ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ СТРУКТУРАМИ УКРАЇНИ ТА ВИЩИМИ НАВЧАЛЬНИМИ ЗАКЛАДАМИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Збірник наукових статей за матеріалами доповідей учасників Міжнародної науково-практичної конференції 22 грудня 2017 р.

Львів 2018

УДК 004
П 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 5 від 27.12.2017)

П 78 **Проблеми** застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання : збірник наукових статей за матеріалами доповідей Міжнародної науково-практичної конференції 22 грудня 2017 року / упорядник Т. В. Магеровська / – Львів: ЛьвДУВС, 2018. – 407 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками Міжнародної науково-практичної конференції «Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання», що проводилася 22 грудня 2017 р. у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

УДК 004

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

Інформаційне забезпечення захисту свідків, які беруть участь у кримінальному судочинстві

Бабецький Роман Васильович,

ад'юнкт кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

Одним із потужних резервів оптимізації захисту свідків під час розслідування кримінальних правопорушень є широке використання достовірної інформації. Саме кваліфікований аналіз та синтез інформації про суб'єкти, які мали відношення до злочинної події, отриманої з різноманітних джерел, її інтерпретація та вміле використання лежать в основі розслідування кримінальних проваджень. Особливе місце серед джерел такої інформації займають масиви та бази даних різних за цільовим призначенням та відомчою належністю інформаційних систем, з іншої сторони є використання засобів масової інформації (ЗМІ) щодо висвітлення процесу розслідування.

Потреба у накопиченні та обробці інформації для неодноразового її використання в подальшому зумовила появу величезної

кількості інформаційних систем в різних сферах людської діяльності, у тому числі й безпосередньо призначених створювати умови для розслідування кримінальних проваджень – криміналістичних інформаційних систем [1, с.11].

Особливе місце в інформаційному забезпеченні свідків в кримінальному судочинстві належить оперативно-довідковими та оперативно-розшуковими обліками, який містить відносно стислий (довідковий) опис об'єктів обліку. Основне їх призначення – попередження, розкриття та розслідування кримінальних правопорушень, шляхом перевірки наявності настановних даних про об'єкт та його місцезнаходження на момент запиту, а також вирішення таких основних завдань: встановлення особи затриманих і заарештованих; отримання даних про минулу злочинну діяльність осіб, стосовно яких здійснюється оперативна перевірка або кримінальне провадження та ін. [2, с.91].

Отож, на наш погляд, необхідну інформацію, у виявлені злочинів що вчиняються проти свідків у кримінальному провадженні, можна класифікувати залежно від призначення, розділяючи її на:

а) оперативно-розшукову інформацію і інші відомості, використовувані під час виявлення ознак злочинів що вчиняються проти свідків;

б) оперативно-розшукову інформацію, використовувану для визначення фігурантів злочину, що вчиняються проти свідків, способів учинення злочинів, їх маскування і інших обставин, необхідних для обрання тактики ведення оперативного спостереження за особами або груп, що становлять оперативний інтерес;

в) відомості, необхідні для здійснення документування епізодів злочинів що вчиняються проти свідків, виявлення організаторів і співучасників, а також їх зв’язків;

г) оперативно-розшукову інформацію, використовувану для успішної реалізації оперативних даних і подальшого використання їх у розслідуванні;

г) оперативні відомості, використовувані для визначення злочинної групи та злочинів що вчиняються проти свідків;

д) оперативно-розшукову і іншу інформацію, використовувану для оцінки впливу діяльності злочинів на свідків у кримінальному проваджені.

Особливою складовою забезпечення захисту свідків, під час розслідування злочинів, являється систематичне в необхідному напрямі інформування представників засобів масової інформації про хід проведення розслідування та створення суспільної думки щодо захования показів особливо важливих свідків.

В світовій практиці сьогодні використовуються три основні види техніки поширення і впливу ЗМІ: письмо, слово та звукове зображення. Такі засоби, як газета, журнал (сприймаються індивідуально), театр, кіно, радіо та телебачення, Інтернет, комплекси технічних пристроїв, що забезпечують швидку передачу інформації називаються засобами масової інформації [3, с. 202].

Фактично сьогодні ЗМІ є основним джерелом продукування і поширення інформації про діяльність правоохоронних органів для більшості населення України та світу, яку отримують із повідомлення радіо, телебачення, Інтернету і періодичних видань, а це значить, що ЗМІ повинні виконувати, як позитивну стратегічну, так і тактичну функцію – надавати допомогу органам влади і місцево самоврядування у розслідуванні і розкритті злочинів. Проте існує реальна проблема меж висвітлення подій, пов'язаних з учиненням злочинів. На жаль, до тепер немає жодного закону чи відомчого нормативного акта, який би чітко врегулював механізм передачі інформації ЗМІ про факти вчинення злочинів.

На думку О.В. Коташевського, потрібно видати міжвідомчий нормативний акт, в якому повинно передбачатися механізм, хто має право, з чийого дозволу та у яких випадках і обсягах давати інформацію про факти вчинення і розслідування злочинів для ЗМІ [4, с. 94].

Ще однією складною проблемою є неправдиве та непрофесійне тлумачення представниками ЗМІ права на інформацію. Відомо, що стосунки між органами розслідування та ЗМІ не рідко бувають не тільки гострими, але і вкрай конфліктними. Оскільки основним прагненням ЗМІ є отримання інформації для забезпечення сенсації в суспільстві, але інколи юридична некомпетентність представників ЗМІ якраз і сприяє конфлікту між ЗМІ та правоохоронними органами.

За нашими дослідженнями встановлено, що злочинці та їх оточення отримували інформацію про покази свідків: від адвокатів (55%), від журналістів (45 %).

Водночас вважаємо, що повідомлення певної інформації суспільству переданої за допомогою ЗМІ не може перебувати у суперечності із таємницею слідства. Відомо, що інститут таємниці слідства було введено для того, щоб перешкодити реальній протидії з боку злочинців особам, які проводять розслідування злочинів та їх судовий розгляд [5, с. 9]. Оскільки інформаційна безпека є вкрай важливою, то очевидно, що інформація, яка стосується правової процедури розслідування окремого злочину повинна бути збережена у таємниці, а данні щодо конкретного свідка мають бути зашифровані. В окремих випадках ЗМІ необхідно використовувати як спосіб оприлюднення неправдивою інформації щодо особливо цінних свідків.

---

1. Інформаційно-довідкове забезпечення кримінальних проваджень; підруч. за заг ред. В.В. Бірюкова. – К.: «Центр учбової літератури», 2014. – 288 с.
2. Усманов Р. А. Информационные основы предварительного расследования [Текст]: моиография / Под ред. д.ю.н., А. А. Белякова. – М : Издательство «Юрлитинформ», 2006. – 367 с.
3. Карпенко Л. А. Психология: словарь / Л. А. Карпенко, под общ. ред. В. Петровського, М. Г. Ярошевського. – 2-е изд., испр. и доп. – М.: Политиздат, 1990. – 304 с.
4. Коташевський О. В. Використання засобів масової інформації для розкриття, розслідування і попередження умисних вбивств / О. В. Коташевський II Слідча практика України: із досвіду слідчої роботи органів прокуратури. – К.: Крим Арт. – Вип. 1. – С. 91-94.

5. Ляш А. О. Недопустимість розголошення відомостей досудового розслідування / А. О. Ляш // Часопис Національного університету «Острозька академія». Сер. «Право». – 2013. – № 1 (7). – С. 1–14.

Інформаційне забезпечення протидії злочинності як комплексний підхід до державної безпеки

Бесчастний Віктор Миколайович,

ректор Донецького юридичного інституту МВС України, доктор наук з державного управління, професор

Назимко Єгор Сергійович,

перший проректор Донецького юридичного інституту МВС України, доктор юридичних наук, старший науковий співробітник

Волобуєва Олена Олексіївна,

завідувач кафедри кримінально-правових дисциплін та судових експертиз Донецького юридичного інституту МВС України, кандидат юридичних наук, доцент

Політика у сфері протидії злочинності, як і будь-яка інша політика, повинна розроблятися і реалізуватися на основі об'єктивної інформації стосовно процесів та явищ, які перебувають у сфері її інтересів.

Створення системи, яка сприятиме істотному вдосконаленню інформаційної взаємодії правоохоронних та інших державних органів у сфері боротьби зі злочинністю, поліпшенню координації їх діяльності, забезпеченню спільного формування та використання інформаційних ресурсів для ефективної боротьби зі злочинністю, провадженню аналітичної, статистичної та управлінської діяльності у сфері захисту конституційних прав та свобод людини і громадянина від злочинних проявів як найбільш небезпечної загрози державній безпеці України, що визначалось завданням для Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів [1],

залишається актуальним при реалізації Стратегії розвитку інформаційного суспільства в Україні до 2020 року [2].

Інформаційне забезпечення при розслідуванні злочинів визначають як впровадження конкретних засобів, що сприяє ефективному виявленню, дослідженню і фіксації джерел інформації у передбаченому законом порядку з метою формування на їх основі доказів про обставини вчинення злочинів, методи їх встановлення та використання у кримінальному провадженні. Інформаційне забезпечення на досудових стадіях – це і постійне узагальнення слідчої практики, виявлення недоліків і назрілих проблем, наукова їх розробка і відповідне законодавче, методичне й інші форми вирішення [3, с. 23].

Ми вважаємо, що інформаційне забезпечення у протидії злочинності – це сукупність засобів, методів та заходів, які використовуються для отримання своєчасної, цінної та важливої інформації, що впливає на точність та визначеність при прийнятті рішень, спрямованих на усунення, зменшення або нейтралізацію факторів існування злочинності та вчинення злочинів.

Ми поділяємо думку, що інформаційне забезпечення є особливою формою контролю над тими загрозами, які можуть надходити від злочинності [4, с. 146]. Тому у процесі реформування органів правоохоронних системи, з урахуванням стрімкого розвитку інформаційних технологій та їх впровадження у всіх сферах життєдіяльності, не перестає бути актуальним питання інформаційного забезпечення протидії злочинності.

У практичній діяльності ефективність роботи правоохоронних органів оцінюють за показниками розкриття, який щомісячно визначається для співробітників оперативних підрозділів, без врахування складності проваджень та об’єктивних обставин, що необхідні для розкриття злочинів. А отже, орієнтування на запобігання злочинам залишається формальною складовою, що не є першочерговим завданням в реаліях практичної діяльності.

Актуальним напрямом інформаційного забезпечення процесу протидії злочинності є усунення безсистемності в зборі інформації, неузгодженості між різними суб’єктами в аналізі

інформації про криміногенну обстановку та розробкою заходів реагування, у випадку її ускладнення, що у результаті не дозволяє прийняти ефективне управлінське рішення і знижує рівень їх реалізації [5, с. 107-108].

Однією з проблем інформаційного забезпечення є розосередженість обліків злочинів по окремим відомствам, що створює умови для відомчого впливу, викривлення державної статистичної звітності, маніпуляцій із цифровими показниками, уявної, а не реальної оптимізації діяльності щодо протидії та запобігання злочинності в державі. Існуюча система збирання показників кримінально-правової статистики про злочинність через відомчий підхід до неї не сприяє формуванню об'єктивної і достовірної картини про стан злочинності в країні та про результати роботи правоохоронної системи. Ситуація, що склалася, негативно впливає й на використання статистичних даних для визначення тенденцій, стратегії і тактики протидії злочинності та іншим правопорушенням [6].

Сьогодні система збирання показників кримінально-правової статистики про злочинність зазнала низка організаційних змін. Серед переваг електронних баз зареєстрованих злочинів та осіб, які вчинили злочини, визначають: по-перше, електронні бази містять індивідуалізовані відомості про злочин, які дозволяють визначити кримінологічні ознаки та тип кожного посягання, оцінити більш точно ступінь його суспільної небезпечності. По-друге, зазначені відомості характеризують стан злочинності в реальному часі на певній території, тобто дають змогу оперативно оцінювати тенденції злочинності та розробляти заходи реагування, а також більш точно прогнозувати її стан у майбутньому. По-третє, інформація щодо кожного зафіксованого в електронній базі даних злочину, на відміну від документів первинного обліку злочинів та статистичної звітності, не втрачає індивідуального характеру, що дає можливість швидко узагальнювати її за будь-якою ознакою та встановлювати зв'язки між окремими ознаками [7, с. 52-57].

Отже, спроба подолати проблему розосередженості обліку злочинів, які здійснювали різні відомства, здійснена. Відповідно до

Положення про порядок ведення Єдиного реєстру досудових розслідувань його користувачами є: керівники прокуратур та органів досудового розслідування; прокурори; слідчі органів поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, та Державного бюро розслідувань, детективи Національного бюро; інші уповноважені особи органів прокуратури та досудового розслідування, які виконують функції з інформаційно-аналітичного забезпечення правоохоронних органів та ведення спеціальних обліків [8].

Єдиний реєстр досудових розслідувань утворений за допомогою автоматизованої системи електронної бази даних і ведеться з метою забезпечення:

- реєстрації кримінальних правопорушень (проваджень) та обліку прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження;
- оперативного контролю за додержанням законів під час проведення досудового розслідування;
- аналізу стану й структури кримінальних правопорушень, вчинених у державі;
- інформаційно-аналітичного забезпечення правоохоронних органів.

Установлені форми документів первинного обліку, довідників є єдиними для Реєстраторів усіх правоохоронних органів, що є вимогою та необхідністю для ведення єдиного обліку. Відповідний припис спрямований на визначення єдиної схеми аналізу інформації про злочин.

Внесення відомостей здійснюється шляхом фіксації та вибору даних у довідниках для заповнення документів первинного обліку про:

- кримінальне правопорушення за формою у додатку 1;
- наслідки досудового розслідування кримінального правопорушення за формою, наведеною у додатку 2;
- заподіяні збитки, результати їх відшкодування та вилучення предметів злочинної діяльності за формою, наведеною у додатку 3;

- особу, яка вчинила кримінальне правопорушення та яка підозрюється у його вчиненні, за формою, наведеною у додатку 4;
- рух кримінального провадження за формою, наведеною у додатку 5.

Правоохоронна система працює з величезним масивом інформації, що щоденно поновлюється. В інформаційній мережі поліції України функціонують такі основні інформаційні підсистеми:

- «Статистика»;
- «Інтегрована інформаційно-пошукова система органів внутрішніх справ (ІІПС ОВС)»;
- «Оперативно-довідкова картотека (ОДК)»;
- функціональна підсистема «Єдиної державної інформаційної систем у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»;
- «Інтегрований національний банк даних про транспортні засоби».

Зазначені системи забезпечують збирання, накопичення інформації та обмін нею між підрозділами правоохоронної системи.

Отже, проведений аналіз стану інформаційного забезпечення протидії злочинності, дозволяє зробити такий висновок: наявність інформаційних ресурсів у інших служб і відомств не забезпечує оперативної обробки запитів, все ще переважає система письмових запитів. Навіть за необхідності оперативного реагування викають ситуації з розголошенням інформації. Ці недоліки та упущення багато в чому зумовлені створенням нових підрозділів і служб, що дублюють повноваження, відсутністю налагодженої взаємодії, угод про співпрацю, про надання інформації, що, в свою чергу, пов’язано з постійною зміною (не плановою ротацією) керівного складу підрозділів, плинністю кадрів. Отже, використання потенціалу автоматизованих систем, програмно-апаратних комплексів, баз даних в органах державної влади здатне значно підвищити

можливості оперативного реагування на злочинність і пов'язані з нею фактори. Але умовою досягнення цього є визнання пріоритету запитів правоохоронних органів, спрощена система доступу до певної інформації у разі необхідного оперативного реагування на рівні керівника підрозділу за кодовим зверненням. Оскільки не визнання пріоритету отримання інформації з метою протидії злочинності під час співпраці різних органів державної влади, недержавних інституцій, а покладання відповідних завдань лише на рівні особистих контактів працівників підрозділів не вирішує ситуацію.

1. Про затвердження Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов`язана з боротьбою із злочинністю: Постанова Кабінету Міністрів України від 08.04.2009 р. № 321. URL: http://zakon0.rada. gov.ua/laws/show/321-2009-%D0%BF (дата звернення: 20.09.2016).
2. Стратегія розвитку інформаційного суспільства в Україні: розпорядження Кабінету Міністрів від 15.05.2013р. №386-р URL: http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80/page (дата звернення: 20.09.2016).
3. Міжнародна організація з міграції. URL: http://iom.org.ua/ua (дата звернення: 20.09.2016).
4. Желудков М. А. Особенности информационного обеспечения деятельности органов внутренних дел по противодействию экономической преступности. Вестник Владимировского юридического института. 2007. № 3 (4). С. 146-149.
5. Годунов И. В. Некоторые аспекты информационно-аналитической работы в деятельности правоохранительных органов в сфере противодействия преступности. Человек: преступление и наказание. 2012. № 4 (79). С. 107-108.
6. Проблеми інформаційно-аналітичного забезпечення протидії злочинності в Україні. URL: http://www.info-library.com.ua/ books-text-10120.html (дата звернення: 20.09.2016).
7. Кулик О. Кримінологічний аналіз злочинності в Україні: напрями вдосконалення методології та методики. Право України. 2009. № 7. С. 52–57.
8. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: наказ Генеральної прокуратури

України від 06.04.2016 р. № 139 . URL: http://www.gp.gov.ua/ua/pd.html ?_ m=publications&_t=rec&id=110522 (дата звернення: 20.09.2016).

Особливості використання працівниками Національної поліції України нагрудних відеокамер

Бобонець Маргарита Миколаївна,

здобувач ступеня бакалавра факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

Рвачов Олексій Михайлович,

старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

В травні 2015 року під час зустрічі з майбутніми патрульними поліцейськими Міністр внутрішніх справ України Арсен Аваков повідомив, що нагрудна відеокамера стане невід'ємною частиною в роботі кожного українського поліцейського [1].

Оснащення та використання працівниками поліції нагрудних відеокамер (відеореєстраторів) розглядається ними як засіб захисту себе від упереджених заяв з боку громадян щодо їхньої неправомірної поведінки [2].

Відеокамера являє собою електронний оптичний пристрій, призначений для перетворення світлового потоку, що проходить через об'єктив і групу лінз, сфокусований на CCD-матриці, у мінливий за часом повний відеосигнал [3].

В залежності від конструктивних особливостей відеокамери поділяються на безліч типів, серед яких: модульні, корпусні, купольні, вуличні, керовані, цифрові й аналогові, провідні та безпровідні, гіростабілізіровані відеокамери [4].

У відповідності до ч. 2 ст. 19 Конституції України «органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах

повноважень та у спосіб, що передбачені Конституцією та законами України» [5].

Згідно до ст. 40 Закону України «Про Національну поліцію» засіб відеозйомки (наприклад, нагрудна відеокамера або відеореєстратор) повинен розміщуватися на однострої (форменому одязі) працівника поліції, про що повинно бути розміщено відповідне попередження (наприклад, вишивка або наліпка, бейдж із відповідним написом або зображенням тощо) [6].

У відповідності до «Інструкції про порядок зберігання, видачі, приймання, використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції та доступ до відеозаписів з них», яка на теперішній час втратила чинність, нагрудна відеокамера (відеореєстратор) повинна була активуватися працівником патрульної поліції та знаходилась в режимі відеозйомки при будь-якому контакті з особами, зокрема, але не виключно:

- при оформленні дорожньо-транспортної пригоди;
- при перевірці документів;
- при арешті або затриманні особи;
- при поверхневому огляді;
- при загрозі використання фізичної сили, спеціальних засобів або вогнепальної зброї;
- при наданні допомоги особам;
- у випадках, коли усвідомлення особою факту відеофіксації її поведінки може сприяти вирішенню конфліктної ситуації.

При цьому зазначається, що «після активації нагрудної відеокамери все спілкування повинно бути записане безперервно» [7].

На сьогодні існують різні моделі портативних відеокамер (відеореєстраторів), що використовуються працівниками правоохоронних органів світу та які відрізняються різними способами їх кріплення або розміщення:

- в руках працівника – побутові портативні відеокамери;
- на тілі працівника:

- на форменому одязі (в районі грудної клітини або на плечі) за допомогою кліпси (зажиму), липучки або магніту;
- на бронежилеті;

- на голові працівника:
  - на сонцезахисних окулярах;
  - на головному уборі або шоломі чи касці;
  - за вухом;
- на вогнепальній зброї;
- на транспортних засобах:
  - в середині салону автомобілю за лобовим склом;
  - на даху автомобілю;
  - на рулі велосипеду тощо.

В Україні під час створення Національної поліції для оснащення працівників патрульної поліції було придбано персональний мобільний відеореєстратор «DMT-1», що кріпиться на однострої (форменому одязі) працівника за допомогою металічної кліпси з можливістю обертання на 360 градусів [8].

З наведених вище варіантів кріплення персональних мобільних відеореєстраторів, найбільш не практичним є закріплення відеокамери на форменому одязі працівника в районі грудної клітини, тому що під час використання відеокамери, яка кріпиться таким способом, вона знімає все те, що відбувається за напрямом проходження оптичної осі об'єктиву відеокамери та з урахуванням куту його огляду. Наприклад, працівник стоїть на місці та дивиться у лівий бік, а відеокамера знімає все те, що відбувається перед працівником, а не те на що дивився працівник. В такому випадку камера не зафіксує події, які побачив поліцейський та на підставі яких прийняв рішення про вчинення певних дій, наприклад, про застосування фізичної сили, спеціальних заходів або вогнепальної зброї.

Найбільш ефективною і точною у зйомці є відеокамера, яку закріплена на голові працівника (на сонцезахисних окулярах, головному уборі або шоломі чи касці, за вухом). Така відеока-

мера фіксує саме ті об'єкти та події, на які дивився працівник під час забезпечення публічної безпеки та порядку.

---

1. Кулеш С. Новые украинские патрульные будут носить нагрудные камеры // ITC.UA. 06.05.2015 в 17:09. URL: https://itc.ua/news/novyie-ukrainskie-patrulnyie-budut-nosit-nagrudnyie-kameryi/ (дата звернення: 11.12.2017).
2. Крапивін Є. Нагрудна камера (відеореєстратор) патрульного: правове регулювання і порушення права на приватність // Асоціація українських моніторів дотримання прав людини в діяльності правоохоронних органів. 14.04.2016. URL: http://umdpl.info/police-experts.info/2016/04/14/article-videofixation/ (дата звернення: 11.12.2017).
3. Відеокамера // Корпорация СИРИУС – Служба Безопасности. URL: https://sirius.kiev.ua/ru/videokamera (дата звернення: 11.12.2017).
4. Типи відеокамер // Світ перекладів. 26.06.2012. URL: http://worldtranslation.org/uk/news/86-types-of-video-cameras.html (дата звернення: 11.12.2017).
5. Конституція України: Закон від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/254%D0%BA (дата звернення: 11.12.2017).
6. Про Національну поліцію : Закон України від 02.06.2015 № 580-VIII // База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/580-19 (дата звернення 11.12.2017).
7. Про затвердження Інструкції про порядок зберігання, видачі, приймання, використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції та доступ до відеозаписів з них : наказ Департаменту патрульної поліції НПУ від 03.02.2016 № 100. // Асоціація українських моніторів дотримання прав людини в діяльності правоохоронних органів. URL: http://umdpl.info/police-experts.info/orders/nakaz-departamentu-patrulnoji-politsiji-npu-vid-03-02-2016-roku-100/ (дата звернення: 11.12.2017).
8. Персональний мобільний відеореєстратор DMT-1 // ТОВ «НК ІТ-ПРОЕКТ» URL: https://mmigroup-it.prom.ua/p444643940-personalnij-moblnij-vdeoreyestrator.html (дата звернення: 11.12.2017).

Методи розмежування доступу до інформаційних ресурсів у базах даних МВС України

Бондаренко Вікторія Анатоліївна,

доцент кафедри іноземних мов та культури фахового мовлення Львівського державного університету внутрішніх справ, кандидат юридичних наук

Розробникам Програми створення єдиної телекомунікаційної системи, іншим посадовим особам, які при підготовці проектів нормативних правових актів описують зміст заходів щодо забезпечення захисту інформації, необхідно визначатися, який метод розмежування доступу будуть застосовувати, усвідомлюючи, що в кінцевому підсумку від цього залежить забезпечення цілого ряду прав і свобод людини та громадянина, зокрема права на життя, гідність особи, недоторканність приватного життя. В автоматизації процесів інформаційного обміну в органах МВС залучені відомості конфіденційного характеру, що передбачено Положенням про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України [1].

Аналіз науково-технічної літератури з питань забезпечення інформаційної безпеки дає змогу виділити поширені методи розмежування доступу до інформаційних ресурсів у базах даних: доступу за списками; використання матриці встановлення повноважень звернення з інформаційними ресурсами; доступу за рівнями конфіденційності; парольне розмежування доступу. При цьому важливо уникнути суто технічних підходів у забезпеченні важливого елементу забезпечення захисту інформації в базах даних – розмежування доступу. Наприклад, виключно технічний підхід до вирішення даної проблеми є в системі захисту інформації VipNet, яка активно впроваджується в органах МВС. З огляду на технологічний аспект шаблон політики безпеки (технічний термін) – це набір параметрів безпеки, який містить мережеві фільтри та правила трансляції IP-адрес з можливим об'єднанням вузлів у підрозділи та шаблон для окремих вузлів і підрозділів [2, с. 104]. Розробка моделей є завданням експлуатуючої організації. Поки що в цьому питанні

у нормативних правових актах МВС є суттєві розбіжності, що насамперед виявляється у збільшенні використання технікоюридичних норм у викладі нормативних приписів (наприклад, заміна наказу МВС від 17.02.2015 № 169 на 04.07.2016 № 596 з однаковою назвою) [3].

Модель обігу конфіденційної інформації в загальному являє собою спрощену модель обігу відомостей, що становлять державну таємницю, де застосовується принцип розмежування доступу за рівнями, заснований на ступені секретності інформації. Але тільки допуску до цих відомостей недостатньо – необхідно адміністративне дозвіл уповноваженої посадової особи на ознайомлення з конкретною інформацією у межах ступеня секретності та документів з відмітками «літер «М», «літер «К» і «СІ» [4].

До відомостей конфіденційного характеру в органах МВС потенційно можуть бути допущені всі військовослужбовці, поліцейські, державні службовці та службовці, так як спеціальної процедури оформлення допуску до цієї інформації не передбачено. Але це не означає, що будь-який співробітник має право ознайомитися з будь-якими відомостями, які містяться в базах даних конфіденційної інформації, так як це може призвести до витоку інформації. У даний час технічними прийомами цей процес зупинити не вдається, але захист інформації не може бути самоціллю та превалювати над службовою необхідністю у доступі до потрібних відомостей. Залишаються організаційно-правові методи.

У реалізації методу розмежування доступу за списками існують два підходи – для кожного користувача визначається перелік інформаційних ресурсів, до яких він може бути допущений, або для кожного інформаційного ресурсу визначається список користувачів. Для численних баз даних органів МВС повинні застосовуватися обидва різновиди цього методу. Це тягне за собою рішення достатньо масштабне, але необхідне завдання – встановлення для кожного бази даних способу розмежування доступу до інформації. Причому робити це доведеться на основі характеристик самих користувачів.

Практика використання Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України показує на існування двох схем вирішення вищевказаного завдання. Виділяються дві категорії співробітників, які слугують основними учасниками схем – керівники та співробітники підрозділів. У свою чергу, керівники повинні підрозділятися на загальних і керівників структурних підрозділів. Загальні керівники (начальник органу МВС та його заступники, починаючи з рівня територіального органу) повинні мати доступ до всіх інформаційних ресурсів МВС, в яких накопичується інформація конфіденційного характеру, в тому числі до баз даних, перелічених у Законі України від 02.07.2015 № 580-VIII «Про Національну поліції», за винятком категорії відомостей передбачених Законами України від 18.02.1992 № 2135-XII «Про оперативно-розшукову діяльність», від 23.12.1993 № 3782-XII «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», від 01.06.2010 № 2297-VI «Про захист персональних даних». У даному випадку мова йде про осіб: щодо яких порушені справи оперативного обліку; які підлягають державному захисту. Відомості про осіб, щодо яких порушені справи оперативного обліку, найчастіше підпадають під категорію державної таємниці, але навіть якщо і не підпадають, то тільки підрозділи, які ведуть таку розробку, вирішують, кому, крім прямих начальників, можливо повідомити ці відомості. До відомостей, пов'язаних із заходами, проведеними щодо осіб, що підлягають державному захисту, повинно бути допущено мінімальна кількість осіб, прямо пов'язаних з реалізацією зазначених заходів. Відповідно, до таких баз даних є доступ за заздалегідь визначеним списком користувачів.

У перспективі, з погляду на дослідження В. Білоуса, до переліку закритих баз даних доцільно включити геномну реєстрацію, якою необхідно доповнити Закон України від 16.03.2017 № 1951-VIII «Про Єдиний державний реєстр військово-зобов’язаних» [5]. Геномна реєстрація належать до категорії біометричних персональних даних, і для ознайомлення повинні передбачатися окремі умови доступу [6].

Наступний метод, пов'язаний насамперед з цілісністю і достовірністю інформації, – метод матриці встановлення повноважень. Згідно з цим методом в формалізованому списку визначається набір повноважень, якими має право володіти конкретний користувач щодо певних інформаційних ресурсів. Наприклад, він має право: тільки знайомитися; знайомитися і доповнювати; знайомитися, доповнювати і коригувати, копіювати, видаляти тощо. Даний формальний набір повноважень дуже важливий і повинен бути ретельно продуманий і зафіксований у нормативно-правовому акті, що регулює соціально-технічні відносини.

Наприклад, керівник підрозділу, який в силу своїх посадових повноважень приймає рішення про модифікацію та видалення відомостей з бази даних, не повинен володіти можливістю фактичної реалізації такого повноваження, а реалізовувати своє волевиявлення через певну процедуру дачі документально оформленого доручення. Технологічними можливостями внесення цих змін повинен володіти адміністратор бази даних або спеціально уповноважений користувач, діяльність яких перевіряється згідно Інструкції з організації контролю за виконанням документів у системі МВС України (Наказ МВС України від 23.04.2012 № 350), і Інструкції з організації контролю за виконанням документів у Національній поліції України (Наказ МВС України від 13.06.2016 № 503) [7].

Далі виділяють методи розмежування доступу є розмежування за рівнями конфіденційності (категоріями). Даний метод добре працює при формальному поділі інформації за ступенями секретності в системі віднесення відомостей до державної таємниці. Водночас, метод є схематичний, так як масиви інформації, віднесені до ступеня секретності «таємно», «цілком таємно» (за винятком відомостей категорії «особливої важливості»), з відмітками «літер «М», «літер «К», «СІ» є досить великими та різнорідними за змістом [8].

У переважній більшості баз даних Національної поліції можна виділити деякі локальні сегменти, які необхідно охороняти найбільш ретельно, детально регламентуючи порядок доступу, коло

осіб, порядок фіксації фактів звернень до змісту сегмента бази даних, що вимагає спеціального нормативно-правового регулювання на рівні МВС України.

Ефективним є парольний метод розмежування доступу до відомчих баз даних, інтегративний щодо всіх описаних вище, так як дає змогу закласти загальне, матричне та категоріальне повноваження доступу. Парольна система є універсальна, але має недолік – зміст пароля може стати відомим не уповноваженому суб'єкту, який може тривалий час отримувати доступ до відомостей, що знаходяться в базі даних. Для вирішення вказаної проблеми в автоматизованих інформаційних системах застосовується метод захисту, щодо обмеження числа паралельних сеансів доступу для кожного облікового запису користувача. Суть цього методу полягає у фіксації спроби отримання доступу в систему під обліковими даними в той момент, коли такий доступ має легальний користувач, і блокування другого процесу. Описане вище – це технології, за якими повинні бути певні правові дії: блокування ключа легального користувача, призначення розслідування за фактом витоку інформації та визначення обсягів відомостей, до яких був здійснений несанкціонований доступ, генерація нового ключа для легального користувача тощо.

Така адміністративна процедура повинна бути предметом нормативно-правових актів, що регулюють питання захисту інформації в органах МВС. Однак у нормативно-правових актах які є відкритих джерелах регламентації цих питань не має.

У контексті інформаційного обміну найбільш небезпечним є віддалений доступ, який здійснюється з місць, що знаходяться за межами зони технічного контролю (наприклад, за межами адміністративного будинку, в якому розташоване комп'ютерне обладнання, що містить базу даних).

З огляду на основи інформаційних технологій і систем існують дві принципи організації віддаленого доступу до автоматизованих баз даних по виділених телекомунікаційним каналах і телекомунікаційним каналами загального користування на

підставі Закону України від 18.11.2003 № 1280-IV «Про телекомунікації». У разі організації доступу по виділених, а ще краще – захищених телекомунікаційних каналів, проблема несанкціонованого доступу, буде зведена до звичайної технічної помилки, так як коло осіб, які мають доступ є обмежене.

1. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС : Наказ МВС України від 04.07.2016 № 596 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z1055-16/paran21#n21
2. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова Кабінету Міністрів України від 19.10.2016 № 736 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/736-2016-%D0%BF
3. Ковалів М. В. Основи управління в органах внутрішніх справ України : навч.-практ. посіб. / М. В. Ковалів. – Львів, Львів. держ. ун-т внутр. справ. 2010. 340 с.
4. Про Єдиний державний реєстр військовозобов'язаних : Закон України від 16.03.2017 № 1951-VIII // Відомості Верховної Ради. 2017. № 18. Ст. 217.
5. Білоус В. В. Про впровадження державної геномної реєстрації в Україні / В. В. Білоус // Наук. вісник Херсонського держ. ун-ту. Сер.: Юридичні науки. 2015. Вип. 4. Т. 3. С. 89–95.
6. Про затвердження Інструкції з організації контролю за виконанням документів у Національній поліції України : Наказ МВС України від 13.06.2016 № 503 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z0944-16
7. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова Кабінету Міністрів України від 19.10.2016 № 736 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/736-2016-%D0%BF
8. Питання реформування органів внутрішніх справ України : Розпорядження Кабінету Міністрів України від 22.10.2014 № 1118-р [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1118-2014-%D1%80

Удосконалення зв'язку в системі управління нарядами патрульної служби Національної поліції України

Вишня Володимир Борисович,

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

Стаття призначена дослідженню особливостей діяльності нарядів мобільної патрульної служби та її удосконалення.

Одним із важливих елементів в реформування міліції та розбудови Національної поліції України є створення мобільних патрульних нарядів, які першими реагують на виклик про допомогу, або повідомлення про вчинене правопорушення чи злочин. Тому доцільно розглянути ефективність реагування на сповіщення підрозділів Національної поліції України (у подальшому – поліція) та відпрацювання нарядами мобільної патрульної служби отриманого завдання.

Найбільш вдосконаленим технічним рішенням даної проблеми є створення системи централізованого управління нарядами патрульної служби («ЦУНАМІ»), що являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами мобільних нарядів поліції. Він включає пов'язані між собою блоки оператора 102, диспетчера, чергового районного відділу поліції, та обладнання автопатруля у вигляді блока керування та відображення (у подальшому – планшет) з системою супутникового GPS-позиціонування і особистого відеорегістратора патрульного. Диспетчер системи є оперативним черговим і куратором кожного конкретного райвідділу поліції, відповідального за організацію реагування на злочини та пригоди в рамках району. Оператор 102 здійснює прийняття і реєстрацію повідомлень про злочини та події, виконує попередню їх кваліфікацію. Заповнена оператором 102 електронна картка надходить до диспетчера – чергового

відповідального за управління мобільними нарядами поліції, де призначається екіпаж мобільного патруля для реагування на сповіщення, що надійшло. Одночасно електрона картка поступає черговому районного відділу поліції, до території якого відноситься звернення, де повідомлення громадян реєструється у журналі «Єдиного обліку злочинів і правопорушень районного управління».

При ефективної взагалі роботи системи проявляється суттєвий недолік – відсутня можливість у диспетчера оперативно відслідковувати хід подій та дії патрульного безпосередньо при виконанні отриманого їм завдання. Тим самим виключається можливість у чергового диспетчера, в разі необхідності, вмішуватися в хід виконання завдання нарядом, оперативно коригувати дії наряду, виключити випадки некваліфікованих дій патрульних.

Тому нами були проведені дослідження по удосконаленню системи зв'язку між диспетчером та поліцейським наряду мобільної патрульної служби при виконанні отриманого завдання.

В основу вдосконалення зв'язку в системи управління нарядами мобільної патрульної служби пропонується, шляхом уведення нових зв'язків елементів, забезпечити можливість відображення у диспетчера інформації, яка попадає у поле зору об'єктиву відеорегістратора патрульного. Це дозволяє диспетчеру в режимі реального часу оперативно контролювати дії патрульного поліцейського в процесі відпрацювання поставленого завдання і, при необхідності, своєчасно втручатися в його роботу, і за рахунок цього підвищити ефективність та безпеку діяльності патрульного наряду.

Поставлена задача вирішується тим, що у відомій системі централізованого управління нарядами патрульної служби, що включає пов'язані між собою блоки оператора 102, чергового районного відділу поліції, диспетчера, планшет мобільного патрульного наряду з системою супутникового GPS-позиціонування та блок особистого відеорегістратора патрульного, вводяться

канали передачі відео потоків, якими сполучено відповідно блок особистого відеорегістратора патрульного до планшету мобільного патрульного наряду, від нього – до блоку диспетчера з можливістю висвітлення кожномоментно на моніторі диспетчера місця події з об'єктиву особистого відеорегістратора патрульного при відпрацюванні завдання.

На рис. 1 представлена схема удосконаленої системи управління нарядами мобільної патрульної служби, яка включає блок 1 оператора 102, вхід якого приєднаний до телефонної мережі зв'язку, а виходи підключені відповідно до першого входу блока 2 диспетчера та першого входу блока 3 чергового райвідділу поліції, другий вхід якого зв'язаний з телефонною мережею зв'язку. В той же час, вихід блоку 3 чергового райвідділу поліції підключений до другого входу блока 2 диспетчера, третій вхід якого (сумісний з виходом) зв'язаний з планшетом 4 мобільного патрульного наряду, до якого приєднаний перший канал передачі відеопотоку 6 від особистого відеорегістратора патрульного 5 та другий каналу передачі відеопотоку 7 планшету 4 до блоку диспетчера 2.

Система реалізується в такий спосіб. Сповіщення поліції про злочини та події або виклик допомоги, що здійснюються за телефоном 102, приймаються і обробляються оператором 102 (блок 1). В результаті створюється електронна картка повідомлення, яка відразу надходить до диспетчера 2 – чергового відповідального за управлінням мобільними нарядами патрульної поліції, який призначає вільний екіпаж мобільного патруля для реагування на повідомлення. Одночасно, електронна картка повідомлення надсилається черговому (блок 3) райвідділу поліції, до території якого відноситься звернення, яке реєструється у журналі Єдиного обліку злочинів і правопорушень райвідділу. Слід відмітити, що повідомлення громадян може поступити безпосередньо на телефон чергової частини райвідділу (блок 3). В цьому разі воно реєструється в журналі райвідділу і пересилається до оперативного диспетчера (блок 2) для реагування.

Виділений диспетчером 2 мобільний патрульний наряд (автопатруль) приступає до виконання отриманого завдання. На

протязі усієї роботи екіпаж за допомогою планшету 4 підтримує голосовий або автоматичний зв'язок з диспетчером (блок 2), відмічає етапи виконання завдання. Зокрема, після прибуття наряду на місце вказане в повідомлені громадян в планшеті 4 фіксується час прибуття і автоматично активізуються канали передачі відеоінформації 6 і 7 відповідно між особистим відеорегістратором 5 патрульного і планшетом 4 та між планшетом 4 і блоком 2 диспетчера. С цього моменту по цім каналам диспетчеру передається відеоінформація, яка попадає в об'єктив відеорегістратора 5 патрульного. По завершенню виконання завдання в планшеті 4 робиться відповідна відмітка і канали передачі відключаються.

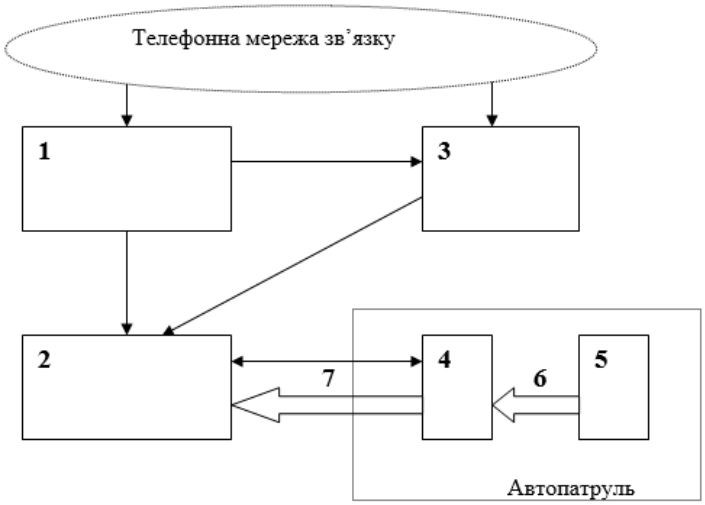


Рис. 1. Удосконалена система управління нарядами мобільної патрульної служби

З метою зменшення витрат на експлуатацію системи доцільно побудувати перший канал передачі 6 в стандарті «Wi-Fi» (безкоштовне користування), а другий канал передачі 7 – на платформі 4G або 5G.

Висновок. Перевагою запропонованої системи управління нарядами мобільної патрульної служби є можливість диспетчера

системи спостерігати в режимі «On Line» за місцем події або злочину і діями патрульних, корегуючи їх при необхідності, рекомендувати вірні управлінські рішення.

Оптимізація інформаційно-аналітичного забезпечення оперативних підрозділів у протидії злочинам, що вчиняються організованими злочинними групами

Гула Лев Федорович,

професор кафедри кримінального права і процесу Навчально-наукового Інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, доцент

Ефективна протидія злочинам, що вчиняються організованими злочинними групами, передбачає підвищення рівня оперативної обізнаності з процесами, які відбуваються в злочинному середовищі, планами й намірами його лідерів та учасників угруповань, уможливлює якісне інформаційне забезпечення оперативних підрозділів.

На думку Я. Ю. Кондратьєва та В. Г. Хахановського, під інформаційно-аналітичним забезпеченням діяльності оперативних підрозділів міліції слід розуміти консолідацію масивів інформації у вигляді баз і банків даних, упорядкування, систематизацію, а також перетворення оперативної інформації з отриманням нових знань для прийняття управлінських рішень [1, с. 63].

Основною метою системи інформаційного-аналітичного забезпечення діяльності протидії злочинності є всебічна інформаційна підтримка практичної діяльності оперативних підрозділів на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів [2, с. 162]. Для цього необхідним є створення інформаційної системи.

Актуальність проблеми інформаційного забезпечення оперативно-розшукової діяльності оперативних підрозділів, спрямованої на бо-

ротьбу зі злочинами, що вчиняються організованими злочинними групами із розширеними міжнародними і міжрегіональними кримінальними зв'язками, характеризується такими чинниками:

а) комплексним характером процесу боротьби з такими злочинами, в якому беруть участь різні служби органів внутрішніх справ, інші правоохоронні органи, а також державні та суспільні організації;

б) широкими просторовими масштабами діяльності організованих злочинних груп (78 % респондентів), мобільністю, технічною оснащеністю;

в) необхідністю здійснення оперативно-розшукових заходів щодо боротьби зі злочинами, що вчиняються організованими злочинними групами, на території різних районів, регіонів, держав;

г) жорсткими тимчасовими межами здійснення оперативно-розшукових заходів і слідчих (розшукових) дій, особливо на первинному етапі;

д) особливостями оперативно-розшукової характеристики таких злочинів і злочинних груп, що їх вчиняють;

е) сучасним станом організованої злочинності у різних сферах.

Суттєво підвищить ефективність оперативних підрозділів у протидії злочинам, що вчиняються організованими злочинними групами, наявність:

- єдиного інформаційного простору, узагальнення та інтегрування різноманітної інформації, яка надходить від оперативних та інших джерел правоохоронної системи України;
- постійного об'єктивного аналітичного дослідження інформаційних потоків і незалежної від інтересів окремих служб оцінки для забезпечення розшукової та іншої діяльності оперативних підрозділів;
- прогнозування ймовірних форм і напрямів розвитку злочинних процесів у економічній та управлінській сферах суспільної та державної діяльності;

- розробки відповідних форм і методів діяльності з нейтралізації злочинних процесів і знешкодження організованих злочинних груп.

Найважливішими напрямами аналітичного пошуку оперативними підрозділами злочинів, що вчиняються організованими злочинними групами, можуть бути:

- щоденні зведення про злочини (85,7%);
- аналіз розслідуваних злочинів, що вчиняються організованими злочинними групами (63,3%);
- матеріали щодо вилучення вогнепальної зброї, яка незаконно перебувала у володінні особи, виявлення і вилучення наркотичних засобів та ін. (42,7%);
- матеріали контролюючих фінансових органів, повідомлення, заяви і скарги громадян(46,4%).

З огляду на це, на увагу заслуговує думка С. С. Овчинського: «Враховуючи той факт, що організована злочинність гідна того, аби у боротьбі з нею застосовувалися методи, характерні для спецслужб, які забезпечують державну безпеку, необхідно вдосконалювати практику ведення інформаційно-накопичувальних справ із використанням аналітичної розвідки. Аналітична розвідка побудована на застосуванні останніх досягнень інформаційних технологій, відтак є одним із основних напрямів діяльності Інтерполу в боротьбі з транснаціональною організованою злочинністю» [3, с. 319].

Інформаційно-аналітична розвідка – це спеціальний захід, призначений для вирішення оперативно-тактичних завдань з метою отримання нових чи додаткових даних про осіб, що становлять оперативний інтерес, і встановлення причинно-наслідкових зв'язків між об'єктами, які вивчаються, заснований на комплексному дослідженні інформації за допомогою багатофакторного аналізу розрізнених відомостей про об'єкт шляхом їх системної обробки з використанням різноманітних прийомів і методів. Основними напрямами інформаційно-аналітичної розвідки є оперативна ідентифікація (ототожнення) та аналіз оперативної обстановки [4, с. 192].

У підсумку необхідно зазначити, що інформаційно-аналітичне забезпечення оперативних підрозділів у протидії злочинам, що вчиняються організованими злочинними групами має функціонувати у трьох напрямах:

- підготовка регулярних аналітичних оглядів щодо змін оперативної обстановки, поточних подій і чинників, що на них впливають, для своєчасного інформування керівництва й прийняття необхідних управлінських рішень;
- довгострокова оцінка процесів і тенденцій, що відбуваються на окремій території чи об'єктах (у сферах, галузях), рівня розвитку та утворення ймовірних негативних наслідків;
- вивчення окремих питань за завданням оперативних підрозділів для заповнення прогалин в розвідувально-інформаційному супроводі кримінальних проваджень, розробка в яких потребує додаткового використання заходів інформаційного та аналітичного забезпечення.

---

1. Кондратьєв Я. Ю. Боротьба з організованою злочинністю і корупцією / Я. Ю. Кондратьєв, В. Д. Сущенко, М. І. Камлик // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2000. – № 2. – С. 61–62.
2. Єчкенко В. М. Інформаційне забезпечення взаємодії карного розшуку та міліції громадської безпеки з метою розкриття злочинів / В. М. Єчкенко // Наук. вісник Луган. акад. внутр. справ. Спецвип. – Луганськ : ЛАВС, 2004. – С. 161–166.
3. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. – М. : ИНФРА, 2000. – 367 с .
4. Цветков О. Г. Організовані групи та злочинні організації як особливий об'єкт оперативно-розшукової діяльності. Правові й організаційно-процедурні основи здійснення оперативно-розшукової діяльності органів внутрішніх справ Україні. Загальна частина : навч. посіб. / [Б. І. Бараненко, Д. О. Бабічев, О. В. Бочковий та ін.] ; за ред. А. В. Іщенка, Б. І. Бараненка. – Луганськ : Луган. держ. ун-т. внут. справ МВС ім. Е. О. Дідоренка, 2011. – С. 98–114.

Моделі, засоби збору та опрацювання параметрів трафіку телекомунікаційних мереж

Дронюк Іванна Мирославівна,

доцент кафедри автоматизованих систем управління Національного університету «Львівська політехніка», кандидат фізико-математичних наук

Кліщ Юрій Ігорович,

магістр кафедри автоматизованих систем управління Національного університету «Львівська політехніка»

Сучасний світ неможливо уявити без телекомунікаційних мереж. Величину залежності теперішньої цивілізації від телекомунікацій можна порівняти з залежністю від електрики. І ця тенденція з кожним роком значно зростає. Неполадки у роботі телекомунікаційних систем можуть мати такі негативні результати, що співмірні з наслідками аварій енергосистем, а у деяких випадках – наслідки можуть носити катастрофічний характер. Тому завдання створення надійних і економічно ефективних телекомунікаційних систем має актуальний характер.

Сучасні тенденції змін телекомунікаційних мереж

Одним з найсерйозніших викликів нині стає поширення та поглиблення таких концепцій, поступовий перехід від концепції Internet of Devices до нової концепції Internet of Things, враховуючи прагнення розробників цих концепцій до підвищення рівня їх доступності для користувача, а також зростання вимог до динамічної масштабованості мереж, що відрізняються за масштабами, типом чи функціональністю. Також революційний вплив на зміну параметрів трафіку має зміна його внутрішньої структури. На основі сучасних досліджень Інтернету фірмою Cisco на сьогодні 75 % мобільного трафіку – це відео [1]. І за прогнозами цієї ж фірми частка відео-контенту у майбутньому буде тільки зростати. Іншим чинником, що суттєво впливає на структуру трафіку є широке впровадження хмарних технологій. Парадигма хмарних

обчислень став основою сучасної економіки, пропонуючи послуги на основі підписки в будь-який час, у будь-якому місці з оплатою послуг користувачами. Сучасними тенденціями, що відкривають нові можливості для управління трафіком, є також перехід багатьох технологій на розподілені обчислення, програмно-керовані мережі та оброблення даних на мережному рівні у вузлах мережного обладнання [2].

На сьогодні комп'ютерні мережі не позбавлені недоліків, таких як: складність управління мережею, висока вартість мережевого обладнання, недостатньо ефективне використання каналу зв'язку через передавання великої кількості інформації для управління мережею замість корисного трафіку.

Метою дослідження є розробка моделей, засобів збору та опрацювання даних та параметрів трафіку телекомунікаційних мереж. Встановлення відповідності між властивостями трафіку як реалізації цілочислового випадкового процесу і трафіку як послідовності випадкових інтервалів часу між подіями (потоку подій).

Моделювання поведінки трафіку

Сучасні телекомунікаційні мережі та мережне обладнання не використовують максимально свої функціональні можливості. Одна з причин – складність у поведінці мережного трафіку, який впливає на параметри якості обслуговування.

Однією з найбільш актуальних проблем дослідження трафіку є адекватне врахування його особливостей. Дослідження показують, що трафік сучасних телекомунікаційних мереж володіє особливою структурою, яка не дозволяє використовувати для проектування мережного обладнання класичні методи, що базуються на марківських моделях і формулах Ерланга [3]. Це ефект самоподібності трафіку, що приводить до пульсацій його надходження. Це явище значно погіршує характеристики (збільшує втрати, затримки, джиттер) при проходженні самоподібного трафіку через вузлове мережне обладнання, тому дослідження цього показника дозволить передбачити та зменшити вплив таких небажаних факторів.

Дослідження різних типів мережевого трафіку за останні півтора десятка років доводять, що мережевий трафік є самоподібним (self-similar) або фрактальним (fractal) за своєю природою. З цього випливає, що класичні методи, які використовуються моделювання мережевих систем, що базуються на використанні пуасонівських потоків [4], не дають повної і точної картини того, що відбувається в мережі.

Крім того, самоподібний трафік має особливу структуру, яка зберігається при багаторазовому масштабуванні. При проходженні трафіку у мережі, як правило, присутня деяка кількість пульсацій при відносно невеликому середньому рівні трафіку. Дане явище погіршує характеристики (збільшує затримки, джиттер пакетів) проходження самоподібного трафіку через вузли мережі. На практиці це реалізується таким чином, що пакети, при високій швидкості їх руху у мережі, надходять на вузол не окремо, а цілою пачкою, що може призводити до їх втрат через обмеженість буфера, розрахованого за класичними методиками.

У багатьох сучасних роботах відзначається, що об'єднання трафіку від декількох змінних ON/OFF джерел збільшує самоподібні властивості трафіку. Трафік стає сильно автокорельованим з довготривалою залежністю. Об’єднання великої кількості джерел даних характеризується синдромом нескінченної дисперсії і в результаті дає самоподібний об'єднаний мережевий трафік, який прагне до фрактального броунівського руху. Крім того, дослідження різних джерел трафіку вказує, що надто мінлива поведінка трафіку - це функція, яка властива архітектурі клієнт / сервер [5].

Не існує єдиного причинного фактору, який викликає самоподібність. Різні кореляції, що існують в самоподібному мережевому трафіку і які впливають на різних часових масштабах, можуть виникати з різних причин, змінюючи характеристики у конкретних часових масштабах.

Слід зазначити, що функціональність взаємодії на основі різних технологій сприяє зміні параметрів трафіку, бо механізми

маршрутизації пакетів мережевих зв'язків вимагають фрагментації при передачі між мережами з різними максильними розмірами блоку. Фрагментований механізм при обмеженні об’єму буферної пам'яті навіть із високим ступенем надійності на рівні каналу передачі, може призвести до значних втрат на рівні транспортних сполучень та, таким чином, до повторної передачі. Це також фактор, що впливає на властивості посилення самоподібних властивостей трафіку.

Висновки. На сьогодні у телекомунікаційних системах з пакетним передаванням інформації трафік є пачковим, що оцінюється відношенням пікової інтенсивності надходження пакетів до її середнього значення. Нові тенденції у розвитку комп’ютерних мереж створюють необхідність нових підходів та стратегій їх дослідження, а також переоцінку моделей, розроблених для вирішення таких питань, як масштабованість, еластичність, надійність, безпека, стійкість та застосування моделей поведінки трафіку. Робота має практичне застосування для підвищення продуктивності роботи комп’ютерних мереж. Кінцевими користувачами розроблених моделей та методів для підвищення ефективності роботи мережевого обладнання в майбутньому можуть стати різноманітні суб’єкти підприємницької діяльності та державні установи, що використовують у своїй діяльності телекомунікаційні мережі.

Подяка. Дане дослідження виконано за підтримки Міністерства освіти та науки України у рамках українсько-австрійського договору про співпрацю «Моделювання трафіку та телекомунікаційних мереж» (номер держреєстрації 0117U001612).

1. The Zettabyte Era: Trends and Analysis [Електронний ресурс]. – режим доступу: https://www.cisco.com/c/en/us/solutions/collateral /service-provider/visual-networking-index-vni/vni-hyperconnectivity - wp.html
2. Gelembe E. Steps towards self-aware networks.//Commun. ACM 52(7), 66-75 (2009).

3. Dronyuk, I.,Fedevych, O. Traffic flows ateb-prediction method with fluctuation modeling using Dirac functions// Communications in Computer and Information Science, Vol. 718, 2017, Pages 3-13; DOI: 10.1007/978-3-319-59767-6_1
4. Климаш М.М., Стрихалюк Б.М., Кайдан М.В. Теоретичні основи телекомунікаційних мереж.-Львів, 2011. – 496 С.
5. Демидов І. В. Аналіз методів підвищення продуктивності телекомунікаційних мереж хмарних сервісних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Телекомунікаційні та інформаційні технології. – 2016. – №1. – С. 41-47.

Як технологія 3D сканування змінює якість розслідування кримінальних правопорушень

Дуфенюк Оксана Михайлівна,

доцент кафедри криміналістики, судової медицини та психіатрії факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Технологія 3D сканування відома ще з 60-их років минулого століття і знайшла своє застосування у багатьох галузях діяльності людини (будівництво, маркшейдерські роботи, геодезія, архітектура і проектування, деформаційний моніторинг тощо). Для української криміналістичної науки тематика 3D сканерів також не нова, про що свідчать праці С.В. Данця, А.С. Непоради, А.І. Терешкевича, Р.М. Шехавцова та ін. Досвід іноземних фахівців пристосування цієї технології до потреб практики досудового розслідування кримінальних правопорушень, а також аналіз результатів впровадження 3D сканерів в польових умовах при збиранні та фіксації первинної інформації про злочини дозволяє виокремити цілий ряд позитивних характеристик, які здатні змінити якість цифрового документування слідчих (розшукових) дій, а разом з тим і якість розслідування кримінальних правопорушень. Розглянемо ці характеристики більш докладно.

1. Висока точність. Перше, на що звертають увагу фахівці – це точність документування інформації у графічній формі. Завдяки

системі лазерного сканування формується хмара тривимірних точок високої щільності, що має вигляд фотореалістичного зображення сканованого об'єкта (приміщення, відкритої ділянки, транспортного засобу, конкретного сліду тощо). Лазер рухається міліметр за міліметром, скануючи усі поверхні у відповідному діапазоні. Результатом є не анімація чи симуляція, а реалістична картина, масштабне моделювання, здатне забезпечити перебування слідчих на місці події та побачити обстановку такою, якою бачив її злочинець [1]. У різних сканерів може бути різне поле зору (вертикальне/горизонтальне), дальність сканування, швидкість сканування точок в секунду (обертання дзеркала), точність сканування, параметри вбудованої камери та інші технічні характеристики, проте поза сумнівом є те, що вербальна фіксація у протоколі значно програє у презентативності матеріалу й жодним чином не може надати настільки ж вичерпну картину місця події. Натомість 3D-модель дозволяє не тільки реалістично відтворити загальний вигляд місця події, але й точно зафіксувати розміри, відстані, просторові, кількісно-якісні та інші характеристики об'єктів. Особливої ефективності ця технологія набуває при необхідності документування місць події з насиченою слідовою картиною (пожежі, місця вибухів, місця авіакатастроф та інших транспортних пригод, вбивства тощо).

2. Швидкість. Для детального опису стандартної однокімнатної квартири традиційним вербальним способом знадобиться від півтори до двох, трьох, а інколи й більше, годин, тоді як 3D сканер дозволить створити фотореалістичну модель за кілька хвилин. Так, наприклад, американські фахівці штату Вісконсін на сканування місця виявлення мертвої жінки з вогнепальним ушкодженням витратили біля 30 хв. (чотири сканування тривалістю біля 6 хв. кожне, а також додатково 1-2 хв. на зміну локації сканера). Обробка даних була здійснена після сканування. Оператор швидко залишив місце події для того, щоб інші фахівці могли приступити до виконання своїх завдань [1]. Про значну економію часу та інших ресурсів при застосуванні 3D сканування місця події говорять польські

криміналісти [2, s. 54]. Схожими є результати проведених досліджень в Україні. Зокрема, за словами С.В. Данця, середній час сканування ДТП від 9 до15 хв. [3, с. 168].

3. Додаткові функції. Йдеться про можливості обробки даних, що забезпечуються програмним забезпеченням та технічними характеристиками 3D сканера. Очевидно, що від конкретної моделі та конкретного виробника залежатиме набір інструментів, здатних забезпечити різнопланову обробку даних для використання у кримінальному провадженні. Утім можна виокремити цілу низку таких напрямів, які відображають додаткові можливості технології 3D сканування під час досудового розслідування, крім візуалізації обстановки місця події:

- дослідження біологічні (зображення слідів крові у тривимірному зображенні, відтворення траєкторії бризок крові і можливість аналізу механізму їх утворення на місці події);
- дослідження дактилоскопічні (сканування відбитків пальців, що підвищує якість сканування через відсутність контакту зі сканером, створення баз даних тривимірних моделей відбитків);
- дослідження балістичні (створення 3D-моделей куль, гільз, на поверхні якої чітко відтворюються жолобки і борозенки, залишені після пострілу, за якими експерти можуть з достовірністю ідентифікувати застосовану зброю; розрахунки та наочна демонстрація траєкторії кулі) [4, с. 142];
- дослідження трасологічні (створення 3D-моделей об’ємних слідів взуття, босих ніг, протекторів шин, якщо вони виявлені на крихких, сипких поверхнях або маловидимий рельєф сліду; створення 3D-моделей слідів зубів);
- дослідження обставин ДТП (реконструкція механізму ДТП; детальне зображення деформації транспортного засобу, довжини слідів юза, подряпин на асфальті та ін., завдяки тому, що кожна зі сканованих крапок має свій набір координат X, Y, Z [3, с.169];

- дослідження антропоскопійні (створення 3D-моделей знівеченого обличчя, пошкодженої черепної коробки невпізнаного трупа особи);
- додаткові опції при необхідності підготовки цифрових фотографій, проекцій, планів та схем, інших додатків до протоколів [2, s. 54; 5, с. 251].

4. Простота використання. Технологія 3D сканування не є надто складною і після проходження спеціальних тренінгів інспектор–криміналіст чи слідчий може її опанувати і ефективно застосовувати. Підготовчий етап передбачає виставлення сканера за показами вбудованого нівеліру так, щоб він не відхилявся відносно вимог спеціальних датчиків, та виставлення орієнтирів (наприклад, для 3D сканерів FARO® – білих сфер, які дозволяють потім «зшити» окремі скани окремих ділянок). При цьому слід відмітити, не менш функціональними можуть бути ручні сканери, які існують на ринку новітніх технологій, як наприклад, FARO Freestyle3D X Scanner. Такі мобільні сканери не мають штативів і фахівець самостійно скеровує камери, за допомогою яких проводиться сканування [6]. Робочий етап передбачає сам процес сканування. Отримані файли копіюють у ноутбук або планшет з відповідним програмним забезпеченням. На завершальному етапі відбувається обробка даних залежно від поставлених цілей, можливостей технічного пристрою та модифікації програм. Простота використання стала одним із елементів маркетингової концепції одного із найбільших виробників 3D сканерів – вищезгаданої компанії FARO®. Суть її полягає в тому, що одна особа робить три прості кроки (One Person. Three Easy Steps): сканує місце події (Scan the Scene) – аналізує дані (Analyze the Data) – збирає докази (Deliver the Evidence) [7].

Окремої уваги заслуговує питання вартості технології. Впродовж останніх 15 років вартість сканера значно знизилася, що дозволяє поліцейським установам його придбати [1]. Компанії виробники постійно працюють над удосконаленням технічних характеристик, функціональністю та програмним забезпеченням свого продукту на ринку 3D технологій. На жаль, сьогодні можна констатувати

лише поодинокі випадки апробації 3D сканування у практиці українських експертних служб [8; 9, с.191]. Однак, враховуючи світові тенденції, широке впровадження таких інновацій у діяльності правоохоронних органів, зокрема у практиці досудового розслідування, є тільки питанням часу.

1. Why police should use new crime scene mapping technology [Електронний ресурс] – Режим доступу: https://www.policeone.com/police-products/3D-Laser-Scanners/articles/290043006-Why-police-should-use-new-crime-scene-mapping-technology.
2. Wykorzystanie możliwości skanowania 3D w oględzinach i dokumentowaniu miejsca zdarzenia / L. Kożmiński, M. Brzozowska, J. Kościuk, W. Kubisz // PROBLEMY KRYMINALISTYKI. – 2010. – № 267 (styczen-marzec). – S. 47–56.
3. Данець С.В. Застосування новітніх технологій лазерного сканування під час огляду місця дорожньо-транспортної пригоди / С.В. Данець // Криміналістичний вісник. – 2014. – № 2 (22). – С. 166–171.
4. Непорада А.С. Новітні технології в криміналістиці: 3D сканування під час огляду місця події / А.С. Непорада // Криміналістичний вісник. – 2016. – № 2 (26). – С. 141–143.
5. Шехавцов Р.М. Можливості використання технологій 3D сканування під час розслідування злочинів / Р. М. Шехавцов // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2010. – Вип. 3. – С. 247–251. [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/Vlduvs_2010_3_32.
6. FARO Freestyle3D X Scanner [Електронний ресурс] – Режим доступу: http://www.publicsafety.faro.com/assets/freestyle3dx_techsheet.pdf.
7. Scan. Analyze. Deliver. [Електронний ресурс] – Режим доступу: http://www.publicsafety.faro.com.
8. Терешкевич А.І. Застосування методу 3D сканування об’єктів в експертній службі МВС України / А.І. Терешкевич // Криміналістичний вісник. – 2016. – № 2 (26). – С. 158–160.
9. Данець С.В. Застосування автоматизованих засобів дослідження обставин ДТП / С.В. Данець // Вестник ХНАДУ. – 2013. – Вып.61–62 – С. 190–194.

Програмне забезпечення для кримінального аналізу

Зачек Олег Ігорович,

доцент кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Козаченко Вадим Вадимович,

здобувач ступеня бакалавра факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

У процесі розвитку суспільства постійно відбуваються суспільно-економічні та політичні зміни, що відображають діяльність тих чи інших категорій людей, організацій та об'єднань. Такі зміни часто зумовлюють виникнення криміногенних явищ та різноманітних форм злочинності, як простих форм, так і організованої злочинності. Для ефективної протидії злочинності необхідно використовувати усі найсучасніші досягнення науково-технічного прогресу. Одним із основних чинників, що впливають на ефективність здійснення оперативно-розшукової діяльності правоохоронних органів, є рівень їх інформаційного забезпечення. Перспективним є використання у діяльності правоохоронних органів кримінального аналізу, який призначений для забезпечення оперативно-розшукових підрозділів необхідною інформацією в рамках роботи щодо оперативно-розшукових справ. Історично концепція кримінального аналізу полягала у неформальному методі ідентифікації злочину із використанням патрульних поліцейських та детективів [1].

Кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого

проведення оперативного і стратегічного аналізу [2]. По суті, це обробка значного масиву цифрових даних за допомогою комп'ютерної програми. Дані оформлення адміністративних матеріалів, дані скоєних злочинів, дані щодо торгівлі алкоголем, публікації у соціальних мережах і афіша концертного туру – всі ці показники можуть корелювати. Кримінальний аналіз як засіб для правоохоронних органів, в тому числі для поліції є необхідним, а його робота – запорука ефективності, адже він полегшує роботу та створює необхідні умови для виконання таких завдань, як: розкриття злочинів, створення превентивної стратегії та тактики, розшук правопорушників, покарання правопорушників, покращення безпеки громадян, оптимізація внутрішніх процесів у Національній поліції, визначення пріоритетності патрулювання і розслідування [3].

Серед комп'ютерних програм, які забезпечують здійснення кримінального аналізу, існують такі: IBM i2 Analyst's Notebook, IBM i2 iBase, iConnect, iGlass, iBridge 8 та інші [4].

Для проведення кримінального аналізу доцільним є використання спеціалізованої аналітичної системи «IBM i2 Analyst's Notebook», яка дозволяє об'єднувати дані, які вже накопичені і розміщені за різними вкладками, здійснювати аналіз без додаткового завантаження, конвертації та перемикання між завданнями. Вибір аналітичного програмного забезпечення «IBM i2 Analyst's Notebook» не випадковий і ґрунтується на тому, що дана аналітична система фактично є міжнародним стандартом для проведення аналітичних досліджень під час розслідування злочинів. Цю систему використовують правоохоронні органи, силові відомства, банки, страхові компанії, телекомунікаційні компанії 70-ти країн, у тому числі: Інтерпол, Європол, ООН, НАТО [4].

