\cdot 4\cdot 2=16,\quad C(6)=2\cdot 6\cdot 2=24.$$

Проблема 4: мінімізація витрат графічно

Враховуючи описані ситуації в проблемах 1 і 3, зважаючи на ізокванти та ізокости, необхідно графічно зобразити скільки праці та капіталу фірма повинна використати для виробництва 4 та 6 одиниць продукції?

Шукаючи на даній ізокванті точку дотику з ізокостою, знаходимо, що при x=4 вартість мінімальної факторної комбінації дорівнює (2,8), а при x=6 ця вартість становить (3,12).

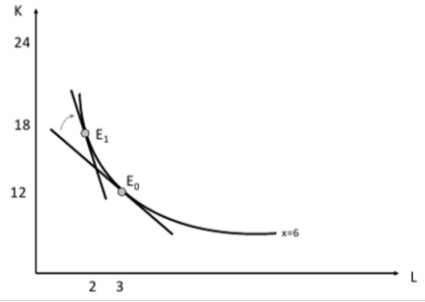
Проблема 5: зміни в оптимальному виробництві

За попередніми даними w=4, q=1. Зміни соціальної системи безпеки призвели до вищої оплати персоналу (цей зріст призвів до w=9). Знайдемо значення ресурсів при x = 6:

$$L^*=x\left(\frac{q}{w}\right)^{0,5}=6\left(\frac{1}{9}\right)^{0,5}=2,\qquad K^*=x\left(\frac{w}{q}\right)^{0,5}=6\cdot 3=18.$$

Новий нахил ізокост $K=-\frac{w}{q}L+\frac{C}{q};\quad MRMS=\frac{w}{q}.$

$$K=-4L+24,\ MRMS=4;\quad K=-9L+36,\quad MRMS=9.$$



Якщо ціновий фактор зміниться, то рівність зміститься на однакову ізокванту.

Використовуємо менше трудових ресурсів, але більше капіталу. Тоді при w=4 і q=1 строгі правила безпеки праці призводять до збільшення експлуатаційних витрат машин. Ціна на фактор капіталу зростає до q=4.

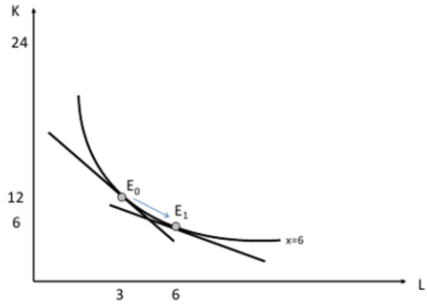
Нова мінімальна вартість комбінаційного фактору при x=6:

$$L^* = x\left(\frac{q}{w}\right)^{0,5} = 6\left(\frac{4}{4}\right)^{0,5} = 6, \qquad K^* = x\left(\frac{w}{q}\right)^{0,5} = 6 \cdot 1 = 6.$$

Новий нахил ізокост (q=1): $K = -\frac{w}{q}L + \frac{C}{q}; \quad MRMS = \frac{w}{q}.$

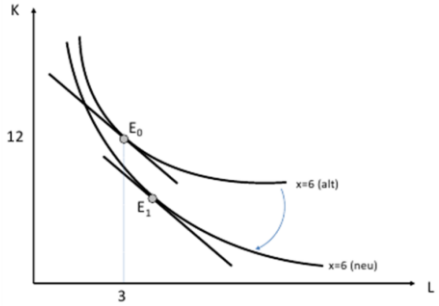
$$K = -4L + 24, \; MRMS = 4, \quad K = -L + 6, \; MRMS = 1.$$

Затрачено більше трудових ресурсів і менше капіталу.



Вища гранична продуктивність праці призводить до більш різкого нахилу ізокванти і встановлює, що для збереження незмінного випуску продукції повинен бути зменшений внесок (праця і капітал). Тому графік повертається у вихідне положення.

Обидва ефекти призводять до таких змін на графіку:



1. Ковальчук Т.В. Виша математика для економістів / Т.В. Ковальчук, В.С. Мартиненко. – Ч.1. – К. : КНТЕУ, 2005.
2. Ковальчук Т.В. Виша математика для економістів / Т.В. Ковальчук, В.С. Мартиненко, В.І. Денисенко. – Ч. 2. – К. : КНТЕУ, 2007.
3. Кремер Н.Ш. Высшая математика для экономистов / Н.Ш. Кремер. – М. : ЮНИТИ, 2001.
4. Красс М.С. Математика для экономических специальностей / М.С. Красс. – М. : Дело-М, 2002.
5. Вітлінський В.В. Моделювання економіки: Навч. посібник / В. Вітлінський – К.: КНЕУ, 2003.
6. Панчишин С.М. Макроекономіка : Навч. Посібник / С. М. Панчишин. – К. : Либідь, 2001.

Програмне забезпечення для розрахунку та налаштування параметрів дослідження камери сушіння деревини

Соколовський Я.І.,
завідувач кафедри інформаційних технологій
Національного лісотехнічного університету України,
доктор технічних наук, професор
Сінкевич О.В.,
здобувач освітнього ступення «магістр»
Національного лісотехнічного університету України

В даній роботі було проведено аналіз основних принципів побудови камер сушіння деревини. На основі проведеного ана-

лізу було реалізовано програму, що дозволяє нам не лише визначати базові геометричні характеристики камер сушіння деревини, але й розраховувати характеристики її компонентів. Окрім цього, програма дозволяє здійснювати автоматичний вибір компонентів камери сушіння деревини, згідно вхідних параметрів, введених користувачем.

Актуальність даної теми пояснюється постійним технологічним розвитком людства, за рахунок якого не зникає потреба у висококваліфікованих фахівцях для розповсюдження та підтримки найрізноманітніших систем в робочому стані. Суттєво прискорити та оптимізувати даний вид діяльності допомагають комплексні системи автоматизованого проектування, котрі дозволяють практично повністю змоделювати процес створення та розповсюдження продукції з подальшою її підтримкою.

Основним завданням створеного програмного забезпечення являється оптимізація розмірів лісосушильної камери чи її компонентів, що в свою чергу дозволяє нам здійснювати перебудову лісосушильної камери шляхом зміни вхідних даних, та представляти результати її роботи у вигляді збірки програми SolidWorks.

Програмне забезпечення було реалізовано за допомогою мови програмування C # в середовищі програмування Microsoft Visual Studio 2010.

Вкладка введення вхідних даних

Одним з головних завдань програми являється отримання базових вхідних даних, які вводить користувач. В подальшому ці дані будуть використовуватися для проведення розрахунку, результати якого дозволять програмі вибрати параметри компонентів камери для сушіння деревини. Вхідні дані вводять у першій вкладці головного вікна програми, вигляд якої наведено на рисунку 1.

Ця вкладка дозволяє здійснювати такі операції:

- вибирати породу деревини;
- вказувати відстань до країв камери сушіння деревини;
- встановлювати висоту від штабелів до фальшстелі;
- встановлювати висоту піддонів та відстань між штабелями;
- вказувати загальну кількість штабелів;
- задавати необхідну кількість пиломатеріалів в одному штабелі;

- вибирати тип розмірів та вказувати їхні значення;
- отримувати характеристики всіх прокладок між пиломатеріалами;
- здійснювати розрахунок параметрів лісосушильної камери згідно вхідних даних.

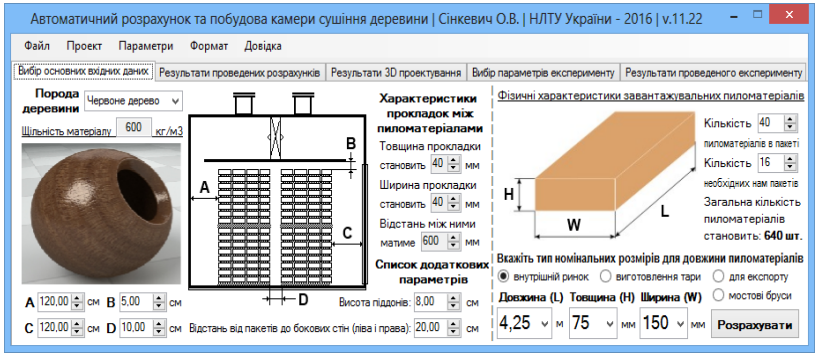


Рис.1. Вкладка введення вхідних даних

Програма розроблена таким чином, щоб бути максимально зрозумілою для користувача, тому вона містить лише основні параметри, які необхідні для вдалого виконання поставленого завдання. В разі необхідності користувач може скористатися довідковою системою, яка вбудована безпосередньо у програму і тому не потребує з'єднання з інтернетом. Окрім цього програма відповідає існуючим стандартам у галузі деревооброблювальних технологій, що дозволяє використовувати реальні розміри для проведення розрахунків і проектування компонентів лісосушильної камери.

Вкладка результатів розрахунку

Для того, щоб спроектувати компоненти для камери сушіння деревини, користувач повинен ознайомитися, і в разі необхідності внести зміни в ряд параметрів, значення яких програма визначає автоматично, виходячи із заданих вхідних даних. Значення цих параметрів наведено у другій вкладці головного вікна програми, вигляд якої наведено на рисунку 2.

Згідно цієї вкладки ми бачимо, що наша програма буде автоматично визначати наступні параметри:

- сушильний простір спроектованої камери (довжина, висота, ширина, об'єм);

- корпус сушильної камери (довжина, висота до фальшстелі, ширина, товщина стін);
- фальшстеля сушильної камери (висота, ширина проходів, розміри припливно-витяжних каналів);
- система теплопостачання (тип калорифера, кількість, візуалізація, перегляд характеристик);
- система зволоження повітря (тип форсунок, кількість, перегляд характеристик);
- система вентиляції повітря (тип вентилятора, кількість, візуалізація, перегляд характеристик).

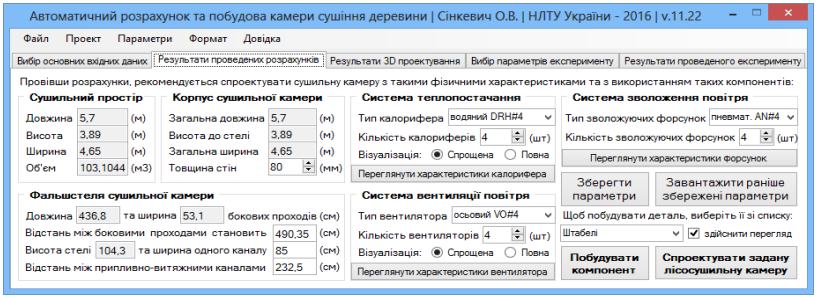


Рис.2. Вкладка результатів розрахунку

Автоматичне визначення параметрів сушильної камери відбувається програмно, і залежить насамперед від сушильного простору, значення якого розраховується згідно вхідних даних.

Визначивши параметри, користувач може повністю побудувати камеру сушіння деревини, або один компонент, вибравши його зі списку і натиснувши відповідну кнопку.

Процес побудови є автоматичний і здійснюється шляхом використання прикладного інтерфейсу SolidWorks API. Для реалізації всіх необхідних нам функціональних можливостей було використано компоненти трьох базових бібліотек SolidWorks, які є передумовами використання макросів.

Вкладка результатів 3D-проектування

Результати побудови лісосушильної камери та її компонентів, а також їхній перелік можна переглянути у третій вкладці, вигляд якої наведено на рисунку 3.

За допомогою цієї вкладки здійснюються такі операції:

- відкривання деталей чи збірок solidworks;

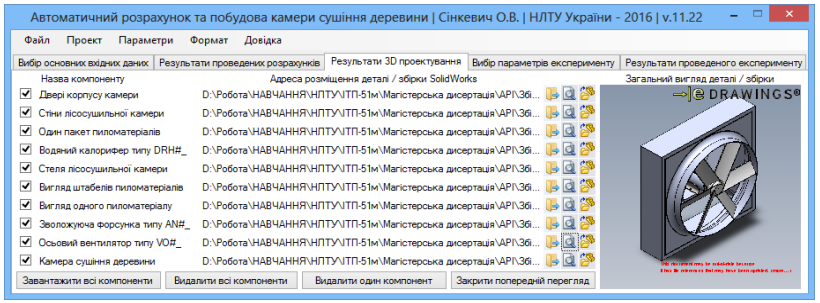


Рис.3. Вкладка результатів 3D-проектування

- редагування документів шляхом їхнього відкриття;
- завантаження нових документів;
- видалення одного чи більше документів;
- перегляд завантажених деталей чи збірок;
- отримання інформації про завантажені документи.

Пройшовши третю вкладку ми маємо усі необхідні нам компоненти лісосушильної камери і тепер можемо приступати до створення та налаштування нового дослідження.

Вкладка вибору параметрів експерименту

Дана вкладка служить для надання інформації щодо створення нового або налаштування існуючого експерименту у середовищі гідро-газо-динамічних досліджень SolidWorks Flow Simulation. Наприклад на рисунку 4 наведено вигляд вибору початкових умов дослідження при створенні нового проекту. Варто зауважити, що усі наведені у цій вкладці налаштування застосовуються до раніше спроектованої лісосушильної камери.

Висновки

В результаті виконання роботи було розроблено програмне забезпечення, що дозволяє нам визначати параметри лісосушильної камери, здійснювати їхнє 3D проектування, а також надавати інформацію щодо створення та налаштування нових проектів дослідження SolidWorks Flow Simulation.

Виконавши роботу можна підкреслити її значущість, адже робота такого типу дозволяє краще зрозуміти сутність процесу моделювання, проектування та дослідження роботи лісосушильних камер, що дозволяє в подальшому суттєво зекономити час та матеріальні ресурси при підготовці реальних проектів з метою їх впровадження на ринки збуту.

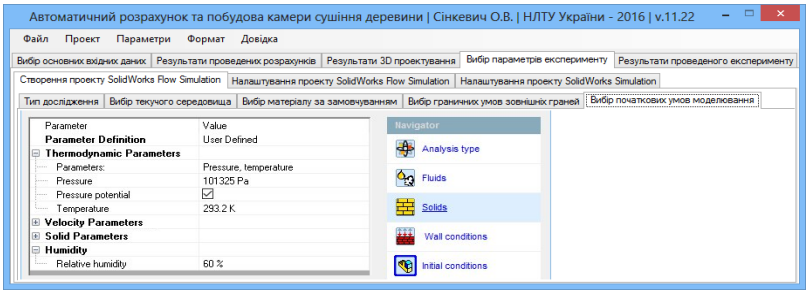


Рис.4. Вкладка вибору параметрів створення проекту

1. [Сайт роботи з Microsoft VS] – http://www.msdn.microsoft.com
2. [Сайт роботи з SolidWorks] – http://www.fsapr2000.ru
3. Наталя Дударєва, Сергій Загайко «SolidWorks 2009 на прикладах» «БХВ». – Санк-Петербург, 2009 рік – 530 с.
4. Прохороенко В.П. SolidWorks. Практическое руководство – М.: ООО «Бином-Пресс», 2004 рік – 448 с.
5. Білей П. В. Теоретичні основи теплової обробки і сушіння деревини. – Київ: Видавництво «ВІК», 2005. – 360 с.
6. Сінкевич О.В. Розроблення програмного забезпечення для проектування лісосушильної камери за допомогою інтерфейсу SolidWorks API // Advanced computer information technologies : Матеріали VI Всеукраїнської школи-семінару молодих вчених і студентів ACIT'2016, 20-21 травня 2016 р., Тернопіль, Україна – ТНЕУ, 2016. – С. 153-155.

Математичне та програмне забезпечення розподіленої САПР гідрологічної системи

Соколовський Я.І.,
завідувач кафедри інформаційних технологій Національного лісотехнічного університету України, доктор технічних наук, професор
Дубанич О.П.,
здобувач освітнього ступення «магістр»
Національного лісотехнічного університету України

Вода необхідна для життя на Землі. Вона має першочергові соціальні та економічні цінності, тому її використання буде істотно впливати на розвиток нашого суспільства. Збалансоване

управління та охорона навколишнього водного середовища є однією з ключових проблем 21-го століття, і чисельні імітаційні моделі в значній мірі будуть сприяти її вирішенню. Чисельні моделі знищують прірву між системами чи доменами і фізичними процесами. Вони можуть моделювати фізичні процеси, що стосуються потоку і транспортування води, а також інших рідин і речовин в різних гідро- і екологічних системах, а також можуть робити прогнозування. Для вирішення цих важливих проблем, існує нагальна необхідність у розробці та застосуванні ефективних імітаційних моделей, що складаються з ефективних чисельних методів, пов'язаних з ефективними методами обробки інформації. Саме тому в даній роботі було розроблено сервер-орієнтовану CAD систему для моделювання процесів в гідрологічному середовищі.

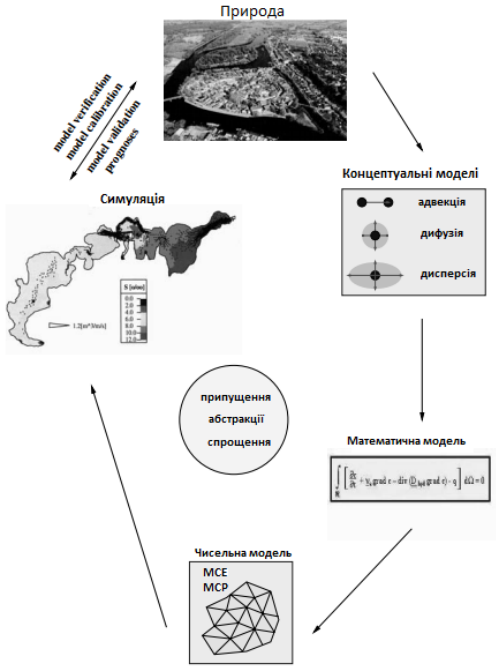


Рис. 1. Концептуальна модель

Програмна реалізація

Аби вирішити поставлене завдання, було розроблено ПЗ, що складається з двох частин: сервера та клієнта.

Серверна частина має наступний функціонал:

- збирання та обробка вхідних даних для розрахунків та моделювання;
- моделювання процесів, що беруть участь в гідрологічних системах;
- зберігання результатів моделювання у БД;
- надання зрозумілого API для взаємодії із різноманітними додатками;
- можливість отримання з сервера інформації про проведене дослідження за датою чи ключовими словами;
- засоби експорту результатів у популярні формати.

Взаємодія клієнтського додатку із сервером відбувається за допомогою API, що надається останнім. Всі запити виконуються за REST архітектурою.

Отож, клієнтський додаток використовує API сервера для надсилання інформації до вирішувачів чисельних методів для подальшого процесу моделювання, а також для управління задачами на сервері і отримання результатів виконання останніх.

Серверна частина була розроблена на платформі .Net 4.5 і Web API 2. Архітектуру клієнт-серверної взаємодії розробленого ПЗ можна побачити на рис. 2.

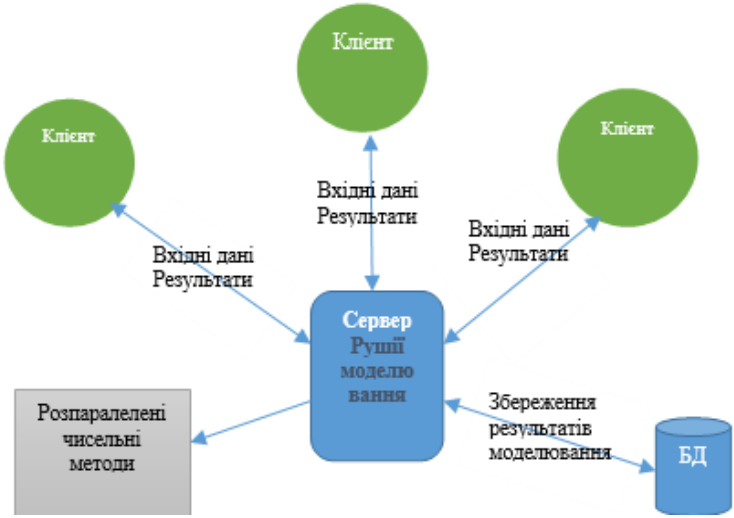


Рис. 2. Архітектура ПЗ

В результаті цієї роботи була розроблена САПР для розподілених обчислень чисельних методів у процесах, що мають місце в гідрологічних системах і був створений веб-сайт для відправки завдань на сервер для довготривалого імітаційного моделювання. Додатково, сервер виконує складні розрахунки, використовуючи розпаралелені алгоритми чисельних методів. Саме тому розроблене ПЗ має високу ефективність при роботі з великими обсягами вхідних даних, тому що воно використовує всі переваги мультипроцесорних систем. Приклад результату моделювання показано на рис. 3.

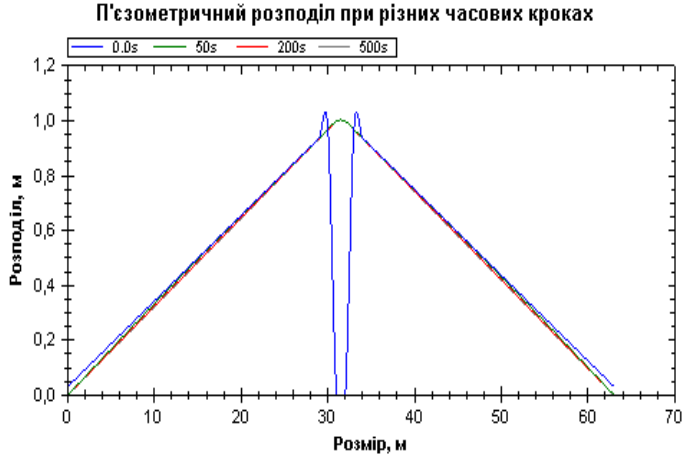


Рис. 3. Результати моделювання

---

1. Hinkelmann R (Efficient Numerical Methods and Information-Processing Techniques for ModelingHydro- and Environmental Systems), 2005. – 81- 217 с.
2. A. V. Starchenko, V. N. Bertsun «Parallel computing methods», 2013. – 430 с.
3. Herbert Shield, «C# 4.0. The complete reference». 2011. – 234-289, 401-408 с.
4. Andrew Troelsen, Pro C# 5.0 and the .NET 4.5 Framework, 2015. – 23-89 с.

Сучасні проблеми дослідження криміналістичних особливостей кіберзлочинів

Усатий О.О.,
здобувач освітнього ступення «магістр»
Одеського державного університету внутрішніх справ
Ісмайлов К.Ю.,
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ,
кандидат юридичних наук

Процеси глобалізації виводять економічні відносини на принципово новий інформаційний рівень взаємодії. З розширенням впливу транснаціональних корпорацій розвивається і транснаціональна злочинність, об'єктом і предметом якої стають засоби комп'ютерних технологій. Від своєчасності і правильності виявлення їх особливостей безпосередньо залежить ефективність проведення слідчих (розшукових) дій, спрямованих на розкриття даного виду злочинів.

Кількість кіберзлочинів щороку зростає як на території України, так і в усьому світі. Актуальність боротьби з даним видом злочинів, а також їх розслідування і розкриття, мають пріоритетне значення для всієї держави, але з огляду на його специфічність виникають проблеми дослідження особливостей кіберзлочинів.

При дослідженні криміналістичних особливостей злочинів в сфері інформаційних технологій можна виділити ряд проблемних питань:

- висока латентність;
- складність збору доказів і процесу доказування, так як з'явився новий вид сліду, а саме «віртуальний слід»;
- широкий спектр криміналістично значущих ознак злочинів;
- відсутність єдиної програми боротьби з кіберзлочинами;
- складність розслідування комп'ютерних злочинів;
- відсутність узагальненої судової та слідчої практики у провадженнях даної категорії.

Для вирішення зазначених проблем необхідно виділити криміналістично значущі елементи характеристики кіберзлочинів:

- спосіб вчинення злочину;
- особливості слідової інформації;
- особливості обстановки скоєння злочину (місце скоєння злочину, час вчинення злочину та ін.);
- особистісна характеристика злочинця;
- особливості безпосереднього предмета злочинного посягання.

Спосіб вчинення злочину в криміналістиці є системою взаємообумовлених, рухливо детермінованих дій, спрямованих на підготовку, вчинення і приховування злочинів, пов'язаних, з використанням відповідних знарядь і засобів, а також часу, місця і інших обставин об'єктивної обстановки скоєння злочину.

У криміналістичній літературі можна зустріти безліч класифікацій способів скоєння комп'ютерних злочинів. Крилов В.В. наводить опис можливих способів порушення конфіденційності і цілісності комп'ютерної інформації без їх класифікації:

- розкрадання носіїв інформації у вигляді блоків і елементів ЕОМ;
- копіювання інформації;
- копіювання документів з вихідними даними;
- запам'ятовування інформації;
- фотографування інформації в процесі її обробки;
- виготовлення дублікатів вхідних і вихідних документів;
- використання недоліків програмного забезпечення та операційних систем;
- підміна елементів програм і баз даних.

Кіберзлочини залишають специфічну слідову картину: на місці події можна виявити як «традиційні» сліди, так і комп'ютерні сліди (віртуальні, комп'ютерно-технічні сліди), що залишаються в пам'яті електронних пристроїв.

Під віртуальними слідами розуміють сліди скоєння будь-яких дій (включення, створення, відкривання, активації, внесення змін, видалення) в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем і мереж [1, с. 47].

Будь-які дії з комп'ютерними або іншими програмованими пристроями (мобільними телефонами, смартфонами, планшетами і т.д.) отримують своє відображення в пам'яті, наприклад:

- в журналах адміністрування, журналах безпеки відображаються такі дії як включення, виключення, різні операції з вмістом пам'яті комп'ютера;
- в реєстрі комп'ютера відображаються дії з програмами (установка, видалення, зміна і т.д.);
- в log-файлах відображаються відомості про роботу в мережі Інтернет, локальних та інших мережах;
- у властивостях файлах відображаються останні операції з ними (наприклад, дата створення, останніх змін).

Віртуальні сліди можуть послужити доказами незаконного проникнення в пам'ять комп'ютера або іншого пристрою (злому), створення, використання і поширення шкідливих комп'ютерних програм, здійснення або підготовки скоєння злочину особою або групою осіб.

Обстановка місця скоєння злочину знаходиться в тісному зв'язку зі способом скоєння злочину і особистістю злочинця, так як спосіб вчинення злочину вибирається злочинцем з урахуванням можливої обстановки, в якій воно буде відбуватися, і конкретизується з урахуванням реально сформованої обстановки. Обстановка вчинення злочину може змінюватися під впливом застосованого злочинцем способу вчинення злочину.

Стосовно даного виду злочинів це перш за все означає, що спосіб вчинення комп'ютерного злочину буде визначатися найбільш характерними складовими обстановки:

- місцем і часом дії злочинця;
- особливостями організації інформаційної безпеки;
- можливостями порушення цілісності комп'ютерної інформації без безпосередньої участі людини;
- рівнем кваліфікації фахівців, що забезпечують захист інформації, а також адміністрування комп'ютерних мереж.

На сьогоднішній день одним з найбільш проблемних питань є визначення місця події. При вчиненні одного злочину, наприклад, неправомірного доступу до комп'ютерної інформації, може бути кілька місць події:

- робоче місце, робоча станція – місце обробки інформації, що стала предметом злочинного посягання;
- місце постійного зберігання або резервування інформації – сервер або стример;

- місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що знаходиться в іншому місці, при цьому місце використання може збігатися з робочим місцем, але перебувати поза організацією (наприклад, при сторонньому зломі шляхом зовнішнього віддаленого мережевого доступу);
- місце підготовки злочину (розробки вірусів, програм зламу, підбору паролів) або місце безпосереднього використання інформації (копіювання, поширення, спотворення), отриманої в результаті неправомірного доступу до даних, що містяться на ПК [2, с. 112].

Місцем події може бути одне приміщення, де встановлено комп'ютер і зберігається інформація, ряд приміщень, в тому числі в різних будівлях, розташованих на різних територіях, або ділянки місцевості, з якого проводиться дистанційний електромагнітний або аудіо перехват.

Також цікавим є питання, про те, чим же є кіберпростір і яке місце воно займає в криміналістичній характеристиці?

Найчастіше мережа Інтернет використовується як засіб скоєння злочину. Мережа може бути застосована для отримання інформації, що полегшує вчинення злочину, наприклад, відомостей про те, як створити вибуховий пристрій або виготовити складний синтетичний наркотик в домашніх умовах. З іншого боку можна застосувати кіберпростір для поширення незаконних матеріалів, інформації, в такому випадку він використовується для знаходження покупців, для пересилки інформації, і грошових коштів і таким чином використовується безпосередньо для здійснення суспільно небезпечного діяння. Саме використання глобальної мережі дозволяє в даному випадку створити розширену мережу збуту і сприяє як настанню злочинного результату, так і дозволяє залишити цю діяльність поза увагою правоохоронних органів.

При вчиненні злочину за допомогою кіберпростору можна говорити, що застосована нова сукупність прийомів, методів, послідовність дій, яка надає злочину унікальні властивості, не характерні для злочинів без використання мережі. Звісно ж, що в такому трактуванні вчинення злочину за допомогою Інтернет, сама мережа і є способом злочину [3, с. 92], і в той же час інформаційний простір є засобом як сукупність предметів і процесів

матеріального світу. Таке подвійне значення інформаційного простору під час скоєння злочину можливе завдяки його природі, яке є одночасно набором принципів, алгоритмів, правил взаємодій і в той же час воно реалізовано в матеріальному світі у вигляді сукупності з'єднаних комп'ютерів.

Виходить, що у випадках, коли кіберпростір безпосередньо використовується для вчинення злочину, він є способом і засобом одночасно, а в інших – лише засобом. Можна зробити висновок, що при скоєнні злочинів за допомогою кіберпростору змінюється його характеристика.

Також кіберпростір виступає не тільки засобом, а й місцем скоєння злочину, що досить сильно ускладнює процес розслідування комп'ютерних злочинів. В такому випадку традиційні способи огляду місця події вже не підходять, необхідна розробка та опрацювання абсолютно нової методики розслідування і розкриття кіберзлочинів, відповідно до властивостей із характерними особливостями Інтернет-простору.

1. Крылов В. В. Информационные компьютерные преступления : [учеб. и практ. пособие] / Крылов В. В. – М. : ИНФРА-М, 1997. – 276 с.
2. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : монографія / [И.Р. Шинкаренко и др.]. – Донецк : РВВ ЛДУВС, 2007. – 267 с.
3. Хахановський В.Г. Особливості криміналістичної характеристики кіберзлочинів / В.Г. Хахановський // Юридичний часопис Національної академії внутрішніх справ. – 2011. – № 1(1). – С. 89-93.

Застосування деяких аспектів аналітичної геометрії у задачах економіки

Фірман Л.Ю.,

старший викладач кафедри природничо-математичних дисциплін та інформаційних технологій Львівського інституту економіки і туризму

Рівняння лінії є найважливішим поняттям аналітичної геометрії. Найпростішою лінією на площині є пряма. Щоб скласти

рівняння прямої лінії на площині, треба певним способом задати умови, які визначають положення прямої відносно координатних осей. Пряму на площині відносно системи координат можна задати, наприклад, двома різними точками, точкою та напрямом (вектором), точкою та вектором, перпендикулярним до прямої, або іншими способами. Таких способів кілька, тому ми можемо дістати рівняння прямої в різних формах.

Існують такі види рівняння прямої на площині:

1. Рівняння прямої, що проходить через дану точку перпендикулярно до заданого вектора.
2. Рівняння прямої, що проходить через дану точку в заданому напрямі (рівняння пучка прямих).
3. Канонічне рівняння прямої.
4. Рівняння прямої, що проходить через дві задані точки.
5. Рівняння прямої з кутовим коефіцієнтом.
6. Рівняння прямої у відрізках.
7. Загальне рівняння прямої.

У цій доповіді будемо використовувати три останні із згаданих видів рівняння прямої на площині, тобто

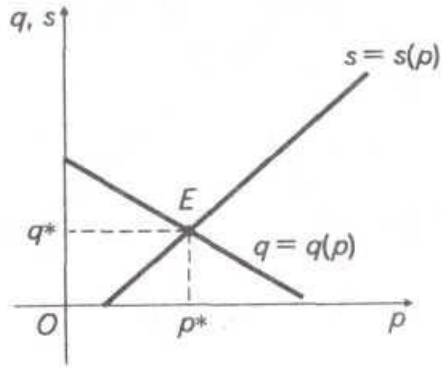
- рівняння прямої з кутовим коефіцієнтом.
- рівняння прямої у відрізках.
- загальне рівняння прямої.

Розглянемо першою **модель рівноваги ринку**, в якій основними є співвідношення між двома величинами: ціною одиниці товару та обсягом товару на ринку. Розглянемо ціну одиниці товару та обсяг товару як упорядковану пару чисел і поставимо їй у відповідність точку з координатами на площині.

Позначимо через $s(p)$ число одиниць товару, які пропонують для продажу продавці, тоді $s = s(p)$ функція пропозиції товару. Через $q(p)$ позначимо число одиниць товару, які покупці бажають купити, тоді $q = q(p)$ – функція попиту на товар.

З економічних міркувань функція пропозиції $s = s(p)$ зростаюча, а функція попиту $q = q(p)$ спадна.

Означення 1. Ціну, за якої попит на певний товар дорівнює пропозиції цього товару на ринку, називають **рівноважною ціною**. Тобто за рівноважної ціни виконується рівність $s(p^*) = q(p^*)$. Точку $E(p^*; q^*)$ називають **точкою рівноваги.**



Розглянемо таку задачу. Нехай задані лінійні функції $s(p)=bp-a$ та $q(p)=c-dp$, функція $s=s(p)$ визначає пропозицію, а функція $q=q(p)$ попит на певний товар на ринку. Треба знайти рівноважну ціну.

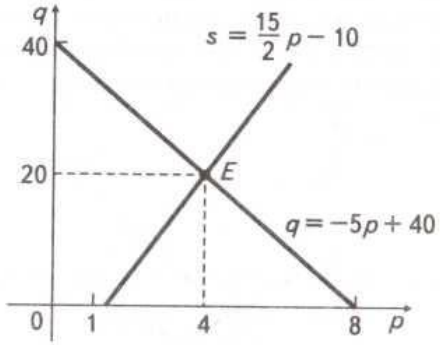
Якщо відсутні всілякі податки, то рівноважна ціна визначається як розв'язок рівняння $s(p^*)=q(p^*)$ або системи рівнянь $\begin{cases} s^*=bp^*-a \\ q^*=c-dp^*. \end{cases}$

Звідси

$$bp^*-a=c-dp^* \quad \Rightarrow \quad p^*(b+d)=a+c \quad \Rightarrow \quad p^*=\frac{a+c}{b+d}.$$

Приклад 1. а) Знайдіть точку рівноваги, якщо функції пропозиції і попиту мають вигляд

$$s(p)=\frac{15}{2}p-10 \quad \text{і} \quad q(p)=-5p+40.$$



Знайдемо точку рівноваги.

$$p^* = \frac{a+c}{b+d} = \frac{10+40}{\frac{15}{2}+5} = \frac{50\cdot 2}{25} = 4,$$

$$s^* = q^* = -5\cdot 4 + 40 = 20.$$

Е (4;20) –точка рівноваги (рівноважна ціна).

б) Як зміняться рівноважна ціна та обсяг товару, якщо встановлений акцизний податок Т=1 грн./одн.?

У цьому випадку функція пропозиції зміниться і задаватиметься співвідношенням

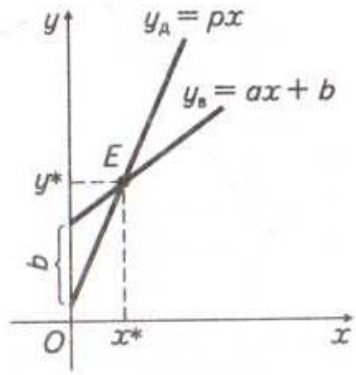
$$s^T = \frac{15}{2}(p-T)-10 \quad \text{і} \quad q^T = -5p+40.$$

А функція попиту залишиться незмінною. Тоді нову точку рівноваги визначаємо з умов рівноваги $s(p^T) = q(p^T)$. Отже, нова рівноважна ціна збільшиться $p^T = 4 + \frac{3}{5}T = 4{,}6$ *грн.*

Обсяг товару зменшується: $s^T = q^T = 20 - 3T = 17.$

Розглянемо далі **модель рівноваги доходів і збитків компаній.**

Компанія випускає продукцію і продає її за ціною *p* (грн.) за одиницю. Встановлено, що загальні щомісячні витрати на виготовлення продукції y_B змінюються за законом: $y_B = ax + b$ де *x* − кількість продукції.



Знайдемо **точку рівноваги, області прибутків і збитків компанії.**

Дохід від продажу x виробів продукції за ціною p за одиницю визначається функцією доходу $y_Д = px$. Отже, для рівноваги доходів і витрат потрібно, щоб виконувалась умова $y_Д = y_B$, тобто знаходимо розв'язок рівняння

$$px^* = ax^* + b \quad \Rightarrow \quad x^* = \frac{b}{p-a}.$$

Отже, точка рівноваги

$$E\left(\frac{b}{p-a}; \frac{pb}{p-a}\right).$$

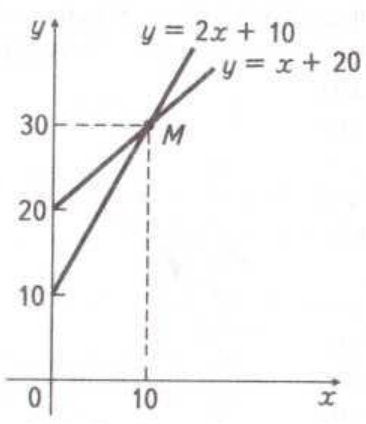
Розглянемо коли компанія отримує прибуток, а коли збитки. Прибуток компанії визначається рівністю

$$P = y_Д - y_B = px - ax - b = x(p-a) - b.$$

Якщо $0 \le x \le x^*$, то графік функції доходу проходить нижче за графік функції витрат і компанія несе збитки.

Якщо $x > x^*$, то графік функції доходу проходить вище за графік функції витрат і компанія одержує прибуток.

Приклад 2. Транспортні витрати на перевезення одиниці вантажу залізничним транспортом виражаються функцією $y = 2x + 10$, а автомобільним транспортом $y = x + 20$, де x вимірюється десятками кілометрів. На які відстані вигідніше перевозити вантажі залізничним і автомобільним транспортом?



Знайдемо точку перетину прямих. Графічний аналіз функцій витрат дає змогу зробити такі висновки.

Якщо x<100км, то транспортні витрати на перевезення вантажу автомобільним транспортом нижчі ніж залізничним;

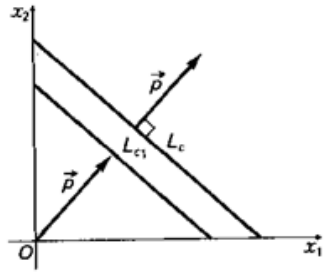
Якщо x>100 км, то рентабельнішим є залізничний транспорт.

Також ми можемо використовувати поняття рівняння

прямої на площині в **бюджетних множинах й лініях бюджетного обмеження.**

Розглянемо *n*-вимірний простір товарів С. Нехай задано вектор цін $\vec{p} = \left(p_1, p_{2,\ldots}, p_n \right)$. Тоді ціна набору товарів $\vec{x} = \left(x_1, x_{2,\ldots}, x_n \right)$ є скалярним добутком цих векторів: $C\left(x \right) = \vec{p} \cdot \vec{x} = \sum_{i=1}^{n} p_i x_i$.

Для простоти розглянемо простір двох товарів. Легко побачити, що набори товарів, котрі мають однакову ціну $C\left(x \right)$, це множина точок, які утворюють частину прямої L_c, заданої рівнянням $p_1 x_1 + p_2 x_2 = c$ і розміщеної в першому квадранті (оскільки $x_1 \geq 0$, $x_2 \geq 0$) перпендикулярно до вектора цін.



Якщо $C_1 < C$, то пряма L_c, задана рівнянням $p_1 x_1 + p_2 x_2 = c_1$, паралельна прямій L_c і лежить ближче до початку координат.

Нехай зафіксовано деяку грошову суму R, яку ми називатимемо бюджетом (або доходом).

Означення 2. Множину всіх наборів товарів, ціна яких не перевищує R, називають **бюджетною множиною** й позначають $B\left(p, R \right)$.

Бюджетну множину можна визначити за допомогою звичайних або векторних нерівностей

$$B(p,R)=\{x\in C; p_1x_1+p_2x_2\le R,\ x_1\ge 0,\ x_2\ge 0\}$$

Означення 3. **Мережею бюджетної множини G** називають множину наборів товарів, які мають ціну рівно R.

Межу бюджетної множини можна визначити за допомогою звичайних або векторних рівностей

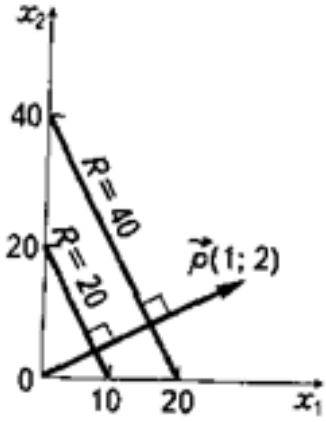
$$G(p,R)=\{x\in C: p_1x_1+p_2x_2=R\}$$

Якщо простір товарів дво- або тривимірний , то бюджетну множину можна зобразити наочно.

Приклад 3. Розглянемо бюджетні множини за різних цін p і бюджетів (або доходів) R.

Якщо задано бюджет R=20 умовних грошових одиниць і вектор цін $\vec{p}=(2;1)$, то бюджетна множина задається нерівністю $2x_1+x_2\le 20,\ x_1\ge 0$.

Будуємо межу бюджетної множини: це буде пряма, задана рівнянням $\frac{x_1}{10}+\frac{x_2}{20}=1$. Враховуємо, що $x_1\ge 0,\ x_2\ge 0$.

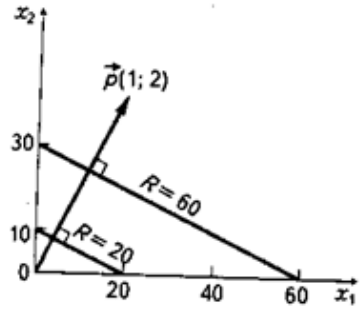


У випадку, коли R=40, а $\vec{p}=(2;1)$, бюджетна множина

$$B(p,40)=\{(x_1,x_2): 2x_1+x_2\le 40,\ x_1\ge 0,\ x_2\ge 0\},$$

а її межа

$$G(p,40)=\left\{(x_1,x_2):\frac{x_1}{20}+\frac{x_2}{40}=1\right\}.$$



При R=20, а $\vec{p}=(1;2)$, бюджетна множина

$$B(p,\ 20)=\{(x_1,x_2):x_1+2x_2\le 20,\quad x_1\ge 0,\quad x_2\ge 0\},$$

а її межа

$$G(p,20)=\left\{(x_1,x_2):\frac{x_1}{20}+\frac{x_2}{10}=1\right\}.$$

При R=60, а $\vec{p}=(1;2)$, бюджетна множина

$$B(p,60)=\{(x_1,x_2):x_1+2x_2\le 60,\quad x_1\ge 0,\quad x_2\ge 0\},$$

а її межа

$$G(p,60)=\left\{(x_1,x_2):\frac{x_1}{60}+\frac{x_2}{30}=1\right\}.$$

Із рисунків видно, що межею бюджетної множини буде відрізок між осями координат у першому квадранті, перпендикулярний до вектора цін.

Очевидно, що бюджетна множина $B(p,R)$ залежить від цін p і бюджету (доходу) R. У разі збільшення бюджету R межа бюджетної множини паралельно рухається в напрямі від початку координат. При зменшенні цін бюджетна множина також зменшується.

На завершення зазначимо, що поняття, які було введено в цій доповіді, можуть бути використані в теорії оптимального планування, лінійного програмування та в мікроекономіці.

1. Грисенко М.В. Математика для економістів: Методи і моделі, приклади й задачі: Навч. посібник. – К.: Либідь, 2007 р.
2. Бугір М.К. Математика для економістів. – К., «Академія», 2003р.

Проблеми використання програмного забезпечення як засобу оперативної техніки оперативними підрозділами поліції

Хараберюш І.Ф.,
професор кафедри права та публічного адміністрування
Маріупольського державного університету,
доктор юридичних наук, професор

У Закон України «Про Національну поліцію» надає повноваження поліції здійснювати оперативно-розшукову діяльність (п. 26 ст. 23 Закону). Цей пункт опосередковано надає право певним суб'єктам поліції використовувати оперативну техніку взагалі і засоби для негласного отримання інформації зокрема. Також в цьому Законі (п. 2 ст. 25) поліція в рамках інформаційно-аналітичної діяльності може використовувати інформаційні системи, які також відносяться до засобів спеціальної (оперативної) техніки. Крім того ми бачимо, що ст. 40 дає право поліції для забезпечення публічної безпеки і порядку використовувати автоматичну фото- і відеотехніку, що також може бути використано її оперативними підрозділами для отримання необхідної інформації. Однак прямого припису щодо використання поліцією науково-технічних засобів щодо реалізації своїх повноважень в Законі немає, що, ми вважаємо, потребує його введення.

Чинний Кримінальний процесуальний кодекс України суттєво покращує можливості використання технічних засобів та результатів їх застосування у кримінальному провадженні. Дійсно, матеріали засобів фіксування кримінального провадження можуть бути джерелами доказів у якості *документів* (п. 2 ст. 84 КПК України) або *додатками* до протоколу процесуальної дії (п. 3 ч. 2. ст. 105), які значно доповнюють його зміст або повністю

замінюють його текст за умови, що жоден з учасників процесуальної дії не наполягає на протилежному (п. 2. ст. 104).

Далі ми знаходимо підтвердження значущості оперативної техніки у визначенні кримінальним процесуальним законом поняття *документу*, під яким розуміється спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків (наприклад, протокол), *звуку, зображення* (матеріали фотозйомки, звукозапису, відеозапису та *інші носії інформації*) тощо відомості, які можуть бути використані як доказ факту чи обставини, що встановлюються під час кримінального провадження [1, ч. 1 п. 2 ч. 2 ст. 99]. Але існує ряд проблем, які ускладнюють процес використання окремих засобів оперативної техніки та результатів її застосування у кримінальному провадженні та оперативно-розшуковій діяльності.

Проводячи аналогію між оперативно-технічними заходами (ОТЗ) та негласними слідчими (розшуковими) діями (НСРД), ми повинні підкреслити, що усі вони проводяться за допомогою оперативної техніки, яка у відповідності до Закону України «Про оперативно-розшукову діяльність» є прерогативою оперативних підрозділів. Нагадаємо, що під оперативною технікою ми розуміли спеціальну техніку, яка використовується в оперативно-розшуковій діяльності правоохоронних органів щодо протидії злочинності, тобто сукупність технічних, програмно-технічних та програмних засобів, автоматизованих систем, спеціальних пристроїв, речовин та науково обґрунтованих тактичних прийомів та способів, що використовуються правоохоронними органами із суворим дотриманням законності з метою виконання завдань оперативно-розшукової діяльності [2, с. 85-86].

В умовах дії чинного Кримінального процесуального кодексу функція оперативної техніки дещо змінилася. Тому ми пропонуємо нове визначення цього виду спеціальної техніки. Оперативна техніка – це сукупність оперативно-технічних засобів та науково обґрунтованих тактичних прийомів та способів їх використання із суворим дотриманням законності з метою виконання правоохоронними органами завдань оперативно-розшукової діяльності та кримінального провадження.

Суттєве значення має проблема інструментарію, у вигляді програмного забезпечення, використовуваного при проведенні ОТЗ та НСРД «Зняття інформації з електронних інформаційних систем». Так, сучасні реалії процесу поширення програмного забезпечення в рамках співдружності незалежних держав свідчать про те, що практично повсюдно використовується неліцензійне або несертифіковане програмне забезпечення, у тому числі й у діяльності правоохоронних органів. Така обставина може мати досить негативне значення при оцінці судом результатів цих заходів і дій, експертизи або огляду комп'ютерної техніки з використанням неліцензованого програмного забезпечення.

Рішення вищевказаної проблеми програмно-технічного забезпечення можливо двома способами. Перший реалізується придбанням спеціального програмного забезпечення, розробленого закордонними компаніями (наприклад, EnCase, Knoppix-STD, Penguin Sleuth Kit і ін.), які спеціалізуються на виготовленні такого програмного продукту. Другий шлях, найбільш доцільний, вирішення проблеми програмно-технічного забезпечення правоохоронних органів – створення національними підприємствами необхідного програмного забезпечення, ліцензованого, сертифікованого і спеціально призначеного для вирішення експертних досліджень, оперативно-розшукових і негласних слідчих (розшукових) дій. Для цього потрібно визначитись з розробниками або створити відповідні підрозділи в структурі СБ України.

Підводячи підсумок можемо констатувати, що протидія злочинам оперативними підрозділами поліції вимагає застосування оперативної техніки в ОТЗ та НСРД, які повинні проводитись визначеними законодавством суб’єктами з використанням ліцензійних та сертифікованих засобів негласного отримання інформації.

1. Кримінальний процесуальний кодекс України. Закон України «Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям КПК України» станом на 02 липня 2012 року: (Відповідає офіц. текстові). – К.: Алерта, 2012. – 304 с.
2. Хараберюш І.Ф. Протидія злочинності засобами спеціальної техніки: концептуальний підхід: монографія / І.Ф. Хараберюш. – Донецьк: Вид-во «Ноулідж», 2011. – 362 с.

Застосування БПЛА для підвищення ефективності роботи правоохоронних органів

Цибуляк Б.З.,
професор кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат фізико-математичних наук, доцент
Дідун П.Л.,
курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Дворічний досвід проведення бойових дій на сході України довів необхідність застосування сучасних методів розвідки, стеження, патрулювання, коригування вогнем із застосуванням БПЛА. Ситуативно діяльність підрозділів МВС часто є подібною до бойової роботи ЗСУ: проведення операцій національної гвардії, приборкання заворушень у місцях багатотисячного скупчення людей на стадіонах, у розважальних закладах, на вулицях та площах міст, проведення спецоперацій затримання злочинців із застосуванням зброї тощо. Ефективність роботи правоохоронних органів у таких випадках буде суттєво залежати від попередньої підготовки проведення операції, розстановки сил та засобів, своєчасного отримання інформації про реальний стан справ на місці події, організації управління під час виконання поставлених завдань.

Зазвичай, для виконання завдань під час проведення спеціальних операцій підрозділами МВС створюється оперативний штаб для управління силами і засобами. Його функції полягають у необхідності оперативно відстежувати зміни в обстановці та відпрацьовувати варіанти коригування рішення командира.

Під час ліквідації масових заворушень можуть застосовуватися кілька підрозділів МВС, що виконують різнопланові завдання окремо один від одного у складі зведеного загону. Крім того, обстановка може дуже динамічно змінюватись. Тому питанням своєчасного отримання достовірної інформації із місця виконання завдання в режимі реального часу є надзвичайно актуальним.

Як показує досвід багатьох європейських держав, США та Ізраїлю, комплекси БПЛА уже давно використовуються у їхніх

правоохоронних органах. Наприклад, у підрозділах МВС Російської Федерації ще з літа 2006 року під час проведення спеціальних операцій для оперативності та достовірності отримання інформації у режимі реального часу ефективно використовуються комплекси безпілотних літальних апаратів 7AI.A 424-04 [1].

Ці апарати оснащені системою автоматичного керування, яка дозволяє задавати маршрут, контролювати й коригувати політ у режимі реального часу. Система спостереження, установлена на апаратах, може виконувати на безпечній для операторів відстані такі завдання як моніторинг місцевості, охорона територій, відеоспостереження за найнебезпечнішими ділянками доріг з метою запобігання аваріям і терористичним атакам, обстеження територій, об'єктів чи важкодоступних місць на предмет можливого мінування або руйнування тощо.

Такі БПЛА не лише супроводжують всі масові заходи в Москві, виконуючи фотографування й відеоспостереження за скупченнями людей з повітря, а й проводять патрулювання у звичайний час.

На жаль, навіть позитивний досвід використання малої авіації та поодиноких БПЛА у 2010 році, коли протягом одного місяця вдалося виявити та знищити понад 250 наркоплантацій із використанням досить обмежених ресурсів не став переконливим аргументом впровадження у підрозділи МВС окремих груп, що могли б ефективно застосовувати потенціал безпілотників для спрощення виконання багатьох завдань безпекової галузі.

Під час проведення заходів масштабу Євро-2012 була розроблена спільна стратегія безпеки фінальної частини Чемпіонату Європи з футболу, викладена у відповідній Декларації про співпрацю, яку підписали міністри внутрішніх справ України та Польщі [2]. Вона передбачала проведення двома державами низки синхронних дій у галузі розбудови безпекової інфраструктури та впровадження сучасних технологій у діяльність правоохоронних відомств. Аби така стратегія позитивних змін втілювалася через поступальне виконання окремих тактичних завдань й була налагоджена тісна комунікація і фаховий діалог поміж згаданими міністерствами.

Під час однієї з робочих зустрічей представники польської поліції продемонстрували своїм українським колегам можливості

передової технології застосування під час проведення спецопера-цій, розвідки, контролю за масовими акціями і спортивними захо-дами безпілотних літальних апаратів. Наприклад, один комплекс з 3-4 БПЛА може забезпечувати безперервне цілодобове спосте-реження у тактичній зоні площею у кілька сотень квадратних кілометрів.

Отже, перспектива застосування БПЛА у сьогоднішній роботі правоохоронних органів є беззаперечною. Необхідно наганяти втрачені десятиліття. Досвід застосування різних типів таких апаратів у проведенні АТО показує, що на сьогодні є нагальна потреба у розробці та впровадженні власної поліційної мікроавіації, яка на відміну від військових апаратів, спрямованих в основному на знищення ворога, має максимально сприяти затриманню об'єкта і його збереженню для подальшого процесу правосуддя, а також проведенню відеоспостереження і передачі у режимі он-лайн інформації, виконувати доставку вантажу та ін. в інтересах правоохоронних органів. Тому у системі МВС необхідно створити підрозділи з розвідувальними комплексами на базі БПЛА та на час проведення спеціальної операції залучати їх до складу зведених загонів. Паралельно слід впроваджувати засоби захисту від зловмисників, наприклад, магніторезонансні установки, які здатні навіть без пострілу нищити ворожі БПЛА.

Інший аспект проблеми – використовувати мікроавіацію правоохоронцям як засіб моніторингу й керування ситуацією закон не забороняє, але й не допомагає. В Україні досі не розроблене правове поле застосування відеоматеріалів, отри-маних із БПЛА, щоб вони могли стати доказами у процесі судових розглядів.