Відповідно до трактування з офіційного джерела IBM Knowledge Center, IBM i2 Analyst's Notebook – це автономний продукт для настільних комп'ютерів, призначений для надання користувачам потужного, багатовимірного інструменту візуального аналізу. Об'єкти Analyst's Notebook представляють об'єкти реального світу, такі як банківські рахунки і телефони,

або події, наприклад, зустрічі. Зв’язки представляють взаємозв’язки між об'єктами, такі як відносини між людьми, володіння транспортними засобами, трансакції між банківськими рахунками або зустрічі між людьми. У Analyst's Notebook об’єкти та зв’язки називаються елементами. Властивості використовуються, щоб зберігати інформацію, яка відома про елемент, таку, як наявність у людини судимості або дата і час зустрічі. Важливо продумати, де розмістити ті чи інші відомості. Такі рішення впливають на доступні після цього типи аналізу і на надання інформації. Наприклад, нехай ви вирішили зберігати інформацію, таку як дата народження людини або модель транспортного засобу, як атрибут, а не як картку. Тоді властивість можна вивести на поверхню схеми і використовувати в аналізі [5].

IBM i2 Analyst`s Notebook дозволяє швидко та ефективно здійснювати аналіз системи взаємопов’язаних об’єктів, динаміки послідовних подій. Результати дослідження відображаються у вигляді зручних для розуміння схем і діаграм. Інформація зображена на діаграмі у вигляді об’єктів, до яких за необхідності можна додати додаткові атрибути, карточки даних з коментарями. Об’єкти на діаграмі зображені не лише у вигляді піктограм, але і у вигляді фотографій, файлів, аудіозаписів тощо. Тобто система візуального аналізу IBM i2 Analyst’s Notebook перетворює складну для сприйняття інформацію в діаграми та схеми. Функція Link Notebook підтримує схеми аналізу зв’язків, фінансових потоків тощо, у той час як Case Notebook «відповідає» за тимчасові графіки – схеми послідовності подій, діаграми дій у кожній із подій і комплексні діаграми, що відображають події та їх хід [4].

Для підвищення ефективності боротьби зі злочинністю у Національній поліції України створили управління кримінального аналізу. Завдання управління – консолідація і подальший аналіз всієї оперативної інформації. Головна задача управління – зведення всієї оперативної інформації в одну базу, її подальший аналіз. За словами тимчасово виконуючого обов’язки начальника Управління кримінального аналізу

Національної поліції України Володимира Єрофєєва в системі поліції існує багато джерел розрізненої інформації, що аналізується автономно співробітниками різних служб. Дані мають накопичуватись та зберігатись у спільній базі, адже інформація належить державі, як один із продуктів діяльності поліції. Таким чином, пріоритетною задачею є консолідація всієї оперативної інформації, її подальший аналіз, що допоможе у розкритті в першу чергу тяжких та особливо тяжких злочинів. Оперативний аналіз необхідний для збирання та обробки даних по резонансних злочинах аби скоординувати роботу слідчо-оперативної групи. Тактичний аналіз дає можливість оцінити обстановку через нанесення інформації на карти, визначаючи райони з підвищеним ризиком скоєння злочинів. Нарядам патрульної поліції надаватимуться рекомендації для проведення цільових відпрацювань районів. Стратегічний аналіз спрямований на аналіз діяльності організованих злочинних груп, а відтак – і на перспективу в роботі по боротьбі з ними [6].

Міністр внутрішніх справ України Арсен Аваков у розмові з генеральним секретарем Інтерполу Юргеном Штоком зазначив, що для забезпечення ефективної роботи підрозділів кримінального аналізу необхідно створити єдиний інформаційний простір, який дасть можливість доступу до баз даних Національної поліції, МВС, державних інформаційних реєстрів, даних Інтерполу та Європолу, GIS-систем, забезпечить можливість збору даних із відкритих джерел інформації [7].

Отже, аналізуючи вищевикладене, можна дійти висновку, що використання в роботі Національної поліції України спеціального програмного забезпечення «IBM i2 Analyst's Notebook» значно підвищує якість забезпечення процесу прийняття оперативних рішень, спрямованих на розслідування конкретних ситуацій, у тому числі за умов виявлення непередбачуваних зв'язків об'єктів та необхідності проведення аналізу великих масивів інформації. Але для ефективного використання таких засобів необхідне створення захищених інформаційних мереж правоохоронних органів, які дозволять одержати доступ до необхідної інформації.

1. Власюк О.В. Використання кримінального аналізу у боротьбі зі злочинністю: виникнення та становлення // Університетські наукові записки. 2012. № 4 (44). С. 351-356.
2. «Основи кримінального аналізу» — тренінг для правоохоронців [Електронний ресурс] // Одеський державний університет внутрішніх справ: [сайт]. Одесса, 2016. URL: http://oduvs.edu.ua/news/osnovi-kriminalnogo-analizu-trening-dlya-pravoohorontsiv/ (дата звернення: 30.11.2017).
3. Власюк В. Про сучасну модель підготовки нових поліцейських [Електронний ресурс] // Блог Владислава Власюка на LB.ua від 09.06.2017. URL: https://lb.ua/blog/vladyslav_vlasyuk/368596 pro_suchasnu_model_pidgotovki_novih.html (дата звернення: 30.11.2017).
4. Кіреєва О. Використання альтернативних аналітичних інструментів у кримінальному аналізі // Збірник наукових праць Національної академії державної прикордонної служби України. Серія: військові та технічні науки. 2016. № 4 (70). С. 64-76.
5. Данные Analyst's Notebook [Електронний ресурс] // IBM Knowledge Center. IBM Corporation, 2017. URL: https://www.ibm.com/support/knowledgecenter/ru/SS3J58/com.ibm.i2.anb.doc/items.html (дата звернення: 30.11.2017).
6. Кримінальний аналіз – це ефективна робота поліції та безпека громадян [Електронний ресурс] // МВС України: [сайт]. Новини від 30.11.2017. URL:http://mvs.gov.ua/ua/news/10309_Kriminalniy_analiz___ce_efektivna_robota_policii_ta_bezpeka_gromadyan_FOTO.htm (дата звернення: 30.11.2017).
7. Усі підрозділи Нацполіції України отримають доступ до баз даних Інтерполу з упровадженням системи I/24-7 [Електронний ресурс] // Інформаційне агентство Interfax-Україна. Новини від 22.11.2017. URL: http://ua.interfax.com.ua/news/general/463987.html (дата звернення: 01.12.2017).

Використання методів групування та кластеризації в NodeXL під час здійснення кримінального аналізу

Калиновський Олександр Валерійович,

заступник начальника відділу організації науково-дослідної роботи Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

Школьніков Владислав Ігорович,

здобувач ступеня магістра Національної академії внутрішніх справ

Актуальність. Інформатизації суспільства призводить до все більшого використання пересічними громадянами, у тому числі правопорушниками, таких соціальних мереж як Facebook, LinkedIn, Twitter. Не зважаючи на заборону використання Вконтакте та Одноклассники на теренах України спостерігається тенденція до використання правопорушниками і цих соціальних мереж. На жаль, в практичній діяльності органів Національної поліції мало використовуються можливості таких програмних продуктів як IBM i2 Analyst`s Notebook, NodeXL тощо. Саме останні активно можуть використовуватися при аналізі соціальних мереж, а також під час здійснення оперативного кримінального аналізу.

Метою статті є розкриття сутності методів групування та кластеризації, які використовуються в такому програмному аналітичному продукті як NodeXL.

Виклад основного матеріалу. NodeXL – це програмний пакет в Microsoft Excel 2007/2010/2013/2016 для соціального аналізу та візуалізації інформації.

За допомогою даного програмного пакету можливо здійснювати аналіз таких соціальних мереж як Facebook, Twitter, Youtube та ін.

NodeXL дозволяє об'єднувати в єдину групу конкретні об'єкти, які підлягають аналізу. Об'єктами аналізу в NodeXL можуть бути:

- дані, які вказані користувачем соціальної сторінки та є у відкритому або такому доступі, що дозволяє слідчому (оперативному працівнику) отримати останню (наприклад, в рамках здійснення такої негласної слідчої (розшукової) дії як зняття інформації з інформаційних електронних систем, доступ до яких не обмежується володільцем);
- учасники конкретних груп, публічних сторінок в Facebook;
- соціальні зв'язки користувача соціальної сторінки на Facebook;
- хеш-теги сайту Flickr (веб-сайт, який призначений для розміщення фотографій та відеоматеріалів, для їх перегляду, оцінки та архівування);
- соціальні зв'язки користувача Flickr;
- твіти (записи, які публікуються в Twitter) тощо.

Актуальним напрямком використання NodeXL в правоохоронній діяльності є об'єднання номерів телефонів з метою визначення групи спільних абонентів. Наприклад, алгоритми NodeXL можуть допомогти у встановлені групи абонентів, які потенційно є членам сім'ї тощо.

Node XL підтримує створення кластерів або груп різними способами:

- за атрибутами;
- за зв'язаними компонентами;
- за допомогою алгоритмів кластеризації.

Вибір вищезазначених способів можливо здійснити, знайшовши їх в меню «Аналіз». Так, створення груп за атрибутами означає створення об'єднань об'єктів коефіцентом кластеризації, обчисленим рівнем власного вектору, ступеня, близькості тощо. Це стандартні індикатори, які використовуються під час здійснення аналізу соціальних зв'язків. Також існує можливість аналізувати і за іншими атрибутами, які створені користувачем. Наприклад, таким атрибутом може виступати новостворена колонка в NodeXL під назвою «Followers» (кількість осіб, які слідкують за публічною сторінкою, особою тощо).

Створення груп за зв’язаними компонентами означає, що кожен об’єкт аналізу повинен бути суворо пов’язаний з іншим.

На прикладі вказаному на рис. 1 слід відмітити, що в кожній групі (G1, G2) є спільний номер мобільного телефону, який поєднує всі інші номери. І не обов’язковою є умова про те, що кожен із номерів телефонів групи повинен був зв’язуватися з іншим номером тієї ж групи. Головна ознака – наявність одного загального для всіх зв’язуючого компоненту. За допомогою візуалізації в IBM i2 ANB можливо цю ознаку простежити (рис. 2).

	A	B
1	Group	Vertex
2	G1	456819398
3	G1	465013464
4	G1	422559501
5	G1	456070550
6	G1	452164298
7	G1	442486164
8	G1	429930774
9	G1	461236107
10	G1	425509274
11	G1	463680482
12	G1	446751303
13	G1	432836160
14	G1	436593175
15	G1	424903213
16	G1	420244262
17	G1	428166782
18	G1	462490160
19	G1	422265166
20	G1	424424930
21	G1	420060085
22	G1	435275181
23	G2	462240906
24	G2	451678486
25	G2	432347836
26	G2	466345748
27	G2	467276899
28	G2	436218800
29	G2	440388324
30	G2	422676762
31	G2	438631723
32	G2	445745069
33	G2	432084891
34	G2	434964378
35	G2	454499305
36	G2	460520664
37	G2	430317084
38	G2	426295032
39	G2	437548986
40	G2	456383941
41	G2	426588454
42	G3	444214372
43	G3	434595141
44	G3	436592066

Рис. 1. Групування номерів мобільного телефону

Створення груп за допомогою алгоритмів кластеризації поділяють на: Clauset-Newman-Moore; Wakita-Tsurumi; Girvan-Newman.

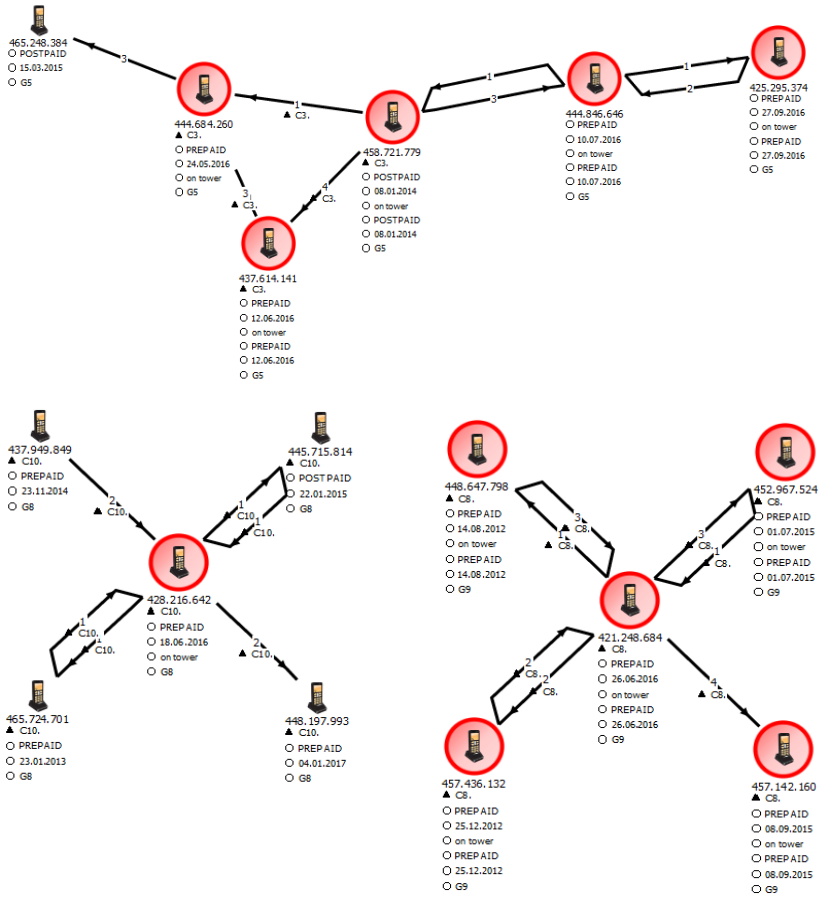


Рис. 2. Приклади візуалізації групування за допомогою NodeXL в IBM i2 ANB (атрибути G5, G9, G8)

Загальна ідея кластерного аналізу зводиться до багатовимірної процедури, яка полягає в упорядкуванні об’єктів в порівняно однорідні групи, тобто кластери. Основна мета кластерного аналізу – це знаходження груп схожих об’єктів у вибірці.

Висновки. Великі масиви інформації вимагають від працівників правоохоронних органів наявності спеціальних навичок роботи

з аналітичними інструментами та обізнаності в методах аналізу. Слід відмітити недостатню розвиненість аналізу соціальних зв'язків (social network analysis) у діяльності органів Національної поліції. Саме раціональне застосування методів аналізу соціальних зв'язків дає змогу підвищити аналітичну підтримку досудового розслідування кримінальних проваджень та здійснення оперативно-розшукової діяльності.

1. Nasre Messarra. NodeXL for beginners [Електронний ресурс]. – Режим доступу: http://nasri.messarra.com
2. Peter Aldhous. NodeXL for Network analysis [Електронний ресурс]. – Режим доступу: http://www.peteraldhous.com/CAR/CAR2013_NodeXL.pdf

Проблеми застосування інформаційних технологій правоохоронними органами України: історичний аспект

Комісарчук Юлія Анатоліївна,

доцент кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Карандюк Ольга Михайлівна,

здобувач освітнього ступеня бакалавра факультету №1 ІПФПНП 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. Висококваліфіковане 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.

Розглянемо процес впровадження інформаційних технологій у діяльність правоохоронних органів в історичному аспекті. Варто зауважити, що фазу просування інформатизації діяльності правоохоронних органів України наприкінці XX століття можна класифікувати, як початкову. Основи існуючого інформаційного забезпечення органів внутрішніх справ України були закладені у 70-х роках та орієнтовані в напрямі інформаційної підтримки оперативно-службової діяльності підрозділів у боротьбі зі злочинністю. Вирішення цих завдань на той час досягалося повною централізацією інформаційних обліків. Принципи побудови відображали притаманний тим рокам рівень розвитку технічних засобів і досягнень технології [1].

Аналіз стану інформатизації, наведений в Концепції розвитку системи інформаційного забезпечення органів внутрішніх справ України на 1997 – 2000 роки, показав, що існуючі банки даних (БД) оперативно-розшукового і оперативно-довідкового призначення, розробка і впровадження яких були здійснені наприкінці 80-х та початку 90-х рр., в чималій мірі застаріли і не виконували покладені на них функції.

Багаторічний досвід практичної експлуатації БД дозволив визначити їх основні недоліки:

- неузгодженість при створенні та впровадженні інформаційних банків даних;
- дублювання збирання і багаторазова переробка однакових даних різними галузевими службами і на різних рівнях;
- багаточисельність та недосконаліть первинних облікових документів;
- слабкий інформаційний зв'язок між обліково-реєстраційними, оперативно-розшуковими і довідковими фондами різних служб;
- недостатня повнота і вірогідність даних;
- несвоєчасне надходження до споживачів оперативно-службової інформації через недосконаліть технології

подання відомостей в банки даних і слабкого використання сучасних засобів комп'ютерної техніки і зв'язку;
- застарілість технічних комплексів МВС України в областях, переважна більшість яких виробила свій ресурс;
- недосконалість організаційно-кадрового забезпечення інформаційних підрозділів МВС в областях та в галузевих службах;
- нераціональне використання відповідного фінансування на підтримку та розвиток інформаційної системи;
- недосконалість та неврегульованість нормативно-правової бази інформаційних банків даних [2].

Причинами цього, з одного боку, є недоліки установчих розробок систем, а з іншого – відірваність конкретних споживачів інформації (практичних працівників органів внутрішніх справ) від банків даних, неможливість чи незручність безпосереднього доступу до інформації, і як наслідок – їх незацікавленість в підтримці інформаційних підсистем у якісному та актуальному стані.

Здійснення аналізу ефективності роботи правоохоронних органів щодо декриміналізації суспільства, практика боротьби зі злочинністю переконливо свідчить про суттєву, а в багатьох випадках пріоритетну роль системи інформаційного забезпечення органів Національної поліції (далі – НП) як ланки, що зумовлює ефективність роботи правоохоронних структур. Система інформаційного забезпечення здійснює інформаційну підтримку органів НП у розкритті і попередженні злочинів, установленні і розшуку злочинців, надає багатоцільову статистичну, аналітичну та довідкову інформацію [1].

Досвід використання комп'ютерних інформаційних систем і технологій в правоохоронній сфері обумовлює основні тенденції їх розвитку та удосконалення:

- удосконалення форм та методів керування системами інформаційного забезпечення;
- впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних обліків;

- централізацію та інтеграцію комп'ютерних банків даних;
- розбудову та широке використання ефективних та потужних комп'ютерних мереж;
- застосування спеціалізованих засобів захисту та безпеки інформації;
- налагодження ефективного взаємного обміну кримінологічною інформацією на міждержавному рівні [3].

Концентрація зусиль на визначених напрямах має забезпечити суттєве підвищення рівня ефективності володіння інформаційними технологіями в системі МВС.

Ставлення до даних проблем, на наш погляд, повинно бути критичним саме в тому плані, що усі негаразди і протиріччя, у тому числі і злочинного характеру, мають місце завдяки недосконалості тієї чи іншої системи, її не цивілізованості, або недостатньої цивілізованості, а також в неспроможності задовольнити потреби її громадян. Тому вихід з даних критичних ситуацій слід шукати в удосконаленні вже існуючих інформаційних технологій, та спрямувати діяльність НП на забезпечення своїх працівників та підрозділів в цілому – інноваційними інформаційними технологіям, що в свою чергу дасть змогу правоохоронцям якісно та швидко здійснювати свої повноваження щодо захисту прав, свобод та законних інтересів громадян.

---

1. Про інформацію: Закон України від 02 жовтня 1992р. № 48, ст.651, станом на 06 квітня 2000 р. № 27, ст. 213.
2. Про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: положення від 16 травня 2016 р. № 460 // Наказ Міністерства внутрішніх справ. – 2016. – № 436.
3. Аніловська Г.Я. Інформаційна безпека держави в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

Перспективи розвитку інформаційних технологій у діяльності органів Національної поліції України

Комісарчук Юлія Анатоліївна,

доцент кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Моняков Максим Миколайович,

здобувач освітнього ступеня бакалавра факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

Дмитришин Олена Олегівна,

здобувач освітнього ступеня магістра факультету № 6 Львівського державного університету внутрішніх справ

У зв'язку із стрімким розвитком комп'ютерних технологій, удосконаленню електронно-обчислювальних машин, використанням таких технологій у повсякденному житті, виникає необхідність належного забезпечення передачі та аналізу інформації, яка становить службовий інстерес для підрозділів Національної поліції України. Сьогодні на багатьох підприємствах, в установах, організаціях практично всі документи створюються в електронному вигляді з використанням певних технологій, автоматизуються процеси обробки даних. Особливо актуальним залишається практичне введення електронних систем документообігу у функціонуванні державних органів та силових структур [1].

Визначимо яке ж значення мають поняття «інформаційні технології» та «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. 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 [2]. На сьогоднішній день АІС вико-

ристовується у різних підрозділах Національної поліції для вирішення покладених на поліцію завдань. Проте, незважаючи на чималу кількість видів АІС, на даному техногенному розвитку вони вважаються застарілими та вразливими для стороннього втручання, що може призвести до витоку інформації, тобто вчинення кіберзлочинів щодо несанкціонованого втручання у автоматизовані системи. Проте, на думку окремих експертів, діяльність державних органів повинна бути спрямована на «вербування» осіб, які в міру своїх вмінь і навичок вже змогли несанкціоновано втрутитись у роботу АІС, тому вони в свою чергу можуть створити і захист від такого втручання, а також систематично вдосконалювати окремі види АІС.

У жовтні 2016 року відбулася масштабна конференція у Кремнієвій долині щодо інвестування іноземного капіталу в інформаційні технології України та інших держав, де один із українських проектів переміг в головному змаганні заходу. Один із організаторів – Нік Білогорський звернув увагу на те, що в Україні є достатньо талановиті «хакери», які зможуть залучатися іноземними державами для розробки чогось нового. Оскільки в Україні ведеться війна, це відлякує іноземних інвесторів і не дає у повній мірі використовувати можливості українських хакерів. На думку Ніка Білогорського головною проблемою недостатності просування українських хакерів є відсутність інвестицій у сферу інформаційних технологій, як зарубіжних країн, так і з боку державної влади. [3] Тому, про ефективну координацію діяльності щодо удосконалення інформаційної системи України сьогодні говорити важко. Передусім, досі незрозуміло, хто, власне, відповідає за кібербезпекову тематику в державі.

В. Горбулін вважає, що Україна не просто може, а вимушена стати на аналогічну позицію інших держав щодо розуміння актуальності і важливості розвитку інформаційних технологій і перестати концентруватися виключно на оборонних заходах. Маючи один із найкращих у світі людських потенціалів – фахівців з інформаційних технологій, Україна має всі підстави

вийти на передові позиції світового рейтингу у розвитку інформаційних технологій. Також було зазначено, що CERT-UA – підрозділ, який займається забезпеченням безпеки проти несанкціонованого втручання, оголосив про набір хакерів і повідомив, що очікувана заробітна плата становитиме 3,5-5 тис. грн. З'ясувалося, що патріотизм багатьох фахівців не сягає так далеко, аби працювати за таку суму на державній службі. Це могла бути незначна кількість молодих фахівців, які пройшли серію національних кіберзмагань (що в більшості розвинених держав є одним із джерел пошуку таких фахівців) та довела свій певний рівень та фах [4].

Сучасний розвиток інформаційних технологій вимагає належного захисту інформації, яка зосереджена в автоматизованих інформаційних системах. Існує думка, що такий захист можуть забезпечувати лише ті особи, які довели, що можуть зламати аналогічний захист в певній системі. Перспектива розвитку інформаційних технологій безпосередньо залежить від внутрішньої політики держави. Ця політика повинна бути спрямована на удосконалення інформаційних систем органів Національної поліції та залучення осіб, які могли б створювати ці системи та здійснювати заходи щодо їх захисту. Саме тоді буде підвищена ефективність виконання завдань, які покладені на поліцію.

1. Верескун, М. В. Інформаційні технології як інструмент підвищення ефективності управління Національною поліцією / М. В. Верескун // Національна поліція Донеччини: проблеми становлення та стратегія розвитку – 2016 : Всеукр. наук.-практ. конф. (Маріуполь, 21 жовтня 2016 р.) : тези доповідей / ДВНЗ «ПДТУ», Головне упр. Нац. поліції в Донецькій області, Донецькій юридичний ін-т. – Маріуполь, 2016. – С. 161–163.
2. Снегірьова Т. Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС.
3. Скирта О. Ник Белогорский: «Украину можно продвигать, как страну с хакерами в хорошем смысле» [Електронний ресурс] /

Олена Скирта // Журнал \»Platforma\». – 2016. – Режим доступу до ресурсу: http://platfor.ma/magazine/text-sq/projects/nik-belogorskii/.
4. Горбулін В. У пошуках асиметричних відповідей: кіберпростір у гібридній війні [Електронний ресурс] / Володимир Горбулін // Газета \»ZN,UA\». – 2015. – Режим доступу до ресурсу: http://gazeta.dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html.

Питання інформаційно-аналітичного забезпечення діяльності правоохоронних органів

Кубрак Володимир Петрович,

старший викладач кафедри інформаційних технологій Харківського національного університету

Ефективність боротьби з правопорушеннями, і перш за все з кримінальними правопорушеннями, в значній мірі залежить від інформаційного забезпечення діяльності правоохоронних органів.

Ціль системи інформаційного забезпечення полягає в здійсненні інформаційної підтримки діяльності правоохоронних органів щодо попередження, розкриття і розслідування кримінальних правопорушень, встановлення і розшуку осіб, які їх вчинили, наданні всебічної статистичної, аналітичної і довідкової інформації про стан кримінальних правопорушень і результати боротьби з ними.

Складовою частиною системи інформаційного забезпечення діяльності правоохоронних органів є інформаційно-аналітичне забезпечення, яке своїм завданням має забезпечення правоохоронних органів відомостями про стан та динаміку кримінальних правопорушень, фактори, що їх обумовлюють, а також відомостями про результати роботи правоохоронних органів щодо виконання поставлених перед ними завдань.

На сьогодні під час швидкого розвитку процесів інформатизації, комп’ютеризації проблема інформаційного-аналітичного забезпечення діяльності правоохоронних органів України набуває досить важливого значення.

Система правоохоронних органів України під час своєї діяльності спирається на певні джерела інформації, інформаційні процеси та ресурси. Тому ефективне функціонування правоохоронної системи можливе лише при застосуванні відповідного комплексу заходів, що включає в себе подання, приймання та комп'ютерну обробку певних статистичних даних та використання аналітичних процедур для їх різностороннього та поглибинного аналізу, прийняття відповідних рішень.

Наявність об'єктивного та достатнього обсягу аналітичної інформації є головними умовами прийняття вірних управлінських рішень по попередженню негативних тенденцій, ефективному керуванню силами та засобами, своєчасному наданню підлеглим органам необхідної допомоги та поширенню передового досвіду.

Завданнями інформаційно-аналітичного забезпечення є:

- дати чисельну характеристику стану та динаміки правопорушень, діяльності правоохоронних органів щодо боротьби з ними;
- виявити статистичні зв'язки, залежності, співвідношення, закономірності стану та динаміки правопорушень. Оскільки на правопорушення, і, перш за все кримінальні, впливають різні соціальні, економічні, політичні та інші фактори, то необхідно виявити вплив цих факторів на стан та динаміку правопорушень;
- визначити тенденції розвитку правопорушень, скласти статистичний прогноз;
- виявити «тривожні» моменти в характеристиці правопорушень, позитивні сторони та недоліки в роботі правоохоронних органів, щоб на основі цих даних вчасно прийняти рішення, розробити заходи щодо поліпшення роботи та усуненню недоліків.

Потреба створення і використання інформаційно-аналітичного забезпечення визначається тим, що на сучасному етапі раціональне поєднання і взаємодія в просторі і часі наявних сил і засобів правоохоронних органів для досягнення конкретних

цілей в боротьбі зі злочинністю, можлива тільки при наявності найбільш повних і точних відомостей про злочинність, як про об'єкт дослідження.

Для визначення кращих рішень потрібне більш своєчасне зібрання даних про стан злочинності, про зв'язки між різними видами злочинності та соціально-економічними процесами, що протікають в суспільстві, про кількісні та якісні характеристики злочинності в минулому, сьогоденні і майбутньому.

Таким чином, інформаційно-аналітичне забезпечення має представляти собою сукупність математичних методів, моделей і алгоритмів, які є основою для розробки прикладних програм при вирішенні завдань обліку інформації про злочинність і її аналізу. Інформаційно-аналітичне забезпечення створюється на основі інтеграції функціональних, інформаційних, алгоритмічних, програмно-технічних засобів окремих елементів, при цьому інтеграція не має на меті дублювання існуючих інформаційно-аналітичних служб, а орієнтована на використання потоків впорядкованої інформації для отримання своєчасної і об'єктивної оцінки стану злочинності, прогнозування динаміки її розвитку, визначення комплексу заходів по боротьбі зі злочинністю.

Внаслідок інтеграції функціональних підсистем забезпечується функціональний та інформаційний зв'язок центральних елементів з інформаційними службами на регіональному, відомчому та об'єктному рівнях. Потоки і фонди інформації накопичуються і циркулюють в процесі взаємодії всіх служб з населенням і між собою як по вертикалі так і по горизонталі на всіх рівнях управління в системі правоохоронних органів. В організаційному плані ефективне функціонування і подальший розвиток інформаційно-аналітичного забезпечення обумовлюється активною участю зацікавлених служб, оперативністю і узгодженістю роботи користувачів, що виражається в своєчасному зборі необхідної інформації, перевірці її вірогідності, коригуванні фондів інформації, обробки і видачі даних в необхідних аспектах.

Національна поліція України вирішує покладені на неї завдання у взаємодії з іншими міністерствами, відомствами і організаціями. Серед органів державного управління країни окрему підмножину складають органи прокуратури, національної поліції України, юстиції, СБУ, суд. Ці органи управління керують різними галузями, однак реалізована ними підмножина функцій держави має високий ступінь спільності. Тісний взаємозв'язок зазначеної підмножини органів державного управління обумовлений і тим, що завдання, які ними вирішуються, базуються на єдиних інформаційних фондах та нормативних актах.

Таким чином, при створенні інформаційно-аналітичного забезпечення правоохоронної діяльності необхідно мати єдині інформаційні фонди правоохоронних органів з метою забезпечення повноти інформованості та координації діяльності різних правоохоронних органів, здійснити узагальнення накопиченої інформації з подальшим її використанням для аналітичних досліджень, використовувати основні показники стану і динаміки злочинності, а також показники діяльності правоохоронних органів. Єдине інформаційно-аналітичне забезпечення дозволяє на основі більш повного використання всіх даних, що надходять, сучасних методів і засобів створити основу для ефективної роботи правоохоронних органів та визначення варіантів необхідних управлінських рішень.

Ефективність від впровадження такого інформаційно-аналітичного забезпечення виражається в скороченні термінів обробки інформації, поліпшенні точності і достовірності одержуваних даних, зниженні впливу суб'єктивних факторів при прийнятті рішень, оптимізації розстановки сил і засобів та покращенні інших кількісних і якісних показників.

Інформаційно-аналітична робота в органах НПУ здійснюється всіма галузевими службами, всіма підрозділами в межах їх компетенції. Вимоги до організації цієї роботи для кожного рівня системи НПУ різні в зв’язку з різними завданнями цих органів і їх неоднаковими можливостями. Як складова частина управлінської діяльності інформаційно-аналітична робота

притаманна кожному органу, кожному його структурному підрозділу, хоча, маючи забезпечуючий характер, вона більш розвинута на рівні МВС України, ГУМВС, УМВС, де є навіть спеціальні інформаційні та аналітичні підрозділи.

Тому ознайомлення з питаннями інформаційно-аналітичної роботи в органах НПУ повинне стати складовою частиною знань, які отримують курсанти системи МВС України в процесі навчання. До того ж якась частина курсантів після закінчення навчання буде працювати в інформаційних та аналітичних підрозділах НПУ, тому знання інформаційно-аналітичної робота їм необхідне.

Треба знайомити курсантів з методикою проведення конкретного аналітичного дослідження, з етапами, які необхідно пройти при проведенні цього дослідження.

Треба мати уявлення про джерела отримання інформації при проведенні інформаційно-аналітичної роботи. Найважливішими джерелами інформації є державна статистична звітність правоохоронних органів, дані економічної, соціальної, демографічної статистики, результати вивчення громадської думки про злочинність і роботу правоохоронних органів. Комплексний аналіз цих матеріалів дає змогу отримати найбільш повну характеристику стану та динаміки злочинів, контингенту осіб, які їх вчинили, факторів, які обумовлюють стан та динаміку злочинності, а також ефективність заходів боротьби зі злочинністю.

Курсантів треба знайомити з методикою проведення статистичної роботи в правоохоронних органах, як частини інформаційно-аналітичної роботи, документами, які використовуються для обліку правопорушень.

Прийняттю управлінських рішень в сфері боротьби з правопорушеннями і забезпечення правопорядку, як правило, повинен передувати прогноз злочинності. Тільки тоді рішення стають ефективними, такими, що дозволяють попереджувати негативні тенденції. Прогнозування злочинності становить процес визначення ймовірності злочинних дій, в основі якого

лежить вивчення емпіричних даних і облік тенденцій розвитку. Курсантів необхідно знайомити з формами та методами математичного прогнозування злочинності.

Питання інформаційно-аналітичної роботи не можливо вирішувати без використання комп'ютерної техніки. Тому в процесі вивчення цих питань курсантам необхідні знання як з юридичних дисциплін, так і з комп'ютерних наук.

Таким чином, інформаційно-аналітичне забезпечення правоохоронних органів є необхідною умовою їх ефективної діяльності, а знання питань проведення інформаційно-аналітичної роботи є необхідною складовою частиною знань, які повинні отримати курсанти системи МВС України.

Проблема оцінки якості спеціального програмного забезпечення інформаційних систем Національної поліції

Кудінов Вадим Анатолійович,

професор кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент

Відповідно до статті 25 Закону України «Про Національну поліцію» [1] поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень [2]. В рамках цієї діяльності поліція формує бази (банки) даних, що входять до Єдиної інформаційної системи Міністерства внутрішніх справ України, користується цими базами (банками) даних та інших органів державної влади тощо. Крім того, поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень [1]. При цьому потребує свого вирішення проблема оцінки якості спеціального програмного

забезпечення (далі – СПЗ) інформаційних систем (далі – ІС) Національної поліції.

Необхідність ретельного дослідження якості цього СПЗ обумовлена тим, що воно несе більше функціональне навантаження при вирішенні завдань управління, ніж технічні засоби. Тому якість СПЗ в значній мірі визначає якість системи в цілому. Витрати на розробку СПЗ мають тенденцію до збільшення і складають 50-80 % витрат на розробку ІС в цілому. Якість СПЗ є критично важливим фактором для забезпечення адекватної та ефективної роботи відповідних ІС. Низька якість СПЗ, що використовується, може привести до серйозних і навіть фатальних негативних наслідків, глобальність яких залежить від специфіки використання СПЗ. Навіть якщо і вдається уникнути надзвичайних подій, використання неякісних програм завдає шкоди ефективності роботи.

Процеси розробки і впровадження складних систем, до яких відноситься, зокрема, СПЗ, повинні знаходитись під твердим управлінським контролем. В даний час практично в усіх підрозділах та організаціях, що займаються розробкою СПЗ, забезпечується контроль найважливіших характеристик, пов’язаних з виробництвом і використанням програмних продуктів, таких як час, фінансові засоби, ресурси і т. ін. Однак у більшості випадків поза межами сфери контролю виявляється найбільш важлива характеристика програмних продуктів, заради якої, власне і здійснюються витрати часу, фінансових засобів і ресурсів – це цільова якість програмного продукту (цільова якість означає необхідну і достатню якість, що відбиває реальні потреби користувача). Відсутність можливості установки повного контролю викликає зростання кількості необґрунтованих рішень, збільшує проектні ризики, пов’язані з розробкою і впровадженням систем.

Значної частини труднощів, що виникають при розробці та впровадженні СПЗ, можливо уникнути, якщо с самого початку створювати систему забезпечення якості у відповідності до певної методології. Ця методологія повинна враховувати безперервність процесів розробки та впровадження, статичність

цілей розробника, динамічність вимог замовника, необхідність забезпечення високої надійності та точності функціонування, зручності експлуатації та гнучкості системи при зміні нормативних даних та інформаційних масивів.

При створенні СПЗ необхідно враховувати те, що витрати на доробку вже діючих програм та усунення помилок, що виявляються в процесі використання, досягають іноді 75 % загальної суми експлуатаційних витрат [3]. За іншими даними на це витрачається від 30 до 50 % загального бюджету розробки [4], а помилки, що не виявлені на початку життєвого циклу, коштують від 70 до 85 % вартості переробки. Набагато дорожче виправити помилки, які знайдено пізніше в проекті [5].

Для забезпечення необхідного рівня якості програмних продуктів у міжнародній практиці знаходили застосування два підходи: орієнтований на продукт і орієнтований на процес. Обидва підходи вимагають наявності системи управління якістю.

При першому підході акцент робиться на контроль якості шляхом іспиту готового програмного продукту. Цей підхід базується на припущенні, що чим більше виявлено і усунуто помилок у програмному продукті при іспитах, тим вище його якість. Тестування розробленого програмного забезпечення, що проводиться у відриві від інших процесів, може попередити упровадження некондиційного продукту, але не гарантує раціональності використання ресурсів на попередніх етапах розробки СПЗ. Недолік такого підходу полягає в тому, що: 1) усунення помилок у готовому продукті на етапі іспитів обходиться в десятки разів дорожче, ніж якби ці помилки були відвернені чи усунуті вчасно на ранніх етапах життєвого циклу програмного продукту; 2) відсутні методи і засоби іспиту програмного продукту, що гарантують повне виявлення у випробуваних програмних продуктах помилок і недоліків.

При другому підході акцент робиться на вживання заходів по запобіганню, оперативному виявленню і усуненню помилок у програмному продукті шляхом завчасного визначення відповідальності, планів забезпечення, основних процедур по

забезпеченню якості розроблювальних програмних продуктів і проведення відповідних заходів, починаючи із самих ранніх етапів життєвого циклу. Реально працююча система забезпечення якості повинна охоплювати всі процеси, що пов'язані із створенням СПЗ: з моменту першого контакту із замовником і визначення його вимог аж до вилучення СПЗ із експлуатації. Цей підхід у даний час можна вважати загально прийнятим. Дослідження доводять: чим вище якість процесу розробки, тим вище якість розробленого в цьому процесі програмного забезпечення. Якість на кожній стадії проекту збільшується в основному за рахунок використання проміжного продукту більш високої якості, що був вироблений на попередній стадії життєвого циклу.

На основі цього можливо зробити наступні висновки: 1) якість накопичується в програмному продукті кумулятивним чином, причому вклад в якість, що був здійснений на ранніх стадіях, більш впливовіший на кінцевий продукт; 2) тестування і оцінка якості СПЗ повинні відбуватися на всіх стадіях життєвого циклу.

Важливою особливістю є наявність великої кількості різнорідних класів СПЗ, що обов'язково необхідно враховувати і що унеможливлює застосування будь-якої стандартної моделі якості. Специфіка СПЗ вимагає проведення його детальної класифікації та чіткого ранжирування по важливості відповідно до моделі якості для гарантування якісного виконання ним завдань за функціональним призначенням.

Таким чином, для забезпечення цільової якості спеціального програмного забезпечення інформаційних систем Національної поліції необхідно її оцінку проводити у відповідності до спеціально розробленої методології з урахуванням специфіки застосування СПЗ на кожному етапі його життєвого циклу. Універсалізація стандартної моделі якості може бути досягнута шляхом визначення пріоритетності її складових для різних типів СПЗ.

1. Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/580-19/page.
2. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28 жовтня 2015 року № 877. Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/877-2015-%D0%BF.
3. Б. Боэм. Характеристики качества программного обеспечения / [Б. Боэм, Дж. Браун, Х. Каспар и др.]. Пер. с англ. Е.К. Масловского. – М.: Мир, 1981. – 206 с.
4. Boehm B.W., Philip N. Papaccio. Understanding and Controling Software Costs. IEEE Transactions on Software Engineering, № 14(10), 1988. – P. 1462-1476.
5. Grady R.B. An economic release decision model: insights into software project management // In proceedings of the applications of software measurement conference, Orange Park, Fl: Software Quality Engineering, 1999. – P. 227-239.

Незаконне розповсюдження медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів мережі Інтернет: питання спеціальних експертиз

Кунтій Андрій Ігорович,

доцент кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук

Технологічний прогрес, що відбувається сьогодень, має чимало позитиву, проте, нажаль, Інтернет простір став ще одним способом учинення різноманітних злочинів. Сьогодні саме в мережі Інтернет зосереджена основна частина медіа контенту, проте його безконтрольне поширення завдає чималої шкоди різним сферам життєдіяльності людини. Незаконне розповсюдження медійного контенту є способом вчинення злочинів, що посягають на різні об’єкти, які знаходяться під кримінально правовою охороною. Найпоширенішими видами порушень як в мережі Інтернет, так і при наданні програмних

послуг є: незаконне відтворення і копіювання музичних, художніх, літературних творів чи комп'ютерних програм без попереднього надання на це згоди автором чи правовласником. Це виражає порушення прав авторів, до яких відноситься авторське та суміжні права. Власне досліджуваний нами вид кримінального правопорушення найбільш пов'язаний із порушенням авторських та суміжних прав.

Питанням, пов'язаних з розслідуванням порушенням авторського та суміжних прав Т.В. Авер'янова, В.П. Бахін, Р.С. Бєлкін, П.Д. Біленчук, В.Б. Вєхов, А.Ю. Головін, В.О. Голубєв, В.Г. Гончаренко, В.А. Журавель, А.В. Іщенко, О.Н. Колесніченко, В.К. Лисиченко, І.М. Лузгін, Г.А. Матусовський, Б.В. Романюк, М.В. Салтевський, В.В. Тіщенко, В.Ю. Шепітько та інші.

Як свідчить статистика, все популярніше стає такий вид порушень як плагіат. Такі порушення в мережі Інтернет порушують матеріальні і нематеріальні права авторів. За офіційними даними у 2015 році було зареєстровано 250 фактів порушення авторських та суміжних прав; у 2016 році – 157; протягом січня-серпня 2017 року – 78[1].

Під час розслідування злочинів у сфері комп'ютерної інформації можуть призначатися та проводитися і традиційні криміналістичні (трасологічна, почеркознавча, експертиза речовин і матеріалів), економічні, судово-бухгалтерські, і спеціальні – комп'ютерно-технічні експертизи (КТЕ) та експертизи з питань інтелектуальної власності.

Так, предметом експертизи об'єктів інтелектуальної власності є в першу чергу встановлення на основі спеціальних знань фактичних даних, що підтверджують або спростовують можливу контрафактність даного примірника твору. Найчастіше подібні експертизи проводяться комплексно, оскільки ними вирішуються питання, пов'язані з різним спеціальностям.

[1]Єдині звіти про кримінальні правопорушення за 2015 – серпень 2017 року [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua.

Особливу увагу потрібно приділяти змісту питань, які слідчий ставить перед експертом. Як правило, при призначенні експертизи об'єктів інтелектуальної власності рекомендується ставити такі основні питання:

1. Хто є власником немайнових прав на об'єкти авторського права (твори), що містяться на матеріальних носіях (вказати вид носія, наприклад, цифровий накопичувач і т. д.), представлених на експертизу?

2. Чи є матеріальні носії, з творами, що містяться на них, що представлені на експертизу об'єктами авторського права (творами), та чи містять вони ознаки контрафактності?

Об’єктами комп’ютерно-технічного дослідження є: цифрові носії інформації (накопичувачі на гнучких і жорстких магнітних дисках, диски для лазерних систем зчитування, флеш-накопичувачі, картки пам’яті), комп’ютер загалом, його окремі блоки та пристрої, комп’ютерні комплекси, програмні продукти, супутникові ресивери тощо.

До основних завдань експертизи комп’ютерної техніки та програмних продуктів належать:

- установлення робочого стану комп’ютерно-технічних засобів;
- установлення обставин, пов’язаних із використанням комп’ютерно-технічних засобів, інформації та програмного забезпечення;
- виявлення інформації та програмного забезпечення, що містяться на комп’ютерних носіях;
- установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Орієнтовний перелік вирішуваних питань експертизи комп’ютерної техніки та програмних продуктів:

- чи містить наданий на експертизу супутниковий ресивер налаштування на цифрові теле- та радіоканали, які присутні у вигляді списків та налаштувань на різні супутники Hotbird, Amos тощо?

- яку операційну систему використовує наданий на експертизу ресивер?
- чи дозволяє ресивер перегляд закодованих каналів? Якщо так, то яка система та які ключі застосовуються при цьому?
- чи є можливість застосування кардшарингу на наданому на експертизу ресивері, якщо так, то чи використовувалася вона на наданому на дослідженні ресивері та які програми використовувалися для цього?
- чи міститься на цьому носії інформація стосовно медійного контенту й у якому вигляді?
- чи містить носій досліджуваного комп'ютера інформацію про певні дії користувача щодо розповсюдження медійного контенту?
- які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію щодо медійного контенту?
- чи містить накопичувач інформації досліджуваного комп'ютера певне програмне забезпечення, спрямоване на розповсюдження медійного контенту?
- які функціональні несправності має це комп'ютерне обладнання або його окремі складові та пристрої й як ці несправності впливають розповсюдження медійного контенту?
- чи можливе розповсюдження медійного контенту за допомогою цього програмного продукту?
- чи має об'єкт, що досліджується, ознаки передачі (програми) організації мовлення? Якщо так, то які саме ознаки передачі (програми) організації мовлення притаманні об'єкту, що досліджується?
- чи мало місце повне або часткове використання програми (передачі) організації мовлення (назва) у процесі діяльності особи (назва юридичної особи або прізвище, ім'я, по батькові фізичної особи)?
- який розмір матеріальної шкоди завдано автору (правовласнику) об'єкта права інтелектуальної власності унаслідок дій особи (назва юридичної особи або прізвище, ім'я, по батькові фізичної особи)?

Серед комп'ютерно-технічних експертиз можна виокремити: апаратно-комп'ютерну експертизу; програмно-комп'ютерну

експертизу; інформаційно-комп'ютерну експертизу (даних) та комп'ютерно-мережеву експертизу для дослідження фактів і обставин, пов'язаних із використанням мережевих і телекомунікаційних технологій.

Таким чином, в ході дослідження ми визначили орієнтовний перелік питань, що слід ставити на вирішення спеціальних експертиз, зокрема експертизи об'єктів інтелектуальної власності та експертизи комп'ютерної техніки та програмних продуктів.

Використання інформаційних технологій для визначення місцезнаходження об'єкта

Лепеха Олег Миколайович,

керівник Поліського управління кіберполіції Департаменту кіберполіції Національної поліції України, кандидат юридичних наук

Кондратюк Олександр Володимирович,

професор кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Для оперативного пошуку фактичних даних шляхом моніторингу телекомунікаційних мереж необхідне застосування спеціальних знань у сфері комп'ютерних систем і інформаційних технологій. Силами Департаменту кіберполіції хоча і активізувалася розробка спеціального програмного забезпечення, що дозволяє автоматично визначати наявність ознак протиправної діяльності в завантажених контентах, проте наразі такі програми працюють в тестовому режимі, а виявлення оперативно значущої інформації відбувається людським ресурсом в ручному режимі. Частина зловмисників вважає, що дистанційне спілкування через телекомунікаційні системи гарантує злочинній діяльності конфіденційність, а відтак і уникнення покарання. Сьогодні існує значна кількість способів ідентифікації та локалізації підключеного до мережі Інтернет комп'ютерного обладнання – від складних, до простих способів.

Залежно від типу телекомунікаційної мережі визначення місця знаходження терміналу абонента спостереження поділяється на: географічне місцезнаходження (ідентифікатор країни, міста або оператора телекомунікації, зони приймання для мереж рухомого зв'язку тощо); фізичне місцезнаходження (номер у мережі фіксованого телефонного зв'язку, доступ до якої здійснюється із застосуванням стаціонарного кінцевого обладнання тощо); логічне місцезнаходження (IP-адреси для мереж передачі даних, єдиний UPT-номер для універсального персонального зв'язку). Встановлені у провайдерів телекомунікаційні засоби управління системою перехоплення мають здійснювати наведені визначення особи, щодо якої здійснюється перехоплення телекомунікації (абонента спостереження), у випадках успішної або неуспішної спроби встановлення сеансу зв'язку для вихідного виклику від абонента спостереження та успішної спроби встановлення зв'язку для вхідного виклику до абонента спостереження; обміну службовими повідомленнями між терміналом та обладнанням телекомунікаційної мережі; надання послуги, що асоціюється з місцезнаходженням абонента спостереження; передання спеціального запиту від засобів управління системою перехоплення щодо визначення місцезнаходження абонента спостереження. Враховуючи, що оперативний пошук − це ініціативна активна та самостійна діяльність оперативника (хоча не заборонено залучати спецагентів чи фахівців-спеціалістів у певній галузі), охарактеризуємо найпростіші алгоритми ідентифікації обладнання (комп'ютера), з якого здійснено вихід в мережу Інтернет. З'єднання між комп'ютерами в мережі Інтернет відбувається за протоколом TCP/IP. Кожен комп'ютер у мережі TCP/IP має адреси трьох рівнів: локальну адресу сайту, що визначається технологією, за допомогою якої побудована окрема мережа, в яку входить цей вузол. Для вузлів, що входять в локальні мережі – це MAC-адреса мережного адаптера або порту маршрутизатора, наприклад, 11–A0–17–3D–BC–01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, оскільки управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти – ідентифікатор фірми виробника, а

молодші 3 байти призначаються унікальним способом самим виробником. Для вузлів, що входять в глобальні мережі, такі як X.25 або frame relay, локальна адреса призначається адміністратором глобальної мережі; IP-адреса, що складається з 4 байт (приміром – 109.22.18.101). Ця адреса використовується на мережевому рівні. Він призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі та номера вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Network Information Center, NIC), якщо мережа повинна працювати як складова Internet. Зазвичай провайдери послуг Internet отримують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами; символьний ідентифікатор-ім'я, наприклад, SERV5.IBM.COM. Ця електронна адреса призначається адміністратором і складається з декількох частин, наприклад, імені ЕОМ, імені організації, імені домену. Така адреса, означена також DNS-ім'ям, використовується на прикладному рівні (в протоколах FTP або telnet). Знаючи IP адресу комп'ютера, можливо встановити особу користувача комп'ютера, звернувшись із запитом до провайдера, у якого цей IP зареєстрований. Існує кілька способів визначити IP адресу. Найпростіший спосіб − це передання файлу. Під час з'єднання між двома комп'ютерами, і поки йде передача файлу, можна встановити IP. При використанні для передання файлу ICQ, зовнішній IP відображається автоматично, але видно його тільки в тому разі, коли файл вхідний. Якщо ж файл вихідний необхідно: відкривши командний рядок (Пуск – виконати – cmd – enter), прописуємо команду netstat – enter. Далі потрібно запропонувати передати файл-приманку потенційному зловмиснику. Після того, як почалася передача файлу, необхідно натиснути в командному рядку клавішу enter і IP зловмисника автоматично визначиться в командному рядку. Також можна використовувати спеціальну програму – «сніффер», надіславши відповідне посилання-пастку в відповідний чат, який є полем оперативного пошуку (відпрацювання), написавши відповідний супровідний текст, зміст якого викликає підвищену зацікавленість у відвідувачів (користувачів)

чату. Зацікавленому користувачу, який перебуває в активному пошуку, важко стриматися, щоб не натиснути на таке «цікаве» посилання. Його також можна помістити на попередньо створену підрозділом кіберполіції «власну» сторінку-пастку, помітивши, що саме вона є вашим (оперативника) особистим сайтом, і таким способом забезпечити можливість моніторингу злочинних намірів. Он-лайн «сніффер» або http web sniffer (eng) – це спеціальна програма на Perl або PHP, яка відкладає в спеціальний файл на сервері (лог сніффер) інформацію про користувача, а саме: його IP адресу, час відвідування сторінки-сніффер, а також адресу сторінки, з якої користувач зробив перехід на сніффер. Користувачем у цьому разі є будь-який користувач CGI скриптів, таких як форум, блог, гостьова книга або соціальна мережа (Vkontakte, Odnoklassniki, Facebook, агент Mail.ru), а також ICQ, QIP. Зміст дій оперативника полягає в тому, що йому необхідно передати користувачеві посилання на «сніффер», зацікавивши його так, щоб він обов'язково перейшов за посиланням, після чого в балці «сніффер» відобразиться очікувана IP адреса. Наприклад, онлайн-сніффер http://sniffs.narod.ru/aneksniff/index.html. Посилання ми відправляємо злочинцю – http://www1.hut.ru/ testi.shtml?Your_ID; замість Your_ID прописуємо на латиниці будь-яке слово, яке вам добре запам'ятовується і зацікавить, але водночас є нейтральним. Самі за посиланням не переходимо. Перейшовши за посиланням, зловмисник побачить сторінку, а оперативник бачить IP або відразу стежить за цим в логах (лог сніффера- http://www1.hut.ru/ aneksniff/testisnf.txt). Оперативник переходить за цим посиланням і шукає за тим самим ключовим словом, яке було ним же задано на початку, IP, який необхідно обов'язково відразу скопіювати. Після цього можна встановити, у якій країні, регіоні, місті, знаходиться обладнання (комп'ютер) зловмисника, а також довідатися, яким провайдером надаються послуги виходу в Інтернет цьому користувачеві. Для цього існує спеціальний сервіс, Whois. Також існує безліч сайтів, що надають послуги Whois, але набагато зручніше використовувати спеціальні програми, такі як «Magic Net Trace», http://softsearch.ru/ programs/159-393-magic-nettrace-download.shtml. Згадані програми видають більш повну інформацію про запитувану IP-адресу і

одночасно виконують трасування з'єднання, що дає змогу дізнатися, через скільки і які саме вузли (сервера) проходить з'єднання. Часто трапляються випадки, коли IP адресу визначити неможливо через те, що користувач використовує захищене з'єднання на зразок проксі або VPN (спеціальні сервіси, що дозволяють відвідувати мережу або сайти анонімно). У такому разі оперативник отримує лише IP проксі-сервера або VPN-сервера і подальше отримання інформації стає неможливим, але іноді програми трасування пробивають проксі. Тобто, якщо в балках трасування останній IP проксі-сервера, то можна спробувати піднятися по балці трохи вище, на 1−2 IP-адреси, і подивитися, яка інформація вказана про них. Інколи вдається отримати реальний IP користувача. Якщо ж результат негативний, то можна спробувати встановити IP за допомогою прямого передання файлу, оскільки дія проксі та VPN поширюється виключно на браузер.

Розслідування комп'ютерних злочинів

Мирошниченко Володимир Олексійович,

доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

Бакало В.О.,

здобувач ступеня бакалавра факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

На сьогоднішній день інформатизація суспільства активно вторгається в усі сфери нашого життя. Усі найважливіші функції, так чи інакше, здійснюються з використанням комп'ютерів, автоматизованих систем та комп'ютерних мереж. Завдяки динамічному розвитку комп'ютерних систем з'являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних злочинів з використанням інформаційних технологій. Все частіше і частіше роль власності змінюється, особливу роль відіграє так звана інформаційна власність. Це пов'язано з тим, що світова спільнота вступила в

нову епоху – інформаційного суспільства, в якій життєдіяльність людства певною мірою залежить від телекомунікаційних технологій, що використовуються практично в усіх сферах діяльності людини (енергетика, водопостачання, фінанси, торгівля, наука, освіта тощо) [1]. Всі ці засоби дозволяють передавати та отримувати інформацію на досить значній відстані, що насамперед є досить зручним для нас. У зв'язку з постійною модернізацією технологічних процесів все частіше виникають та вчиняються суспільно небезпечні діяння, що заподіюють шкоду нормальній роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Розвиток та розширення сфери застосування інформаційних технологій обумовили в тому числі істотні трансформації правового регулювання.

Сферою широкого застосування комп'ютерної техніки є банківська діяльність та платіжні системи, тому більшість злочинів проти власності так чи інакше пов'язана зі злочинами в сфері використання комп'ютерної техніки. Йдеться про: «злам» електронної пошти з метою отримання реквізитів доступу до банківських рахунків, блокування інтернет ресурсу з метою вимагання, використання «скімерів» (спеціальних пристроїв, що приховано встановлюється зловмисниками на банкомати) для отримання реквізитів платіжних карток або розробка та використання шкідливих програмних засобів, призначених для незаконного віддаленого доступу до бухгалтерського програмного забезпечення підприємств, установ чи організацій, збут клієнтських баз даних скомпрометованих фінансових систем, введення банківськими працівниками до автоматизованих систем банківського обслуговування неправдивих відомостей щодо здійснених фінансових операцій, невжиття необхідних технічних заходів інформаційної безпеки, що призвело до компрометації автоматизованої системи фінансової установи тощо [1].

З розвитком технічного прогресу та еволюцією людства з'являються нові, раніше невідомі злочини та способи їх

вчинення. Так, з появою та розвитком Інтернету виникли нові форми вчинення доведення до самогубства, що поширюються у світі разом із зростанням кількості постійних користувачів цієї всесвітньої мережі. Значних обертів набрали самогубства підлітків, яких спонукали до цього у так званих «групах смерті» у соцмережах. Вперше про «групи смерті» на кшталт спільнот «Синий кит», «Тихий дом», «Разбуди меня в 4:20» заговорили ще у травні 2016 року. За даними Національної поліції України, тільки в одній такій спільноті було виявлено більше двох сотень активних користувачів з України.

Одним із способів вчинення комп'ютерного злочину є використання із злочинною метою шкідливих програмних продуктів. Термін «злочини, що здійснюються з використанням комп'ютерних технологій», охоплює всі дії, що передбачають використання досягнень цих технологій і ті, які зазіхають на комп'ютерну інформацію [2].

Сліди злочинів у сфері використання інформаційних технологій утворюються за результатами зовнішнього доступу до інформації, що виключає певні зміни, пов'язані з подією злочину. Такими змінами можуть бути сліди знищення, модифікації, копіювання інформації, блокування інформаційної системи. Сліди змін залишаються в машинних носіях і відображають зміни в інформації, яка в них зберігається [2].

Питанням дослідження проблем використання спеціальних знань у боротьбі зі злочинами у сфері використання інформаційних технологій учені-криміналісти (О.Р Росинська, В.О. Мещеряков, В.Б. Вехов , В.О. Голубєв, І.Ю. Михайлов , А.І. Усов, В.Ю. Шепітько та ін.) приділяють значну увагу останні два десятиліття, однак у зв'язку зі стрімким розвитком інформаційних технологій і швидкими змінами поколінь комп'ютерної техніки та програмного забезпечення існує нагальна потреба в подальшому дослідженні цього напряму для уточнення окремих наукових положень, зокрема - виокремлення специфічних слідів комп'ютерних злочинів та розроблення способів їх виявлення з використанням спеціальних знань.

Комп'ютерна інформація, як джерело доказу є новим об'єктом криміналістичного дослідження, а тому її аналіз потребує використання спеціальних знань. Вивчення кримінальних проваджень з розслідування комп'ютерних злочинів показав, що до проведення огляду, допиту, залучення експерта та ін. слідчих дій у більшості випадків залучається спеціаліст, який під час слідчої дії надає допомогу слідчому, роз'яснюючи останньому питання, що містять відомості технічного характеру. На сьогодні з використанням спеціальних знань розроблена значна кількість ефективних сучасних засобів пошуку (відновлення) знищеної електронної інформації. Практика показує, що якнайповніше доказову базу можна сформувати, залучаючи фахівців у галузі інформаційних технологій, які постійно використовують у своїй повсякденній діяльності новітні програмні засоби. Зокрема, судовими експертами України на сьогодні використовуються такі сучасні програмні продукти, як X-Ways Forensics, EnCase Forensics, FTK, AccessData Forensic Toolkit, Forensic Disk Decryptor, MailPro, FileLister та ін. Сліди злочинів у сфері використання інформаційних технологій утворюються за результатами зовнішнього доступу до комп'ютерної інформації, що викликає певні зміни, пов'язані з подією злочину. Такими змінами можуть бути сліди знищення, модифікації, копіювання інформації, блокування інформаційної системи. Сліди змін залишаються на машинних носіях інформації і відображають зміни в інформації, яка в них зберігається (порівняно з попереднім станом). Часто злочинці здійснюють модифікації баз даних, програм, текстових файлів, що містяться на стаціонарних і змінних носіях інформації, призначених для багаторазового її перезапису. Інформація може зберегти сліди її часткового знищення або модифікації (видалення з каталогів імен файлів, видалення або додавання окремих записів, фізичного руйнування або розмагнічування носіїв тощо). Інформаційними слідами є також результати роботи антивірусних і тестових програм. Такі сліди можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду тощо [3].

1. Матеріали Міжнародної науково-практичної конференції «Політика в сфері боротьби зі злочинністю» з нагоди відзначення 25-річчя навчально-наукового юридичного інституту, - Івано-Франківськ, 2017.-255с) стор.147
2. Оптимізація розслідування злочинів з використанням потенціалу комп'ютерних технологій [Електронний ресурс] / Д. В. Бірюков // Південноукраїнський правничий часопис. – 2016. – № 2. – С. 140-143. – Режим доступу: http://nbuv.gov.ua/UJRN/ Pupch_2016_2_40
3. Використання спеціальних знань у боротьбі з комп'ютерною злочинністю [Електронний ресурс] / Г. К. Авдєєва // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2016. – Вип. 1. – С. 268-277. – Режим доступу: http://nbuv.gov.ua/UJRN/Vlduvs_2016_1_30

Аналіз актуальності інформаційних технологій у правоохоронній діяльності

Пахомов Владислав Борисович,

здобувач ступеня бакалавра ХННІ ДВНЗ «Університет банківської справи»

Кавун Сергій Віталійович,

завідувач кафедри інформаційних технологій ХННІ ДВНЗ «Університет банківської справи», доктор економічних наук, Ph.D., професор

В сучасних умовах особливе значення набуває актуальність інформаційних технологій в правоохоронній діяльності, з їх допомогою працівники правоохоронних органів можуть як здобувати більш високі навики для справ, так і вдосконалювати та убезпечити виконання своєї роботи [3].

З тим що інформаційні технології «доторкнулись» до правоохоронних органів сперечатись марно, адже чи не найвагомішим доказом є нещодавно створений Департамент кіберполіції Національної поліції України, який направлений на боротьбу з кіберзлочинами у сферах використання платіжних

систем, у сфері електронної комерції та господарської діяльності, у сфері інтелектуальної власності та у сфері інформаційної безпеки. Якщо раніше, люди які натрапили на шахрайство в мережі Інтернет знали що вдіяти та обходились лише отриманням гіркого досвіду для себе, то тепер людина може з легкістю звернутись до поліції та бути впевненою, що злочинці будуть покарані, а кошти повернені власнику [1].

Ще однією інновацією зв'язаною з інформаційними технологіями є боді-камера, яку тепер має кожен поліцейський. Камера знаходиться на грудях та фіксує усе що відбувається в момент виклику працівників правоохоронних органів [2].

З вище перерахованих аспектів видно, що інформаційні технології мають попит у правоохоронній діяльності, але це далеко не все чим можна убезпечити та поліпшити роботу правоохоронних органів в нашій країні.

В роботі проведено аналіз як актуальність інформаційних технологій взагалі, так і актуальність різних засобів інформаційних технологій та безумовно актуальність інформаційних технологій у правоохоронній діяльності. Задіяно дев'ять країн за допомогою яких визначається актуальність інформаційних технологій, законодавчих актів, правоохоронних органів і т. д. До списку цих країн відноситься: Україна, Росія, Білорусь, Польща, Словаччина, Румунія, Молдова, Угорщина та Болгарія. Вище перелічені країні обрані через географічну близькість до нашої країни. На основі запитів мешканців цих країн, було побудовано графіки на яких відображаються данні за період – 10 років, дозволяючи зробити висновки якою є актуальність інформаційних технологій у тій чи інший галузі.

Таким чином проведений аналіз дозволяє зробити висновок, що розвиток інформаційних технологій у сфері правоохоронної діяльності характеризується стійкими позитивними трендами: розробляється та впроваджується все більше і більше інформаційних систем та засобів, для більшої зручності використання, підвищення функціоналу, та швидкості роботи правоохоронних органів.

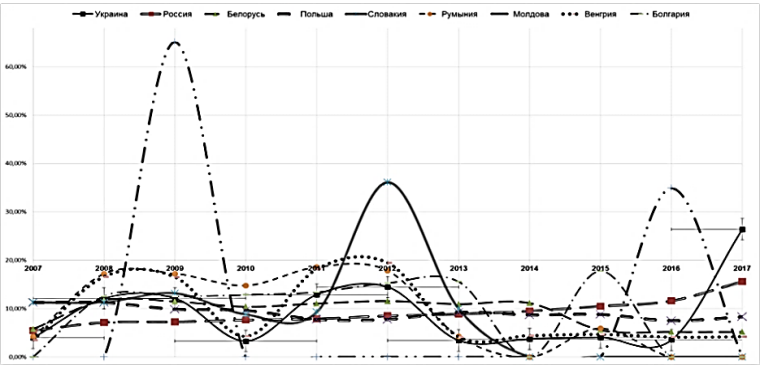


Рис. 1. Кількість посилань на тег «Законодавчі акти»

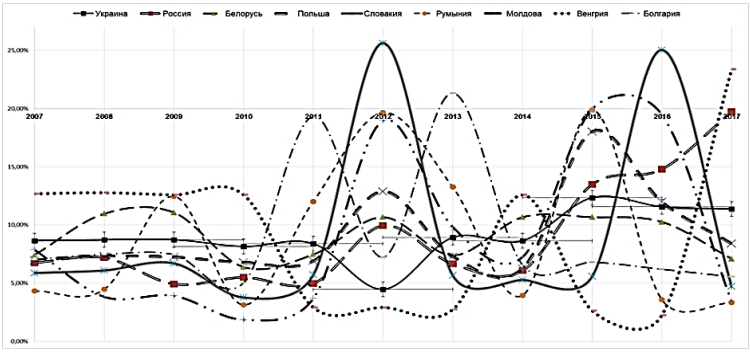


Рис. 2. Кількість посилань на тег «Анонімність»

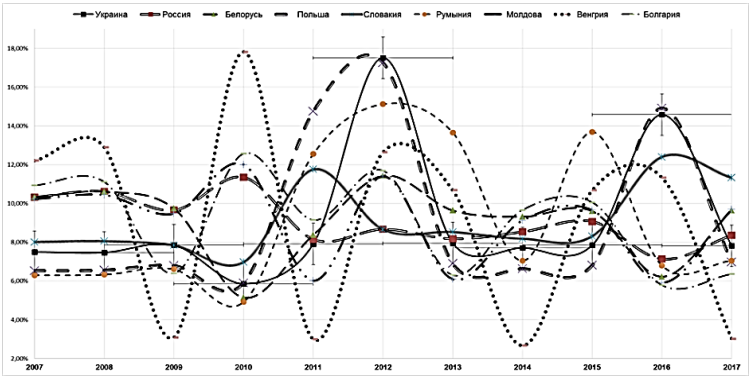


Рис. 3. Кількість посилань на тег «VPN»

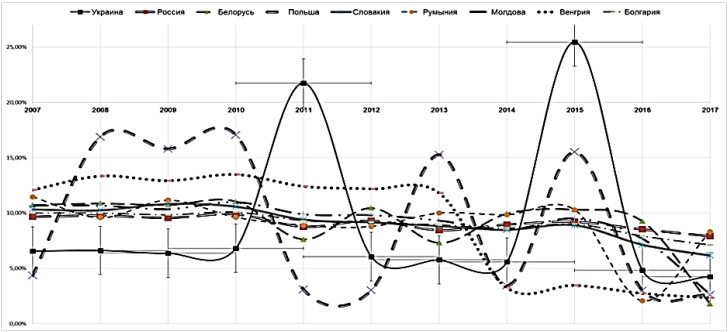


Рис. 4. Кількість посилань на тег «Правоохоронні органи»

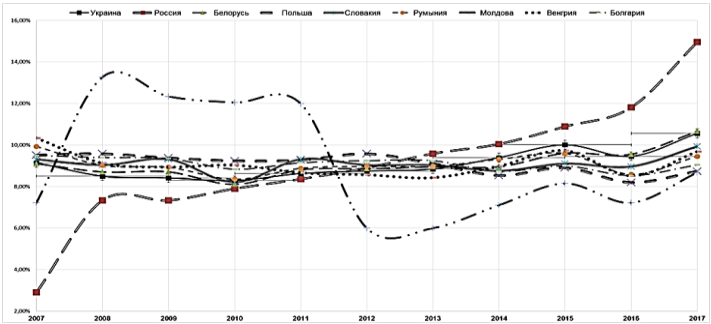


Рис. 5. Кількість посилань на тег «Інформаційні технології»

Ці тенденції будуть зберігатись в силу розвинення рівня злочинності, та силу необхідності підвищення якості роботи правоохоронних органів.