---

1. Українська мікроавіаційна армада: коли виліт? / Електронний ресурс. http://www.imzak.org.ua/articles/article/ id/4534
2. Слідкувати за правопорядком під час ЄВРО-2012 міліції допомага-тимуть… безпілотні літаки / Електронний ресурс. https://www.npu.gov.ua/uk/publish/printable_article/231165

Формування поверхні деревних волокнистих матеріалів

Шабатура Ю.В.,
завідувач кафедри електромеханіки та електроніки
Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор
Дулепа Н.В.,
здобувач освітнього ступення «магістр»
Національного лісотехнічного університету України

В даний час, у світовій промисловості використовується настільки велика кількість всіляких САПР, що, напевно, немає такого підприємства, заводу або конструкторського бюро, в якому б не використовувалися САПР.

Значне поширення спричинило за собою створення програмних комплексів САПР, які включають в себе можливості відразу декількох різновидів. Найбільш часто в таких програмних комплексах зустрічаються різні системи об'ємного моделювання та експрес-тестів. Одною з популярних САПР у наш час є SolidWorks, яка і використовується в даній роботі.

Цей легкий в освоєнні засіб дозволяє інженерам-проектувальникам швидко відображати свої ідеї в ескізі, експериментувати з елементами і розмірами, а також створювати моделі і докладні креслення.

В даній роботі продемонстровано як можна використовувати САПР для формування поверхні деревних волокнистих матеріалів із заданими параметрами.

На сьогоднішній день деревина є цінною екологічно чистою виробничою сировиною, тому його використання є актуальним і широко використовуються. Рівна якість поверхні є основною характеристикою формування кінцевого продукту. Обробка ширини та глибини заготовки залежить від основного енергетичного показника, такого як потужність. Базуючись на вищесказаному, актуальним є розроблення системи автоматизованого проектування формування поверхні деревних волокнистих матеріалів із заданими параметрами.

Ціллю даної роботи є формування поверхні деревних волокнистих матеріалів із заданими параметрами.

Об'єктом дослідження даної роботи є етапи формування кінцевого продукту.

Предметом дослідження визначення швидкості різання та потужності відповідних верстатів на кожному етапі формування кінцевого продукту.

В результаті виконання даної роботи було спроектовано етапи побудови кожного кінцевого продукту та проміжні вигляди заготовок на кожному з етапів її обробки. Для кожного верстату було визначено швидкість різання та його потужність. Також було описано технологічний процес для виготовлення меблевого щита.

Технологічний процес складається з таких етапів:

1. Розпилюємо колоду на лісопильній рамі марки РД75-2 на необрізну дошку.
2. Перероблюємо необрізну дошку на обрізну дошку на кромко-обрізному круглопилковому верстаті марки ЦД3.
3. Формуємо товщини заготовок на двобічному рейсмусовому верстаті марки С2Р12.
4. Нарізаємо зубчастий шип на бокових кромках дощок на фрезувальному верстаті марки ФС-1.
5. Склеюємо заготовки у меблевий щит.
6. Формуємо товщини меблевого щита на двобічному рейсмусовому верстаті марки С2Р12.

Потужність під час різання круглими пилками визначимо за формулою:

$$N_{д.р.} = K_T * a_{попр} * F(V_S/60) * i \text{ , [Вт].}$$

Для визначення табличного значення питомої роботи різання K_T розрахуємо співвідношення:

$$K_T * S_Z = (N_{д.р.} * \eta_{м.р.} * 60 * 1000) / (a_{попр} * b_{пр} * h * i * z * n),$$

де

$N_{д.р.}$ – потужність двигуна механізму різання, [Вт];

$\eta_{м.р.}$ – коефіцієнт корисної дії механізму різання верстата;

$a_{попр}$ – поправковий множник, який враховує умови процесу різання, який визначаємо за формулою:

$$апопр = an * aρ * aw * aб * av * ah ,$$

де

a_n – поправковий множник на породу деревини,
a_ρ – поправковий множник на затуплення інструменту,
a_w – поправковий множник на вологість деревини,
$a_б$ – поправковий множник на кут різання,
a_v – поправковий множник на швидкість різання,
a_h – поправковий множник на висоту пропилу;
$b_{пр}$ – ширина пропилу [мм], визначаємо за формулою:

$$bпр = s + 2 * s1,$$

де
s – товщина диска, [мм]
s1 – розширення зубчастого вінця, [мм];
$h_{пр}$ – висота пропилу, [мм];
i – кількість пилок;
z – кількість зубців, [шт];
n – частота обертання круглої пилки, [$хв^{-1}$].

В підсумку можна зробити висновок про те, що формування поверхні деревних волокнистих матеріалів із заданими параметрами дозволяє отримати розрахунок швидкості різання та потужності верстатів. Розроблена програма дає можливість зобразити етапи побудови кінцевого продукту та проміжні вигляди заготовок на кожному з етапів.

1. Альбом кінематичних схем деревообробних верстатів: М.Д. Кірик, В.В.Шостак, О.О. Волошинський, А.С. Григор'єв, В.І. Тарас; Редакційно видавничий центр НЛТУ України, 2006. – 115 с.
2. Деревообробні верстати загального призначення: Підручник / В.В.Шостак, Я.І. Савчук, А.С. Григор'єв та ін.; За ред. В.В. Шостака. – К.: Знання, 2007. – 279 с.
3. Кірик М.Д. Механічне оброблення деревини та деревних матеріалів. Підручник для вищих навчальних закладів. – Львів, КН, 2006. – 412 с.
4. Худяков В. А. Деревообрабатывающие станки и работа на них. – М.: Лесн. пром-сть, 1982. – 324 с.
5. Шумега С. С. Спеціальна технологія меблевого виробництва. – К.: Вища шк. Головне вид-во, 1981. – 242 с.
6. Шумега С. С. Технология столярно-мебельного производства. – М.: Лесн. пром-сть, 1984. – 265 с.
7. Шостак В.В., Пишніх І.М. «Технічна експлуатація і ремонт деревообробного обладнання». – Київ; 1990, – 232с.

Розроблення програмного комплексу дистанційної діагностики несучої здатності деревних конструкцій в САПР

Шабатура Ю.В.,
завідувач кафедри електромеханіки та електроніки
Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор
Стась С.В.,
здобувач освітнього ступення «магістр»
Національного лісотехнічного університету України

В останні роки в розробці клієнт-серверних програм стає популярною тенденція «тонкого» клієнта і «товстого» сервера. Суть підходу полягає в тому, щоб перенести більшість логіки на сторону сервера, а клієнт в основному займається лише введенням-виведенням. Цей підхід надає гнучкість для системи оновлення версій ПЗ, тому що оновлення відбувається на сервері і стає доступним відразу всім користувачам даного ПЗ.

Метою даної роботи є вдосконалення способу аналізу несучої здатності деревних конструкцій таким чином, щоб програмний комплекс, який буде вирішувати дану задачу, був повністю незалежним від конкретник САПР і таким чином міг легко інтегруватися в будь яку з них засобоми протоколу розробленого за стандартом RESTful API, що в кінцевому результаті надає системі великої гнучкості і вирішує проблему портування під конкретну платформу чи ОС.

Отже використання клієнт-серверного підходу вирішує проблему підтримки декількох версій одночасно і доставлення нових версій до кінцевого клієнту.

Реалізація

В даному проекті використовується акустичний метод діагностики деревини. Його суть полягає у посиланні аудіо імпульсу до деревини і аналізі сигналу, який повернеться у відповідь. Перевірити отриманий сигнал з записами з бази данних кожен з яких відповідає певному стану деревини (тріщини, пошкодження шкідниками, тощо).

Кінцевий вигляд системи:

1. Система отримує аудіо запис і тип деревини через RESTful API.
2. Система здійсює пошук аудіо у базі данних, який відповідає типу пошкодження або ж навпаки хорошому стану деревини.
3. Повертає відповідь клієнту через API.

Пошук аудіо

Отже ключовим елементом роботи є пошук за аудіо.

Кроки пошуку аудіо:

1. Перетворення аудіо у спектрограму.

Для цього аудіо розділяється на короткі відрізки. Далі ці відрізки використовуються для визначення частоти сигналу.

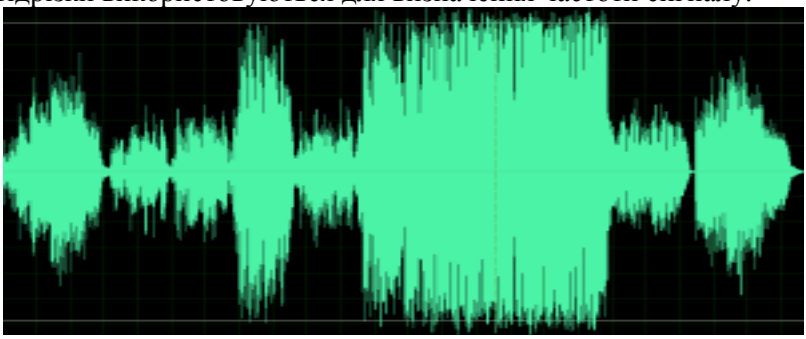


Рис.1. Перетворення аудіо у спектограму

2. Пошук ключових точок.

Так як і люди мають відпечатки пальців, ключові точки аудіо є унікальними ідентифікаторами аудіо сигналу.

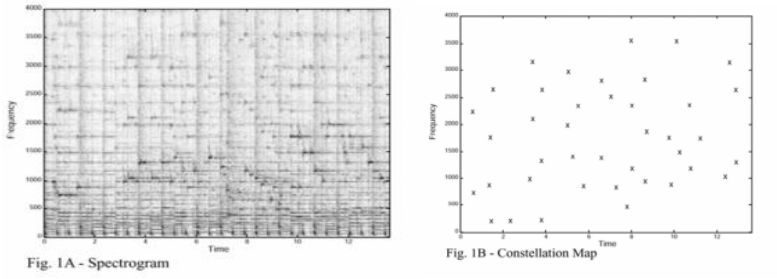


Рис.2. Пошук ключових точок

3. Хешування.

Хеш таблиця складається обчисленням ключових аудіо і часу, коли вони мають місце у аудіо сигналі. Далі ці дані запаковуються в 32 бітові числа, які зберігаються в хеш таблиці.

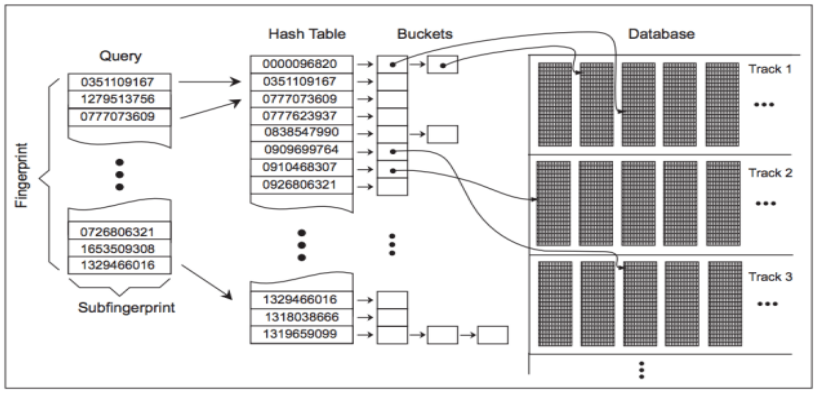


Рис.3. Хешування

4. Пошук за хешем у базі даних.

Можна зробити висновок, що розроблювана система володіє такою перевагою як легка інтегрованість – її можна легко інтегрувату у будь-яка САПР шляхом виклиуів RESTful API. Таким чином САПР, яка буде використовувати дану систему, може використовувати будь-яку платформу і це ніяк не завадить інтегації системи діагностики несучої здатності деревини.

1. Кисельов М.М., Крисаченко В.С., Гардащук Т.В. Методологія екологічного синтезу. Єдність людини та природоохоронних аспектів. – К.: Наук. думка. – 1995. – с. 122-123
2. Van Cooten, Cornelis. Land resource economics and sustainable development/ – Van Cuver, 1993, pp.79.
3. A Review of Algorithms for Audio Fingerprinting (P. Cano et al. In International Workshop on Multimedia Signal Processing, US Virgin Islands, December 2002)
4. Content-Based Retrieval of Music and Audio by Jonathan Foote, ISS, National University of Singapore.
5. Avery Li-Chun Wang and Julius O. Smith, III., WIPO publication WO 02/11123A2, 7 February 2002, (Priority 31 Ju

Система знешкодження безпілотних розвідувальних апаратів на основі їх опромінення ультракороткими радіоімпульсами

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

Ідея використання безпілотних літальних апаратів (БПЛА) для вирішення задач розвідки відома уже досить давно. Такі літальні апарати створювалися і використовувалися насамперед в збройних силах провідних країн світу ще у минулому столітті, однак лише в останнє десятиліття у зв'язку з бурхливим розвитком електроніки, інформаційних та телекомунікаційних технологій розпочалося масове створення і використання безпілотних літальних апаратів різноманітних типів і конструкцій. Сьогодні ці здебільшого малогабаритні, а тому малопомітні і практично невразливі типовими засобами протиповітряної оборони літальні апарати здатні виконувати практично будь-які задачі розвідки, а в окремих випадках вони можуть і безпосередньо наносити вогневі ураження.

Таким чином задача знешкодження малогабаритних літальних апаратів сьогодні є надзвичайно актуальною і важливою. Над її вирішенням працюють вчені багатьох країн світу, вони розробили і запропонували чимало варіантів її вирішення, однак усі вони мають суттєві недоліки, які пов'язані або з високою вартістю їх застосування, або з їх низькою ефективністю.

Попередній аналіз показує, що дана задача знешкодження БПЛА є комплексною, вона включає в себе кілька важливих аспектів – самостійних задач, серед яких потрібно виділити задачу виявлення БПЛА, причому бажано до моменту вирішення ворожим безпілотником розвідувальної задачі і задачу визначення місцеположення БПЛА, принаймні кутовий сектор і відстань

до нього, тому зупинимося більш детально на вирішенні безпосередньо задачі ураження БПЛА.

Ураження БПЛА може здійснюватися за кількома варіантами: знищення шляхом механічного пошкодження; дезорієнтація; зіпсування бортової електроніки; засліплення оптичних скануючих систем; примусова посадка. Сьогодні основним варіантом залишається механічне пошкодження. Воно здійснюється на основі застосування вогнепальної зброї. Однак практика показує, що збити таку малорозмірну ціль як безпілотник є вкрай важкою задачею, яка вимагає використання значної кількості боєприпасів і має вкрай низьку ймовірність успішного виконання.

Сьогодні стали відомими окремі розробки засобів боротьби з БПЛА, які не пов'язані з використанням вогнепальної зброї. Зокрема це система дистанційної дезорієнтації БПЛА відома під назвою «гвинтівка DroneDefender». Її загальний вигляд показано на рис.1.

Рис.1. Гвинтівка DroneDefender

Аналіз відкритих публікацій свідчить, що дана гвинтівка генерує сигнал на частотах систем супутникової навігації і здатна дезорієнтувати БПЛА, який використовує ці системи на відстані до 400 м. Час підготовки до здійснення «пострілу» DroneDefender

складає всього 0,1 секунди, загальна вага пристрою 4,5 кг. Розробники стверджують, що DroneDefender може використовуватися як стаціонарно так і в портативному варіанті за рахунок використання додаткового акумулятора. Зрозуміло, що для БПЛА військового призначення цей пристрій може виявитися мало ефективним, крім того його потреба в надійному і потужному джерелі живлення накладає серйозні обмеження для його застосування в бойових умовах.

Пропонується новий підхід до створення пристроїв знешкодження БПЛА на основі їх опромінення потужними радіоімпульсами, які виведуть з ладу їх бортову електроніку. Ідея такого підходу є давно відомою і базується на явищі електромагнітної індукції відкритому ще Фарадеєм. Для практичної реалізації необхідно створити направлений і дуже потужний електромагнітний імпульс. Очевидно, що при обмеженому енергетичному ресурсі підвищення потужності є можливим лише за рахунок компресії часу виділення енергії, тобто зменшення протяжності імпульсу.

Загальна структура запропонованої системи приведена на рисунку 2.

Рис.2. Загальна структура пропонованої системи

Оригінальні науково-технічні рішення закладені в кожній структурній частині даної системи. Енергетичною основою системи є джерело живлення. За його основу вирішено взяти надійне і добре перевірене часом джерело енергії що розсіюється при пострілах стрілецької зброї. Воно створюється на основі лінійного електромагнітного генератора, який приводиться в рух пороховими газами від стрілецької зброї, завдяки спеціальній насадці, яка накручується на ствол. Спрощений вигляд насадки в розрізі показано на рисунку 3.

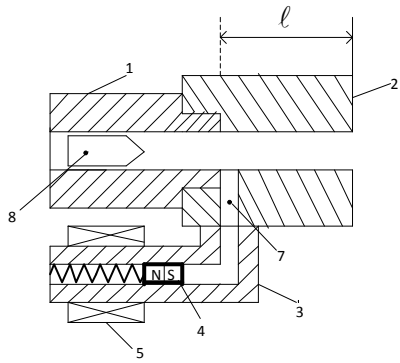


Рис.3. Насадка в розрізі

На рисунку прийняті наступні позначення: 1 дульна частина ствола стрілецької зброї; 2 корпус насадки загвинченої на ствол, яка подовжує канал ствола на довжину ℓ; 3 газовідвідний патрубок; 4 постійний магніт в оболонці, який контактує з пружиною 6; 5 обмотка нерухомого статора лінійного генератора; 7 газовідвідний канал; 8 куля в каналі ствола.

Пристрій діє наступним чином. В момент часу коли куля під дією порохових газів досягає газовідвідного каналу насадки, порохові гази через канал 7 починають штовхати магніт 4 в результаті чого він заходить в котушку 5 де в результаті зміни магнітного поля відбувається створення електрорушійної сили. Для збільшення амплітуди коливань обмотку 4 підключено до обмотки підвищувального трансформатора. Спрощена еквівалентна схема електромагнітної системи лінійного генератора показана на рис. 4

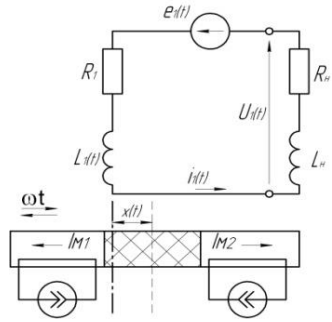


Рис.4. Еквівалентна схема лінійного генератора.

На показаній схемі $L_1(t), R_1$ – індуктивність і активний опір робочої обмотки; L_H, R_H – – індуктивність і опір навантаження; $e_1(t)$ – ЕРС, яка наводиться в робочій обмотці.

Згідно еквівалентної електромагнітної схеми можна записати рівняння електричної рівноваги:

$$e_1(t) = i_1(t)(R_1 + R_H) + i_1 \frac{dL_1(t)}{dt} + (L_1 + L_f)\frac{di_1(t)}{dt}.$$

В схемі показано два постійні магніти, які моделюються еквівалентною фіктивною обмоткою збудження увімкненою до джерела струму:

$I_i = \frac{F_i}{w}$, причому $I_м = I_{м1} = I_{м2}$, $w1 = w2 = 1$.

Таким чином вираз для вихідної напруги генератора можна записати у вигляді:

$$U_1(t) = i_1(t)R_H + L_f \frac{di_1(t)}{dt}.$$

Отримана таким чином енергія направляються в спеціальний зарядний пристрій де відбувається її накопичення і перетворення в надпотужні ультракороткі імпульси, які направляються в антенну систему, яка повинна бути з однієї сторони добре узгодженою з генератором для якомога більш повного відбору потужності згенерованого імпульсу, а з іншого боку добре узгодженою з «вільним простором» у який цей імпульс повинен випромінюватися. Крім того антенна система повинна бути компактною і мати вузько направлену діаграму випромінювання для високої концентрації енергії імпульсу в обмеженій ділянці простору.

Висновки. В роботі запропонована система знешкодження безпілотних літальних апаратів на основі їх опромінення ультракороткими надпотужними радіоімпульсами. В основі роботи системи лежить ефект Фарадея. Практичне здійснення системи передбачає використання енергії, яка розсіюється під час пострілів з стрілецької зброї. Причому, це не призводить до погіршення тактико-технічних характеристик даної зброї. Попередній розрахунок дає підстави визначити відстань ураження БПЛА в діапазоні 800 – 1200 м.

Підвищення точності систем електроприводу наведення та керування вогнем з індукційними давачами кутового положення на основі використання математичних методів обробки їх сигналів

Шабатура Ю.В.,
завідувач кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор
Снітков К.І.,
офіцер відділу підготовки військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Будь-яке застосування вогнепальної зброї в обов'язковому поряду вимагає вирішення задачі її прицілювання, яка в свою чергу, пов'язана з наведенням по кутам азимуту і місця. Тобто точність стрільби прямим чином залежить від точності кутових вимірювань. Таким чином задача підвищення точності визначення кутових переміщень є важливою і актуальною задачею.

Сучасні системи електроприводів наведення, слідкування, позиціювання, які використовують у системах наведеннях гармати танка, керованих ракетах, системах спостереження, тощо вимагають наявності давача кута (ДК) з високою розділовою здатністю та малою похибкою вихідних даних.

У даних системах електроприводу для визначення кута найчастіше використовують електромеханічний індукційний перетворювач (ЕМП) – обертовий трансформатор. Для підвищення точності цих систем доцільно використовувати алгоритми обробки вихідних сигналів. Забезпечити точність даних систем на рівні одиниць кутових секунд можливо лише на основі застосування відповідних математичних методів обробки вихідних сигналів давача, оскільки резерв підвищення точності механічного виготовлення уже практично вичерпано. Розв'язати цю задачу можна на основі переходу до цифрових систем вимірювання.

Пряме вимірювання фази сигналу, що поступає з індукційного давача кута, можливе лише з невисокою точністю внаслідок низки технічних причин, зокрема:

- рівень «зашумленості» сигналу з обмоток давача може складати декілька відсотків, що значно знижує точність правильного визначення переходу сигналу через нуль і, отже, його фази внаслідок «розмивання» моменту переходу через нуль, яке може складати за несприятливих умов навіть 5–10 кут. град.;
- для типової частоти збудження індукційного давача 1 кГц і необхідної точності 10 кут. сек. швидкість реакції системи безпосереднього визначення фази сигналу повинна бути меншою 5 нс, що технічно складно реалізувати навіть засобами сучасної електроніки.

Запропонована спрощена структурна схема переходу до цифрової системи вимірювання показана на рис. 1, де позначено ADC – *m*-канальний аналого-цифровий перетворювач (АЦП) розрядністю n_a з частотою вибірок f_g ; FCS – цифровий блок формування чисел *c* і *s*; R – блок регістрів, який містить *2m* масивів «оцифрованих» опорних функцій sin і cos *m*-фазної системи, розмірністю n_o кожен; D – цифровий детектор фази за значеннями величин *c* і *s* (ЦДФ); G – генератор опорних імпульсів частоти f_g для синхронізації роботи блоків ADC і FCS.

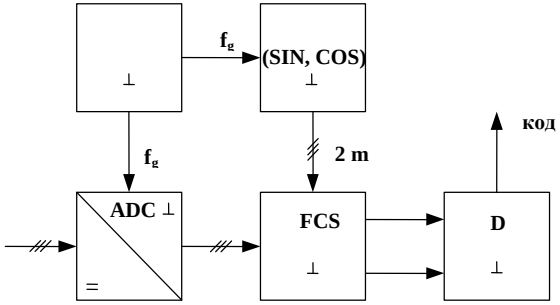


Рис.1

Функціонування запропонованого вторинного перетворювача сигна ВП відбувається таким чином: «оцифровані» з частотою f_g генератора G значення вихідних сигналів ДК e_{si} частоти f синхронно з відповідними значеннями функцій sin і cos подають на блок FCS, який реалізує алгоритм за (22*) у [3]. ЦДФ за одним з відомих алгоритмів [1] визначає фазу хвильового пакета прямої послідовності сигналів e_{si} , яка є носієм інформації про кутове

положення ротора ДК. Як показує аналіз структурної схеми, оброблення інформаційних сигналів у цифровому форматі неминуче передбачає їх квантування як за рівнем, так і за часом (дискретизацію), застосування відповідних алгоритмів обробки сигналів повинно пройти етап попередньої перевірки на математичній моделі, яка дозволить врахувати як похибки дискретного перетворення сигналів, так і вади виготовлення індукційного давача кута. Перевірки вимагають як окремі складові алгоритмів, так і алгоритми в цілому для порівняння їх ефективності, зокрема, потрібно перевірити:

- вплив похибки квантування (розрядності АЦП) за рівнем на похибку визначення кута за допомогою обернених тригонометричних функцій;
- вплив кількості відліків за період сигналу на величину похибки вимірювання кута;
- вплив виду алгоритму обробки даних на величину похибки вимірювання кута.

Висновки. Поява широко доступних персональних комп'ютерів і математичних застосунків до них (Mathcad, MATLAB тощо) дає змогу на основі використання числових процедур спростити перевірку алгоритмів і в багатьох випадках уникнути тривалого і складного аналітичного математичного аналізу. Тому на даному етапі основним інструментом досліджень доцільним є числовий експеримент.

Реалізації переходу до цифрових систем у системах визначення кута, які широко використовуються в електроприводах слідкування (сервоприводи), позиціювання, наведеннях і управління вогнем керованих ракетах, системах спостереження тощо можливо здійснити на базі сучасної мікропроцесорної техніки.

1. Завгородній В. Квантово-механічна модель давачів кута індукційного типу (Частина 5. Аналіз алгоритмів обробки вихідних сигналів) / В. Завгородній, В. Мороз, А. Бойко // Електротехніка і електромеханіка. – 2004. – №4. – С. 27–33.
2. Мороз В. Аналіз реалізацій визначення кута при обробці сигналів з індукційних давачів кута / В. Мороз, І. Снітков, Д. Довгань, П. Болкот // Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. пр. – Кам’янець-Подільський: Кам'янець-

Подільськ. нац. ун-т, 2014. – Вип. 10. — С. 112-118. – Бібліогр.: 3 назв. – укр.
3. Завгородній В.Д., Мороз В.І., Петрова О.А. Квантово-механічна модель давачів кута індукційного типу (Частина 4. Аналіз методів обробки вихідних сигналів) // Електротехніка і електромеханіка, 2003, № 4. – С. 36-41.
4. Мороз В. Вплив розрядності даних на точність визначення кута в індукційних давачах кута / В. Мороз, В. Оксентюк, П. Болкот, К. Снітков // Вісник Національного університету «Львівська політехніка» «Електроенергетичні та електромеханічні системи». – 2016. – №840. – С. 90–97.

Мікропроцесорна система оперативного визначення завантаженості колісних транспортних засобів спеціального призначення

Шабатура Ю.В.,
завідувач кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор
Паливода О.Л.,
курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Діяльність підрозділів державних силових відомств, а саме Міністерства Оборони України, Міністерства Внутрішніх Справ, Служби Безпеки нерозривно пов’язана з вирішенням задач транспортування озброєння і військової техніки, особового складу та різного роду вантажів. Незважаючи на значну кількість різноманітних транспортних засобів призначених для вирішення таких задач, саме колісні транспортні засоби були і залишаються основним транспортним засобом масового використання у силових відомствах.

Лідируючі позиції колісних транспортних засобів забезпечуються тактико-технічними характеристиками таких засобів, їх спроможністю пересуватися по бездоріжжю, досягати значних

швидкостей пересування, високою маневреністю, прохідною здатністю, а також великою вантажопідйомністю у поєднанні з високою економічною ефективністю. Сучасні колісні транспортні засоби спеціального призначення є високотехнологічними технічними системами, які насичені складними комплексами навігації, автоматичного та дистанційного керування озброєнням і рухом і т.д. Однак надзвичайно важливим і до цих пір не вирішеннм завданням є визначення маси вантажу, який завантажується в колісний транспортний засіб безпосередньо на місці завантаження.

Традиційно цю задачу вирішують лише за допомогою спеціально обладнаних і стаціонарно розташованих автомобільних ваг. Зрозуміло що такий варіант вирішення є мало прийнятним для військової техніки. Необхідність визначення ваги вантажу безпосередньо в місці його завантаження пов'язана з вирішенням інших важливих задач, які впливатимуть на можливості виконання даним колісним засобом задач експлуатації. Зокрема перевищення ваги вантажу значення допустимої вантажопідйомності колісного транспортного засобу різко знижує надійність його експлуатації (суттєво зростає ймовірність виходу з ладу підвіски, зчеплення, силової передачі і т.д.), крім того знижується маневреність, прохідність, швидкість руху, а також суттєво зростають витрати палива. Знання точного значення ваги вантажу дозволяє правильно розраховувати можливу швидкість руху транспортного засобу, витрати пального, прохідну здатність, тому його оперативне визначення є надзвичайно важливим при плануванні військових задач.

Основна ідея, яка лежить в основі розробленої мікропроцесорної системи оперативного визначення завантаженості колісних транспортних засобів спеціального призначення ґрунтується на очевидній фізичній закономірності, суть якої полягає в тому, що, якщо виміряти тиск повітря і його температуру в шинах коліс транспортного засобу безпосередньо перед завантаженням і одразу після завантаження і при цьому цей засіб залишається бажано нерухомим, або принаймні, при необхідності зміни положення він залишається на однотипній поверхні, то, на підставі зафіксованої зміни тиску повітря в шинах і значення температури, з врахуванням можливої її зміни, а також відповідної аналітичної

залежності, яка визначається для кожного типу колісного транспортного засобу, можна розрахувати точне значення маси завантаженого вантажу. Оригінальність даної ідеї зафіксована у вигляді патенту на спосіб вимірювання [1]

З'ясуємо деякі фізико-математичні залежності, які виконуються в системі взаємодії навантажене колесо – опорна поверхня. Типова конструкція колеса являє собою двоелементну систему: колісний диск і шина з розміщеною всередині резиновою камерою. Колісний диск є достатньо жорсткою системою можливі деформації якої є нехтовно малими, тому розглянемо більш детально саме шину з камерою. Аналіз геометрії шини дозволяє прийняти рішення про її допустиму апроксимацію геометричною фігурою відомою під назвою – тор. Основні геометричні параметри тора наведені на рисунку 1.

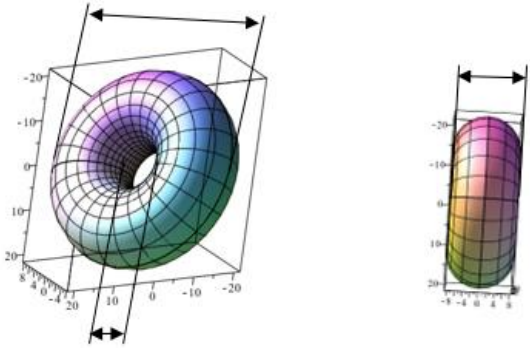


Рис.1. Геометрична апроксимація шини

На наведеному вище рисунку використані наступні позначення: D зовнішній діаметр шини; d внутрішній діаметр отвору; H ширина шини. З врахуванням введених позначень можна обчислити площу поверхні тора і його внутрішній об'єм.

$$S = \pi^2 Dd = \pi^2 d^2 H$$

$$V = \pi^2 dH^2/4.$$

Отже, якщо виміряти тиск повітря в шині [кг/см^2], то можна обчислити еквівалентну вагу приведену до поверхні і відповідно оцінити зміну тиску при зміні ваги навантаження на дану шину. Причому враховуючи те, що внутрішня поверхня тора обмежена металевим диском, тому вона фактично не зазнає деформації.

Врахування площі внутрішньої поверхні обмеженої колісним диском, а також того, що тор є наближеною апроксимацією поверхні шини дає приблизну оцінку зменшення «активної» площі поверхні шини по відношенню до еквівалентного тора на коефіцієнт ¼.

Практичне застосування розглянутого підходу до створення мікропроцесорної системи оперативного визначення ваги вантажу завантаженого в колісний транспортний засіб вимагає синтезування для кожної марки колісного транспортного засобу аналітичної функціональної залежності, яка зберігатиметься у пам'яті системи і матиме загальний вигляд:

$$M = F\left(P_1^i, P_2^i, t_1^i, t_2^i, K_A, K_{\text{п}}\right),$$

де P_1^i, P_2^i тиск в кожній i-шині транспортного засобу відповідно до і після завантаження, t_1^i, t_2^i температура в кожній i-шині транспортного засобу відповідно до і після завантаження, K_A функціональні коефіцієнти визначені для кожної марки колісного транспортного засобу, $K_{\text{п}}$ функціональні коефіцієнти визначені для основних видів опорної поверхні.

З метою перевірки адекватності отриманих функціональних залежностей плануються експериментальні дослідження для основних марок колісних транспортних засобів, які знаходяться на озброєнні в Збройних Силах України.

Висновки. У роботі розроблений новий принцип оперативного визначення величини завантаженості колісних транспортних засобів спеціального призначення. Окреслені основні особливості практичної реалізації у вигляді портативної мікропроцесорної системи, яка на основі вимірювань тиску повітря та температури в шинах транспортного засобу до завантаження і після, а також вибору марки даного виду транспортного засобу і виду опорної поверхні обчислює значення ваги завантаженого вантажу.

У плані подальших досліджень передбачається розроблення моделі для визначення оцінки точності вимірювання вантажу в діапазоні можливих варіацій вхідних даних.

1. Шабатура Ю.В. Свирида В.А. Патент України на винахід №53005 «Спосіб вимірювання ваги вантажу» Бюл. Промислова власність, 2003. – №1

Забезпечення навігації безпілотних літальних апаратів в якості спеціальних засобів на основі використання мережі стільникового зв'язку

Шабатура Ю.В.,
завідувач кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного,
доктор технічних наук, професор
Бурдейний М. В.,
старший викладач циклової комісії технічного та тилового забезпечення Військового колежу сержантського складу Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Результативність діяльності оперативних підрозділів залежить не тільки від особистих ділових якостей, але і от ефективності системи інформаційно-аналітичного забезпечення та оперативно-технічної оснащеності співробітників. Особливо це важливо при виконанні наприклад антитерористичних операцій пов'язаних з високим ризиком для життя та здоров'я особового складу підрозділу.

Важливе значення має підвищення ефективності та створення безпечних умов праці для працівників оперативних підрозділів.

Поява GPS технологій дозволила не тільки надавати інформацію про пересування об'єкту спостереження у реальному часі, що було неможливо у випадку використання радіочастотного устаткування а і можливість створення роботизованих спецзасобів де присутність людини обмежена або не ефективна.

Не обходиться без використання системи GPS управління безпілотними літальними апаратами (БПЛА) з метою:

- доставки світлозвукових пристроїв сімейства ТЕРЕН для припинення протиправних дій з масовим безладдям шляхом тимчасового придушення психовольової стійкості світловим і звуковим імпульсами високої інтенсивності або аерозольної хмари сльозоточивих і дратівних речовин;
- відстеження крадених авто;
- моніторингу патрульних екіпажів поліції і т.п.

- способів нагляду та спостереження за правопорушником, що виходять за межі традиційних пенітенціарних заходів нагляду та виконання покарань;

Нажаль Україна не має власної Супутникової навігаційної системи (СНС), а використання СНС інших Держав не завжди доцільно. Створення власної СНС для України на даний час непосильна задача як з фінансової точки зору так із питання часу. Проте останнім часом в ряді публікацій [3] згадуються псевдо-супутникові навігаційні системи, які працюють за аналогічним принципом що і СНС.

Розвиток технологій мобільного зв'язку стрімко просувається вперед. Станом на сьогодні вже більше 95% території України має покриття стільникового зв'язку. Стабільне функціонування мережі стільникового зв'язку забезпечується системою базових станцій (БС), які власне і формують конфігурацію стільникової мережі. Базові станції точно прив'язані в геодезичному відношенні, їхні координати визначені з великою точністю, кожна з них працює на окремій частоті та має власний унікальний код [2].

Для визначення задач навігації БПЛА потребує розрахунків дальності надійного прийому сигналів БС. Для цього потрібно розглянути конструкції та діаграми направленості антен (ДНА) БС.

Існує велика кількість модифікацій антен БС тому з метою врахування найгіршого випадку в розрахунках використовувались дані з найвужчими діаграмами направленості у вертикальній площині [4].

В статті [1] розроблені науково-методичні засади використання розташованих на території України базових станцій (БС) стільникових мереж в якості станцій псевдо-супутникової навігаційної системи. Виконаний аналіз запропонованого рішення підтвердив можливість забезпечення постійного, якісного, завадостійкого, високоточного і відносно дешевого навігаційного забезпечення літальних апаратів в умовах реального часу по всій території України та за її межами до 600 кілометрів.

Навігаційна система на основі використання БС спроможна забезпечити точне визначення координат БПЛА а з його допомогою об'єкта що спостерігається в місцях де сигнал GPS слабкий або взагалі втрачений.

Дана пропозиція особливо актуальна для підрозділів МВС України які можуть забезпечуватись необхідним мінімумом спецзасобів для ефективного виконання завдань по охороні громадського порядку лише за умови виділення необхідних коштів на їхню закупівлю, а також проведення відповідних науково-дослідних і дослідно-конструкторських робіт, запланованих Державною програмою розвитку озброєння та військової техніки.

1. Шабатура Ю.В. Принцип корекції навігаційної системи тактичних та оперативно-тактичних ракет на основі використання мережі стільникового зв'язку. / Шабатура Ю.В., Бурдейний М.В. / Системи озброєння і військова техніка // Науковоий журнал – Харків: ХУПС, 1(1) – Т'2016. 105–110 с. Таємно. Інв. № 2642 у НАСВ.
2. По следам мобильного телефона. Геолокация с помощью сотовой сети. Аналітичний огляд 05.2015/ [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/company/megafon/blog/167905/
3. T.Morley, G.Lachapelle «GPS Augmentation with Pseudolites for Navigation in Constricted Waterways» Navigation: Journal of Instituteof Navigation vol.44, No. 3, Fall 1997
4. 790 – 2500 MHz Base Station Antennas for Mobile Communications / KATHREIN Antennan Elektronik C. -170.

Перспективи застосування вентильних реактивних двигунів для електротрансмісій колісних транспортних засобів

Юрченко А.В.,
курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Військова техніка вимагає використання шасі з високою питомою потужністю, автоматичною трансмісією, високою маневреністю і високими експлуатаційно-технічними якостями. Найбільш перспективними в цьому відношенні є електричні приводи. Зокрема, розробники військових колісних засобів класу бронетранспортерів все частіше відмовляються від механічної і гідромеханічної трансмісій на користь електромеханічної [1]. Обмежене застосування електромеханічної трансмісії на транспорті до

теперішнього часу пояснювалося труднощами безступінчастого регулювання швидкості обертання і навантаженням тягових електродвигунів, великою масою і габаритами блоків управління [1].

Так, на озброєнні бельгійської армії знаходиться багатоцільова гусенична броньована машина з електротрансмісією «Cobra», дослідні зразки машини розвідки RST-V-розробник General Dynamics (США) і розвідувальної бойової машини Rooikat виробництва ПАР [1].

Основними компонувальними рішеннями для електротансмісій є:

- встановлення електродвигунів для приводів мостів виключає карданий зв'язок (універсальне шасі HEMTT);
- встановлення електродвигунів в корпусі зі збереженням колісних редукторів;
- встановлення електродвигунів в колесі (дослідні зразки машини розвідки RST-V).

Установка електродвигунів в корпусі забезпечує можливість об'єднати їх з електронною системою управління і таким чином зібрати їх в більш компактні герметизовані блоки з мінімальною кількістю зовнішніх електричних з'єднань і з'єднань системи охолодження. Вона також забезпечує їм меншу вразливість і не дає значного збільшення маси машини [1].

Електротрансмісія може бути рекомендована для використання при проектуванні колісних бронетранспортерів і спеціальних шасі нового покоління. Також вона може бути використана при модернізації існуючих машин з незначними доопрацюваннями в корпусі. Технологія електропривода колісних транспортних засобів, в зв’язку з наявною комбінованою системою забезпечення енергії, пріоритетна для застосування на території України. При виготовленні дослідних зразків можна базуватися, як на вітчизняні, так і на імпортні комплектуючі [1].

Як база для виготовлення електротрансмісій можуть використовуватись асинхронні двигуни з короткозамкненим ротором, які забезпечують компроміс між низькою масою, вартістю, простотою і міцністю. Разом з тим, синхронні двигуни з постійними магнітами мають переваги за масою. Але їх виробництво є більш

дорогим, головним чином через високу вартість постійних магнітів. Вентильні реактивні двигуни (ВРД) мають ряд переваг перед іншими електричними двигунами: конструктивно вони простіші, а отже, більш технологічні в виготовленні, обслуговуванні і ремонті, мають малу собівартість; володіють більшою енергоефективністю і більш високою перевантажувальною здатністю в порівнянні з АД і СД, постійною потужністю в широкому діапазоні частот обертання на відміну від СД з ПМ, вібростійкістю, надійністю і відмово-стійкістю, що має рішуче значення для надійної техніки військового призначення [2].

Вентильно-індукторний привід з незалежним збудженням з точки зору управління і принципу роботи еквівалентний класичній синхронної машині. Застосування розподіленої обмотки статора замість зосередженої зменшить перемагнічування заліза ротора, потенційно знизить рівень шуму, що актуально для транспортного застосування [3]. Прикладом використання ВРД для електротрансмісій колісних транспортних засобів у наших найближчих сусідів є проект модернізації тягового електроприводу кар'єрного самоскида БелАЗ-75131 вантажопідйомністю 136 т з електромеханічною трансмісією змінно-постійного струму [2].

Але найкраще характеризує перспективи використання ВРД для колісних засобів військового призначення їх використання у новій бойовій машині Крымск, розробленій у Росії [4].

Як показали експерименти [4], глибина послаблення поля в вентильно-індукторний привід з незалежним збудженням обмежена тільки залишковим потоком і може бути значно більше (10: 1 і більше), ніж в синхронному приводі з постійними магнітами, що збільшує діапазон швидкостей при роботі з постійністю потужності. Для керування приводом [3, 4] застосована стандартна силова база і класична структура векторного керування, доповнена деякими алгоритмом ослаблення поля. При всьому цьому машина технологічна у виготовленні, допускає великий перегрів, дозволяє легко відводити тепло з статора, що робить перспективним використання вентильно-індукторного приводу з незалежним збудженням як тягового електроприводу [3] для колісних засобів військового призначення.

1. Поторока А.В. Применение электромеханических трансмиссий для машин класса бронетранспортеров / Поторока А. В., Решетило Е. И. та ін. // Механіка та машинобудування. –2012. – № 2. – с. 152 – 158.
2. Птах Г.К. Вентильно-индукторный реактивный электропривод средней и большой мощности: зарубежный и отечественный опыт // Электротехника: сетевой электронный научный журнал. – 2015. – Т.2, №3. – С. 23 – 33.
3. Козаченко В.Ф. Вентильно-индукторный электропривод с независимым возбуждением для тягового применения / Козаченко В. Ф., Лашкевич М. М. // Электротехнические и компьютерные системы – 2011. – № 03(79). – С. 103 – 108.
4. Лашкевич М.М. Разработка системы управления электротрансмиссии с тяговыми вентильно-индукторными двигателями: автореф. дисс. … канд. техн. наук: 05.09.03 / М. М. Лашкевич. – М., 2013. – 155 с.

Розділ 3.
НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ ПРОЦЕСІ

Використання тестових технологій у навчанні іноземної мови

Бондаренко В.А.,
доцент кафедри мовної підготовки Львівського державного університету внутрішніх справ, кандидат юридичних наук

Питаннями дослідження тестових технологій при вивченні іноземної мови, класифікації тестів, використання лінгводидактичного тестування, а також теоретичних проблем тестування у навчанні іноземної мови займається багато дослідників як в Україні, так і за кордоном. При цьому зазначимо, що більш важливі питання, пов'язані з тестуванням, розкрито у наукових працях В. Кокотти, О. Петращук С. Ніколаєвої, О. Квасової, Л. Гнаповської, Р. Мільруд, Джемері Хамера та інших.

Тестування – метод дослідження, що передбачає виконання випробуваним спеціальних завдань. В основі цієї форми контролю лежить використання завдань стандартної форми, які отримали назву «тесту», що в перекладі означає випробування, дослідження, перевірка. Тест визначається як «підготовлений відповідно до певних вимог комплекс завдань, які пройшли попереднє опробування з метою визначення його показників якості» [2, с. 43]. Він дає можливість виявити у тестованого ступінь його лінгвістичної і комунікативної компетенції. Цей комплекс завдань існує у формі сукупності питань, що забезпечують однозначність відповідей випробовуваних. Його відрізняє ретельність розробки відповідно до певних правил і процедур, попередня експериментальна перевірка, наявність таких характеристик ефективності, як валідність і надійність. Наявний еталон відповіді

гарантує об'єктивність результатів тестування, які піддаються кількісному обліку.

Основна відмінність тесту від контрольної роботи полягає в тому, що він завжди передбачає вимір. Іншою важливою відмінністю є те, що тести проходять процедуру стандартизації. Тому оцінка, що виставляється за підсумками тестування, відрізняється більшою об'єктивністю, ніж оцінка контрольної роботи, винесена на підставі особистого судження перевіряючого.

Тест складається з двох частин – інформаційної та операційної. В інформаційній частині ясно і просто сформульовано інструкцію і приклади правильного виконання завдань. Операційна частина складається з певної кількості завдань або питань. Тестове завдання містить основу (stem) у вигляді стверджувального речення (повного або неповного), питання або невеликого тексту. Тестове завдання може супроводжуватися набором відповідей (responses), які називають також вибірковими відповідями або альтернативами. Серед відповідей міститься одна правильна відповідь (key / correct option) і кілька неправильних (destractors). Всі варіанти вибору повинні бути приблизно однаковими за обсягом та одного рівня складності. Тести з багатьма завданнями називаються комплексними тестами.

У вітчизняній практиці навчання іноземних мов роль тестування стає дедалі більше. Інтерес до тестування пояснюється тим, що окрім своєї основної функції – контролю, воно може бути засобом діагностики труднощів мовного матеріалу для студентів, мірою визначення якості навченості і способом прогнозування успішності чи неуспішності навчання.

У методичній літературі і практиці навчання мови набули поширення два види тестів: нормативно-орієнтовані і критеріально-орієнтовані [3, с. 301–302].

Нормативно-орієнтований тест (norm-referenced test) призначений для порівняння навчальних досягнень окремих випробовуваних. До цієї групи можна віднести прогностичні тести, метою яких є визначення здатності того чи іншого студента до вивчення іноземної мови. Вони можуть бути використані при професійної орієнтації студентів.

Критеріальною-орієнтований (criterion-referenced test) тест використовується для оцінки ступеня володіння випробуваним

пройденим матеріалом. Сюди можна віднести діагностичні тести. Діагностичний тест – це набір стандартизованих завдань за певним матеріалом, який встановлює ступінь володіння його студентами.

Найбільшу актуальність для викладача іноземної мови мають так звані тести успішності, які визначають, наскільки успішно сформована комунікативна компетенція тестованого і чи готовий він до іншомовного спілкування в рамках тих комунікативних завдань, які зумовлені тим чи іншим рівнем володіння іноземною мовою. Такі тести є засобом поточного і підсумкового контролю.

У сучасній методичній літературі виділяють такі види тестових завдань:

Перехресний вибір (matching) – завдання полягає в підборі пар з двох блоків за тими чи іншими ознаками;

Альтернативний вибір (true-false);

Множинний вибір (multiple choice) – завдання полягає у виборі правильної відповіді з трьох і більше варіантів;

Впорядкування (rearrangement) – використовується для перевірки вміння скласти зв'язаний текст з окремих частин або речення з поданих слів;

Завершення (completion) – студентам пропонується самостійно закінчити речення, керуючись змістом;

Підстановка (substitution) – виконання завдання передбачає зміну форми слова або структури речення загалом;

Трансформація (transformation) – виконання завдання передбачає зміну речення відповідно до зразка;

Внутрішньомовні перефразування (intralingual paraphrasing) – суть завдання полягає в передачі своїми словами змісту тексту;

Міжмовне перефразування (cross-language paraphrasing) – передбачає вміння студентів знайти еквівалентну форму для передачі змісту тексту, вираженого засобами мови, що вивчається.

Клоуз-тести (cloze test) – передбачає відновлення пропущених слів у тексті. За його допомогою перевіряють загальний рівень володіння мовою.

За наявністю або відсутністю варіантів відповіді виділяють тести закритої та відкритої форм [4, с. 36]. Закриті тестові завдання перевіряють повноту засвоєння лінгвістичної змістової лінії навчальної програми та рівень сформованості у студентів мовної

компетенції: – завдання з простим вибором одноелементних відповідей використовуються для перевірки вміння правильно відтворювати набуті знання. Завдання складається з двох частин: у першій – якомога стисло і чітко, без двозначності формулюється запитання, а в другій – пропонується на вибір декілька відповідей, одна з яких є правильною. Варіанти відповідей мають бути не абсурдними, близькими до істинної відповіді, відрізнятися одне від одного повнотою, точністю. Для того щоб вибрати правильну відповідь, студент повинен проаналізувати усі відповіді, що пропонуються; – завдання з простим вибором багатоелементних відповідей використовуються для перевірки вміння характеризувати або знаходити спільне в явищах, які вивчаються. На відміну від попередніх завдань тут пропонується сформувати правильну відповідь з декількох часткових відповідей; – завдання з перехресним вибором одноелементних відповідей використовуються для перевірки вміння вільно орієнтуватися в групі схожих понять, процесів, явищ. У даному випадку завдання містять кілька запитань і стільки ж відповідей, розташованих у двох колонках таблиці. Необхідно для кожного завдання, розміщеного ліворуч, вибрати однозначну відповідь з правої колонки таблиці; – завдання з перехресним вибором багатоелементних відповідей використовується для перевірки уміння узагальнювати, виділяти, застосовувати знання при розв'язанні конкретних практичних завдань. Кожному запитанню, що подане у першій частині (ліворуч), може відповідати кілька відповідей з другої частини (праворуч); – завдання з поетапним вибором відповіді використовуються для перевірки вміння аналізувати і синтезувати факти, процеси, явища, визначати послідовність подій. Відповіді можуть бути одноелементними або багатоелементними; – завдання з альтернативними відповідями використовуються для перевірки вміння зробити правильний вибір або прийняти рішення у згорнутій, скороченій формі. Можливі альтернативи типу «так-ні», «1-0», «змінний-постійний» тощо; – завдання на заповнення пропусків застосовуються для перевірки чіткого, однозначного розуміння явищ, процесів, понять. У цих завданнях пропускаються ключові слова або символи, які необхідно вставити самостійно, або обрати з декількох запропонованих; – завдання на конструювання правильної відповіді використовуються для перевірки знань і умінь розуміти сутність окремих понять, явищ, процесів, уміння вирішувати різні практичні завдання. У цих завданнях вимагається самостійно, без

підказки сформулювати відповідь. Такого роду завдання використовуються лише тоді, коли відповідь може бути сформульованою однозначно у формі слова, букви, знака, цифри, схеми тощо.

Мовне тестування є процедурою педагогічних вимірювань, яка не позбавлена протиріч. З одного боку, тестування має цілий ряд переваг: можливість охопити велику кількість студентів (всю групу або курс), використовуючи однаковий матеріал і однакові умови процедури тестування; економія аудиторного часу, що дуже важливо в немовних вишах, де час на вивчення мови лімітований; зорієнтованість на сучасні технічні засоби навчання та використання комп'ютерних навчальних та контролюючих систем; збільшення об'єктивності педагогічного контролю, мінімізація суб'єктивного чинника під час оцінювання відповідей. З іншого – слід вказати на недоліки тестового контролю знань: при застосуванні тестів закритого типу можливість оцінки лише кінцевого результату (правильно – неправильно), у той час як сам процес, що привів до нього, не розкривається; ймовірність випадкового вибору правильної відповіді; психологічний недолік – стандартизація мислення без врахування рівня розвитку особистості; велика затрата часу на складання необхідного «банку» тестів, їх варіантів, трудомісткість процесу; тести не сприяють розвитку мови.

1. Біднячук О. М. Тестування як ефективний засіб організації контролю у навчанні іноземної мови / О. М. Біднячук // Соціум. Наука. Культура. [Електронний ресурс]. – Режим доступу: http://intkonf.org/bidnyachuk-o-m-testuvannya-yak-efektivniy-zasib-organizatsiyi-kontrolyu-u-navchanni-inozemnoyi-movi/
2. Конышева А. В. Контроль результатов обучения иностранному языку [Текст] : материалы для специалиста образоват. учреждения / А. В. Конышева. – Санкт-Петербург : Каро ; Минск : Четыре четверти, 2004. – 135 с.
3. Щукин А. Н. Обучение иностранным языкам: теория и практика : Учебное пособие для преподавателей и студентов / А. Н. Щукин. – М. : Филоматис, 2004. – 416 с.
4. Коккота В. А. Лингводидактическое тестирование : [науч.-теор. пособие] / В. А. Коккота. – М. : Высш. школа, 1989.–352 с.
5. Чорна Н. В. Сутнісні ознаки тестів успішності в педагогіці США / Н. В. Чорна // Наукові записки Вінницького державного педагогічного університету імені М. Коцюбинського. Серія : Педагогіка і психологія. – Вінниця. – 2002. – Вип. 7. – С. 75–80.

6. Гарматюк Н. Д. Особливості застосування тестового контролю при вивченні іноземної мови у вищих навчальних закладах / Н. Д. Гарматюк, В. П. Марценюк // Медична освіта. – 2013. – № 3. – С. 17–24. – Режим доступу: http://nbuv.gov.ua/UJRN/Mosv_2013_3_6.
7. Контроль в обучении иностранному языку [Текст] : учебное пособие / ред. Е. И. Пассов, Е. С. Кузнецова. Воронеж : Интерлингва, 2002. – 40 с.
8. Ніколаєва С. Ю. Практикум з методики тестування іншомовної лексичної компетенції (на матеріалі англійської мови) / С. Ю. Ніколаєва. – К. : ІЗМН, 1996. – 312 с.
9. Петращук О. П. Тестовий контроль у навчанні іноземної мови в середній загальноосвітній школі : [монографія] / О. П. Петращук. – К. : Видавничий центр КДЛУ, 1999. – 261 с.