---

1. В Украине будет создана киберполиция, – Аваков. ИНФОГРАФИКА [Електронний ресурс] // ЦЕНЗОР.НЕТ. – 2015. – Режим доступу до ресурсу: https://censor.net.ua/photo_news/355818/v_ukraine_budet_sozdana_kiberpolitsiya_avakov_infografika.
2. Наказ Департаменту патрульної поліції НПУ від 03.02.2016 року № 100 [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.slideshare.net/krapzen/03022016-100.
3. Інформаційні технології в діяльності [Електронний ресурс] – Режим доступу до ресурсу: http://bo0k.net/index.php?p=achapter&bid=8692&chapter=1.

Проблеми інформаційно забезпечення діяльності підрозділів карного розшуку в процесі протидії втягненню неповнолітніх у злочинну діяльність

Поляк Святослав Петрович,

ад'юнкт кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ

Статистичні дані щодо втягнення неповнолітніх у злочинну діяльність свідчать про позитивні тенденції щодо зниження рівня цих кримінальних правопорушень, а також про виникнення нових факторів, що висвітлюють низку проблем у діяльності поліції щодо протидії цьому злочину. Так у 2013 році в Єдиному реєстрі досудових розслідувань було обліковано 783 факти втягнення неповнолітніх у злочинну діяльність, у 2014 зареєстровано 615 таких кримінальних правопорушень, у 2015 – 524, 2016 – 322, а в період до жовтня 2017 – 246 [1]. На нашу думку, подвоєнням результативності у процесі протидії цій категорії злочинів має стати належне інформаційне забезпечення підрозділів карного розшуку, а також створення спеціально уповноважених підрозділів чи наділення окремими повноваженнями конкретних співробітників для здійснення ОРД щодо вказаних кримінальних правопорушень, створення відповідних баз даних.

Сьогодні інформація є важливим ресурсом поряд із цінностями та економічними можливостями. Боротьба за доступ до ретранслятора інформації здійснюється непомітно проте цілеспрямовано. Інформаційні шпигунські війни та брудні технології ставлять під питання існування інформаційної безпеки та незалежності як окремих держав так і людства вцілому. Все це підтверджує знаменитий вислів «хто володіє інформацією – той володіє світом», озвучений Натаном Ротшильдом більше двох століть тому.

О.М. Бандурка зазначає, що інформаційне забезпечення є серцевиною оперативно-розшукової діяльності [2, с. 282].

Саме тому інформаційне забезпечення правоохоронної діяльності, в тому числі оперативно-розшукової, є запорукою недопущення вчинення злочину. Інформаційний дефіцит породжує невизначеність в діяльності оперативного підрозділу і впливає на швидкість та якість прийняття як управлінсько-організаційних так і процесуальних рішень щодо протидії злочинності.

Проблемами інформаційного забезпечення оперативних підрозділів займалися видатні науковці та практики юридичної сфери такі як О.М. Бандурка, Е.О. Дідоренко, В.П. Захаров, А.В. Мовчан, Д.Й. Никифорчук, В.Л. Ортинський, М.А. Погорецький, В.В. Шендрик, І.Р. Шинкаренко, В.Г. Хахановський.

Наступними болючими питаннями є збирання, систематизація, аналіз, зберігання та охорона оперативно-розшукової інформації за конкретними категоріями злочинів, в тому числі і щодо досліджуваного нами.

Виникнення нових джерел отримання інформації дітьми, наявність безособового електронного спілкування між ними та іншими особами, наявність в підлітків електронних засобів здобуття інформації, з однієї сторони робить їх «мішенями» для зловживання і використання злочинцями задля реалізації своїх протиправних намірів, а з іншої повинно надавати можливість оперативним співробітникам контролювати зміст такої інформації, здійснювати моніторинг та пошук оперативної інформації, яка є підставою для здійснення ОРД.

Вдале визначення оперативно-розшукової інформації запропонував С.С. Овчинський. Він вважає, що оперативно-розшукова інформація містить знання про явища, які свідчать про злочинну діяльність конкретних осіб і розкривають не тільки механізм злочинів, а й механізм виникнення інформації про них [3, с. 17–18].

Так як підрозділи карного розшуку щодо виявлення та документування фактів втягнення неповнолітніх у злочинну діяльність мають право здійснювати оперативно-розшукову діяльність, то у ст. 8 Закону України «Про оперативно-розшукову діяльність» вони наділені правом створювати і

застосовувати автоматизовані інформаційні системи. Відповідно, законодавець натякає, що відомості, які накопичуються в таких системах повинні бути спрямовані на якісне, об'єктивне та швидке досудове розслідування та судовий розгляд, позаяк працівники карного розшуку здійснюють оперативне супроводження кримінального провадження аж до успішного винесення рішення судом та застосування покарання до винної особи. Тому, підрозділи, що використовують автоматизовані інформаційні системи в оперативно-розшуковій діяльності, повинні забезпечити можливість видавати дані про особу на запит органів досудового розслідування, прокуратури, суду. В місцях зберігання інформації повинна бути гарантована її достовірність та надійність охорони [4].

І.П. Козаченко розкриває три основні методи інформаційного забезпечення ОРД: 1) інформаційно-аналітичний метод оцінки оперативної обстановки; 2) інформаційно-аналітичний метод отримання, обробки відомостей про особу, події та факти, що становлять оперативний інтерес; 3) метод пошуку та використання відомостей, що знаходяться в інформаційно-пошукових системах [5, с. 26].

Баз даних, як загального так і спеціального характеру, щодо накопичення інформації про факти втягнення неповнолітніх у злочинну діяльність, включаючи агентурну інформацію, осіб, які залучають дітей до даної діяльності, характеру та ступеню взаємозв'язків між такими особами, їх правові та процесуальні статуси, соціальні ролі, економічні можливості, психофізіоло–гічні характеристики, біометричні дані та низку інших фактів немає. Бази даних ІІПС, що ведуться різними підрозділами поліції містять подекуди розрізнену, загального характеру інформацію, класифіковану за обмеженими параметрами.

Відповідно до Закону України «Про Національну поліцію» поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, зокрема бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону [6].

Крім того, спостерігається низький рівень негласного співробітництва, щодо отримання оперативно-розшуковою інформації з соціальних кіл неповнолітніх. В дечому тут дається взнаки розформування підрозділів кримінальної міліції у справах неповнолітніх та налагодження нових контактів у закладах освіти і з такою категорією осіб. Та і саме законодавство поки обмежує можливості конфіденційного співробітництва з неповнолітніми. По друге, спостерігається низький рівень взаємодії оперативного співробітника з іншими підрозділами, зокрема підрозділами патрульної поліції та ювенальної превенції. Це зумовлено також реформацією підрозділів та в деякій мірі нерозумінням спільної цілі діяльності та специфіки діяльності оперативного підрозділу. Все це зменшує шанси оперативника на отримання інформації про факти втягнення неповнолітніх у злочинну діяльність.

Інформаційне забезпечення в цій сфері є фундаментом для планування, прогнозування і здійснення оперативно-розшукової діяльності, ухвалення оптимальних управлінських рішень, контролю за їх виконанням. Автоматизовані інформаційні системи поряд з інформацією отриманою від конфіденційного співробітництва є найважливішими елементами організації оперативно-розшукової діяльності підрозділів карного розшуку поліції у протидії втягненню неповнолітніх у злочинну діяльність.

Тому, за необхідне стоїть питання перегляду принципів та методів негласної роботи в частині конфіденційного співробітництва, що стосується отримання важливої оперативної інформації для протидії розглядуваному злочину, а також створення окремих баз даних ІІПС за конкретними видами злочинів, в тому числі і щодо втягнення неповнолітніх у злочинну діяльність.

---

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua/ua/stst2011.html?dir_id=106782&libid=100820.
2. Бандурка О.М. Оперативно-розшукова діяльність: підручник / О.М. Бандурка. – Харків: НАВС, 2002. – 334 с.

3. Оперативно-розыскная информация / под ред. А.С. Овчинского и В.С. Овчинского. – М.: ИНФРА, 2000. – 367 с .
4. Про оперативно-розшукову діяльність: закон України від 18.02.1992 р., № 2135–XII // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2135-12/page (дата звернення: 06.12.2017).
5. Козаченко І.П. Правові, морально-етичні та організаційні основи оперативно-розшукової діяльності / І.П. Козаченко, В.Л. Регульський. – Львів: ЛІВС, 1999. – 219 с.
6. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 06.12.2017).

Правовий захист інформації

Проць Іванна Миколаївна,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук

Кузьмочка Юлія Володимирівна,

здобувач ступеня бакалавра факультету № 6 Львівського державного університету внутрішніх справ

Становище України як правової держави, інтеграція в її європейський простір реформування економіки та оборони викликало необхідність створення, тільки нової системи захисту правової інформації та законодавчого регулювання інформаційних відносин. Правова безпека, на сьогодні є одним із загальних понять. На даний час у чинному законодавстві України відбувається зближення антроцентричного та техноцентричного понять визначення інформації, що позитивно впливає на правове регулювання інформаційних відносин у суспільстві. Також на сьогоднішній час інформація перетворилася на потужний ресурс, що є великою цінністю, ніж фінансові, трудові, природні та інші ресурси.

На державному рівні правовий захист інформації передбачає, організацію ефективної нормативчої правоохоронної та правозахисної діяльності. Тому дуже часто правовий напрямок захисту інформації на рівні держави об’єднується з організаційним напрямом [1, с. 223].

Існує багато класифікацій правової інформації, але основними для правового регулювання відносин є класифікація за змістом і за режимом доступу до неї.

До публічної інформації відноситься інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чиним законодавством. У зв’язку з тим, що розвиваються процеси інформатизації та комп’ютеризації суспільства захист інформації є загальнодержавною проблемою, яка потребує суспільного вирішення. Система законодавчих актів розроблена на базі нормативних та організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням з боку правоохоронних органів [2, с. 22].

Під інформаційно-правовою безпекою України, мається на увазі, захист національних інтересів в цій сфері, який визначається певною кількістю збалансованих інтересів особи, суспільства та держави. Конституція України, що стала гарантом побудови правової держави не могла не затвердити інформаційно-правовий захист в суспільстві. Тому ряд статей (ст. 17, 32, 34) забезпечують захист інформатизації в Україні [3, с. 152].

Інформаційно правова інформація має документальний і офіційний характер. Для неї характерна вся сукупність нормативно-правових актів які ґрунтуються на основі Конституції України.

Правова інформація – дані(відомості) про події, предмети осіб явища, які відбуваються у правовій сфері, що містяться в правових джерелах і використовуються для вирішення завдань правотворчості, у правозастосовчій та правоохоронній діяльності, захисту прав і свобод громадянина [4 с.189].

Визначними є положення чинного інформаційно-правового законодавства. Закон України «Про інформацію» прийнятий у жовтні 1992 року заклав правові основи інформаційно- правової діяльності, проте він не завжди виконується на теренах України в достатній мірі. В Законі чітко прописано, що створення правової основи захисту інформації це забезпечення інформаційно-правового статусу.

Отже, велика кількість законів і нормативно правових актів у сфері інформаційно-правових відносин ускладнює пошук їх, аналіз та узгодження для практичного застосування.

Також, інколи спостерігаються розбіжності у розумінні структури складу системи законодавства у сфері інформаційних підходів до їх формування.

На нашу думку, потрібно вдосконалити правові акти суспільних інформаційно-правових відносин тому, що є неузгодженість концептуальна з прийняттям рішень, що призводять до правового хаосу. Національне інформаційне законодавство повинно стати на шлях систематизації через кодифікацію, тобто створення системоутворюючого Кодексу.

---

1. Стоцький А.Б., Тимошенко О.І, Туз А.М. Організаційно-правові основи захисту інформації з обмеженим доступом: [навчальний посібник] / А.Б. Стоцький, О.І. Тимошенко, А.М. Туз та ін. за заг. ред. В.С. Сідака. – К: Вид-во європейського університету, 2006. – 223 с.
2. Басков В.Ю. Адміністративно-правовий режим інформації з обмеженим доступом: автореф. дис. на здобуття наук ступ. канд. юрид. наук: спец.12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В.Ю. Баскаков. – К., 2012.– 22 с.
3. Таликін Є.А. Інформаційне право. Тексти лекцій (для студентів денного та заочного відділення спеціальності «Правознавство») /Укладач: Є.А. Таликін. – Луганськ: вид-во СНУ ім. В. Даля, – 2013. – с. 152–156.
4. Шемшученко Ю.С. Юридична енциклопедія / Ю. С. Шемшученко (голова редкол.) та ін. – К: Українська енциклопедія, 1998.-Т1-189 с.

Історичні етапи становлення інформаційної діяльності Національної поліції України

Сеник Святослав Володимирович,

науковий співробітник відділу організації наукової роботи Львівського державного університету внутрішніх справ, здобувач кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ

У повсякденній діяльності правоохоронних органів інформація, її обробка та аналіз відіграє важливу роль, оскільки розкриття, попередження та профілактика злочинів включає її постійний обіг. Інформаційна діяльність у правоохоронних органах є широкою та багатогранною сферою здійснення ними своїх функцій, головною метою якої є отримання максимально корисного результату від інформації для правильної оцінки ситуації, передбачення перспективи її розвитку, що у кінцевому випадку веде до прийняття правильних управлінських рішень.

Загальний генезис становлення та розвитку інформаційної діяльності правоохоронних органів на території сучасної України становить близько триста років. У 1721 році Петром І створено регулярну поліцію, а у 1811 році створене Міністерство поліції та третє відділення у його складі, яке займалось збором інформації щодо вчинених злочинів та правопорушень [1]. У 1826 році організовано третє відділення на базі Особливої канцелярії, завданням якого став збір будь-якої інформації, що стосувалась діяльності поліції, а саме: статистичні відомості, факти про вчинені правопорушення, осіб які перебували під наглядом поліції тощо. У цей же період створено три архіви, два із яких стали таємними. Згодом почали формувати картотеки з фотографіями злочинців. Загалом, історію становлення інформаційно-аналітичної діяльності в органах правопорядку можна поділити на п’ять етапів.

Перший етап (дореволюційний) – з початку XVIII ст. до 1917 р. – це період, коли з’явилася перша систематизація знань про

боротьбу зі злочинністю, а саме перші системи криміналістичної реєстрації за антропологічними даними, фотографіями, відбитками пальців тощо. На початку XX ст. при МВС Росії створено Центральне реєстраційне бюро та розшукове відділення, до функцій якого належала реєстрація злочинців, підозрюваних у вчинені злочинів. Саме у цей період відбулася централізація обліків та створення реєстраційної мережі, що стало основою сучасної інформаційно-аналітичної роботи.

Другий період (ранній Радянський) (1917 р. до середини 1950-х рр.) –розпочинається формування правоохоронних органів Радянського Союзу. Характерною рисою цього часу є те, що після 1917 р. обліки поліції були знищені, а це суттєво ускладнило боротьбу зі злочинністю, яка на той час почала сягати значних масштабів. У зв'язку із цим, у 1918 році створено обліково-реєстраційні служби, які почали здійснювали алфавітну та дактилоскопічну реєстрацію злочинців [2, с. 13]. Згодом було створено статистичне бюро яке вивчало стан злочинності та результати розкриття злочинів. Карний розшук став центральним суб'єктом інформаційно-аналітичної роботи до середини 30-х рр. XX ст. У 1938 р. створено Перший спеціальний відділ НКВС як головний інформаційно-аналітичний орган у правоохоронній системі. Після реформи НКВС у на початку 40-х рр. років до складу цього відділу відійшли оперативно-довідкова картотека, архів, алфавітна, дактилоскопічна картотека та картотека з обліку ув'язнених. На базі цього відділу було створено єдиний центр обліку злочинів.

Третій етап (автоматизації інформаційної діяльності) (середина 50-х рр. – початок 90-х рр.). характеризується початком стрімкого розвитку інформаційно-аналітичної роботи завдяки розвитку електронно-обчислювальних систем. У 1970-х рр. вперше створено централізовану систему інформаційних центрів, що зосередили в собі 30 різних картотек, хоча загалом їх було близько 70. У цей же період започатковано основи інформаційно-аналітичного забезпечення органів внутрішніх справ України – Республіканський інформаційний центр МВС

УРСР, основними завданнями якого стало: надання статистичної, оперативно-довідкової, розшукової інформації, збір, обробка, аналіз, зберігання інформації про злочинців, злочини, розшукуваних осіб, втрачених, викрадених речей, ідентифікації зброї тощо. Одними із перших були створені автоматизовані системи «Профілактика – Розшук», «Розшук», «Статистика».

Четвертий етап (інформатизації ОВС України) (початок 90-х – 2015 рр.). Початок даного періоду характеризується створенням незалежної Української держави. У цей час приймаються нові нормативно-правові акти, які у подальшому дали поштовх розвитку інформаційного забезпечення правоохоронних органів, у тому числі органів внутрішніх справ. До таких нормативних документів слід віднести: Конституцію України, Закони України «Про міліцію» [3], «Про інформацію», [4] «Про оперативно-розшукову діяльність», [5] «Про захист інформації в інформаційно-телекомунікаційних системах», [6] «Про державну таємницю» [7] тощо. Характерною рисою даного періоду стало створення міжвідомчих обліків, інтегрованих банків даних, стрімкий розвиток комп'ютерної розвідки та аналітичних технологій, створення комунікаційних та інформаційних мереж.

П'ятий етап (інформаційного забезпечення Національної поліції України. Це період з 2015 року по наш час. Окремо цей період виділяється у зв'язку із створенням Національної поліції України та відокремлення інформаційних підрозділів. Відповідні інформаційні підрозділи створені як у структурі МВС України, так і у структурі Національній поліції [8]. В структурі МВС України інформаційну діяльність здійснює Департамент інформаційних технологій, а в у свою чергу Національна поліція має окремі підрозділи інформаційного забезпечення, такі як: Департамент організаційно-аналітичного забезпечення та оперативного реагування та Департамент інформаційно-аналітичної підтримки.

1. Линдер И. Б. Спецслужби России за 1000 лет Материалы секретных фондов / И. Б. Линдер, С. А.Чуркин – М. : Рипол Класик, 2006. – 736 с.
2. Іщенко О. М. Історія створення інформаційного підрозділу органів внутрішніх справ України / О. М. Іщенко, С. П. Черних, І. А. Аршинов // Від арифмометра до високих технологій. – Запоріжжя: Просвіта, 2012. – С. 11–15.
3. Про міліцію : Закон України // Відомості Верховної Ради УРСР (ВВР). – 1991. – № 4. – ст. 20. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/565-12
4. Про інформацію : Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650){Вводиться в дію Постановою ВР № 2658-XII (2658-12) від 02.10.92 ; ВВР, 1992, № 48, ст. 651.
5. Про оперативно-розшукову діяльність : Закон України // Відомості Верховної Ради України (ВВР). – 1992. – № 22. – ст. 303.
6. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України (ВВР). – 2005. – № 26. – ст. 347.
7. Про державну таємницю : Закон України // Відомості Верховної Ради України (ВВР). – 1994. – № 16. – ст. 93.
8. http://mvs.gov.ua/ua/pages/Struktura_Ministerstva_vnutrishnih_sprav_Ukraini.htm

Сучасні інструментальні засоби кримінального аналізу

Узлов Дмитро Юрійович,

начальник УІАП Головного управління Національної поліції в Харківській області, кандидат технічних наук

Струков Володимир Михайлович,

завідувач кафедри інформаційних технологій Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

Наслідком стрімкого розвитку інформаційних технологій протягом останніх десятиріч є поступовий масовий перехід із сфери матеріальних відносин у віртуальну сферу. Цей процес не

обходить і правоохоронні органи. Зокрема, це постійне щоденне накопичення інформації у базах даних правоохоронних органів. Так навіть на регіональному рівні кількість записів в ІІПС налічує в окремих областях більше десятка мільйонів. Використовувати для обробки таких великих обсягів інформації традиційні пошукові системи (ІІПС та подібні). Крім того, кримінально значима інформація міститься не лише в базах даних правоохоронних органів, а і у відкритих мережах (соціальні мережі та ін.). В таких умовах є абсолютно необхідним застосовувати для обробки доступної інформації більш ефективні наукоємні системи, зокрема, системи, в яких використовуються технології Data Mining, Visual Mining, Web Mining, Text Mining [1, 2]. Аналіз існуючих автоматизованих інструментальних засобів кримінального аналізу свідчить про те, що в Україні відсутні ефективні засоби автоматизованого кримінального аналізу, в світі існують певні аналітичні системи (Palantir, I2, ANACAPA, CRIMEVIEW Server, My Neighborhood Map System, CRIMEDC, Holms2), кожна з яких має свої переваги і недоліки, але жодна з них не охоплює повною мірою рішення задач кримінального пошуку та кримінального дослідження з використанням геоінформаційних засобів в реальному часі. Більшість цих систем пропонують рішення для інформування громадськості та, що принципово важливо, йдеться не про інтеграцію в уже діючі системи, а установку їх як незалежних систем. Найбільш ефективними з перелічених систем є Palantir (США), I2 (фірма IBM), Holms2 (Великобританія). Palantir використовується в ЦРУ, АНБ, ФБР, поліцейських управліннях Нью Йорка, Лос Анджелеса, банку JP Morgan (ціна – від 5 до 100 мільйонів доларів). В I2 дуже обмежено використовуються геоінформаційні технології. Holms2 використовується лише у Великобританії.

В Україні розроблена система кримінального аналізу RICAS, яка ґрунтується на наступних принципових моментах: 1) вивчення особливостей масивів даних, що обробляються, дозволило побудувати спеціальну метрику [2, 3] у просторі багатовимірних об’єктів різнотипних ознак, яка забезпечила можливість застосувати для обробки даних класичні методи

Data Mining (кластерізації і класифікації); 2) система виконана як надбудова (оболонка) існуючої ІІПС ОВС України, і, що принципово важливо, дозволяє при її впровадженні не видаляти стару систему або припиняти її функціонування, а просто і безболісно істотно поліпшувати її функціональність і ефективність; 3) при розробці системи використані ліцензійно чисті інструментальні системи.

Інструментарій системи базується на математичних моделях і методах інтелектуального семантичного аналізу, візуального темпорального аналізу, аналізу поведінкового профілю, аналізу прихованих закономірностей.

Інтелектуальний семантичний аналіз включає в себе потужне ядро по роботі з семантикою. Аналіз неструктурованих даних відбувається в режимі реального часу. Для уніфікації пошукових функцій і побудови поведінкового профілю використовується алгоритм класифікації або «тегування», а також антиципаційний алгоритм.

Семантичне ядро системи дозволяє будувати складні пошукові запити, які включають в себе всілякі динамічні і статичні компоненти – обмеження за часом, методу скоєння злочину, дислокації і тощо. Всі функції виконуються миттєво і дозволяють максимально швидко візуалізувати інформацію і виконувати аналітичну роботу.

Візуальний темпоральний аналіз. Відображення хронології подій, що відбулися, і розмежування в часі дозволяє оперативно виявляти приховані просторово-часові закономірності між різними подіями.

Аналіз поведінкового профілю. Найбільш постійним і точним з точки зору психології злочинця є його поведінковий профіль. Він відображає багато параметрів діяльності злочинця – звичний спосіб вчинення злочину, місця скоєння та інші дрібні залежності, які в сукупності відповідають одному профілю. Наявність тих чи інших поведінкових ознак з певною часткою ймовірності може свідчити про те, що даний суб'єкт може бути причетний до події. З цього принципу формується так званий

груповий поведінковий аналіз. Безумовно, поведінковий профіль злочинця ніяк не може існувати без впливу на інших суб'єктів. Аналіз групового поведінкового профілю дозволяє визначати подільників, спільників без явних зв'язків між ними.

Аналіз прихованих закономірностей. Між особами, яким-небудь чином причетними до правопорушення, об'єктивно існують зв'язки (родинні, за родом професійної діяльності, географічні - по прив'язці до місця проживання, місця відбування покарання і т. п.). Подібні зв'язки існують також між особами і подіями, а також між різними подіями. Такі зв'язки можуть бути явними, опосередкованими і прихованими. Крім того, група пригод, скоєних однією і тією же особою, обов'язково має певні характерні загальні риси, які явно не зафіксовані. Виявлення таких прихованих закономірностей з високою часткою ймовірності завжди може ідентифікувати зв'язок між злочинцем і всіма здійсненими ним злочинами.

Система розроблялася з використанням сучасних технологій у веб-просторі та є мультиплатформною. Її можна використовувати на будь-яких стаціонарних і мобільних пристроях при наявності захищеного каналу зв'язку.

1. Aggarwal C.C. Data Mining. – Cham: Springer Ltd. Publ. Switzerland, 2015. – 734p.
2. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies / C. Westphal. – Boca Raton : CRC Press, 2009. – 426p.
3. Бодянский Е.В., Струков В.М., Узлов Д.Ю. Задача оценки близости многомерных объектов анализа данных // УСиМ. – 2016. – № 6. – С. 67-72.
4. Бодянский Е.В., Струков В.М., Узлов Д.Ю. Обобщенная метрика в задаче анализа многомерных данных с разнотипными признаками // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2017. – Випуск 3(52). – С. 98-101.

Особливості огляду місця події за фактами вчинення злочинів, спосіб вчинення яких пов'язаний з використанням комп'ютерної та телекомунікаційної техніки

Хахановський Валерій Георгієвич,

професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ,
доктор юридичних наук, професор

Широке використання сучасних електронних пристроїв та мережі Інтернет відкрило злочинцям нові можливості для протиправної діяльності. З'явились нові види злочинів, а також нові методи вчинення традиційних злочинів. Саме тому юристи, особливо – правоохоронці повинні бути обізнаними про електроні докази та методи поводження з ними.

Нині майже кожне правопорушення так чи інакше пов'язане з електронним пристроєм, у якого є пам'ять чи програмне забезпечення. Навіть якщо електронний пристрій не був безпосереднім знаряддям злочину, достатньо імовірно, що дії злочинці зафіксовані на камеру відеоспостереження чи телефонний/автомобільний GPS-пристрій. Цифрова експертиза електронних даних стала основним інструментом притягнення злочинців до відповідальності.

Розвиток Інтернет і веб-додатків призвів до того, що докази можуть знаходитись не тільки на персональних комп'ютерних пристроях, а й на веб-сайтах, в соціальних мережах, в електронній пошті та в чаті. З'явились хмарні технології, де додатки і дані зберігаються на сервері, розташованому у невизначеному місці на території іншої держави. Тому нині особливо важливо, щоб обробка потенційних електронних доказів здійснювалась відповідно до перевірених і надійних принципів практики.

Відомо, що докази відіграють дуже важливу роль у кримінальному провадженні, на їх основі суд вирішує питання щодо винуватості підозрюваного у вчиненні кримінального правопорушення. Відповідно до статті 84 Кримінального

процесуального кодексу України, доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

Електронні дані не мають матеріальної реалізації, тому їх набагато легше змінити чи підробити, ніж традиційні форми доказів. Це створює для правоохоронної системи додаткові труднощі: потрібна розробка таких правил поводження з електронними даними, які дозволять забезпечити допустимість доказів.

Електронні докази багато у чому схожі з традиційними, разом з тим їм притаманна низка унікальних характеристик, а саме:

- електронні докази не видно «неозброєним оком» (без спеціальних інструментів);
- їх незначна стійкість до впливу фізичних факторів;
- їх можна копіювати, як правило, без втрати якості.

Для оцінювання допустимості електронних доказів, як правило, застосовують такі критерії: справжність; повнота; надійність; переконливість; пропорційність.

Електронні докази можна визначити як будь-яку накопичену, збережену чи передану в цифровій формі інформацію, необхідну для підтвердження або спростування факту, який є предметом кримінального провадження.

Принципами роботи з електронними доказами є: цілісність даних; документування процесу; експертна підтримка; відповідна підготовка; законність.

Комп'ютерні засоби вилучаються та досліджуються згідно з: Конституцією України; законами України: «Про інформацію»; «Про Національну поліцію»; «Про оперативно-розшукову діяльність»; «Про судову експертизу»; «Про телекомунікації»; «Про Національну програму інформатизації»; Кримінальним кодексом України (розділ XVI); Кримінальним процесуальним

кодексом України; Міжнародною конвенцією «Про кіберзлочинність»; наказом МВС України від 03.11.2015 № 1339 «Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події»; Положенням про Експертну службу МВС України.

Пошук та вилучення комп'ютерних систем та інформації з них можуть здійснюватися під час кримінального провадження відповідно до КПК України шляхом проведення таких слідчих (розшукових) дій:

- проникнення до житла чи іншого володіння особи (ст. 233 КПК);
- обшуку (ст. 234 КПК) на підставі ухвали слідчого судді (ст. 235 КПК);
- огляду (ст. 237).

Крім того, пошук та вилучення КС та інформації з них можуть здійснюватися шляхом проведення негласних слідчих (розшукових) дій відповідно до гл. 21 КПК України.

Джерелами електронних доказів є електронні пристрої: комп'ютери і периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої (гаджети), у тому числі пристрої для зберігання інформації, а також мережа Інтернет. Інформація з цих джерел не має фізичної форми. Разом з тим, електронні докази багато в чому схожі з традиційними: сторона, яка збирає їх у кримінальному провадженні, має продемонструвати, що вони відбивають ті самі обставини і фактичні дані, які існували на момент вчинення злочину. Тобто, треба довести, що дані не підлягали зміненню, додаванню чи видаленню, і в них не вносились (не можуть бути внесені) ніякі правки.

Під час документування огляду (обшуку, виїмки) важливо підготувати детальний опис з відображенням розташування і стану комп'ютерів, носіїв інформації та інших електронних і традиційних пристроїв.

При описанні місця необхідно зафіксувати таку інформацію:

- фізичне розташування об’єктів (зробити замальовку системи, розташування її складових частин;
- зробити фото- і відеозйомку приміщення (за можливістю, кругову);
- позначити місцезнаходження систем і електронних компонентів (пристроїв) обладнання і описати, яким чином вони зв’язані між собою;
- зафіксувати:
- докладну інформацію про всі виявлені пристрої, які мають відношення до розслідування (з позначенням їх марки, моделі і серійних номерів;
- дані про стан і розташування всіх комп’ютерних систем, які містять чи являють собою електронні докази, включаючи інформацію про те, у якому стані знаходиться комп’ютер (включений, вимкнутий, у сплячому режимі);
- інформацію про кабельне і безпровідне підключення комп’ютерних систем;
- позначити порти і кабелі, з’єднання з периферійними пристроями: у подальшому це допоможе відновити точну конфігурацію системи;
- для визначення носіїв даних знайти стикувальні вузли ноутбука;
- вказати характеристики монітора;
- сфотографувати передню частину комп’ютера, монітор та інші комплектуючі;
- описати вміст екрана монітора;
- зняти включені програми на відео чи докладно описати те, що на екрані;
- інформацію про осіб, які знаходяться на місці проведення слідчої дії;
- опитати осіб, які знаходяться в місці, внести їх відповіді у певні форми;
- задокументувати:
- персональні дані всіх осіб, які знаходяться на місці;
- персональні дані всіх осіб, які використовували комп’ютерні системи і обладнання;
- інформацію і коментарі, надані свідками і користувачами/володільцями комп’ютерних пристроїв;
- опис всіх дій, здійснюваних на місці;

- скласти протокол огляду (обшуку) з описом всіх дій і часу їх виконання.

На завершення слід звернути увагу на те, що термінологія у цій сфері нині лише формується. Тому до певних визначень і термінів слід підходити з обережністю. Зокрема, останнім часом з'явилися такі поняття, як «кіберпростір» та «віртуальний простір». А деякі «письменники» пішли далі – запровадили таке поняття, як «віртуальні докази». Разом з тим, віртуальне – це те, чого не існує в реальності. Тому з такими доказами криміналісти й процесуалісти працювати не зможуть.

---

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012. // Голос України. – 2012. – 19 травня (№ 90-91).
3. Наказ Міністерства внутрішніх справ України від 03.11.2015 № 1339 «Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події». [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua›laws/show/z1392-15.
4. Гора І. В. Криміналістика: навч. посіб./ Гора І.В., Іщенко А.В., Колесник В.А. – 4-те вид., випр. та доп. – К.: Вид. Паливода А.В., 2007. – 236 с.
5. Інформаційно-довідкове забезпечення кримінальних проваджень : підручн. / В. В. Бірюков, В. Г. Хахановський, В. С. Бондар, С. В. Шалімов. – К. : Центр учбової літератури, 2014. – 288 с.
6. Огляд місця події при розслідуванні окремих видів злочинів: Наук.-практ. посібник / За ред. Н. І. Клименко. – К.: Юрінком Інтер, 2005. – 216 с.
7. Попередження та розкриття кіберзлочинів: Курс лекцій / Никифорчук Д.Й., Хахановський В. Г., Кудінов В.А. та ін. // К.: ПВП «За друга», 2013. – 282 с.
8. Хахановський В. Г. Проблеми теорії і практики криміналістичної інформатики: монографія / В. Г. Хахановський. – К. : Вид. Дім «Аванпост-Прим». – 382 с.

Сучасні проблеми інформаційно-правового забезпечення особистої безпеки працівників органів правоохоронної діяльності

Чистоклетов Леонтій Григорович,

професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології НУ «Львівська політехніка», доктор юридичних наук, професор

Хитра Олександра Леонтіївна,

доцент кафедри адміністративного права та адміністративного процесу факультету № 3 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук

Шишко Валерій Йосипович,

старший викладач кафедри інформатики Львівського державного університету внутрішніх справ

На всіх етапах історичного розвитку людської цивілізації інформація була як найважливішим об'єктом, так і засобом захисту прав та законних інтересів громадян, протидії злочинності, тероризму та забезпечення безпеки держави і особистості.

Сучасний період суспільно-політичного розвитку України, після Революції Гідності, характеризується різноманітними способами та формами інформаційного забезпечення, які суттєво впливають на життєдіяльність громадян. Сьогодні відбуваються кардинальна переорієнтація державної інформаційної політики, спрямованої на забезпечення національної безпеки держави, прав, свобод, законних інтересів людини, протидії злочинності. І в цих умовах, не зважаючи на те, що працівники правоохоронних органів перебувають під захистом Конституції та законів, численні факти злочинних зазіхань на їх життя і здоров'я під час виконання ними службових обов'язків вказують на їх вразливість.

Як показує практика, на сьогодні забезпечення особистої безпеки працівників Національної поліції, а в загалом і всіх правоохорон-

них органів, ще не має належного рівня, оскільки щорічно гине та отримує тяжкі поранення, психічний розлад або закінчення життя самогубством значна кількість правоохоронців [1].

З даним твердженням слід погодитися. Для прикладу, у повідомлені ГУ Національної поліції України в Дніпропетровській області, за інформацією «Depo.Дніпро» [2], у ніч з 4 на 5 листопада 2017 року у будинку № 46 по вулиці Немировича Данченко слідчу оперативну групу та патрульних поліцейських, які прибули до будинку за викликом «квартирна крадіжка» закидали гранатами та обстріляли з вогнепальної зброї, в наслідок чого було поранено п'ять працівників поліції.

Окремі правові основи інформаційного забезпечення різних соціальних систем управління фрагментарно досліджувалися в контексті проблематики інформаційного права та правової інформатики такими науковцями як: Е.Е. Аблякимовою, І.В. Арістовою, О.А. Барановим, Ю.П. Бурило, Р.А. Калюжним, Б.А. Кормичем, Є.Б. Кубко, В.А. Ліпканом, А.М. Новицьким, Н.Б. Новицькою, Г.П. Середою, В.С. Цимбалюком, В.О. Шамраєм та іншими.

Забезпечення особистої безпеки працівників правоохоронних органів є об'єктом дослідження С.В. Городянка «Організаційно-правове забезпечення безпеки діяльності працівників ОВС України» (Київ, 2007) та А.І. Суббота «Адміністративно-правові засоби забезпечення особистої безпеки працівників правоохоронних органів» (Ірпінь, 2013). У цих роботах ґрунтовно досліджені організаційні та правові аспекти забезпечення особистої безпеки працівників окремих органів правоохороних, однак питання інформаційного забезпечення їх особистої безпеки спеціально не досліджувалися і у подальшому потребують теоретичного аналізу і детальної розробки обґрунтованих науково-практичних рекомендацій.

Досліджуючи термін «безпека», наведемо визначення, що було висловлено В. М Заплатинським, який трактує безпеку як умови, в яких перебуває складна система, коли дія зовнішніх факторитетів і внутрішніх чинників не призводить до процесів,

що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [3].

Однак для повного розуміння сутності інформаційно-правового забезпечення особистої безпеки працівників органів правоохоронної діяльності, нам слід також визначитися з поняттям терміну «особиста безпека». Так на думку Л.І. Казміренко та Є.М. Моісеєва особиста безпека – це організаційно-правові, фізичні і тактико-психологічні заходи, які дозволяють забезпечити збереження життя та здоров'я працівника правоохоронних органів і підтримання високого рівня ефективності його професійних дій [4, с. 143]. Таким чином, особиста безпека є результатом реалізації комплексу заходів, спрямованих на зниження рівня професійного ризику до реально можливого мінімуму, що дозволяє гарантувати збереження життя і здоров'я, нормального психічного стану і дієздатності працівників правоохоронних органів при високій ефективності вирішення ним професійних завдань.

Розглядаючи категорію особиста безпека, не можна обійти увагою поняття терміну «небезпека». С.В. Городянко її визначає як сукупності різних за змістом, характером, силою та наслідками впливу умов, об’єктів, предметів, факторів і процесів, які загрожують безпеці діяльності осіб рядового і начальницького складу і здатні заподіяти шкоду життю, здоров’ю, честі, гідності та недоторканності останніх у процесі виконання ними посадово-функціональних обов’язків [5, с. 6].

Таким чином, як слушно зазначає В.В. Богуславський, особиста безпека працівників в діяльності сил охорони правопорядку одночасно є як метою діяльності (для збереження їх життя та здоров'я як найголовніших соціальних цінностей), так і умовою діяльності, оскільки ефективна охорона правопорядку можлива тільки при неушкодженому стані людей, які її здійснюють. При цьому ці аспекти особистої безпеки часто бувають взаємовиключними, оскільки в рамках охорони правопорядку доводиться діяти в умовах ризику для власного життя та здоров'я [6, с. 49].

Підтвердження цього твердження можна зробити і на прикладі норм положення про організацію службової підготовки працівників Національної поліції України, затверджене Наказом Міністерства внутрішніх справ України № 50 від 26 січня 2016 року, в якому особиста безпека виступає одночасно і як метою проведення курсів, і як умовою їх проведення [7].

Загалом інформаційно-правове забезпечення особистої безпеки працівників правоохоронних органів повинно забезпечуватися такими блоками:

- організаційно-правовим – комплексом об'єктивних передумов для ефективного і безпечного здійснення професійної діяльності;
- мотиваційно-особистісним – морально-поведінкові установки, психологічна готовність «на виживання», тобто дотримання норм, правил і спеціальних процедур, що гарантують особисту безпеку.

Організаційно-правовий блок забезпечується такими державними інституціями як: Кабінет Міністрів, Національна поліція, Служба безпеки України, Міністерство інформаційної політики України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство фінансів України тощо. Правовий напрямок повинен включати в себе нормативно-матеріальний та нормативно-процесуальний, а також нормативно-правовий та індивідуально-правові аспекти.

Суб'єкти другого блоку – працівники – для забезпечення особистої безпеки повинні:

- знати і неухильно виконувати відповідні і директивні вказівки керівництва;
- знати основні тактико-операційні та психологічні прийоми інформаційного забезпечення особистої безпеки у різноманітних ситуаціях професійної діяльності;
- уміти аналізувати і узагальнювати інформацію щодо досвіду безпечної поведінки колег по роботі та інших працівників у екстремальних умовах оперативно-службової діяльності;

- знати, застосовувати і творчо збагачувати тактику, прийоми і засоби інформаційного забезпечення особистої безпеки та безпеки колег.

Не меншою загрозою, яка посягає на процес інформаційно-правового забезпечення особистої безпеки працівників органів правоохоронної діяльності є фактор зростання кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів, в тому числі на об'єктах критичної інформаційної інфраструктури. З метою убезпечення цього злочинного прояву у парламенті 5 жовтня 2017 року було ухвалено закон «Про основні засади забезпечення кібербезпеки України».

Таким чином, з метою поліпшення правоохоронної діяльності та підвищення авторитету представників правоохоронних органів, державна інформаційна політика у сфері забезпечення особистої безпеки цих органів повинна реалізовуватися шляхом її забезпечення на законодавчому, виконавчому та судовому рівнях, з подальшим удосконаленням кадрової роботи з відбору кандидатів та систематичним навчанням працівників правоохоронних органів правилам особистої безпеки.

---

1. Трояновський В.С. Особиста безпека поліцейського під час виконання службових обов'язків: зарубіжний досвід. – [Електронний ресурс]. Режим доступу : http: ///C:/Users/Acer/Downloads/Pupch_2016_1_24%20(2).pdf.
2. У Дніпрі поліцейських закидали гранатами: Поранено п'ятеро: – [Електронний ресурс]. Режим доступу : https://dnipro.depo.ua/ukr/dnipro/u-dnipri-policeyskih-zakidali-granatami-poraneno-chetvero-20171105670405.
3. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоровя людини. / [редкол.: П. С. Атаманчук (відп. Ред..) та ін.]. — Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. – Випуск 5. (−336 с.) С. 90-98.

4. Юридична психологія: Підручник / За заг. ред. Л.І. Казміренко, Є.М. Моісеєва. – К.: КНТ, 2007. – 360 с.
5. Городянко С.В. Організаційно-правове забезпечення безпеки діяльності працівників ОВС України: автореф. дис. на здобуття наук. ступ. канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / С.В. Городянко. – К., 2007. – 20 с
6. Богуславський В. В. Адміністративно-правове регулювання інформаційного забезпечення особистої безпеки працівників сил охорони правопорядку: дис. … кандидата юрид. наук: 12.00.07 / Богуславський Віктор Владимирович. – Дніпропетровський державний університет внутрішніх справ, 2017. – 202 с.
7. Положення про організацію службової підготовки працівників Національної поліції України, затверджене Наказом Міністерства внутрішніх справ України № 50 від 26 січня 2016 року. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0260-16.

Learning Management Systems for Homeland Security Training

Danuta Kaźmierczak,

Doktor nauk społecznych.
Uniwersytet Pedagogiczny im. KEN w Krakowie, Polska

Abstract:

The technological advances influence human life in all spheres, produce positive as well as negative effects. The same ICT systems that foster development can be used to threaten the world with terrorism and cyberterrorism. The homeland security departments bear more and more responsibilities for protecting societies. The aim of this paper is to show the better side of new technology and suggest implementation of the learning management systems (LMS) for professional training of government officials and police officers for their jobs. The preparation involves practical and theoretical training that can be provided with both traditional and modern methods. LMS can offer tools for developing skills and competencies as well as deliver analysis how the single official's performance translates into

the performance of the whole department. To show that LMS is not only the whim of that time but necessity and the future, the author presents also the directions of its development.

Key words: LMS, training, homeland security, technology, IA

Introduction

The scope of homeland security department responsibilities is to secure the society from many threats, and involves: anti- terrorism, border security, immigration and customs, cyber security, and disaster prevention. Patrick J. Massey categorizes threats into inherently external in nature, i.e. inflicted upon us: earthquakes, terrorist bombings, hurricane, flooding. We can protect against, prepare for, and anticipate them but actually we are their passive victims. Yet, most of threats to the country are not immediate but long-term, and are not external, but internal – self-generated threats as we are doing them to ourselves or we are vulnerable to them. Undoubtedly, they pose a catastrophic risk to social stability. The list includes: the enormous indebtedness of treasury, global warming, an inferior mathematics and science educational system, decaying physical infrastructure, the mass-privatization of government services (leading to the increase of decision-making authority amongst those unconcerned about the public good); over-reliance on foreign energy sources, and the dual demographic pressures of dropping birth-rates amongst the native-born, which results in a rapidly aging population and population increases fueled by massive economic or war immigrants [1].

These threats are unpredictable, changing, growing in strength and consequences and difficult to control. To minimize them or fight effectively the homeland security needs adequate equipment but first of all, well trained officials and police officers.

Training programs should be designed in a way to provide current content, develop required skills to number of officials and officers in the right time place quantity, quality and costs. They will be even more effective if include the evaluation system providing feedback for a trainer and trainee. These expectations can be met with Learning Management Systems (LMS). The aim of this paper is to

present generally the possibilities the learning management applications offer as well as the directions of their development and transformation into artificial intelligence for learning.

1. Learning Management Systems and their tools

Learning management systems have mainly been used to deliver formal learning, assign eLearning courses to students, track their progress, and evaluate their level of knowledge retention. At present, the market offers LMS with more functionalities like social learning features that allow users to consult mentors, ask questions, cooperate, motivate and reward content contribution.

Other features that a good LMS should include are:

- Automated Admin Tasks – to automate recurring tasks: user grouping, group enrollment, and new user population,
- Certifications and Retraining – to manage recurring training/continuing education/ compliance programs, Mobility – to accessed the content anytime, anywhere, regardless of device,
- Course and Catalog Management – to create and manage courses and course catalogs to deliver more targeted learning to the users,
- Content Integration and Interoperability – to support learning content packaged according to interoperable standards (SCORM, AICC, and xAPI),
- Content Marketplace – to provide learners with off-the-shelf courses from global eLearning content providers,
- Notifications – to support automatic, real-time feedback indicating learner progress, course completions, certifications, achievements, and comments,
- Gamification – to motivate by allowing learners to achieve points, badges, awards,
- Integrations – to allow for third-party integrations with other platforms, such as CRM, video conferencing tools,
- Ecommerce – to benefit from selling courses,
- Reporting – to track and measure the impact that training programs have on general performance of the trainer and the department. A gap analysis evaluation identifies the lack of the skills and competencies necessary to perform successfully. Then

a personalized learning plan can be designed to increase the officers' skills (and subsequently, their operational performance and performance of the department) [2].

2. The future of learning technologies

When Heidi and Alvin Toffler formulated a futuristic and rather creepy vision of artificial intelligence able to fight, think and make decisions for us or against us [3], people still believed that it is in the realm of fantasy not reality. Yet, experts and technological developments show that gradually this vision comes to life. According to research firm IDC, worldwide spending on robotics will top $188 billion by 2020, up from $91.5 billion in 2016, due to new use cases and acceptance in the marketplace. Innovators in the field of robotics are delivering robots that can perform a wide range of tasks well or better than humans, which foster the adoption of robotics into many industries.

Boston Dynamics, known for its terrifying-looking robots, has recently presented a humanoid robot able to jump from block to block and do a backflip.

There is also pressure on governments from some experts to regulate artificial intelligence and robotics, much like society does with other sectors, such as food and drugs [4].

Artificial Intelligence is also useful in the field of learning. LMS administrators spend long hours on error prone, and repetitive tasks such as managing users, enrolling users to courses, or tagging content. AI will automate most of these tasks and, even will do the job better. Below are a few examples:

An administrator makes decisions using manual steps and AI will be able to suggest or assign learning assets to learners based on a set of criteria like:

- Learning objectives: identifying the relevant learning objectives and topics for the role and the task at hand
- Skills data: suggesting what has worked in the past to increase specific skills in similar roles,
- Performance Data: suggesting what has worked in the past to increase specific KPIs (Key Performance Indicator, e.g. reach

80% of successfully completed operations, solved cases, identified crimes),

- Learning style: suggesting preferred learning style/format: e.g. a full course or a collection of small content bytes,
- Preferred channel: suggesting the use of mobile for people that are constantly on the go or full desktop for highly technical and detailed instructions,
- Personal interests: considering user preferences,
- Organizational behavior: considering the characteristics of the department the learners are a part of,
- Learning interventions: modifications according to a change in regulations, compliance, or in company policy,
- Content Discovery Beyond automating processes: AI will discover new learning content for a given population of learners by analyzing what is available through online systems, such as video platforms (e.g. YouTube, Vimeo, Kaltura), online learning and teaching marketplaces and social platforms to provide highly personalized learning opportunities,
- Chatbots AI algorithms: provide learners with answers. Subject matter experts (SME) will no longer train people; they will train robots who will, in turn, train the end users. Chatbots can be specific to the job: an Onboarding Chatbot who trains new employees on the first few days, a Security Chatbot,
- Keeping Humans in the Loop: chatbots can also identify subject matter experts in the organization to meet learners' needs. For example, when a chatbot is not able to provide an answer, it could direct the question to someone who has been identified as an expert on the topic at hand,
- Content Creation Consider even the authoring of content [5].

Conclusion

The training management system can effectively support learning as it actually happens (i.e., via a mixture of formal and informal methods) and provide a channels to deliver, monitor, and measure learning activities. The key advantages of LMS is that it can provide metrics to measure productivity and progress, as well as make the connection between how learning impacts organizational performance.

The research by Brandon Hall Group shows that 54% of organizations who have invested in learning technology have seen improvements in productivity and engagement. 91% of these organizations also reported a stronger link between learning and organizational performance [2].

Another crucial advantage of LMS implementation for homeland security departments is that the system provides the up-to date content recognizing needs of the single officer/learner, the department and society as it draw from social media, which definitely transfer to identification of threats, vulnerabilities in society and ability to respond to them.

LMS is the demand of time, helpful tool to increase performance and make use of AI services in the future.

1. Massey P.J., Generational Hazards, HOMELAND SECURITY AFFAIRS, The Journal of the NPS Center for Homeland Defense and Security Home , Volume XIII – 2017, https://www.hsaj.org/articles/142(30.11.2017)
2. BACK TO BASICS: LMS 101 The complete guide to learning management systems by Docebo, 2017.
3. Toffler A.H., Wojna i antywojna, Wydawnictwo Kurpisz S.A. Poznań, 1993
4. Ciaccia Ch., Elon Musk is freaked out by the creepy backflipping robot, Fox News; http://www.foxnews.com/tech/2017/11/27/ elon-musk-is-freaked-out-by-creepy-backflipping-robot.html (30.11.2017)
5. Canonico M., EMERGING TRENDS: L&D AND THE ARRIVAL OF AI, Docebo 2017.

Strategy for computerization of organizations, institutions functioning in defense and security

Kuck Jerzy, Grzegorz,

Doctor of military science,
specialization in management of information systems

Abstract: The aim of the paper is to present the range of the research and experiences of the author, in implementation of new IT solutions.

Especially, these solutions connected with building and implementing the integrated multilevel IT systems for logistics, finances and HR for defence and security. The detailed research concerned the strategy for informatization, business process management and implementation of the system of product identification as the foundations for IT systems.

The hypothesis assumes that presently operating IT systems do not meet the needs. Implementation of new IT solutions should improve the performance in logistics, finances and HR for defence and security and their implementation in both areas would be the most effective approach to manage the capacity rationally.

To verify the formulated assumptions the author analysed how to design and implement the strategy of informatization, how to acquire the new IT solutions for defence and security.

In the social science the defence and security are interconnected and implementation of new IT systems for logistics, finances and HR could, in the author's opinion, integrate them even more and this way improve the effectiveness and operational efficiency in time of peace, crisis and war.

Key words: strategy of informatization, processes, IT systems, logistics, finances, HR

Strategy of organization and strategy of informatization

Closely associated with the technological progress, the information society is being created to change along with the spreading information technologies of the new generation, successively in the field of economy, the public sector and as well as social structures[2]. Continuous technological development, market competitiveness and new scopes of knowledge encourage application of new information technologies (solutions). Such technologies enable collection, transfer, storage and distribution of information almost without any limits of time and distance.

Popularization of knowledge of modern IT systems in defense and security brings remarkable and quick benefits. This concerns students as well as experts willing to expand their knowledge.

[2] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Helion, Gliwice 2004, s. 51.

Meeting expectations of future readers the research was continued to perform the analysis of modern and effective management in defense and security. Such approach promotes informatization of logistics in organizations, institutions and makes establishment of the Integrated (Multilevel) IT System of Logistics, Finances and HR easier in defense and security. The strategies for informatisation of organizations, institutions including Integrated Multilevel IT systems for logistics, finances and HR are suggested to implement modern technologies for management efficiently.

Strategy in the general sense means the economic, social, military orientation which set the direction of actions for particular system. This general orientation is the main line and at the same time guideline for the management in the situations happening in their environment considering their own human, organizational, financial and technical-productive capacity. However, it is important to emphasize the comprehensive nature of the strategy in its basic dimension since it is a project for a future organization and operation of the whole system[3].

Strategy from the informatics approach is the pattern of actions project, which defines the algorithms and identifies them in a form of classes so that it is possible to adapt each of them interchangeably and during the application operation and independently of the users.

Presentation of strategy of informatisation for organizations, institutions in defense and security should encourage discussion, afterthought and sharing findings, suggestions and asking questions. The first question can be: **Does the success begins with information and what can the informatics do for defense and security in the nearest future?**

Perhaps the earliest question should be: what can defense and security do for themselves?

The experts claim that firstly, the areas which are to be informatized should be organized and defined. Only then the process of informatization should commence to finish with success.

Cezary RUTKOWSKI in his essay *«**Nowa cywilizacja. Stare organizacje**» in the magazine Myśl Wojskowa claims that the strategy of*

[3] https://pl.wikipedia.org/wiki/Strategia [10.12.2017].

success «besides the rules for thinking, the best methods and tools, knowledge and skills we should list four more (perhaps the most important) conditions for success, sources of chances, i.e.: identity, creativity, passion and amity». Moreover, he suggests that «for us, people of the 21st century, the strategy of success may be based on taking two chances: firstly, we ought to identify opportunities undiscovered by others; secondly, we should start and finish developing specific skills, which others cannot develop or develop them slower».

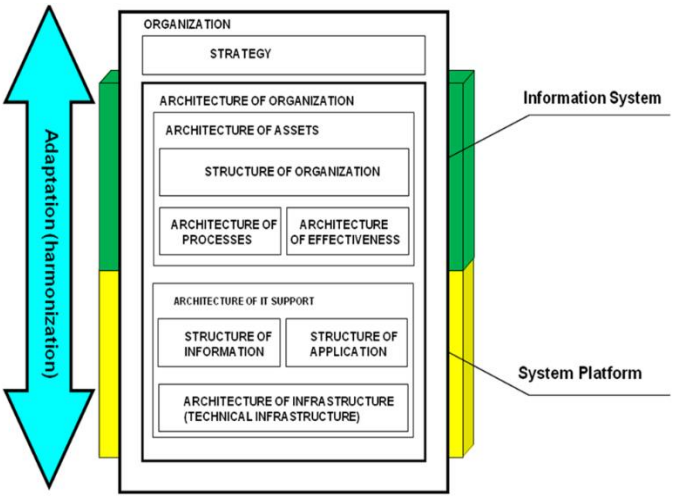
This approach communicates that after defining the strategy of an organization, institution the next step can be preparation and implementation of the strategy of informatization. The IT system is an integral part of the whole organization and does not exist without it, as an independent solution. A strategy of an organization defines the way of action and adaptation of particular organizational elements. In other words, the strategy of an organization is a characteristic combination of people, resources and methods to accomplish organizational goals within a defined time scope.

The presented model is useful for defining guidelines for IT support of an organization. Figure 1 shows the operational area of an IT system and its technical aspects – the system platform in the organization. It is very important to adapt the platform for circulation of information already at the stage of building and later, while exploiting it[4].

The technical layer of the system should include the organizational structure with the users and their roles, the range of information and the place of the event recorded in databases. Generally, the models of processes reflected in the information structure involve: managing, command and control, informing, reporting, planning and numerous areas connected with logistics, finance and HR. This is a key to success of the whole enterprise. This is so, because the information structure determines the application pattern.

The conducted analysis indicate proposals and suggestions how to employ the strategy of informaization for institutions and organizations in defense and security, including:

[4] J. Kuck. *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015, p. 62.



Source: J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013, p. 97.

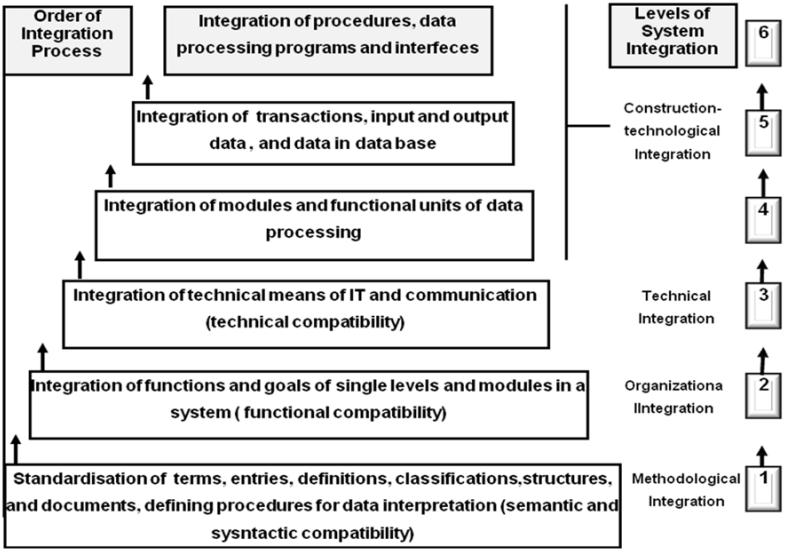
Fig. 1. The basic model of organization with IT support elements.

- Basic directions of development of informatization,
- Strategic aims of informatizations and ways of achieving them,
- Expected results and threats that can inhibit implementation of planned solutions.
- Moreover, it is important to establish:
- If organizations and institutions are prepared to face challenges of the 21st century?
- If presented new solutions (IT systems) should be an integral part of defense and security including logistics, finances and HR?
- What should the integrated IT system connecting defense and security «look» like?
- Should it be connected with the national economy, NAO and EU systems?
- How should this system be built?
- Who should implement it and on which organizational levels should this system operate?
- When will it operate on all organizational levels in defense and security?
- What are the costs?

Implementations of new ICT technologies needs the strategy of informatization for defense and security, understood there, as a specific connection of people, assets (means) and methods of action to achieve defined aims in a specific time. Some experts draw attention to the fact that commencing informatization of organizations and institutions of defense and security at the preset state without prior reorganization the situations will be even worse than before startin the whole project.

Reorganization of structures and levels of integration of IT systems

Complexity of the enterprise rises the need for standardization and defined order of the integration steps on each level where the system is implemented. Such order should be as follows:



Source: Z.J. Klonowski, Systemy informatyczne zarządzania przedsiębiorstwem. Modele rozwoju, właściwości funkcjonalne. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004, p. 181.

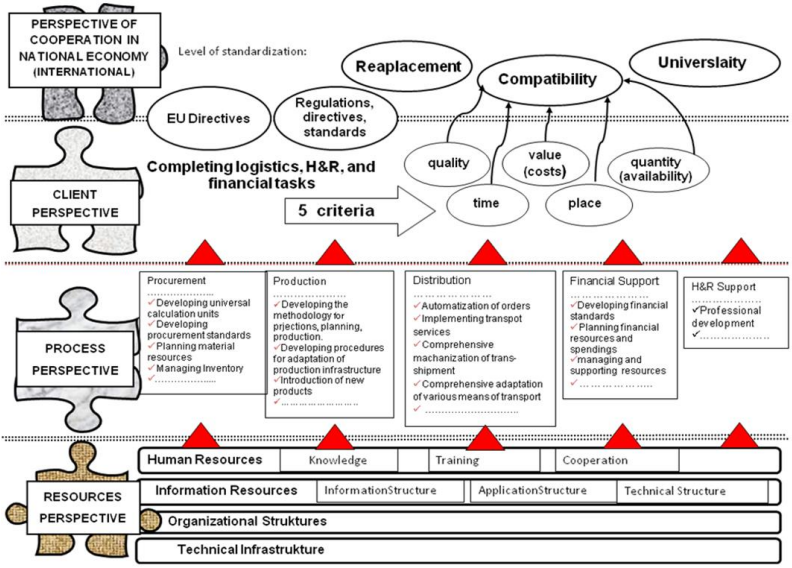
Fig 2. The order of integration steps and the levels of integration for the IT system

The importance of subsequent steps changes with the integration level and implementation of IT solutions. For logistics, finances and

HR it means firstly, standardization of concepts, entries, definitions, product coding, identification of limits of any kind, defining standards, accounts, etc. For the integration process as a whole, at any levels and range it is necessary to standardize the software, equipment and the network and to ensure teleinformation security[5].

Such a solution will create new quality. Furthermore, it will support inventory of assets with such criteria as: quality, quantity and value in all units (branches) at particular organizational levels. The experience of other countries prove that starting to build the integrated (multilevel) IT system, it is first necessary to organize and at the same time identify logistics, financial and HR tasks in the areas which would be integrated.

Stable and transparent organizational structures should create strong foundations of the system



Source: elaborated on J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013, p. 102.

Fig.3. Detailed map of organization strategy (variant)

[5] J. Kuck. *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015, p. 47.

The objective of such system is to support:

- Comprehensive integration within an organization, institution or company and their external surrounding,
- Perfect performance of tasks in single units (branches) at all organizational levels,
- Perfect process management,
- Rational resources management to provide for the defense and security.

While building the system, the range and time of introducing single standardization levels (compatibility, exchangeability, universality) should comply with the task performance critera, such as quality, quantity, time, place and value. The precisely defined tasks should improve the organizational structures, human resources (including knowledge, training and skills), information and the technical infrastructure.

In the process of decision making in logistics, finance and HR and the right flow of information play the important role. As never before, it is obvious that advantage is gained by the one who possesses information. To get hold of the information in real time, it is necessary to implement IT tools for single processes. IT support for information processing in logistics, finance and HR should streamline the following:

- Command and control, managing,
- Informing,
- Planning,
- Predicting,
- Simulating,
- Inventory and reporting,
- Developing structures and norms,
- Monitoring and evaluating[6].

Efficiency of an IT system should be ensured by implementing good-quality applications and proper technical infrastructure. The

[6] J. Kuck. *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015, p. 65-66.

application structure in such system may be discussed at two levels: the logical and the physical one. The technical structure is used to collect, process, store and distribute (transfer) information while single elements of an IT system are closely linked with each other.

The strategic aims and stages of informatizations

The planned organizational and functional structure of the system should reflect the structure of the organization and institution on the particular organizational levels functioning in the defense and security. What structures such a system.

The strategic aims that condition the informatization and building the Integrated Multilevel IT System Supporting Logistics, Finances and Human Resources in organizations and institutions in the defense and security:

- Identification of defense products (identification, ultimately coding and identification of products on the level of warehouses),
- Securing automatic classified and unclassified data exchange with land-based and field computer networks and providing adequate ICT security at the same time,
- Integration of quality-quantity-value records,
- Building of IT structures for logistics, finances and HR on the particular organizational levels,
- Providing compatibility of IT systems in the defense and security with National Economy, NATO and EU systems,
- Securing financial means for informatization of logistics of the ministry of defense.

So far analysis and proposals indicate that it is the most rational to conduct informatization of logistics, finances and HR in the defense and security at two stages.

The first stage (the nearest task) should include identification of tasks, assets and processes. Then, on the basis of the central data base the IT systems and subsystem for logistics, finance and HR management on the particular organizational levels for a given departments should be built:

- Implement systems for identification of defense products (an index base, ultimately code base and identification of the product on the warehouse level),
- Built IT systems and subsystems for logistics, finance and HR management on the particular organizational levels for a given departments to integrate quantity-quality-value records,
- Connect to classified and unclassified networks particular executive elements of logistics, finances and HR,
- Design and build the central database for quantity-quality-value measure including single systems (materials, technical, medical, transport and troop movement, and infrastructure connected to finance and HR).

The second stage (the further task) includes building the Integrated Multilevel IT System for Logistics, Finances and Human Resources in the defense and security and connect in networks all organizations and institutions supporting logistics, finance and HR.

After implementation is completed, the Integrated Multilevel IT System for Logistics, Finances and Human Resources in the defense and security:

- Provides in a real time the reliable information about the whole assets of the defense and security, and the collected information refers to quantity and value and qualitative characteristics of the assets,
- Provides more current, complete and reliable information as a base for evaluation, planning and decision making processes,
- Support effective monitoring of assets flow among single elements and includes time, place, quality, quantity and value,
- Supports automatic information exchange and reporting in logistics, finance and HR,
- Supports effective record and monitoring of expenditures on logistics, finance and HR processes,
- Makes logistic support more effective during transition from the command and control system operating in time of peace to the system operating in time of war, including logistic, financial and HR support for mobilization and operational development of troops and operations outside the country,

- Is compatible with the solutions of the national economy, NATO and EU[7].

To complete this comprehensive project embracing single departments and units of logistics, finance and HR in organizations and institutions of the defense and security successfully, it is necessary to assign the adequate amount of money. The foregoing experience proves that we can expect the best effect if the financial means are collected in one place.

Drawing on experience of companies and materials from the armies of other EU and NATO members, completing such an extensive project needs setting the analytical-design-implementation team on the central level. This team should count 150 – 200 people. It should include experts in defense and security as well as civilians.

Drawing on experience of the leading NATO countries which employed «*SAP for Defense & Security*» technologies which facilitate planning and completing processes of **HR, logistics and finance management** we can make it cheaper in a much shorter time. The right choice of technologies (in that case SAP) facilitates **integration of main logistic, financial and HR processes**.

Concluding:

Logistics, finance and HR in the defense and security are mostly flexible to informatization, yet, the effects and results of informatization are not feeding frenzy. It is long and mundane intellectual and technical process that needs consistency and the expected result will come after a few years and they are not going to be spectacular. At present many European countries have the informatization strategies, identified and optimized processes, implemented system of products identification and coding, eclectronic shopping and distance learning systems.

The actions taken and positive results give optimistic projection for the future implementation of new IT solutions as the common standard. The experience of the countries which implemented these

[7] J. Kuck. *Nowoczesność, efektywność o bezpieczeństwo współczesnej logistyki*, AON, Warszawa 2015, s. 199.

solutions show, that implemented new IT solutions produce **significant economical and organizational benefits**.