Електронні освітні відеоресурси у навчальному процесі

Глинський Я.М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент
Магеровська Т.В.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент
Пелех Я.М.,
завідувач кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент
Ряжська В.А.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

З розвитком новітніх інформаційних технологій стає все складніше підтримувати інтерес студентів до традиційних моделей навчання. Тому актуальною є проблема залучення суб'єктів навчання до навчальної діяльності з використанням електронних

освітніх відеоресурсів, які можуть бути використані в традиційних чи хмарно орієнтованих освітніх середовищах, які у свою чергу можуть бути застосовані для підтримки очного чи дистанційного навчання чи різновиду останнього – мобільного навчання.

Вдало створені електронні освітні відеоресурси (ЕОВ): відеоуроки, відеолекції і відеокурси – є тими альтернативними засобами демонстраційного навчання, які можуть виправдати покладені на них очікування, забезпечивши високу мотивацію до навчання. Оскільки розробка україномовних ЕОВ є порівняно новим видом педагогічної діяльності, то проблематика аналізу існуючих ЕОВ і розробки нових є актуальною. Зауважимо, що дослідження на тему електронних освітніх ресурсів були систематизовані в [1, 2, 3]. Ми ж досліджуємо і розробляємо відеоресурси.

Розробка відеоресурсів (відеокурсів, окремих відеоуроків, відеолекцій чи їх колекцій) була і є в центрі уваги як окремих фахівців та і великих компаній і корпорацій за кордоном та в Україні. Як вдалий український досвід слід відзначити комерційні розробки сервісно-освітнього центру «Інтершкола» (м. Дніпропетровськ), виконані у 2000-х роках під керівництвом І. Каплаушенко, теперішнього директора компанії «Є-підручники». У тих же 2000-х першість за кількістю та якістю ЕОВ належала корпорації Microsoft. Для підтримки і поширення своїх XP-продуктів (Windows XP, Office XP) були створені сотні високоякісних відеоуроків як англійською мовою, так і мовами багатьох народів світу, зокрема, російською. Українською мовою відеоресурси не створювались оскільки, як стверджували згодом співробітники корпорації, ніхто не звертався до Microsoft з відповідним клопотанням. З виходом продуктів «великої сімки» (Windows 7, Office 2007) відеоуроки XP-серії стали не актуальними, а від централізованого створення нових відеоуроків корпорація відмовилася, обмежившись гіпертекстовими довідниками, що виправдано в умовах короткого (трирічного) періоду виходу оновлених версій її програмних продуктів.

Новим лідером, який пропонує зокрема ЕОВ головно у форматі відеоуроків і відеолекцій, став відеохостинг YouTube. Але проведений нами аналіз показав, що переважна частина відеоконтенту в YouTube або англомовна, або російськомовна, і

часто застаріла. На нашу думку іноземна мова є суттєвим, але не головним обмежуючим фактором. Багато відеоресурсів з різних освітніх тем, які можна знайти в YouTube, створені не програмними засобами захоплення відео з екрана комп'ютера (це комп'ютерні відеоресурси), а шляхом записування за допомогою відеокамери аудиторних лекцій (це натурні відеоресурси). Відсоток корисних відеоуроків є невеликий, їх важко відшукати, а частка україномовних ресурсів мізерна.

Окремо слід згадати відкриті освітні середовища (ВОС) (інший термін – масові відкриті онлайн курси (МВОК)) такі як: edX (edx.org) від Масачусетського технологічного інституту і Гарвардського університету, Coursera (coursera.org) від Стенфордського університету, Prometheus (Prometheus.org.ua) від декількох українських університетів і Lynda (lynda.com) від компанії LinkedIn, яку до кінця 2016 року планує викупити корпорація Microsoft. Перші три гомогенні за будовою оскільки складаються з цільних відеокурсів, а Lynda – гетерогенна за структурно бо складається з великої кількості розрізнених відеокурсів, відеолекцій і відеоуроків. Крім цього, на відміну від перших трьох, Lynda є платним репозиторієм з десятиденним безкоштовним trial-доступом, але з вимогою до користувача авансом ввести реквізити банківської картки з попередженням, якщо користувач не вийде вчасно з trial-режиму, то автоматично з картки зніматимуться 30 USD щомісяця. ВОС Coursera надає як платні, так і безплатні відеокурси з багатьох дисциплін, причому великий російськомовний сегмент є достатньо якісним і цілком безплатним. Україномовних курсів тут немає. МВОК edX надає доступ до багатьох безкоштовних англомовних відеокурсів провідних університетів світу, де користувач за бажанням може замовити сертифікат про закінчення курсів, який коштує від 50 до 100 USD. ВОС Prometheus створене з ініціативи трьох українських університетів за фінансової підтримки проектів Посольством США і провідними українськими ІТ-компаніями. На даний час Prometheus налічує більше десяти відеокурсів українською мовою і закликає до співпраці нових авторів і розробників ЕОВ. ВОС використовують YouTube як кінцевий відеохостинг. У даній статті немає змоги описати контент конкретних ЕОВ, але корисною буде така рекомендація користувачам-педагогам, які

ще не знайомі з ВОС: реєструйтесь у ВОС, ознайомлюйтесь з його вмістом, шукайте потрібний курс, ознайомлюйтесь з ним чи реєструйтесь на навчання, аналізуйте і порівнюйте курси, створюйте власні ЕОВ. Зауважимо, що з 1 червня 2013р. відкрито доступ до репозиторіїв вихідних кодів платформи edX, що дає змогу не тільки вивчати велику кількість курсів у відповідних МВОК, але й створювати власні портали для дистанційного навчання. Платформа написана мовою Python, деякі частини – мовами Ruby і NodeJS. Код поширюється за ліцензією AGPL.

Розробку ЕОВ варто починати створенням короткого відеоуроку програмами oCam чи Camtasia Studio. Найбільш корисними є комп'ютерні відеоуроки, присвячені технологічним аспектам технічних дисциплін, які за обмежений проміжок часу (орієнтовно до 20 хвилин) розкривають питання, які традиційними засобами лектор розкрити не може через недостатню кількість аудиторного часу чи специфіку матеріалу. Такі відеоуроки дають змогу автоматизувати навчальний процес шляхом перерозподілу навчального часу на користь позааудиторної самостійної роботи студентів, що може здійснюватися у дистанційному чи мобільному режимах. Студент може переглядати короткі відеоуроки багаторазово вдома чи під час лабораторних занять доти, доки не освоїть відповідних вмінь і навичок. Показовим у цьому плані є відеоурок з основ алгоритмізації та програмування, розроблений одним з авторів, з яким можна ознайомитися на каналі hlynsky1 в YouTube [4]. Для створення відео використовувалась 30-денна безкоштовна (trial) версія Camtasia Studio. Для забезпечення балансу між якістю і обсягом файлу вибрано формат відеоданих MP4.

Відеоресурс [4] застосовувався як навчальний засіб у різних формах навчання. Спочатку він використовувався фронтально під час традиційної лекції в мультимедійній лекційній аудиторії. Дистанційність трансляції відео з YouTube тут не є принциповою, оскільки демонстрацію можна виконати зі стаціонарного комп'ютера. Педагогічний ефект досягався завдяки зміні форми подання матеріалу з перенесенням викладу прагматичних тем традиційної лекції у відеорежим. За обсягом подання матеріалу один такий 10-хвилинний фільм замінює 30–45-хвилинне усне повідомлення лектора. Студентам дистанційної форми навчання це й же нав-

чальний матеріал подавався засобами відкритої гугл-групи з можливістю перегляду відеоматеріалів в YouTube. У цьому випадку розроблений відеоурок є елементом дистанційного курсу. Але значна кількість переглядів відео пов'язана з мобільною формою навчання, яку ми практикували зі студентами очної форми навчання. Через концентрованість подання матеріалу і його новизну стало очевидно, що одноразового перегляду відео одним суб'єктом навчання недостатньо, щоб навчитися створювати проекти. Студенти переконалися, що для успішного виконання самостійних робіт відеоурок треба переглядати 2–3 рази: спочатку колективно на лекції, потім індивідуально вдома чи в лабораторії, в електричці тощо, використовуючи сучасні мобільні засоби: смартфони, планшети, ноутбуки.

Відеоуроки, відеолекції та цілі відеокурси можна розглядати як перспективне наповнення відкритих чи закритих освітніх середовищ, як розвиток концепції електронних навчально-методичних комплексів (ЕНМК), які розроблялися і розробляються на платформі Moodle. Створені на базі платформи Moodle текстові навчальні матеріали залишаються актуальними, оскільки вони можуть бути доповнені відеоконтентом. Вдалі відеокурси можуть бути опубліковані у всеукраїнському ВОС Prometheus, а у разі доцільності і наявності оригінального наповнення може бути створене локальне освітнє середовище навчального закладу, що може базуватися, наприклад, на базі вільнопоширюваної платформи edX, призначеної для розробки ВОС.

1. Наказ Міністерства освіти і науки, молоді та спорту України № 1060 від 01.10.2012 «Про затвердження Положення про електронні освітні ресурси». [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/go/z1695-12.
2. Манжула А. М. До питання класифікації ЕОР. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/ creativepedagogics/eor.
3. Биков В.Ю. Проект положення про електронні освітні ресурси / В.Ю. Биков, М.П. Шишкіна, Г.П. Лаврентьєва, В.М. Дем'яненко, В.В. Лапінський, Ю.Г. Запорожченко, М.В. Пірко // Інститут інформаційних технологій і засобів навчання НАПН України., 2013. [Електронний ресурс]. – Режим доступу: http://lib.iitta.gov.ua/id/eprint/1041
4. Глинський Я. Другий урок VBA. [Електронний ресурс]. / Я. Глинський, В. Відливаний. – Режим доступу: https://www.youtube.com/watch?v=7cFmSRSfd5o.

Дистанційне навчання у ВНЗ України – переваги, проблеми і перспективи

Кулешник Т.Я.,
викладач Львівської Національної академії мистецтв, начальник ІОЦ
Кулешник О.І.,
старший викладач Львівської Національної академії мистецтв

Тенденції впровадження сучасних інформаційних технологій у процес навчання найбільш розвинених країн показують, що в даний час відбувається процес кардинальних змін в системі освіти. Україна стала учасником Болонського процесу і тим самим взяла на себе зобов'язання розвивати форми і методи ведення навчального процесу у руслі передових світових тенденцій, що має підняти статус власників вітчизняних дипломів про вищу освіту на європейському ринку праці. Відбувається модернізація навчальних закладів відповідно до сучасних вимог якості навчання [1]. Одним з провідних завдань, які стоять перед викладачами та працівниками ВНЗ, є не тільки впровадження системи дистанційної освіти, чого вимагає загально людська потреба у вдосконаленні, а й забезпечення сприятливого впливу нових технологій на освітній процес.

На сьогоднішній день якість освіти – тема більшості дискусій в світових освітніх спільнотах. Якщо декілька років тому ці обговорення стосувалися традиційної освіти, де відбувається безпосередній контакт між викладачем і студентом, то тепер поняття якості застосовується щодо електронного навчання.

Запорукою успішного вирішення цього питання є законність дистанційної форми навчання у кожній країні поруч з традиційною формою. З цією метою необхідно підготувати відповідну нормативно-правову базу. На сьогодні в Україні ми вже маємо наступний перелік правових документів пов'язаних з дистанційним навчанням:

- Наказ міністерства освіти і науки України «Про затвердження Змін до Положення про дистанційне навчання» №761 від 14.07.2015 р.

- Наказ міністерства освіти і науки України «Про затвердження Положення про дистанційне навчання» №466 від 25.04.2013 р.
- Постанова Кабінету міністрів України «Про затвердження Державної програми «Інформаційні та комунікаційні технології в освіті і науці на 2006-2010 роки» від 7 грудня 2005 р. № 1153.
- Рішення Колегії Міністерства освіти і науки України «Про стан і перспективи розвитку дистанційного навчання в Україні» від 23 червня 2005 р.
- Наказ Міністерства освіти і науки України від 21.01.2004 № 40 «Про затвердження Положення про дистанційне навчання».
- Постанова Кабінету міністрів України від 23 вересня 2003 р. № 1494 «Про затвердження Програми розвитку системи дистанційного навчання на 2004-2006 роки».
- Наказ Міністерства освіти і науки України від 07 липня 2000 р. № 293 «Про створення Українського центру дистанційної освіти».
- «Концепція розвитку дистанційної освіти в Україні» від 20 грудня 2000р. затверджена Постановою МОН України.

Дистанційне навчання – це варіант заочної форми навчання з використанням комп'ютерних і телекомунікаційних технологій, які забезпечують інтерактивну взаємодію викладачів та студентів на різних етапах навчання і самостійну роботу з матеріалами, розміщеними в глобальній мережі Інтернет.

Ст. 42 Закону України «Про вищу освіту» [2] (з наступними змінами) від 17.01.2002 р.: «Навчання у вищих навчальних закладах здійснюється за такими формами: денна (очна), вечірня, заочна, дистанційна, екстернатна. Форми навчання можуть бути поєднані».

У перспективність, життєвість дистанційного навчання і адекватність його (по відношенню до традиційних форм) сьогодні повірили не тільки колективи найбільш прогресивних вузів світу, а й самі студенти, яких з кожним роком у світі стає все більше. Визнавши дистанційну форму освіти, Україна намагається йти в руслі світових тенденцій в галузі освітнього процесу.

На Заході ця форма з'явилася вже досить давно і має велику популярність серед населення через її економічні показники і навчальну ефективність. Багато хто з тих хто вже має вищу освіту, через необхідність підвищення кваліфікації або розширення сфери діяльності, змушений швидко і якісно засвоїти нові знання і набути навички роботи. Саме тоді оптимальною формою може стати дистанційне навчання.

Для досягнення в цьому напрямку найкращих результатів, спираючись на класичні методи викладання, необхідно розвивати нові – на основі Інтернет-технологій XXI ст., які вже зараз успішно застосовуються в ряді провідних ВНЗ України.

На відміну від зарубіжних моделей, українська дистанційна освіта більш наближена до нашого споживача і є більш демократичною. Органічно поєднуючи в собі змішані технології відкритої освіти (кейс-технології, TV-технології, мережеві технології), українська дистанційна освіта стає все більше доступна широким масам населення. Без навчання протягом усього життя у сучасному світі не обійтись і тому світовий принцип – «освіта не на все життя, а все життя» стає популярнішим і серед українців.

Механізм засвоєння навчального матеріалу є унікальним для кожної людини. В залежності від цього кожен обирає оптимальний для себе стиль навчання. Так, 90% людей можуть ефективно засвоювати матеріал поза межами конкретної навчальної аудиторії. Це означає, що абсолютна більшість людей потенційно придатна і має здібності для ефективного дистанційного навчання. Звичайно, необхідною умовою для цього є наявність якісного технічного і програмного забезпечення, високого професійного рівня викладацького складу університету, що володіє новітніми технологіями навчання, ефективної організації навчального процесу.

У процесі дистанційного навчання застосовують частково як традиційні технології навчання (на основі паперових та аудіоносіїв) так і новітні, зокрема супутникові (дуже дорогі) та Інтернет-технології, але назагал використовуються усі згадані вище технології у різних пропорціях.

Учасники навчального процесу в мережі дистанційного навчання мають безліч можливостей, зручностей та пріоритетів, серед яких:

- навчатися в зручний для себе час та в обраному університеті;

- саме дистанційна форма навчання є найкращим варіантом для людей із обмеженими можливостям;
- індивідуальний навчальний план та графік навчання;
- можливість розбиття матеріалу на окремі, функціонально завершені модулі, які вивчаються у міру засвоєння матеріалу і відповідають здібностям окремого студента;
- власний on-line консультант;
- доступ до найкращих світових методик викладання та навчання, електронних навчальних курсів європейського рівня, відеолекцій та відеоконференцій;
- об'єктивність оцінювання знань (часткова відсутність людського фактору);
- одночасно навчатися та працювати, не залишаючи основне місце роботи;
- метод навчання дешевший, ніж традиційні, завдяки ефективному використанню навчальних приміщень, полегшеному коригуванню електронних навчальних матеріалів та мультидоступу до них і для декого є оптимальним способом отримання освіти;
- відсутність географічних обмежень, що дає можливість навчатися на різних курсах у кращих закордонних університетах;
- можливість навчання на двох спеціальностях одночасно або за програмою спільного навчання та отримання диплому європейського зразка.

Для навчання за дистанційною формою освіти необхідне виконання деяких технічних умов, а саме: наявність власного комп'ютера, бажано веб-камера, хороший інтернет-зв'язок, програмне забезпечення на вашому комп'ютері для ведення конференцій (наприклад *Skype*), доступ до електронної бібліотеки університету, власна електронна пошта та ін. Так наприклад, для проведення захисту курсових робіт і надання консультацій у режимі *on-line* «викладач-студент» із залученням відеофіксації роботи обох необхідне спеціальне програмне забезпечення «*On-line спілкування з відео фіксацією*». Зрозуміло, що на сьогодні не всі регіони України, та й не всі сім'ї забезпечені такими умовами. Не останню роль у технології дистанційного навчання відіграє

методичний супровід цього процесу і як завжди людський фактор.

Як вибрати потрібний університет? Дистанційна освіта у нашій країні з'явилась не так давно, тому будьте обережні із вибором навчального закладу. В першу чергу в університеті повинна законно бути дистанційна форма навчання. Якщо є можливість, з метою економії коштів, поцікавтеся чи немає поблизу вашого місця проживання філії цього університету за обраною вами спеціальністю. Обов'язково пройдіть відповідний тренінг, де вам зобов'язані дати вичерпну інформацію на наступні запитання: що являє собою дистанційне навчання як форма здобуття освіти, як саме повинен здійснюватися процес навчання (вимоги до виконання контрольних, розрахункових, аналітичних, курсових робіт, спосіб складання іспитів та тестів, проходження практики, спосіб спілкування з науковим керівником та виконання дипломної роботи), скільки він триває, які саме вимоги ставляться до студентів, що навчаються за цією формою, як довго вже існує ця програма, який відсоток студентів успішно завершив її, скільки буде коштувати навчання та інше. Бажано особисто зв'язатися зі студентом чи випускником даного ВНЗ та форми навчання і поставити усі ті запитання, які вас цікавлять. Якщо мова іде про вибір курсу за кордоном, слід особливо ретельно перевірити наявність у навчального закладу акредитації, виданої відповідним органом. Приміром, у США акредитувати школу має право Council for Higher Education Accreditation (Рада з акредитації освітніх закладів).

Ця інформація допоможе вам зробити правильний вибір на користь того чи іншого навчального закладу.

Разом з тим, дистанційне навчання не позбавлене і ряду недоліків як на організаційному рівні держави так і навчання студента:

- нечітко сформульована та недостатньо обгрунтована стратегія розвитку дистанційної освіти з боку Міносвіти (нормативно-правові, фінансові питання, критерії та оцінка якості);
- недостатній рівень комп'ютеризації системи навчальних закладів та суспільства вцілому;

- непрозорий набір студентів призвів до розпорошення наукового потенціалу, дублювання розробок програмного забезпечення та повне ігнорування авторських прав;
- для ВНЗ на сьогодні залишається проблемою якісна організація дистанційного навчального процесу, особливо коли йде мова про технічні спеціальності з великою кількістю лабораторних робіт де використовується спеціальне обладнання;
- надлишкова завантаженість викладачів українських ВНЗ у порівнянні з європейськими та світовими стандартами, результатом якої є недостатній контакт між викладачем і студентом;
- самостійне освоєння навчального матеріалу вимагає від студента самоорганізації, відповідальності та мотивації, що підсилу не всім;
- відсутність особистого контакту між самими студентами (чим з задоволенням користуються студенти очної форми навчання);
- відсутність спеціальної підготовки кадрів викладачів, методистів, деканатів для застосування телекомунікаційних технологій.

Висновки. Сучасний ринок освіти пропонує багато можливостей навчатися дистанційно. З подальшим розвитком інформаційних технологій дистанційна освіта може стати широко вживаною формою навчання, але сьогодні слід уважно вибирати ВНЗ та навчальну програму і оцінювати свої можливості. Слід пам'ятати і бути готовим до цього, що не всі студенти дистанційної форми навчання отримують бажаний диплом. Особливо це стосується закордонних університетів, наприклад в Німеччині диплом за дистанційною формою навчання отримують тільки 20% з тих студентів, котрі вибрали саме дистанційну форму навчання.

Першу освіту, краще отримати по повній програмі за очною формою навчання. До дистанційної освіти зручно звертатися при отриманні другої вищої освіти, проходженні додаткових курсів підвищення кваліфікації, особливо, якщо ви зупинили свій вибір на західній бізнес-школі, а часу та можливості їхати навчатися за кордон просто немає.

На даному етапі дистанційна освіта в Україні успадкувала майже всі ознаки та недоліки заочної форми навчання, тому поки що вона не в повній мірі оправдовує покладених на неї сподівань.

1. Веремчук А. Проблеми і перспективи дистанційного навчання у ВНЗ.
2. Електронний ресурс topcareer.ru.
3. Закон «Про освіту» від 01.07.2014 № 1556-VI.
4. Наказ міністерства освіти і науки України «Про затвердження Змін до Положення про дистанційне навчання» №761 від 14.07.2015 р.
5. Рішення Колегії Міністерства освіти і науки України «Про стан і перспективи розвитку дистанційного навчання в Україні» від 23 червня 2005 р.
6. «Концепція розвитку дистанційної освіти в Україні» від 20 грудня 2000р. затверджена Постановою МОН України.
7. Васюк О. Теоретико-методичні аспектиорганізації дистанційної освіти / О.Васюк// Вісник книжкової палати України. – 2011. – №2. – С.–30–32.

Стан дистанційної освіти в країнах світу

Кулешник Я.Ф.,
доцент кафедри інформатики Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Рудий Т.В.,
професор кафедри інформатики Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент
Андрецуляк Д.Д.,
курсант Львівського державного університету внутрішніх справ

Дистанційне навчання, як спосіб спілкування між вчителем та учнем, виникло в Європі, коли у 1840 році англієць Ісаак Пітман вирішив використати поштовий зв'язок для навчання студентів. Німецькі викладачі Чарльз Тюссе та Густав Лангеншейдт у 1856 році розпочали заочно викладання мови у Німеччині. У 80-х

роках XX століття поширився термін «дистанційна освіта» (ДО), основною характеристикою якої є відокремлення вчителя від учня. Саме в цьому полягає різниця між ДО та традиційною освітою. ДО включає в себе дві підсистеми: дистанційне викладання та дистанційне навчання.

Головною метою створення системи дистанційної освіти (СДО) в Україні, як і у всому світі, є забезпечення загальнонаціонального доступу до освітніх ресурсів шляхом використання сучасних інформаційних технологій та телекомукаційних мереж і надання умов для реалізації громадянами своїх законних прав на здобуття освіти.

СДО може позитивно впливати на вирішення таких соціальних проблем як:

- підвищення рівня якості освіти та освіченості суспільства;
- реалізація потреб населення в освітніх послугах;
- підвищення соціальної і підприємницької активності населення;
- формування єдиного освітнього простору в рамках усього світового співтовариства.

Сьогодні дистанційна освіта – поширене явище у багатьох країнах світу. З кожним роком застосування та популярність її зростає. У табл. 1 показані деякі країни світу, провідні університети, кількість студентів та напрямки підготовки.

Таблиця 1.

Порівняльні характеристики провідних університетів світу з дистанційного навчання

№ з/п	Країна	Університет	Дата засну-	Кількість	Напрямки підготовки	Кількість курсів (центрів підготовки)
1.	Індія	Національний відкритий університет Індіри Ганді	1985	Більше 185000	Програми для жінок, інвалідів, домогосподарок, людей з низькими доходами	

Таблиця 1. (продовження)

2.	Китай	Національна мережа радіо- та телевізійних університетів (CRTVU)	1979		Природничі науки, інженерія й технологія, гуманітарні науки, економічне управління, сільське господарство й лінгвістика	229
3.	Туреччина	Університет Анадолу	1982	Більше 300000	курси в галузі економіки й адміністративного права, архітектури, медицини, фармакології, комунікації й зв'язку із громадськістю	
4.	Ізраїль	Відкритий університет Ізраїлю	1974	Більше 12000	природничі науки, математика, обчислювальна техніка, управління, іудаїстика, музика та мистецтво	більше 200 курсів; 60 навчальних центрів по всьому світу
5.	Індонезія	Університет Тербука	1984	Більше 172000	сільське господарство, статистика, комп'ютерні та інформаційні технології, соціальні науки тощо	32 центри у різних країнах світу
		Індонезійський інтитут розвитку банківської справи	1985	5000	програма підготовки фахівців з позик; банківське управління в сільському господарстві	Навчаються тільки жителі Індонезії
6.	Німеччина	Заочний університет міста Хаген		50000		

Таблиця 1. (продовження)

7.	Шрі-Ланка	Відкритий Університет Шрі-Ланка	1980	Більше 16000	Підприємництво, текстильна технологія, юриспруденція, освіта тощо	Університет має мережу регіональних центрів у всіх великих містах країни, 20 навчальних програм
8.	Тайвань	Національний Відкритий університет	1986	Більше 62000	спеціалізовані курси: комерція, бухгалтерський облік, інформаційні технології, юриспруденція, статистика, торгівля, психологія, соціологія тощо.	курси трьох типів: обов'язкові курси, іноземні мови, спеціалізовані курси
9.	В'єтнам	В'єтнамський національний інститут відкритого навчання	1968	Більше 50000	електротехніка, металообробка, комп'ютерна техніка, економіка, маркетинг, лінгвістика тощо	
10.	Тайланд	Сукотай Таматірат Відкритий університет	1978	Більше 70000	мистецтво, управління, юриспруденція, сільське господарство, охорона здоров'я, політичні науки	
11.	Пакистан	Відкритий університет	1974	90000	функціональне навчання, підготовка вчителів, середня освіта, дослідницькі програми дистанційного навчання	більше 200 курсів за 36 програмами

Таблиця 1. (завершення)

12.	Південна Африка	INTEC college	1908	більше 68000	курсів в галузі бізнесу, технічних спеціальностей, комп'ютерних наук, мистецтва й педагогіки	більше 100 курсів, що методично й змістовно відповідають освітнім стандартам ПАР
13.	Велика Британія	Відкритий університет Великої Британії	1969		пропонує 3 види навчання: на ступінь бакалавра, післядипломне й продовжене	250 навчальних центрів, розташованих у багатьох містах країни й світу
14.	Іспанія	Національний університет дистанційної освіти	1972	124000	курси навчання на рівні бакалаврату, магістратури й продовженої освіти	50 навчальних центрів та 8 центрів за межами Великобританії
15.	США	Національний технологічний університет (Колорадо)	1984		забезпечує потреби в дипломованих інженерах й адміністраторах, а також присвоює ступені й видає сертифікати рівня магістра	понад 40 університетів США беруть участь в академічних програмах, запропонованих Національним технологічним університетом
16.	Канада	Університет Атабаска	1970	Більше 11000	управління, мистецтво, торгівля, а також ступеня магістра в галузі дистанційної освіти	більше 250 курсів
		Телеуніверситет Квебеку	1972	20000	менеджмент, зв'язок, соціальні та гуманітарні науки, тощо	навчання за 13 сертифікованими програмами та 12 короткими програми професійної перепідготовки

Фінансування дистанційної освіти.

Проблема фінансування дистанційної освіти є значущою в її організації та функціонуванні, і кожна країна має свій власний досвід у її вирішенні. У табл. 2 показано варіанти вирішення питання фінансування СДО у деяких країнах світу.

Таблиця 2.

Фінансування СДО у деяких країнах світу

Країна	Внесок держави (%)	Внесок студентів (%)	Інші вкладники (%)
Іспанія	46	47	7 (спонсори)
Велика Британія	85	15	
Китай	100 (зареєстровані слухачі)	$200 (вільні слухачі)	
Канада	75-80	10	10-15
Корея	60	40	
Японія	85	15 (134 грн.)	
Україна		3000 – 7000 (грн.)	

Висновки. На основі поданих таблиць можна зробити висновок, що система дистанційної освіти використовується по всіх материках землі. Особливого розвитку такий спосіб навчання отримав у країнах Азії та Північної Америки. В Україні за останніх майже десять років значно зросло число користувачів СДО, але значні проблеми і затримки з виробленням стратегії розвитку та фінансування гальмують бажане впровадження якісної дистанційної освіти.

1. Демида Б., Сагайдак С., Копил І. Системи дистанційного навчання: огляд, аналіз, вибір // Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. – 2011. – № 694. – С. 98−107. 5.
2. Величко В.Ю., Камишин В.В., Стрижак О.Є. Інформаційні технології формування сучасних систем знань як основа інноваційного розвитку освіти // Матеріали міждисциплінарної науково-практичної конференції «Інноваційні технології навчання обдарованої молоді» 08–09 грудня 2010 року в м. Київ. – ІОД. – 2010. – 168 с.
3. Стефаненко П. В. Теоретичні й методичні засади дистанційної освіти у вищій школі. − К. – 2002.
4. Кухаренко В.М., Рибалко О.В., Сиротенко Н.Г. Дистанційне навчання. Умови застосування. Дистанційний курс. За ред. Кухаренко В.М. – Харів: Торсінг, 2001. – 320 с.

Використання інформаційних технологій у профорієнтаційній роботі вищого навчального закладу

Левус Є.В.,
доцент кафедри програмного забезпечення
Національного університету «Львівська політехніка»,
кандидат технічних наук, доцент
Лешкевич І.Ф.,
здобувач освітнього ступення «магістр»
Національного університету «Львівська політехніка»

Професійна орієнтація – це наукова дисципліна, яка допомагає людині обрати свою майбутню професію з урахуванням всіх її здібностей, потреб і бажань. Відповідно, як наукова дисципліна, професійна орієнтація має зв'язок з такими сферами як соціологія, статистика, психологія, медицина, педагогіка.

Основною метою будь-якої професійно-орієнтаційної роботи є насичення ринку праці мотивованими та конкурентноздатними працівниками, що сприяє економічному розвитку держави.

Профорієнтаційна робота складається з таких етапів:

1. **Інформаційний етап**. На цьому етапі людина отримує інформацію про різноманітні професії та галузі. По завершенню цього етапу у людини формується бачення поточної ситуації на ринку праці, розуміння суті різних професій і відмінності між ними. Статистика свідчить, що на даний час існує більше 40000 професій.
2. **Діагностичний етап**. Якщо на попередньому етапі усі професії розглядалися як рівнозначні та з нейтральної точки зору, то на цьому етапі основне завдання – встановити нахили та уподобання особи, розділити усі професії на *бажані*, *прийнятні* та *неприйнятні*. Для цього існують різні психологічні методики, наприклад тести на визначення складу характеру (меланхолік, сангвінік, тощо), тест на визначення професійної спрямованості за методикою Голланда та інші.
3. **Консультаційний етап.** На відміну від інших етапів, консультаційний етап завжди проводиться індивідуально. На

цьому етапі абітурієнт отримує індивідуальну консультативну допомогу спеціаліста з професійної орієнтації. У процесі консультації може відбутися як затвердження обраної на попередньому етапі професії, або спроба переорієнтації особи на іншу спеціальність, з урахуванням її здібностей та можливостей, якщо обрана нею професія є неактуальною, або її здобуття є нереалістичним.

4. **Етап трудових спроб.** Цей етап проходять особи, що остаточно визначилися з професією на попередньому етапі. Суть цього етапу в ознайомленні особи з типовими умовами праці, робочими місцями, оснащенням. Цей етап часто поєднується з навчальною практикою. Цей етап проводиться безпосередньо на реальних робочих місцях.
5. **Етап співбесіди.** Цей етап по суті означає завершення профорієнтаційної роботи, оскільки полягає в проходженні об'єктом співбесіди з працедавцем з метою визначення ступеня його готовності до реальної роботи та його професійних навичок. Цей етап здебільшого не відносять до професійно-орієнтаційної роботи, оскільки на момент проходження співбесіди особа уже фактично оволоділа професією.

Оскільки в Україні відсутня єдина та цілісна програма професійної орієнтації, багато навчальних закладів намагаються вирішувати проблему локально, здійснюючи такі заходи, як:

- встановлення профорієнтаційних терміналів (у школах);
- проведення екскурсій, днів відкритих дверей та інших подібних заходів на підприємствах, фірмах, чи запрошення їх представників до навчального закладу для проведення агітаційної роботи;
- створення на базі навчальних закладів посади працівника з профорієнтаційної роботи.

Створення спеціалізованих інформаційних порталів на базі навчальних закладів є іншим типовим способом вирішення проблем у галузі професійної орієнтації. Більшість з цих порталів є схожими і, відповідно, мають спільні недоліки, зокрема:

- із всіх етапів профорієнтаційної роботи такі портали проводять лише перший, інформаційний;

- інформація, надана такими ресурсами, часто є надто загальною;
- уся інформація подана у вигляді звичайного нагромадження тексту, що заважає її сприйняттю користувачем;
- відсутній зворотній зв'язок з відвідувачами порталу.

Усі ці недоліки призводять до того, що профорієнтаційні інтернет ресурси не користуються популярністю серед школярів та їх батьків, а отже мало сприяють вирішенню проблеми професійної орієнтації. Тому однією з пріоритетних задач при створенні власного подібного порталу є врахування негативного досвіду ресурсів-аналогів та знаходження ефективних способів виправлення описаних недоліків.

Веб-ресурси, що відтворюють певну підмножину необхідного функціоналу. Зокрема:

1. Освітній портал http://prof.osvita.org.ua/ Благодійного фонду «Розвиток України». Основними перевагами сайту є інформативність, зручна організація інформації, можливість проходження різноманітних профорієнтаційних тестів. Недоліки: незручна для користувача візуальна форма представлення інформації, а сама інформація рідко оновлюється.
2. Профорієнтаційний портал Кафедри інформаційно-вимірювальної техніки НТУУ «КПІ» http://imt-career.kpi.ua/. Сайт орієнтований на вступників до НТУУ «КПІ». Переваги: розділ новин часто оновлюється, присутній зворотній зв'язок. Недоліками є нестача інформації, візуальні недоліки, відсутність профорієнтаційних тестів.
3. Портал Інтелектуального навчально-наукового центру професійно-кар'єрної орієнтації НУ «ЛП» http://abc.lp.edu.ua/. Перевагами є зручний дизайн, актуальність представленої інформації, але всі ці переваги перекреслює той факт, що на сайті повністю відсутня інформація пов'язана з професійною діяльністю, натомість висвітлюються питання вступу та наукової діяльності.

Пропонується розробити продукт вигляду веб-сайту, що складатиметься з декількох розділів різного призначення. Основні групи функціональних можливостей описано діаграмою прецедентів (Рис. 1).

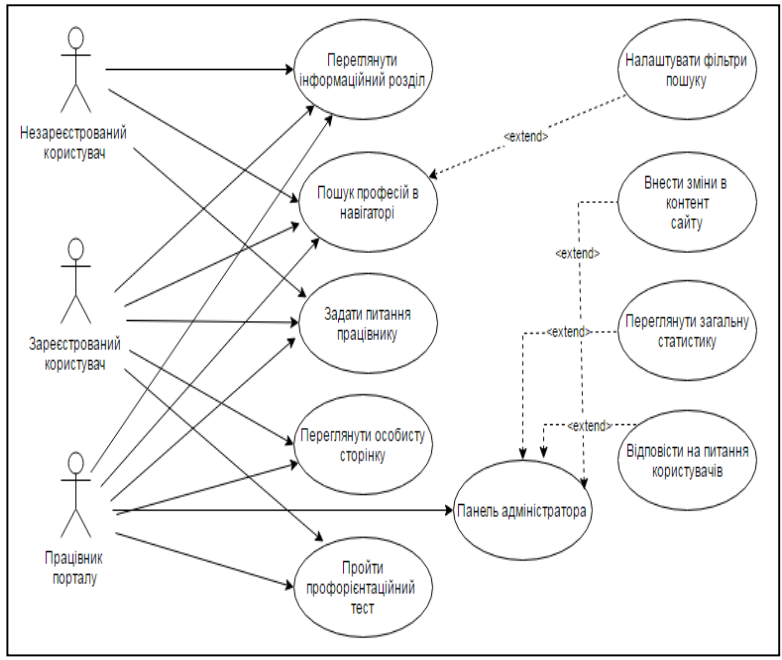


Рис.1. Моделювання функціональних вимог профорієнтаційного веб-порталу.

Приклад роботи у розділі «Навігатор професій», який призначений для пошуку професій з використанням фільтрів представлено на Рис.2.

З точки зору маркетингу освітніх послуг важливо відслідковувати популярність тої чи іншої професії, а також відповідного навчального закладу. Інновацією може бути використання підходу *бренд-трекінгових систем*, що типово використовуються у комерції.

Бренд-трекери – автоматизовані системи, які відстежують згадування та коментарі за ключовими словами/тегами з можливістю визначення тональності повідомлень та вивантаження даних у зручному для сприйняття форматі. Аналізуючи усі відгуки і будь-які згадки про спеціальність і відповідний ВНЗ у соціальних мережах, ВНЗ отримує інформацію, яка є важливою для репутації і популярності як самого ВНЗ, так і відповідної спеціальності.

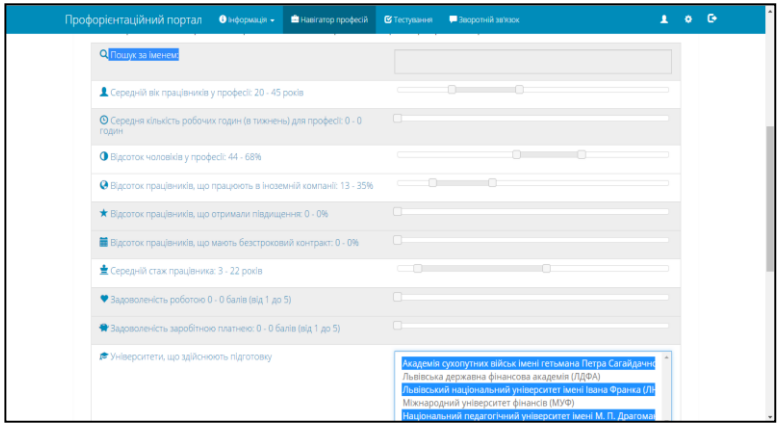


Рис.2. Панель фільтрації професій у «Навігаторі»

Варто передбачити дві частини системи:

- Бренд-трекер для соціальної мережі (н-ад, ВКонтакте), який служить для отримання та аналізу відгуків про ВНЗ в режимі реального часу;
- Веб-сайт для перегляду інформації про топ-ВНЗ та результати аналізу відгуків.

Висновок. Успіх профорієнтаційної роботи залежить як від ефективного використання ІТ, так і вміло застосованих методів педагогіки і психології. Запропоноване рішення у вигляді Веб-порталу є багатофункціональною системою, перспективи розвитку якої у застосуванні методів штучного інтелекту.

1. Schiersmann, C., Ertelt, B.-J., Katsarov, J., Mulvey, R., Reid, H, & Weber, P. (eds.) (2012). NICE Handbook for the Academic Training of Career Guidance and Counselling Professionals. Heidelberg: Heidelberg University, Institute of Educational Science. – p. 7.
2. Верьовка П. Етичні засади соціальної профорієнтаційної роботи державної служби зайнятості / Соціальний захист. – 2000. – № 4. – С. 31-37.
3. Професійна орієнтація як система [Електронний ресурс]. Режим доступу: http://library.if.ua/book/147/9778.html.
4. Ожиєвська А. Моніторинг соціальних медіа: «хороший тон чи необхідність для бізнесу» / Lviv SMM Camp 2014 [Електронний ресурс] – http://www.slideshare.net/ojynka/monitoring-oguevska-smm-camp-lviv

Напрями застосування інформаційно-аналітичного прогнозування у виявленні та припиненні злочинних дій з платіжними картками

Лепеха О.М.,
ад'юнкт кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ

Одним із безпосередніх і кваліфікованих напрямів оперативно-службової діяльності відокремлених територіальних підрозділів кіберполіції є виявлення та припинення кримінальних правопорушень у сферах платіжних систем, зокрема злочинних дій із платіжними картками, відповідальність за які передбачена ст. 200 Кримінального кодексу України. Одним із дієвих заходів оперативно-розшукової діяльності, який дозволяє ефективно протидіяти незаконному обігу платіжних карток, є інформаційно-аналітичне прогнозування.

Аналітична робота незалежно від сфери застосування представляє собою творчу діяльність, пов'язану із оцінкою наявної інформації і підготовкою на цій основі управлінських рішень. Пасивне очікування потоку корисної в оперативному аспекті інформації суперечить принципам оперативно-розшукової діяльності. З цією метою ефективної протидії «картковій» злочинності силам оперативно-розшукової діяльності необхідно передбачати можливий розвиток криміногенних тенденцій в майбутньому з метою їх випередження та недопущення настання суспільно-небезпечних наслідків. В контексті дослідження, завданням інформаційно-аналітичного прогнозування злочинних дій з платіжними картками є необхідність взаємоузгодження заходів із швидкого та ефективного реагування зацікавлених суб'єктів з метою нейтралізації суспільно-небезпечних дій з платіжними картками. Ефективність існування зазначеного заходу обумовлюється існуванням наступних елементів:

1. Формування розгорнутого реєстру інформаційних ресурсів (гласних, негласних).
2. Створення системи відбору та аналізу оперативної значимої інформації.

3. Створення інтегрованої системи повідомлення про надходження та визначення «корисної» інформації.

Інформаційно-аналітичний прогноз злочинних дій з платіжними картками – передбачення можливостей із пошуку та отримання відкритої інформації з інформаційно-телекомунікаційних систем, інших мереж та джерел про тенденції виникнення, розвитку та припинення злочинних дій з платіжними картками.

Метою інформаційно-аналітичного прогнозування є визначення напрямів і форм діяльності суб'єктів протидії злочинним діям з платіжними картками (банківські установи, правоохоронні органи, міжнародні організації) та наслідків прийнятих в майбутньому організаційно-управлінських рішень.

Інформаційно-аналітичне прогнозування може здійснюватися як щодо проблеми в цілому, так і по відношенню до конкретної оперативно-розшукової ситуації та спрямоване на передбачення ознак злочинної діяльності із платіжними картками. Інформаційно-аналітичне прогнозування здійснюється фізичною особою (аналітиком) чи ЕОМ із спеціалізованим програмним забезпеченням. До основних об'єктів інформаційно-аналітичного прогнозування злочинних дій з платіжними картками відносимо:

- соціальні явища;
- фактори, що визначають тактику протидії злочинним діям із платіжними картками (рівень, структура, динаміка злочинності; соціально-економічні зміни в суспільстві; тенденції кримінальних структур та їх учасників).

Функціями інформаційно-аналітичного прогнозування злочинних дій з платіжними картками є:

- прогнозування можливої поведінки членів організованих груп після вчинення кримінальних правопорушень з метою вибору тактики їх виявлення та припинення, у тому числі затримання при спробі збуту платіжних карток;
- прогнозування розвитку конкретної ситуації з визначенням та розстановкою сил та засобів оперативного документування;
- прогнозування оперативного перекриття визначених об'єктів, що становлять конкретний оперативний інтерес, довіреними особами та агентами;

- прогнозування поведінки неформальних груп, які спеціалізуються на використанні комп'ютерних технологій, індивідуальної злочинної поведінки – для профілактики та попередження злочинних дій з платіжними картками.

Сьогодні наукою розроблено методи для систематизації важливих зв´язків отриманої інформації. Вибір методу залежить від спеціалізації фактичного матеріалу та заданої мети. У процесі інформаційно-аналітичного прогнозування злочинної діяльності з платіжними картками доцільним є застосування наступних методів: аналіз ділової документації (здобуття інформації із електронних масивів з метою виявлення специфічних транзакцій); аналіз кримінальних проваджень (виявлення причин і умов скоєння злочинної діяльності із платіжними кратками); оперативний аналіз (аналіз оперативно-розшукової ситуації в межах оперативно-розшукової справи чи справи контрольного провадження); аналіз фінансової документації (дослідження операцій по конкретному рахунку з метою виявлення ознак злочинної діяльності); метод аналогії (зіставлення із схожими випадками злочинної діяльності); метод експертних оцінок (оцінка результатів на підставі передбачень спеціалістів).

Враховуючи той факт, що в кінцевому результаті платіжні картки будуть використані як платіжний засіб, важливим в інформаційно-аналітичному прогнозуванні фактором є обмін даними із фінансово-кредитними установами, зокрема банками, в яких є власні служби безпеки, аналітичні відділи

Розробка програмного забезпечення для спрощення наповнення СЕН на базі moodle

Мельничин А.В.,
доцент кафедри теорії оптимальних процесів Львівського національного університету імені Івана Франка, кандидат технічних наук, доцент

Однією з особливостей нашого часу є перехід країн світу від індустріального до інформаційного суспільства. Як свідчать дослідження, кожні два-три роки обсяги знань, породжені світовою

спільнотою, подвоюються. Тому в сучасному інформаційному суспільстві виникає потреба здобувати, критично осмислювати та використовувати актуальну інформацію.

Основою процесу інформатизації суспільства є інформатизація освіти, що є не менш важливою, аніж інформатизація інших напрямів суспільної діяльності, оскільки саме тут формуються загальнокультурний соціальний і професійний фундамент для інформаційного суспільства.

Саме системи електронного навчання (СЕН) дозволять найбільш ефективно реалізувати можливості, що закладені в нових вимогах, які перед нами висуває сьогодення технологіях.

Електронне навчання – сукупність сучасних технологій, що забезпечують доставку інформації в інтерактивному режимі за допомогою використання інформаційно-комунікаційних технологій від тих, хто навчає, до тих, хто навчається.

Основними принципами електронного навчання є інтерактивна взаємодія у процесі роботи, надання студентам можливості самостійного освоєння досліджуваного матеріалу, а також консультаційний супровід у процесі дослідницької діяльності.

Основною метою впровадження електронної форми навчання є швидке та зручне поширення знань, забезпечення доступності освіти всім верствам населення.

Електронне навчання можна розділити на вивчення дистанційних курсів. Головна мета дистанційного курсу – на основі єдиної системи вивчення всього теоретичного і практичного матеріалу розкрити теоретичні основи предметної області, важливі для вивчення курсів спеціальних дисциплін, формувати практичні вміння і навички, необхідні для аналізу, дослідження і розв'язання прикладних задач, надати допомогу викладачам у здійсненні диференційованого підходу до навчання, сприяти повнішому і глибшому засвоєнню студентами навчального матеріалу.

Переважна більшість навчальних закладів за впровадження систем електронного навчання, якщо ці системи не власної розробки, модифікують їх або додають до них певні модулі.

Тому актуальною є задача проектування та розробки засобу для спрощення створення дистанційних курсів.

Власне така система пропонується у даній роботі. На рис. 1 наведено загальну схему програмної розробки.

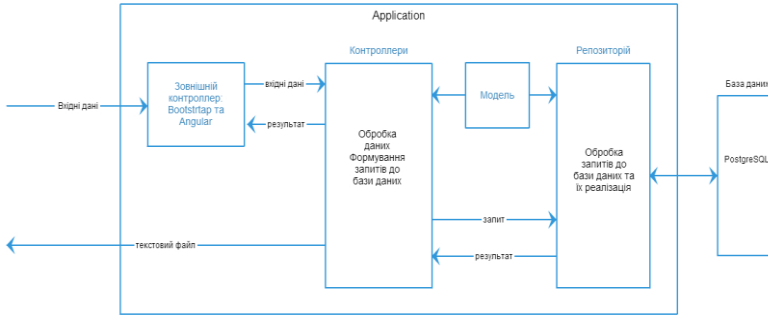


Рис. 1. Схема взаємозв'язків компонентів системи

Необхідні дані, які введені автором курсу, опрацьовуються контроллером. В даній реалізації використано такі контроллери:

- *HomeController* – аналізує початкову сторінку та перенаправляє клієнєна на форму для створення курсу.
- *CourceControlle* – відповідає за отримання та аналіз даних, структуризує їх за допомогою моделі і заносить в БД.
- *ConvertController* – виконує перетворення даних з БД у формат, прийнятний для імпортування в середовище *Moodle*.
- *FileDownloadController* – виконує завантаження сформованого файлу із сервера на персональну машину користувача.

На рис. 2 можна побачити інтерфейс системи у процесі створення електронного курсу.

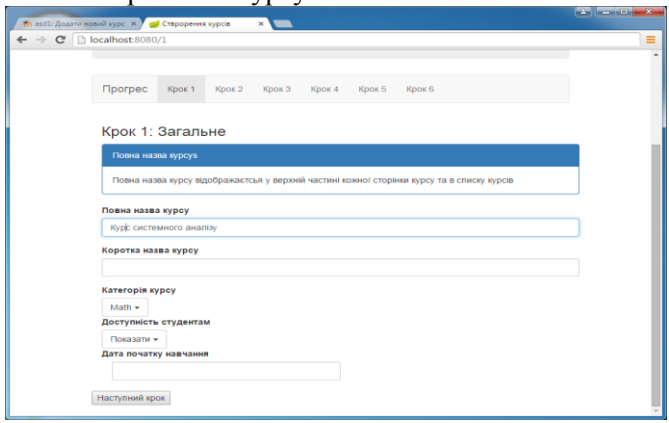


Рис. 2. Вигляд інтерфейсу системи

У роботі проведено теоретичний аналіз і здійснено практичну реалізацію системи спрощення створення навчальних курсів для системи електронного навчання на базі *Moodle*.

При проведенні теоретичного вивчення питання здійснено порівняльний аналіз різних систем електронного навчання, виявлено основні переваги та недоліки різних систем електронного навчання, що дало можливість спроектувати та реалізувати програмне забезпечення з використанням передових технологій у дані сфері.

1. Електронне навчання [Електронний ресурс]. – Режим доступу : http://www.lnu.edu.ua/academics/e-learning/ – Назва з екрана.
2. Офіційний сайт системи MOODLE [Електронний ресурс]. – Режим доступу : http://www.moodle.org – Назва з екрана.
3. Система електронного навчання ВНЗ на базі MOODLE: Методичний посібник / Ю. В. Триус, І. В. Герасименко, В. М. Франчук // За ред. Ю. В. Триуса. – Черкаси. – 220 с.

Використання Big Data у R

Неспляк Д.М.,
доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук
Магеровська Т.В.,
доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент
Мельничин А.В.,
заступник декана факультету прикладної математики та інформатики з навчально-методичної роботи, кандидат технічних наук, доцент
Тучапський Р.І.,
науковий співробітник відділу механіки тонкостінних елементів конструкцій, кандидат фізико-математичних наук
Протиняк Д.А.,
студент Львівського державного університету внутрішніх справ

Big Data [1, 3, 4] показує свій широкий вплив на наше суспільство, сильно трансформує його і буде продовжувати привертати

увагу експертів і громадськості у майбутньому. З величезного обсягу даних з різних джерел і зростаючої швидкості його генерації стає очевидним, що ми живемо в епоху Big Data. Кожні два роки відбувається двократне зростання даних. У даній статті основна увага приділяється доступним системам для роботи з великими об'ємами даних, які включають в себе набір інструментів і техніки для завантаження, вибірки та обробки різнорідних даних, використовуючи при цьому величезну паралельну обчислювальну потужність для виконання складних перетворень і аналізу.

Будь-яка система з використанням Big Data стикається з низкою технічних проблем. Через велике розмаїття різних джерел даних і величезний обсяг надзвичайно важко зібрати, інтегрувати та аналізувати великі об'єми даних. З точки зору швидкого пошуку, масштабованості і безпеки потрібно управляти, зберігати і інтегрувати зібрані великі набори даних і в той же час забезпечувати продуктивність. Big Data аналітики повинні ефективно здійснювати моделювання, візуалізацію, прогнозування та оптимізацію з великими обсягами даних на різних рівнях в режимі реального часу або в майже реальному часі для того щоб отримати додаткові переваги при прийнятті рішень. Розподілені файлові системи і нереляційні бази даних підходять для постійного зберігання і управління масивними схемами вільних наборів даних. У R модель Map Reduce є основою для вирішення завдань групової агрегації у Big Data. Hadoop [2] інтегрує зберігання та обробку даних, управління системою, а також інші модулі, щоб сформувати потужне рішення на рівні системи, яка стає основою у вирішенні Big Data проблеми.

По суті, Big Data означає не тільки великий обсяг даних, але і інші особливості, які відрізняють його від понять «масивні дані» і «дуже великі обсяги даних». Історія Big Data представлена в термінах розміру даних, що представляють інтерес. У 1970-х і 1980-х роках найбільш рання проблема Big Data полягала в переході від мегабайт до гігабайт. В кінці 1980-х років популяризація цифрових технологій спричинила розширення обсягів даних до декількох гігабайт або навіть терабайт, які знаходилися за межами зберігання або можливостей обробки однієї великої комп'ютерної системи. Тоді було запропоновано розпаралелювання

даних для того, щоб розширити можливості зберігання даних і поліпшити продуктивність за рахунок розподілу даних і пов'язаних з ними завдань, таких як побудова індексів і оцінки запитів, в розрізнених апаратних засобах. В кінці 1990-х років почалася епоха швидкого розвитку інтернету разом з масивними напівструктурованими або неструктурованими масивами даних. Проте, беручи до уваги різні набори даних в Big Data задачах, як і раніше складною задачею залишається проблема ефективного представництва, доступу і аналізу неструктурованих або напівструктурованих даних.

При проектуванні розподілених Big Data систем необхідно дотримуватися наступних принципів: хороша архітектура; підтримка різних аналітичних методів; обробка повинна бути розподілена для обчислень в оперативній пам'яті; зберігання даних має бути розподіленим; необхідна координація між обробкою даних і самими даними.

Для того, щоб отримати корисну інформацію з великих об’ємів даних розроблені нові методи і технології для їх аналізу. Розроблено широкий спектр методів і технологій для збору, аналізу і візуалізації великих обсягів даних. Більшість інструментів пакетної обробки даних, таких як MapReduce, засновані на інфраструктурі Apache Hadoop.

Виділяють наступні алгоритми для роботи з Big Data системами: 1) Decision Tree; 2) Random Forest; 3) Support Vector Machine. Decision Tree використовує дерево рішень в якості прогнозної моделі, яка пов’язує знання про елемент з висновками про цільове призначення елемента. Це є один з прогностичних методів моделювання, які використовуються в статистиці, інтелектуальному аналізі даних і машинному навчанні. Random Forest полягає у використанні комітету (ансамблю) вирішальних дерев. Алгоритм поєднує в собі дві основні ідеї: метод беггінга Брейман і метод випадкових підпросторів, запропонований Tin Kam Ho. Основний принцип полягає в тому, що група «слабких учнів» можуть зібратися разом, щоб сформувати «сильного» учня. Алгоритм застосовується для задач класифікації, регресії і кластеризації. Support Vector Machine (SVM) управляє методами навчання, що використовуються для задач класифікації і регресії. Як метод класифікації, SVM є глобальною моделлю класифікації,

яка генерує розділи, які не накладаються один на одного і зазвичай використовує всі їхні атрибути. Алгоритми SVM засновані на максимальній різниці лінійних дискримінантів і схожі на імовірнісні підходи. SVM покладаються на попередню обробку даних для представлення моделі, як правило, набагато вищої вимірності, ніж вихідна особливість простору. Дані з двох категорій, завжди можна розділити гіперплощиною, коли використовується відповідне нелінійне відображення високої вимірності.