1. Długosz J., Nowoczesne technologie w logistyce, PWE, Warszawa 2009.
2. Klonowski Z.J., Systemy informatyczne zarządzania przedsiębiorstwem. Modele rozwoju, właściwości funkcjonalne. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.
3. Kuck J., Nowoczesne technologie w logistyce, AON, Warszawa 2013
4. Kuck J.. Nowoczesność, efektywność o bezpieczeństwo współczesnej logistyki, AON, Warszawa 2015.
5. Kuck J.. Modern IT solution for logistics, Lviv Galician Publishers, Ltd 2015.
6. Suchorzewska A., Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, Helion, Gliwice 2004.
7. https://pl.wikipedia.org/wiki/Strategia [10.12.2017].

Identification and optimization of processes for defense and security purposes

Kuck Jerzy, Grzegorz,

Doctor of military science,
specialization in management of information systems

Abstract: The aim of the paper is to present the solutions which facilitate ordering structures, tasks, management and control processes of logistics, finance and HR in organizations and institutions in the defense and security. The hypothesis assumes that the business market can offer solutions possible to adapt in the defense and security. Implementation of these solutions could facilitate identification and optimization of processes and so increase their effectiveness.

The conducted analysis shows that ARIS toolset and IDS Scheer implementation competences are one of such solutions. This software offers graphic design and processing of descriptions for complex connections between elements in management systems and IT systems operating in organizations and institutions in the defense

and security. Process tools help design and test a coherent project of a new organizational structure. With this solution it is also possible to simulate and evaluate influence of implemented changes in assign responsibilities of functional workers on a given positions. The paper discusses process management which is one of the most effective tool to support modern, rational and effective operating of the organizations and institutions in the defense and security.

Key words: business process management, ARIS toolset, defense, security

1. The concept and classification of processes

Development of process approach in organizations, institutions and companies, has nowadays become one of the main trends while seeking effective management. Every single process needs proper management. Respective theory and practice offer the opportunity to organize processes and at the same time to improve them, which brings significant organizational and economic benefits. **Evolution of the process approach** started in the early 20th c. and may be divided into three stages.

The first stage fell on the 1920' s when F. Taylor, precursor of the process approach, created the basis of the scientific theory of organization[8].

The second stage – Business Process Reengineering – fell on the 1980's and 1990's and was defined by M. Hammer and J. Champy.

This solution emphasized the role of process managers. It adopted the value analysis developed in the 50's and the system approach for management and the M.E. Porter's concept of chain values that defined two kinds of activities within a company: the basic and the supporting ones[9].

[8] A. Bitkowska. *Zarządzanie procesami biznesowymi w przedsiębiorstwie*, Vizja Prest, Warszawa 2009.

[9] T. Kasprzyk, *Organizacja zorientowana na proces biznesu – modelowanie referencyjne* [w:] tenże (red.), *Modele referencyjne w zarządzaniu procesami biznesu*, Difin, Warszawa 2005, p. 26.

The third stage started in the late 90's – Business Process Management. The revolutionary changes gave way to evolution and constant improvement. The holistic approach became popular among businesses and security services. It facilitated definition, modeling and improvement of the processes of effective management.

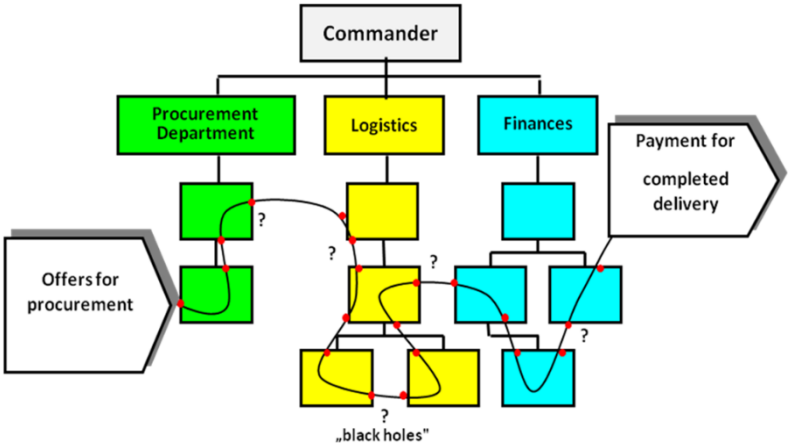
In the 21st century computers facilitate collection, processing, storage and distribution of knowledge as well as the learning process. The global computer network, initiated in the 60's linked millions of computers worldwide and allowed the users to send information through telephone networks and the so-called special connections.

According to their range, the computer networks can be classified into:

- LAN (Local Area Network),
- MAN (Metropolitan Area Network),
- WAN (Wide Area Network),
- Corporation.

Adapting modern methods of IT support for logistics should also involve HR and finance. Such comprehensive process approach facilitates creation of the IT system supporting functions in organization and institution. Accomplishment of this enterprise goes far beyond the technical sphere and calls for multi-sided actions. Only then the IT system will perform as an integral part of the organization or institution (it does not exist as an independent solution). This should streamline building the Integrated (Multilevel) IT System for Logistics, Finance and HR.

Implementation of the system, operating in real time, based on the mechanisms such as: analysis, control, evaluation and planning will dramatically improve inventory in terms of quality, quantity and value. Figure 1 presents the traditional purchasing and identifies the so-called black holes. Implementing modern information technology with the process approach should eliminate such holes.



Source: J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013, p. 69.

Fig. 1. The diagram of traditional purchasing

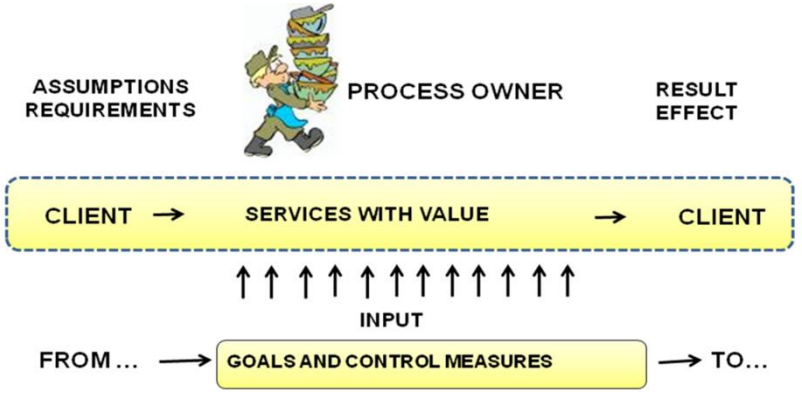
Process approach to organization, institution is considered as one of the main trends in effective management.

The concept of business (economy) process means the chain of changes with the input and a given output result – an achieved goal. The tangible and personal assets of an organization, institution or company undergo such changes.

A process is a sequence of interdependent and linked procedures which begin and end and have clearly defined inputs as well as the end result. In other words, a process is a series of defined actions that lead to a particular result[10].A business process, designed to reach goals defined by an organization, institution, involves connections between suppliers, clients and other entities, business partners, etc. (business process components – Fig.2). A single change in a business process is a function. Decomposition of a function transforms the function into sub-process. With the equal access to resources, technologies and suppliers, organizations

[10] R. Gabryelczyk, *ARIS w modelowaniu procesów biznesu*, Centrum Doradztwa i Informatyki, Difin, Warszawa 2006. p. 15.

compete through efficiency of processes. Measures of process efficiency are: time, cost and quality of the result provided to a client.



Source: H.J. Schmelzer, W. Sesselmann, Geschäftsprozessmanagement in der Praxis, Carl Hanser, München–Wien 2003, p. 40.

Fig. 2 The business process components

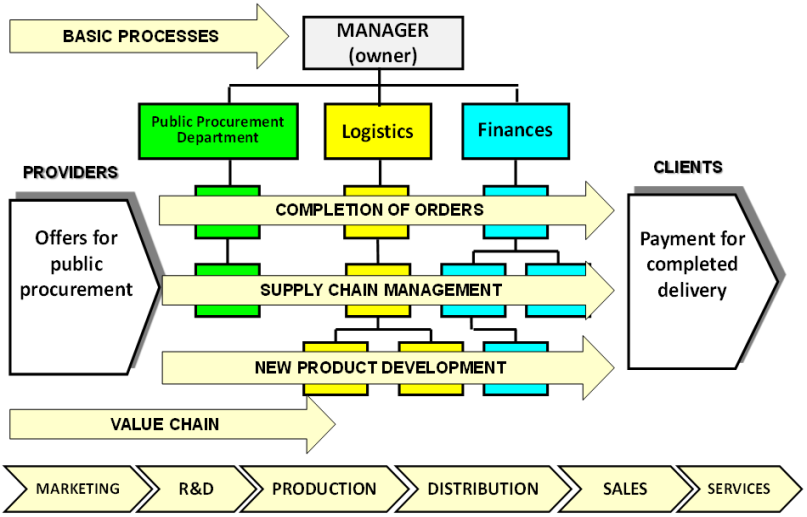
The number and nature of processes depends on the needs of a particular organization, institution or company. There are three different types of business processes:

- **Core processes** (also called primary, essential, operational processes),
- **Support processes**, designed to provide support for primary processes, and performed within an organization,
- **System processes** (management) support and improve the whole management system in an organization.

Core processes (Fig 3), often called main processes, are composed of actions, decisions, information and materials taken together. They have the biggest influence on organization performance and (for a company) its competitive position on the market. Core processes create value and have a strategic meaning, they run through many departments connecting suppliers with the clients. Support processes do not have any strategic meaning and should be clearly separated from the primary ones. They can be accomplished effectively by

outer companies[11]. The literature provides a variety of classifications of processes:

- **Operational, support** (J. Brilman),
- **Megaprocesses, main processes and subprocesses** (K. Zimniewicz),
- **Operating processes (main), support processes** (American Productivity & Quality Center).



Source: R. Kaplan, L. Murdock, Core Process Reengineering, McKinsey Quarterly 2», Summer 1991, p. 29.

Fig. 3. Core processes and a supply chain

W. Kreuz[12] categorizes processes into four types:

[11] J. Kuck, *Procesowa organizacja organizacji, instytucji, przedsiębiorstw oraz firm* [w:] Z. Grzywny, *Bezpieczeństwo w procesach globalizacji – dziś i jutro*, t. I, Wyższa Szkoła Zarządzania Marketingowego i Języków Obcych, Katowice 2013, p. 301.

[12] W. Kreuz, *Transformation the Enterprise, Die nächste Generation des Business Process Eingineering*, [w:] M. Nippa, A. Picot, *Prozeßmanagement und Reengineering*, Campus Verlag, Frakfurt–New York 1996, pp. 99 – 101.

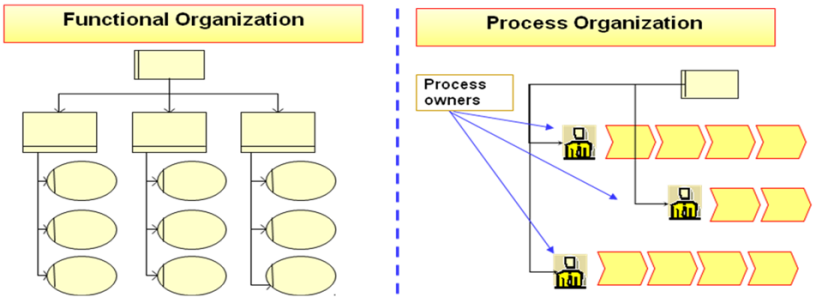
- Key processes ensure the success of an organization, institution or a company by emphasis on high quality of a product or service oriented towards competitors,
- « Leverage « processes that recognize time, costs and quality and optimize them,
- Opportunistic processes deal with different approach to clients, promoting those with whom cooperation generates best profits,
- Supporting processes support the key processes, should maximize effectiveness and eliminate redundant work.

The processes may also be divided by:

a) decision-making positions:
- managing (system) processes,
- executive processes.

b) importance for an organization:
- strategic processes,
- operational processes.

c) submission:
- main processes,
- minor processes.

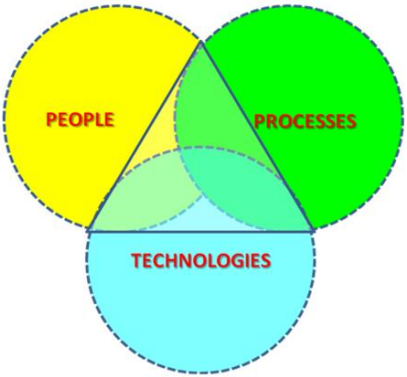


Source: J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013, p. 68.

Fig. 4. Functional and Process Organization – comparison.

It is the owner of the process, who plays the key role in completing a single activity. Connection of people, processes and technology (Fig.5) and well-used power of the boss decide how the process

should be performed. This is the role which cannot be underestimated if the (owner) organization wish to operate on a given level. The owner of the process knows what he possesses at the input, what supplies the process and how the process should end. Moreover, he monitors and reports on the outcome and ensures the contact with suppliers and clients and cares about competences and right information.

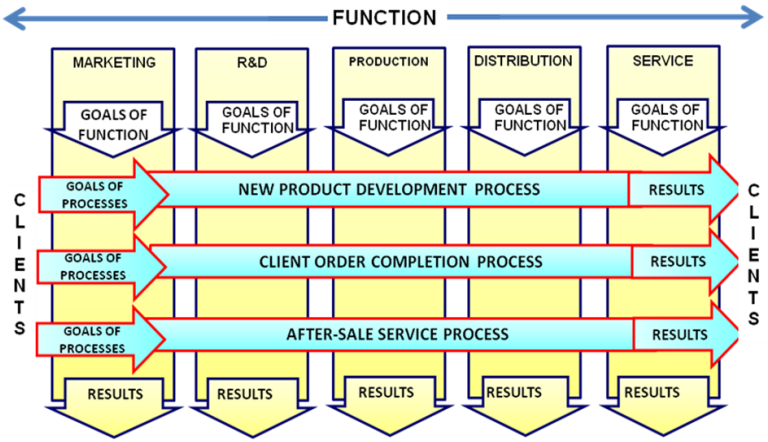


Source: based on T. Emser, The BMP Pyramid: People, Process, and Technology.

Fig. 5. Links between people, processes and technology.

Organizations, institutions and companies which did not adapt the process approach, base upon functions. In this solution activities are not coordinated and each function is performed following its own procedures. This solution is not rationally justified and frequently increases the costs. It is adapted, however, to fulfill the management board ambitions and to satisfy the needs of the company. A functional system needs extensive supervision and control, creates fixed hierarchical structure and extensive bureaucracy, which generate costs.

A functional organization operates (Fig.6) as the goals for single function are defined. In practice, the same actions are performed many times but they do not bring any new value to the work. There is no coordination between single functions and partially existing processes.



Source: H.J. Schmelzer, W. Sesselmann, Geschaftsprozessmanagement…, cit, p. 47.

Fig. 6. Functional and process organization

Managing every single activity (with a particular focus on a given functional departments) is not comprehensive. In process organization the goals are defined for processes, where the emphasis is put on creating value, the way and quality of performance and coordination of functions and the work of individual teams.

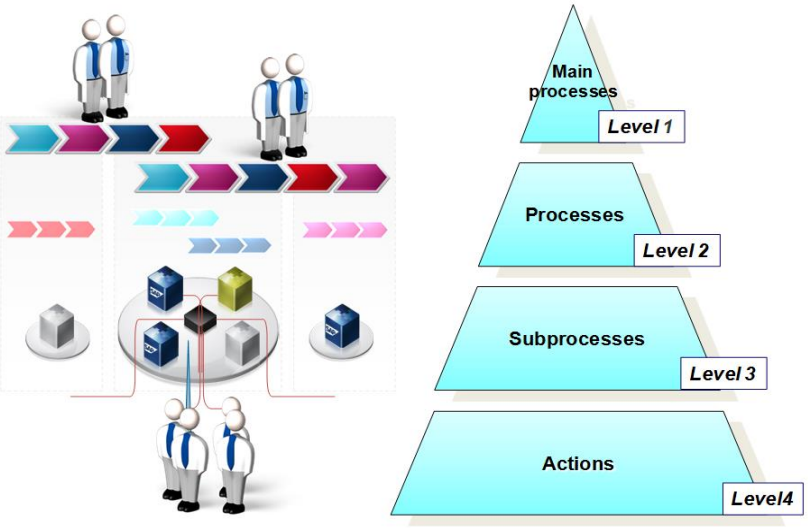
The process maps orientate the system to satisfy the needs of a client (recipient)[13]. When designing the changes in the process approach, the key elements are: organization, people and process structure (architecture) (Fig.7). The process approach may be adapted through:

- one-person command,
- fast one-person decisions,
- one -person responsibility,
- division of work according to competences and position.

Nowadays, information technology is a great help for adapting process solutions and introducing automatization of operational and office tasks in a modern, innovative way. Information technology facilitates modeling, organizing, simulating and analyzing and process management. **The most benefits from implementing IT can be**

[13] Ibidem, pp. 41-42.

gained by introducing radical, thought-over organizational changes. These changes are not about introducing new IT system or computerizing processes. Neither should they commence before processes are clearly defined in a new dynamic surrounding. Information technology can initiate changes of processes in an organization, yet the most beneficial would be in-depth remodeling of processes. Only such approach may bring the best economic effect[14].



Source: J. Kuck, Nowoczesne technologie..., cit., p. 45.

Fig. 7. Levels of process architecture

The success of process oriented projects in an organization, institution or company depends on introduction of the planned changes and overcoming many obstacles and barriers. Generally, they include: the workers' reluctance to changes, lack of qualifications, information techniques, general strategy of informatization, defined processes and the need to include them in the existing organizational structures and systems. Only after making the workers familiar with the concept of process approach and with the benefits effecting from introduction of

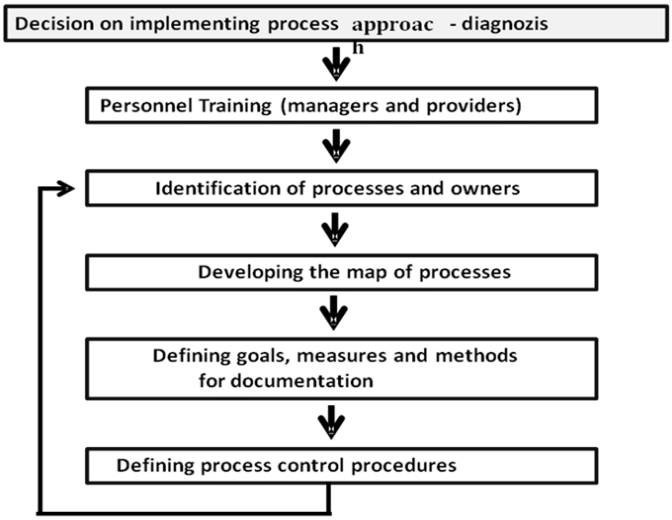
[14] Ibidem, p.43.

the pattern and eventually making them think in a process way, the process-based organization may be created.

If the workers in a given team take to the changes, they willingly model, define, analyze and introduce new processes. It is easier then, to stabilize the situation on a new level. Reaching a new level of changes in an organization does not eliminate the need for constant improvement of processes[15]. The described processes reflect the state of affairs in an organization at a given point of time. Organizations and institutions must constantly develop to prove competitive on a market. So, if they adapt the process approach the processes shall be constantly developed (modeled).

2. Identification and modeling of business processes

Process approach integrates time, quality and prompt completion of tasks, contributes to the increase in value (capacity) of an organization/institution. The process approach is implemented in stages (Fig.8) and concerns both, material and nonmaterial processes.



Source: S. Nowosielski, Podejście procesowe w organizacji, UE, Wrocław 2009, p. 60.

Fig. 8. Process approach implementation stages

[15] Ibidem.

The most important advantages of modeling process in an organization and institution are:

a) copying the current processes and the structure of their connections
b) presenting logical and time connections of activities in a process, facilitating identification of the following limitations.

3. ARIS Software

ARIS[16] of IDS Scheer is an integrated solution portfolio to support all phases in a lifecycle management: the strategy, design, implementation and controlling effectiveness of business processes. The concept of Architecture of Integrated Information Systems (ARIS) was first implemented in 1991 to streamline comprehensive modeling of integrated information systems. In 1993, ARIS-Toolset 1.0 was created and offered tools and methods to develop and implement IT systems. In subsequent years the software was still developed. In 2003 IDS Scheer company initiated strategic cooperation with SAP[17] to develop process tools to implement SAP software. This cooperation is a logic consequence of

[16] **ARIS** is a concept, set of methods and tools for planning, designing, implementing and controlling business projects in an organization. Theoretical and methodological basis were worked out by professor A.W. Scheer in cooperation with partners and co-workers. A. W. Scheer is a German Professor in business administration and business information at the Saarland University, and founder and director of IDS Scheer AG, a major IT service and software company.

[17] **SAP AG** (*Systems Applications and Products in Data Processing*)founded in 1972, headquartered in Walldorf, Germany, with locations in more than 130 countries, SAP AG is the world leader in enterprise software and software-related services. It provides all business sectors with ERP solutions, the latest version of SAP R/3 was *Enterprise 4.70 Extension Set 2.00*. Recently it offered new products based on SAP NetWeaver Platform; SAP ERP 6.0.; SAP Business Information Warehouse (SAP BW) now SAP BI; SAP Supply Chain Management SAP SCM (previously APO – Advanced Planner and Optimizer); SAP Supply Chain Event Management SAP SCEM – defines characteristic aspects of business processes like transport and orders, it is a part of SCM and cannot be implemented without it; SAP Supplier Relationship Management (SAP SRM); SAP Customer Relationship Management (SAP CRM); SAP Master Data Management (SAP MDN – previously PLM Product Lifecycle Management); SAP Exchange infrastructure (SAP XI); SAP Enterprise Portal (SAP EP); SAP Human Capital Management (SAP HCM).

connections between methods and tools of IDS for implementation of SAP software.

More and more organizations, institutions and companies use ARIS tools and IDS Scheer implementation skills. Some clients use ARIS tools mainly for restructuring and reorganizing their structures of organization and activities. Others apply IDS Scheer tools and competencies to implement SAP software which at present is a world standard for solutions in logistics management. ARIS tools can be used for graphic design and processing descriptions of complex connections between components of management systems, information systems and institutions.

Particularly, ARIS facilitates designing and testing a coherent project of a new process-based organizational structure. ARIS helps also to evaluate influence of changes in activities and responsibilities on a given position.

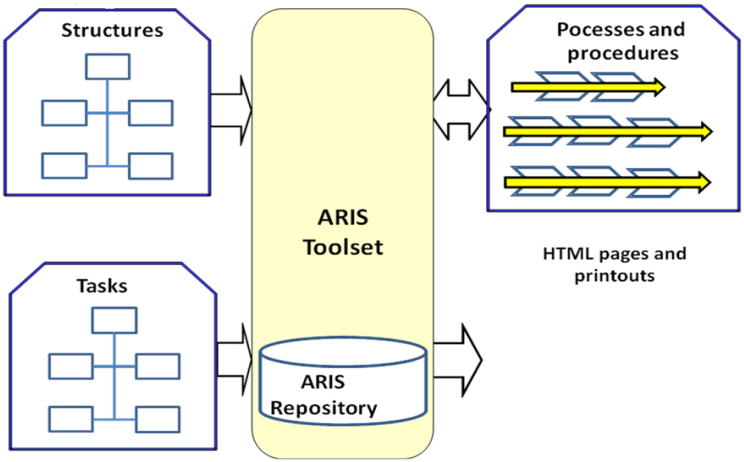
ARIS tools and IDS Scheer implementation competencies involve informatization enterprises with SAP software. ARIS tools are used to analyze the existing processes, develop business concepts (Business Blueprint), define the range of configuration, train and implement documentation. IDS Scheer company participates in creating comprehensive concept for SAP systems integration and other applications with SAP PLM component (Product Lifecycle Management) for the SALE project (Single Army Logistics Enterprise).

ARIS tools are also used for graphic description of processes and systems, characterizing components and single connections and data processing (Fig.9).

In ARIS system the data of diagrams and objects on them are stored in repositories, which is a basic difference between the tools and graphic programs of that standard. The logic of ARIS tools:

- Diagrams describe structures and their elements, e.g.: organizational structure and its elements and activities which are arranged hierarchically. Every activity can be characterized in words, giving priorities, etc:
- Data about diagrams and elements and structures are collected in ARIS repository i.e. the reference database,

- Introduced data may be used to create new diagrams, e.g.: maps of processes. Every map shows the order of activities and the personnel in charge. Units and activities are retrieved from the repository and they do not need to be re-entered,
- The diagram data is processed by scripts created with ARIS programming toolset. Data about objects and connections may be collected from many diagrams and presented in the form of reports, charts or the Internet pages.



Source: The materials by IDS Scheer.

Fig. 9 ARIS tools for analysis and project

ARIS tools included into ARIS Process Platform offer a wide choice of diagrams and objects. At the same time, within one project the number of diagrams available may be restricted down to several, most important ones. The same rule works for symbols, connections and attributes. The most often used diagrams are:

- Diagram of the organizational structure,
- Diagram of the added value chain,
- Diagram of the Event-driven Process Chain (eEPC).

The set of diagrams helps to describe any newly designed organization in terms of organizational structures and business processes. While

building diagrams in a repository at the same time the connections between their elements and diagrams are created. This data is accessible in profiles of diagrams and objects. ARIS graphic language was developed by professor Scheer especially for describing dynamic of processes. The diagrams of Event-driven Process Chain (eEPC) are created in this language. They show time connections between performed activities in a process. The basic elements of the language are:

- Activities (functions),
- Events preceding activities (their conditions) and the effects (outcome of the activities),
- Connections and logic operators,
- Activity performers (from the chart of the organizational structure),
- Software and documents.

ARIS process tools are used by many organizations, institutions and companies. Process identification and description is the first step to adapt these tools. For example, in a material base identifying economic events, like material procurement, circulation can be grouped in the following processes[18]:

The subsequent year the new information about adapted software, data base and technical infrastructure is introduced to ARIS program. The software is connected to the supporting activities. This way, full architecture of an organization, institution or company is built. It describes single connections of elements in these structures, together with mechanisms of functioning. The description of all systems, processes and structures of organization, data bases and their connections is easy to modify. For example, thanks to the repository and ARIS mechanisms the change of the name for any element needs only one operation. All diagrams where the changed element exists will be modified automatically. It is possible as ARIS stores the definition of an element (object) with its name and information about its occurrence in the diagrams separately. The architecture allows for

[18] *Obieg dokumentów materiałowych oraz rejestracja zdarzeń gospodarczych w rejonowej bazie materiałowej*, SGWP, GZL-P4, W-wa 2005, p. 2.

immediate evaluation of the influence of changes on any element (object), e.g.: process or interface.

ARIS offers also the preview of connections of every element with other ones, including diagrams and objects in which this element occurs. For the more complex analysis of elements with indirect connections, ARIS offers a toolset and the programming language to develop more cross-sectional reports.

Concluding:

This work presents the basic solutions (ARIS tools) for process approach and for modeling processes in logistics, finance and HR. The main emphasis was put on the practical aspect which may set an example for all who wish to get familiar with how to define and describe processes. Thus, the hypothesis that the commercial market offers the solutions possible to adapt in the defense and security, has been positively verified. These solutions are ARIS toolset of IDS Scheer.

The aim of this paper is to popularize the process approach and the need for process modeling with the right methods and tools. Process implementation of SAP software has been successfully adapted by many organizations, institutions for IT projects when building the Integrated (Multilevel) IT Systems for Logistics, Finance and HR.

1. Bitkowska. Zarządzanie procesami biznesowymi w przedsiębiorstwie, Vizja Prest, Warszawa 2009.
2. Gabryelczyk R., ARIS w modelowaniu procesów biznesu, Centrum Doradztwa i Informatyki, Difin, Warszawa 2006.
3. Emser T., The BMP Pyramid: People, Process, and Technology,
4. Kaplan R., Murdock L., Core Process Reengineering, McKinsey Quarterly 2», Summer 1991.
5. Kasprzyk T., Organizacja zorientowana na proces biznesu – modelowanie referencyjne [w:] tenże (red.), Modele referencyjne w zarządzaniu procesami biznesu, Difin, Warszawa 2005.
6. Klonowski Z.J., Systemy informatyczne zarządzania przedsiębiorstwem. Modele rozwoju, właściwości funkcjonalne. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.
7. Kuck J., Procesowa organizacja organizacji, instytucji, przedsiębiorstw oraz firm [w:] Z. Grzywny, Bezpieczeństwo w

procesach globalizacji – dziś i jutro, t. I, Wyższa Szkoła Zarządzania Marketingowego i Języków Obcych, Katowice 2013.
8. Kuck J., Nowoczesne technologie w logistyce, AON, Warszawa 2013
9. Kuck J.. Nowoczesność, efektywność o bezpieczeństwo współczesnej logistyki, AON, Warszawa 2015.
10. Kuck J.. Modern IT solution for logistics, Lviv Galician Publishers, Ltd 2015.
11. Kreuz W., Transformation the Enterprise, Die nächste Generation des Business Process Eingineering, [w:] M. Nippa, A. Picot, Prozeßmanagement und Reengineering, Campus Verlag, Frakfurt–New York 1996.
12. Nowosielski S., Podejście procesowe w organizacji, UE, Wrocław 2009.
13. Schmelzer H.J., Sesselmann W., Geschäftsprozessmanagement in der Praxis, Carl Hanser, München–Wien 2003.
14. Suchorzewska A., Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, Helion, Gliwice 2004.

Identification of products as the foundation of information systems operating in defense and security

Kuck Jerzy, Grzegorz,

Doctor of military science,
specialization in management of information systems

Managing capacity in organizations and institutions in the defense and security effectively is possible only with adequate information about its quantity, quality and value. **This idea gave reason for analyzing the product identification system, which is a base of the IT systems in the defense and security**. The paper shows that present identification systems do not meet expectations of the implemented integrated multilevel IT systems for logistics, finance and HR. The analysis is the basis for presentation of the solutions which facilitate identification of products for the defense and security. This solution uses the latest IT technologies including SAP toolset.

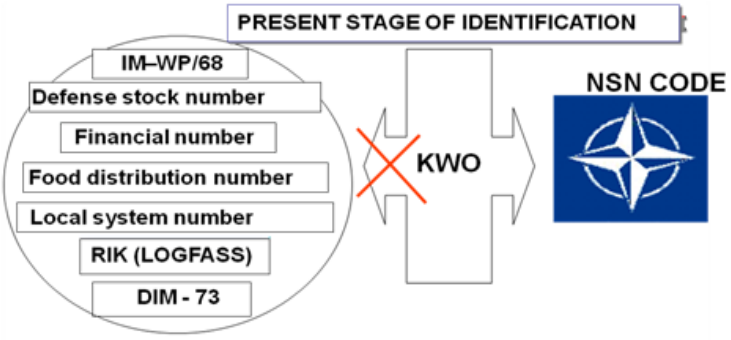
1. Division and typology of product identification

There was no comprehensive standardization. Different military and local systems with different structures and range of information were

used, e.g.: arms and military equipment list, munitions list, food lists, list in the accountancy department and others created for given branches or type of procurement. They had different hierarchical structure and were composed of 3-15 figures (Fig.1) which effected in the following:

- Multiplied identification of the same products with different symbols,
- Different products with the same symbol,
- No comprehensive database with universal stock number in IT systems.

The variety of coding solutions indicates there was no coordination of systems operating in defense and security. Changing of status quo and introducing the universal stock number for all the organizations and institutions would facilitate effective performance, e.g.: fighting natural disasters.



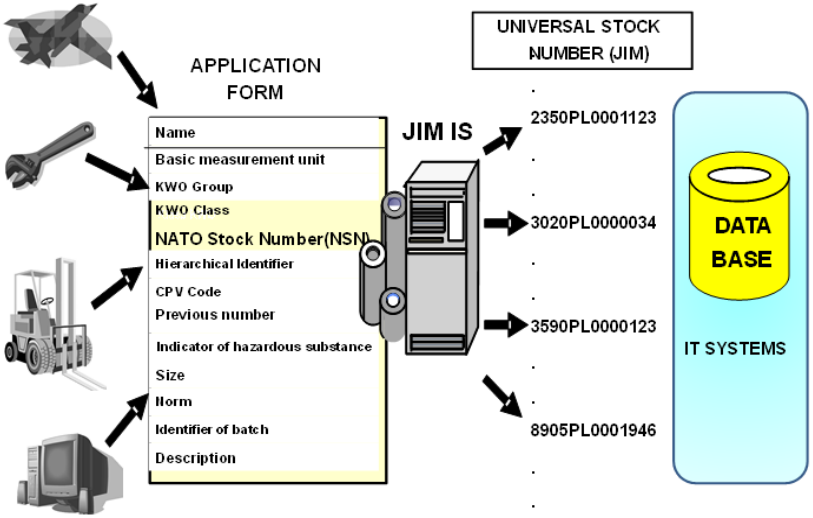
Source: J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013 p. 136.

Figure 1. Present stage of identification

The solution would be the uniform system of identfication (Jednolity Indeks Materiałowy , the Universal Stock Number) with Klasyfikator Wyrobów Obronnych[19] (KWO Identifier for Defense Products).

[19] Rozporządzenie Rady Ministrów z 29 stycznia 1999 r. w sprawie Klasyfikacji Wyrobów Obronnych (KWO), DzU nr 26, poz. 231 ze zm.

The effective management of military assets depends on professional knowledge of the quantity, quality and value of the property. Unified quality-quantity-value identification and material-financial planning based on the integrated IT systems needs **reliable system of identification and classification of all assets approval for use and on stock**. Implementation of this system (Fig.2) would foster proper operation of all systems: planning, inventory, reporting in the operating in defense and security.



Source: J. Kuck, Nowoczesne technologie w logistyce, AON, Warszawa 2013, p. 136.

Fig. 2. The concept of product identification

The basic goal of the Universal Stock Number (JIM) was to provide efficient solution for universal and clear identification of defense products supported by SAP Platform R/3. Implementation of this system facilitated collection of information about all assets used and planned to be used in defense and security.

It was assumed that the system would be a national source of information about the defense products available for all organizational units of operating in defense and security, producers and suppliers and other business institutions.

It was expected that consistent implementation of JIM would considerably accelerate computerization and implementation of the Integrated Multilevel IT System for Logistics, Finance and HR. This application shortened the circulation of sources information and decisions at all organizational levels. As the end-result it will be possible to provide:

- Reliable information about all assets of the Ministry of National Defense, their quality, quantity and value in a real time,
- Updating, complete and more reliable information for evaluation, planning and decision-making processes,
- Safe electronic interchange of information and reporting,
- Tools for monitoring budget spending and unification of material-financial planning process,
- Single, integrated quantity-quality-value inventory to monitor spending in logistics and finance,
- Efficiency of logistics support in the transition period from the command and control system in time of peace to the one in time of war; mobilization and operational development of forces and operations abroad,
- Complete inventory of the organizations and institutions assets and the data base for all IT systems supporting management;
- Access to information about the created entries and codes for producers and suppliers and other business institutions,
- Interoperability between different terminology systems / standards bodies in a national economy, NATO and EU,
- The Central Data Base (CBD) about the assets, logistics resources, introducing bar codes and product tracing system.

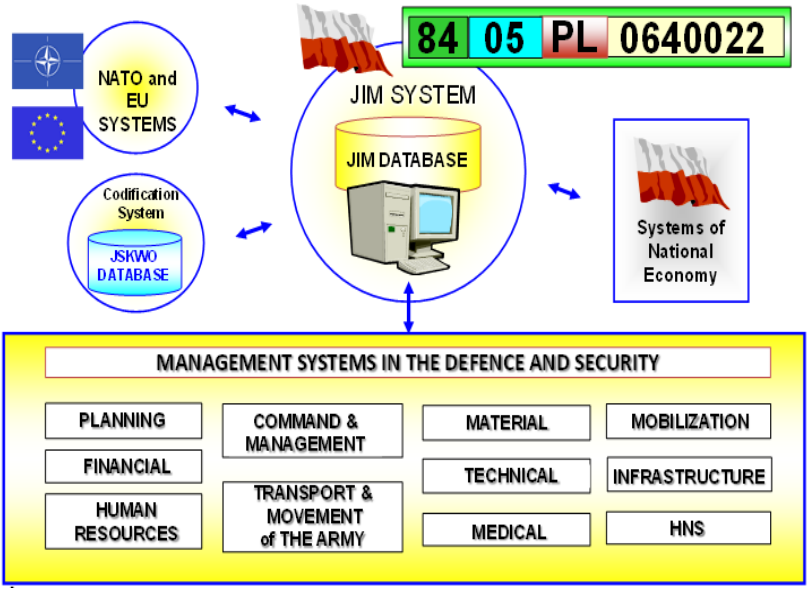
2. Characteristics of JIM

JIM created and developed by Inspektorat Wsparcia (note: the Inspectorate for Support of the Armed Forces) and administered by the IT Depatment will streamline the management of assets in the national system. Identification and classification with JIM will create the basis for quantity-quality-value inventory and necessary stock-record of defense products. After implementing the integrated, multilevel IT system with JIM it will be possible to identify those

products which because of their *innovative support position* will be codified according to NCS in the first place[20].

At present the Universal Stock Number is the only complete source of information about the defense products. JIM Data base organizes, identifies and classifies products and at the same time serves as a platform which integrates all systems of managing the defense products. The internal and external (operating) environment of JIM system is presented in Fig. 3.

The internal environment of JIM system is the Ministry of National Defense (MON) using the universal, standardized information from SI JIM data base in all processes supporting the command and control of the armed forces in time of peace, crisis and war.



Źródło: A. Skierkowski, J. Kuck, W. Wiszniewski, Identyfikacja wyrobów obronnych, «Myśl Wojskowa» nr 2/2006, s. 103.

Rys 3. Otoczenie systemu Jednolitego Indeksu Materiałowego

[20] J. Kuck, *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015, s. 71.

The external environment of that system is the national industry using the sources of the JIM data base for selling, purchasing items for the army. Moreover, JIM can support codification for NATO and EU systems.

If JIM system is introduced in other branches of the defense and security services of the organizations and institutions operating in defense and security it enables effective information exchange and sharing for common operations in time of natural disasters. Judging by experience and examples, the efficient performance of the services may save lives of many.

3. Organizational-functional Structure of the Universal Stock Number (JIM)

One of the basic principles for the concept of JIM is the coordinated cooperation of single system users. The role the users play in JIM system is defined by the functional structure of the following elements:

1) **The administrative and management bodies** are:

Inspektorat Wsparcia (note: the Inspectorate for Support) which manages works on identification system and Telecommunication and IT Department which administers the IT system for JIM IS.

The task of the administrative and management bodies are:

- appointment of personnel responsible for IT operations,
- issuing single, unique identification number,
- managing database,
- approving applications,
- generating, maintaining and distributing,
- removing defined items from the central data base,
- staff training.

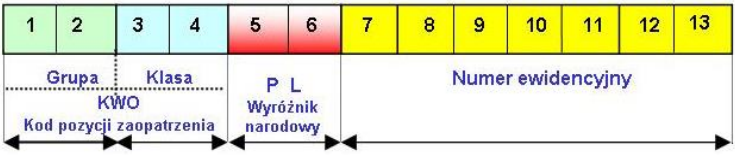
2) **The executive body** – gestor – identifies the needs for issuing JIM and manages data. The tasks are:

- Applying for JIM,
- Modifying data about items in the JIM central database,
- Applying for removal of items from JIM central database,

- Training JIM system users in the subordinate organizational units.

3) **The user (recipient)** – of the organizations and institutions operating in defense and security and the national industry using JIM pursuant to their legal rights and needs.

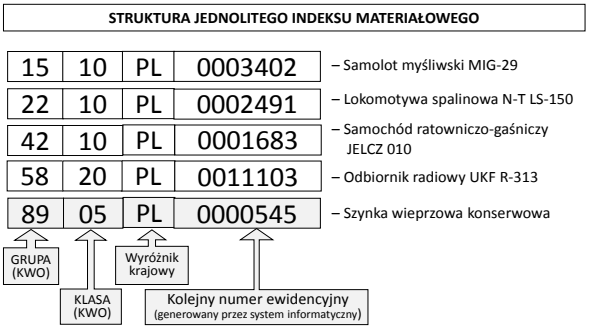
For the efficient JIM system it is important to provide the system users with equipment and software and connect them to network. The JIM system classifies item names by group and class, under the provisions of the Regulation of the Council of Ministers of 29 January 1999 on the Classification of the Defense Products (KWO) and STANAG 3150 and 3151. The JIM system has a hierarchical 13-digit structure (Fig.4).



Source: J. Kuck, Nowoczesne technologie..., cit., p. 137.

Figure 4. Structure of the Universal Stock Number

Universal Stock Number of a single defense product is a sequence of 13 alphanumeric digits which uniquely identify a given product and differentiate it from all others. The Universal Stock Number for single products is presented in Figure 5.



Source: A. Skierkowski, J. Kuck, W. Wiszniewski, Identyfikacja wyrobów..., cit.., p. 100.

Fig.5. The Universal Stock Number for Single Products

4. The procedures for issuing the Universal Stock Number

The procedures of issuing the Universal Stock Number are divided into three stages:

Stage I – after the gestor's application to issue the Universal Stock Number, it is prepared, the product is identified on a structural level (in a vertical pattern) of the hierarchical identifier.

The hierarchical identifier is a method of grouping, formalized by a gestor, in order to:

- Define norms and payments due,
- Provide overall lists at different organizational levels of the Ministry of National Defense (MON),
- Prepare reports and analysis (data aggregation)[21].

In the JIM IT system there are eight hierarchical levels (to 18 characters with 4-2-2-2-2-2-2-2 structure) which identify an item according to other gestor's demands. The exemplary classification is presented in Figure 6.

Source: A. Skierkowski, J. Kuck, W. Wiszniewski, Identyfikacja wyrobów..., cit., p. 106.

Fig.6. The Structure of the Hierarchical Identifier – the example.

[21] J. Kuck, *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015, s. 74.

The first level of the identifier refers to the group and class of KWO. The next levels include details of a given group of items. The Universal Stock Number works properly if it is assigned to the right node of the hierarchical identifier.

Stage II – identification of the item and preparation of the application for issuing JIM for the item by the executive body, i.e. gestor means defining:

- the item in a given group and class of KWO,
- the name of the item,
- the full name and other features of the item,
- the basic measurement unit,
- supplier,
- the hierarchical identifier (identifying the nod),
- the classifier for a package,
- NSN if assigned,
- additional technical and functional parameters of the item (at the gestor's request):
  - reference to another identification systems (current symbol/number),
  - CPV code,
  - Indicator of risk material,
  - Exchange,
  - Standards (international, European, Polish, defense, industry),
  - Catalogue symbol,
  - Package.

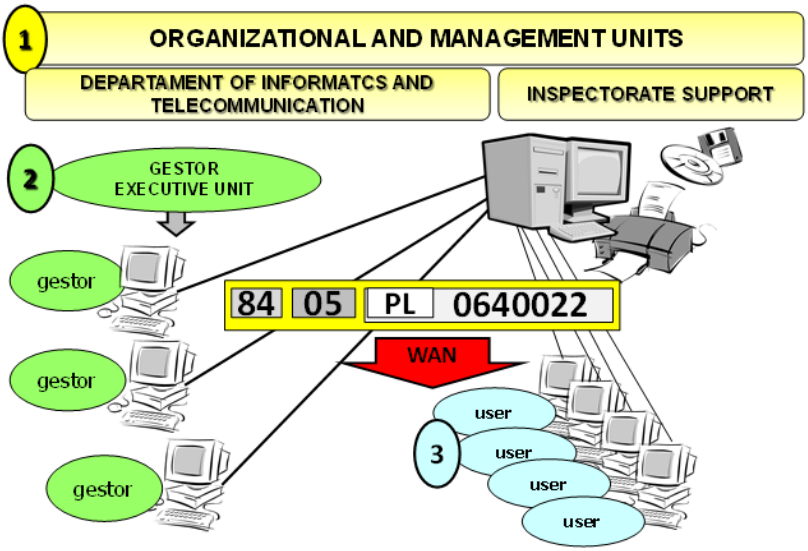
Stage III – issuing the JIM by the administrative and management body, i.e. Inspektorat Wsparcia involves:

- Registering the application,
- Verifying the description of the item,
- Issuing the JIM (by IT system),
- Entering new information to the JIM IS central database.

Activities at all stages are supported by the IT system of JIM. The applications use SAP platform R/3 which allows for distant generation and approval of the application for identification as well as distant access to JIM database. The JIM IT system is presented in Figure 8.

Source: J. Kuck, Nowoczesne technologie..., cit., p. 145.

Fig.7. Strukture of Hieraarchical Identifier – an example



Source: J. Kuck, Nowoczesne technologie..., p. 147.

Fig.8. The JIM IT system

The basic and most popular form of distribution is by distant access to JIM database, administered by Telecommunication and IT Department. JIM IS database works according to the following principles:

- Data about items previously prepared and verified by gestor are entered in real time (with extended network),
- The data are verified and controlled by Ispektorat Wsparcia,
- JIM is distributed cyclically or on demand of Inspektorat Wsparcia,

Distribution of JIM ensures effective access to information about items in JIM IS database for the authorized users. This solution facilitates:

- Electronic distribution of JIM IS database,
- Traditional (paper)documentation with the content of JIM IS database,
- Distant access to JIM data base in the network.

Concluding: The increasing complexity and speed of business operations requires immediate access to data to gain the demanded competitive advantage. Automation of the identification of products and in the future also services should foster implementation of the integrated multilevel IT systems for logistics, finance and HR in the defense and security. This approach to defense and security meet the needs of the 21st century.

1. Rozporządzenie Rady Ministrów z 29 stycznia 1999 r. w sprawie Klasyfikacji Wyrobów Obronnych (KWO), DzU nr 26, poz. 231 ze zm.
2. Kuck J., Nowoczesne technologie w logistyce, AON, Warszawa 2013
3. Kuck J., *Modern IT solution for logistics*, Lviv Galician Publishers, Ltd 2015.
4. A. Skierkowski, J. Kuck, W. Wiszniewski, *Identyfikacja wyrobów obronnych*, «Myśl Wojskowa» nr 2/2006.

Cybersecurity – the most popular methods of cyberattacks

Pieronkiewicz Jarosław,

IT Expert

Abstract: The new technologies gave way to creation of cyberspace and a human activity in that area resulted in new threats and so

necessity for cybersecurity measures. The paper presents the most popular methods of cyberattacks and the ways to protect systems. The presented examples and statistics of cyberattacks can be a real proof of root case analysis.

New technologies contributed to an increasing role of information as a strategic asset in all sectors: business, social and military. They also created the fifth dimension of any human activity – cyberspace, where states, societies, businesses and individuals face new challenges and threats. Cybersecurity plays a key role in strategic plans for state security.

The aim of the paper is to present the most popular methods of cyberattacks and the ways to protect systems. The examples and statistics presented should bring us closer to the scale of threats and risks of attacks in cyberspace.

In addition, in this article, we can get acquainted with the data on expenses incurred due to preventive action as well as mitigate of the risk the emergence of a threat. Among many other definitions of cybersecurity the NATO handbooks provide with the following one: [1].

«The concept of 'national cyber security' that is seemingly emerging by default, rather than by intent, addresses a more modest set of requirements than notions of cyber power. While military capabilities and international power-projection still play a role, the view is often more orientated towards managing the cyber risks

that a nation faces, rather than proactively trying to exploit those cyber risks in advancing its global power».

According to that definition we can understand cybersecurity is something more than only computer system and it is mainly related to protection of computer systems.

In this article I would like to focus on IT aspects of cybersecurity. The statistics from 2017 presented below show the scale and impact of attacks and significance of state activities in the area of cybersecurity.

Trends from the 2017 cyberattacks:

- **Motivation behind attacks** is mainly Cyber Crime «there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:
  - Advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software;
  - Cyber-enabled crime – many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism» [2].

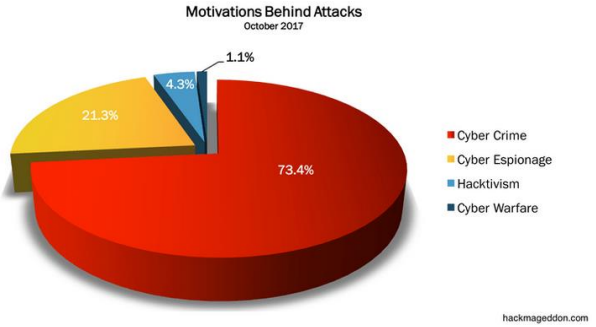


Fig.1. Motivations behind attacks.

Source: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

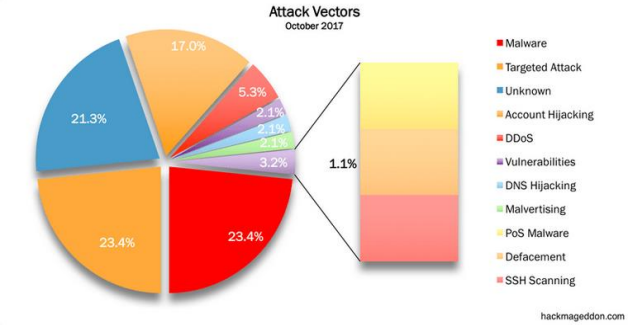


Fig. 2. Attack vectors

Source: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

- **Attack Vectors** - An attack vector is a path or means by which an attacker can obtain an access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors allow attackers to exploit system vulnerabilities, including the human element [3]. The chart presented below shows that **Malware is** on the top of attacks per type (more details about malware will be presented in next section).
- **Distribution of Targets** – on the top 3 of this category in October 2017 there were sectors: Industry, Single Individuals and Government.

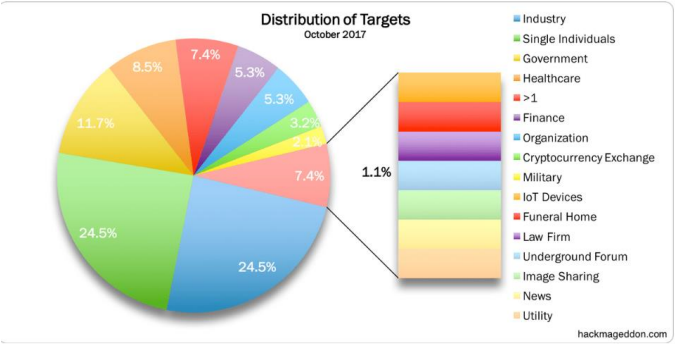


Fig.3. Distribution of targets

Source: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Numbers and facts:

- **Cyber crime damage costs around $6 trillion annually by 2021.** It all begins and ends with cyber crime. The cybersecurity community and major media estimated that cyber crime damages will cost the world $6 trillion annually by 2021.
- **Cybersecurity spending to exceed $1 trillion from 2017 to 2021. According to information provided by Gartner cyber crime costs achieved around** $86.4 billion in 2017
- **Cyber crime will more than triple the number cybersecurity jobs, It is expected that it reach 3.5 million by 2021.**
- **Human attack surface is going to reach 6 billion people by 2022.** There are 3.8 billion internet users in 2017 around 51% of the

world's population and it is growing very fast comparing to 2 billion in 2015. Cybersecurity Ventures expects that there will be 6 billion internet users by 2022 and it will reach 75% of whole world population.

- **Global ransomware damage costs are estimated to exceed $5 billion in 2017. In 2015 the total cost was** $325 million so in fact it increased 15 times [4].

There is the possibility to observe cyberattacks on-line on the Norsecorp web page :http://map.norsecorp.com/#/. On this page we can find the word map with the information about attack origins, attack types, attack targets and live attacks.

To summarize, nowadays we are observing a rapid increase in cost related to ransomware campaigns. There are also other types of programs used by Cyberattackers. Those programs can be categorized in four main groups: **worms, viruses, trojans, ransomware** and cybeattackers design it to infect computers and mobile devices. The common definition to describe all these programs is **malware**. Malware is a combination of words **manicous** and **software**. Cyberattackers are trying to install these types of software on computers or mobile devices to control them. Once it has been installed the attackers can use malware to spy your activities, steal your passwords and files or use your system to attack other users in network. Malware can infect any device no matter what operating system is running on it.

One of the most popular malware is keylogger. Attacker can use keylogger software to capture everything what have been typed on your keyboard including your passwords, usernames, email messages.

The next group of malware is ransomware. When ransomware attack your computer it encrypts all your files and deny access to them. Recently we have had a lot of ransomware attacks.

The top 5 worst ransomware attacks of 2017:

- NotPetya. NotPetya started as a fake Ukranian tax software update and infected hundreds of thousands of computers in more than 100 countries. It caused a lot of issues for the business

sector in the US. One of examples can be the attack that cost pharmaceutical giant Merck more than $300 million in Q3.

- WannaCry has been one of the most devastating ransomware attacks in history, affecting several hundred thousand machines located in banks, law enforcement agencies, and other infrastructure.
- Locky is currently on the top in terms of ransomware and across all malware families
- CrySis - it can be installed manually using Remote Desktop Services. Mainly it has been active in Australia and New Zealand.
- Nemucod has been active since 2015, and usually has been propagated in the form of a phishing email that appears to be a shipping invoice [5].
- There are many methods to protect against malware. Mainly used are:
- Policies and user training.
- Scanners or signature scanners searching for strings whose presence is characteristic of a known virus.
- Activity monitor which can perform operations very similar to an automated form of traditional auditing.
- Heuristic Scanners which can perform intelligent analysis of unknown code [6].

Unfortunately even if we install all above mentioned security devices and software we cannot avoid mistakes caused by human factor.

The next type of attack is related to human nature and it is called Social Engineering.

«Social engineering is a way that cybercriminals use human-to-human interaction in order get the user to divulge sensitive information. Since social engineering is based on human nature and emotional reactions, there are many ways that attackers can try to trick you- online and offline» [8].

One of the famous hackers who is familiar with these methods is Kevin D. Mitnick. In his book «The Art of Deception» he described methods of social engineering which has been successfully used during real attacks. In the Chapter 4 we can find a bullet: «TRUST:

THE KEY TO DECEPTION» and Kevin said that: «The e TRUST: THE A KEY TO DECEPTION», where Kevin said that: «more a social engineer can make his contact seem like business as usual, the more he allays suspicion. When people don't have a reason to be suspicious, it's easy for a social engineer to gain their trust. Once he's got your trust, the drawbridge is lowered and the castle door thrown open so he can enter and take whatever information he wants» [8].

In the above mentioned quotations Kevin as well as other hackers confirmed that human factor is truly security's weakest point. In this book we also can find description of The Social Engineering cycle. It consists of four elements:

- **Research** means collecting information that is usually widely available as annual reports, marketing brochures, press clippings and the content of the website.
- **Developing rapport and trust** – at this stage use of insider information, misrepresenting identity, need for help, or authority.
- **Exploiting trust** - asking potential victim for information or an action, manipulate victim to ask attacker for help.
- **Utilize information** - if obtained information is only a step to final goal, attacker returns to earlier steps in cycle until goal is reached [8].

Nowadays, we are facing sophisticated methods of cybersecurity attacks: cybercrimes, malicious software and social engineering. Each of those methods could be a potential threat to every user in the global network. Along with the development of technology we can expect more unidentified attacks in future.

---

5. National Cyber Security Framework Manual - Alexander Klimburg, NATO.
6. Source:https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
7. http://searchsecurity.techtarget.com/definition/attack-vector).
8. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
9. https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

10. CISSP ISC2 Official Study Guide, Sybex, 7th ed. 2016
11. https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
12. Kevin D. Mitnick, «The Art of Deception», John Viley & Sons, USA, 2001.

РОЗДІЛ 2
НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ

Використання безкоштовних програмних засобів

Гавриш Олег Степанович,

викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Упровадження комп'ютера в сферу освіти стало початком революційного перетворення традиційних методів і технологій навчання та всієї галузі освіти. Важливу роль на цьому етапі, крім комп’ютерів, відіграють такі інформаційні комп’ютерні технології (ІКТ): телефонні засоби зв'язку, телебачення, космічні комунікації, що переважно застосовуються в процесі управління процесом навчання і системах додаткового навчання.

Новим етапом глобальної технологізації передових країн стала поява сучасних телекомунікаційних мереж та їх інтеграція з інформаційними технологіями, тобто поява ІКТ. Вони стали основою для створення небаченої інфосфери, оскільки об'єднання комп'ютерних систем і глобальних телекомунікаційних мереж зробило можливим створення і розвиток планетарної інфраструктури, що зв'язує нині все людство.

Освітні технології (ОТ) є одним із головних елементів системи освіти, оскільки вони безпосередньо спрямовані на досягнення головних цілей: навчання і виховання. Під ОТ розуміють як реалізацію навчальних планів і навчальних програм, так і передавання студенту системи знань, а також використання методів і засобів для створення, збирання, передавання, збереження і оброблення інформації в конкретній галузі. Наука накопичила величез-

ний досвід з передавання знань від викладача до студента, створення технологій освіти і навчання, а також з побудови їх моделей.

ІКТ здійснюють активний вплив на процес навчання і виховання студентів, оскільки змінюють схему передавання знань і методи навчання. Разом з тим, упровадження ІКТ у систему освіти не тільки впливає на освітні технології, а й уводить до процесу освіти нові. Вони пов'язані із застосуванням комп'ютерів і телекомунікацій, спеціального устаткування, програмних та аппаратних засобів, систем обробки інформації. Вони пов'язані також зі створенням нових засобів навчання і збереження знань, до яких належать електронні підручники і мультимедіа; електронні бібліотеки й архіви, глобальні та локальні освітні мережі; інформаційно-пошукові та інформаційно-довідкові системи.

Але постає питання правомірності використання багатьох ліцензійних програм в освітньому процесі. Проблеми фінансування освіти України вимагають делікатно підходити до цієї проблеми та розробляти організаційні заходи щодо легалізації програмного забезпечення в освітньому процесі, а саме застосувати простий алгоритм:

- визначити вимоги до програмного забезпечення, що використовується;
- заборонити незаконні інсталяції нового програмного забезпечення;
- зобов’язати придбання ліцензійного програмного забезпечення під час закупівлі комп`ютерної техніки;
- організувати в централізованому порядку проведення торгів із закупівлі ліцензійного програмного забезпечення;
- розробити план переходу на ліцензійне локалізоване програмне забезпечення;
- використовувати безкоштовні аналоги комерційного програмного забезпечення; [1]

Але у безкоштовного програмного забезпечення є не тільки позитивні якості але й негативні.

Характеристики безкоштовних ліцензій: [2]

1. Apache Software License2. Ліцензія BSD

3. GNU General Public License
4. Ліцензії MIT
5. Mozilla Public License
6. Консорціум Всесвітньої мережі

Apache Software License – ліцензія на вільне програмне забезпечення Apache Software Foundation.

«Плюси»

- право використовувати програмне забезпечення для будь-яких цілей, вільно поширювати, змінювати, і поширювати змінені копії.
- не ставить умовою незмінність ліцензії розповсюдження програмного забезпечення.
- не наполягає навіть на збереженні його безкоштовного і відкритого статусу.
- сумісність з GPL.

«Мінуси»

- інформувати Apache про факт використання вихідного коду, ліцензованого під ліцензією Apache.
- при поширенні програмного забезпечення необхідно помістити файли LICENSE і NOTICE в кореневу директорію.

Ліцензія BSD. Програмна ліцензія університету Берклі – це ліцензійна угода, вперше застосована для поширення UNIX-подібних операційних систем BSD.

«Плюси»

- одна з найпопулярніших ліцензій для вільного програмного забезпечення і використовуються для багатьох програм.
- дозволяється повторне поширення і використання як у вигляді вихідного коду, так і в двійковій формі, зі змінами або без.
- BSD допускає комерційне використання ПЗ.
- багато ліцензій походять від BSD або вони аналогічні їй.
- в порівнянні з іншими поширеними ліцензіями на вільне програмне забезпечення ліцензія BSD накладає менше обмежень на користувача.

«Мінуси»

- права на вихідний дистрибутив BSD офіційно належать «університету Каліфорнії».

GNU General Public License – ліцензія на вільне програмне забезпечення, створена в рамках проекту GNU в 1988 р

«Плюси»

- ліцензуючи роботу на умовах GNU GPL, автор не відмовляється від права вважатися її автором.
- свободу запуску програми, з будь-якою метою.
- свободу вивчення того, як програма працює, і її модифікації
- свободу поширення копій.
- свободу поліпшення програми, і випуску поліпшень в публічний доступ.

«Мінуси»

- GNU GPL вимагає поширення з двійковими файлами (в тому числі незмінними) вихідного коду або письмового зобов'язання його надати.

Ліцензія MIT (англ. MIT License) – група ліцензій, розроблених Массачусетським технологічним інститутом для поширення вільного програмного забезпечення.

«Плюси»

- оскільки копірайт на дану ліцензію відсутній, інші групи мають право використовувати і змінювати програму для задоволення своїх цілей.
- явно говорить про права кінцевого користувача, включаючи права використання, копіювання, зміни, включення в інший вихідний код, публікації, поширення, субліцензування та / або продажу ліцензованого ПЗ.
- ліцензія вважається академічної ліцензією, тобто визнана придатною до використання в сфері наукових розробок.

«Мінуси»

- ліцензія MIT найбільше відповідає Ліцензії BSD.

Mozilla Public License (скорочено MPL) – одна з ліцензій на вільне програмне забезпечення. MPL містить в собі риси модифікованої ліцензії BSD і GNU General Public License.

«Плюси»

- MPL схвалена в якості відкритої ліцензії Open Source Initiative.
- адаптована іншими розробниками, особливо Sun Microsystems.

«Мінуси»

- вихідний код, скопійований або змінений під ліцензією MPL, повинен бути ліцензований за правилами MPL.
- Фонд вільного програмного забезпечення не рекомендує використовувати MPL в чистому вигляді, тобто без використання множинного ліцензування спільно з GPL або сумісної з нею ліцензією.

Консорціум Всесвітньої мережі (англ. World Wide Web Consortium, W3C) – організація, яка розробляє і впроваджує технологічні стандарти для Всесвітньої павутини.

«Плюси»

- мета W3C – допомогти комп'ютерним програмам досягти здатності до взаємодії в мережі.
- застосування єдиних стандартів в мережі.
- зробити мережу доступною для людей з обмеженими можливостями.
- рекомендації Консорціуму Всесвітньої павутини відкриті, тобто не захищені патентами і можуть впроваджуватися будь-якою людиною без всяких фінансових відрахувань консорціуму.
- рекомендації консорціуму побудовані таким чином, що часткове використання не порушує загальних стандартів.
- рекомендації W3C часто добре опрацьовані і деталізовані.
- більшість рекомендацій доступні для будь-яких категорій користувачів – від експертів-програмістів до початківців веб-майстрів.

- консорціум в цілому набагато більше уваги приділяє проектам з відкритим вихідним кодом.
- в даний час Консорціум є, мабуть, найавторитетнішою організацією в області стандартизації Всесвітньої павутини.

«Мінуси»

- будь-який стандарт W3C проходить 4 стадії узгодження (робочий проект, останнє скликання, можливі рекомендації і пропоновані рекомендації).

Отже при запровадженні безкоштовних аналогів програмного забезпечення в освітньому процесі можливо забезпечити максимальну продуктивність та економію і стимулювати студентів не користуватись піратським ПЗ.

1. Відповідальність за використання нелегального програмного забезпечення [Електронний ресурс]. – Режим доступу:
2. http://smeta.kharkov.ua/index.php?page=interesting7
3. Плюсы и минусы лицензий открытого ПО [Електронний ресурс]. – Режим доступу: https://geektimes.ru/post/69780/

Візуалізація експертного оцінювання якості програмного забезпечення з використанням полярних діаграм

Грицюк Юрій Іванович,

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

Бучковська Анастасія Ігорівна,

здобувач ступеня бакалавра Національного університету «Львівська політехніка»

Вступ. Якість програмного забезпечення (ПЗ) є істотною характеристикою в сфері інформаційних технологій. Особливості застосування моделей оцінювання якості ПЗ за визначеними

методиками розглянуто в роботах [3, 5]. Щодо застосування методів експертного оцінювання якості ПЗ, то ця проблема широко висвітлена в дослідженні [2]. У різних наукових джерелах процес експертного оцінювання якості ПЗ описано з урахуванням сфери компетентності експертів і за умови фіксації вагомостей кожного з експертів за відповідними критеріями [4]. У роботі [1] розглянуто методику отримання комплексної оцінки якості веб-матеріалів з використанням полярної системи координат. В даній роботі спробуємо розробити механізм візуалізації експертного оцінювання якості ПЗ з використанням полярних діаграм, де врахуємо різні вагові коефіцієнти критеріїв якості й вагомості самих експертів.

Подання оцінок експертів у вигляді полярних діаграм. Для реалізації можливості візуалізації статистики опитувань за деякими критеріями якості ПЗ [1] та отримання комплексної оцінки його якості спробуємо використати *полярні діаграми*[22].

Критерії оцінювання якості ПЗ подамо у вигляді векторів полярної системи координат, які утворюють полярну діаграму. Кожний такий вектор характеризується довжиною і кутом між ними. Вважатимемо, що довжина вектора відповідає кількісній оцінці якості ПЗ за відповідним критерієм. Максимальна довжина будь-якого з векторів відповідає 100-відсотковій якості ПЗ за відповідним критерієм. Зазвичай, довжина будь-якого з векторів становить тільки певну частку якості ПЗ.

Кут β між векторами характеризує величину впливу відповідного критерію на результат оцінювання якості ПЗ. Якщо всі критерії мають однаковий вплив, то вектори відповідних критеріїв будуть рівномірно розподілені у секторах полярної системи координат. Для шести критеріїв цей кут між усіма векторами становитиме $\beta = 2\pi/6$. У випадку неоднакового впливу критеріїв на результат оцінювання якості ПЗ кути між відповідними векторами потрібно визначити за формулою

[22] *Полярна діаграма* – графічний спосіб відображення багатовимірних даних у вигляді двовимірної діаграми з трьома або більшою кількістю змінних. Ці змінні подають у вигляді векторів, що мають спільний початок і певні кути нахилу до осі ординат.

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

де: $\tilde{W} = \{w_j, j = \overline{1, N}\}$ – ваговий коефіцієнт оцінки якості ПЗ за j-им критерієм його оцінювання; N – кількість критеріїв оцінювання якості ПЗ.

Якщо відкласти вектори-критерії у полярній системі координат і з'єднати отримані точки, то матимемо неправильний багатокутник, площа якого кількісно характеризуватиме якість ПЗ за всіма критеріями одночасно. Форма багатокутника дає якісну характеристику за вибраними критеріями. Якщо поділити площу неправильного багатокутника на площу круга, в якому знаходиться цей багатокутник, то отримаємо частку якості ПЗ, яку маємо на даний момент. Незаповнена площа круга – та частка якості ПЗ, яку ще потрібно досягти. Тут радіус круга має відповідати 100-відсотковій якості ПЗ за всіма критеріями його оцінювання.

Наведений вище механізм візуалізації комплексних оцінок якості ПЗ та їхнього подальшого аналізу є правомірним за певних умов, а саме: 1) критеріїв-векторів має бути не менше трьох; 2) область полярного сектора з кутом β_j має бути поділена навпіл векторами-критеріями.

Критерії оцінювання якості ПЗ та їхні вагові коефіцієнти, які надаються кожному з експертів. Довжини векторів у полярній системі координат мають дорівнювати значенням відповідних критеріїв оцінювання якості ПЗ, які потрібно визначити через експертні оцінки та ролі кожного з *респондентів*. Зазвичай, респонденти ПЗ є учасниками процесу оцінювання його якості, які можуть виступати в двох ролях – як відповідного *експерта*, так і безпосереднього *користувача*. Відмінність ролей у тому, що оцінка якості ПЗ, яку надає певний *експерт*, повинна мати більшу важливість в зазначеному процесі, ніж оцінка, яку надає *користувач*, позаяк їхня кваліфікація є різною. Для уникнення подальшої плутанини усіх респондентів будемо називати *експертами*. Кожному експерту присвоюються певні вагові коефіцієнти для кожного з критеріїв

оцінювання якості ПЗ, значення яких вказує на їхню обізнаність у певній предметній області [див. 4, табл. 1].

Введемо множину вагових коефіцієнтів, які присвоюються кожному з експертів під час оцінювання якості ПЗ, а саме:

$$\tilde{\tilde{W}} = \left\{ \tilde{W}_i = \{ w_{i,k} = [0..10], k = \overline{1,K} \}, i = \overline{1,M} \right\}, \quad (2)$$

де: $w_{i,k}$ – ваговий коефіцієнт оцінки, яку присвоєно k-му експерту за i-им критерієм оцінювання якості ПЗ; K – кількість експертів; M – кількість критеріїв оцінювання якості ПЗ.

Відповідно до кожного окремого експерта, що взяв участь в оцінюванні якості ПЗ, в базі даних має зберігатися сукупність виставлених ним оцінок. Також в базі даних мають зберігатися ознаки ролей експертів і коефіцієнти їхньої вагомості [див. 4, табл. 2]. Значення коефіцієнтів вагомості можуть бути виражені як у абсолютних одиницях, так і у відносних. Ці значення потрібно використати для врегулювання інтегральних оцінок якості ПЗ, які стосуватимуться окремо статичних і динамічних експертів. Початкові значення коефіцієнтів вагомості експертів, зазвичай, беруть емпірично, виходячи із їхньої важливості на початковому етапі розроблення ПЗ.

Введемо множину коефіцієнтів вагомості, які надаються кожному з експертів під час оцінювання якості ПЗ, а саме:

$$\tilde{Q} = \left\{ q_k = [0..1], k = \overline{1,K} \right\}, \quad (3)$$

де: q_k – коефіцієнт вагомості k-го експерта під час оцінювання якості ПЗ.

Візуалізація комплексних оцінок якості ПЗ для кожного з експертів. Для визначення комплексної оцінки якості ПЗ використаємо сукупність оцінок, які будуть надані відповідними *експертами* – учасниками процесу оцінювання його якості.

Введемо множину оцінок якості ПЗ, які може виставляти будь-який експерт за будь-яким критерієм, а саме

$$\tilde{U} = \{ u_i = [1..10], i = \overline{1,M} \}, \quad (4)$$

де u_i – оцінка якості ПЗ, яку надає експерт за i-им критерієм оцінювання. Кожна окрема оцінка якості ПЗ будь-якого експерта за відповідним критерієм належить цій множині:

$$\tilde{\tilde{X}} = \left\{ \tilde{X}_i = \{ x_{i,k} \in u_i, k = \overline{1,K} \}, i = \overline{1,M} \right\}, \quad (5)$$

де $x_{i,k}$ – оцінка якості ПЗ, яку надає k-ий експерт за i-им критерієм оцінювання.

Відповідно до кожного експерта введемо таке поняття як *визначена комплексна оцінка якості ПЗ* за відповідним критерієм оцінювання, яку потрібно обчислити за формулою

$$\tilde{\tilde{G}} = \left\{ \tilde{G}_i = \{ g_{i,k} = x_{i,k} \cdot w_{i,k} \cdot q_k, k = \overline{1,K} \}, i = \overline{1,M} \right\}, \quad (6)$$

де $g_{i,k}$ – комплексна оцінка якості ПЗ, яка стосується k-го експерта за i-им критерієм оцінювання. Якщо врахувати, що оцінку якості ПЗ $x_{i,k}$ виставляють за 10-бальною шкалою, ваговий коефіцієнт цієї оцінки $w_{i,k}$ – також за 10-бальною шкалою, а коефіцієнт вагомості експерта q_k – безрозмірна величина від 0 до 1, то комплексна оцінка якості ПЗ $g_{i,k}$ матиме значення від 0 до 100.

Визначені комплексні оцінки якості ПЗ подамо у вигляді векторів полярної системи координат, які мають утворити полярні діаграми для кожного експерта. Кожний такий вектор характеризується довжиною і кутом між ними. Як було зазначено вище, довжина вектора має відповідати кількісному значенню комплексної оцінки якості ПЗ за відповідним критерієм.

У випадку неоднакового впливу критеріїв на комплексну оцінку якості ПЗ кути між відповідними векторами потрібно визначити за формулою

$$\tilde{\mathrm{B}}_k = \left\{ \beta_{i,k} = 2\pi \cdot w_{i,k} \Big/ \sum_{j=1}^{M} w_{j,k}, i = \overline{1,M} \right\}, k = \overline{1,K}. \quad (7)$$

Оскільки область полярного сектора з кутом β_j має бути поділена навпіл векторами-критеріями (див. формулу (1)), то перший вектор-критерій має знаходитися на осі ординат. Тому

початок відліку кута $\beta_{1,k}$ ($\forall k$), який відповідає 1-му полярному сектору, почнемо зі значення $\alpha_{1,k} = -\beta_{1,k}/2$ ($\forall k$), а всі інші кути визначимо за такою формулою

$$\tilde{\mathrm{A}}_k = \left\{\alpha_{1,k} = -\beta_{1,k}/2; \alpha_{i,k} = \alpha_{i-1,k} + \beta_{i,k}, i = \overline{2,M}\right\}, k \in K. \qquad (8)$$

З врахуванням (6), значення ординати кожного вектора-критерію потрібно визначити за такою формулою

$$\tilde{A}_k = \left\{a_{i,k} = g_{i,k} \cdot \sin(\alpha_{i,k}), i = \overline{1,M}\right\}, k \in K, \qquad (9)$$

а значення його абсциси – за такою формулою

$$\tilde{B}_k = \left\{b_{i,k} = g_{i,k} \cdot \cos(\alpha_{i,k}), i = \overline{1,M}\right\}, k \in K, \qquad (10)$$

де: $a_{i,k}$, $b_{i,k}$ – відповідно значення абсциси і ординати i-го вектора-критерію, який стосується k-го експерта. Для того, щоб переконатися у правильності виконання розрахунків, потрібно виконати таку дію

$$\tilde{C}_k = \left\{c_{i,k} = \sqrt{a_{i,k}^2 + b_{i,k}^2}, i = \overline{1,M}\right\}, k \in K. \qquad (11)$$

Якщо $g_{i,k} = c_{i,k}$ ($\forall i,k$), то розрахунки виконано правильно.

Маючи довжини значень векторів-критеріїв, отримані за формулою (6), а також координати їхніх вершин, отримані за формулами (9) і (10), можна побудувати полярні діаграми для будь-якого експерта (рис. 1). Як було зазначено вище, форма неправильного багатокутника, побудованого за вершинами векторів-критеріїв, для будь-якого експерта дає якісну характеристику ПЗ за вибраними критеріями його оцінювання. Водночас, отримана площа багатокутника буде кількісно характеризувати якість ПЗ за всіма критеріями його оцінювання одночасно.

Для знаходження площі неправильного багатокутника потрібно використати таку формулу

$$S_k^{\text{бк}} = \frac{1}{2}\sum_{i=1}^{M}\left|a_{i,k} \cdot b_{i+1,k} - b_{i,k} \cdot a_{i+1,k}\right|, k \in K. \qquad (12)$$

Щоб встановити частку наявної якості ПЗ, яку маємо на даний момент, потрібно поділити площу неправильного багатокутника на площу круга, в якому він знаходиться, а саме

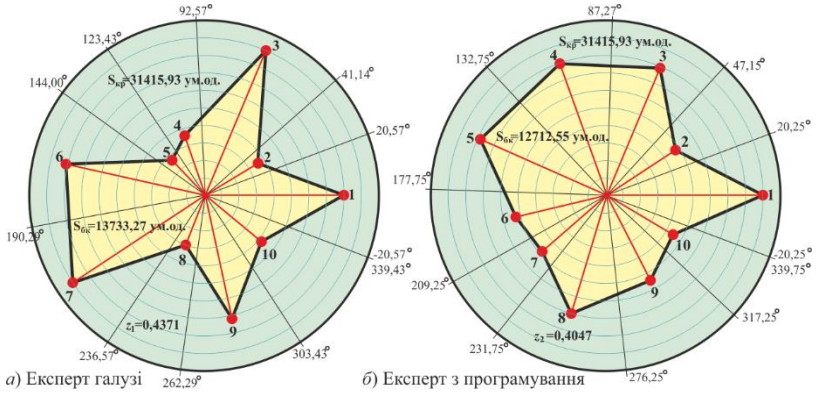


Рис. 1. Подання критеріїв оцінювання якості ПЗ у вигляді полярних діаграм для відповідних експертів

$$z_k = \frac{S_k^{бк}}{\pi r^2}, k \in K, \tag{13}$$

де: z_k – частка наявної якості ПЗ, яку встановлено за даними k-го експерта; r – радіус круга. Як було зазначено вище, комплексна оцінка якості ПЗ $g_{i,k}$ матиме максимальне значення 100, тобто радіус круга становитиме 100 од. Отже, незаповнена площа круга – та частка якості ПЗ, яку ще потрібно досягнути.

Висновки. Запропоновано механізм візуалізації експертного оцінювання якості ПЗ, який полягає у тому, що результатом оцінювання є багатокутник полярної діаграми, отриманий шляхом визначення середнього значення його площі, побудованих за оцінками окремих експертів з врахуванням різних вагових коефіцієнтів критеріїв оцінювання і вагомостей самих експертів. Механізм придатний для подання множини результатів опитувань з поділом на необмежену кількість ролей учасників оцінювання якості ПЗ з відповідно різною їхньою важливістю.

1. Боцула, М. П., & Моргун, І. А. (2011). Метод отримання комплексної оцінки якості веб-матеріалів з використанням полярної системи координат // Вісник Вінницького політехнічного інституту, 1, 84–88. Режим доступу: https://visnyk.vntu.edu.ua /index.php/visnyk/article/view/1367/confere nces.vntu.edu.ua.

2. Воронин, А. Н., Зиатдинов, Ю. К., & Кулинский, М. В. (2011). Многокритериальные задачи: модели и методы: монография. Киев: НАУ. 348 с.
3. Кулямин, В. В., Петренко, О. Л. (2008). Место тестирования среди методов оценки качества ПО. Москва: ИСП РАН. Режим доступу: http://software-testing.ru/library/5-testing/117-2008-10-13-19-25-13.
4. Моргун, І. А. (2011). Метод експертної оцінки якості програмного забезпечення // Інженерія програмного забезпечення: матер. Міжнар. наук.-практ. конф. аспірантів і студентів, 2(6), 33–37. Вінниця. – Режим доступу до журналу: http://jrnl.nau.edu.ua/index.php/IPZ/article/view/3086.
5. ISO/IEC 9126. (1991). Information technology – Software product evaluation – Quality characteristics and guidelines for their use. Geneva: International Organization for Standardization, International Electrotechnical Commission, 136 p. – (International Standard).

Система дистанційного навчання – сучасна педагогічна технологія для правоохоронних органів

Замула Аліна Олександрівна

доцент кафедри інформаційних технологій ХННІ ДВНЗ «Університет банківської справи», кандидат технічних наук, доцент

Кашура Ганна Костянтинівна

здобувач ступеня бакалавра ХННІ ДВНЗ «Університет банківської справи»

Систематичне накопичення достовірної інформації, яка характеризує оперативну обстановку, її слушний і високоякісний розгляд є однією з найважливіших передумов реалізації боротьби з беззаконням в сьогоднішніх умовах. Інформація стала стратегічним продуктом, а застосування методів її опрацювання, найважливішим з яких є комп'ютерне обладнання, зробилося життєво необхідною потребою при ухваленні управлінських розпоряджень. Громадськість, якій не під силу поставити завдання інтенсифікації інформаційного забезпечення керування, наражається на небезпеку безпорадно відбитися від розвинених держав.

Результативна боротьба зі злочинністю характеризується ступенем організації запобіжних заходів, що в свою чергу проводиться органами внутрішніх справ. У свою чергу, підсумки цієї праці залежать від рівня інформаційного сприяння, тому що основні дії практичних спеціалістів у розслідуванні, розкритті та попередженні беззаконня так чи інакше поєднані з одержанням потрібних даних, саме ці необхідні дії і покликана задовольнити система інформаційного забезпечення органів внутрішніх справ.

Забезпечення працівників якісною інформаційною підтримкою є важливим аспектом у отриманні свіжих знань для підвищення кваліфікації, що в свою чергу покращить статистику роботи правоохоронних органів. Ці фактори пов'язані між собою таким чином: знання-практика-досвід-нові знання.

Та окрім практичних вмінь, власного досвіду та теоретичних знань існує ще досвід закордонних фахівців, сучасні наукові розробки та інша інформація, яка допомагає поповнювати власний багаж знань.

Однією з інформаційних криниць є Інтернет. Він значно розширює можливості щодо одержання свіжих знань. Він охоплює всі можливі сфери життя, необхідно тільки задати напрямок пошуку. Щодо правоохоронних органів, то не слід ігнорувати величезну кібермережу.

Але ж для пошуку необхідної інформації йде певна кількість часу, адже не завжди вдається задати правильне формулювання запиту на пошук необхідних даних. Також, будь-яка інформація, знайдена за запитом, не завжди несе необхідну інформацію, але аби зрозуміти це також втрачається час.

Тому, на мою думку, для постійного підвищення кваліфікації необхідно реалізувати систему дистанційного навчання, яка б постійно оновлювалась. Також це вплине на кількість робочих місць, оскільки система повинна оновлюватись в багатьох галузях одночасно, а для цього необхідно залучити достатню кількість людей.

Система дистанційного навчання значно полегшить процес підвищення кваліфікації, а саме зменшить час пошуку та скоротить процес обробки знайденої інформації.

Проте, це повинен бути постійно діючий ресурс, а не разовий захід. Спеціалісти різних галузей, використовуючи певні методики допоможуть оволодіти новою інформацією, а також поглибити вже набуті знання працівників правоохоронних органів.

Цей ресурс має постійно оновлюватись, реагуючи на ряд процесів:

- зміни в чинному законодавстві України;
- поява наукових розробок у правоохоронній галузі;
- новий досвід роботи правоохоронних органів України, зарубіжних країн;
- зміни в нормах міжнародного законодавства.

Найбільше значення у розвитку правоохоронних органів повинен відігравати досвід зарубіжних країн, адже вони в цьому питанні мають певний досвід(боротьба з організованою злочинністю, розповсюдження наркотиків, торгівля людьми, вчинення комп'ютерних правопорушень и т. п.). Проте маємо певні суперечності щодо організація та реалізації системи дистанційної освіти.

Наприклад, у країн світу з розвиненим демократичним порядком(США, Німеччина) мають значний успіх в цій темі, а саме дистанційного навчання, у тому числі з юридичного курсу. У США будь-який бажаючий може «потрудитися» на сайті бібліотеки Конгресу чи належного Університету щодо пошуку правової інформації, необхідно тільки мати вихід в Інтернет.

Щодо України, то можемо її віднести до країн з перехідною економікою. Після розпаду СРСР , Україна не повністю перейшла до ринкової економіки через низький рівень правової обізнаності громадян України.

Одним з прикладів переходу до ринкової економіки є наші недалекі сусіди (Польща, Чеська республіка). Етап переходу до нової економічної політики пройшов і проходить швидкими темпами, через це нові злочини і, відповідно, методи боротьби з ними осягаються активніше та ліквідуються швидше. Наші сусіди гарний приклад для нас, через це встановлення прямих

або опосередкованих контактів з ними, буде дуже корисним для України, в плані удосконалення рівня технічної та правової обізнаності.

Як це втілити в життя? Відкинемо організаційні проблеми щодо узгодження процедури обміну досвідом та повернемося до онлайн системи підвищення кваліфікації.

Фахівці з даного питання по кожному курсу підвищення кваліфікації повинні максимально забезпечити контактними даними щодо спеціалістів та діячів науки обраного курсу удосконалення, надати посилання на веб- сторінки, електронні адреси, адреси онлайн форумів. Щодо онлайн конференцій, потрібно надавати графік їх проведення з перспективою доступу до відео, мультимедіа та аудіо інформації. Можливо, не у всіх є можливість переглядати відео інформацію, проте аудіо файли мають можливість осягати всі працівники правоохоронних органів.

Думаю, участь у таких форумах або семінарах є більш рентабельною у фінансовому плані, оскільки немає потреби нікуди їхати та летіти, оформлювати візу, ніяких транспортних витрат та інших грошових затрат. Потрібно тільки робоче місце, яке є за місцем роботи чи освіти.

Оскільки ми реалізуємо цей ресурс в мережі Інтернет, кожен робітник за необхідністю може вдома (або будь-якому іншому місці нашої країни та за межами неї) також зайнятися самонавчанням в зручний для нього час або приймати участь в конференції, якщо вона буде проходити після закінчення робочого дня. Потрібен тільки доступ до Інтернету.

Не менш значущим пунктом в побудові даного запропонованого ресурсу є розв’язання питання захисту комп’ютерної інформації. Всі знають, що злочинний світ не сторониться користуватися сучасні технічні прийоми та комп’ютерні інформаційні інновації. Через це, досить розумно буде забезпечити багаторівневий доступ до системи дистанційного навчання. Першим рівнем може бути загальнодоступна інформація, для неавторизованих користувачів, другим-інформація, дозволена

тільки авторизованим користувачам, третій-право користування лише адміністраторами(різного рівня також), які мають право корегувати дані в нашому ресурсі.

Захист інформації у таких системах є окремою темою, яка вимагає детального розгляду. Слід зазначити, що, окрім технічних, програмних засобів захисту інформації, існують питання законодавчого врегулювання. У нашій країні на сьогодні законодавчо не вирішене питання електронного підпису як засобу ідентифікації (учасника конференції, інформації).

Слід зосередитись на проблемі навчання спеціалістів правоохоронних органів задля боротьби з комп'ютерними злочинами. Кримінальна відповідальність за здійснення криміналу у колі комп'ютерних даних приходить не тільки за статтями розділу XVI, а й іншими розділами Особливої частини нового Кримінального кодексу України. Однак, у старих посібниках з криміналістики немає способів і тактики боротьби з цим злочинством. Як дієво, хутко вирішити це питання? Авжеж, можлива реалізація доцільної веб-сторінки спецпідрозділів, наприклад у Міністерстві внутрішніх справ України чи у Національній академії внутрішніх справ України.

Щодо адміністрування системи дистанційного навчання, треба сказати, що конкретно від адміністраторів буде залежати наскільки своєчасно нове і сучасне стане відомим та відкритим для слухачів курсів підвищення кваліфікації, хто та на яких умовах (рівнях) отримає право на користування до даних, що надається в рамках системи дистанційного навчання. В ідеалі необхідно реалізувати такий ресурс не у форматі веб-серверу, а у форматі Інтернет-порталу, який буде інтегрувати максимальну кількість запасів Інтернету з визначених напрямів знань (наукові розробки, досвід, практичні наробки).

З вище сказаного, можна зробити висновок: в умовах швидкоплинної обстановки, яка характеризується вираженим дефіцитом часу на прийняття рішень, пов'язаних із глибоким аналізом і прогнозуванням розвитку ситуації, орієнтація на

автоматизовані системи підготовки спеціалістів виступає як першонеобхідне. Створення таких спеціалізованих систем дистанційного навчання для підвищення кваліфікації фахівців правоохоронних органів є нагальною проблемою сьогодення, а вчасно розпочата справа стане порукою її успішного розвитку.

1. Боремчук Л. І. Дистанційне навчання як педагогічна технологія / Л. І. Боремчук. – Режим доступу : http://intkonf.org/boremchuk-li-distantsiyne-navchannya-yak-pedagogina-tehnologiya/ (Дата звернення - 29.11.2017)
2. Дистанционное обучение в ИТ: есть ли будущее? // ITPartner. – 2010. – № 7. – С. 14-15
3. Про затвердження Положення про дистанційне навчання : Наказ Міністерства освіти і науки України від 21 січ. 2004 р. № 40. – Режим доступу http://zakon.rada.gov.ua/cgibin/laws/main.cgi?nreg=z0464-04
4. Організаційно-правові засади професійної підготовки персоналу органів внутрішніх справ України: Наук.-практ. посібник / В.С. Венедиктов, М.І.Іншин, М.М. Клемпарський та ін.; За заг. Ред. проф. В.С. Венедиктова. – Х.: Вид-во Нац. Ун-ту внутр. справ, 2003. – 212 с.

До проблеми створення внутрішньої наукометричної бази ВНЗ

Зачко Олег Богданович,

професор кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності,
доктор технічних наук, доцент

Головатий Роман Русланович,

ад'юнкт кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності

В умовах сьогодення популяризація інтернет-технологій та їхній вплив на формування баз даних для зберігання наукових

доробків створює новітні можливості організації науко-метричних процесів.

Спрощена можливість доступу до різноманіття наукових доробків полегшує пошук необхідної інформації та пришвидшує нарощування показників цитування у працях вчених. В загальному це здійснюється і завдяки внутрішнім наукометричних базам вищих навчальних закладів.

Dspace (рис.1) – відкрите програмне забезпечення, яке дозволяє збирати, зберігати та розповсюджувати контент, охоплюючи наукові організації: вищі навчальні заклади, навчально-наукові установи та інші.

Рис. 1. Головна сторінка Наукового репозитарію Львівського державного університету безпеки життєдіяльності

По своїй суті Dspace – наукова бібліотека, яку можна охарактеризувати як наукометрична база локального рівня.

Розробкою наукових репозитаріїв на основі платформи Dspace займаються науковці Massachusetts Institute of Technology та Hewlett-Packard Company (розробка вперше була запущена 4 листопада 2002 року). Проект Dspace є відкритим та розповсюджується під ліцензією BSD.

Система Dspace має ряд аналогів серед розробок іноземних інженерів, зокрема: Eprints, Fedora, RoGo, OAKList Database, SHERPA та інші. Проте попри наявну велику кількість

суміжних наукових наукометричних баз локального рівня, система Dspace має ряд переваг, зокрема:

- Система зберігає і індексує метадані в різноманітних форматах;
- Система зберігає інформацію про користувачів системи;
- Наявна авторизація користувачів з метою поділу рівнів доступу до сховища;
- Матеріали в архіві доступні за посиланнями в описі конкретного елемента. З цього ж опису можна робити бібліографічні посилання на даний матеріал;
- Система надає автоматичну розсилку повідомлень по електронній пошті через службу підписки;
- Надається можливість обробляти дані довільних форматів, від простих текстових документів до наборів даних і цифрового відео;
- Доступ до перерахованих функціональними можливостями надається за допомогою веб-інтерфейсу.

Подані в Науковий репозитарій університету матеріали зберігатимуться й будуть доступними в мережі Інтернет протягом тривалого часу. Це накладає деякі вимоги щодо оформлення поданих документів. Повний бібліографічний опис, точне і якісне відтворення виду матеріалу – основні акценти при підготовці до внесення їх в Науковий репозитарій. Як правило, прийняті до друку матеріали вже оформлені певним чином згідно з вимогами видавництва.

При публікації у відкритому інституційному науковому репозитарії є певна специфіка щодо оформлення. Вона пов’язана з браком контексту матеріалу для потенційних читачів. Щоб додати такий контекст, рекомендується до вмісту файлів публікацій (у разі наявності вихідних файлів, наприклад, у форматі MS Word .doc або .docx) долучити ще й такі дані:

- Бібліографічний опис матеріалу. Розмістити можна, наприклад, у колонтитулі першої сторінки публікації.
- Автори, бажано подавати всіх та з розкриттям ініціалів.

- Для статей – назва журналу, рік, серія, секція, номер. Варіант розміщення – колонтитули парних/непарних сторінок.
- Ключові слова, анотація.
- Переклад назви, авторів, анотації, ключових слів англійською або іншою іноземною мовою.

З форматів документів, які зберігають форму і мають текстовий шар (у такому разі текст такого документа може бути проіндексованим пошуковими системами), найбільш популярним є PDF. Розглянемо роботу з ним.

Варіантів утворення файлів формату PDF є багато. Зокрема в деяких програмах підготовки документів (Microsoft Office Word, OpenOffice.org та інші) вже є вбудована можливість збереження чи експорту у формат PDF.

Наприклад, для збереження у MS Word версії 2007 (та вище), слід обрати пункт меню «Файл \ Зберегти як…» і вибрати тип файлу – PDF.

Якщо така можливість недоступна, то створити PDF-файл з будь-якої програми дозволить спеціальна програма-драйвер, яка після встановлення на ПК працює як віртуальний принтер. При «друці» на такому принтері будь-якого документа з'являється вікно з пропозицією дати ім'я згенерованому PDF-файлу.

Найкращим варіантом створення PDF-файлів є безпосереднє конвертування з вихідних документів (тобто переважно створених у текстових редакторах). На жаль, деколи вихідні файли є недоступні чи втрачені. У цьому випадку розглянемо варіант оцифровування, що передбачає етапи сканування зображень публікації та їх наступне розпізнавання для створення текстового шару.

Отже, спочатку сканується паперовий оригінал матеріалу. Для доброго відтворення вибирайте сканування в кольорі (у разі наявності кольорових ілюстрацій, схем, діаграм) та роздільну здатність 300 dpi (точок на дюйм). ПЗ для сканування є велика кількість, доволі зручно сканувати у ABBYY FineReader або IrfanView (безкоштовні).

Далі рекомендується провести у названих програмах обрізку, обертання відсканованих сторінок, очищення від «шуму» чи інші операції із зображеннями.

Для можливості повнотекстового пошуку потрібен текстовий шар. Отож ще слід виконати оптичне розпізнавання символів (ОРС) для відсканованого документу. Однією з найбільш популярних програм та функціональних для ОРС є ABBYY FineReader. Крім того, у ній вбудована можливість збереження вихідного документа як у форматі Microsoft Word (.doc, .docx), так і в цільовому форматі – PDF.

Система DSpace наукового репозитарію приймає файли з кириличними назвами, проте для кращої сумісності рекомендується використовувати лише латинські літери, цифри та символи «_,-» а також не використовувати занадто довгі назви (до 128 символів).

---

1. Зачко О.Б. Управління безпекою складних інфраструктурних проектів в системі цивільного захисту / О.Б. Зачко // Управління проектами: стан та перспективи: матер. 10 Міжнар. наук.-практ. конф. – Миколаїв: НУК. – 2014. – С. 91-92.
2. Рак, Ю. П. Безпеко-орієнтоване управління регіональними проектами захисту критичних інфраструктур засобами системи 112 [Текст] / Ю. П. Рак, О. Б. Зачко, Д. С. Кобилкін, Р. Р. Головатий // Управління проектами та розвиток виробництва : зб. наук. пр. – Луганськ : вид-во СНУ ім. В. Даля. – 2016. – № 1 (57). – С. 49–55.
3. Зачко О.Б. Оптимізація структури портфелю проектів в системі забезпечення безпеки життєдіяльності / О.Б. Зачко, Ю.П. Рак, Т.Є. Рак // Управління проектами та розвиток виробництва. – 2008. – № 4(28). – С. 26-30.
4. Zachko, Oleg, Roman Golovatyi, and Alona Yevdokymova. «Development of a simulation model of safety management in the projects for creating sites with mass gathering of people» *Восточно-Европейский журнал передовых технологий* 2 (3) (2017): 15-24.

Розроблення програмно-алгоритмічного забезпечення інтелектуальної системи «Розумна кафедра»

Коваль Сергій Олегович,

здобувач ступеня бакалавра Національного лісотехнічного університету України

Соколовський Ярослав Іванович,

завідувач кафедри інформаційних технологій Національного лісотехнічного університету України, доктор технічних наук, професор

В даний час в умовах швидкого розвитку мікропроцесорної техніки та побудові пристроїв на їх основі виникає потреба і можливість максимального забезпечення реалізації зростаючих вимог до комфортних умов проживання та праці мільйонів людей, гарантування їхньої безпеки та захисту від наслідків технічних аварій. Це стало одним з пріоритетних напрямків розвитку сучасної радіоелектронної та обчислювальної техніки. Ринок програмного забезпечення постійно змінюється та насичується продуктами які дозволяють автоматизувати роботу домашніх та робочих приміщень.

Метою даної роботи є створення десктопного додатку для моніторингу мікроклімату та управління навчальною лабораторією, для зручності використання розробити Web сайт, який надасть можливість користуватись даним функціоналом віддалено.

Даний додаток надає можливість проводити моніторинг мікроклімату у реальному часі за допомогою таких датчиків:

- температури,
- вологості,
- освітлення.

Також додаток надає можливість управління пристроями лабораторії, а саме:

- увімкнення/вимкнення комп’ютерів,
- керування освітленням,
- керування кондиціонером,
- відкривання/закривання дверей навчальної лабораторії.

Управління зовнішніми пристроями та моніторинг мікроклімату лабораторії проводиться за допомогою контроллера Arduino UNO. Arduino Uno – це пристрій на основі мікроконтролера ATmega328. До його складу входить все необхідне для зручної роботи з мікроконтролером: 14 цифрових входів / виходів (з них 6 можуть використовуватися в якості ШІМ-виходів), 6 аналогових входів, кварцовий резонатор на 16 МГц, роз′єм USB, роз′єм живлення, роз′єм для внутрісхемного програмування (ІМТП) і кнопка RESET. Для моніторингу мікроклімату було використано: датчик DHT22 – вимірювання вологості і температури та датчик TSL2561 – вимірювання освітлення.

Для зберігання інформації було розроблено базу даних використовуючи підхід Code First технології Entity Framework. Entity Framework (EF) — це об’єктно-орієнтована технологія доступу до даних, являє собою object-relational mapping (ORM) рішенням для .NET Framework від Microsoft. Надає можливість взаємодії з об’єктами використовуючи LINQ запити у вигляді LINQ to Entities, так і з використанням Entity SQL.

Також було розроблено Web API сервіс для комунікування десктопного додатку з сайтом (клієнтський додаток). Клієнтський додаток розроблений за допомогою технологій: Angular 2, JQuery та Bootstrap.

ASP.NET Web API – це фреймворк який дозволяє досить легко та просто будувати HTTP сервіси, який можуть використовувати різні типи додатків включаючи браузери та мобільні додатки. ASP.NET Web API – це ідеальна платформа для побудови RESTful додатків використовуючи .NET Framework.

AngularJS — JavaScript-фреймворк з відкритим програмним кодом, який розробляє Google. Призначений для розробки односторінкових додатків, що складаються з одної HTML сторінки з CSS і JavaScript. Його мета — розширення

браузерних застосунків на основі шаблону Модель-вид-контролер (MVC), а також спрощення їх тестування та розробки. Фреймворк працює зі сторінкою HTML, що містить додаткові атрибути і пов'язує області вводу або виводу сторінки з моделлю, яка є звичайними змінними JavaScript. Значення цих змінних задаються вручну або отримуються зі статичних або динамічних JSON-даних.

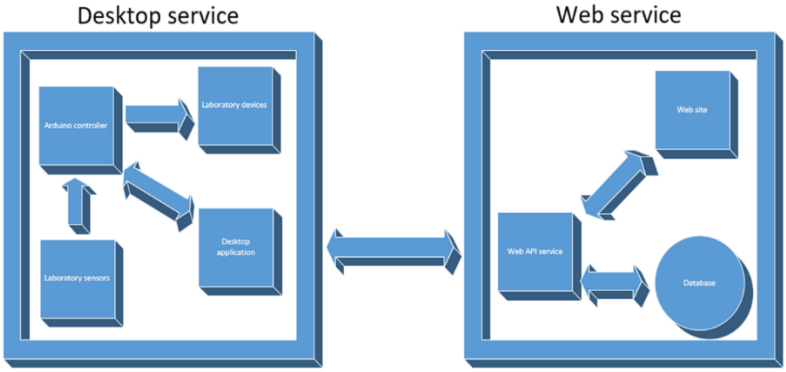


Рис.1. Структура системи

На рисунку 1 зображено структуру розробленої системи, її компоненти та їхню взаємодію.

Під час проектування було проаналізовано вже готові системи управління «Розумними будинками». Вибрано найбільш оптимальні технології для реалізації потрібного функціоналу. Вибраний контроллер для управління зовнішніми пристроями дозволяє легко та просто розширити систему у майбутньому. Вибрані технології для розроблення клієнтського додатку забезпечують кросбраузерність та адаптивність, що дозволяє переглядати та керувати системою навіть з телефону.

---

1. Ендрю Троелсен. Язык программирования C# 2010 и платформа .NET 4. – Изд.: «Вильямс». – 1310 с. – Изд.: «Вильямс». – 2010 – ISBN 0-201-70857-4.

2. Загальні відомості про контролер Arduino UNO [Веб ресурс] – https://planeta-stem.blogspot.com/2016/04/arduino-uno.html
3. Документація Angular2 [Веб ресурс] – https://angular.io/
4. Metanit – сайт про програмування [Веб-ресурс] – https://metanit.com
5. ASP.NET Web API 2 [Веб-ресурс] – https://msdn.microsoft.com/en-us/library/dn448365(v=vs.118).aspx

Застосування інформаційних технологій правоохоронними структурами України та ВНЗ зі специфічними умовами навчання: проблеми та реалії життя

Комісарчук Юлія Анатоліївна,

доцент кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Загацький Володимир Васильович,

здобувач ступеня бакалавра факультету №1 ІПФПНП Львівського державного університету внутрішніх справ

Сьогодні, в епоху розвитку «інформаційного суспільства», як ніколи постає важливим питанням застосування інформаційних технологій в діяльності правоохоронної системи України, а також вищих навчальних закладів зі специфічними умовами навчання. Рівень розвитку людства показує стрімке зростання технологій які допомагають в повсякденній діяльності правоохоронців. Важко собі уявити діяльність судів, органів прокуратури , органів внутрішніх справ, органів служби безпеки, органів митного контролю без застосування сучасних комп'ютерних засобів.

З метою підвищення ефективності діяльності правоохоронних органів створюються державні бази та реєстри. У статті 10 Закону України «Про інформацію» надано вичерпний перелік видів інформації, а саме: 1) інформація про фізичну особу; 2) інформація довідково-енциклопедичного характеру; 3) інформація про стан довкілля; 4) інформація про товари і послуги; 5)науково-технічна

інформація; 6) податкова інформація; 7)правова інформація; 8)статистична інформація; 9) соціологічна інформація; 10) інші види інформації [1]. В державних базах даних можна знайти інформацію про: 1) обліково-реєстраційні дані громадян; 2) правопорушення і кримінальні події; 3) правопорушників і злочинців; 4) викрадені і вилучені речі, а також предмети антикваріату; 5) власників авто-, мото- транспортних засобів; 6) власників вогнепальної зброї; 7) громадян, що знаходяться в розшуку та безвісті зниклих громадян; 8) інша інформація, що підлягає зберіганню. В державних реєстрах зберігається інформація щодо: 1) фізичних осіб платників податків, 2) нормативно-правові акти, 3) громадські об'єднання, 4) цивільний стан громадян, 5) нотаріусів, 6) довіреності, 7) юридичних осіб та фізичних осіб підприємців, 8) осіб, які вчинили правопорушення, 9) інформація про підприємців щодо яких порушено провадження щодо банкрутства та інше.

Таким чином ми бачимо, що правоохоронні органи володіють значною кількістю інформації, що допомагає їм в розкритті, протидії та запобіганні злочинам у різних сферах суспільного життя. З метою систематизації такої кількості інформації створені автоматизовані інформаційні системи(АІС) для швидкого пошуку потрібних даних [2].

Для застосування таких технологій потрібно мати сучасне матеріальне забезпечення, що, нажаль, в системі правоохоронних органів під питанням. Наявне устаткування потребує оновлення у зв'язку з розвитком нових технологій. Так, у відділеннях поліції матеріальне забезпечення потребує оновлення, значна кількість комп'ютерів не підтримує нові програми які здійснюють пошук в базах даних з державними реєстрами та іншими матеріалами. У зв'язку з проведеними реформами у Національній поліції України було звільнено багато спеціалістів які забезпечували належне функціонування і роботу інформаційно-пошукових систем в базах і банках даних.

Для вищих навчальних закладів зі специфічними умовами навчання застосування інформаційних технологій у навчальному процесі є важливим аспектом виховання майбутніх працівників

правоохоронної системи. Безумовно для цього є необхідним відповідне матеріальне забезпечення, яке дасть можливість створення сучасних комп'ютерних класів та лабораторій для того, щоб такі вищі навчальні заклади могли готувати високо-кваліфіковані кадри для боротьби зі злочинністю. У процесі навчання важливою є не сама інформаційна технологія, а методи її реалізації для досягнення освітніх цілей. Таким чином викладач може підготовлювати матеріал для занять не лише як «суху» інформацію, а з належними прикладами у вигляді аудіо-,відео файлів, різноманітних таблиць і діаграм, що має сприяти кращому засвоєнню матеріалу студентами та курсантами. Крім того, лабораторії вищих навчальних закладів, які будуть забезпечені сучасним обладнанням зможуть підготувати експертів відповідної кваліфікації.

Застосування інформаційних технологій є однією з основних тенденцій розвитку освітнього процесу. Тому, необхідно проводити постійні тренінги для викладачів з метою підвищення їхнього кваліфікаційного рівня. Адже сучасній освітній системі потрібні такі науково-педагогічні працівники, які зможуть підготувати якісні кадри для правоохоронної системи, що допоможе знизити рівень злочинності, як в суспільстві, так і в Інтернет просторі.

Дедалі частіше ми маємо справу з інформаційним тероризмом.[3] Як серед української преси, так і з-за кордону надходить велика кількість інформації з метою дезінформації та дезорієнтації населення, що призводить до ескалації конфлікту на Сході нашої держави. Наказом Національної Поліції №85 від 10.11.2015 «Про Департамент кіберполіції НП України», створено міжрегіональний територіальний орган Департамент кіберполіції, який має забезпечувати інформаційну безпеку України. Незаконні територіальні об'єднання які діють в зоні проведення анти – терористичної операції намагаються поширити неправдиві дані через мережі Twitter, Facebook, Вконтакті. Моніторинг соціальних мереж дає можливість констатувати, що сьогодні значна кількість інформації надходить з АТО від незаконних територіальних формувань ДНР та ЛНР, яка виражається у розповсюдженні

хибних даних, пропаганді, агітації воювати на стороні вищевказаних формувань, надавати матеріальну і гуманітарну допомогу. Це пов'язано з тим, що кіберполіції не вистачає кадрів які б могли блокувати таку інформацію. Отже зараз відбувається війна не лише на сході, а й в Інтернет просторі і засобах масової інформації.

Тому, на нашу думку, застосування інформаційних технологій працівниками правоохоронної системи та науково-педагогічними працівниками і курсантами вищих навчальних закладів зі специфічними умовами навчання є критичним питанням, яке потребує термінового розгляду. На державному рівні потрібно розробити стратегію вирішення цього питання, яка б за максимально короткий термін реформувала систему правоохоронних органів та вищих навчальних закладів зі специфічними умовами навчання, щодо запровадження сучасних інформаційних технологій в повсякденній професійній діяльності правоохоронців, студентів, курсантів та викладачів. Адже в сучасному світі неможливо уявити роботу системи МВС без застосування баз і банків даних, державних реєстрів, як необхідної складової діяльності даної системи.

1. Закон України «Про інформацію» від 02.10.1992р. [Ел. ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1906-15
2. Бабаскін В.В., Жалгунова С.А. Проблемні питання інформаційного забезпечення діяльності ОВС // Науковий вісник ЮА МВС. – 2014. – № 3. – С.32-38.
3. Бабенко Ю. Інформаційний тероризм / Ю. Бабенко [Електронний ресурс], - Режим доступу: http://www.aratta-ukraine.com/text_ua.php?id=149
4. Ковальов М. В. Проблеми інформаційного забезпечення діяльності практичних підрозділів ОВС та впровадження інформаційних технологій в навчальний процес / М.В. Ковальов. – Л., 2004. – 201
5. Снегірьова Т. Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС.
6. Бойченко О.В. Медіа тероризм: особливості сучасник ознак інформаційній безпеці / О.В. Бойченко // Інтегровані

інтелектуальні робото-технічні комплекси (ПРТК-2009): друга міжнародна наук.-практ. конф. (25-28 травня 2009 р.). – К.: НАУ,2009. – С.230-232.

Використання класичних статистичних методів для аналізу валідності та дискримінативності результатів тестування

Кулешник Ярко Федорович,

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

Ізьо Марта Ігорівна,

здобувач ступеня магістра факультету № 5 Львівського державного університету внутрішніх справ

Тест – це інструмент, що складається з вивіреної системи завдань, стандартизованої процедури проведення і наперед спроектованої технології аналізу результатів для визначення рівня знань, умінь, навиків, властивостей характеру особистості, розумових здібностей, зміна яких можлива в процесі систематичного навчання.

На сьогодні застосування тестового контролю при проведенні вступних компаній у ВНЗ, при перевірці залишкових знань учнів шкіл, ліцеїв, коледжів та університетів є дуже актуальним.

Головна проблема тестового контролю знань – сам процес створення тестів, їхня уніфікація та методи проведення аналізу. Щоб довести тест до повної готовності для використання необхідна багаторічна кваліфікована праця по складанню позбавлених суб'єктивізму у формулюванні тестових завдань та збору статистичних даних. Для об'єктивної оцінки рівня знань необхідне професійне і грамотне складання тесту. Недостатньо придумати запитання і варіанти відповідей, так як в цьому випадку може виникнути немало протиріч, помилок, невизначеності, завдання можуть дуже простими або ж навпаки,

надто складними. Саме тому тестові завдання повинні проходити процес спеціальної оцінки з використанням елементів математичної статистики.

Історично виділяють два основні підходи до створення тестів. Перший з них набув широкого розвитку в рамках класичної теорії тестів. Згідно з ним, рівень знань учасників тестування оцінюється за допомогою балів, набраних під-час тестування. Бал обчислюється як алгебраїчна сума оцінок виконання кожного завдання тесту. Статистичні методи аналізів результатів лягли в основу класичної теорії тестування знань і методів оцінки якості тестів.

Метою даної роботи є часткова систематизація найпростіших методів, що дозволяють розраховувати тестові характеристики, а саме визначення складності, валідності та дискримінативності деяких тестів, що проводились у ЛьвДУВС, інтерпретація результатів та вироблення спрощених загальних рекомендацій укладачам.

Позначимо через $x_{i,j}$ числову оцінку успішності виконання j-го завдання i-им студентом. Результат тестування звичайно можна представити у вигляді матриці $\{X_{i,j}\}$, що містить n рядків та m стовпців ($i = \overline{1,n};\ j = \overline{1,m}$). Ця матриця показує результат виконання всіх завдань усіма учасниками тестування. На практиці, як правило, використовують дихотомічну шкалу оцінок результатів, тобто у результаті правильного виконання завдання тестований отримує один бал, $x_{i,j}$ =1, в протилежному випадку – нуль балів, $x_{i,j}$ = 0. У такому випадку результатом виконання тесту буде кількість правильних відповідей. Результат можна оцінювати не лише нулем чи одиницею, але й присвоювати певний ваговий коефіцієнт, що відповідає складності завдання, однак суттєвих змін у якість оцінювання тестових завдань він не дає.

Для майбутніх обчислень індивідуальний початковий бал (результат, або кількість правильних відповідей за усі завдання) i-го тестованого після проходження тесту позначимо y_i ($i = \overline{1,n}$), середній результат сумарних балів всіх учасників тестування –

$\overline{y}$, середній результат тестованого за кожним завданням $\overline{x_j}, (j = \overline{1,m})$:

$$y_i = \sum_{j=1}^{m} x_{i,j}, \quad \overline{x_j} = \frac{\sum_{i=1}^{n} x_{i,j}}{n}, \quad \overline{y} = \frac{\sum_{i=1}^{n} y_i}{n} \tag{1}$$

Важливою вимогою до тестових завдань є їх об'єктивний рівень складності. Не можуть в тесті бути завдання з невідомою мірою складності. Завдання можна включати в тест лише після емпіричної перевірки їх міри складності.

Методику розрахунку тестових характеристик покажемо на конкретному прикладі. У тестуванні приймало участь 29 студентів. Тест складався з 30 запитань. До кожного запитання надавалось 3-4 відповіді, серед яких потрібно було обрати правильну. Правильна відповідь оцінювалась 1 балом, неправильна – 0 балів. Ми отримали результати тестування студентів, що показані в таблиці 1.

Складність завдання.

Складність завдання можна визначити двома способами [1]:

- на основі оцінки передбачуваного числа і характеру розумових операцій, необхідних для його вдалого виконання;
- на основі емпіричної перевірки завдань, з підрахунком частки правильних відповідей.

Протягом багатьох років у класичній теорії тестів розглядалися тільки емпіричні показники складності. На сьогодні в дистанційному навчанні застосовуються сучасні теорії навчальних тестів, де більше уваги приділяється характеру розумової діяльності у процесі виконання тестових завдань різних форм.

Емпірично складність завдання визначається додаванням елементів матриці $\{X_{i,j}\}$ по стовпцях і дорівнює числу

правильних відповідей, отриманих за кожним стовпцем (R_j). Чим більше правильних відповідей на конкретне завдання, тим воно легше для даної групи студентів. У зв'язку з різною кількістю тестованих у вибірці для одержання об'єктивних характеристик R_j ділять на число у кожній групі n.

$$p_j = \frac{R_j}{n} \tag{2}$$

У результаті отримаємо нормований статистичний показник – частка правильних відповідей, p_j. Показник p_j довший час використовувався як показник рівня складності завдання в класичній теорії тестів. Пізніше усвідомили, що зі збільшенням значення p_j складність не зростає, а навпаки – спадає. Тому ввели показник складності, що відображав відношення кількості неправильних відповідей W_j до кількості учасників тестування n:

$$q_j = \frac{W_j}{n},\ p_j + q_j = 1 \tag{3}$$

Завдання є не тестовим якщо на нього правильно чи неправильно, тобто однаково, відповідають усі тестовані. Між ними відсутня варіації, іншими словами варіація рівна нулю. Нульова варіація практично означає необхідність викидання завдання з тесту.

Зручною мірою варіації може бути значення дисперсії s_y^2, чи стандартне відхилення s_y сумарних балів кожного тестованого та величина s_j^2 – дисперсії результатів тестованих по j-му завданню:

$$s_y^2 = \frac{\sum_{i=1}^{n}(y_i - \bar{y})^2}{n-1},\quad S_y = \sqrt{\frac{\sum_{i=1}^{n}(y_i - \bar{y})^2}{n-1}},\quad s_j^2 = \frac{\sum_{i=1}^{n}(x_{i,j} - x_j)^2}{n-1}, (j = \overline{1,m}) \tag{4}$$

У випадку, коли результат виконання j-го завдання оцінюється балами 0 чи 1, то міра варіації визначається формулою $s_j^2 = p_j * (1 - p_j)$ або $s_j^2 = p_j * q_j$

Результати розрахунків показані в табл. 1.

Таблиця 1.

	Номер запитання								
Кандидат	1	2	3	…	29	30	Разом	Експертна оцінка	Стандартне відхилення результату (S_y)
1	0	0	0	…	0	0	5	6	5,5
2	0	0	1	…	1	0	13	12	Стандартне відхилення експертних оцінок (S_Y)
3	0	0	1	…	1	0	7	8	4,6
4	1	0	0	…	0	0	10	11	
5	0	0	0	…	1	1	8	7	
…	…	…	…	..	…	…	…	…	Валідність (V)
26	0	0	0	…	1	1	6	7	0,97
27	0	0	0	…	1	0	7	8	
28	0	0	0	…	0	0	6	6	Середнє значення дисперсії (S_j^2)
29	0	0	1	…	0	0	10	12	0,2
правильних відповідей	10	6	8	…	18	7	310	304	
частка правильних відповідей	0,34	0,21	0,28	…	0,62	0,24			
частка неправильних відповідей	0,66	0,79	0,72	…	0,38	0,76			
дисперсія (S_j^2)	0,23	0,16	0,20	…	0,24	0,18			
сер. бал							10,69	10,48	
Maxs(i)	29	29	29	…	29	29	870		
P-показник складності	0,34	0,21	0,28	…	0,62	0,24	0,36		

Валідність.

Дамо декілька визначень поняття валідності.

1. Валідність – придатність тестових результатів для тієї мети, заради чого проводилось тестування [2].
2. Валідність – це характеристика вміння тесту служити поставленій меті вимірювання [3].
3. Валідність – визначає, наскільки тест відображає те, що він повинен оцінювати [4].

Для оцінки валідності тесту зазвичай використовують кореляцію між показниками тесту і деяким зовнішнім критерієм. За такої оцінки дуже важливо вибрати значущий зовнішній критерій. Процес валідації у даному випадку ускладнюється необхідністю встановлення міри узгодженості оцінок експертів, котрих, зазвичай, буває не менше трьох чоловік. Для педагогічних тестів у якості критерію звичайно беруться оцінки, що були виставлені підчас традиційної перевірки знань студентів без застосування тестів, або на основі поточної успішності.

Розрізняють різноманітні види валідності: змістовна, концептуальна, критеріальна, поточна, прогностична та ін.

Валідність визначається за формулою (5):

$$V = \frac{\frac{\sum_{i=1}^{n}(Y_i * y_i)}{n} - \overline{Y} * \overline{y}}{S_Y - S_y} * \frac{n}{n-1} \qquad (5)$$

де:

n – кількість студентів;
i – порядковий номер студента;
Y_i – експертна оцінка i-го студента;
$\overline{Y}$ – середнє арифметичне експертних оцінок;
S_y – стандартне відхилення кількості правильних відповідей;
S_Y – стандартне відхилення експертних оцінок.

$$\overline{Y} = \frac{\sum_{i=1}^{n} Y_i}{n}, \quad S_y = \sqrt{\frac{\sum_{i=1}^{n} (y_i - \overline{y})^2}{n-1}}, \quad S_Y = \sqrt{\frac{\sum_{i=1}^{n} (Y_i - \overline{Y})^2}{n-1}} \qquad (6)$$

Проведемо розрахунки, враховуючи формули (1- 6) та табл. 1 і отримаємо значення коефіцієнта валідності.

Для інтерпретації значення коефіцієнта валідності застосовують наступні критерії:

Значення коефіцієнта	Інтерпретація
від 0,6 до 1,0	Висока валідність тесту
від 0,3 до 0,6	Середня валідність тесту
< 0,3	Низька валідність тесту

У нашому випадку значення коефіцієнта валідності рівне 0,97, що свідчить про високу валідність тестових завдань, тобто тест достатній для того щоб прийняти рішення хто як вчиться. Для того щоб підвищити валідність тесту завдання повинні мати оптимальну складність. Щоб забезпечити нормальний закон розподілу балів по тесту, необхідно провести експертизу якості змісту тесту за допомогою третіх осіб, час виконання тесту повинен бути оптимальним, завдання повинні бути з високою дискримінативністю.

Дискримінативність.

Дискримінативність – це здатність тестових завдань диференціювати (розділити) студентів за ознакою максимального чи мінімального результату. Це поняття введене для того, щоб унеможливити створення неякісних тестових завдань.

Для обчислення коефіцієнта дискримінативності застосуємо метод крайніх груп. Суть цього методу полягає в тому, що при розрахунку дискримінативності тестового завдання враховуються результати найбільш та найменш успішних тестованих. Кількість учасників крайніх груп залежить від величини вибірки, а саме, чим більша вибірка, тим меншу кількість тих що підлягають тестуванню можна залучати в обидві групи. Кількість тестованих в кожній групі повинна бути однаковою і знаходитись в межах від 10% до 33% від загальної

кількості тестованих. У даному випадку ми використаємо 27% для кожної групи, тобто по 7 чоловік у групі, тому що цей відсоток в теорії вважається найкращим для забезпечення максимальної точності визначення коефіцієнта дискримінативності. Індекс дискримінативності обчислюється як різниця між частиною осіб, що правильно розв'язали задачу, з найбільш і найменш успішної групи.

$$D = \frac{Nn_{\max}}{N_{\max}} - \frac{Nn_{\min}}{N_{\min}} \qquad (7)$$

де: $N_{min}=N_{max}$ – загальна кількість тестованих у крайніх групах (27%); Nn_{min} – кількість студентів в групі гірших, що правильно виконали завдання тесту; Nn_{max} – кількість студентів в групі кращих, що правильно виконали завдання тесту.

Результати тестування подані у таблиці 2.

Проведемо розрахунки, враховуючи формулу (7) і отримаємо значення коефіцієнта дискримінативності.

Для інтерпретації значення коефіцієнта дискримінативності застосовують наступні критерії:

Значення коефіцієнта	Інтерпретація
від 0,3 до 1,0	Висока дискримінативність тесту
від 0,1 до 0,3	завдання потрібно проаналізувати на придатність до використання в тесті (низька диференціальна здатність)
< 0,1	завдання неякісне – краща група відповідає гірше, ніж слабша

У нашому випадку значення коефіцієнта дискримінативності рівне 0,39, що свідчить про високу дискримінативність тестових завдань.

Коефіцієнт дискримінативності може приймати значення у межах від -1 до +1. Високе позитивне значення коефіцієнта дискримінативності тестового завдання свідчить про вірний розподіл тестованих на групи, високе від'ємне значення

свідчить про непридатність даної задачі для цього тесту, тобто її невідповідність сумарному результату.

Таблиця 2.

Кандидат	**1**	**2**	**3**	**4**	**5**	**…**	**27**	**28**	**29**	**30**	**Разом**
19	0	0	0	0	0		1	0	1	0	11
6	1	0	0	0	1		1	0	0	0	11
2	0	0	1	0	0		1	0	1	0	12
7	1	1	1	1	0		1	1	0	0	19
24	1	0	1	1	1		1	0	1	1	21
16	1	1	1	0	1		1	0	1	1	23
17	1	1	1	1	0		1	1	1	1	27
Nmax	5	3	5	3	3		7	2	5	3	
1	0	0	0	0	1		0	0	0	0	5
25	0	0	0	0	0		0	0	0	0	5
26	0	0	0	0	0		0	1	1	1	6
28	0	0	0	0	0		0	0	0	0	6
3	0	0	1	0	0		0	0	1	0	7
27	0	0	0	0	0		0	0	1	0	6
5	0	0	0	0	1		0	0	1	1	7
Nmin	0	0	1	0	2		0	1	4	2	
Індекс дискримінативності	0,7	0,4	0,6	0,4	0,1	…	1,0	0,1	0,1	0,1	0,39

У нашому випадку з таблиці 2 видно, що завдання 5, 28, 29, 30 – неякісні, краща група відповідає гірше, ніж слабша.

Для забезпечення високого рівня дискримінативності потрібно щоб ваші тести не були занадто складними; формулювання повинні бути прозорі; жодних неоднозначностей; розв’язки повинні бути неочевидними; варіанти відповідей повинні бути реальні, тобто не абсурдні; не може бути декілька варіантів відповідей, якщо вони неоговорені спеціально.

1. Аванесов В. С. Форма тестовых заданий: учеб. пособие / В. С. Аванесов. М.: Центр тестирования, 2005. – 120 с.
2. Майоров А. Н. Теория и практика создания тестов для системы образования. — Москва: «Интеллект-Центр», 2002. – 296 с.
3. Аванесов В.С. Теория и методика педагогических измерений (материалы публикаций). – М.: ЦТ и МКОУГТУ-УПИ, 2005. – 98 с.

Алгоритм оцінювання якості машинного перекладу англо-української мовної пари

Левус Євгенія Василівна,

доцент кафедри програмного забезпечення Національного університету «Львівська політехніка», кандидат технічних наук, доцент

Бода Ольга Богданівна,

здобувач ступеня магістра Національного університету «Львівська політехніка»

Зростання кількості систем машинного перекладу (МП) зумовлює необхідність в розробці і розвитку надійних способів оцінки якості МП. МП є альтернативним рішенням до традиційного перекладу, здійсненого людиною-експертом, а тому повинен відповідати певним критеріям, які забезпечують комунікативну еквівалентність вихідного тексту до його оригіналу. Виділяють три основні вимоги до перекладу, а саме:

- переклад має забезпечувати збереження послідовності викладу та змісту оригінального тексту;
- переклад повинен відповідати синтаксичним та стилістичним нормам мови перекладу;
- об’єм перекладеного тексту повинен бути приблизно таким самим як і об’єм вхідного тексту.

На жаль, МП практично не забезпечує виконання усіх перерахованих вимог. Це пояснюється недосконалістю алгоритмів перекладу, оскільки дуже важко, а то й неможливо при його

розробці врахувати усі синтаксичні особливості різних мов світу.

Наприклад, текст «Older HTTP/1.0 clients assumed a one-to-one relationship of IP addresses and servers; there was no other established mechanism for distinguishing the intended server of a request than the IP address to which that request was directed. The changes outlined above will allow the Internet, once older HTTP clients are no longer common, to support multiple Web sites from a single IP address, greatly simplifying large operational Web servers, where allocation of many IP addresses to a single host has created serious problems» буде перекладано програмою-перекладачем Google Translate таким чином.

«Більш старі клієнти HTTP / 1.0 прийшли до взаємовідносин IP-адрес та серверів; не існувало іншого встановленого механізму для розмежування призначеного сервера запиту, ніж IP-адреса, на яку був спрямований цей запит. Зміни, викладені вище, дозволять Інтернет, коли колись старі HTTP-клієнти більше не є загальними, підтримувати кілька веб-сайтів з однієї IP-адреси, значно спрощуючи великі операційні веб-сервери, де виділення багатьох IP-адрес для одного хоста викликало серйозні проблеми».

Останнім часом якість комп'ютерного перекладу покращилася завдяки застосуванню в алгоритмах перекладу систем штучного інтелекту. Проте існують проблеми з граматичними та синтаксичними зв'язками у реченні, з відтворенням термінології.

Дослідження ефективності застосування автоматичних метрик оцінювання якості МП для англо-української мовної пари є надзвичайно важливим і зумовлене значними відмінностями в синтаксичній побудові речень, що впливає на якість перекладу. Автоматичні методи оцінки МП мають свої підходи до реалізацій, різновиди, та алгоритми роботи, що спрямовані на більш глибоку та повноцінну оцінку якості МП.

Метрики BLUE та METEOR базуються на використанні та підрахунку n-грам між еталонним та машинним перекладами. Метрика TER базується на підрахунку кількості виправлень, які

необхідно зробити у машинному перекладі, щоб він відповідав еталонному перекладу. До основних недоліків метрики BLEU можна віднести його ненадійність при роботі з одним еталонним перекладом (ЕП). Алгоритм працює з великими текстами і залежить від кількості еталонних джерел. Також недоліком є неврахування збігу синонімів і неможливість відслідкувати велику кількість правильних порядків слів. З цього випливає, що семантична якість перекладу не визначається метрикою BLEU.

Для точного оцінювання якості МП необхідно одночасно застосовувати декілька метрик. Це дозволяє провести критичний аналіз вхідного тексту як на плавність, так і на адекватність. Саме тому доцільно виділити основні переваги та недоліки автоматичних метрик та скомбінувати їх таким чином, щоб мінімізувати негативні сторони представлених алгоритмів, і навпаки – максимізувати сильні сторони представлених метрик.

Таблиця 1.

Порівняльна характеристика BLUE, METEOR, TER

	TER	BLUE	METEOR
Використовує n-грам	ні	так	тільки юніграми
Використовує синоніми	ні	ні	так
Проводить стемінг слів	ні	ні	так
Орієнтована на точність	ні	так	ні
Використовує декілька еталонних перекладів одночасно	ні	так	ні
Вираховує кількість помилок	так	ні	ні

Модифікація метрики BLUE полягає у поєднанні основних характеристик METEOR та BLUE (Рис. 1). А саме: обчислення коефіцієнта точності метрики BLUE з врахуванням зовнішніх лінгвістичних знань. Для дослідження оцінки якості МП створено програмну систему та набір тестових даних різної структури та довжини. МП виконувався онлайн системою перекладу Google Translate.

Основною ідеєю для проведення досліджень є визначення результатів оцінювання МП за допомогою вищезгаданих

алгоритмів на англомовних текстах, які розподілені за синтаксичною структурую на групи.

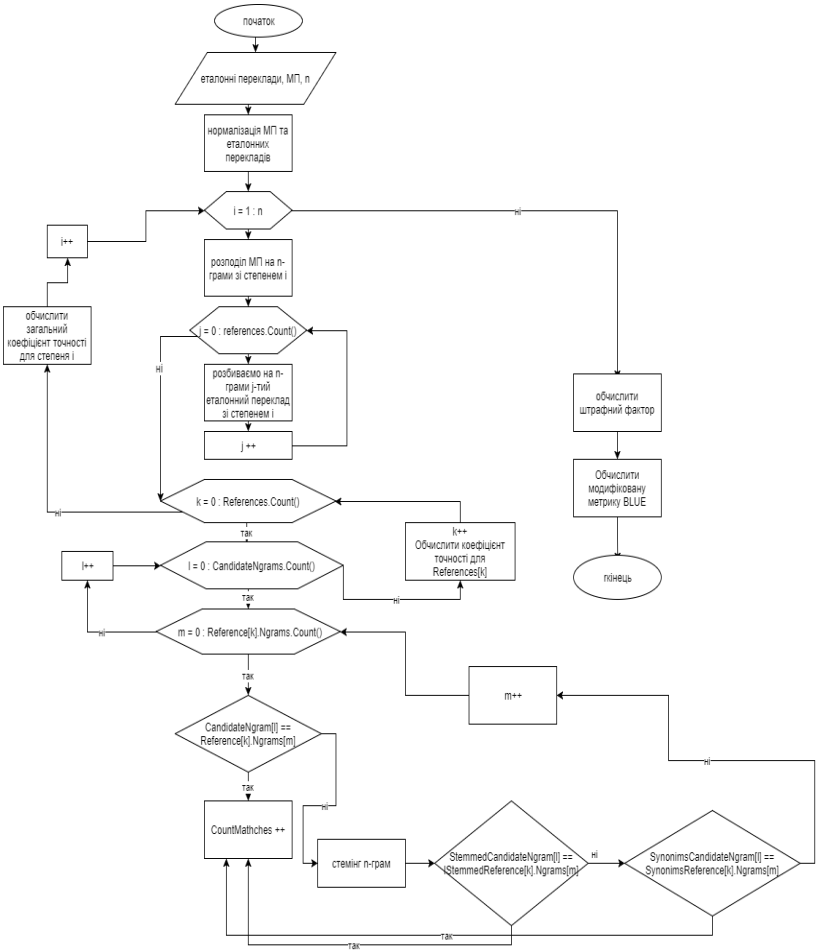


Рис.1. Блок-схема модифікованого алгоритму BLUE.

Серед важливих результатів досліджень:

1. Оцінювання складнопідрядних речень показало, що оцінка представлених алгоритмів дещо відрізняється від оцінки експерта. Модифікований алгоритм BLUE показує точніші результати серед представлених метрик.

2. Результати оцінювання перекладу пасивних речень є менш якісними. Найкращу оцінку надала метрика METEOR. З результатів роботи метрик BLUE та її модифікованої версії можна зробити висновок, що переклад таких речень націлений тільки на адекватність. При перекладі пасивних речень алгоритм перекладу потрібно покращувати. Особливо важливим це є з точки зору перекладу технічної літератури.

Таблиця 2.

Результати роботи алгоритмів для складносурядних речень

	BLUE	METEOR		Оцінка експерта	Модифікований BLUE
1-грам	0,8106	ЕП1	ЕП2	0.69	0,8312
2-грам	0,5732				0,6128
3-грам	0,3483	0,3863	0,4008		0,4002
4-грам	0,1912				0,2323
Оптимальна оцінка	0,48	0.39			0,52

Висновок. Позитивні результати оцінювання якості машинного перекладу метрики показали при їх використанні для простих розповідних, складносурядних та складнопідрядних речень. Оцінка використаних метрик, а зокрема, модифікованої версії BLUE має найменшу кореляцію з експертною оцінкою так коливається від 3% до 17%.

1. Яковина В. С. Огляд та аналіз метрик оцінювання якості машинного перекладу / В. С. Яковина, В. В. Масюкевич. // УДК 81’322.4:004.912. – 2013. – С. 103-105.
2. Papineni, K., Roukos, S., Ward, T., and Zhu, W.-J. (2002). Bleu: a method for automatic evaluation of machine translation. In Proceedings of ACL, pages 311-318.
3. Lavie A. METEOR: An automatic metric for MT evaluation with high levels of correlation with human judgments / A. Lavie, A. Abhaya. // Proceedings of the Second Workshop on Statistical Machine Translation. – 2007. – С. 228-231.

Використання системи візуалізації 3D-об'єктів у навчальному процесі

Мельничин Андрій Володимирович,

доцент кафедри теорії оптимальних процесів Львівського національного університету імені Івана Франка, кандидат технічних наук, доцент

Стрімкий розвиток комп'ютерного, апаратного і різноманітного програмного забезпечення сприяє якісним змінам у традиційних технологіях обробки інформації. З'являються нові нетрадиційні технології, в тому числі й такі, що змінюють сам стиль використання комп'ютерів. Серед них найбільш динамічно розвиваються мережні технології, комп'ютерна графіка, тривимірне моделювання й анімація тощо.

Комп'ютерна графіка є важливою компонентою освіти сучасного спеціаліста. В багатьох випадках потреби в графіці можуть бути забезпечені різними існуючими графічними бібліотеками та системами. Однак, постійно виникає необхідність створювати спеціальні графічні програмні засоби. Саме таким засобом на сьогоднішній день є система візуалізації 3D-об'єктів.

Актуальність дослідження тематики 3D-технологій зумовлена швидким розвитком сучасної обчислювальної і мультимедійної техніки в повсякденному житті. Методи відновлення просторової конфігурації тривимірних об'єктів за їх стереозображеннями використовуються в багатьох галузях науки і техніки. Маючи тривимірну поверхню, можна більш якісно та точно виконати процес розпізнавання об'єктів, що знаходяться на них, ніж виконуючи розпізнавання за двомірним зображенням. У системах розпізнавання на основі двомірних зображень є основний істотний недолік – немає можливості повною мірою побачити фігуру у 3D вимірі, оскільки її поверхня буде плоскою.

Системи, які використовують тривимірні моделі для розпізнавання є більш точними та надійними. Сьогодні

використовують 3D принтери для створення різних об’єктів: від проектування будинків, до створення органів.

У 3D системах створюють ландшафтні дизайни, проекти квартир та ін. Останнім часом з’являється все більше автоматизованих систем побудови тривимірних об’єктів, які майже не потребують участі людини у цьому процесі. Але для отримання якісного результату застосовується складна та дорога техніка.

На сьогоднішній день у світі існує багато систем візуалізації 3D-об’єктів, проте жодне з існуючих рішень не має можливості проектувати просторові фігури. У даній роботі пропонується варіант системи проектування геометричних об’єктів у 3D-просторі за мінімальних затрат. Розроблене програмне забезпечення надає можливість будувати віртуальні просторові об’єкти згідно параметрів, які користувач зможе ввести відповідно до обраного ним класу об’єкта.