Мова R добре відома в якості мови для ведення статистики, аналізу даних, розробки алгоритмів інтелектуального аналізу даних, біржової торгівлі і всіма видами прогнозування. На сьогоднішній день, беручи до уваги стрімко зростаючий потік даних, які повинні бути оброблені і проаналізовані, все більше компаній використовують мову R для досліджень у виробничих процесах.

Людство вступило в еру Big Data, в еру розподілених обчислень, яка є наступним рубежем для інновацій, конкуренції і продуктивності. У цій сфері інформаційних технологій потрібно очікувати нового технологічного стрибка. У представленій оглядовій праці дано короткий огляд можливостей сучасних методів та технологій для роботи з Big Data. Немає ніяких сумнівів в тому, що аналітика для роботи з Big Data все ще перебуває у початковій стадії розвитку, оскільки існуючі методи і інструменти дуже обмежені щоб повністю вирішити реальні проблеми. Таким чином, слід виділяти більші наукові інвестиції з боку урядів і компаній в цю галузь інформаційних технологій.

1. http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal
2. http://www.oracle.com/technetwork/articles/bigdata/hadoop-optimal-store-big-data-2188939.html
3. http://www.oracle.com/technetwork/articles/bigdata/implementing-bigdata-1502704.html
4. https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

Інформаційні технології та технічні засоби у навчальному процесі.

Огірко О.І.,
доцент кафедри економіки та економічної безпеки Львівського державного університету внутрішніх справ, кандидат технічних наук
Огірко І.В.,
професор Української академії друкарства, доктор фізико-математичних наук, професор

Проаналізовано проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності правоохоронних органів та навчальному процесі; представлено впровадження комп'ютерних програм у навчальний процес. Проаналізовано можливості використання інформаційних засобів навчання при підготовці фахівців; представлено впровадження комп'ютерних програм у навчальний процес. Розроблені і впроваджені в навчальний процес навчальні системи з спортивно-педагогічних дисциплінах, математичної статистики, спортивної метрології.

Однією із визначальних інструментів інформатизації суспільства є інформаційні технології. Процес інформатизації освіти припускає використання можливостей сучасних інформаційних технологій, методів і коштів інформатики для реалізації ідей навчання, інтенсифікації всіх рівнів навчально-виховного процесу, і навіть підвищення його ефективності і забезпечення якості, підготовки в умовах інформатизації суспільства. Рівень підготовки в системі вищої освіти вимагає нових підходів та засобів. Згідно стандартів освіти європейського рівня, більшість навчального матеріалу студент має опановувати з використанням сучасних інформаційних систем. Існують передові технології комп'ютерного навчання, які активно впроваджуються. Актуальність проведення досліджень з питань інформатизації навчального процесу полягає у розробці комп'ютерних програм для забезпечення навчально-тренувального процесу. Система інформації формується під впливом багатьох чинників. Її розвиток відбувається синхронно із розвитком науки та практики, а розвиток інформаційних технологій дозволяє виробити принципово

нові підходи до розв'язання поставлених проблем, зокрема вдосконалення системи інформації галузі, оперування інформаційними процесами, створення єдиного інформаційного простору, а відтак, ринку інформації та вироблення спільних методик її використання та розповсюдження; налагодження інформаційної взаємодії інформаційних посередників з метою задоволення потреб в інформації фахівців.

Сучасна галузева інформаційна система сформована на основі масивів навчальної інформації шляхом цілеспрямованого накопичення вітчизняної наукової інформації, фахово обґрунтованого відбору найкращих сучасних наукових видань, створення відповідної до потреб сьогодення системи інформаційного забезпечення навчально-освітнього процесу та надання необхідної інформації для наукових досліджень. Інформаційне середовище – система процесів, в основі яких с накопичення та організація інформаційних ресурсів. Систему інформаційного простору, який об'єднує вищі навчальні заклади, великою мірою визначає процес формування інформації, від якого залежить її тематико-типологічна структура і повнота забезпечення навчальних дисциплін. Це у свою чергу визначає конкретні способи накопичення та джерела отримання інформаційних ресурсів.

Головним критерієм інформаційного процесу накопичення є система її формування та розвиток. В умовах впровадження сучасних інформаційних технологій змінюється технологічна основа функціонування системи наукової інформації. Усе більш популярними стають електронні журнали як сучасна форма подання результатів актуальних, галузевих досліджень. Виникають і розвиваються нові форми отримання та розповсюдження інформації. Відсутність добре організованої системи інформаційного електронного забезпечення наукових досліджень відбивається на якості та термінах виконання науково-дослідних робіт. Вихід із ситуації полягає у реалізації проекту єдиного інформаційного простору. Аналізуючи досвід, для надання якісних і ефективних послуг у системі інформування в першу чергу необхідно: здійснювати фільтрацію інформації;забезпечити доступність інформації для всіх споживачів; забезпечити її достовірність і оперативність; забезпечити централізоване, державне накопичення та поширення інформації; створити єдину галузеву інформаційну

систему по вертикалі структурних підрозділів органів виконавчої влади та органів місцевого самоврядування; забезпечити розвиток інформаційної системи за рахунок бюджетних призначень.

Математичне моделювання динамічних систем вимагає комп'ютерної підтримки. Можливості аналітичних методів рішення складних математичних завдань, однак, дуже обмежені й, як правило, ці методи набагато складніше чисельних. Найважливішим етапом моделювання динамічних систем є поділ вхідних параметрів за ступенем важливості впливу їхніх змін на вихідні. Розглядаються основні принципи моделювання динамічних систем, у стислій формі відображаючи той достатньо багатий досвід, що накопичений до теперішнього часу в області розробки й використання математичних моделей динамічних систем. При прийнятті рішень в практиці управління постає питання про задачу прийняття рішень з урахуванням фактору часу. Задача прийняття рішень спрямована на визначення найкращого (оптимального) або сприятливого способу дій для досягнення однієї або декількох цілей. Під ціллю розуміється в широкому значенні ідеальне уявлення бажаного стану чи результату діяльності.

Методи теорії статистичних рішень використовуються, коли невизначеність ситуації обумовлена об'єктивними обставинами, які невідомі або носять випадковий характер. Для розв'язання таких задач використовуються наступні критерії:

Таблиця Критерії теорії статистичних рішень

Назва критерію	*Принцип оптимізації*	*Формула розрахунку*
Критерій песимізму (критерій Уолда, критерій найбільшої обережності)	**Орієнтація на песимістичний розвиток ситуації**	$Y = \min (\max a_{ij})$
Критерій оптимізму	**Орієнтація на оптимістичний розвиток ситуації**	$Y = \max (\max a_{ij})$
Критерій коефіцієнту оптимізму (критерій Гурвіца)	**Орієнтація на рівень оцінки оптимістичного розвитку ситуації**	$Y = \max [\, k (\max a_{ij}) + (1 - k) (\min a_{ij})]$
Критерій Лапласа	**Орієнтація на випадковий розвиток ситуації**	$Y = \max (\sum_{j=1}^{n} a_{ij} \cdot P_j)$
Критерій жалю (критерій Севіджа)	**Орієнтація на мінімізацію втрат або ризиків**	$b_{ij} = (\max_i a_{ij}) - a_{ij}$ $Y = \min_j (\max_i b_{ij})$

Інформатизація освіти – процес забезпечення методологією та практикою від розробки та оптимального використання сучасних інформаційних технологій, орієнтованих реалізацію психолого-педагогічних цілей навчання і виховання у комфортних умовах. Отже, питання оволодіння сучасними інформаційними і комунікаційним технологіями їх використання стає однією з основних компонентів професіональною підготовкою спеціаліста. Це розробки і впровадження в навчальний процес професійно орієнтованих програмних і програмно-педагогічних засобів і курсів, вкладених у оволодіння необхідними знаннями, і накопичення особистого досвіду їх використання їх у професійно- педагогічній діяльності. В процесі проведення досліджень було виявлено основні напрямки розвитку інформаційних технологій навчання у галузі, аналіз наукових робіт провідних фахівців дозволив визначити наявні комп'ютерні навчально-контролюючі системи. Представлено інноваційну методику використання комп'ютерних засобів навчання та контролю як в поточному процесі підготовки студентів на заняттях, так і при самостійному опануванні навчального матеріалу. Спеціаліст з кібербезпеки займається розробкою охоронних систем для різних комунікаційних мереж і електронних баз даних, тестує і вдосконалює власні і сторонні розробки для уникнення ризиків витоку відомостей, що становлять державну або комерційну таємницю, конфіденційну інформацію. Така професія отримала широке розповсюдження у зв'язку з впровадженням комп'ютерних та мережевих технологій практично в усіх організаціях – від невеликих комерційних фірм до органів держбезпеки. При підготовці фахівців з кібербезпеки враховуються академічні та професійні вимоги до спеціалістів в галузі програмування, комп'ютерних наук та інформаційно-комунікаційних технологій. При цьому значну увагу приділено вивченню та практичному застосуванню технологій інформаційної безпеки при розробці систем керування базами даних та знань, мережевих додатків та Інтернет-сервісів, протоколів передачі та шифрування даних. Курси присвячені методам виявлення, блокування загроз та отримання доказів несанкціонованого доступу до інформації з відповідним ступенем секретності корпоративних, банківських та державних інформаційних ресурсів. Існує багато шляхів захисту комп'ютерів, методи, що ґрунтуються на використанні безпечних операційних систем та апаратного забезпечення,

здатного захистити комп'ютерну систему. Математичні методи кібербезпеки передбачають вивчення як класичних, так і сучасних розділів математики, аналітики, системного проектування, технологій забезпечення якості, теоретичних основ захисту інформації, криптології, моделей аналізу ризиків та безпеки складних систем, технологій кібербезпеки.

Кібербезпека забезпечує захист ресурсів (інформація, комп'ютери, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження. До таких заходів безпеки входять контроль доступу, навчання, аудит та оцінка ризиків, тестування, управління та безпека авторизації. Кібербезпека – це безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам. Ми залежимо від безперервності та коректності функціювання комп'ютерних систем об'єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства.

1. Огірко О. Синтаксис оптимізації моделі та моделювання синтаксису механізму розпізнавання символіки алгебри алгоритмів секвенції // Комп «ютерні технології друкарства, № 5, 2000. – С. 296- 303.
2. Огірко І., Шульжик Ю., Огірко О. Інформаційна економіка як напрям дослідження економіки та інформаційних технологій //Формування ринкової економіки в Україні. Львів ЛНУ ім.І.Франка 2001.
3. Огірко І.В., Серант А.Й., Огірко О.І. Концептуальна модель прийняття індивідуального оптимального рішення // Матеріали науково-практичної конференції: «Ефективність державного управління (регіональний аспект)» 22 січня 2001р. – Львів, ЛФ УАДУ, 2001 – С. 116-117.
4. Огірко О. Модель системи генерації програм СКАНЕР // Комп'ютерні технології друкарства, № 6, 2001. – С. 42-48.
5. Огірко О. Синтаксис оптимізації моделі та моделювання синтаксису механізму розпізнавання символіки алгебри алгоритмів секвенції. // Компьютерні технології друкарства, № 5, 2000. – С. 296- 303.
6. Огірко І., Огірко О. Інформаційні технології безпекометрії в поліграфії.III- Міжнародна науково-технічної конференції «Захист

інформації і безпека інформаційних систем». Національний університет «Львівська політехніка» 05 – 06 червня 2014 р. Львів, Україна – С. 46-51.
7. Ткаченко В. П., Огірко І. В., Огірко О. І. Математична модель оцінювання захисту web-сайтів.сб. – Полиграфические, мультимедийные и web-технологии. Т1. – Харьков: ХНУРЭ, 2016. – с. 98-101.
8. Огірко І., Огірко О. Експертно-інформаційна система інноваційної практики. Збірник «Креативна деструкція: інноваційні практики в академічних дослідженнях»: Опубліковано 2016/04 в категорії «Наукові статті» – «Освітні технології» http://www.edu-trends.info/wp-content/uploads/ 2016/04/%D0%9E%D0%B3%D1%96%D1%80%D0%BA%D0%BE1-2.pdf?c6a0f6
9. Kucherov D.P., Ohirko I.V., Ohirko O.I., Golenkovskaya T.I. Neural Network technologies for recognition characters. Electronics and control systems. «National Aviation University» – № 4 (46). – 2015. – P. 65-71.

Критерії та особливості вибору системи дистанційної освіти

Сватюк О.Р.,
доцент кафедри менеджменту Львівського державного університету внутрішніх справ, кандидат економічних наук
Миронов Ю.Б.,
доцент кафедри туризму та готельно-ресторанної справи Львівського торговельно-економічного університету, кандидат економічних наук
Миронова М.І.,
аспірант кафедри теоретичної та прикладної економіки Львівського торговельно-економічного університету

Дистанційна форма навчання завдяки технічному прогресу за останній час набула широкого поширення і стала альтернативою традиційним системам освіти у багатьох країнах світу. Дистанційна освіта показала себе однією з найперспективніших та найефективніших систем підготовки фахівців різних галузей. До недавнього часу на території багатьох країн, особливо тих що раніше входили до складу «соціалістичного табору», дистанційні технології навчання практично не застосовувалися. Насамперед це

було викликано слабким розвитком і недостатнім поширенням технічних засобів передових інформаційних та комунікаційних технологій. Тепер є технічні передумови для активного впровадження та використання *систем дистанційної освіти (СДО)*, а проблема вибору конкретної *СДО* є актуальною та вимагає вивчення. До головних критерії вибору *СДО* можна віднести такі (таб.1).

Проблема вибору платформи, на якій буде працювати СДО, є ключовою, тому при виборі конкретної СДО варто врахувати всі згадані вище критерії, особливо акцентуючи увагу на кошти, які будуть виділені для придбання та підтримки ефективного функціонування системи. Варто відзначити, що не всі СДО є платними, існують і некомерційні продукти, які практично нічим не поступаються своїм «комерційним» конкурентам. Але у будь якому випадку кошти будуть необхідні для закупки обладнання (комп'ютерів), оплати праці найманого персоналу, який обслуговуватиме СДО, викладачів тощо. Розглянемо детальніше переваги та недоліки комерційних та безкоштовних СДО.

Позитивні сторони *комерційного програмного забезпечення* (ПЗ) добре відомі широкому колу користувачів: як правило, це надійні продукти з належною підтримкою та регулярними оновленнями. Однак таке ПЗ має і негативні сторони. Так, наприклад, існує так звана проблема «закритих дверей», коли програмний код джерела недоступний для співробітників освітньої організації, тому навіть незначні зміни у програмному коді практично неможливі. У такій ситуації організація може спробувати вийти на контакт з компанією-розробником, якщо у неї з'явилися якісь раціональні пропозиції щодо вдосконалення платформи.

СДО здійснюється при наявності в учасників такого аппаратного і ПЗ: комп'ютер з процесором не нижче Intel Core i5 (або аналогічної продуктивності); ОС Windows XP (32 біт) версія SP 3 і вище; браузер Firefox версія 40.0 і вище, або аналогічний; USB або вбудована Web камера з роздільною здатністю відео не нижче 1280x720; акустична система; мікрофон; інтернет-з'єднання зі швидкістю: виходить від 10Мбіт/с; входить 10 Мбіт/с.

До негативних сторін також можна віднести досить високу вартість будь-якого комерційного продукту, наявність плати за користування ліцензією, за збільшення загальної кількості користувачів СДО і т.п. До числа комерційних СДО відносяться такі продукти як «Доцент», «Прометей», «RedClass», «IBM Lotus

Workplace Collaborative Learning», «WebTutor», «Naumen Learning», «Oracle Learning Management», «LMS eLearning Server», «Competentum. Magister», «Competentum. Share Knowledge», «Learn eXact» та ін. [1]

Перевагами *безкоштовного програмного забезпечення з відкритим кодом (Open Source)* є як відсутність будь яких витрат на придбання та користування програмними засобами, так і можливість змінювати програмний продукт згідно власних потреб. У даному випадку з'являється можливість об'єднати досвід та талант багатьох викладачів, студентів, волонтерів-програмістів, які будуть сприяти в розвитку та вдосконаленні різного виду освітніх програмних продуктів. До негативних сторін Open Source можна віднести фактор, який виражає страх, невпевненість та сумнів користувачів в надійності і якості безкоштовних програм. Також частим недоліком такого ПЗ є порушення стандартів доступу (accessibility standards) та недостатнього захисту даних. Серед СДО, створених на базі Open Source, можна виділити такі системи як «Moodle», «Dokeos», «LAMS», «Sakai», «OLAT», «ATutor», «Claroline», «OpenACS» та ін. [1]

Аналізуючи в системі Інтернету інформаційні ресурси та відгуки на численних форумах з проблем СДО було виявлено, що найбільший інтерес серед OpenSource представляє собою система «Moodle». Головною відмінною рисою системи «Moodle» можна вважати те, що навколо неї утворилося досить активне міжнародне співтовариство користувачів, які стали ділиться своїм набутим досвідом роботи, обговорюючи при цьому виникаючі проблеми, проводять обмін досвідом своєї роботи та результатів подальшого розвитку середовища.

Аналіз інформаційних ресурсів мережі Інтернет та відгуків на форумах з проблем СДО показав, що найбільший інтерес серед OpenSource систем викликає проект «Moodle». Характерна особливість «Moodle» полягає в тому, що навколо нього сформувалася активна міжнародна спільнота розробників та користувачів, які діляться досвідом роботи на платформі, обговорюють проблеми, обмінюються планами та результатами подальшого розвитку середовища.

Moodle (Modular Object-Oriented Dynamic Learning Environment) [2] – це система дистанційної освіти, метою якої є створення

якісних дистанційних курсів навчання. Цим програмним продуктом широко користуються більш ніж в 100 країнах світу, його використовують школи, університети, компанії та викладачі. Система «Moodle» за своїми можливостями стоїть на рівні з багатьма відомими комерційними продуктами.

Головні переваги СДО «Moodle»:

1. Поширення програмного продукту у відкритому коді, можливість створення і розробки додаткових модулів, інтеграція з освітніми системами.
2. «Moodle» володіє широкими можливостями для комунікації – чат, форум, розсилка, обмін файлами, внутрішня пошта, рецензування робіт студентів.
3. Застосування різноманітних засобів оцінювання.
4. Представлення повної інформації про роботу учнів, їх активність тощо.
5. Інтерфейс програми дає можливість роботи у системі людям різного рівня освіти, різних культур та фізичних можливостей, що уможливлює користування системою навіть людям з особливими потребами.

Система «Moodle» володіє трьома форматами курсів – форум, структура (сюди входять навчальні модулі без прив'язки до календаря), календар (тут всі навчальні модулі прив'язані до конкретних дат календаря). Такий курс містить необмежену кількість ресурсів, куди входять книги, веб-сторінки, каталоги, посилання на файли, а також будь-яку кількість різного виду інтерактивних елементів: тести, опитування, анкети, завдання, лекції, глосарій та інші елементи.

Використовуючи різні поєднання елементів курсу навчання, викладач створює свою систему навчання таким чином, щоб запропоновані форми навчання повністю відповідали цілям і поставленим завданням конкретних занять.

В «Moodle» створено умови для оцінювання всіх елементів курсу, в тому числі і за шкалами, які були створені самими викладачами. Для кожного курсу створюється зручна сторінка, яка дає можливість переглядати останні зміни в курсі, де за обраний період часу викладач має можливість побачити зарахованих на курс студентів, останні повідомлення на форумах, спроби проходження тестів та виконання завдань курсу. Для

роботи у системі викладачі можуть використовувати зручний і простий у роботі текстово-графічний редактор. Крім цього є можливість вводити різні формули в форматі Algebra або TeX. На сьогоднішній день доволі чисельна українська спільнота користувачів надає достатню технічну підтримку даній системі, яка продовжує вдосконалюватися.

Таблиця 1

Критерії вибору системи дистанційної освіти

Критерій	Характеристика
Функціональність	Означає наявність у СДО набору різноманітних функцій, таких як форуми, чати, можливість аналізувати активність учнів, управління курсами і самими учнями та ін.
Зручність користування	Цей параметр показує зручність адміністрування та можливість легко оновлювати існуючий контент на базі створених шаблонів, а також зручність їх використання для кінцевих користувачів
Система перевірки знань	Дає можливість оцінювати фактичні знання учнів в межах СДО
Модульність	Передбачає наявність широкого набору різноманітних блоків (модулів) навчального матеріалу, які можуть використовуватися в інших курсах навчання конкретної СДО.
Мультимедійність	Можливість використання в якості контенту текстових, гіпертекстових та графічних файлів, 3D-графіків, аудіо, відео, gif- і flash-анімації
Вартість	Складовими частинами вартості системи є її ціна, а також різні додаткові витрати на її впровадження і подальший її супровід, наявність або відсутність ряду обмежень щодо чисельності користувачів СДО і т.п.
Стабільність	Цей критерій відображає ступінь стійкості роботи СДО у залежності від рівня активності користувачів
Технічна підтримка	Можливість підтримки стабільної роботи СДО, усунення можливих помилок із залученням фахівців з розробки СДО
Українська локалізація	Локалізована версія продукту виглядає більш дружньою як для адміністрування, розробки курсів, так і для кінцевих користувачів освітніх послуг

1. Готская И. Б. Выбор системы дистанционного обучения : аналитическая записка / И. Б. Готская, В. М. Жучков, А. В. Кораблев [Електронний ресурс]. – Режим доступу : http://ra-kurs.spb.ru/2/0/2/1/?id=13.
2. Освітня платформа «Moodle»: офіційний веб-сайт [Електронний ресурс]. – Режим доступу : https://moodle.org/.

Застосування сучасних інформаційних технологій у дистанційному навчанні

Сеник В.В.,
завідувач кафедри інформатики Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Тема, яку піднято у даній публікації, звичайно, не є новою, оскільки навчання на відстані без відриву від практичної діяльності великої кількості осіб була втілена суспільством через створення системи заочної освіти давно. Сучасний розвиток інформаційних технологій, а саме програмного та технічного забезпечення, його доступності у суспільстві породили нові ідеї впровадження освіти на відстані – створення системи дистанційного навчання.

Системі дистанційного навчання присвячено багато різноманітних досліджень, публікацій, статей, введено у педагогічну освіту нові дисципліни, присвячені методиці та методології проведення такого виду навчання. Однак постійний розвиток інформаційних технологій потребує оновленого погляду не лише на сутність методології дистанційної освіти, а й на удосконалення критеріїв ефективності такого методу навчання.

Про гносеологію дистанційної освіти можна говорити досліджуючи розвиток чи удосконалення визначень поняття «дистанційне навчання». Одним із перших визначень такого поняття було «варіант заочного навчання». Однак, його явно можна було вважати неповним, оскільки подібність даних двох методів навчання полягає лише у тому, що в основу кожного з цих методів

покладена самостійна робота здобувачів освіти. У зв'язку із цим різні дослідники почали пропонувати свої трактування поняття «дистанційного навчання». Такі трактування, зокрема, породжувалися не лише постійним удосконаленням дистанційної освіти, її технологіями, а й розвитком інформаційних технологій. Це призвело до появи наступного трактування дистанційного навчання: «дистанційне навчання – це нова сходинка заочного навчання, на якій забезпечується застосування інформаційних технологій, заснованих на використанні персональних комп'ютерів, відео- та аудіотехніки, космічної техніки та оптичних систем зв'язку». На нашу думку, дане визначення є куди повнішим, хоча в ньому акцентується увага на технічне забезпечення навчання і фактично опущено момент програмного забезпечення. Аналізуючи існуючі визначення, а також вивчаючи систему дистанційної освіти, В.В. Олійник приходить до висновку, що дистанційне навчання – це самостійна педагогічна технологія, яка відрізняється від існуючих, принципово різниться від заочного і аж ніяк не є його різновидом. Основою цієї технології є самостійна робота слухачів, дидактично забезпечена і контрольована. В її структуру органічно входять сучасні форми і методи відбору, конструювання і відображення навчального матеріалу; елементи модульного і комп'ютерного навчання, теорії і практики керованої самостійної роботи; застосування у навчанні інформаційних технологій, телекомунікаційних мереж тощо. Як бачимо з даного визначення, що одним із основних аспектів дистанційного навчання є використання сучасних, постійно оновлюваних інформаційних технологій, як під час проведення навчання, так і під час самостійної роботи та контролю знань.

Враховуючи мету даної публікації нам би хотілось проаналізувати сучасний стан застосування інформаційних технологій у дистанційному навчанні та їх вплив на ефективність такого навчання, оскільки внаслідок стрімкого розвитку інформаційні технології швидко прогресують і, звичайно, у дистанційному навчанні бажано застосовувати найкращі з них. Окрім цього, саме розвиток інформаційних технологій призводить до застосування нових методів дистанційного навчання, удосконалення не лише ефективності даного методу навчання, а й методів контролю знань у здобувачів освіти.

На даний час усе сучасне інформаційне забезпечення дистанційного навчання можна класифікувати на презентаційне та комунікаційне.

Одним із основних атрибутів презентаційного інформаційного забезпечення дистанційного навчання стали електронні версії підручників, посібників, електронні тексти лекцій, інші навчально-методичні матеріали, які є основою для створення дистанційних курсів. Ці продукти створюють основу віртуального навчального середовища. Сюди також слід віднести комп'ютерні тренінги, які розробляються з використанням на лише текстових та графічних даних, а й з додаванням звуку, відео та анімації.

До презентаційного інформаційного забезпечення слід віднести мультимедіа (сучасний стан його розвитку спрямований в сторону розміщення презентацій в мережі Internet); моделювання у віртуальній реальності, суть якого полягає у моделюванні реальної ситуації під час навчання (моделювання проводиться на електронно-обчислювальних машинах, що дозволяє відтворювати поведінку у різних ситуаціях); проектування, яке відрізняється від моделювання, зокрема, значнішими затратами часу та зусиль; електронні ресурси (основна концепція яких зібрати усі ресурси, що потрібні для навчання до користувацького інтерфейсу).

Як окреме презентаційне забезпечення дистанційного навчання необхідно виділити Internet. Завдяки сервісам Internet, наприклад, таким як WWW, FTP, ще більше розширюються можливості дистанційного навчання. Завдяки Internet здобувачі освіти можуть самостійно отримувати завдання та навчальні матеріали із сервера, шукати додаткову інформацію.

До комунікаційного програмного забезпечення дистанційного навчання слід віднести, в основному, два компоненти: телеконференції те електронну пошту. Телекомунікаційні технології взаємодії дозволяють забезпечити здобувачам освіти постійне спілкування не лише між собою, а з викладачем.