У роботі для створення системи візуалізації 3D-об’єктів використано основи побудови просторових геометричних фігур, моделі їх оптимізації, а також математичні основи комп’ютерної графіки з використанням алгоритмів спрощення 3D-полігональних об’єктів і афінних перетворень у просторі.

Враховуючи затрати на процес реалізації, для спрощення системи використано основні алгоритми побудови об’єктів векторної графіки, що базуються на побудові графічних примітивів, таких як лінії, що з’єднуються вузлами. Слід зауважити, що для побудови складніших об’єктів, кількість таких вузлів значно зростає.

У зв’язку з вище сказаним пропонується використання ітераційних алгоритмів, що дає змогу спростити полігональні моделі, які в свою чергу можна поділити на два типи:

- моделі на основі прориджених вершин;
- моделі, що базуються на методах згортання ребра.

Найшвидшим алгоритмом геометричного спрощення, що належить до категорії проріджування вершин, є алгоритм кластеризації вершин.

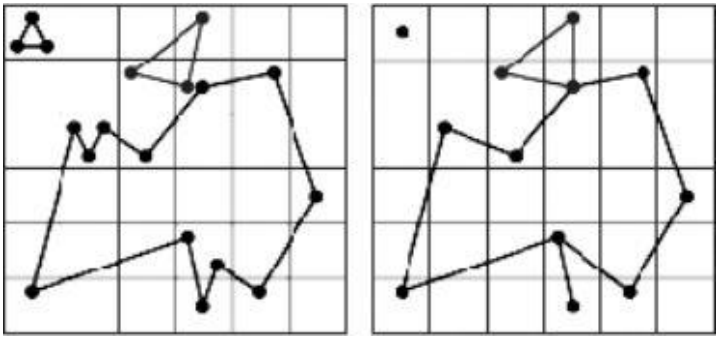


Рис.1. Етапи виконання алгоритму кластеризації вершин

Даний метод полягає в об'єднанні вершин, що містяться в одному кластері простору, в одну. Кластери утворюють собою тривимірну сітку, тобто координати вершин фактично заокруглюються із заданою точністю, а у разі збігу кількох вершин, після заокруглення, ці вершини замінюються однією.

На противагу розрідженню, згортання ребра передбачає операцію злиття двох вершин, які утворюють ребро, в одну (рис. 2). При цьому, в загальному випадку, відбувається видалення двох трикутних комірок. Кількість ітераційних кроків визначається досягненням заданої кількості граней або деякого порогового значення.

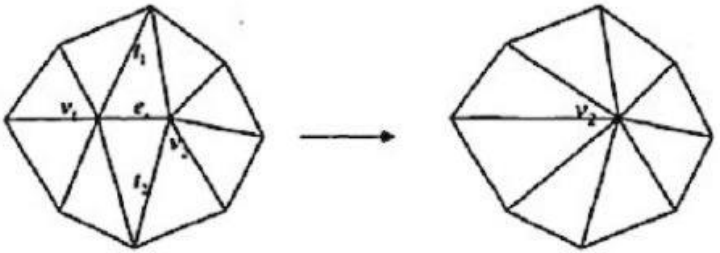


Рис. 2. Процедура згортання ребра e_r *. Вершина* V_1 *переноситься у вершину* V

Подібно до більшості завдань спрощення, також виникає проблема вибору між якістю представлення 3D-моделей і швидкодією їх відтворення. Критерієм ефективності прийнято вважати власне швидкодію.

Обертання об'єктів здійснюємо застосовуючи загальну форму афінних перетворень у просторі, що задається системою рівнянь:

$$\dot{x} = ax + by + ez + m,$$
$$\dot{y} = cx + dy + fz + n,$$
$$\dot{z} = gx + hy + pz + l,$$

де $(\dot{x}, \dot{y}, \dot{z})$ – точки (вектори), що одержуються в результаті цих перетворень.

На сьогоднішній день існує багато продуктів для створення та демонстрації 3D об'єктів, проте кожен з них або громіздкий і потребує значних апаратних потужностей, або платний у використанні.

Використавши існуючі джерела інформації було створено власний додаток для проектування даних фігур.

При цьому для створення програми застосували спосіб побудови зображень за допомогою векторної графіки та скористалися системою координат для побудови просторових зображень.

1. Cohen J., Varshney A., Manocha D., Turk G., Weber H., Agarwal P., Brooks F. and Wright W. Simplification Envelopes. // In ACM SIGGRAPH 96 Conference Proceedings, – 2001 – P. 119–128.
2. Institute for Data Analysis and Visualization [Електронний ресурс] – Режим доступу: http://graphics.cs.ucdavis.edu – Назва з екрана.
3. Анісімов В.А., Терещенко В.М., Кравченко І.В. Основні алгоритми обчислювальної геометрії: Навч. посібн. – К.: Київський університет, 2002. – 82 с
4. Комп'ютерна графіка та обчислювальна геометрія [Електронний ресурс] – Режим доступу: http://cg.unicyb.kiev.ua – Назва з екрана.

Використання пошуку інформації з відкритих джерел мережі Інтернет у навчальному процесі Дніпропетровського державного університету внутрішніх справ.

Прокопов Сергій Олександрович,

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

В епоху розвитку інформаційних технологій все більше джерел інформації знаходить своє відображення в мережі Інтернет. Практично кожна людина залишає свій інформаційний слід у віртуальному середовищі. Це і спілкування у соціальних мережах, і розміщення своїх резюме, і закази у інтернет-магазинах з відображеннями особистих даних, і відомості у електронних реєстрах та інше.

У працівників Національної поліції, в рамках виконання службових обов'язків, доволі часто виникає необхідність пошуку інформації стосовно осіб, які попадають у поле зору правоохоронців по кримінальним провадженням, оперативним розробкам та іншим заходам. Необхідна інформація не завжди є у інформаційних ресурсах Національної поліції, або є, але її не достатньо.

З метою підготовки якісних фахівців для підрозділів Національної поліції у Дніпропетровському державному університеті внутрішніх справ в навчальний процес при вивченні дисциплін «Застосування комп'ютерних технологій Національної поліції» та «Інформаційне забезпечення професійної діяльності» була запроваджена тема «Методика організації пошуку інформації у відкритих джерелах мережі Інтернет».

При вивченні даної теми курсантам надається інформація стосовно особливостей організації простого та розширеного пошуку інформації у пошукових серверах мережі Інтернет, вивчаються логічні та синтаксичні вирази пошукової системи

Гугл. Курсанти опановують навички метапошукових серверів глобальної мережі Інтернет та спеціалізованих метапошукових програмних компонентів, таких як:

- Debriefing (http://www.dogpile.com) Потужна метапошукова система Dogpile використовує для метапошуку не тільки пошукові системи, але і FTP-сервери, а також новинні сайти, котирування фондових бірж і навіть «жовті сторінки» Інтернету.
- Ixquick (https://www.ixquick.com) - система метапошуку Ixquick працює з десятьма зовнішніми базами. Це пошуковики Bing, Yahoo! Ask, All the Web, Cuil, Entire Web, Gigablast, каталоги Qkport і Open Directory, а також Wikipedia. У списку баз відсутня Google, однак охоплення альтернативних систем варто визнати досить широким. Підтримується пошук на вісімнадцяти мовах, в тому числі російською.
- SiteSputnik;
- PDS Поисковик;
- Info Pilot

Також вивчаються методики пошуку людей в глобальних мережах за допомогою он-лайн сервісів, таких як:

- Pipl (https://pipl.com): пошук людей в «невидимому» Інтернеті. Запит в пошуковику Pipl допоможе знайти «невидимі» веб-сторінки, які не можна знайти на регулярних пошукових системах. На відміну від типових пошуковиків, Pipl призначений для отримання інформації з Deep Web. Його роботи вміють взаємодіяти з базами даних для пошуку і вилучення фактів, контактних даних та іншої відповідної інформації з особистих профілів, каталогів, наукових публікацій, протоколів судових засідань та інших численних джерел «глибинної» Мережі.
- Yatedo (https://www.yatedo.com) – он-лайн сервіс для пошуку інформації пов'язаних з людьми. Ви можете просто ввести ім'я людини і з'являться всі он-лайнові результати, що мають відношення до введеного Вами імені. Якщо можливо, то будуть показані в результатах резюме і

фотографія кожної людини в мініатюрі. При натисканні на результат відкриються публічно доступні дані людини. Ви можете фільтрувати ці деталі для отримання новин, оновлень, документів і книг.

Курсанти навчаються пошуку інформації у соціальних мережах за допомогою наступних оболонок:

- Webmii (http://webmii.com) – відображає інформацію про людину, отриману з різних соціальних мереж, сайтів і онлайн-документів. Кожна людина також має свій власний PeopleRank (ранг популярності) який є оцінкою його видимості в Інтернеті. WebMii використовує такі різні сайти, як Facebook, Friendster, Google, Twitter і Yahoo для збору інформації. Крім того, сайт містить посилання на Xing і Friendfeed.
- Snitch.Name (http://snitch.name) – дозволяє шукати людину на сайтах соціальних мереж за його ім'ям і прізвищем та видавати результат пошуку в одному інтерфейсі. Замість того, щоб Ви йшли і окремо шукали когось на Facebook, Twitter, Flickr або MySpace – сервіс надає Вам результати пошуку з цих сайтів в окремих блоках на одній сторінці.

Приділяється увага використанню пошуку інформації в довідково-інформаційних базах даних вільного доступу (державних реєстрів), у посібнику їх близько 80 [1].

На кожному з практичних занять курсанти виконують практичні вправи з пошуку наданих викладачами осіб. На занятті використовуються змагальний принцип – курсанти поділяються на команди, оцінка за заняття ставиться відповідно до швидкості та якості представленого звіту.

Використання у навчальному процесі методики пошуку інформації з відкритих джерел мережі Інтернет дає можливість курсантам отримати практичні навички пошуку необхідної інформації не тільки у інформаційно-пошукових системах Національної поліції, але і у розповсюджених інтернет-ресурсах. Розвиває у них здібності до аналітичної роботи, що позитивно відображується на якості підготовки правоохоронців.

1. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Застосування комп'ютерних технологій в Національній поліції: Навчальний посібник – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – 161 с.

Досвід запровадження проекту «ЛІНІЯ-102» у Дніпропетровському державному університеті внутрішніх справ

Рижков Едуард Володимирович,

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

Відчуваючи свою відповідальність перед суспільним запитом щодо якісної підготовки поліцейських нової генерації та підготовки педагога із стратегічним і мобільним мисленням, в рамках педагогічного експерименту у Дніпропетровському державному університеті внутрішніх справ запроваджена новітня форма підготовки курсантів, студентів та практичних працівників Національної поліції із використанням емулятора платформи інформаційно-технічного забезпечення Національної поліції, розширеного переліку інтерактивних навчальних приміщень та навчальної зали судових засідань під умовною назвою «Лінія 102».

На першому етапі підготовка реалізована в рамках комплексних оперативно-тактичних навчань із курсантами випускного курсу та студентами юридичного факультету як різновид позанавчальної роботи. На другому етапі реалізації проекту можливості інтерактивного комплексу запроваджені у курсантів та студентів у основний навчальний процес.

На другому етапі навчань передбачені навчальні судові засідання, в процесі яких наочно демонструються окремі елементи судової практики та алгоритм розгляду напрацьованих матеріалів кримінальних проваджень.

На першому і другому етапах значна роль відведена не лише науково-педагогічному складу, але й представникам практичних підрозділів, які активно залучаються для надання консультативної та практичної допомоги при виконанні вправ та під час спільного з курсантами та студентами підведення підсумків.

Представлений комплекс є максимально ефективним з точки зору набуття та вдосконалення умінь та навичок здобувачами вищої освіти в процесі виконання оперативно-службових завдань, юридичної та судової практики в умовах, максимально наближених до реальних.

В процесі занять курсанти засвоюють комплекс практичних заходів працівників різних підрозділів поліції, набувають та вдосконалюють навички: опрацювання первинної інформації про кримінальні та інші правопорушення, порядку реєстрації такої інформації, роботі у складі наряду патрульної служби, слідчо-оперативної групи, складання реєстраційних та процесуальних документів, користування технічними засобами фіксації інформації, кваліфікації правопорушень, процесуального порядку проведення слідчих (розшукових) дій, тактичних прийомів дій працівників поліції, аналізу отриманої інформації, взаємодії між працівниками різних підрозділів, прояву винахідливості, ініціативи та самостійності. Студенти оволодівають навичками юридичного забезпечення учасників кримінального провадження та кримінального судочинства.

Таким чином, в університеті в рамках науково-практичного та педагогічного експериментів започатковано пілотний проект, в процесі якого реалізовано повний замкнутий цикл відпрацювання навчальних фабул від отримання первинної інформації про правопорушення до винесення судом відповідного вироку. Безумовною перевагою проекту є його практична спрямованість. За сучасною методикою рольової гри курсанти, студенти та працівники Національної поліції набувають практичних навичок, вивчають та поглиблюють теоретичний матеріал. Максимальна наочність та наближеність до реальних умов підвищує їх мотивацію до навчання здобувачів вищої освіти, сприяє підготовці мотивованого

педагога із нестандартним творчим мисленням. Комплексність у вирішенні навчальних задач сприяє розумінню взаємодії між собою різних суб'єктів правоохоронної, правозастосовної та судової практики.

Робочою групою з числа науково-викладацького складу університету був розроблений Порядок проведення комплексних оперативно-тактичних навчань, який після затвердження науково-методичною радою університету впроваджено у навчальний процес.

Комплексні оперативно-тактичні навчання як різновид позанавчальної роботи проводились відповідно до затвердженого ректором університету графіка проведення навчань.

Крім цього додатково розроблено Положення про проведення професійно-орієнтованої ділової гри «Лінія-102», яка в рамках оперативно-тактичних навчань запроваджена в основний навчальний процес курсантів та студентів.

Таким чином у Дніпропетровському державному університеті внутрішніх справ вперше в системі МВС створено Навчально-інтерактивний комплекс з підготовки здобувачів вищої освіти та практичних працівників Національної поліції, який передбачає повний замкнутий цикл опрацювання інформації про протиправні діяння від її надходження на лінію 102, збору доказової інформації в рамках кримінального провадження до розгляду матеріалів у судовому засіданні в рамках реалізації правозастосовчої, правоохоронної та судової функції та створено інноваційну педагогічну методику для навчальних закладів зі специфічними умовами навчання.

Науково-викладацьким складом кафедри економічної та інформаційної безпеки разом із керівництвом НМВ розроблені та запроваджені у навчальний процес Методичні рекомендації щодо проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції (протокол НМР № 7 від 23.03.2017).

Кафедрою з основними учасниками гри кожної навчальної групи курсантів були проведені додаткові факультативні заняття

щодо якісного засвоєння інформаційно-технічної складової та здійснені заходи щодо вдосконалення робочого місця слідчого на базі наявної навчальної програми емулятор робочої комп'ютерної програми «ЄРДР».

Ділова гра проводились відповідно до затвердженого розкладу навчальних занять.

За другий семестр 2016-2017 навчального року було проведено 96 занять, в яких прийняли участь 10 навчальних груп курсантів та 4 групи студентів юридичного факультету.

До проведення занять були залучені 14 практичних працівників патрульної поліції, слідчих та оперативних підрозділів Національної поліції.

Проведення гри проводилось із використанням повного комплексу матеріально-технічного забезпечення: автотранспорт, рації, криміналістична техніка, планшети, навчальна зброя, спеціальні засоби, відеокамери, програмно-апаратні комплекси, обліки МВС. Сформовано відповідну відеотеку, матеріали якої можуть бути використані в подальших навчальних заняттях.

Курсантами та студентами кожної навчальної групи за результатами проведеної гри були напрацьовані комплекти процесуальних документів в рамках навчальних кримінальних проваджень та судових засідань, які в рамках реалізацію проекту «Лінія 102» проводились вперше. Всього проведено 12 судових засідань.

До проведення ділової гри були залучені працівники відділення психологічного забезпечення університету. Ними проведені попередні інструктажі-консультації, забезпечена безпосередня участь в процесі гри та анкетування курсантів за підсумками проведених занять.

Кафедрою підготовлено навчальний посібник (протокол НМР № 22 від 07.06.2017), один з розділів якого передбачає вивчення навчального матеріалу, що використовується в рамках проекту «Лінія 102».

На наш погляд, запровадження проекту «Лінія 102» у курсантів та студентів 3 курсу як педагогічний експеримент, проведений в

університеті, себе виправдав, але потребує подальшого вдосконалення.

Проведені навчальні заняття сприяли формуванню професійних навичок у курсантів та студентів університету та позитивно вплинули на мотиваційну складову навчального процесу.

З метою популяризації проекту та закріплення за університетом авторських прав кафедрою у співавторстві з керівництвом отримано деклараційний патент на корисну модель «Система управління нарядами мобільної патрульної служби» (висновок МЕРТ України №12898/ЗУ/17 від 06.06.2017). Подані відповідні матеріали на здобуття Державної премії в галузі освіти у 2017 р.

На виконання наказу № 141 від 24.02.2017 Дніпропетровського державного університету внутрішніх справ у 1 семестрі 2017-2018 н. р. з курсантами 4 курсів факультетів ПФПКМ та ПФПДР були продовжені заняття з елементами професійно-орієнтованої ділової гри «Лінія 102».

Заняття проводились в рамках навчальних годин, передбачених для проведення комплексних штабних навчань із додатковим залученням до випускаючих кафедр ОРД та СТ і кримінального процесу науково-викладацького складу кафедр кримінального права, криміналістики, ЕтаІБ.

За другий семестр поточного навчального року було проведено 20 занять в рамках КШН, в яких прийняли участь 10 навчальних груп курсантів та 6 занять в рамках тренінгу із залученням курсантів двох навчальних груп.

До проведення занять були залучені практичні працівники патрульної поліції, слідчих та оперативних підрозділів Національної поліції, чергової частини, керівництво відділу поліції, обласної прокуратури та медичної установи.

Проведення рольової гри проводилось із використанням повного комплексу матеріально-технічного забезпечення: автотранспорт, рації, криміналістична техніка, планшети, навчальна зброя, спеціальні засоби, відеокамери, програмно-апаратні комплекси, обліки МВС.

Сформовано відповідну відеотеку, матеріали якої можуть бути використані кафедрами в подальших навчальних заняттях.

Курсантами кожної навчальної групи за результатами проведеної гри були напрацьовані комплекти оперативно-розшукових та процесуальних документів в рамках навчальних оперативно-розшукових справ, кримінальних проваджень та судових засідань. Проведено 10 тематичних судових засідань.

З метою створення додаткових ситуативних ввідних до проведення ділової гри були залучені представники інших підрозділів університету та студенти.

З початку поточного навчального року з метою якісного засвоєння знань та набуття попередніх навичок до навчальних дисциплін з комп'ютерної тематики у курсантів 3 та 4 курсів розпочато викладання спеціалізованої тематики за «Лінії-102». Крім цього, з метою запровадження окремим сегментом у існуючий проект розпочато викладання матеріалу з аналітичної тематики.

З метою популяризації інноваційних здобутків університету неодноразово проведено демонстрацію результатів функціонування «Лінії-102» делегатам, що перебували в ДДУВС протягом семестру.

Платформа використана при проведенні у листопаді 2017 року квесту з потенційними абітурієнтами та під час інших заходів профорієнтаційного характеру.

В університеті 26-27 жовтня 2017 року серед вишів МВС проведено тематичний тренінг, за результатами якого маємо позитивну реакцію представників команд-учасників та керівництва. Так, наприклад, від керівництва Львівського державного університету внутрішніх справ на адресу університету надійшов лист з проханням про використання в навчальному процесі набутого нами досвіду з проведення «Лінії-102», функціонування її інформаційно-технічної платформи та методичного забезпечення.

З метою запровадження методичних та технічних напрацювань за «Лінією-102» в інших навчальних закладах підготовлено

відповідного листа до Департаменту персоналу, організації освітньої та наукової діяльності МВС України.

Завдяки проведеному тренінгу кафедрами якісно відпрацьовані раніше підготовлені фабули ситуативних задач. Набуто цінний досвід співпраці.

Отримано пропозицію з боку керівництва Національної академії прокуратури України щодо дистанційної он-лайн участі представників прокуратури в діловій грі на етапах відпрацювання роботи слідчо-оперативної групи та виконання функції прокурора на досудовому розслідуванні та у суді.

З метою опрацювання в університеті економічної тематики кафедрами розпочато напрацювання таких тематичних задач та заплановано на грудень 2017 року кафедрою ОРД та СТ проведення у позанавчальній формі тренінгів із використанням сегментів «Лінії-102».

З метою розширення можливостей існуючої навчальної платформи керівництву університету надані пропозиції щодо створення навчального відділу поліції та полігону щодо проведення оперативно-технічних заходів.

В університеті реалізовано перший етап щодо встановлення повного покриття якісним Wi-Fi основної зони проведення ділової гри.

Таким чином, використання Навчально-інтерактивного комплексу «Лінія-102» створює унікальні умови щодо розвитку творчого потенціалу суб'єктів педагогічної діяльності, формує актуальну педагогічну майстерність, на прикладному рівні пов'язує навчальний процес з практичною складовою майбутньої професії, скорочує терміни набуття здобувачами вищої освіти практичних навичок, суттєво підвищує їх мотивацію до навчання, сприяє формуванню емоційно-психологічної стійкості у майбутніх поліцейських, створює умови для заглиблення у аспекти суміжної юридичної та правоохоронної діяльності на навчальному етапі набуття професії, сприяє вдосконаленню навчального процесу у закладах зі специфічними умовами навчання, формує іміджевий потенціал нової поліції.

Методологія застосування інформаційних технологій у ВНЗ із специфічними умовами навчання

Савайда Олена Іванівна,

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

Безперечно, проблема застосування інформаційних технологій правоохоронними органами та ВНЗ зі спеціальними умовами навчання в Україні в сучасних умовах розвитку держави знаходиться на найактуальнішому рівні. Тому, наша зацікавленість в першу чергу, буде стосуватися саме тих інформаційних технологій, які безпосередньо розробляються, використовують та реалізовуються в ВНЗ зі спеціальними умовами навчання, оскільки ми саме належимо до вказаної системи та безпосередньо приймаємо участь у використані вказаних інформаційних технологій під час навчання та реалізації навчального матеріалу.

Як відомо, інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів та тих, хто навчається. Перераховані у визначенні вище способи та методи в певній мірі становлять частину наукової методології, яка є базо для всіх соціальних сфер діяльності людини, й відносин у юридичній діяльності в тому числі.

Звичайно, світ інформаційних технологій швидко та ефективно розвивається. Тому, нові інформаційні та комунікаційні системи, безперечно полегшують та дають нові можливості для навчання та для майбутньої роботи, багато в чому полегшують навчання та працю. Проте, є й певні погрішності в застосування та використання інформаційних технологій, особливо це стосується процесу навчання у ВНЗ зі спеціальними умовами навчання.

Саме різним прийомам та засобам, як основним методологічним засадам буде приділена наша увага. Той методологічний матеріал (засоби, методи, підходи, різні логічні та дидактичні способи, наочні матеріали, практичні приклади, випадки), який використовується під час навчання для навчаючого в сучасних умовах доступу до інформації дає можливість різнобарвно подати навчальний матеріал.

Безперечно, розширені можливості інформаційних технологій дають можливість вільного доступу практично до будь яких відкритих джерел інформації (як вітчизняного так і зарубіжного характеру), що спрощує процес підготовки та опрацювання навчального матеріалу для навчаючого. Проте, тут є один аспект, який полягає у достовірності та правдивості, реальності та дійсності інформації, яка збирається та оприлюднюється. Тому, якісне опрацювання будь-яких відомосте чи інформації лежить в площині відповідальності того, хто їх подає.

Інформаційні технології не можуть обійтися без методологічних основ та засад, які в свою чергу, можуть використовуватися та бути соціально значущою сферою людської діяльності, функцією якої є вироблення й використання теоретично систематизованих об'єктивних знань про дійсність. Саме у цій площині інформаційні технології допомагають усвідомленню більшої кількості інформації, що розширює межі навчання для майбутніх спеціалістів, освіти в цілому та самоосвіти особистості в першу чергу.

Вдалим видається використання інформаційними технологіями під час освоєння та усвідомлення навчального матеріалу таких основних методологічних прийомі, як систематизація, детальний та ґрунтовний пошук відомостей, узагальнення, хронологічність, використання порівняльного методу та методу абстракції тощо.

В умовах світових процесів глобалізації економіки, культури, юриспруденції, стилю та способу буття та життя наукові надбання та наукові дослідження в сфері інформаційних технологій також піддаються процесам глобалізації.

Зокрема, це проявляється в тому, що наука та наукова діяльність дедалі більше стає інтернаціональною. При цьому потрібно

наголошувати на тому, що вказані процеси інтернаціональності чи глобалізації кардинально не повинні впливали на національні елементи нашої держави.

Звичайно, це пов'язано з тим, що сучасні наукові проблеми можуть бути розв'язані переважно колективними зусиллями, на стику фахових досліджень, й тому інформаційні технології мають універсальний характер, який дає можливість використовувати їхні надбання іншими різними навчальними науками та дисциплінами (особливо це актуально для ВНЗ зі специфічними умовами навчання).

Особливої ваги набувають інтеграційні зв'язки між науковцями з різних країн, за яких втрачає сенс національна належність вченого, але не втрачається інтелектуальний обмін думками. Головними стають такі його риси, як науковий та творчий потенціал, комунікабельність і мобільність (за що частково відповідають інформаційні технології).

1. Основи інформаційних технологій і систем : навч. посіб. / В. А. Павлиш, Л. К. Гліненко ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Л. : Вид-во Львів. політехніки, 2013. – 500 с.
2. Основи інформаційних технологій : навч. посіб. [для студентів ВНЗ, які хочуть підвищити свої знання в галузі інформ. технологій згідно із стандартом European Computer Driving Licence] / Т. М. Басюк, Н. О. Думанський, О. В. Пасічник ; за наук. ред. В. В. Пасічника ; М-во освіти і науки України. – [Нове вид.]. – Львів : Новий Світ-2000, 2011. – 390 с.
3. Білуха М.Т. Методологія наукових досліджень: Підручник. – К.: АБУ, 2002. – 480 с.
4. Голоскоков Л.В. Правовые доктрины: от древнего мира до информационной эпохи. М., 2003. – 142с.
5. Дудар С. Методологічні засади системного підходу у сучасній теорії права // Про українське право. Часопис кафедри теорії та історії держави і права. Число IV / За ред. проф. І. Безклубого. – К.: Грамота, 2009. – 384 с.
6. Методологічні проблеми правової науки: Матер. між нар. наук. конф. Харків, 13–14 груд. 2002 р. / Упорядн.: М.І. Панов, Ю.М. Грошевий. – Х.: Право, 2003. – 427 с.

Оцінювання ефективності дистанційного навчання

Сватюк Оксана Робертівна,

доцент кафедри менеджменту факультету № 8 Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

Миронов Юрій Богданович,

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

Миронова Мар'яна Ігорівна,

вчитель економіки Середньої загальноосвітньої школи № 90, м. Львів, Україна, кандидат економічних наук

На сучасному етапі реформування системи вищої освіти в Україні стає все складніше здійснювати пошук ефективних напрямків підготовки висококваліфікованих фахівців за допомогою традиційних засобів навчання, своєчасно і швидко реагувати на виникаючі потреби ринку праці без осмислення великого обсягу актуальної та точної інформації. За умов, коли обсяги інформаційних потоків постійно зростають, зазначені вище проблеми можна вирішити активно використовуючи технології дистанційного навчання. Однак, при цьому постає проблема оцінювання ефективності застосування технологій дистанційного навчання, яка все більше хвилює не тільки фахівців, зайнятих у цій галузі, але й широкі верстви населення.

Дистанційна освіта – це сукупність освітніх послуг, які надаються за допомогою:

- спеціального інформаційно-освітнього середовища на основі специфічної методології навчання;
- інтерактивних та інтенсивних методів навчання, а також сучасних засобів обміну навчальною інформацією на відстані [1].

Роз'єднаність студента та викладача під час навчання вимагає від дистанційних методик не просто забезпечення специфічного

каналу передачі знань, а й зміни освітньої парадигми з педагогічної на андрагогічну, при якій навчання для людини – це діяльність, яку вона сама собі планує та реалізує [4].

За сучасних економічних умов проблема ефективності є вкрай актуальною. Ефективність можна визначити як співвідношення між результатами та витратами. Поняття ефективності навчального процесу, організованого за дистанційною формою, визначається ступенем досягнення освітніх і виховних цілей порівняно з матеріальними, фінансовими, інтелектуальними витратами на їх досягнення. Ефективність в освітньому процесі може бути представлена й у вигляді результативності учня (студента) після завершення навчання.

На нашу думку, ефективність у дистанційному навчанні можна поділити на соціально-педагогічну, організаційну, технологічну й економічну. Охарактеризувати ці види ефективності можна за допомогою рис. 1:

Рис. 1. Ефективність дистанційного навчання

При розгляді напрямків ефективності дистанційного навчання особливу увагу слід приділити саме економічній ефективності.

Економічну ефективність навчання можна розглядати з різних точок зору:

- як зниження витрат на навчання за рахунок впровадження нових науково-технічних розробок;
- як приріст матеріальних благ, який забезпечується завдяки підвищенню професійного та кваліфікаційного рівня спеціаліста;
- як безпосередній внесок працівників освіти в якість освітніх послуг.

Коефіцієнт економічної ефективності дистанційного навчання ($E_{дн}$) ми пропонуємо розраховувати за такою формулою:

$$E_{дн} = \frac{O_{пн} - O_{дн}}{E_{вн}}, \quad (1)$$

де $O_{пн}$ – оцінка знань після навчання (у %); $O_{дн}$ – оцінка знань до навчання (у %); $E_{вн}$ – ефективність витрат на процес навчання.

Оцінка знань слухача дистанційного курсу до та після навчання розраховується як відсоток правильних відповідей за результатами попереднього та підсумкового тестування.

Показник ефективності витрат на навчання ($E_{вн}$) пропонується розраховувати за такою формулою:

$$E_{вн} = \frac{B_1}{B_{заг}} \cdot 100\%, \quad (2)$$

де B_1 – вартість навчання 1 людини; $B_{заг}$ – загальна вартість навчання.

Коефіцієнт економічної ефективності дистанційного навчання близький до нуля свідчить про низьку ефективність системи дистанційного навчання, чим більшим є коефіцієнт – тим ефективнішим можна вважати дистанційне навчання.

Важливо враховувати, що економічна ефективність дистанційного навчання залежить і від:

- вдалого вибору системи дистанційної освіти (СДО) [3];
- якісного управління процесом дистанційного навчання;
- використання сучасних наукових підходів;
- планування та економічного обґрунтування доцільності дистанційного навчання та ін.

Повне виконання перерахованих вище умов підвищення ефективності природно вимагає значних затрат, але є необхідним і в результаті виправданим. Визначення цілей, завдань і дій для їх досягнення – це предмет стратегічного планування. Виявлення технології перетворення ресурсів в задані результати є тактичне завдання. Таким чином, цільову ефективність можна визначити як стратегічну, а витратну – як тактичну.

Управління ефективністю здійснюється на основі кількісних і якісних оцінок (показників) освітньої організації, до яких відносяться:

- діяльність освітнього закладу в цілому;
- ступінь задоволення потреб та інтересів учнів, викладачів та обслуговуючого персоналу освітньої організації;
- якість управлінської, обслуговуючої та освітньої діяльності;
- організація навчання за певними напрямами (спеціальностями);
- використання матеріальних та інтелектуальних ресурсів тощо.

Проаналізувавши стан управління в організації, що працює за системою дистанційного навчання, розробляються заходи щодо його вдосконалення. Для проведення такого аналізу необхідно володіти техніко-економічною інформацією, бухгалтерськими, статистичними даними, які всебічно характеризують діяльність навчальної організації з економічної точки зору [2].

На нашу думку, підвищення ефективності дистанційного навчання можливо досягти за рахунок:

- підвищення кваліфікації, професійного рівня професорсько-викладацького складу, обслуговуючого персоналу;

- підвищення якості навчання за рахунок залучення до підготовки навчально-методичних матеріалів провідних фахівців і викладачів;
- впровадження індивідуально орієнтованих навчальних планів;
- застосування сучасних інформаційних та освітніх технологій;
- підвищення престижу навчального процесу та його соціальної значущості за рахунок привабливості навчання, пов'язаного із застосуванням сучасних технічних засобів.

---

1. Бордияну И. В. Совершенствование организации и управления дистанционным обучением в системе высшего образования Республики Казахстан : диссертация на соискание ученой степени доктора философии (PhD) / И. В. Бордияну. – Алматы, 2011. – 144 с.
2. Романов А. Н. Технология дистанционного обучения в системе заочного экономического образования / А. Н. Романов, В. С. Торопцов, Д. Б. Григорович. – М. : ЮНИТИ-ДАНА, 2000. – 231 с.
3. Сватюк О. Р. Критерії та особливості вибору системи дистанційної освіти / О. Р. Сватюк, Ю. Б. Миронов, М. І. Миронова // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : матеріали Всеукр. наук.-практ. конф. (м. Львів, 23 грудня 2016 р.). – Львів : ЛьвДУВС, 2017. – 313 с. – С. 285-290.
4. Якса Н. В. Андрагогічна модель навчання / Н. В. Якса // Андрагогічний вісник. – 2014. – Випуск 5. – С. 47-52.

Деякі методологістичні аспекти підготовки кадрів для підрозділів кіберполіції в Україні

Світличний Віталій Анатолійович,

доцент кафедри кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук

На теперішній час складно переоцінити актуальність підготовки фахівців кібербезпеки, особливо під час російської агресії, коли гостро відчувається потреба в таких спеціалістах, тому що

кібербезпека – це одне з пріоритетних завдань держави, що визначено в основних нормативно-правових актах України.

Проблематика підготовки національних кадрів у сфері кіберебезпеки, міжнародний досвід організації навчального процесу, досягнення й пропозиції у сфері боротьбі з кіберзлочинністю досить часто обговорюється фахівцями в інформаційній сфері в монографіях, наукових статтях, тезах доповідей на наукових конференціях, семінарах, круглих столах і в засобах масової інформації. Багато аспектів підготовки фахівців кібербезпеки вивчали К. Бєляков, С. Битко, В. Бутузов, А. Волеводз, В. Голубєв, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Е. Рижков, В. Хахановський, Т. Тропіна, О.Орлов, Є. Тітуніна. Але наразі недостатньо ґрунтовних досліджень з проблем підготовки фахівців з протидії злочинам у сфері кібербезпеки.

Головними напрямами практичної діяльності фахівця з кібербезпеки є: протидія правопорушенням, що вчиняються з використанням високих інформаційних технологій; підвищення ефективності правоохоронної діяльності Національної поліції України за допомогою використання сучасних засобів управління; впровадження в діяльність поліції комп'ютерних систем обробки та аналізу інформації, сучасних інформаційних технологій та методик використання технічних засобів.

Міжнародний досвід свідчить, що комп'ютерні злочини мають розслідуватись лише тими підрозділами або співробітниками поліції, які мають спеціальні навички для ведення таких справ та пройшли відповідну підготовку. Тому що, робота з комп'ютерним обладнанням вимагає спеціальних знань і умінь.

Підготовкою фахівців з кібербезпеки займаються багато ВНЗ, в тому числі Харківській національний університет внутрішніх справ (ХНУВС), який здійснює підготовку фахівців з вищою освітою для підрозділів Національної поліції України, що займаються протидією кіберзлочинності, злочинам у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності. Готовність випускників ХНУВС до практичної діяльності на рівні професійної майстерності

визначається низкою кваліфікаційних та професійних вимог. У порівнянні з навичками уміння в напрямку кібербезпеки мають велику змінність, носять усвідомлений характер виконання дій з переходом у наукову творчість. Зміна вимог до характеру умінь є відповіддю на зростання наукової інформації, швидку заміну старих знань новими. У цих умовах особливого значення набуває оволодіння людиною не стільки комп'ютерною технікою з відповіднім програмним забезпеченням, скільки оперативною методикою виконання практичних завдань. Якщо такий підхід важливий у навчанні курсантів інших спеціальностей, то при підготовці фахівців з кібербезпеки він є цілком необхідним. Адже фахівцям з кібербезпеки частіше, ніж іншим поліцейським доводиться оновлювати свої знання, переглядати методи роботи, опановувати нові уміння. Це складний процес, що включає інтелектуальний, емоційний і вольовий прояв особистості.

На нашу думку, з метою більш якісної підготовки фахівців з кібербезпеки у ХНУВС потрібно враховувати академічні та професійні вимоги до спеціалістів в галузі програмування, комп'ютерних наук та інформаційно-комунікаційних технологій, а також у супутніх галузях. Тому курсантів потрібно навчити нестандартно мислити, добре володіти іноземною мовою, щоб спілкуватися зі своїми колегами з інших країн для ознайомлення з зарубіжним досвідом в галузі боротьби з кіберзлочинністю. При цьому значну увагу потрібно надавати вивченню та практичному застосуванню:

- технологій кібербезпеки при користуванні та розробці систем аналітичних досліджень;
- керування базами даних та знань;
- мережевих додатків та Internet-сервісів;
- протоколів передачі та шифрування даних.

Крім того потрібно ознайомлювати курсантів та студентів з методиками сертифікації, експертизи та проведення спеціальних досліджень (в тому числі з використанням паралельних та квантових обчислювальних середовищ) засобів і систем кібернетичного захисту інформаційних ресурсів.

Для вирішення вищевказаних питань на нашу думку потрібно створити у ХНУВС (на базі існуючої кафедри кібербезпеки) кафедру розкриття і розслідування кіберзлочинів. Основними напрямами науково-педагогічної діяльності кафедри буде:

- розробка та застосування методик розслідування кіберзлочинів;
- застосування інформаційно-аналітичної роботи в оперативно-розшуковій діяльності поліції;
- використання методик проведення експертиз під час розслідування кіберзлочинів;
- використання сучасних інформаційних технологій в оперативно-розшуковій, слідчий діяльності при розслідувані злочинів у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності.

Роль викладання комп'ютерного аналізу даних у підвищенні професійної підготовки фахівців для підрозділів Національної поліції України

Сеник Володимир Васильович,

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

Сучасний стан реформування підрозділів МВС України та Національної поліції вимагає перед навчальними закладами із специфічними умовами навчання, до яких входять вищі навчальні заклади МВС України, інноваційних підходів щодо підвищення якості підготовки фахівців. Адже фахівець – це особа, яка не лише володіє певним багажем теоретичних знань, а й уміє застосовувати їх в умовах практичної діяльності, мислити та приймати рішення. На формування такого фахівця спрямовані без винятку усі навчальні дисципліни. Однак, хотілося б виділити ті навчальні дисципліни, які відповідно до своєї специфіки мають найбільше значення для вирішення цього

завдання. Це, насамперед, дисципліни, у яких вивчаються різні способи аналізу інформації. У таблиці приведено ряд дисциплін, які, включають до своєї структури питання аналізу даних під час підготовки фахівців для підрозділів Національної поліції України у Львівському державному університеті внутрішніх справ.

Табл. Деякі дисципліни, під час вивчення яких здобувачами вищої освіти у Львівському державному університеті внутрішніх справ використовується аналіз даних

Спеціальність	Освітній ступінь	Дисципліна
081 Право	бакалавр	Інформаційне забезпечення професійної діяльності
		Інформаційно-пошукові системи
	магістр	Інформаційні технології в правозастосовній діяльності
	бакалавр	Застосування інноваційні технології в психології
262 Правоохоронна діяльність	бакалавр	Інформаційне забезпечення професійної діяльності

Потенціал цих дисциплін щодо вирішення питання професійної підготовки поліцейських визначається сукупністю в них аналітичного змісту з необхідністю використання засобів обчислювальної техніки, оскільки розмовляти в умовах сучасності про аналіз даних без використання комп'ютерної техніки, щонайменше, некоректно.

У зв'язку із викладеним, постає питання про узгодження методики викладання аналізу даних під час навчання. Через те, виникає необхідність для початку розглянути поняття аналізу даних. Під *аналізом даних* ми будемо розуміти напрямок діяльності, що визначає розробку методів обробки даних незалежно від їх природи і який включає в себе виконання послідовних логічних дій з інтерпретації зібраних даних, їх перетворення у статистичні форми, що необхідні для прийняття рішень. Виділяють наступні етапи аналізу даних: отримання даних; обробка даних; проведення аналізу; інтерпретація [1].

Під час проведення підготовки фахівців у різних дисциплінах, на наш погляд доцільно використовувати як математичні (статистичні), так і інтелектуальні [2] методи аналізу даних, з метою формування відповідних уявлень про характер об'єкта чи явища, які ці дані описують.

Однак, не залежно від обраного методу аналізу даних з використанням обчислювальної техніки сутність підходу до навчання фахівців різних напрямків діяльності повинні відповідати таким основним положенням:

- перед навчанням аналізу даних важливо пояснити здобувачам вищої освіти про те, яким чином дані добувають, ознайомити їх з класифікацією інформації, навчити виділяти основні дані. Здобувачі вищої освіти повинні усвідомлювати, що некоректна обробка масивів неопрацьованих даних створює нікому не потрібний смітник даних;
- наявність обчислювальної техніки, новітнього програмного забезпечення, зростання комп'ютерної грамотності сучасного населення призвели до того, що засоби аналізу стали доступнішими. Фактично кожен може скористатися засобами аналізу даних. Проте здобувачі вищої освіти повинні усвідомлювати, що не розуміючи сутність того чи іншого методу аналізу даних неможливо й зрозуміти, який результат буде отриманий під час його застосування, а значить і неможливою стане інтерпретація результатів. Це у подальшому призводить до відсутності правильних висновків та відповідно прийняття правильних управлінських рішень;
- здобувачам вищої освіти слід довести, що математичні (статистичні) методи аналізу даних можуть бути використані як інструмент розв'язку змістовних задач. Використання ж інтелектуальних методів аналізу доцільно застосовувати під час пошуку у великих обсягах даних неочевидних, об'єктивних і корисних на практиці закономірностей. Перед використанням даних методів необхідно роз'яснити, на яких підставах їх обирають та для

якого типу задач доцільно їх застосовувати. Найпоширеніші задачі, які можливо вирішити застосовуючи математичні (статистичні) методи аналізу даних – це аналіз зв'язку емпіричних даних з метою розуміння та прогнозування певного явища. Визначення типу задач дає можливість вибрати стратегію аналізу даних, а також визначити можливості застосування математичних (статистичних) методів;

- на основі двох–трьох пакетів програм дати здобувачам вищої освіти практичні навички з використання різного програмного забезпечення для проведення аналізу даних, застосувати методи візуалізації для наочного представлення результатів;
- під час розв'язання задач різного типу виникає необхідність залучити здобувачів вищої освіти до комплексного використання математичних та інтелектуальних методів аналізу різного типу, тобто вирішення завдань різними методиками. Це дає можливість формувати у здобувачів вищої освіти системне мислення;
- під час навчання здобувачів вищої освіти аналізу даних з використанням обчислювальної техніки потрібно використовувати системний підхід, тобто враховувати систему навчання, систему методичних та дидактичних засобів, міжпредметні зв'язки тощо;
- дидактичні матеріали слід підбирати з урахуванням як рівня попередньої підготовки здобувачів вищої освіти, місця дисципліни у плані підготовки, кількості занять, так і з рівнем освіти яку вони здобувають (бакалавра чи магістра);
- для проведення ефективного навчання необхідно довести до здобувачів вищої освіти чіткі вимоги до знань і вмінь, якими вони повинні оволодіти.

Таким чином, використання вказаних шляхів та удосконалення методики навчання здобувачів вищої освіти методам аналізу даних призведе до формування у майбутніх фахівців-поліцейських системного мислення, надасть практичних навичок у використанні інформаційних технологій у професійній діяльності.

1. Аналіз даних [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Аналіз_даних
2. Поняття про інтелектуальний аналіз даних [Електронний ресурс]. – Режим доступу: http://stud.com.ua/25070/menedzhment/ponyattya_intelektualniy_analizi_danih

Інформаційні системи у наукових розробках працівників ОВС

Сибірна Рома Іллінічна,

професор кафедри психології діяльності в особливих умовах факультету № 7 Львівського державного університету внутрішніх справ, доктор біологічних наук, професор

Хомів Олена Володимирівна,

доцент кафедри економіки та економічної безпеки факультету № 8 Львівського державного університету внутрішніх справ кандидат економічних наук, доцент

Стрімкий та динамічний розвиток інформаційних відносин у теперішній час щораз більше впливає на трансформацію різних сфер життя людини у всіх країнах світу. Широке впровадження інформаційно-комп'ютерних технологій та систем, удосконалення технологічних засобів збирання, зберігання, використання та поширення інформації призвели до стрімкого розвитку інформаційних відносин, розбудови інформаційного суспільства та формування світового інформаційного простору. В усіх сферах життєдіяльності все частіше використовуються категорії, пов'язані з поняттям «інформація», як-от: «інформаційні технології», «інформаційні системи», «інформаційна війна», «кіберпростір», «кіберзлочинність», «електронне урядування» тощо [2, с. 37].

Сьогодні інформаційні системи посіли чільне місце в усіх сферах життєдіяльності людини. З огляду на посилені тенденції реформування української поліції, не обійтися і без активного застосування інформаційних систем в оптимізації діяльності правоохоронних органів.

Досліджуючи сутність поняття «інформація» в соціальній сфері, можемо стверджувати, що за своїм значенням воно найбільш співзвучне з поняттями «дані», «відомості». Спільними для них є такі характеристики, як вірогідність, точність, повнота, первинність, вторинність, корисність, старіння тощо. З впровадженням інформаційних систем та комп'ютеризацією діловодства в ОВС, поруч з поняттям «інформація» вживається поняття «комп'ютерна інформація». Комп'ютерна інформація – це не самі дані, а форма їх представлення у машинному вигляді, сукупність символів, яка зафіксована у пам'яті комп'ютера, або на машинному носії. Враховуючи специфіку діяльності ОВС, слід пам'ятати, що за певних обставин й фізичні поля можуть виступати носіями інформації, зокрема при розгляді справ. Для систематизації та обробки інформації використовують класифікацію інформації за різними ознаками. За джерелами отримання інформації її поділяють на первинну і вторинну, за формою фіксації – на документальну і не документальну; за способом передачі – на ручну та механізовану; за способом обробки – на вихідну та оброблену, за повнотою – на повну та часткову; за ступенем доступу – загальну, службову (ДСК), таємну та цілком таємну тощо.

Інформаційне забезпечення у наукових розробках працівників ОВС України слугує всебічній інформаційній підтримці основних напрямів діяльності органів внутрішніх справ, зокрема у боротьбі зі злочинністю, в тому числі й економічною. Основою діяльності підрозділів ОВС є комплекс організаційних, нормативно-правових, фінансових, технічних, програмних та інших заходів, які залежать від повноти та достовірності інформації. Розрізняють загальновідомчі та галузеві інформаційні підсистеми, які складають основу системи інформаційного забезпечення органів внутрішніх справ. Система інформаційного забезпечення ОВС сформована за такими принципами: функціонального призначення; нормативно-правової забезпеченості; фактичності даних; доцільності впровадження та експлуатації; нарощення та розвитку.

Інформаційні підсистеми як складові частини системи інформаційного забезпечення, призначені для збирання,

накопичення, зберігання та обробки інформації певних напрямків обліків й орієнтовані на використання в діяльності багатьох служб, мають загальновідомчий характер і відносяться до загальновідомчих інформаційних підсистем.

Інформаційні підсистеми можуть належати до певного рівня та визначатися принципами територіальності, специфіки використання та обсягом інформації, яка обробляється. Кожен з рівнів має свої особливості, зокрема: перший рівень – центральний, інтегрує інформаційні підсистеми ОВС загальновідомчого значення та галузевих служб МВС України; другий рівень – регіональний, охоплює інформаційні обліки, які є складовими загальновідомчих інформаційних підсистем, і використовуються службами ГУМВС, УМВС, УМВСТ; третій рівень – територіальний, охоплює інформаційні обліки, що є складовими загальновідомчих інформаційних підсистем і які використовуються в міських, районних та лінійних ОВС, спеціалізованих підрозділах поліції [1, с. 84].

Завдання системного реформування органів внутрішніх справ (ОВС), що має на меті якісне підвищення ефективності їх роботи по боротьбі зі злочинністю, охороні громадського порядку і захисту прав громадян, передбачає якісне реформування існуючого інформаційного забезпечення, яке має відповідати змінам структури ОВС і відповідати вирішуваним ними завданням.

На сьогоднішній день в ОВС розроблені і активно використовуються цілий ряд інформаційних систем («ІБД», «Розшук», «Арсенал» та ін.), що складають загальну систему інформаційного забезпечення ОВС. В існуючому вигляді вона забезпечує вирішення наступних завдань:

- надання можливості оперативного отримання співробітникам або підрозділам ОВС інформації в повному, систематизованому і зручному для використання вигляді для розкриття, розслідування та попередження злочинів і пошуку злочинців;
- збір, обробка та узагальнення оперативно-довідкової, аналітичної, статистичної та контрольної інформації для

оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління ОВС;
- вдосконалення організаційно-кадрового та інформаційного забезпечення підрозділів;
- інтеграція та систематизація інформаційних обліків ОВС на всіх рівнях, а також створення умов для їх ефективного використання.

У рамках здійснюваної в даний час в Україні реформи МВС змінюється парадигма правоохоронної системи. Ліквідується цілий ряд існуючих підрозділів і створюються нові з іншими завданнями і функціями.

У цих умовах система інформаційного забезпечення ОВС також повинна бути адекватно перебудована з тим, щоб відповідати зміненим завданням і умовам.

Реформа інформаційної системи ОВС повинна розвиватися за наступними напрямками:

- визначення цілей і завдань модернізації системи інформаційного забезпечення ОВС;
- розробка нормативно-правових актів, що визначають порядок і механізм модернізації;
- розробка та впровадження системи стратегічного планування і управління процесами інформатизації ОВС України;
- розробка інформаційних підсистем (підзадач) для нових підрозділів ОВС та їх інтеграція в існуючу систему; вдосконалення телекомунікаційної складової з метою забезпечення виконання нових завдань реформованої системи ОВС;
- модернізація існуючої системи захисту інформації;
- підготовка особового складу до змін у загальній системі інформаційного забезпечення, а також навчання співробітників нових підрозділів грамотному використанню інформаційних систем для вирішення оперативно-службових завдань;
- підготовка персоналу для супроводу, адміністрування та технічного обслуговування інформаційних підсистем;

- модернізація існуючої технічної бази відповідно до змінених вимог [3].

Найбільш продуктивними на сьогоднішній день є інформаційно-довідкова, інформаційно-пошукова, інформаційно-модельована та інформаційно-консультаційна системи [4, с. 175].

Найпоширенішими із них у правоохоронних органах є інформаційно-довідкова та інформаційно-пошукова. За принципами роботи з інформацією вони подібні та забезпечують надання інформації про об'єкт у такому вигляді, в якому вона була внесена. Більш складною є інформаційно-модельна система, призначена для пошуку й обробки даних, але, на відміну від наведених, результатом її застосування виступають певні інформаційні моделі. Можна зазначити про об'єкти інформаційно-довідкових обліків, які є моделями об'єктів, що мають доказове значення. Надання працівникам слідчих підрозділів такої криміналістичної інформації дозволяє приймати правильні тактичні рішення в різних складних слідчих ситуаціях. Значні перспективи мають інформаційно-консультаційні системи. Саме вони на підставі аналізу вихідної інформації допомагають правильно сформувати слідчі версії та сприяти в обранні тактики проведення окремих слідчих (розшукових) дій. Так, слідчий може одержати дані про всі можливості інформаційно-довідкових картотек і колекцій про об'єкти, які в них вміщені, про шляхи отримання цієї інформації за проведення слідчих (розшукових) дій, але ця форма застосування спеціальних знань і криміналістичних обліків на практиці використовується нечасто. У розслідуванні кримінальних правопорушень здебільшого використовуються інформаційно-пошукові системи, які забезпечують збирання, збереження та видачу інформації за запитом користувача. Своєю чергою, автоматизована інформаційно-пошукова система створена та впроваджена з метою подальшого вдосконалення централізованого накопичення, обробки та пошуку довідкової, орієнтувальної та іншої інформації [5].

Загострення оперативного стану в Україні, збільшення обсягів інформації, що надходить і переробляється, зумовило гостру

потребу в підвищенні ефективності всіх служб МВС на основі новітніх інформаційних технологій. Уже сьогодні в цьому напрямку спостерігаються певні позитивні тенденції, серед яких загальне підвищення комп'ютерної грамотності працівників ОВС; збільшення переліку комп'ютерних інформаційних обліків; поширення використання сучасних засобів комп'ютерної техніки в діяльності всіх ланок ОВС; впровадження безпаперових технологій оброблення інформації; створення комп'ютерної мережі обміну інформацією.

Головною метою робіт, що проводяться, є забезпечення інформаційної підтримки діяльності ОВС:

- оперативне отримання працівниками та підрозділами ОВС повної інформації, необхідної для розкриття, розслідування, попередження злочинів і розшуку злочинців у систематизованому та зручному для користування вигляді;
- збирання та оброблення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінювання ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності ОВС;
- ефективна інформаційна взаємодія з іншими правоохоронними органами і державними установами.

У сфері управлінської та контрольно-методичної роботи виконуються такі завдання комп'ютеризації:

- збирання і нагромадження даних про скоєні злочини;
- аналіз статистичної звітності за встановленими формами;
- контроль за дотриманням процесуальних строків, розглядом заяв громадян, виконанням планових заходів;
- складання управлінських документів;
- створення і використання баз даних (знань) та автоматизованих інформаційно-пошукових систем для одержання інформації про нормативні акти, наукову літературу, методичні розробки, матеріали передового досвіду слідчої та судової практики;
- аналіз робіт з профілактики злочинів та оцінювання їх ефективності;

- нагромадження інформації про експертні установи, їх можливості, види експертиз, приблизні питання експертам тощо;
- аналіз інформації щодо нерозкритих злочинів минулих років, розробка рекомендацій щодо їх розкриття та використання типових ознак і ситуацій;
- формування моделей процесуальних дій зі збільшенням обсягу стандартної інформації стосовно - розслідування різних видів злочинів;
- розробка методик розслідування кримінальних справ з комп'ютерних та інших видів злочинів.

У сфері розслідування злочинів автоматизації підлягають:

- процес слідчого виробництва з використанням баз процесуальних та інших документів, що оформляються на стадії попереднього розслідування;
- планування заходів по конкретних кримінальних злочинах;
- створення календарних планів і мережних графів розслідування;
- складання слідчих та інших документів (у першу чергу, постанов щодо притягнення як обвинуваченого та висновків з обвинувачення) на основі даних, занесених у базу;
- передача до суду протоколів допитів, постанов та інших процесуальних документів на магнітних носіях та по каналах зв'язку;
- вибір та передача необхідної інформації для проведення відповідних заходів у ході оперативно-розшукової діяльності, її оформлення згідно з кримінально-процесуальним кодексом;
- організація та проведення бухгалтерських ревізій та експертиз, різноманітні розрахунки з кримінальних проваджень по економічних злочинах;
- контроль з боку керівників підрозділів за розслідуванням кримінальних проваджень на всіх етапах;
- використання у ході розслідування програм з методиками розслідування злочинів різних видів [6, с. 41].

Таким чином, інформаційне забезпечення наукових розробок працівників ОВС України слугує всебічній інформаційній підтримці основних напрямів діяльності, зокрема у боротьбі зі злочинністю. Основою цієї діяльності є комплекс організаційних, нормативно-правових, фінансових, технічних, програмних та інших заходів, які залежать від повноти та достовірності інформації. З огляду на вказане, інформаційні системи у наукових розробках працівників ОВС відіграють вагоме значення.

1. Бездух І.Я. Інформаційні системи в ОВС та захист інформації / І.Я.Бездух, Х.В Бовшик, П.Б Живко // Збірник наукових статей за матеріалами доповідей науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі» (26 грудня 2014 р.). – Львів: ЛьвДУВС, 2014. – 249 с.
2. Гаврильців М.Т. Застосування інформаційних технологій у сфері підготовки працівників правоохоронних органів в україні / М.Т. Гаврильців // Збірник наукових статей за матеріалами доповідей науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі» (26 грудня 2014 р.). – Львів: ЛьвДУВС, 2014. – 249 с.
3. Головко О.М. Застосування інформаційних технологій у правоохоронній діяльності [Електронний ресурс]. – Режим доступу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/420/Zastos_inf_tehn_u_pravooh_diyl_2015.pdf?sequence=1&isAllowed=y
4. Журавель В. А. Информационное обеспечение процесса расследования: пути и средства / В. А. Журавель // Вісник Академії правових наук. – 2004. – № 2. – С. 175–179.
5. Дабіжа Д.В. Використання інформаційних систем під час розслідування кримінальних правопорушень. [Електронний ресурс]. – Режим доступу: http://journal.lvduvs.edu.ua/visnyky/nvsy/04_2015/15ddvrkp.pdf
6. Нагачевський С.В. Проблеми і концепція розвитку інформаційних систем ОВС України / С.В. Нагачевський // Збірник наукових статей за матеріалами доповідей науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних

технічних засобів у діяльності ОВС та навчальному процесі» (26 грудня 2014 р.). – Львів: ЛьвДУВС, 2014. – 249 с.

Проблемні питання розробки та впровадження компонентів інформаційних технологій у освітньому процесі

Тулупов Володимир Володимирович,

доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

Пересічанський Валерій Миколайович,

старший викладач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Постановка проблеми. На теперішній час розробка та впровадження компонентів інформаційних технологій для підготовки фахівців з організації захисту інформації має суттєву прикладну компоненту наближення до проблематики діяльності підрозділів технічного захисту інформації правоохоронних органів. Комп'ютеризація та тренажерізація відносяться до числа найбільш наукомістких областей, що вимагають величезних витрат інтелектуальної праці, у тому числі праці методистів вищої кваліфікації.

Щоб представити масштаб проблем, досить звернути увагу на такі фактори.

По-перше, найбільш ефективна комплексна комп'ютеризація та тренажерізація професійної підготовки фахівців, що забезпечують усі стадії життєвого циклу виробу: проектування, розробку, випробування, виробництво, експлуатацію, технічне обслуговування, ремонт та успішного виконання учбового завдання [1, с. 237].

По-друге, розробка однієї години високоефективної навчальної комп'ютерної програми, як показує вже наявний досвід, вимагає

витрат багатьох людино-годин праці кваліфікованих програмістів і методистів. При цьому контроль якості навчаючих програм та ефективності тренажерної підготовки є справою складною, що потребує спеціальних знань, тестів, участі експертів тощо. Без такого контролю та сертифікації можливі негативні результати навчання, виникнення помилкових навичок, втрати природного інтелекту у особи, що навчається та ін. Також до цього варто додати констатацію неухильного зросту вартості апаратних і програмних засобів як існуючих тренажерів так і інших навчаючих інтерактивних систем.

По-третє, високий темп розвитку інформаційних технологій зумовлює:

- оновлення засобів матеріально-технічного забезпечення навчального процесу новими зразками техніки та інформаційними технологіями;
- оновлення кадрового потенціалу кафедр зі специфічними умовами навчання та взаємопроникнення інформаційних технологій та спеціальних знань в суміжні дисципліни, що викладаються;
- впровадження нових методик і прийомів навчання, комп'ютеризація та інформатизація навчального процесу;
- тісний зв'язок з передовими науково-технічними розробками в сфері інформаційних технологій та спеціальної техніки [1, с. 238].

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

На теперішній час пропонуються різні тренажерні комплекси (комп'ютерні тренажери) технічного захисту інформації (ТЗІ) для практичного навчання фахівців, професійна діяльність яких пов'язана не тільки з технічним захистом інформації наприклад:

- програмно-апаратний комплекс «Салют», що призначений для пошуку та локалізації відеокамер та акустичних розвідувальних засобів, включаючи тренажер для підготовки операторів;
- навчаючий тренажерний комплекс «Зоря», що призначений для підготовки фахівців в галузі атестації об'єктів;
- навчаючий тренажерний комплекс «Спектр», що призначений для підготовки фахівців в галузі пошуку та виявлення радіозакладних пристроїв);
- автономний імітатор радіозавад «Кобра», що призначений для імітації постановки завад радіоелектронним засобам різного призначення та типу з метою навчання операторів розв'язанню задач в умовах дії навмисних завад, а також відпрацювання дій груп пошуку та знищення передавачів завад, що були занесені та/або встановлені [2].

Наприклад, вищезазначені тренажерні комплекси, а також існуючи розробки кафедр зі специфічними умовами навчання, дозволять у деякій мірі замінити тренування на штатних існуючих або відсутніх на таких кафедрах або в практичних підрозділах приладів – засобами сучасних інформаційних технологій, шляхом виконання учбово-тренувальних задач за допомогою інтер-активного середовища на персональному комп'ютері.

Можливі підходи до розв'язання проблем. Впровадження нових методик навчання здійснюється також в системі відомчої освіти, зокрема в Харківському національному університеті внутрішніх справ, де здійснюється підготовка фахівців за напрямом 6.170102 – «Системи технічного захисту інформації» та спеціальністю 125 – «Кібербезпека».

Розв'язання деяких вищезазначених проблем знайшли своє відображення в розробках кафедр «Інформаційних технологій» та «Кібербезпеки» факультету № 4, наприклад: комп'ютерний тренажер «Селективний мікровольтметр та вимірювач напруги завад SMV 8.5» призначений для отримання курсантами та студентами первинних практичних навичок роботи з селективним мікровольтметром та вимірювачем напруги завад SMV 8.5.

Тренажер являє собою спрощений інтерактивний аналог (симулятор) пристрою SMV 8.5 та має наступні можливості:

- ознайомлення користувача з призначенням пристрою;
- ознайомлення з технічними характеристиками SMV 8.5;
- ознайомлення з комплектацією пристрою;
- ознайомлення з органами управління пристроєм;
- демонстрація використання пристрою при виконанні учбово-тренувальних задач;
- безпосереднє виконання учбово-тренувальних задач для оволодіння навичками роботи з пристроєм;
- тестування користувача.

Також для забезпечення проведення лабораторних робіт з дисциплін: «Методи та засоби захисту інформації», «Метрологія та вимірювання», «Системи та засоби зв'язку», «Електроніка та схемотехніка» також було розроблено комп'ютерні тренажери а саме: «Виміри за допомогою селективного мікровольтметру SMV 11», «Виміри за допомогою селективного нановольтметру Unipan-233» та «Вимірювач шуму та вібрацій ВШВ-003-М2» з використанням мультимедійної платформи Adobe Flash та інших технологій. У рамках дипломного проектування розробляються комп'ютерні тренажери для інших пристроїв з подальшим впровадженням їх у навчальний процес.

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

1. Тулупов, В.В. Актуальні аспекти побудови комп'ютерних тренажерів для професійної підготовки кадрів органів внутрішніх справ [Текст] / В.В. Тулупов, О.М. Рвачов // Матеріали науково-практичної конференції (Київ, 25 листоп. 2011 р.) «Спеціальна техніка у правоохоронній діяльності». – К.: НАВС, 2012. – С. 236-239.
2. «НЕЛК» Научно-производственный центр [Електронний ресурс]. – Режим доступу: http://www.pemi.ru

РОЗДІЛ 3
СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ ІТ-ТЕХНОЛОГІЙ В АКТУАЛЬНІ СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ ДІЯЛЬНОСТІ

Використання інформаційних технологій під час досудового розслідування

Ангеленюк Анна-Марія Юріївна,

старший викладач кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук

Проблеми та питання використання інформаційних технологій під час досудового розслідування у сучасному світі є вкрай важливими, оскільки ефективність взаємодії між суб'єктами у досудовому розслідуванні залежить від використання у цьому процесі можливостей сучасної техніки.

Автоматизація процесу розслідування розглядалась у роботах Г.К. Авдєєвої, А.І. Анапольської, В.О. Коновалової, В.В. Крилова, В.Є. Корноухова, В.Ю. Шепітька та інших учених. Однак автоматизація розглядалась здебільшого з точки зору полегшення роботи з окремими документами конкретними суб'єктами процесу (слідчим, прокурором та ін.), але не достатньо звернено увагу на питання щодо автоматизації процесу документообігу між вказаними суб'єктами.

Слід зауважити, що актуальним питанням сьогодення є дослідження проблем спільної діяльності на досудовому розслідуванні саме між слідчим та прокурором, а також вдосконалення цієї діяльності за допомогою сучасних технологій.

З прийняттям нового КПК у 2012 р. такі процесуальні дії як повідомлення про підозру особі чи обрання запобіжного заходу підозрюваному потребують злагодженої взаємодії не тільки

слідчого та оперативного підрозділу, а й слідчого та прокурора, як процесуального керівника. Досліджуючи питання спільної діяльності слідчого та прокурора під час досудового розслідування слід зазначити, що найбільш проблемним є прийняття процесуальних рішень, що складені слідчим та потребують погодження прокурора, як процесуального керівника у кримінальному провадженні, в тому числі рішення щодо повідомлення особі про підозру та обрання запобіжного заходу підозрюваному, саме як такі, що потребують максимальної оперативності під час їх організації та виконання. Щодо взаємодії між прокурором та слідчим на етапах початку та закінчення досудового розслідування зауважимо, що ці питання достатньо вирішує система єдиного реєстру досудових розслідувань (далі ЄРДР). Враховуючи наведене розглянемо проблеми, що виникають між слідчим підрозділом та прокуратурою на прикладі повідомлення особі про підозру та обрання їй запобіжного заходу.

Згідно статті 277 КПК України письмове повідомлення про підозру складається прокурором або слідчим за погодженням з прокурором.

Згідно зі статтею 276 КПК України, слідчий, прокурор зобов'язані невідкладно повідомити підозрюваному про його права після чого слідчий, прокурор на прохання підозрюваного зобов'язані детально роз'яснити кожне із зазначених прав [1].

Письмове повідомлення про підозру, згідно статті 278 КПК України, вручається в день його складення слідчим або прокурором, а у випадку неможливості такого вручення - у спосіб, передбачений цим Кодексом для вручення повідомлень. Слід звернути увагу, що письмове повідомлення про підозру затриманій особі вручається не пізніше двадцяти чотирьох годин з моменту її затримання. У разі якщо особі не вручено повідомлення про підозру після двадцяти чотирьох годин з моменту затримання, така особа підлягає негайному звільненню [1].

Отже з введенням в дію положень процесуального керівництва збільшилось коло питань які слідчий та прокурор повинні

вирішувати разом, а отже процесуально взаємодіяти між собою. Процесуальною взаємодією слід вважати відносини, які виникають у процесі застосування кримінальних процесуальних норм, що визначають засади і порядок співробітництва [2, с. 25].

Щодо повідомлення особі про підозру та обрання їй запобіжного заходу зауважимо, що діяльність слідчого пов'язана з діяльністю прокурора не тільки у процесуальному плані, а й у технічному: оскільки внесення відомостей у систему Єдиного реєстру досудових розслідувань (далі ЄРДР) вимагає як від слідчого так від прокурора, як процесуального керівника спільних дій. Так, наприклад під час повідомлення особі про підозру слідчий зобов'язаний внести ці дані у ЄРДР після чого ця інформація обов'язково підтверджується прокурором як керівником у кримінальному провадженні і тільки після цього можуть бути подані вказані дані у інформаційний центр обліку даних. Враховуючи наведене та необхідність вчинення таких дій у максимально стислі часові рамки вважаю, що взаємодія слідчого та прокурора, як процесуального керівника повинна бути високоефективною, що може бути досягнуто завдяки використанню інформаційних технологій.