Для керування процесом дистанційного навчання, контролю знань, доставки навчального контента здобувачам освіти і забезпечення дидактичними матеріалами потрібно застосовувати відповідне спеціалізоване програмне забезпечення, яке потребує постійного вдосконалення з урахуванням прогресу інформаційних технологій. Воно повинно містити систему автоматизованого

документообігу, словники термінів і інтерактивні мультимедійні підручники, електронні інформаційні бази даних, інші електронні матеріали по всіх курсах. Програмне забезпечення встановлюється на сервері навчального закладу. Але суть дистанційного навчання полягає не лише у наданні навчально-методичних матеріалів. Важливо забезпечити необхідні організаційні заходи для прийому здобувача освіти на навчання, управлінням його навчанням. Також необхідно забезпечити і проведення проміжного і підсумкового контролю знань.

На основі розглянутого вище програмного забезпечення дистанційного навчання необхідно організовувати віртуальні навчальні курси, а також проводити консультації, мережне тестування і підготовку абітурієнтів, забезпечувати самостійну роботу здобувачів освіти, у тому числі денного навчання, створювати індивідуальні навчальні плани і програми, реалізовувати індивідуальні графіки занять поза стінами навчального закладу.

Окрім цього, дану систему у перспективі навчальний заклад може активно використовувати для тестування кандидатів під час прийому на роботу, атестації науково-педагогічних працівників, поширенню та передачі передового досвіду, аналізу ефективності навчання тощо.

Не дивлячись на те, що на даний час залишаються не вирішеними до кінця окремі питання дистанційного навчання, наприклад, питання контролю знань в режимі on-line, дослідження ринку дистанційного навчання говорять про те, що темпи його росту досить високі, а на Заході він оцінюється мільярдами доларів. Тому поважаючий себе вітчизняний освітній заклад повинен бути заінтересований отримати відповідне місце на даному ринку освітніх послуг. Це дозволить не лише підвищити прибуток, а й ліквідує ряд проблем, основними з яких, як правило, є недостача аудиторій, кадрові питання (за допомогою відеоконференції, читати лекції зможуть професори навчальних закладів з інших міст і навіть закордонних країн) тощо.

1. Інформаційний вісник. Вища освіта №17/2005. 2. Сайт Українського центра дистанційного навчання. www.distance-learning.com.ua
2. Олійник В.В. Дистанційне навчання в післядипломній педагогічній освіті : організаційно-педагогічний аспект : навч. посібник / В. В. Олійник. – К. : ЦІППО, 2001. – 148 с.

Сучасні інформаційні технології у науково-дослідницькій діяльності

Сибірна Р.І.,
професор кафедри психології діяльності в особливих умовах Львівського державного університету внутрішніх справ, доктор біологічних наук, професор
Сибірний А.В.,
доцент кафедри менеджменту Львівського державного університету внутрішніх справ, кандидат біологічних наук, доцент
Хомів О.В.,
доцент кафедри економіки та економічної безпеки Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

В умовах сьогодення всі елементи науково-дослідницької роботи тісно пов'язані із збереженням, переробкою та зберіганням інформації, яка являє собою сукупність відомостей (повідомлень, даних), що визначає міру знань про ті чи інші явища, події та їх взаємозв'язки. Тобто, інформація – це відомості, які є об'єктом обробки, передачі і зберігання. Вона є основним поняттям кібернетики – науки про загальні закономірності в процесі управління та передачі інформації.

У своїй діяльності науковець перш за все повинен встановити цільове призначення інформації, оскільки одна і та ж інформація може використовуватися для різних цілей. Зокрема, для створення нових концепцій, встановлення і вирішення проблем пошуку тощо. Цінність інформації визначається економічним ефектом, який дає її використання. Практичним завданням, що стоїть перед дослідником, є визначення того, яка інформація йому необхідна. Разом з тим, необхідно видаляти інформацію, яка не має прямого відношення до об'єкту дослідження.

В умовах сьогоднішніх інформаційних технологій найбільш використовуваними у науково-дослідній діяльності є комп'ютерні мережі та електронні бібліотеки.

Комп'ютерна мережа являє собою систему розподіленої обробки інформації, що складається з кількох комп'ютерів, які

взаємодіють між собою за допомогою спеціальних засобів зв'язку, тобто сукупність з'єднаних один з одним комп'ютерів та інших електронних пристроїв (принтерів, факсимільних апаратів, модемів і т.п.). Мережа дає можливість окремим науковцям взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів, дозволяє їм одержувати доступ до даних, що зберігаються на персональних комп'ютерах у віддалених офісах, і встановлювати зв'язок між ними.

При цьому, інформаційні мережі призначені головним чином для вирішення завдань користувачів з обміном даними між їхніми абонентами. Вони орієнтовані, в основному, на надання інформаційних послуг користувачам.

Практика свідчить, що в умовах широкої конкуренції об'єкти наукової діяльності не можуть весь час ефективно функціонувати, якщо сучасні засоби електронної обчислювальної та інформаційної техніки не використовуватимуться в усіх процесах оперативного збирання та обробки інформації.

На сьогоднішній день всі учасники науково-дослідницької діяльності можуть стати, за бажанням, клієнтами мережі «Internet». Кількість клієнтів, які поповнюють і використовують існуючу інформацію в мережі, постійно зростає.

За останній час в мережі «Internet» з'являються «електронні бібліотеки» фізичних осіб, які користуються широкою популярністю. Глобальна комп'ютерна мережа «Internet» з погляду інформаційної насиченості стає всебічним і безмежним банком даних, що постійно збільшує свій ресурс.

У сучасному інформаційному суспільстві бібліотеки відіграють надзвичайно важливу роль не тільки в науково-дослідницькій, але й у просвітницькій та навчальній діяльності. Завданням бібліотек є найбільш повне розкриття змісту наявних ресурсів шляхом створення бібліографічних баз даних, каталогів та картотек, котрі значно скорочують користувачам шлях до інформації. Новітні інформаційні технології у сучасних бібліотеках надають можливість значно полегшити та розширити цю діяльність, зокрема, за допомогою доступу до бібліографічних ресурсів через мережу «Інтернет» та розміщення їх на веб-сторінці бібліотеки.

Назва «віртуальна бібліотека» використовується для визначення комплексу інформаційних джерел, доступних через глобальні комп'ютерні мережі, що в сукупності утворюють Internet. Віртуальна бібліотека не має єдиного місцезнаходження – її ресурси розподілені по всьому світі, а інформаційний потенціал на кілька порядків перевищує ресурси будь-якої книгозбірні.

Під «цифровою бібліотекою» розуміється бібліотека, в якій вся інформація зберігається в оцифрованому вигляді та не передбачає наявності документів на традиційних носіях.

В електронній бібліотеці основні процеси здійснюються з використанням комп'ютерів, однак у таких бібліотеках документи на машинних носіях співіснують з аудіо-, аудіовізуальними та іншими матеріалами. Електронна бібліотека включає в себе й цифрову, в якій, окрім суто дискретного подання документів, допускається і їх відбиття в іншій електронній (наприклад, аналоговій) формі. Цифрова та електронна бібліотеки, на відміну від віртуальної, являють собою сукупність документів, що мають конкретне місцезнаходження.

Таким чином, основна роль інформації у наукових дослідженнях полягає у виключенні суб'єктивних висновків та можливості отримання оптимальних рішень проблеми. Рівень наукових досліджень залежить від достовірності, ступеня використання інформації та здатності дослідника опрацювати отриману інформацію.

З метою поліпшення інформаційного забезпечення науково-дослідницької діяльності необхідно змінювати психологічне ставлення суспільства до інформатизації, створювати умови для оптимального доступу до інформаційного середовища, розвивати та підвищувати ефективність використання сучасних інформаційних технологій. Вітчизняним науковцям слід інтенсивно вдосконалювати відповідні знання з метою ширшого використання інформаційних видань, довідково-інформаційних фондів та пошуку наукової інформації.

---

1. Інформаційне забезпечення наукової роботи. Стаття. [Електронний ресурс]. – Режим доступу: https://docs.google.com/document/d/1LKMDKTcEnHnmQHw8YyVDM0lye5NXzASeVJY1IxTLLs/edit.
2. Крушельницька О.В. Методологія та організація наукових досліджень. Навчальний посібник. [Електронний ресурс]. – Режим доступу:

http://biology.univ.kiev.ua/images/stories/Upload/Kafedry/Biofizyky/2014/kryshelnytska_metod_org_nayk_dosl.pdf.
3. Філіпова А. Питання змісту бібліотечних веб-сайтів в Інтернеті /А. Філіпова//Бібліотеч. планета. – 2008. – № 3. – С.12–15.
4. Бібліотека – інтелектуальний центр наукових досліджень. Структура і організація економічної бібліографії. http://www.info-library.com.ua/books-text-8411.html.

Інформаційні технології в освіті: проблеми та перспективи

Турчак О.В.,
старший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор юридичних наук, доцент

Рівень розвитку країни значною мірою визначається рівнем освіти, яка повинна на нинішньому етапі розвитку цивілізації швидко й адекватно реагувати на потреби суспільства, позбавляючись шляхом проведення кардинальних реформ притаманного теперішній освіті консерватизму. Одним із важливих чинників реформування освіти є її інформатизація.

Сьогодні, коли інформація стає невід'ємною рисою світової економіки, освіта продовжує залишатися основою персонального і професійного успіху будь-якої людини.

Прискорення науково-технічного прогресу поставило перед педагогічною наукою завдання – виховати та підготувати покоління молодих фахівців, здатне активно включитися в якісно нові умови розвитку сучасного інформатизаційного суспільства.

Виконання цього завдання у значній мірі залежить від технічної оснащеності навчальних закладів сучасною компютерною технікою з відповідним навчальним, демонстраційним обладнанням та від готовності вихованців до сприйняття постійно зростаючого потоку навчальної інформації.

З огляду на це, стає актуальною розробка нових методичних підходів до використання засобів новітніх інформаційних технологій для реалізації ідей розвиваючого навчання, розвитку особистості студента.

Сучасні інформаційні технології навчання, що використовуються в навчальному процесі, значною мірою сприяють розв'язанню актуальних проблем активізації навчально-пізнавальної діяльності.

Використання цих технологій у навчальному процесі дозволяє підвищити якість навчального матеріалу й підсилити освітні ефекти від застосування інноваційних педагогічних програм і методик, оскільки дає викладачам можливості для побудови індивідуальних освітніх траєкторій. Їх застосування дозволяє реалізувати диференційований підхід до студентів з різним рівнем готовності до навчання.

Система навчання з використанням інформаційних технологій має ряд переваг:

- дозволяє зменшити непродуктивні витрати живої праці педагога, який перетворюється в технолога сучасного навчального процесу, де провідна роль приділяється не стільки й не тільки навчальній діяльності педагога, скільки навчанню самих студентів;
- дає слухачам широкі можливості вільного вибору власної траєкторії навчання в процесі набуття знань;
- припускає диференціальний підхід до слухачів, заснований на визнанні того факту, що у них різний попередній досвід і рівень знань, кожний слухач приходить до процесу оволодіння новими знаннями з власним інтелектуальним багажем, який визначає ступінь розуміння нового матеріалу і його інтерпретацію;
- підвищує оперативність і об'єктивність контролю й оцінки результатів навчання;
- гарантує безперервний зв'язок у відносинах «слухач-викладач»;
- сприяє індивідуалізації навчальної діяльності (диференціація темпу навчання, важкості навчальних завдань і т.п.);
- підвищує мотивацію навчання;
- сприяє розвитку у слухачів продуктивних, творчих функцій мислення, росту інтелектуальних здібностей, формуванню операційного стилю мислення.

Важливим є завдання забезпечення психолого-педагогічними та методичними розробками, спрямованими на виявлення оптимальних умов використання засобів нових інформаційних технологій з метою інтенсифікації навчального процесу, підвищення його ефективності і якості.

Зараз відкриваються нові унікальні можливості цих новітніх засобів, реалізація яких створює передумови інтенсифікації освітнього процесу, а також створення методик, орієнтованих на розвиток особистості студента. Це, зокрема:

- негайний зворотний зв'язок між користувачем і засобами інформаційних технологій;
- комп'ютерна візуалізація навчальної інформації про об'єкти чи процеси, явища, що реально відбуваються, так і «віртуальних»;
- зберігання великих обсягів інформації з можливістю легкого доступу до неї;
- автоматизація процесів інформаційно-пошукової діяльності;
- автоматизація процесів інформаційно-методичного забезпечення, управління навчальною діяльністю та контролю за результатами засвоєння програмового матеріалу.

Для реалізації цих можливостей слід організувати такі види діяльності як:

- реєстрація, збір, накопичення, зберігання, обробка інформації про досліджувані об'єкти;
- інтерактивний діалог – взаємодія користувача з програмною системою, що характеризується більш розвиненими засобами ведення діалогу (наприклад, можливість задавати питання в довільній формі, з використанням «ключового» слова, у формі з обмеженим набором символів); при цьому буде забезпечуватися можливість вибору варіантів змісту навчального матеріалу, режиму роботи;
- автоматизований контроль (самоконтроль) результатів навчальної діяльності, корекція за результатами контролю, тренування, тестування.

Нині існує тенденція, коли комерційні фірми, вклавши величезні кошти у розробку мультимедійних компакт-дисків, наповнюють ринок програмними продуктами навчального

призначення, про які викладачі мало проінформовані. Студенти можуть користуватися ними для самостійної підготовки. Проте чи відповідає такий продукт програмі визначеної дисципліни або курсу, а також як застосувати його в конкретному ВНЗ. Як правило, викладачі визнають лише те програмне забезпечення навчального призначення, що розроблено ними самими або апробовано і рекомендовано колегами.

У значній мірі від сучасних інформаційних технологій залежить розвиток особистості, підготовка індивіда до комфортного життя в умовах інформаційного суспільства.

Застосування новітніх інформаційних технологій сприятиме:

- розвитоку мислення (наочно-дієвого, наочно-образного, інтуїтивного, творчого, теоретичного тощо);
- естетичному вихованню (за рахунок використання можливостей комп'ютерної графіки, технології мультимедіа);
- розвитоку комунікативних здібностей;
- формуванню умінь приймати оптимальне рішення або пропонувати варіанти вирішення ситуації (за рахунок використання комп'ютерних ігор, орієнтованих на оптимізацію діяльності з прийняття рішення);
- формуванню інформаційної культури, умінь здійснювати обробку інформації розвитоку умінь здійснювати;
- експериментально-дослідницьку діяльність (за рахунок реалізації можливостей комп'ютерного моделювання).

Засоби інформаційних технологій можуть бути використані в якості:

1. Засобу навчання, що удосконалює процес викладання, підвищує його ефективність і якість.
2. Інструменту пізнання навколишньої дійсності і самопізнання.
3. Засобу інформаційно-методичного забезпечення і управління навчально-виховним процесом. навчальними закладами, системою навчальних закладів.
4. Засобу автоматизації процесів контролю, корекції результатів навчальної діяльності, комп'ютерного педагогічного тестування і психодіагностики.
5. Засобу комунікацій з метою поширення передових педагогічних технологій.

6. Засобу розвитку особистості учня.
7. Засобу автоматизації процесів обробки результатів експерименту.
8. Засобу організації інтелектуального дозвілля.

Вивчення вітчизняного і зарубіжного досвіду використання цих засобів з метою навчання, а також теоретичні дослідження в галузі проблем інформатизації освіти дозволяють констатувати, що включення комп'ютера в навчальний процес надає певний вплив на роль засобів навчання, що використовуються в процесі викладання того чи іншого предмета (курсу), а саме застосування засобів нових інформаційних технологій деформує вже традиційно сформовану структуру навчального процесу.

Відсутність комплексного підходу до проблеми використання таких засобів з метою освіти, недооцінка того, що застосування комп'ютера у відриві від інших засобів навчання не може привести до позитивних зрушень у сфері підвищення ефективності процесу навчання, спричинило поширення практики використання комп'ютера в якості засобу, призначеного для «латання дір» традиційної методики навчання. Це дискредитує саму ідею інформатизації освіти.

Розглядаючи педагогічні аспекти проблем інформатизації освіти, слід констатувати, що в процесі спілкування студента з засобами новітніх інформаційних технологій, він підміняє об'єкти реального світу або моделями, зображеннями цих об'єктів, або символами, при цьому сприйняття реального світу підміняється опосередкованим його сприйняттям, що часто призводить до втрати предметності діяльності, до відірваності від дійсності. Крім того, робота за комп'ютером пов'язана з високим емоційним напруженням, яке не завжди і не кожному може бути корисно.

Новітні інформаційні технології і комп'ютер, зокрема, слід розглядати лише як елемент системи засобів навчання.

При цьому під системою засобів навчання розуміється сукупність взаємопов'язаних і взаємодіючих елементів і компонентів. Програмно-методичне забезпечення має бути орієнтоване на підтримку процесу викладання певного навчального предмета або курсу. Слід попрацювати над об'єктно-орієнтованими програмними системами. Застосування засобів навчання, що функціонують на базі НІТ (новітніх інформаційних технологій) забезпечить предметність діяльності, її практичну спрямованість. У

навчальних цілях слід використовувати системи штучного інтелекту, (наприклад, навчальні бази даних, експертні навчальні системи, навчальні бази знань).

Система «мультимедіа» стає одним з провідних напрямів розвитку інформаційних технологій. Технологія мультимедіа дозволяє реалізовувати більшість методів навчання, контролю й активізації пізнавальної діяльності студентів на якісно новому рівні. Практичне застосування технології мультимедіа може удосконалити або частково замінити в навчальному процесі такі класичні методи навчання, як методи усного викладу навчального матеріалу, методи наочного і практичного навчання, методи закріплення одержаних знань, методи самостійної роботи. Багато знаних педагогів і психологів вказували на те, що для підвищення ефективності навчання методи усного викладу повинні сполучатися з наочними і практичними методами, а також з методами активізації сприйняття.

Системи мультимедіа сприяють комплексному використанню комп'ютера за рахунок включення в єдину систему різних вправ, функцій, гіпертекстових і гіпермедіа способів обробки інформації. Усе це дозволяє навчати аудіюванню, читанню й іншим видам мовної діяльності.

Глобальне розширення інформаційного потенціалу призвело до реорганізації освіти й забезпечення нового рівня якості підготовки спеціалістів та формування гнучкої системи підготовки кадрів із швидкою орієнтацією до швидкоплинних умов професійної діяльності. Сучасна наука зосереджує увагу на теоретичній розробці концепції й структурно-організаційних моделей комп'ютеризації освіти, тому що на даний момент, через відсутність стабільних позицій у цьому питанні, реальна комп'ютеризація навчального процесу на місцях фактично відсутня.

У системи засобів навчання на базі розвитку новітніх інформаційних технологій доцільно включати і традиційні засоби навчання, що забезпечують підтримку процесу викладання того чи іншого навчального предмета. Необхідність цього обумовлена їх специфічними функціями, які передати засобами новітніх інформаційних технологій або неможливо, або недоцільно з психолого-педагогічної чи гігієнічної точки зору. Наприклад, демонстрацію статичної інформації, а також систематизовані відомості,

довідкові дані, які повинні запам'ятати студенти, слід пред'являти у вигляді навчальних таблиць, схем. При цьому використання комп'ютера навіть недоцільно. Якщо ж довідковий матеріал не підлягає запам'ятовуванню, а потрібен лише для короткочасного використання, його доцільно виводити на екран. Аналогічні міркування можна віднести до використання навчальних кінофільмів, тощо, включення яких до навчального процесу має бути педагогічно виправдано.

Важливо визначити оптимальне співвідношення комп'ютерних і без комп'ютерних форм навчання. Необхідно чітко представити, що застосування комп'ютера в навчальному процесі є не тільки передумовою вдосконалення навчання, а й потенційним джерелом низки негативних наслідків.

Засоби навчання, у тому числі і ти що функціонують на базі новітніх інформаційних технологій, в сукупності з навчально-методичними матеріалами (підручники, навчальні посібники, методичні посібники, рекомендації для викладачів) утворюють певну цілісність, представлену певним складом і структурою, – Навчально-методичний комплекс на базі засобів нових інформаційних технологій.

Слід зауважити, що у процесі використання комп'ютера в навчальному процесі виникають наступні психолого-педагогічні проблеми: – комп'ютер підвищує активність роботи студента, збуджує інтерес до навчання; – індивідуальна робота з комп'ютером сприяє розвитку самостійності; – спілкування з комп'ютером привчає до точності, акуратності, послідовності дій; – робота з комп'ютером сприяє розвитку здатності до аналізу й узагальнення; – комп'ютер полегшує засвоєння абстракцій, дозволяючи представити їх конкретними.

Необхідно відзначити, що за умов використання комп'ютера знімається і такий психологічний аспект, як страх відповіді.

Важливим засобом розвитку мислення студентів у процесі навчання є творчі форми розв'язання навчальних задач. У зв'язку з цим одним з перспективних напрямів вдосконалення навчального процесу є використання комп'ютера як універсального засобу моделювання. За допомогою комп'ютера може бути реалізована особистісна манера спілкування, що створює більш сприятливу атмосферу для навчання.

Необхідність впровадження інформаційних технологій у навчально-виховний процес не викликає сумнівів. Однак варто зазначити, що нині у сфері освіти склалася своєрідна ситуація: можливості комп'ютера величезні, але серйозного впливу на масову практику освіти, що відповідає цим можливостям, поки що не здійснюється. Причина полягає, насамперед, у тому, що, незважаючи на наявність концептуальних розробок, методичні основи використання інформаційних технологій навчання потребують системного обґрунтування.

Нині рівень інформатизації українського суспільства в порівнянні з розвиненими країнами складає лише 2-2,5%, відсутній єдиний інформаційний простір в масштабі держави. Звідси фрагментарність, і відсутність системного підходу в реалізації інформаційних освітніх технологій, неможливість тиражування вдалих результатів освітніх проектів і окремих комп'ютеризованих курсів в інших освітніх установах.

З досвіду підготовки кадрів для підрозділів кіберполіції

Хахановський В.Г.,
професор кафедри інформаційних технологій Національної академії внутрішніх справ, доктор юридичних наук, професор

Останнім часом у різних країнах світу створені спеціалізовані підрозділи кіберполіції, зокрема, з метою збирання та аналізу «електронних доказів». Зарубіжний досвід свідчить, що такі злочини мають розслідуватись тими правоохоронцями, які мають спеціальні знання.

Ще на початку цього століття у Проекті Концепції стратегії і тактики боротьби з комп'ютерною злочинністю в Україні було визначено модель підготовки фахівців, які спеціалізуються на розкритті злочинів, що вчиняються з використанням комп'ютерних технологій.

Проблемам підготовки, перепідготовки та підвищення кваліфікації кадрів для правоохоронних органів присвячено ряд наукових робіт [1, с. 201–204; 2, с. 59–62; 3, с. 188–192; 4, с. 91–98; 5, с. 179–182; 6, с. 276–279].

Сьогодні існують різні погляди низки вітчизняних та зарубіжних вчених до проблем підготовки кадрів для боротьби з такими злочинами (зокрема, В.В. Бачила, В.Є. Козлов, Е. В. Рижков та ін.). У 2010 р. Національна академія внутрішніх справ була визначена провідним вищим навчальним закладом системи МВС України з підготовки фахівців по боротьбі з кіберзлочинністю. У зв'язку з цим фахівцями академії було вивчено позитивний досвід викладання та на основі потреб практичних підрозділів розроблено освітньо-кваліфікаційну характеристику та освітньо-професійну програму з підготовки нової спеціалізації – «Протидія кіберзлочинності».

Підготовку кадрів для боротьби із такою злочинністю, на наш погляд, треба здійснювати у відомчих вищих навчальних закладах за умови виконання низки організаційних заходів. Зокрема, це можна робити на базі відповідної вищої технічної освіти наданням другої вищої освіти – юридичної (за умови укладання відповідного контракту з такими фахівцями).

Разом з тим, не виключаємо можливості підготовки фахівців у цій сфері з числа юристів. Так, з 2010–2011 навчального року НАВС розпочала підготовку оперативних працівників за спеціалізацією «Протидія кіберзлочинності». Було розроблено навчальну програму, тематичні плани, навчально-методичні комплекси та лекційні матеріали низки спеціалізованих навчальних дисциплін.

Адже відповідні знання та навички мають бути отримані та вироблені шляхом вивчення ряду дисциплін, зокрема – дисципліни «Комп'ютерні мережі та засоби телекомунікацій», яка є органічним, розширеним продовженням навчальної дисципліни «Інформатика». Головними завданнями цього спеціалізованого навчального курсу є: розгляд принципів будови комп'ютерних мереж; отримання знань про їх види, системну архітектуру; ознайомлення з їх топологіями; протоколами передачі даних; отримання уявлення про безпровідні комп'ютерні мережі. Вивчення цієї дисципліни дозволить у подальшому здійснити викладання низки спеціалізованих навчальних дисциплін.

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

В межах дисципліни «Захист інформації в інформаційно-телекомунікаційних системах» вивчаються правові та організаційно-технічні засади захисту інформації в інформаційно-телекомунікаційних системах; а також апаратні та програмні засоби захисту інформації в інформаційно-телекомунікаційних системах.

Нарешті, у випускній дисципліні «Комп'ютерна розвідка» вивчається спеціальна термінологія програмістів та специфіка хакерського жаргону; недокументовані можливості пошукових систем Інтернет; спеціальні аналітичні системи – процесори для збирання даних; відпрацьовуються методики пошуку, отримання та аналітичної обробки інформації; моніторингу Інтернет-ресурсів, тощо.

Така побудова навчального процесу з основним нахилом на практичне відпрацювання певних умінь та навичок, разом з викладанням інших дисциплін, зокрема: «Особливості розкриття кіберзлочинів», «Інформаційно-аналітична робота в оперативно-розшуковій діяльності» тощо, дозволить, на наш погляд, підготувати сучасних правоохоронців, які зможуть адекватно протидіяти кіберзлочинцям.

---

1. Хахановський В. Г. Організація підготовки фахівців по боротьбі зі злочинністю у сфері високих технологій / В. Г. Хахановський // Науково-практичний журнал МНДЦ. – № 3. – 2001. – С. 201–204.
2. Хахановський В. Г. Науково-педагогічні аспекти забезпечення боротьби з організованою злочинністю в інформаційній та комунікаційній сферах / В. Г. Хахановський // Правова інформатика. – № 1/2003. – К. : НДЦПІ АПН України. – 2003. – С. 59–62.
3. Хахановський В. Г. Організаційні та методичні проблеми підготовки кадрів у сфері протидії комп'ютерним злочинам / В. Г. Хахановський // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : Матер. міжнар. наук.-практ. конф. – Донецьк, 2007. – С. 188–192.
4. Козлов В. Е. К вопросу о структуре специальных знаний, необходимых для осуществления противодействия компьютерной преступности правоохранительными органами / В. Е. Козлов // Там само. – С. 91–98.
5. Титов А. М. Розслідування комп'ютерних злочинів : кадровий аспект / А. М. Титов // Там само. – С. 179–182.
6. Рыжков Э. В. Кадровое обеспечение борьбы с компьютерной преступностью / Э. В. Рыжков // Там само. – С. 276–279.

Зміст

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС ТА НАВЧАЛЬНОМУ ПРОЦЕСІ

Збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції
23 грудня 2016 р.

Відповідальний за випуск В.В. Сеник
Упорядник Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська
Опубліковано в авторській редакції

Підписано до друку 10.01.2017 р.
Формат 60х84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк. 18,2
Тираж 100 прим.

Львівський державний університет внутрішніх справ
79007, м. Львів, вул. Городоцька, 26

Свідотство про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.