З метою подальшого аналізу можливостей автоматизованого документообігу між слідчим та прокурором, як процесуальним керівником у кримінальному провадженні, розглянемо детальніше питання внесення даних у ЄРДР щодо повідомлення особі про підозру.

Дата та час повідомлення про підозру, правова кваліфікація кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність невідкладно вносяться слідчим, прокурором до ЄРДР [3].

Єдиний реєстр досудових розслідувань - створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюються збирання, зберігання, захист, облік, пошук, узагальнення даних, 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.

Реєстраторами Реєстру є: прокурори, у тому числі керівники прокуратур; керівники органів досудового розслідування; слідчі органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, та органів Державного бюро розслідувань; детективи підрозділів детективів та внутрішнього контролю Національного антикорупційного бюро України, що уповноважені здійснювати досудове розслідування кримінальних правопорушень.

Користувачами Реєстру є: керівники прокуратур та органів досудового розслідування; прокурори; слідчі органів поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, та Державного бюро розслідувань, детективи Національного бюро; інші уповноважені особи органів прокуратури та досудового розслідування, які виконують функції з інформаційно-аналітичного забезпечення правоохоронних органів та ведення спеціальних обліків (оперативних, оперативно-облікових, дактилоскопічних тощо) відповідно до чинного законодавства. Користувачі і реєстратори отримують носії з електронним ключем доступу у регіональних прокуратурах за місцем розташування цих прокуратур [3].

Таким чином ЄРДР є достатньо захищена електронна система даних, яка може містити у своїх базах інформацію, що стосується матеріалів досудового розслідування. Однак ЄРДР не вирішує питань документообігу між органами досудового розслідування та прокуратури.

Приділення уваги питанням автоматизованому документообігу зумовлено необхідністю економії часу як слідчого, так і прокурора-процесуального керівника, що при сучасних умовах праці є особливо актуальним. Слід зазначити, що інститут процесуального керівництва, що є відносно новим у практиці, вимагає узгодження дій між учасниками, що також включає

взаємодію у процесі документообігу між ними та внесенні відомостей у систему ЄРДР. Відповідно до сучасного законодавства слідчий зобов'язаний погодити у процесуального прокурора підозру та клопотання про обрання запобіжного заходу, а саме після складення тексту вказаних документів слідчий зобов'язаний подати їх процесуальному керівнику провадження після чого, узгодивши зауваження щодо тексту, виправити їх. Відповідно оперативність зазначених вище дій залежить безпосередньо від рівня та якості взаємодії між слідчим та прокурором, що в основному базується на їх особистих відношеннях. Зауважимо, що саме слідчий є відповідальним за вчасне повідомлення підозри особі, вчасно подане клопотання про обрання міри запобіжного заходу у суд, так як він згідно закону є самостійним у своїй процесуальній діяльності, а також відповідає за організацію вказаних вище дій. Однак оперативність та організація дій, пов'язаних з оголошенням підозри та поданням клопотання про обрання запобіжного заходу не залежить тільки від слідчого, так як потребує погодження. Створивши офіційну автоматизовану систему документообігу між слідчим відділом та прокуратурою можна суттєво скоротити час на організаційні моменти та максимально скоротити час потрібний на погодження вказаних вище спільних документів. Звичайно при наданні слідчим документів на погодження прокурору можна користуватись звичайною електронною поштою, однак, на мою думку, не слід використовувати такий варіант передачі даних під час ведення досудового розслідування, оскільки звичайна електронна пошта не має відповідного рівня захисту, а інформація, що пов'язана з повідомленням про підозру та обранням запобіжного заходу у кримінальному провадженні вимагає дотримання таємниці досудового розслідування. В іншому випадку слідчому фактично слід пройти у прокуратуру і тільки після узгодження всіх дій продовжувати їх організацію та виконання, що відповідно збільшує затрачений час.

У сучасних умовах слідчий має у своєму провадженні достатню велику кількість кримінальних проваджень, тому слід за допомогою технічних засобів максимально оптимізувати роботу

слідчого. Цим питанням приділено увагу у науковій літературі, так з метою покращення ефективності роботи слідчого запропоновано використовувати спеціальні програмні пакети автоматизованих робочих місць слідчого «Робоче місце слідчого» (Україна), інформаційно-аналітична система «АРМЕКС» (Україна) у яких реалізується автоматизація складання процесуальних документів у вигляді баз даних із бланками цих документів, або у вигляді еталонних їх зразків та переліків питань (обставин), що повинні бути в них відображені [4, с. 3]. Однак такі програмні пакети не вирішують питання взаємодії та документообігу між слідчим та прокурором-керівником у кримінальному провадженні.

На мою думку, з метою покращення ефективності взаємодії слідчого з процесуальним прокурором слід створити окрему електронну систему документообігу, або забезпечити функціонування такої у межах ЄРДР, що повинно бути закріплено у нормах кримінального процесуального кодексу.

Введення в повсякденне користування слідчих, прокурорів та працівників оперативного підрозділу України подібної автоматизованої інформаційної системи документообігу та регламентування її у правовому полі забезпечить якісну взаємодію між ними, а зокрема у питаннях пов’язаних з повідомленням особі підозри та обранні їй запобіжного заходу.

---

1. Кримінальний процесуальний кодекс України від 13.04.2012 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/4651-17
2. Взаємодія слідчих та оперативних підрозділів під час досудового розслідування: навч. посібник / Р.І. Благута, М.П. Климчук, В.М. Сакал, М.С. Цуцкіридзе. – К.: ТОВ «НВП»Інтерсервіс», 2014.
3. Положення про порядок ведення Єдиного реєстру досудових розслідувань, затверджені Наказом Генеральної прокуратури України від 06.04.2016 № 139 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/z0680-16
4. Автоматизоване робоче місце як один із напрямів удосконалення роботи слідчого / А.І. Анапольська [Електронний ресурс]. – Режим доступу: aspirantura.16mb.com/doc/conf2015/s2

Адміністративно-правове регулювання інформаційного забезпечення діяльності МВС України в сфері міграції

Бортник Надія Петрівна,

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

Єсімов Сергій Сергійович,

доцент кафедри адміністративно-правових дисциплін факультету № 6, Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

В умовах асоціації України і ЄС і прискореного технологічного розвитку проблема вдосконалення адміністративно-правового регулювання інформаційного забезпечення діяльності в сфері міграції досить складна та багатопланова, вимагає серйозного теоретичного осмислення, аналізу відповідних нормативно-правових актів, вивчення практики державно-управлінської діяльності МВС України в досліджуваній сфері. Підкреслює значимість досліджуваної проблематики Конституція України, декларуючи, що збір, зберігання, використання та поширення інформації про приватне життя особи без її згоди не допускаються. Про актуальність наведеного свідчать положення Доктрини інформаційної безпеки України, констатуючи, що інформаційні технології набули транскордонний характер і стали невід'ємною частиною всіх сфер діяльності особи, суспільства та держави.

Стратегія державної міграційної політики України на період до 2025 року, передбачає вдосконалення механізмів збору, зберігання, обробки та поширення інформації в сфері міграції, удосконалення надання державних послуг і виконання державних функцій із застосуванням інформаційних технологій у контексті інформаційно-аналітичного забезпечення постійно зростаючих міграційних показників. Прогноз міграційної ситуації демонструє тенденцію до збільшення числа мігрантів, які прибувають на територію країни.

Наукові дослідження в сфері інформаційного забезпечення є дуже важливий напрям діяльності. Не випадково одним з повноважень МВС України, згідно з Положенням про Міністерство внутрішніх справ України, затвердженого постановою Кабінету Міністрів України від 28.10.2015 № 878, є здійснення інформаційно-правового забезпечення діяльності органів підпорядкованих МВС.

МВС України відповідно до покладених на нього завдань, згідно п. 17 ст. 4 зазначеного Положення, забезпечує належне функціонування єдиної інформаційно-телекомунікаційної системи МВС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційно-телекомунікаційної системи МВС, здійснює обробку персональних даних в межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні послуги, створює інформаційні системи, системи зв'язку та передачі даних, використовуючи в діяльності досягнення у галузі науки та техніки, інформаційно-телекомунікаційну інфраструктуру.

Разом з тим, недостатня точність змісту даного явища, відсутність його однозначного юридичного трактування можуть послужити об'єктивною перешкодою для подальшого розвитку та вдосконалення не тільки діяльності МВС України в сфері міграції, а й усього механізму адміністративно-правового регулювання міграційних процесів в України.

Поняття «інформаційне забезпечення» в нормативно-правових актах використовується в чотирьох основних контекстах: інформаційно-правове забезпечення; інформаційних масиви, баз даних, банків даних; забезпечення інформацією, використання засобів масової інформації, інформаційна доступність (відкритість); використання інформаційних технологій і програмного забезпечення, які можна об'єднати в дві групи: забезпечення інформацією та поліпшення доступу до неї, з одного боку, використання комп'ютерної техніки (програм) – з іншого.

У своїй безпосередній діяльності Державна міграційна служба України, діяльність якої спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ,

який реалізує державну політику у сферах міграції, забезпечує створення, удосконалення, розвиток, супроводження та підтримку функціонування Єдиного державного демографічного реєстру, Єдиної інформаційно-аналітичної системи управління міграційними процесами, Національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, розпорядником яких є Державна міграційна служба, а також здійснює заходи із захисту інформації в них, здійснює збір, обробку, накопичення, зберігання та надання інформації споживачеві на базі інформаційних технологій; ведення довідкової інформації; забезпечення інформаційного обміну між службами та підрозділами [1].

Відповідно інформаційне забезпечення діяльності у сфері міграції це діяльність уповноважених служб і підрозділів МВС України (Державної міграційної служби, Національної поліції, Державної прикордонної служби України, Національної гвардії України) з пошуку, збору, обробці, накопичення, зберігання та надання інформації, що відповідає певним вимогам, необхідна та достатня для вирішення завдань МВС визначених у нормативно-правових документах, що регулюють міграційну сферу.

Стратегія державної міграційної політики України на період до 2025 року, схвалена постановою Кабінету Міністрів України від 12.07.2017 № 482-р, не визначає безпосередньо загальні напрями удосконалення інформаційного забезпечення діяльності МВС України у сфері міграції, тому доцільного доповнити розділ «Питання у сфері міграції, що потребують правового регулювання» Стратегії щодо загальних напрямів: вдосконалення реєстраційної діяльності, розробка та впровадження автоматичних інформаційних систем з інтегрованими обліками, в яких буде накопичуватися, систематизуватися та розглядатися неоднорідна за своєю природою інформація про різні об'єкти обліку на підставі удосконалення адміністративно-правового регулювання інформаційного забезпечення.

Адміністративно-правового регулювання інформаційного забезпечення діяльності у сфері міграції являє собою сукупність адміністративно-правових і процесуальних норм, які регулюють

суспільні відносини в ході реалізації органами державної влади управлінських функцій у сфері міграції.

Доцільно зауважити, що період здійснення покрокового переходу від обліків населення у вигляді паперових картотек до накопичення даних обліків в електронному вигляді з використанням інформаційно-комунікаційних і біометричних технологій передбачено у ході виконання Плану заходів з імплементації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, на 2014-2017 роки (затвердженого розпорядженням Кабінету Міністрів України від 17.09.2014 № 847-р). Водночас, для реалізації заходів необхідна наявність нормативно-правового акта, який буде механізмом для удосконалення інформаційного забезпечення діяльності у сфері міграції, на основні певних принципів, і відповідні технічні можливості.

Основні принципи інформаційного забезпечення в діяльності МВС у сфері міграції поділяються на: загальні, які функціонують в будь-якій системі інформаційного забезпечення діяльності МВС України; спеціальні, що відносяться до окремих її видів; приватні, властиві деяким її аспектам або окремим інформаційним процедурам.

До загальних принципів відносить законність, дотримання та повага прав і свобод людини та громадянина, науковість, універсальність, публічність. Спеціальні принципи поділяються на: управлінські (плановість, оптимальність, функціональність); методичні (єдність, комплексність, ідентифіковані, ефективність); програмно-технічні (оперативність, підзвітність, справжність). Приватні принципи включають в себе цінність, точність, цілісність, вибірковість, інтеграцію, повноту, уніфікацію, багаторазовість, компактність, конфіденційність, своєчасність, інтенсифікацію, захист від несанкціонованого доступу.

Впровадження розглянутих принципів дозволяють розкрити сутність інформаційного забезпечення діяльності у сфері міграції відповідних структур і служать основою його подальшого розвитку та вдосконалення.

Важливим аспектом у сфері міграції виступає взаємодія державних і місцевих органів, органів місцевого самоврядування. Взаємодія, в тому числі інформаційна, між підрозділами з питань міграції МВС України і органами виконавчої влади здійснюється за двома напрямами – в галузі міграційного та реєстраційного обліку (за місцем проживання та за місцем перебування) громадян України, іноземних громадян та осіб без громадянства в межах України. Приклад ЄС показує, що використання комплексного підходу у вирішенні питання про протидію негативним явищам у сфері міграції можливо за допомогою інформаційного забезпечення діяльності зацікавлених служб у контексті Єдиної інформаційно-аналітичної системи управління міграційними процесами (далі ЄІСУМП). Водночас, дана Єдина система поки що існує у вигляді Концепції, яку доцільно доповнити створенням єдиної мережі органів, що протидіють незаконній міграції. Основною ланкою мережі може бути МВС.

Впровадження ЄІСУМП з можливістю отримання доступної інформації в режимі он-лайн, дозволило б значно розширити та поліпшити взаємодію різних органів виконавчої влади, істотно скоротити терміни перевірок, що проводяться, зменшити документообіг, оперативно отримувати відповіді на запити в режимі он-лайн. Для реалізації Концепції Єдиної інформаційно-аналітичної системи управління міграційними процесами доцільно прийняти постанову Кабінету Міністрів України «Про міжвідомчу інформаційну взаємодію органів державної влади в Єдиній інформаційно-аналітичній системі управління міграційними процесами», що охопила би інформаційну взаємодію за: об'єктом, масштабами, змістом, спрямованістю.

У зазначеному контексті доцільно виділити п'ять основних напрямів вдосконалення адміністративно-правового регулювання інформаційного забезпечення діяльності МВС України в сфері міграції: нормативно-правовий (вдосконалення законодавства, введення нових норм права, розробка проектів нових правових актів); адміністративно-управлінський (створення нових структур, органів, мережі органів, підрозділів тощо); інноваційно-технологічний (вдосконалення АІС, розробка нових інформаційних

систем, сегментів і ін.); міжвідомчої взаємодії (обмін інформацією, електронний документообіг та ін.), кадровий (професійний відбір, підвищення кваліфікації співробітників, навчання впроваджуються інноваційним технологіям і ін.).

1. Постанова Кабінету Міністрів України від 20.08.2014 № 360 «Про затвердження Положення про Державну міграційну службу України». [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/360-2014-%D0%BF

Державна інформаційна політика та проблеми інформаційного забезпечення відкритості державної влади в Україні

Гаврильців Марія Теодорівна,

доцент кафедри адміністративно-правових дисциплін факультету № 8 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Розвиток всесвітнього процесу інформатизації XXI століття викликав нову глобальну проблему – інформаційної безпеки людини, держави та суспільства. Сьогодні інформаційний фактор є інтегруючим базисом життєдіяльності соціуму, а забезпечення інформаційної безпеки вступає однією з важливих принципів його подальшого розвитку. За таких обставин, особливого значення набуває формування виваженої державної інформаційної політики.

Проблема захисту інформації набула особливого значення в наш час. Захист інформаційного суверенітету тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута як захищеність внутрішньої інформації як такої, що припускає захищеність якості інформації, її надійність, захищеність різних галузей інформації (державної, банківської, комерційної таємниці) від розголошення, захищеність інформаційних ресурсів [1].

Глобалізація є об'єктивним явищем нинішнього часу. Її істотною рисою є інформаційна революція, що полягає у створенні єдиного

інформаційного простору, всесвітньої мережі спілкування на базі новітніх медіатехнологій та Інтернету. Ключовою рушійною силою глобалізаційних трансформацій є повсюдне розгортання новітніх інформаційно-комунікативних технологій. Технічний прогрес значно скоротив вартість накопичення, обробки та передачі інформації в планетарних масштабах, що позначилося на показниках економічного зростання.

Слід визнати, що у XXI ст. місце і роль держав у світі визначатимуть масштаби та глибина поширення цифрових технологій, супутникового зв'язку, оптичних волокон, комп'ютеризації та Інтернету. Їхній потужний вплив визначатиме взаємини в людській цивілізації, змінюватиме економічне та соціокультурне середовище, закладаючи засади нової форми суспільного устрою інформаційного типу.

Сучасну епоху називають ерою інформації або інформаційним суспільством, що характеризується домінуючою роллю інформації та знань, створенням глобального інформаційного простору, в якому завдяки високо розвинутим інформаційно-комунікативним мережам і технологіям забезпечуватиметься стале економічне та соціальне зростання, вільний доступ до світових інформаційних ресурсів, що дозволить людям у повній мірі використовувати свій потенціал та реалізовувати власні прагнення.

За цих умов надзвичайної актуальності набуває проблема впровадження дієвої системи державного управління в процесі переходу до високотехнологічного інформаційного суспільства. Процеси глобалізації торкаються дедалі нових сфер діяльності. Інформаційна також стає не тільки найважливішою сферою міжнародної співпраці, а й об'єктом суперництва.

Проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними загострюються внаслідок політичного й економічного протиборства держав. Це стає актуальним для забезпечення національної безпеки України.

Державна інформаційна політика в умовах глобалізації повинна відображати і враховувати більшість інтересів громадян, суспільних організацій, регіональних і муніципальних органів

влади, державних організацій і комерційних структур. Державна інформаційна політика України, як держави, розташованої на великому геополітичному просторі, повинна приймати до уваги різні рівні соціально-економічного, науково-технічного і культурного розвитку регіонів країни. Звідси виникає необхідність активної участі всіх зацікавлених громадян і структур у конкретизації, розвитку і реалізації державної інформаційної політики [2, с. 6].

Державна інформаційна політика в умовах глобалізації представляє собою сукупність цілей, що відображають національні інтереси України в інформаційному середовищі, стратегічних напрямів їх досягнення і систему заходів їх реалізації. Державна інформаційна політика є важливою складовою частиною внутрішньої і зовнішньої політики держави і охоплює всі сфери життєдіяльності кожного індивіда. Довгостроковою стратегічною метою інформаційної політики є забезпечення переходу до нового етапу розвитку України – побудови демократичного інформаційного суспільства і входження країни у світову інформаційну спільноту. Основою цього переходу є створення єдиного інформаційного телекомунікаційного простору країни як основи вирішення задач соціально-економічного, політичного і культурного розвитку країни та забезпечення її безпеки [2, с. 7].

Системна цілеспрямована інформаційна політика покликана забезпечити реалізацію насамперед таких стратегічних напрямів розвитку суспільства і держави: захист конституційних прав та свобод громадян в інформаційній сфері – свободи висловлювання й права на поінформованість; протидія структурам міжнародної організованої злочинності, що зловживають прозорістю світових інформаційних потоків; інформаційно-аналітичне забезпечення діяльності ЗМІ, владних, наукових, господарських та інших структур; пришвидшене входження України до європейського та світового інформаційного простору; розв'язання суперечностей між національною нормативно-правовою базою і європейським та міжнародним законодавством в інформаційній сфері тощо;

розвиток в Україні «електронного врядування» на засадах пришвидшеного розвитку національного сегмента Інтернету та впровадження новітніх медіа-інформаційних технологій; формування бюджету розвитку, який стимулював би примноження «людського капіталу» й протидіяв «відпливу розумового потенціалу» з України; стимулювання «інтелектуальної економіки» на засадах нормативно-правової бази, спрямованої на ефективний захист в Україні інтелектуальної власності, інтелектуальних продуктів і боротьбу з проявами «піратства» [3, с. 36].

Отже, найголовнішим завданням національної інформаційної політики є входження України у глобальне інформаційне суспільство. Для цього потрібно: модернізувати національну інформаційну інфраструктуру, створивши або запозичивши відповідні інформаційні технології; повною мірою реалізувати конституційні права громадян, суспільства та держави на інформацію; розв'язати низку актуальних проблем становлення та розвитку національних інформаційних ресурсів, інформаційно-аналітичного забезпечення діяльності владних, наукових, господарських та інших структур; розробити принципово нові напрями інформаційної діяльності, починаючи від електронного мережевого врядування та управління й закінчуючи електронною мережевою торгівлею тощо [3, с. 37-38].

Державна інформаційна політика належить сьогодні до пріоритетних напрямів розвитку української державності. Оскільки Українська держава не має реального суверенітету у власному інформаційному просторі, формується низка небезпек, викликів і загроз суспільному розвитку. Загальновідомо, що багато іноземних телекомпаній, радіостанцій, друкованих ЗМІ та Інтернет-видань відверто використовуються в інформаційно-психологічних операціях, які давно провадяться проти українських національних інтересів.

Отже, інформаційний суверенітет та відкритість державної влади є справді актуальною проблемою, адже лише відкрита, але водночас суверенна інформаційна політика може бути істинною передумовою належного інформаційного забезпечення

демократичного розвитку суспільства і держави. Тільки здійснюючи таку інформаційну політику, Україна посідатиме гідні позиції на світовій арені як впливова держава. Саме така інформаційна політика потрібна громадянам України, оскільки вона забезпечить реальну свободу слова й реальний громадянський контроль за діями та намірами влади, ефективні комунікації з центральною і місцевою владою [4, с. 373, 374].

Інформаційна відкритість і прозорість публічної влади є обов'язковими передумовами сталого демократичного розвитку суспільства та держави. Тільки на засадах відкритості й прозорості ґрунтується реальний громадський контроль і зміцнення довіри громадян до влади.

Поняття «відкритість і прозорість державної влади» слід розуміти як наявність у конкретній державі певних соціально-політичних інституцій, які мають можливість забезпечити ефективний вплив громадян на владу, спрямувати дії влади. У такій інтерпретації відкритість є ефективним інструментом забезпечення оптимального державного управління в інтересах людей та діалогу між владою і громадянським суспільством.

Суверенність і відкритість інформаційної політики в Україні є питанням ефективного функціонування нашої держави за участі соціально-політичних інституцій, що спроможні спрямувати дії публічної влади на захист загальнонаціональних інтересів.

Таким чином, інформаційна політика держави в нинішніх інтеграційних умовах буде ефективною лише за умови, якщо вона буде носити комплексний, системний характер, буде прозорою та відкритою для громадян, спрямованою на забезпечення інтересів суспільства і держави.

---

1. Крюков О. І. Інформаційна безпека держави в умовах глобалізації / О. І. Крюков. // Державне будівництво. – 2007. – №2. – Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12.
2. Пожуєв В. І. Формування концепції державної інформаційної політики в умовах глобалізації / В. І. Пожуєв // Гуманітарний

вісник Запорізької державної інженерної академії: збірн. наук. праць. – 2010. – Вип. 43. – С.4–12.
3. Інформаційна політика України: європейський контекст: монографія / Л. В. Губерський, Є. А. Макаренко, Є.Є. Камінський та ін. – К.: Либідь, 2007. – 360 с.
4. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: вибр. наук. праці / О. С. Власюк. – К.: НІСД, 2016. – 528 с.

Проектування та дослідження ВЕБ-орієнтованої системи приватних оголошень на базі 3 LAYERED ARCHITECTURE

Герич Андрій Іванович,

здобувач ступеня магістра Національного лісотехнічного університету України

Процах Наталія Петрівна,

професор кафедри вищої математики Національного лісотехнічного університету України, кандидат фізико-математичних наук, доцент

Інформаційні технології досягли такого розвитку, що, мабуть, не залишилося сфер людського життя, які не охоплені глобальною мережею Інтернет. В даний час інтерес до мережі Інтернет продовжує зростати. Розроблений в роки інформаційного вибуху Інтернет став невід'ємною, частиною життя більшості людей всього світу.

Зараз дуже актуальною є тема створення web-сайтів. Різні підприємства, навчальні заклади, міністерства мають свою сторінку в Інтернеті. Це найкраща реклама, інформаційний портал для будь-якої організації, це важливий крок компанії до розширення кордонів власного бізнесу та здобуття нової аудиторії. Науковцю, аспіранту, фахівцю творчої професії також важливо мати свою власну WEB-сторінку в Internet, на якій розміщується резюме, звіт про творчі досягнення тощо.

Також в наш час стає поширеним використання сайтів з виконанням різних видів послуг. Йдуть у минуле ті часи, коли

для того, щоб орендувати квартиру чи машину потрібно було здійснювати тривалі подорожі по різних місцях, шукати дошки з зазвичай неактуальними оголошеннями. Тепер в наше життя активно входять «дошки оголошень», які надають користувачам можливість створювати та переглядати оголошення таких категорій, як оренда житла, транспорту, вантажні перевезення та інші.

Мета роботи полягає в комбінуванні різних засобів та технологій, щоб в результаті отримати ефективну систему обробки інформації. Веб-орієнтована система використовує такі мови програмування та засоби: мова програмування C#, мови розмітки веб-сторінок HTML та CSS, бібліотеки Jquery та Angular 2, сервіс карт GoogleMaps API. Цього цілком достатньо, щоб створити хороший інтерфейс, бізнес-логіку та реалізувати трирівневу архітектуру. На сьогоднішній день, трирівнева архітектура досить добре показала себе в плані продуктивності, безпеці передачі даних та можливості підтримки і розширення без значних зусиль.

Основні задачі дослідження можна поділити на дві групи: практична та логічна. До практичних задач можна віднести аналіз наукової літератури, написання програмного коду і вдосконалення навичок та вмінь. Логічні задачі являють собою використання наявних знань для вирішення логічних та математичних проблем. В деяких частинах роботи потрібно буде правильно застосувати вже наявні алгоритми, щоб створити дійсно громіздку, корисну та ефективну веб-орієнтовану систему.

Трирівнева архітектура являє собою наявність в системі наступних компонент:

- клієнтський застосунок (веб-сайт, динамічний завдяки бібліотеці Angular 2)
- сервер (сервіс, реалізований на мові C#),
- сервер бази даних (система керування базами даних Miscrosoft SQL Server).

Зазначені вище засоби будуть використані для:

- створення інтерфейсу системи (те, що буде бачити і з чим буде взаємодіяти користувач);
- створення бізнес-логіки (логіки обробки інформації, коректного введення і виведення, проведення розрахунків та обчислень);

- створення частин системи, які можна буде використати в інших предметних областях та системах подібного типу;
- створення алгоритмів та методів для візуальної обробки інформації.

C# (вимовляється Сі-шарп) – об'єктно-орієнтована мова програмування з безпечною системою типізації для платформи .NET. На сьогоднішній момент мова програмування C# одна з найпотужніших, що швидко розвиваються і затребуваних мов в IT-галузі. На даний момент на ньому пишуться найрізноманітніші програми: від невеликих десктопних програм до великих веб-порталів і веб-сервісів, які обслуговують щодня мільйони користувачів.

З релізом .NET 4.5 в нашому розпорядженні опинився ще один інструмент для створення веб-служб – Web API. Концепція Web API являє собою новий підхід до реалізації веб-додатків. Контролери Web API застосовують стиль REST. Взагалі підтримка архітектури REST (Representation State Transfer або «передача стану») є одним з основних вузлових пунктів технології Web API. Для взаємодії з сервером в REST-архітектурі використовуються методи HTTP: GET (читання), POST (запис), PUT (оновлення), DELETE (видалення).

jQuery – популярна JavaScript-бібліотека з відкритим сирцевим кодом. Синтаксис jQuery розроблений, щоб зробити орієнтування у навігації зручнішим завдяки вибору елементів DOM, створенню анімації, обробки подій, і розробки AJAX-застосунків. jQuery також надає можливості для розробників, для створення плагінів у верхній частині бібліотеки JavaScript. Використовуючи ці об'єкти, розробники можуть створювати абстракції для низькорівневої взаємодії та створювати анімацію для ефектів високого рівня. Це сприяє створенню потужних і динамічних веб-сторінок.

Angular 2 – JavaScript-фреймворк з відкритим програмним кодом, який розробляє Google. Призначений для розробки односторінкових додатків, що складаються з одної HTML сторінки з CSS і JavaScript. Його мета – розширення браузерних застосунків на основі шаблону Модель-вид-контролер (MVC), а також спрощення їх тестування та розробки. Фреймворк працює зі сторінкою HTML, що містить додаткові атрибути і пов'язує області вводу або виводу сторінки з моделлю, яка є звичайними

змінними JavaScript. Значення цих змінних задаються вручну або отримуються зі статичних або динамічних JSON-даних.

Google Maps – набір додатків, побудованих на основі безкоштовного картографічного сервісу і технологій, які надає компанія Google. Сервіс являє собою карту та супутникові знімки всього світу і надає користувачам можливості панорамного перегляду вулиць (Google Street View), аналізу трафіку у реальному часі (Google Traffc), прокладання маршруту (автомобілем, пішки, велосипедом або громадським транспортом). З сервісом інтегрований бізнес-довідник і карта автомобільних доріг, з пошуком маршрутів, яка охоплює США, Канаду, Японію, Гонконг, Китай, Велику Британію, Ірландію (тільки центри міст) і деякі райони Європи.

Веб-орієнтована система допомагає користувачам заощаджувати час на пошуки необхідних послуг (наприклад, оренда квартири чи транспорту) або ж з легкістю створювати власні оголошення. Сервіс Google Maps дозволяє прив'язати оголошення до певного місця, щоб інші користувачі змогли шукати оголошення прямо на карті. Це дозволить швидко знайти квартиру в необхідному місті, районі і навіть вулиці.

Гнучка система фільтрування дозволить підібрати оголошення використовуючи критерії унікальної категорії та цінові діапазони. Для підтримки актуальності оголошень, буде використано функціонал оновлення оголошень один раз в два тижні. Це дозволить користувачеві бачити тільки найбільш актуальні оголошення в процесі пошуку.

Розроблена структура буде мати практичне значення в різних проектах. Наявну бізнес-логіку та математичні операції з відношеннями можна буде використати в інших цілях та проектах. Також можна вдосконалити вже існуючу логіку, щоб збільшити швидкість роботи системи, створити більш гнучні та глобальні алгоритми для пошуку, обробки, відображення різних наборів даних тощо.

Під час проектування був проведений аналіз предметної області, вибраних технологій, математичного забезпечення синтезу та функціонування трирівневої архітектури. Як подальше

вдосконалення веб-сайту представляється можливим доопрацювання інтерфейсу, функціоналу та розширення вже наявних можливостей з метою подальшого підвищення швидкості роботи, інформативності і зручності використання системи.

1. Інькова Н. А. Сучасні інтернет-технології в комерційній діяльності: навч. посібник / Н. А. Кнькова. Видавництво «Омега-Л», 2007. – 188с,
2. Е. Троелсен, Язык программирования C# 5.0 и платформа .NET 4.5, Видавництво «Вильямс», 2015. – 1312с.
3. В. Дронов, HTML 5, CSS 3 и Web 2.0. Разработка современных web-сайтов. Видавництво «БХВ-Петербург», 2011. – 416с.
4. Пабло Дилеман, Изучаем Angular 2. Видавництво «ДМК Пресс», 2017. – 356с.
5. Документація jQuery [Веб-ресурс] – https://api.jquery.com
6. Документація Google Maps [Веб-ресурс] – https://developers.google.com/maps
7. Metanit – сайт про програмування [Веб-ресурс] – https://metanit.com

Відеоресурс як темотвірний елемент методичної системи навчання

Глинський Ярослав Миколайович,

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

Ряжська Вікторія Анатоліївна,

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

Підготовка студентів загальнотехнічних спеціальностей в рамках дисципліни «Вища математика» передбачає вивчення основ математичного аналізу, лінійної алгебри, елементів теорії ймовірності, математичної статистики та інших питань. У час бурхливого розвитку інформаційно-комунікативних технологій

постає задача ознайомлення студентів із сучасними засобами комп'ютерної математики. Зазвичай лише на деяких напрямах підготовки, де вивчають числові методи чи методи математичного моделювання в конкретних предметних областях, використовують засоби комп'ютерної алгебри на кшталт Mathcad, Matlab, Maple, Mathematica, вивчення яких потребує певних часових затрат і зусиль. Короткий порівняльний огляд цих програм можна знайти в [1].

Зазначимо, що особливу популярність в інженерних колах мають програми Mathcad і Matlab. Ці програми належать до класу засобів автоматизації математичних розрахунків. Їх порівнюють з такими програмними комплексами, як Maple, Mathematica, а також з їх аналогами MuPAD, SciLab, Maxima та ін. Система Maple, наприклад, призначена головно для виконання аналітичних (символьних) обчислень і має для цього один з найпотужніших у своєму класі арсенал спеціалізованих процедур і функцій (понад 3000). Така комплектація для більшості користувачів, які стикаються з необхідністю виконання математичних розрахунків середнього рівня складності, є надлишковою. Можливості Maple орієнтовані на користувачів – професійних математиків. Розв'язування задач в середовищі Maple потребує не тільки вміння оперувати тією чи іншою функцією, але й знання закладених в неї методів розв'язування. Те ж саме можна сказати і про Mathematica. Це одна з найпотужніших систем. Вона має надзвичайно велику функціональну наповненість (є навіть синтезатор звуку). Mathematica характеризується високою швидкістю обчислень, але потребує вивчення доволі незвичайної мови програмування.

Mathcad і Matlab, на відміну від Maple, створювалися для чисельного розв'язування математичних задач. Вони орієнтовані на розв'язування задач саме прикладної, а не теоретичної математики, коли потрібно отримати результат без заглиблення в математичну суть задачі. Символьне ядро Mathcad, на відміну від оригінального Maple (MuPAD), штучно обмежене (доступно близько 300 функцій), але цього в переважній більшості випадків цілком достатньо для розв'язування задач інженерного

характеру [1]. Наявні 15 релізів Mathcad і новіші чотири релізи Mathcad Prime є платними, а доступні 30-денні trial-версії маю суттєво обмежені функційні можливості.

Базуючись на багаторічному досвіді роботи із засобами комп'ютерної математики ми стверджуємо, що одним із кращих навчальних програмних засобів для широкого кола студентів є програма Microsoft Mathematics 4.0. Ця програма характеризується достатньо повним функціоналом, простотою і зручністю у використанні, є freeware, не потребує особливих ресурсів локального комп'ютера і легко завантажується на локальний комп'ютер користувача з сайту корпорації Microsoft.

Програма Microsoft Mathematics на нашу думку є оптимальним засобом не тільки для стартового ознайомлення, але й для прикладного використання початківцями. Її можна опанувати за короткий час самостійно. Для цього достатньо продемонструвати на лекції чи порекомендувати студентам переглянути у відеохостингу в Youtube відеофільм про цю програму одного з авторів даного матеріалу [2], який можна завантажити чи переглянути за адресою https://www.youtube.com/watch?v=nAg-ZmW0NGA&t=928s.

Програма надає набір інструментів, які допомагають студентам швидко і просто справлятися з багатьма навчальними завданнями з курсу вищої математики. Її рекомендуємо вивчати власне в рамках дисципліни «Вища математика» на першому курсі без затрат академічного часу, а за рахунок годин, які надаються на самостійну роботу студентів. Засобами Microsoft Mathematics можна навчитися покроково розв'язувати системи лінійних і нелінійних рівнянь, будувати графіки, освоїти основні поняття лінійної алгебри, математичного аналізу і статистики. Крім цього програма надає довідник основних формул з фізики, хімії та елементарної математики, за допомогою яких можна негайно виконати обчислення, якщо відомі вхідні дані.

За допомогою програми Microsoft Mathematics можна виконувати дії з комплексними і дійсними числами, аналітичні перетворення виразів (розкладати на множники, зводити подібні члени,

диференціювати, знаходити частинні похідні, первісні, обчислювати границі, інтеграли, скінченні та нескінченні суми та добутки), а також можна виконувати дії з числовими множинами.

Програма має достатні 2D- і 3D-графічні засоби. Графіки функцій можна будувати як в прямокутній, так і в полярній системі координат, а також функцій, заданих параметрично. Є зручний засіб трасування, який дає змогу отримати числові значення у будь-якій точці графіка. Поверхні можна обертати для огляду з різних кутів. Ефективно реалізований графічний метод розв'язування систем і сукупностей нерівностей.

Просто і особливо зручно реалізовані матричні операції (дії з матрицями, зокрема, обертання і транспонування матриці, обчислення визначника і сліду). Можна обчислювати скалярні і векторні добутки векторів, вектор-градієнт функції в деякій точці тощо.

В Microsoft Mathematics є три способи виконання дій: 1) за допомогою графічного інтерфейсу, 2) засобами традиційних меню, 3) шляхом введення команд вручну. Останній спосіб потребує певної підготовки. Перші два способи реалізують лише головні функційні можливості програми (що достатньо для студентів загальнотехнічних спеціальностей), а фахівцям варто ознайомитися з усіма командами, які описані у help-довіднику програми і освоїти практичну роботу з командами. Довідник добре структурований і не залишить байдужим не лише студента, але й досвідченого педагога. Так розділ «Статистика» у графічному інтерфейсі містить лише елементарні операції (максимум, мінімум, медіану, моду набору даних), тоді як у довіднику користувач знайде команди для обчислення кореляції та коваріації двох наборів даних, різні усереднення (геометричне середнє, середнє квадратичне, середнє відхилення, дисперсію) набору даних та інше.

Суттєвою перевагою є те, що програма цілком безкоштовна (freeware). Для ознайомлення з програмою її треба завантажити з сервера корпорації Microsoft, виконавши спочатку гугл-пошук джерела за назвою програми. Якщо на комп'ютері користувача

немає Microsoft Office, то для функціювання програми слід додатково завантажити з цього ж сервера Microsoft .Net Framework 3.5.

У даній роботі стверджується, що зі змісту навчальних програм з вищої математики для студентів загальнотехнічних спеціальностей, випливає, що програма Microsoft Mathematics цілком підходить для першого знайомства студентів з основами сучасної комп'ютерної алгебри власне в рамках дисципліни «Вища математика». Але використання цього засобу потребує подолання декількох перепон: 1) відсутність академічних годин у навчальних планах на вивчення питань комп'ютерної математики; 2) не передбачено доступ до комп'ютерних класів для проведення лабораторного практикуму; 3) не всі викладачі-математики готові швидко освоїти програмний продукт і методику його використання; 4) не створені дидактичні засоби підтримки навчального процесу. Тому важливою нашою задачею є описання шляхів подолання цих труднощів.

Перш за все зазначимо, що переважна більшість студентів мають у особистому користуванні персональні комп'ютери різних конфігурацій, а студенти, які їх не мають, можуть скористатися для самопідготовки вільним доступом до комп'ютерної техніки, який є в багатьох навчальних закладах. Тому вивчення питань комп'ютерної математики можна реалізувати в рамках годин, відведених на самостійну роботу студентів, що знімає перші три перепони. Четверту перепону ліквідовуємо ми. Згаданий вище відеоурок «Основи комп'ютерної математики з Microsoft Mathematics» дає змогу організувати ознайомче вивчення базових понять комп'ютерної математики (комп'ютерної алгебри) в рамках дисципліни «Вища математика» чи іншої дисципліни без проведення аудиторних занять на цю тему, що веде до економії аудиторного часу навчання і забезпечує високий рівень навчального процесу. Для цього викладач може і не знати глибоко суті питання оскільки йому достатньо продемонструвати на лекції чи на іншому занятті відеоресурс чи порекомендувати самостійно переглянути відеоресурс, який автоматично виведе студента на рівень знань, достатній для виконання практичних задач. Коло

задач і завдань стартового рівня наведено в [3]. Бажано, щоб навіть не працюючи особисто з програмою, викладач ознайомився з її можливостями, наприклад, прочитав help-файли (довідник від розробників програми) для того, щоб сформулювати завдання з курсу вищої математики, які доцільно розв'язати, використовуючи Microsoft Mathematics. Оскільки відеоресурс майже повністю закриває проблему ефективного впровадження у навчальний процес нової актуальної теми ми стверджуємо, що даний відеоресурс виконує темотвірну роль, тобто є темотвірним засобом у методичній системі навчання. Якщо раніше ми мали справу з навчальними відеоресурсами демонстраційного призначення, що були додатковими елементами методичної системи навчання, то тепер ми розробили відеоресурс, який є невід'ємною складовою навчального процесу, тобто такого, без якого обійтися не можливо. Оскільки відеоресурс є необхідною умовою впровадження нової теми у навчальний процес, то цим доводиться, що він є темотвірним елементом методичної системи навчання. Достатньою умовою побудови ефективного навчального процесу є активна участь викладача у підборі завдань (дидактичних матеріалів з вищої математики), які мають бути запропоновані студентам з урахуванням можливостей цієї програми.

Актуальними постають питання розробки аналогічних відеоресурсів для вивчення інших програм комп'ютерної математики, таких як Mathcad та Matlab, оскільки наші дослідження відеохостингів показали, що ефективних навчальних відеоресурсів на цю тему майже немає, а україномовних немає взагалі.

1. Mathcad. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia. org/wiki/ Mathcad.
2. Ярослав Глинський. Основи комп'ютерної математики з Microsoft Mathematics. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=nAg-ZmW0NGA&t=144s.
3. Глинський Я.М. Інформатика. Практикум з інформаційних технологій. «Підручники і посібники», Тернопіль – 2014.

Автоматизоване проектування та моделювання руху дискової фрикційної муфти засобами SOLIDWORKS API та SOLIDWORKS SIMULATION

Горлатий Руслан Михайлович,

здобувач ступеня магістра Національного лісотехнічного університету України

Головатий Андрій Ігорович,

доцент кафедри інформаційних технологій Національного лісотехнічного університету України, кандидат технічних наук

Дана робота присвячена принципу роботи дискової фракційної муфти, моделювання руху збірки, автоматизованому проектуванню деталей, аналіз слабких місць спроектованої муфти, використовуючи засоби SolidWorks API та SolidWorks Simulation.

Дискова фракційна муфта служить механізмом включенню лебідки бурового верстата. Вона включається на ходу і передає крутний момент провідного валу механізму на відомий. На рис.1 представлено розріз даної муфти.

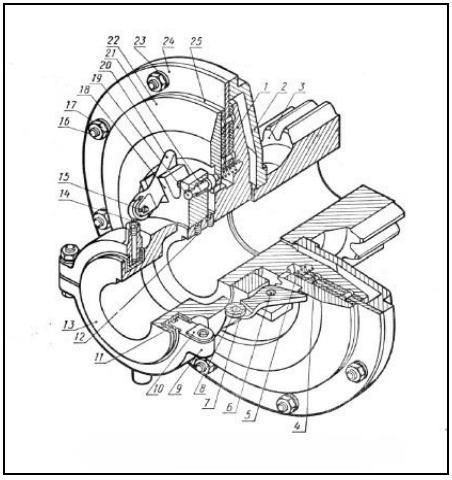


Рис.1. Дискова фракційна муфта

Умовно муфту можна поділити на три частини: рухомий елемент складається із двох дисків основного (1) і фіксуючого (22); керуючий – конус включення (13), регулятор(18), кулачок (20), ролик (7), палець регулятора (19); робочий – робочих накладок (25), півкілець (24), фланець (2), зубчасте колесо (3).

Для автоматизованого проектування дискової фракційної муфти, було розроблено програмний додаток засобами SOLIDWORKS API на мові програмування C#. Даний додаток дозволяє будувати деталі з різними розмірами, матеріалами, зберігати і зчитування параметри в окремий файл.

Алгоритм створення деталі є досить гнучким та простим. Для створення нової деталі не потрібно починати писати код спочатку, все що потрібно – це документація класів програми. Вона відтворює модель використовуючи структуру об'єктів керування побудови моделі, за допомогою бібліотек SOLIDWORKS API програма послідовно будує об'єкт в програмі SOLIDWORKS.

Використання додатку дозволить зберігати не готову модель, а компактний файл програми формату xml з параметрами та інструкціями для побудови деталі. Зміна розмірів в програмі з легкістю змінює бажаний розмір. На рис. 2 зображено основну форму програми.

Користувачу для створення моделі необхідно натиснути файл-відкрити_файл, програма зчитає розміри, прив'язки, об'єкти побудови: лінії, кривої, елемент витиснення або повернення ескізу.

Проаналізувавши збірку і принцип роботи муфти, досліджували фіксуючий диск оскільки він найбільше отримує навантаження особливо між включенням і виключенням лебідки верстата. В досліді 1 присвоїв матеріал алюміній, дослід 2 берилію, нержавіюча сталь в досліді 3. Найкращі результати показав дослід 3 оскільки деталь отримала найменше напруження, і незначні деформації з високим запасом міцності.

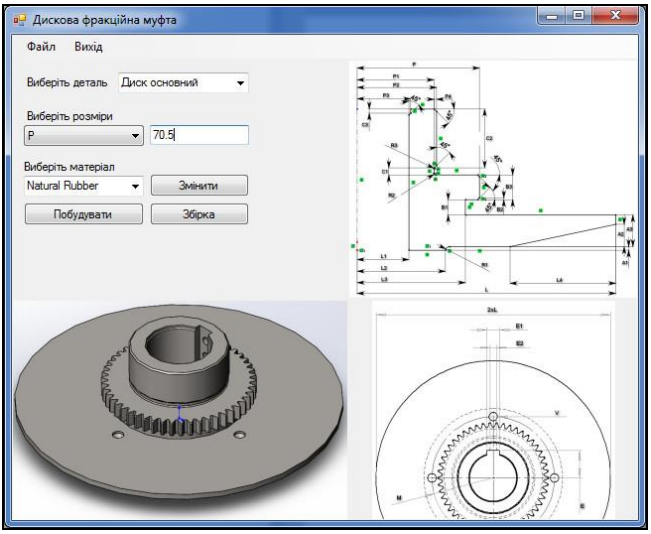


Рис. 2. Основна форма програми

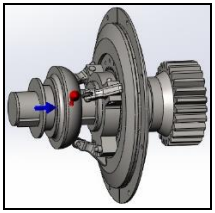


Рис.3. CAD-модель

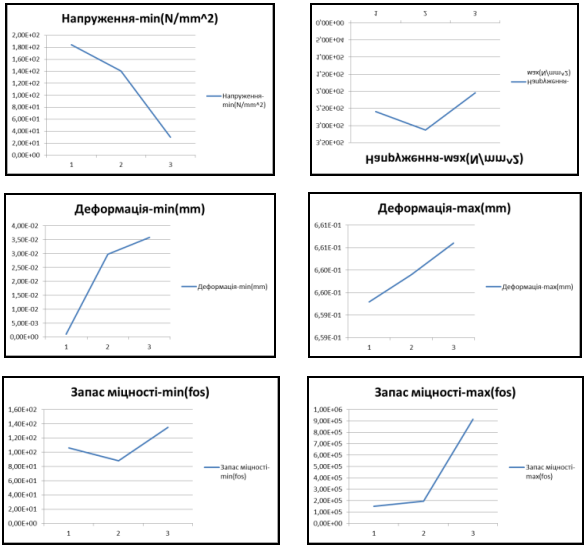


Рис.4. Результати моделювання

1. Наталя Дударєва, Сергій Загайко, «SolidWorks 2009 на прикладах» «БХВ». – Санки-Петербург, – 2009. – 530
2. Алямовський А. А. «SolidWorks комп'ютерне моделювання в інженерній практиці» «БХВ». – Санки-Петербург, – 2005. – 800 с.

Система класифікації наукових статей

Дендюк Ірина Михайлівна,

здобувач ступеня магістра Національного лісотехнічного університету України

Дендюк Михайло Володимирович,

доцент кафедри інформаційних технологій Національного лісотехнічного університету України, кандидат технічних наук, доцент

Процик Юрій Степанович,

доцент кафедри інформаційних технологій Національного лісотехнічного університету України, кандидат фізико-математичних наук

Актуальність завдання. В даний час йде постійний і швидкий ріст обсягів інформації. Значну частину цієї інформації складають дані у всесвітній мережі Інтернет. У зв'язку з цим постає проблема створення засобів класифікації та пошуку потрібної інформації у багатотерабайтному гіперпросторі. Сучасні засоби пошуку, класифікації, опису текстів, зокрема, пошукові сервери не завжди забезпечують можливість знайти детальну інформацію для деякого об'єкта. Розроблення інтелектуальної системи класифікації наукових статей є дуже актуальним завданням, оскільки надає змогу підвищити ефективність пошуку інформації та здійснювати статистичний аналіз результатів пошуку.

Постановка завдання. Класифікація наукових статей проведена на прикладі Наукового вісника НЛТУ України.

Складовими такої системи будуть підсистеми наповнення інформацією БД, обробки пошукових запитів, лексичного аналізу та класифікації статей (рис.1).

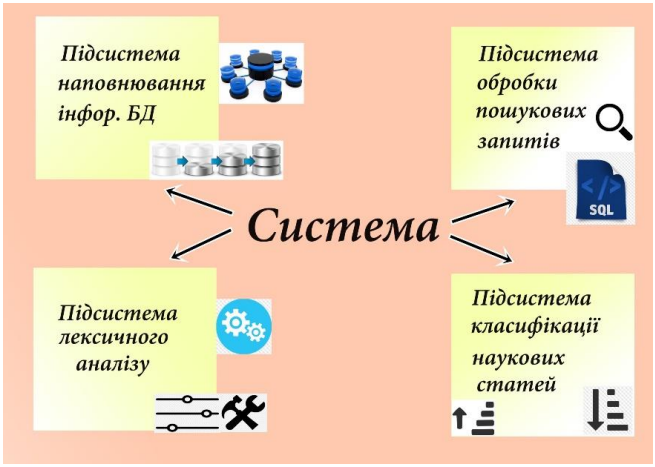


Рис. 1. Структурна схема системи класифікації наукових статей

Реалізація. Робота будь-якої інформаційної системи починається з введення вхідної інформації. У даній роботі вхідна інформація за результатами парсингу з використанням регулярних виразів заноситься у клієнт-серверну БД для подальшої обробки.

Опрацювання інформації з БД здійснюється застосунком користувача, розробленого за технологією ADO.Net. Такий підхід надає змогу багатокористувацького доступу до результатів парсингу і передбачає дворівневу архітектуру інформаційної системи (рис. 2).

Парсинг складається з двох етапів:

- парсинг HTML-коду;
- парсинг вмісту PDF-файлів.

Спочатку проводиться парсинг HTML-коду веб-сторінки архіву збірників науково-технічних праць, визначаючи атрибути кожного номера збірника, в тому числі і його адресу в мережі Інтернет. За цими адресами здійснюється парсинг HTML-коду

кожного збірника за розділами, результатом якого є отримання відповідної назви розділу, авторів та назв статей.

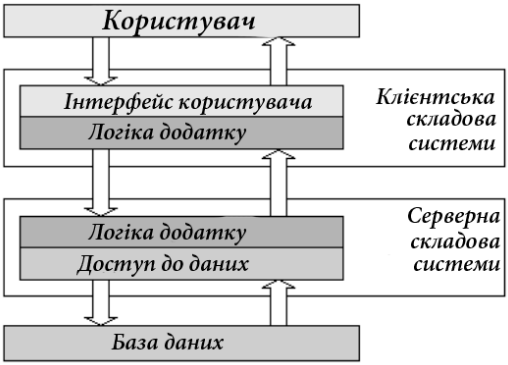


Рис. 2. Дворівнева архітектура інформаційної системи класифікації статей

Для парсингу PDF-файлів було розроблено програмне забезпечення, яке дозволяє розпізнавати текст, розміщений у декілька колонок. Як наслідок, було отримано перелік ключових слів до кожної статті. При розпізнаванні PDF-файлу враховувалось положення поточних координат, що дало змогу визначити межі колонок.

Завдання класифікації полягає в проведенні статистичного аналізу отриманої інформації у БД (рис. 3).

Рис. 3. Способи класифікації статей

Зокрема, отримано сумарну інформацію для публікацій в розрізах за авторами та ключовими словами, знайдено споріднені назви статей. Проведено лінгвістичний аналіз та здійснено класифікацію результатів парсингу – наукових статей.

Для досягнення поставленої мети передбачено розв'язання таких завдань:

- вивчення структури сайту Наукового вісника НЛТУ України;
- розроблення підсистеми синтаксичного аналізу;
- розроблення підсистеми наповнення БД;
- розроблення підсистеми пошукових запитів;
- розроблення підсистеми класифікації наукових статей;
- аналіз отриманих результатів та формування висновків.

Результатом проведеної роботи є система, яка:

- виконує синтаксичний та лінгвістичний аналіз з використанням регулярних виразів для знаходження потрібної інформації в HTML-файлах сайту Наукового вісника НЛТУ України;
- виконує синтаксичний та лінгвістичний аналіз PDF-файлів з використанням регулярних виразів, у яких інформація зберігається у декілька колонок;
- здійснює статистичний аналіз отриманої інформації, за яким реалізовано класифікацію наукових статей.

Висновки. Аналіз статистичних результатів класифікації наукових статей показав, що найбільша кореляція слів у назвах статей в межах одного розділу дозволяє здійснювати досконалішу класифікацію статей за словами в їх назвах. Кореляція ж ключових слів в межах одного розділу різних вісників надзвичайно низька, тобто ключові слова у статях в межах одного розділу не повторюються для різних авторів і тому класифікацію статей за ключовими словами не рекомендується здійснювати.

1. Е. Троелсен, Язык программирования C# 5.0 и платформа .NET 4.5, Вильямс, 2015. – 1312 с.
2. Роббинс.Дж. Отладка приложений для Microsoft .NET. К: Русская Редакция, Питер, 2008. – 512 с.

3. Липаев В.В. Обеспечение качества программных средств. Методы и стандарты. М.: Синтег, 2001. – 246 с.
4. Інькова Н. А. Сучасні інтернет-технології в комерційній діяльності: навч. посібник / Н. А. Кнькова. Москва: Видавництво «Омега-Л». – 188 с. – (Бібліотека вищої школи), 2007.
5. Полное руководство по языку программирования C# 7.0 и платформе .NET 4.7 / [Електронний ресурс]: режим доступу: https://metanit.com/sharp/tutorial/.
6. Паттерны проектирования в C# и .NET / [Електронний ресурс]: режим доступу: https://metanit.com/sharp/patterns/.
7. Платформа ADO.NET и Entity Framework NET / [Електронний ресурс]: режим доступу: https://metanit.com/sharp/ado.php.

Використання MapReduce для обробки великих об'ємів даних

Дідик Христина Ігорівна,

здобувач ступеня бакалавра Львівського державного університету внутрішніх справ

Пасічник Софія Богданівна,

здобувач ступеня бакалавра Львівського державного університету внутрішніх справ

Неспляк Дмитро Михайлович,

доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук

Тучапський Роман Ігорович,

науковий співробітник відділу моделювання композитних структур і складних систем Інституту прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, кандидат фізико-математичних наук

На даний час все більшу і більшу роль відіграють інформаційні технології для ефективної обробки великих об'ємів даних. Обсяг інформації у світі зростає більш ніж вдвічі кожні два роки. Тому особлива уваго приділяється алгоритмам і методам

для обробки та аналізу даних з використанням комп'ютерних кластерів. Проте такий вид обробки завжди є дуже складним, і багато часу витрачається на вирішення рекурсивних проблем, таких як паралельна обробка даних, розподіл даних на обчислювальні вузли та обробка помилок. Щоб звільнити розробників від цих повторюваних завдань, Google представив модель розподілених обчислень MapReduce та розробив абстрактний шар, який розподіляє потік даних на два основні етапи: map та reduce [1 – 3]. Обчислення можуть відбуватися паралельно на декількох комп'ютерах як на етапі map так і на етапі reduce. Програми з використанням MapReduce можуть виконуватись паралельно на комп'ютерному кластері. Програмна платформа з відкритим кодом Apache Hadoop, що імплементує MapReduce може бути встановлена на стандартному обладнанні та дає можливість запустити кластер MapReduce, який може динамічно розширюватися за допомогою додавання більшої кількості комп'ютерів.

Основа системи MapReduce – це розподілена файлова система. Найпопулярнішим прикладом такої файлова системи є Hadoop Distributed Filesystem (HDFS). Характерною особливістю даної системи є те, що великі файли поділяються на блоки однакового розміру, які розподіляються в кластері для зберігання. Дані організовані у виді деякого набору упорядкованих записів (рядків). Оскільки завжди може виникнути збій комп'ютера у кластері, то кожен блок потрібно зберігається декілька разів (як правило, тричі) на різних комп'ютерах.

При імплементації MapReduce використовується почергове застосування функцій map та reduce. Труднощі, що виникають у процесі паралельного виконання цих функцій обробляються системою автоматично. Ітерація складається з трьох фаз: map, shaffle та reduce.

Фаза map застосовує функцію map до всіх вхідних даних. Для цього функції map запускаються на всіх комп'ютерах кластера, завданням яких є обробка блоків у вхідному файлі, що зберігається локально на комп'ютері. Тобто обчислення відбуваються там, де зберігаються дані. Оскільки не існує

залежностей між різними функціями map, то вони можуть працювати паралельно та незалежно один від одного. Якщо на якомусь комп'ютері у кластері виникає збій, то останні або ще не обчислені результати map функції можуть бути перераховані на іншому комп'ютері, який виконує копію відповідного блоку. Під час фази map вміст блоку обробляється по рядку, а кожен рядок інтерпретується як пара key-value. Функція map виконується окремо для кожної з цих пар і створює довільно великий список нових пар key-value: map(key, value) ⇒ List(key', value').

Фаза shaffle локально сортує отримані пари з фази map за допомогою їхніх ключів, після чого MapReduce присвоює ці пари до reduce відповідно до їхніх ключів. Фреймворк гарантує, що всі пари з однаковими ключами призначаються для одного й того ж reduce. Оскільки вихідні результати з фази map можуть бути розподілені довільно по всьому кластері, то вони повинні передаватись через мережу до потрібних reduce під час фази shaffle. Тому на даній фазі великі об'єми даних передаються через мережу.

Під час фази reduce об'єднуються всі пари з однаковим ключем і створюються відсортовані списки з відповідних значень для кожного ключа. Ключі та відсортовані списки значень служать вхідними даними для функції reduce. Функція reduce зазвичай стискає список значень, щоб створити коротший список шляхом агрегування значень. Як правило, він повертає одне значення як результат. Функція reduce створює як завгодно великий список пар key-value як і функція map: reduce(key, List(values)) ⇒ List(key', value')

Модель MapReduce для розподілених обчислень може бути використана для дослідження та обробки великого об’єму статистичних даних, які можуть оброблятись на багатьох серверах.

---

1. Dean, J., S. Ghemawat. «MapReduce: Simplified Data Processing on Large Clusters.» In: OSDI ’04: 6th Symposium on Operating Systems

Design and Implementation (USENIX and ACM SIGOPS, 2004), pp. 137-150
2. Сухобоков А. А. Влияние инструментария Big Data на развитие научных дисциплин, связанных с моделированием. М.: МГТУ им. Н. Э. Баумана, 2015. 51 с.
3. Натан М. Большие данные. Принципы и практика построения масштабируемых систем обработки данных в реальном времени. М.: Вильямс, 2015. 368 с.

Щодо проблем використання даних ДНК-аналізу під час розслідування злочинів

Дмитрик Юрій Іванович,

доцент кафедри оперативно-розшукової діяльності факультету № 2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Гарват Тетяна Вікторівна,

здобувач ступеня бакалавра факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

Станом на сьогоднішній день перед органами досудового розслідування стоїть завдання щодо впровадження в систему доказів все більш ширших сучасних можливостей судових експертиз. Одним із таких досліджень, під час розслідування кримінальних правопорушень, може виступати метод генотипоскопії при біологічній експертизі або так званий ДНК-аналіз [1, с.278] в основі якого лежить принцип дослідження біоматеріалу людини, який містить генетичну інформацію.

Як відомо, дезоксирибонуклеїнова кислота (ДНК) є одним із двох типів природних нуклеїнових кислот, що забезпечує зберігання, передачу з покоління в покоління і реалізацію генетичної програми розвитку й функціонування живих організмів [2].

За своєю природою дезоксирибонуклеїнова кислота є індивідуальним кодом спадкової інформації для кожної особи та найбільш захищеним елементом з поміж усіх відомих біоло-

гічних зразків, які підлягають використанню для проведення експертного дослідження під час розслідування злочинів. Такі природні властивості молекули ДНК унеможливлюють спроби підробки біологічного матеріалу з метою приховування інформації про особу справжнього злочинця.

Варто зазначити, що однією з найбільш суттєвих переваг ДНК-аналізу, під час розслідування злочинів, є використання високотехнічних засобів, за допомогою яких можна отримати результат з імовірністю помилки менше ніж один раз на декілька мільярдів випадків, тим самим виділити одну єдину людину зі всіх, хто проживає на планеті. Таким чином, можна стверджувати, що універсальність та висока індивідуальність визначають генотипоскопію як найбільш дієвий спосіб попередження, виявлення та припинення кримінальних правопорушень, пошуку осіб, що їх вчинили та осіб які переховуються від органів досудового розслідування [1, с. 278].

Використання даних ДНК-аналізу є досить ефективним способом розслідування злочинів оскільки його можна застосовувати для визначення належності біоматеріалу конкретній особі, встановлення факту настання вагітності внаслідок згвалтування, ідентифікація померлої особи за рештками, встановлення зв'язку між різними злочинами тощо.

З одного боку, ДНК-аналіз надасть змогу правоохоронним органам виявляти злочинців які вчинили кримінальне правопорушення чи можуть бути причетні до його підготовки або вчинення, а з іншого – результати ДНК-аналізу нададуть можливість спростувати причетність невинуватої особи до вчинення кримінального правопорушення, що в свою чергу значно спростить процедуру доказування.

Однак, у зв'язку з високою вартістю та неможливістю примусового відібрання біоматеріалу для генотипоскопії особи, даний вид аналізу, зазвичай, використовується в рамках цивільного судочинства, до прикладу для встановлення батьківства (материнства), виключно за кошти фізичних або юридичних осіб.

На противагу використання ДНК-аналізу в Україні варто звернути увагу на досвід Великобританії, яка є країною, що

започаткувала даний вид дослідження. У 1995 році Великобританія створена Національну базу ДНК-даних – NDNAD (UK National Criminal Intelligence DNA Database), в яку вносять інформацію про будь-яку затриману поліцією особу, навіть якщо потім її вина не підтвердиться. Крім того, в Шотландії передбачена процедура добровільної здачі громадянами держави своїх ДНК-зразків, з метою можливої ідентифікації в майбутньому у цивільних справах. Таким чином, у Великобританії створена найбільша колекція генетичної інформації населення держави, яка складає приблизно 5,2% від загальної чисельності населення.

У США експериментальні бази ДНК були запущені в шести штатах і криміналістичних лабораторіях у 1990 році, а в 1994 був прийнятий закон про примусовий збір зразків ДНК у людей, засуджених за скоєння тяжких та особливо тяжких злочинів. В 1998 році у США створена Національна база даних із генетичної інформації. До 2002 року в ній зберігалося понад 800 тис. генотипів. Сьогодні вже у всіх 50 штатах передбачений обов'язковий збір ДНК зразків у осіб, які скоїли злочин з застосуванням сексуального насилля чи вбивство. В 47 штатах збирають ДНК у всіх засуджених злочинців [3, с.164].

Однак, для правоохоронних органів України, на відміну від інших розвинених держав світу, практика використання ДНК-аналізу, під час розслідування злочинів, та створення подібних інформаційних баз є новою.

Разом з тим, облік генетичних ознак людини ведеться в ДНДЕКЦ МВС України, відповідно до наказу МВС від 10.09.2009 № 390 «Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС», зареєстрованого в Міністерстві юстиції України 15.10.2009 №963/16979 [4]. Станом на початок 2017 року до центрального обліку генетичних ознак людини ДНДЕКЦ МВС України поміщено 17467 ДНК-профілів осіб. Проте, зазначена кількість ДНК-профілів осіб, в центральному обліку генетичних ознак людини ДНДЕКЦ МВС України, є недостатньою для ефективної роботи правоохоронних органів. Також законодавчо

не визначено підстави, які є передумовою внесення ДНК-профілів осіб до обліку генетичних ознак людини.

Таким чином, з метою створення умов для належного та ефективного експертного забезпечення правосуддя, необхідно вдосконалити регулювання судово-експертної діяльності на законодавчому рівні та створити єдину Національну базу обліку генетичних ознак людини, яка буде обліковувати інформацію не лише про правопорушників, але й осіб, діяльність яких пов'язана зі значним ризиком для життя (військовослужбовці, учасники антитерористичної операції, співробітники СБУ, МВС тощо).

1. Коропецька С.О. ДНК-аналіз та особливості відбирання для його проведення біологічних зразків / С.О. Коропецька // Електронне наукове фахове видання «Порівняльно-аналітичне право». – 2015 р. – № 5. – С.278-280.
2. Дезоксирибонуклеїнова кислота [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Дезоксирибонуклеїнова_кислота
3. Петряєв С. Ю. Щодо питання формування національної бази ДНК-даних в Україні / Петряєв С. Ю., Трофименко М. В. // Вісник НТУУ «КПІ». Політологія. Соціологія. Право : збірник наукових праць. – 2010. – № 3 (7). – С. 164–166.
4. Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС : наказ МВС України від 10.09.2009 р. № 390 [Електронний ресурс] – Режим доступу: ttp://zakon3.rada.gov.ua/laws/show/z0963-09

Інформаційне забезпечення виявлення злочинів, що вчиняються під час публічних закупівель у сфері охорони здоров'я

Доліновський Юрій Степанович,

аспірант кафедри кримінального права і процесу Навчально-наукового Інституту права та психології Національного університету «Львівська політехніка»

Для вжиття ефективних заходів з виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері

охорони здоров'я, оперативні підрозділи повинні мати змогу здійснювати систематичне збирання та аналіз інформації з усіх відповідних джерел, щоб використовувати оперативні дані і у стратегічних, і тактичних цілях. Отримання оперативних даних передбачає оброблення й аналіз значного обсягу інформації про осіб, які підозрюються у причетності до вчинення злочину. Методи, що застосовуються для отримання і використання такої інформації, регламентуються законодавством і відомчими нормативними актами.

Основною метою системи інформаційного з виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я є всебічна інформаційна підтримка практичної діяльності оперативних підрозділів на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів.

Інформаційне забезпечення – система пошуку й отримання відомостей про злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я, є процес нагромадження, опрацювання, аналіз даних отриманих при здійснені обслуговуванням установ та об'єктів галузі охорони здоров'я.

Одне з найбільш ґрунтовних визначень цього поняття дав Д.В. Гребельський, зазначивши, що це сукупність первинних і перевірених даних про осіб, які причетні до підготовки злочинів, стану оперативно-розшукових сил і засобів, а також умов, у яких здійснюється діяльність органів міліції щодо боротьби зі злочинністю [1, с. 17–23]. Це визначення доповнювали й уточнювали В.І. Лебеденко [2, с. 240–244], В.О. Лукашов [3] та інші вчені. Тому процес збирання інформації оперативними підрозділами під час оперативного пошуку залежить від особливостей оперативної обстановки, що формується на об'єктах охорони здоров'я, її оцінка та аналіз неможливі без вивчення особливостей функціонування їх господарювання. Вони складаються зі значної кількості відомостей, що мають важливе значення для діяльності оперативних підрозділів і ефективного виконання покладених

на ці підрозділи завдань. Проте ці відомості перебувають у різних інформаційних системах у хаотичному стані. Щоб вони перетворились на інформацію, котра здатна забезпечити потреби оперативних підрозділів, їх потрібно систематизувати, впорядкувати, тобто створити з них інформаційний потік, що спеціально призначений для оперативних служб.

Із застосуванням спеціальних технічних засобів і комп'ютерних технологій для отримання, обробки й аналізу оперативно-розшукової інформації, як зазначає А.С. Овчинський, формуються нові напрями, що спираються на можливості аналітичної та комп'ютерних баз даних, використання мультимедійних систем. Розробка і впровадження в оперативну практику автоматизованих інформаційно-пошукових систем органічно збіглися і стимулювали розвиток теоретичних уявлень про те, що оперативно-розшукова діяльність складається з двох фактично пов'язаних між собою частин: пізнавальної (пошук, збирання, аналіз та оцінка інформації, що становить оперативний інтерес) і діяльної (активної) (практична реалізація отриманої інформації) [4, с. 97].

І.М. Гриненко пропонує впровадити в Україні Британську модель інформаційно-аналітичної роботи, де співробітництво здійснюється через Європол. Ключовим елементом цієї моделі є поняття «аналітичної інформації» і означає інформацію, що пройшла відповідну аналітичну обробку та представлена у вигляді певного інформаційного продукту. Цей процес інформаційного аналізу, що охоплює інтеграцію та інтерпретацію даних від різних джерел, з метою визначення напрямів подальшої діяльності, часто має проактивний характер, спрямований на передбачення подальшого перебігу подій, фокусується на типах злочинної діяльності та категоріях правопорушників, виявлення потенційних жертв, визначає поточні цілі оперативно-розшукової діяльності та сприяє формуванню доказової бази під час розслідування кримінальних справ [5, с. 139].

Зростання ролі інформаційного аналізу безпосередньо пов'язано із упровадженням підходу «правоохоронної діяльності на ґрунті аналітичної інформації» (intelligence-led policing).

Ця ідея була сформована у Великобританії, поширилася в інших країнах Європейського Союзу та в США і полягає у використанні аналітичної роботи для постійного моніторингу змін оперативної обстановки з метою підвищення ефективності правоохоронної діяльності.

Такий підхід дозволяє ефективно планувати правоохоронну діяльність і відстежувати хід подій, координувати збір інформації відповідно до конкретних справ, формувати реалістичну картину діяльності об'єктів, виявляти зв'язки між подіями, робити обґрунтовані прогнози, формувати профіль злочинної поведінки, виявляти осіб, що займають ключові позиції у кримінальних мережах, і визначати їхню роль, відстежувати прибутки, отримані злочинним шляхом, ефективно спрямовувати обмежені ресурси правоохоронних органів, удосконалювати співробітництво з партнерськими структурами на національному та міжнародному рівнях.

З метою комплексного інформаційного забезпечення виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я необхідно використовувати інформаційні масиви Державної казначейської служби України про: установлення бюджетних асигнувань розпорядникам бюджетних коштів на основі та в межах затвердженого розпису бюджету; затвердження кошторисів, паспортів бюджетних програм (у разі застосування програмно-цільового методу в бюджетному процесі), а також порядку використання бюджетних коштів; взяття бюджетних зобов'язань; отримання товарів, робіт і послуг; здійснення платежів відповідно до взятих бюджетних зобов'язань; використання товарів, робіт і послуг тощо.

---

1. Гребельский Д.В. О состоянии криминалистических и оперативно-розыскных характеристик / Д.В. Гребельский // Криминалистическая характеристика преступлений: сб. науч. тр. – М.: Всесоюзный ин-т по изучению причин и разработке мер по предупреждению преступности, 1984. – С. 17-33.

2. Лебеденко В.І. Джерела, фіксація та аналітична обробка агентурної інформації / В.І. Лебеденко // Вісник Львівського ін-ту внутр. справ. – Львів: ЛІВС. – № 2 (16). – С. 240–244.
3. Лукашов В.А. Организация и методика аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел / В.А. Лукашов. – Омск: Омская высшая школа МВД СССР, 1983. – 32 с.
4. Овчинский А.С. Информация и оперативно-розыскная деятельность: монография / А.С. Овчинский. – М.: ИНФРА-М, 2002. – 390 с.
5. Гриненко І.М. Британська модель інформаційно-аналітичної роботи у сфері протидії організованій злочинності. МВС України у протидії економічним злочинам: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвідомчому семінарі-нараді / І.М. Гриненко; відп. ред. Л.П. Скалозуб, В.І. Василинчук, В.Д. Сапсай. – К., 2009. – С. 138–147.

Використання мікроконтролера ARDUINO

Іванців Віталій Ігорович,

здобувач ступеня бакалавра Національного лісотехнічного університету України

Шабатура Юрій Васильович,

професор кафедри інформаційних технологій Національного лісотехнічного університету України, доктор технічних наук, професор

У наш час існує безліч різноманітних контролерів та платформ для їх використання, основними компонентами яких є плата мікроконтролера з елементами вводу/виводу та середовище розробки Processing/Wiring на мові програмування. Мікроконтролер – мікросхема, призначена для управління електронними пристроями. Типовий мікроконтролер поєднує в одному кристалі функції процесора і периферійних пристроїв, містить ОЗУ і (або) ПЗУ. По суті, це однокристальний комп'ютер, здатний виконувати досить прості завдання.

Основні типи мікроконтролерів:

- вбудовані 8-розрядні мікроконтролери;
- 16- і 32-розрядні мікроконтролери;
- цифрові сигнальні процесори (DSP).

Arduino – торгова марка апаратно-програмних засобів для побудовиня простих систем автоматики і робототехніки, орієнтована на не фахових користувачів. Програмна частина складається з безкоштовної програмної оболонки для написання програм, їх компіляції і програмування апаратури. Апаратна частина являє собою набір змонтованих друкованих плат.

Мова програмування Arduino є стандартним C ++ з деякими особливостями, що полегшують новачкам написання першої працюючої програми.

Окрім того, що контролер Adruino буде просто використовувати навіть новачку, до нього існує безліч зовнішніх модулів, таких як:

- реле – застосовуються там, де потрібно контролювати електричне коло за допомогою сигналу з низьким енергоспоживанням з повною гальванічною розв'язкою;
- microsd card reader – для використання microsd карт;
- модуль годинника реального часу;
- матрична клавіатура – для взаємодії із користувачем;
- різноманітні джойстики;
- запрограмовані модулі для розпізнавання голосових команд;
- силові модулі;
- різноманітні сенсори та датчики;
- електромагнітні замки;
- вимикачі;
- та інші модулі.

Всі ці модулі можуть бути підключеними практично водночас та взаємодіяти через потужну платформу Arduino із використанням зовнішніх або власноруч написаних бібліотек.

Даний мікроконтролер можна використовувати обмежившись лише вбудованим середовищем Adruino, яке постійно оновлюється та підтримується компанією.

Інтегроване середовище розробки Arduino це багатоплатформовий додаток написаний на мові Java, що включає в себе редактор коду, компілятор і модуль передачі прошивки в плату. Середовище розробки спроектоване для програмування новачками, не знайомими близько з розробкою програмного забезпечення. Строго кажучи, це C++, доповнений деякими бібліотеками. Програми обробляються за допомогою препроцесора, а потім компілюється за допомогою AVR-GCC.

```
#define LED_PIN 13

void setup () {
  pinMode (LED_PIN, OUTPUT); // Включити контакт 13 для цифрового виводу
}

void loop () {
  digitalWrite (LED_PIN, HIGH); // Включити світлодіод
  delay (1000); // Зачекати одну секунду (1000 мілісекунд)
  digitalWrite (LED_PIN, LOW); // Вимкнути світлодіод
  delay (1000); // Зачекати одну секунду
}
```

Рис.1. Приклад програмного коду

Метою даної роботи є розроблення програмного забезпечення яке буде інстальоване у ОС Windows та дозволятиме застосування техніки управління ПК та зовнішніми пристроями за допомогою голосових команд.

Дана програма допомагає заощаджувати час користувачів, оскільки людині простіше продиктувати команду комп'ютеру, який у свою чергу обробить команду ти виконає певні дії за лічені секунди ніж виконувати ці дії вручну.

Для реалізації системи одного середовища Arduino буде недостатньо, оскільки для реалізації такої системи потрібно створити користувацький інтерфейс, який буде максимально зручним та зрозумілим для кінцевого користувача, тому було прийнято рішення використовувати середовище програмування Visual Studio.

Для використання контролера Adruino необхідно виконати наступні кроки:

- встановити необхідні драйвери для плати Arduino та підключити плату через USB порт;
- запрограмувати мікроконтролер (за допомогою середовища Arduino);
- у середовищі програмування Visual Studio підключити необхідні бібліотеки для використання COM портів ПК.

Після виконання вищезгаданих кроків потрібно лише «комунікувати» із контролером за допомогою послання та прийому сигналів із вказаного COM потру до якого він підключений.

Подальша розробка системи передбачала реалізацію розпізнавання команд за допомогою систем для обробки голосу.

Для обробки голосу користувача було використано технологію Google Speech API. Ця технологія дозволяє швидко розпізнавати текст у потоці аудіо даних. До переваг технології розпізнавання голосу від компанії Google можна віднести використання рекурентних нейронних мереж, які постійно самонавчаються та покращують точність розпізнавання відповідно, підтримку більш ніж 110 мов, що дозволяє використовувати технологію у багатьох кранах світу та відсутність труднощів у використанні.

В результаті ми отримали систему яка здатна «комунікувати» із зовнішніми пристроями за допомогою апаратно-програмних засобів описаних вище. Така система є легко розширювальною і обмежується по суті лише фантазією розробника.

1. Ендрю Троелсен. Язык программирования C# 2010 и платформа .NET 4. –Изд.: «Вильямс». – 1310 с. – Изд.: «Вильямс». – 2010 – ISBN 0-201-70857-4.
2. Документація Arduino [Веб ресурс] – https://www.arduino.cc/en/Main/Docs
3. Документація Google Speech API [Веб ресурс] – https://cloud.google.com/speech/docs/
4. Документація Visual Studio – https://www.microsoft.com/ru-ru/SoftMicrosoft/vs2017

Тренди кібербезпеки

Кавун Сергій Віталійович,

завідувач кафедри інформаційних технологій ХННІ ДВНЗ «Університет банківської справи», доктор економічних наук, кандидат технічних наук, Ph.D., професор

Ломакіна Вікторія Віталіївна,

здобувач ступеня бакалавра ХННІ ДВНЗ «Університет банківської справи»

Кібербезпека представляє собою набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до керуванню ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберпростору, ресурсів організацій і користувачів. Кібербезпека має на увазі досягнення і збереження властивостей безпеки і ресурсів організації або користувачів, спрямованих проти відповідних кіберзагроз.

Основними задачами забезпечення безпеки вважаються: доступність, цілісність, що включає автентичність, а також конфіденційність. Кібербезпека є необхідною умовою розвитку інформаційного суспільства.

Питання кібербезпеки стають з кожним роком все більш гострими, тому що все більшу кількість гаджетів люди починають використовувати у своєму житті постійно і вже не можуть без них обходитися [1].

Інтернет речей, скорочено IoT міцно увійшов в наше життя. Сьогодні близько 13 різних пристроїв у середньому є в кожному будинку. Крім звичних комп'ютерів, ноутбуків і смартфонів, це різні IoT-девайси: роутери, IP-камери, цифрові відеореєстратори, DVR-системи.

Всі вони можуть бути заражені і використовуватися для здійснення DDoS-атак. Уразливості девайсів пов'язані в першу чергу з браком кваліфікованих фахівців. На нашу думку, саме ЛЮДСЬКИЙ ФАКТОР вельми серйозно впливає на кібербезпеку і вразливість гаджетів [2].

1. Захист IoT від хакерських атак

Основна проблема порушення кібербезпеки виникає через захоплення IoT-девайсів різними ботнетами і використанні їх для організації DDoS-атак. IoT-пристрої є для хакерів істинної золотою жилою.

СТАТИСТИКА:

- У 2017 р. у всьому світі буде близько 28,4 мільярдів IoT-пристроїв, підключених до інтернету. Це на 5,5 мільярда більше, ніж в 2016 р.
- До 2020 р. ці показники зростуть приблизно до 50 мільярдів.
- Вже більше 1 мільйона пристроїв, підключених до інтернету, є чиїмись ботами.
- Наприклад, 96% ботів Gafgyt – це різні IoT-гаджети.
- Найбільш уразливі IoT-девайси, які працюють на базі x86, MIPS і ARM.
- Протягом 2016 р. хакери використовували невеликі IoT-пристрої для відключення дуже великих доменів і провайдерів, таких як Spotify і Twitter.
- Самим шкідливим ПЗ в 2016 р. стали Mirai і Bashlight, вони разом здійснили захоплення понад 1 мільйон IoT-девайсів для зараження ботами.

2. Компанії активізують свою роботу по запобіганню атак

Ще одним важливим трендом кібербезпеки є активізація дій компаній, спрямована на запобігання атак. Для цього вже зараз багато хто проводить всебічну оцінку всіх слабких місць корпоративної мережі. Особливу увагу слід звертати не тільки на IT-девайси, але і на людський фактор та підвищення кваліфікації фахівців.

В першу чергу, необхідно обмежити кількість пристроїв, якими співробітники компанії можуть користуватися в робочий час. Так як забезпечити кібербезпеку мобільних гаджетів набагато важче, ніж стаціонарних.

На робочому місці для забезпечення безпеки даних вже недостатньо використання логіна і пароля співробітника. Прогнозується всебічне застосування двофазної авторизації.

3. Посилення безпеки веб-сайтів і додатків

У 2017 році набагато більшу увагу приділяли безпеці веб-сайтів і мобільних додатків. Вибір розробника веб-ресурсу повинен ґрунтуватися на гарантії того, що розробник буде використовувати сучасні технології та методу захисту інформації [3].

Компаніям слід відповідальне ставитися до забезпечення безпеки власного веб-ресурсу. Для цього фахівець або компанія, яка здійснює підтримку, повинні регулярно проводити такі заходи як:

- оновлення CMS (програмної частини) веб-сайту;
- здійснювати зміну облікових даних не тільки в адмін-панелі сайту, але і до бази даних MySQL, панелі FTP / Plesk;
- використовувати сучасні протоколи передачі даних HTTPS / HSTS.

4. Захист від інформаційних атак через соціальні мережі і фальшиві новини

Можливо, зараз люди не замислюються як багато недостовірної інформації атакує нас в повсякденному житті. У 2017 році фільтрація фальшивих новин і захист від спаму була важливим трендом кібербезпеки.

Незважаючи на те, що фальшиві новини в буквальному сенсі не вірно назвати кібератакою, проте вони надають дуже негативний вплив і змивають кордон між правдою і брехнею, що знижує довіру.

Недостовірні новини бувають різних форм: це і новинні стрічки з інтригуючими заголовками, і перекрученими новинами, і відео ролики, і псевдо-звіти з помилковою статистикою.

Отже, вважаємо, що кібербезпеку неможливо купити - її можна тільки побудувати.

---

1. Lomakina V.V. Problems of cybersecurity of Ukraine. Newly made strategy of cybersecurity of Ukraine / V. V. Lomakina // XXXXI

International Scientific Conference «CURRENT ISSUES IN SCIENCE»: Materials XXXXI International Scientific Conference, Chernivtsi, May 30-31, 2016. – Режим доступу: https://drive.google.com/open?id=0B8Ty4PhaAv0JYWtLMFRmYzRqczE3VUVtTVBrYjdpTWhQbVgw.
2. Деловой информационно – новостной сайт «ДЕЛО»: ежедневные новости политики, экономики, безнеса, технологий и событий в Украине и мире // «10 важных тезисов для кибербезопасности» – Режим доступу: https://delo.ua/tech/10-vazhnyh-tezisov-dlja-kiberbezopasnosti-329632/ © delo.ua.
3. Сайт веб-студії «АВАНЗЕТ» // «Хакерские атаки – угроза безопасности для веб-сайта» – Режим доступу: https://a1z.ru/sistemy-upravleniya-sajtom/489-khakerskie-ataki-ugroza-bezopasnosti-dlya-veb-sajta.html.

Розробка пристрою екстреної допомоги співробітнику МВС

Кавун Сергій Віталійович,

завідувач кафедри інформаційних технологій ХННІ ДВНЗ «Університет банківської справи», доктор економічних наук, кандидат технічних наук, Ph.D., професор

Шмаков Вадим Володимирович,

здобувач ступеня бакалавра ХННІ ДВНЗ «Університет банківської справи»

Постановка проблеми. В наш час питання безпеки і відстеження здоров'я є одним з пріоритетних, а безпека поліцейських особливо. Адже ніхто не знає які небезпеки чекають вартових закону за тим чи іншим кутом. З цього дана розробка допоможе відстежувати стан поліцейського і в разі необхідності викликати їм допомогу.

Аналоги

Зчитування інформації з допомогою датчиків телефону. Датчики, вбудовані в телефон, дозволяють автоматично зчитувати окремі види інформації про стан здоров'я, коли вони пов'язані з відповідними додатками.

Зчитування інформації про здоров'я за допомогою окремих датчиків. Як відомо, смартфон дозволяє підключитися до окремих датчиків. Ось кілька пристроїв, які можна підключити до телефону, щоб відстежувати інформацію про здоров'я:

- Датчики фізичної активності: наприклад, Fitbit, Jawbone.
- Монітори артеріального тиску.
- Глюкометри.
- Пульсоксіметри для вимірювання частоти серцевих скорочень і насичення крові киснем.

Вибір датчиків

Arduino Nano. Платформа Arduino Nano, побудована на мікроконтролері ATmega328 (Arduino Nano 3.0) або ATmega168 (Arduino Nano 2.x), має невеликі розміри [1].

Живлення. Зовнішній USB-TTL перетворювач дозволяє живити Arduino, незалежно від поточного положення перемикача живлення на платі. Під час автономної роботи, пристрій може живитися від акумулятора, або від зовнішнього джерела живлення.

GPS-МОДУЛЬ VK16E

Arduino GPRS/GSM Shield надає вам можливість використовувати мережу мобільного GSM зв'язку для віддаленого прийому і передачі даних для Arduino-проектів. Цього можна досягти за допомогою одного з трьох способів: 1) SMS; 2) Аудіо; 3) GPRS [2].

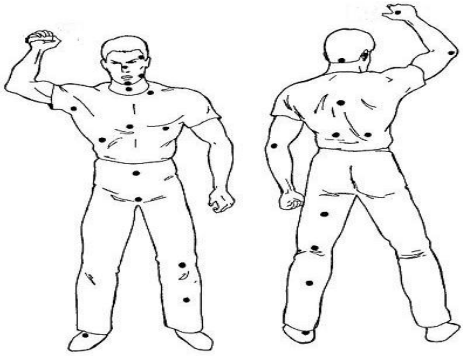


Рис.1. Можливі ділянки установки датчиків на патрульного

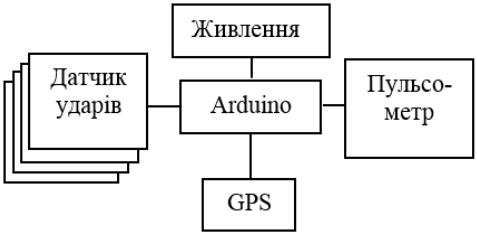


Рис. 2. Концептуальна схема пристрою

WEB-інтерфейс. Web-інтерфейс – відображення на Яндекс.Картах поточного (останнього переданого) положення або маршруту за обраний період.

При побудові маршруту по мітках будується полігон, для кожної мітки відображається час. Для швидкої побудови сторінки передбачена константа максимальної кількості міток.

Канал передачі даних

Дальність дії сигналу Wi-Fi мережі найбільш залежить від типу точки доступу або бездротового роутера.

Радіус дії зі стандартною антеною з посиленням 2 dBi у поширених роутерів стандарту 802.11g, за умови, що вони підключені до комп'ютера або ноутбука з антеною з таким же посиленням, можна оцінити близько 150 м на відкритій місцевості і 50 м в приміщенні [3].

МОДУЛЬ SD КАРТИ ARDUINO

Якщо у проекті необхідно забезпечити завантаження аудіо, відео, графіки, записи будь-яких даних, виникає питання зовнішньої пам'яті. У більшості мікроконтролерів вбудована пам'ять дуже обмежена. При завантаженні графічних або музичних файлів напевно знадобиться мінімум 1 мегабайт сховища. Карти пам'яті часто називають SD або microSD картами і вони дозволяють зберігати гігабайти інформації. [4]

Переваги. Перевагами даного приладу є: автономність роботи, автоматичний режим роботи, можливість відстежувати стану здоров'я і місця розташування патрульного в реальному часі.

1. Arduino Nano [Електронний ресурс]. – Режим доступу до ресурсу: http://arduino.ru/Hardware/ArduinoBoardNano.
2. GPS модуль VK16E [Електронний ресурс]. – Режим доступу до ресурсу: https://litl-admin.ru/zhelezo/podklyuchaem-gps-modul-vk16e-k-arduino.html.
3. Радиус действия Wi-Fi сети [Електронний ресурс]. – Режим доступу до ресурсу: http://routers.in.ua/radius-dejstviya-wi-fi-seti/.
4. Модуль SD карты и Arduino [Електронний ресурс] – Режим доступу до ресурсу: http://arduino-diy.com/arduino-SD-karta.

Деякі особливості використання відеокамер у діяльності правоохоронних спецпідрозділів

Кириченко Катерина Василівна,

здобувач ступеня бакалавра факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

Рвачов Олексій Михайлович,

старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

Під час проведення оперативно-розшукових заходів, слідчих (розшукових) та негласних слідчих (розшукових) дій, а також заходів забезпечення кримінального провадження, припинення правопорушень, що вчиняються учасниками злочинних угруповань, звільнення заручників, проведення антитерористичних операцій, нерідко залучаються працівники правоохоронних спецпідрозділів, які здійснюють силову підтримку з метою забезпечення переважаючої вогневої потужності над правопорушниками.

На теперішній час до правоохоронних спецпідрозділів України можна віднести:

- підрозділи особливого призначення Національній поліції України (наприклад, Департаменту КОРД (Корпус Оперативно-Раптової Дії), патрульної служби поліції особливого

призначення ГУНП), а також підрозділи Департаменту внутрішньої безпеки;
- окремі загони та батальйони спеціального призначення Національній гвардії України (наприклад, «Азов», батальйон ім. Кульчицького, «Ягуар», «Омега»);
- підрозділи Державної прикордонної служби України – окремий загін оперативного реагування «ДОЗОР»;
- підрозділи боротьби з тероризмом і захисту учасників кримінального судочинства та працівників правоохоронних органів Служби безпеки України – «Альфа»;
- підрозділи Національного антикорупційного бюро України – Управління спеціальних операцій.

При виконанні покладених на них завдань, працівники правоохоронних спецпідрозділів можуть використовувати спеціальні відеокамери з метою фіксації:

- дії правоохоронців під час проведення спецоперацій та участі у певних слідчих діях (наприклад, під час проведення обшуку) або під час припинення правопорушень (наприклад, звільнення заручників);
- процедури проведення поверхневого огляду громадян;
- фактів правомірного застосування правоохоронцями фізичної сили, спеціальних засобів та вогнепальної зброї до громадян;
- тощо.

Отриманні відеоматеріали можуть використовуватися для:

- висвітлення в засобах масової інформації звітів про роботу правоохоронних органів;
- аналізу можливих помилок під час проведення тактико-спеціальних навчань;
- об'єктивного розслідування дій або бездіяльності правоохоронців з метою встановлення справедливості;
- захисту працівників від неправдивих обвинувачень з боку громадян; тощо.

Для вирішення зазначених вище завдань можуть використовуватися спеціальні відеокамери різних видів:

- нагрудні відеокамери;
- відеокамери, що кріпляться на головному уборі працівника (по центру, збоку або наверху каски чи шолому) – екшен-відеокамери;
- відеокамери на вогнепальній зброї;
- бездротові тактичні панорамні відеокамери;
- відеокамери на квадрокоптерах.

Також працівники можуть використовувати:

- побутові відеокамери, бажано із ремінцем для тримання в руці;
- відеокамери мобільних телефонів.

Кожен із зазначених вище видів відеокамер може мати певні недоліки та переваги під час їхнього використання.

Недоліком використання нагрудних відеокамер під час проведення спеціальних операцій є те, що в ході проведення таких операцій правоохоронець тримає на рівні грудей свою табельну вогнепальну зброю і, таким чином, перекриває кут огляду відеокамери через що відеокамера не зможе зафіксувати важливу інформацію.

Під час використання мобільних телефонів у якості відеокамери нерідко здійснюється вертикальна відеозйомка, тому що тримання мобільного телефону у горизонтальному положенні під час спецоперацій може призвести до того, що мобільний телефон може випадково випасти із рук оператора.

Під час проведення спецоперацій руки у працівник повинні бути вільними, тому використання відеокамер, які необхідно тримати під час зйомки в руках, є недоцільним.

Відеокамери, що використовуються працівниками правоохоронних спецпідрозділів повинні мати такі характеристики, як:

- водонепроникність;
- ударостійкість;
- автоматичний перехід в режим «нічної зйомки» в залежності від рівня освітленості навколишнього середовища.

Найбільш доцільним є використання працівниками правоохоронних спецпідрозділів відеокамер, що кріпляться на головному уборі працівника. Використання такого виду відеокамер дозволяє фіксувати ті події та обстановку, яку безпосередньо бачив працівник під час участь у спецоперації, та на підставі якої він приймав ті або інші рішення, у тому числі по відношенню до громадян. Наприклад, це дозволяє перевірити правомочність застосування правоохоронцем фізичної сили, спеціальних засобів та вогнепальної зброї до громадян.

Програмне та алгоритмічне забезпечення інформаційної системи розпізнавання зображень нейронними мережами

Ковалик Павло Андрійович,

здобувач ступеня магістра Національного лісотехнічного університету України

Оптичне розпізнавання тексту дозволяє редагувати текст, здійснювати пошук слова або фрази, зберігати його в компактнішій формі, демонструвати або роздруковувати матеріал, не втрачаючи якості, аналізувати інформацію, а також застосовувати до тексту електронний переклад, форматування або перетворення в мовлення. Оптичне розпізнавання тексту є досліджуваною проблемою в галузях розпізнавання образів, штучного інтелекту і комп'ютерного зору.

Метою даної роботи стало розроблення програмного забезпечення для розпізнавання тексту, а саме для перетворення зображення в текст.

Точне розпізнавання латинських символів у друкованому тексті зараз можливе тільки, якщо доступні чіткі зображення, такі як друковані документи. Точність при такій постановці задачі перевищує 99%, абсолютна точність може бути досягнута тільки шляхом наступного редагування людиною. Проблеми розпізнавання рукописного «друкованого» тексту й стандартного рукописного тексту, а також друкованих текстів

інших форматів (особливо з дуже великою кількістю символів) зараз є предметом активних досліджень. [1].

Для розпізнавання символів використано Tesseract OCR Engine.

Tesseract Engine – добре відома відкрита версія OCR двигун, що випускається під ліцензією Apache 2.0. використовуючи це для побудови бібліотеки OCR для Android,і для реалізації програми Android OCR перетворючи зображення машинно-друкованих форм. Tesseract Android Tools: надає набір API для Android та створення файлів для Tesseract OCR та Android SDK. [2].

Вбудований OCR перетворює текст, вбудований в знімок, у текстовий формат Unicode. Крім того, платформа Android все частіше стає звичайною у відповідності зі своїми функціями, такими як низька вартість, доступна операційна система. Коли ми робимо знімок з будь-якого зображення чи будь-якого документа за допомогою камери, ця програма витягує числові значення, подібно до номера телефону, і зберігає його на сервері бекендального сервера.Результат розпізнавання показаний наступним чином. Рис. 3: – показує оригінальний документ з українською мовою. Після захоплення камерою смартфону дані обробляються шляхом binarization для сегментації об'єктів. Потім ми можемо побачити результати розпізнавання на екрані смартфону Рис. 4. [3].

Рис.1. Головне вікно застосунку

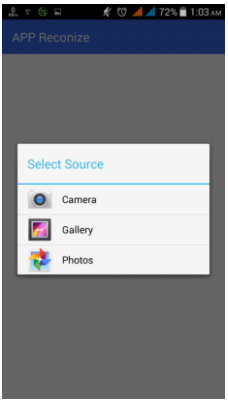


Рис.2. Вибір для завантаження зображення

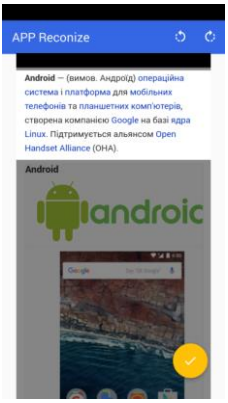


Рис.3. Вибір області розпізнавання

Для розроблення графічного інтерфейсу програми використано середовище AndroidStudio. На рисунку 1 показано головне вікно програми.

Як бачимо, інтерфейс застосунку дозволяє обирати дії для завантаження зображення для обробки (Рис.2). Наступним кроком є вибір області для розпізнавання зображення (Рис.3).

Останнім кроком роботи застосунку є вибір мови тексту який розпізнається (Рис.4).

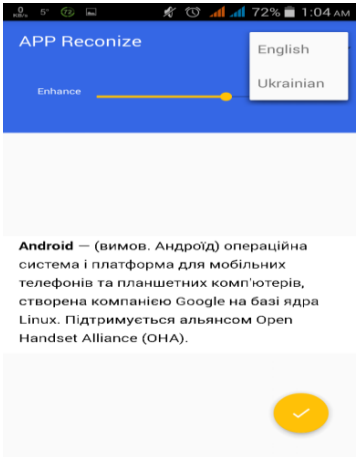


Рис.4. Вибір мови

Отже, в ході роботи було виконано аналіз предметної області, вибраних технологій та засобів проектування. Результатом є застосунок розпізнання зображень.

Результати роботи програми виводяться у графічне поле. Користувач має змогу переглянути результати роботи застосунку, а також змінити яскравість тексту. Застосунок розроблений мовою програмування JAVA середовищі Android Studio.

---

1. Оптичне розпізнавання символів [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Оптичне_розпізнавання_сиволів

2. J.L. Blue, G.T. Candela, P.J. Grother, R. Chellappa, C.L. Wilson, Evaluation of pattern classifiers for fingerprint and OCR applications, Pattern Recognition, 27(4), 1994, 485–501.
3. R. Smith, An overview of the Tesseract OCR engine, Proc. Int. Conf. Document Analysis and Recognition (ICDAR 2007), 2007, 629-633.

Реалізація права на доступ до інформації за інформаційним запитом

Ковалів Мирослав Володимирович,

завідувач кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

Хіміч Анна Миргасанівна,

здобувач ступеня магістра Львівського державного університету внутрішніх справ

Законодавство України передбачає право на доступ до інформації за інформаційним запитом.

Відповідно до ст. 19. Закону України «Про доступ до публічної інформації» [1] запит на інформацію – це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні. Запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

Запит на інформацію може бути індивідуальним або колективним. Запити можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

Письмовий запит подається в довільній формі та має містити наступні відомості:

- ім’я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв’язку, якщо такий є;

- загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;
- підпис і дату за умови подання запиту в письмовій формі.

З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

У разі якщо з поважних причин (інвалідність, обмежені фізичні можливості тощо) особа не може подати письмовий запит, його має оформити відповідальна особа з питань запитів на інформацію, обов'язково зазначивши в запиті своє ім'я, контактний телефон, та надати копію запиту особі, яка його подала.

Розпорядник інформації має надати відповідь на запит на інформацію не пізніше п'яти робочих днів з дня отримання запиту. Якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана не пізніше 48 годин з дня отримання запиту.

Клопотання про термінове опрацювання запиту має бути обґрунтованим.

У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може продовжити строк розгляду запиту до 20 робочих днів з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі не пізніше п'яти робочих днів з дня отримання запиту. Інформація на запит надається безкоштовно.

Якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом більш як 10 сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк. Розмір фактичних витрат визначається відповідним розпорядником на копіювання та друк в межах граничних норм, встановлених Кабінетом Міністрів України. Коли розпорядник інформації не встановив розміру плати за копіювання або друк, інформація надається безкоштовно. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується.

Розпорядник інформації має право відмовити в задоволенні запиту в таких випадках:

- розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;
- інформація, що запитується, належить до категорії інформації з обмеженим доступом;
- особа, яка подала запит на інформацію, не оплатила передбачені фактичні витрати, пов'язані з копіюванням або друком;
- не дотримано вимог до запиту на інформацію, передбачених Законом.

Відповідь розпорядника інформації про те, що інформація може бути одержана запитувачем із загальнодоступних джерел, або відповідь не по суті запиту вважається неправомірною відмовою в наданні інформації.

Розпорядник інформації, який не володіє запитуваною інформацією, але якому за статусом або характером діяльності відомо або має бути відомо, хто нею володіє, зобов'язаний направити цей запит належному розпоряднику з одночасним повідомленням про це запитувача. У такому разі відлік строку розгляду запиту на інформацію починається з дня отримання запиту належним розпорядником.

У відмові в задоволенні запиту на інформацію має бути зазначено:

- прізвище, ім’я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;
- дату відмови;
- мотивовану підставу відмови;
- порядок оскарження відмови;
- підпис.

Відмова в задоволенні запиту на інформацію надається в письмовій формі.

Відстрочка в задоволенні запиту на інформацію допускається в разі, якщо запитувана інформація не може бути надана для ознайомлення в передбачені Законом строки у разі настання обставин непереборної сили. Рішення про відстрочку доводиться до відома запитувача у письмовій формі з роз’ясненням порядку оскарження прийнятого рішення.

У рішенні про відстрочку в задоволенні запиту на інформацію має бути зазначено:

- прізвище, ім’я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;
- дату надсилання або вручення повідомлення про відстрочку;
- причини, у зв’язку з якими запит на інформацію не може бути задоволений у встановлений цим Законом строк;
- строк, у який буде задоволено запит;
- підпис.

Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені до керівника розпорядника, вищого органу або суду.

Запитувач має право оскаржити:

- відмову в задоволенні запиту на інформацію;
- відстрочку задоволення запиту на інформацію;
- ненадання відповіді на запит на інформацію;
- надання недостовірної або неповної інформації;

- несвоєчасне надання інформації;
- невиконання розпорядниками обов'язку оприлюднювати інформацію
- інші рішення, дії чи бездіяльність розпорядників інформації, що порушили законні права та інтереси запитувача.

Оскарження рішень, дій чи бездіяльності розпорядників інформації до суду здійснюється відповідно до Кодексу адміністративного судочинства України.

Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

- ненадання відповіді на запит;
- ненадання інформації на запит;
- безпідставна відмова у задоволенні запиту на інформацію;
- не оприлюднення інформації відповідно до статті 15 Закону України «Про доступ до публічної інформації»;
- надання або оприлюднення недостовірної, неточної або неповної інформації;
- несвоєчасне надання інформації;
- необґрунтоване віднесення інформації до інформації з обмеженим доступом;
- нездійснення реєстрації документів;
- навмисне приховування або знищення інформації чи документів.

Особи, на думку яких їхні права та законні інтереси порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди в порядку, визначеному Законом.

---

1. Про доступ до публічної інформації : Закон України від 13.01.2011 // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

Інформаційні технології в забезпеченні безпеки бізнесу

Комісарчук Юлія Анатоліївна,

доцент кафедри кримінального процесу факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Багин Сергій Сергійович,

здобувач ступеня бакалавра факультету № 1 ІПФПНП Львівського державного університету внутрішніх справ

У процесі своєї діяльності будь-яка компанія оперує інформацією як специфічним товаром значної вартості. Володіння достовірною і своєчасною інформацією, а також її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу. Тому проблема забезпечення інформаційної безпеки (ІБ) будь-якої компанії є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій (ІТ), яка супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми [1].

Результатом забезпечення економічної безпеки підприємства є стабільність його функціонування, ефективність фінансово-економічної діяльності, особиста безпека персоналу. Безпека підприємства включає в себе чотири основних напрямки: інформаційне забезпечення комерційної діяльності підприємства в ринкових умовах; захист інтелектуальної власності (в тому числі комерційної таємниці); захист матеріальних і фінансових цінностей; захист персоналу [2, с.90]. За оцінками експертів, витрати на створення системи безпеки підприємства і його оптимальне функціонування можуть досягати 25% витрат на весь процес виробництва. В свою чергу з розвитком комп'ютерної техніки та використанням комп'ютерних мереж постає проблема захисту джерел інформації. Сфери застосування електронного бізнесу різноманітні: електронна торгівля, банківські операції, страхові операції, купівля-продаж різних продуктів, операції на фондовій біржі, IP-телефонія тощо. Банки пропонують послуги

управління рахунком і платежі в режимі реального часу. Інтернет став простим і зручним засобом зв'язку між підприємцями (business-to-business, B2B), між підприємцями і споживачами (business-to-consumer, B2C), між споживачами (consumer -to-consumer, C2C) та реалізації інших видів електронної комерції [3]. Будь-яке несанкціоноване вторгнення може призвести до втрати важливої інформації, її секретності, і як наслідок – використання цієї інформації в будь-яких корисливих цілях. Як вважають експерти, витік 20% комерційної інформації в шістдесяти випадках зі ста призводить до банкрутства підприємства [4].

Аналізуючи інформацію про забезпечення інформаційної безпеки підприємства спостерігаємо негативну практику керівників, які, в основному, проводять лише реактивні дії на ті, чи інші інциденти ІБ. Крім того, різні підрозділи, які в рамках однієї компанії займаються питаннями оцінювання загроз та управління ІБ, діють найчастіше роз'єднано й фрагментарно покривають тільки явно видимі проблеми. Внаслідок цього інформаційні процеси ніби і контролюються, але далеко не всі, які варто було б відстежувати. Виходить як за Райкіним – ґудзики пришиті відмінно, кишені на місці, але костюм при цьому «якийсь не такий», до прикладу розвинуті країни світу витрачають близько 9-12 % свого прибутку на забезпечення безпеки власного бізнесу.

Основними видами шахрайських дій зловмисників є: придбання товарів і послуг за реквізитами вкрадених пластикових кредитних карток; злам баз даних, що містять інформацію з пластикових карт (відомості про власників пластикових карт, які здійснюють покупки в електронних магазинах); організація шахрайських електронних магазинів [1, с.92]. Виділяють декілька складових елементів захисту електронного бізнесу: – інженерно-технічний захист інформації призначений для пасивної і активної протидії за допомогою комплексів технічних засобів; – програмно-математичний захист інформації призначений для захисту цінної інформації, що обробляється і зберігається в комп'ютерах, локальних мережах і різних інформаційних системах; – організаційний захист інформації містить заходи, що спонукають персонал дотримуватися правил захисту цінної інформації

підприємства. Ці заходи складають 50-60% у структурі більшості систем захисту інформації. Це пов'язано з низкою факторів, а також з тим, що важливою стороною організаційного захисту інформації є підбір, розстановка і навчання персоналу, який буде здійснювати на практиці принципи і методи захисту [4].

Стурбованість бізнесу викликає й інша глобальна сфера – це інциденти у кіберпросторі, що включають кіберзлочини або несанкціоновані втручання в бази даних, а також технічні збої в інформаційно-комунікативних системах. Так на початку 2017 року експертами редакції Форіншурер було проведено дослідження з метою визначення «барометру ризиків підприємств Європи на 2017 рік, за дані дослідження наведені в таблиці (табл. 1). Варто зауважити, що п'ять років тому у першому дослідженні тільки 1% респондентів розглядав кіберінциденти як ризик.

«Компанії по всьому світу готуються до періоду невизначеності. Зміни в законодавчій, геополітичній та ринковій сферах по всьому світу – предмет для постійної уваги ризик-менеджерів та керівників компаній. Розвивається актуальність нових ризиків, які виходять за рамки, що стали «прибутковими» пожежами та природними катаклізмами, і це вимагає не тільки особливого уваги з боку компаній, але і переосмислення підходів до моніторингу потенційних загроз, а також інструментів ризик-менеджменту» – говорить генеральний директор AGCS Крис Фішер Хирс.

Таблиця 1

1	Перерва у виробництві (включаючи збої у постачанні)	37%
2	Ринкові зміни	31%
3	Кіберінциденти (кібер злочини, витік даних, збої IT)	30%
4	Стихійні лиха	24%
5	Зміни в законодавстві (економічні санкції)	24%
6	Макроекономічні зміни (програма жорстокої економії, зріст цін на товари, інфляція/дефляція)	22%
7	Пожежа, вибух	16%
8	Політичні ризики (війна, тероризм, безпорядки)	14%
9	Втрата репутації і вартості бренда	13%
10	Нові технології (нанотехнології, 3Д-друк, штучний інтелект, дрони)	12%

*Рейтинг складений експертами Редакції Форіншурер http://www.fin.org.ua/news/1228676

Зміст складових елементів захисту, методи і засоби захисту змушені регулярно змінюватись з метою ефективнішого запобігання їх розкриттю, у зв'язку з цим на підприємствах все частіше впроваджуються наступні механізми безпеки: шифрування, електронний цифровий підпис, контроль доступу, забезпечення цілісності даних, забезпечення аутентифікації.

Забезпечення аутентифікації передбачає проведення процедури перевірки автентичності іншої сторони: перевірка справжності користувача шляхом порівняння введеного їм пароля з паролем, збереженим в базі даних користувачів; підтвердження справжності електронного листа шляхом перевірки цифрового підпису листа з відкритим ключем відправника тощо. Основними характеристиками кожного заходу є вартість захисту та економічний ефект використання [3].

Сучасна корпоративна система інформаційної безпеки покликана забезпечувати захист конфіденційної інформації від несанкціонованого доступу, запобігати зловмисним або випадковим змінам (контролювати цілісність) і давати необхідний рівень доступу. Забезпечення інформаційної безпеки зводиться до трьох основних напрямів – це комбінація технічних, адміністративних і організаційних заходів. Таким чином, у сучасних умовах господарювання, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємним складником системи економічної безпеки господарюючого суб'єкта й економічної безпеки держави загалом. Головне в організації бізнесу – не тільки грамотно використовувати наявну інформацію, але і забезпечити її якісний захист всіма доступними засобами.

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http:// nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf
2. Дробышева, В.Г. Роль и место информационных технологий в системе экономической безопасности государства [Текст] /

В.Г. Дробышева, А.П. Черноиванов // Социально-экономические явления и процессы. – 2011. – №3-4. – С. 87-93.
3. Козивкин, В. В. Экономическая безопасность промышленного предприятия [Електронний ресурс] / В.В. Козивкин. – Режим доступу \www/ URL: http://secandsafe.ru/pravovaya_baza/blogi/ekonomicheskaya_bezopasnost/ekonomicheskaya_bezopasnost_promyshlennogo_predpriyatiya. – Заголовок з екрана, доступ вільний, 08.10.2016
4. Павлов, А. П. Информационные технологии экономической безопасности бизнеса [Електронний ресурс] / А.П. Павлов, А. В. Колосов // Мир науки. Научный Интернет журнал. – 2013. – Вып. 1. – Режим доступу \www/ URL: http://mir-nauki.com/PDF/02EMN113.pdf. – Заголовок з екрана, доступ вільний, 08.10.2016.
5. 10 Глобальных бизнес-рисков предприятий в 2017 году. Allianz представил новый «Барометр рисков» [Електронний ресурс] – Режим доступу http://www.fin.org.ua/news/1228676

Автоматичне проектування та моделювання теплового двигуна із зовнішнім підводом тепла засобами SOLIDWORKS API, SOLIDWORKS SIMULATION

Курносов Максим Вікторович,

здобувач ступеня магістра Національного лісотехнічного університету України

Крошний Ігор Михайлович,

доцент кафедри інформаційних технологій Національного лісотехнічного університету України, кандидат технічних наук

Дана робота присвячена автоматизованому проектуванню та дослідженню моделі двигуна зовнішнього згорання. Вона є актуальною, оскільки двигун може працювати на любому виді палива, включно з використанням сонячного тепла. За досліджувану модель було взято двигун Стирлінга гамма типу, оскільки це одна з найбільш популярних моделей. Ці двигуни більше підходять для статичної роботи. Тобто в якості насосу, або генератора електроенергії.

Двигун складається з двох циліндрів, які є з'єднані між собою через отвори в корпусі. В циліндрі який ми нагріваємо, знаходиться пустотілий поршень який не щільно прилягає до корпусу циліндра і переганяє тепле повітря в інший його кінець, який є менш нагрітий і через канал в корпусі до другого циліндра, в якому поршень має мінімальний зазор. За основним законом термодинаміки, повітря або інший газ, який знаходиться в циліндрах та каналі між ними при переході з гарячої частини до холодної, створює зону підвищеного тиску яка і виштовхує поршень. Поршні передають роботу на колінчастий вал, який обертає маховик. Готова збірка двигуна спроектованого в SolidWorks виглядає наступним чином.

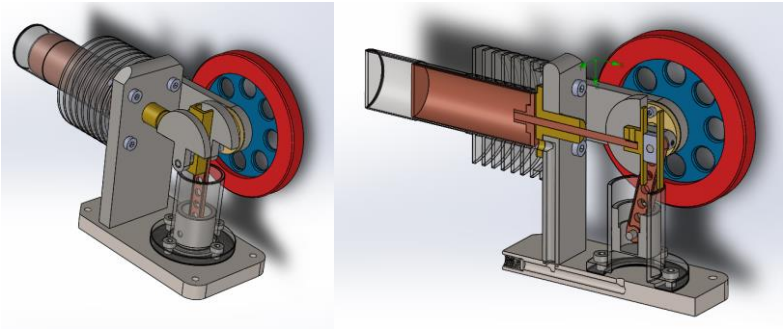


Рис.1. Вигляд моделі двигуна (повний та в розрізі).

Розроблений мною додаток може будувати будь-яку деталь з заданими користувачем розмірами та матеріалами в середовищі SolidWorks, та збирати деталі в збірку над якою можна виконувати досліди. Наприклад переглядати як поведе себе той чи інший матеріал, при заданих обертах маховика, чи подивитися як буде розподілятися тиск в циліндрах.

На Рис. 2 подану основну форму програми. Для побудови звичайної деталі, користувачу необхідно вибрати деталь зі списку та натиснути кнопку «Побудувати деталь». Для побудови нестандартної деталі необхідно вибрати необхідний розмір, ввести його значення та натиснути кнопку «Перебудувати деталь». Для зміни матеріалу, достатньо вибрати матеріал зі списку та натиснути кнопку «Змінити матеріал».

Також можна переглянути центр мас або побудувати збірку зі всіх деталей.

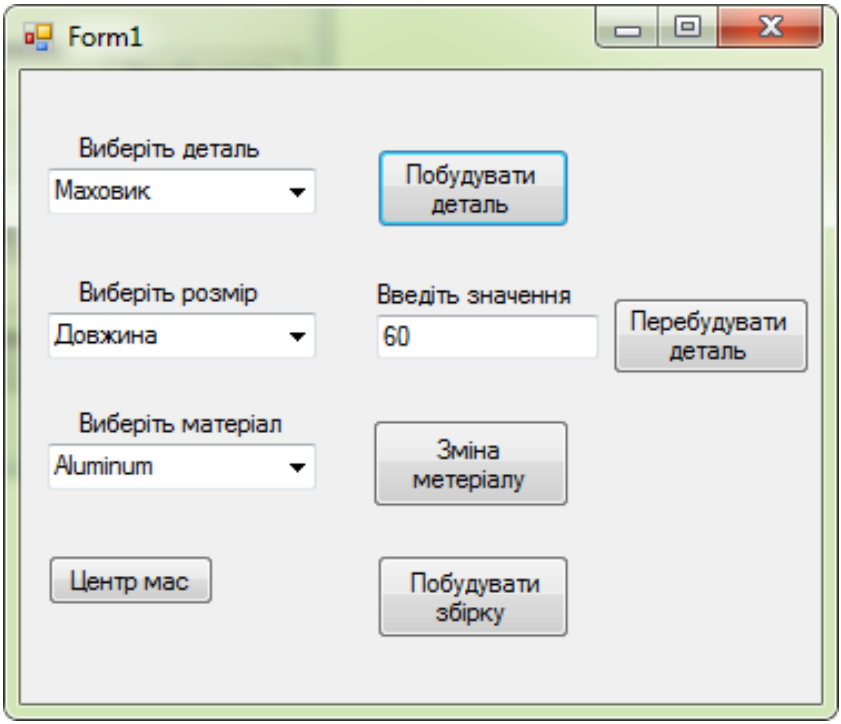


Рис.2. Головна форма розробленого додатку.

Таблиця 1 – навантаження, деформації та запас міцності на поршнях з різними металами.

	Титан	Сталь	Алюміній
Навантаження макс.	23 630,30	22 135,70	7 089,70
Навантаження мін.	2,8	4,2	1,7
Деформація макс	1,42E-01	1,43E-01	1,42E-01
Деформація мін.	4,79E-02	1,99E-04	4,73E-04
Запас міцності (FOS) макс.	291 153 216	148 308 256	43 451 880
Запас міцності (FOS) мін.	34 278,03	28 028,10	10 578,68

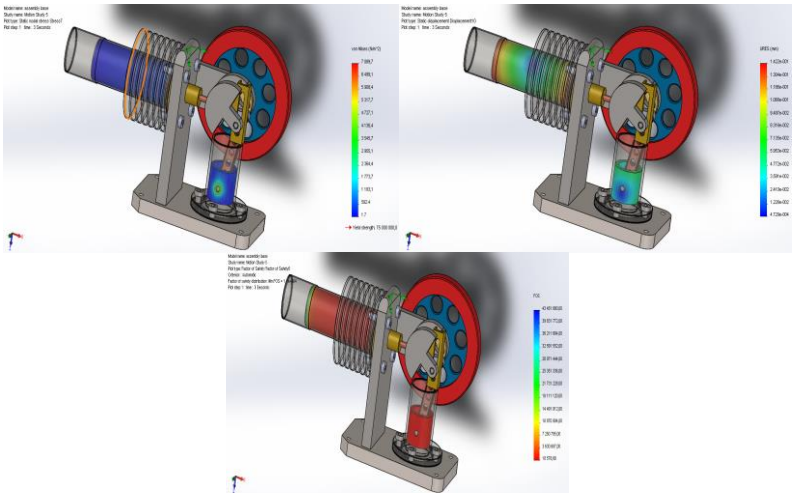


Рис.3. Результати тестувань для алюмінію.

Таким чином ми маємо зручний для користувача додаток, можемо дослідити двигун з різними розмірами, та визначити оптимальний матеріал з огляду ціна-якість, чи просто по найкращих якостях металів, переглянути деформації, запас міцності та навантаження на них.

1. Наталя Дударєва, Сергій Загайко «SolidWorks 2009 на прикладах» «БХВ». – Санки-Петербург, – 2009. – 530
2. Алямовський А. А. «SolidWorks комп'ютерне моделювання в інженерній практиці» «БХВ». – Санки-Петербург, – 2005. – 800

Захист інформаційного суверенітету як складова політики національної безпеки України

Лук'янова Галина Юріївна,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

За роки незалежності в інформаційній сфері сталися значні зміни в структурі та інтенсивності загроз національній безпеці

України. Сучасні інформаційні технології приникають у всі сфери життя нашої держави, спричиняють не тільки нові можливості, але й певні загрози. Внаслідок виникнення, накопичення, використання та розповсюдження великої кількості інформації та її спроможності поширюватись майже миттєво на величезні відстані виникає 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 [4, с. 367].

Суверенітет (нім. souvergdnitdt, франц. souverainete – верховна влада, похідні від латин. super – над) у юридичній науці – найважливіша ознака держави, що виявляється у її верховенстві, повноті, самостійності, реальності та теподільності, тобто верховенстві 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 [2, с. 106].

На відміну від нормативного визначення, що дається у Законах України «Про національну програму інформатизації», «Про інформацію», «Про науково-технічну інформацію», 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» [5, с. 535].

Державна політика забезпечення інформаційної безпеки України є складовою частиною політики національної безпеки. Вона має передбачати системну превентивну діяльність органів влади з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству загалом, а саме: створення умов для своєчасного виявлення джерел інформаційних загроз та визначення можливих наслідків їх дії; визначення комплексу превентивних заходів з

метою нейтралізації або зменшення (послаблення)негативних наслідків реалізації інформаційних загроз; створення умов (можливостей) забезпечення своєчасної, повної і точної інформації для ухвалення рішень; здійснення ефективного (рівноправного, взаємовигідного) міждержавного інформаційного співробітництва [1, с. 99].

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 [3, 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 [6].

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 [3, 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. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: вибр. наук. праці / О. С. Власюк. – К.: НІСД, 2016. – 528 с.

2. 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.
3. 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.
4. 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.
5. 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.
6. Чупрій Л.В. Створення позитивного іміджу України у світі / Чупрій Л.В. // [Електронний ресурс]. – Режим доступу: http://opros-dim.com/index.php.html.

Використання засобів Motion Capture для створення симуляторів допиту свідка

Магеровський Дмитро Вікторович,

здобувач ступеня магістра Національного університету «Львівська політехніка»

Магеровська Тетяна Валеріївна,

доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

Пелех Ярослав Миколайович,

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

Гошко Зіновія Олександрівна,

асистент кафедри обчислювальної математики та програмування Національно університету «Львівська політехніка»

Офіцеру силових відомств, окрім фізичного виховання, необхідно вміти швидко приймати правильні рішення у ситуації, що

гіпотетично склалася, а також прекрасно розумітися у психології, для роботи з людьми, як потерпілими чи зловмисниками, так і зі свідками. Переважно, свідки не поводять себе однаково, кожен реагує у ситуації по-своєму. Хтось у повній мірі відповість на запитання працівника силового відомства, хтось рознервується й упустить важливі для подальшого слідства деталі, а хтось спробує збрехати. Працівник силового відомства повинен розуміти, яким чином себе поводить людина, для чого необхідні тренування. Одним з потенційних методів навчити людину правильно проводити допит свідка є впровадження спеціальних симуляторів, з допомогою яких можна буде провести симуляцію допиту, після чого система згенерує звіт про проходження чи не проходження тесту, а також вкаже на помилки.

У 2011 році студією Team Bondi була випущена відеогра LA Noire, де гравцеві належало розкрити ряд злочинів, у тому числі проводячи допит свідків. У грі було використано технологію захоплення руху під назвою Facial MotionScan, розробником якої виступає студія Depth Analysis. Завдяки цій розробці можливо з високою якістю передати будь-які емоції персонажа. На рис. 1 представлено ігровий процес допиту свідка.

Рис 1. Ігровий процес відеогри LA Noire

Таким чином гравець, слухаючи та спостерігаючи за свідком може визначити, чи йому було надано неправдиві покази.

Симулятор допиту свідка запропоновано запровадити аналогічним образом. З допомогою вбудованого діалогу курсант повинен буде допитати свідка, після чого система покаже помилки та особливості, на котрі варто буде звернути увагу. При цьому, свідки та ситуації оператор може задати вручну, що підвищить інтерактивність, що в свою чергу допоможе працівнику силового відомства краще розуміти ситуації у реальному житті.

Motion Capture

Вищезазначена технологія MotionScan належить до стеку технологій Motion Capture – технологій захоплення руху. Дана технологія почала активно використовуватися з кінця 90-х років, таким чином методи й технології уже визначені та можна провести порівняльний аналіз технологій та обрати найбільш підходящий для симулятора допиту свідка.

Motion Capture поділяється на 2 види – **маркерні** та **безмаркерні**.

Маркерні системи

Системи даного типу використовують спеціальні датчики – маркери, що кріпляться до актора. Дані з датчиків зчитуються та поступають на комп'ютер, де створюється тривимірна модель, що відтворює дії актора, на основі яких в подальшому створюється анімація персонажа. Таким же ж методом можна анімувати й міміку актора. До переваг систем даного типу можна віднести їх точність у порівнянні із безмаркерними системами, а також велику розповсюдженість даної технології. Не всі маркерні технології здатні до розпізнавання міміки обличчя. Так, міміку не здатні розпізнати такі системи: оптичні активні; магнітні; механічні; гіроскопічні.

Оптичні пасивні системи. До обличчя актора чіпляють маркери, що відбивають послане на них світло, проте самі не світяться. Інфрачервоне світло на маркери посилається з допомогою високочастотних скробоскопів, після чого потрапляє назад у об'єктив камери, визначаючи таким чином їх місцерозташування. Недоліками даної технології є тривалість

розміщення маркерів на акторі. Також, при швидкому русі та близькому розташуванні маркерів, система може їх плутати. На рис. 2 зображено роботу актора із оптичною пасивною системою.

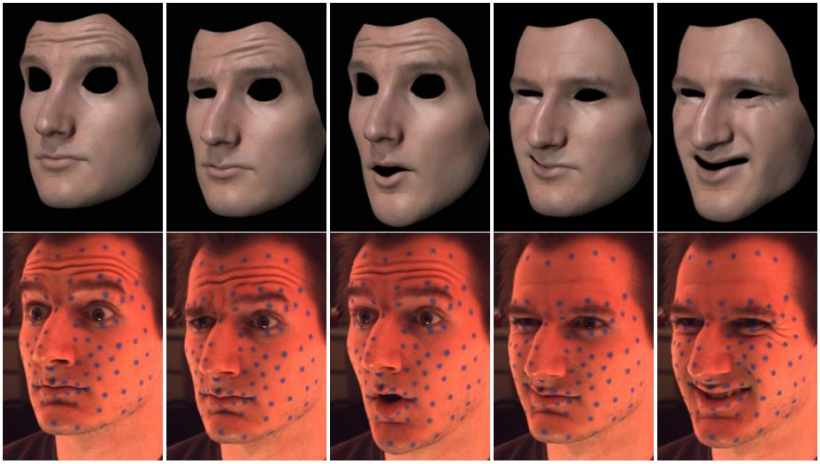


Рис. 2. Робота актора із оптичної пасивною системою

Безмаркерні системи

Системи даного типу не потребують спеціальних датчиків або костюму. Основою технології слугує розпізнавання образів. Актор може зніматися у звичайному одязі, що прискорює підготовку до зйомок. Залежно від точності отриманих результатів, дані системи можуть відчутно різнитися в ціні від маркерних, як в менший так і в більший бік.

MotionScan. Технологія, що використовувалася у відеогрі LA Noire. Технологія дозволяє з високою точність передавати емоції персонажа. Для запису актора використовують 32 камери високої чіткості, що працюють із частотою 30 кадрів на секунду. Після чого програмне забезпечення опрацьовує отримані дані та створює тривимірну модель обличчя персонажа (рис. 3). Недоліками даної системи є велика кількість даних, котру необхідно обробити та зберегти, а також те, що права на неї ексклюзивно належать австралійській компанії Team Bondi.

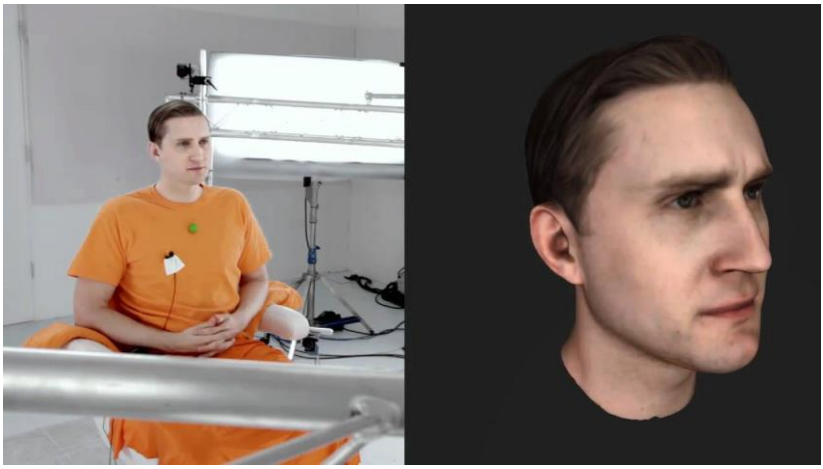


Рис. 3. Робота актора із MotionScan.

Прогресивну безмаркерну технологію використовує режисер Джеймс Кемерон у роботі над своїми фільмами. На актора надягають шолом, до котрого прикріплена камера, що направлена на нього. На обличчя наносять спеціальні кольорові точки що зчитуються камерою (рис. 4). Незважаючи на високу точність й реалістичність отриманого результату, даний метод є надзвичайно дорогим для його масового використання.

Рис. 4. Кадр із зйомок фільму «Аватар»

MashMe. Однойменна хорватська компанія запустила на Kickstarter збір коштів на технологію, де користувачі зможуть спілкуватися змінюючи свій образ на цифрових аватарів, що повторюють рухи й міміку (рис. 5). Дана технологія використовує лиш 1 камеру. Попри перспективність технології в індустрії розваг, точність зчитування міміки є недостатньо висока для роботи симулятора допиту, основою якого повинна бути точна передача міміки підозрюваного.

Рис. 5. Технологія MashMe

Висновок. Було описано технології та потенційну механіку симулятора допиту свідків. На основі отриманих даних можна зробити висновок, що для успішної реалізації симулятора силами українських розробників найдоречнішим буде використання маркерної технології, де використовуються оптичні пасивні маркери. За наявності більшої кількості фінансів було би доречно використати безмаркерну технологію MotionScan, що зменшило би часові затрати на розробку симулятора.

1. MashMe Turns You Into An Animated Character Automagically [Електронний ресурс]: Режим доступу https://techcrunch.com/2015/05/13/mashme-turns-you-into-an-animated-character-automagically/

2. MotionScan [Електронний ресурс]: Режим доступу http://lanoire.wikia.com/wiki/MotionScan
3. Технологія Motion Capture [Електронний ресурс]: Режим доступу https://masterok.livejournal.com/1614463.html

Проблеми реалізації фінансового моніторингу в Україні

Павлова Н.В.,

старший викладач кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук

Матвійчук І.В.,

здобувач ступеня бакалавра Дніпропетровського державного університету внутрішніх справ

Сучасний досвід показує, що найефективнішими засобами протидії організованої злочинності є контроль за фінансовими інституціями шляхом постійного проведення фінансового моніторингу. Тому можна говорити, що актуальним завданням сьогодення є створення дієвої інформаційної автоматизованої системи фінансового моніторингу, яка включає елементи планування, контролю, обліку, звітності та економічного аналізу фінансових потоків, та спрямована на досягнення й підтримання збалансованості економіки, має формуватися на основі варіантних прогнозів, до яких повинні входити крім традиційних макроекономічних показників, показники, що характеризують рівень фінансової рівноваги та безпеки в різних галузях, регіонах та у державі в цілому [2, с.64].

Досліджуючи проблеми фінансового моніторингу, в першу чергу, хотілося б звернути увагу на визначення його поняття. Так, згідно чинного законодавства, а саме Закону України від 14 жовтня 2014р. «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» фінансового моніторинг – це сукупність заходів, які

здійснюються суб'єктами фінансового моніторингу у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, що включають проведення державного фінансового моніторингу та первинного фінансового моніторингу [2]. Виходячи з даного поняття, об'єктом фінансового моніторингу в Україні виступають дії з активами, пов'язані з відповідними учасниками фінансових операцій, які їх проводять, за умови наявності ризиків використання цих активів з метою легалізації доходів, одержаних злочинним шляхом, або фінансування тероризму, а також будь-яка інформація про такі дії чи події, активи та їх учасників [3, с. 1].

Окрім цього, слід звернути увагу й на суб'єктивну складову фінансового моніторингу. Зокрема, суб`єкти первинного фінансового моніторингу забезпечують виявлення операцій, які підлягають обов`язковому фінансовому моніторингу та операцій, пов`язаних з легалізацією доходів, шляхом порівняння нормативно закріплених ознак операцій, які підлягають обов`язковому та внутрішньому фінансовому моніторингу, з ознаками операцій, які проводить суб`єкт первинного фінансового моніторингу [8, с. 306]. До суб'єктів первинного фінансового моніторингу відносяться: 1) банки, страховики (перестраховики), кредитні спілки, ломбарди та інші фінансові установи; 2) платіжні організації, члени платіжних систем, еквайрингові таклірингові установи; 3) товарні, фондові та інші біржі; 4) професійні учасники ринку цінних паперів; 5) компанії з управління активами; 6) оператори поштового зв'язку, інші установи, які проводять фінансові операції з переказукоштів; 7) філії або представництва іноземних об'єктів господарської діяльності, які надають фінансові послуги на території України; 8) спеціально визначені суб'єкти первинного фінансового моніторингу [2].

В свою чергу, суб`єкти державного фінансового моніторингу забезпечують перевірку інформації, у тому числі шляхом застосування інформаційних технологій, про зв`язок фінансових

операцій з легалізацією доходів, здобутих злочинним шляхом, а також здійснюють регулювання та нагляд за діяльністю суб`єктів первинного фінансового моніторингу [4, с. 305; 8].

Слід сказати, що, не дивлячись на законодавче врегулювання в Україні фінансового моніторингу, все ж на практиці існує низка проблем, що пов'язана з його реалізацією. Зокрема, існує проблема неопрацьованої системи індикаторів виявлення сумнівних операцій. Це пов'язано з тим, що чинним законодавством чітко окреслено лише ознаки сумнівності операцій, проте конкретно не зазначено показники, критерії чи індикатори чіткого віднесення таких операцій для моніторингу [7]. Крім того, потребують невідкладного нормативно-правового врегулювання процедури фінансового моніторингу операцій з векселями (векселями з бланковим індосаментом на пред'явника). Як показує світова практика, саме операції з цінними паперами є високо ризикованим фінансовим інструментом, через який відбувається легалізація доходів, тому на часі розробити і прийняти відповідні зміни до законодавства, в частині мінімізації ризиків відмивання коштів на ринку цінних паперів [6, с. 129-132].

Однією з проблем щодо ефективного проведення фінансового моніторингу з попередження, виявлення легалізації (відмивання) доходів, одержаних злочинних шляхом, є недосконала організація взаємодії з цього питання між органами загального державного фінансового контролю та спеціальними органами, які його здійснюють. Причинами такого стану є: різні оцінки діяльності взаємодіючих сторін, відомчі інтереси та не розкриття певної наявної інформації, низький рівень нормативно-правової рекомендації взаємодії відомств, відсутність належного науково-методичного забезпечення організації та здійснення взаємодії, неналежний рівень професійної підготовки співробітників, що безпосередньо здійснюють фінансовий моніторинг, щодо використання можливостей інформаційних баз даних та складність виявлення фактів легалізації (відмивання) злочинів, одержаних злочинним шляхом [1].

Для подолання вище вказаних проблем необхідно створити єдину інформаційну базу даних, що має свідчити про ділову репутацію суб'єкта господарювання; застосовувати превентивні заходи для попередження підозрілих операцій, як наприклад лімітування обсягів проведення операцій, як в часовому розрізі так і за обсягами; введення відповідальності на законодавчому рівні за порушення моніторингового законодавства посадовими особами суб'єктів первинного фінансового моніторингу; застосування значних розмірів штрафних санкцій саме для посадових осіб, та передбачити процедуру контролю за якістю їх діяльності [5].

Виходячи з вище викладеного можемо зробити висновок, що система фінансового моніторингу в Україні створена з метою протидії легалізації доходів, отриманих злочинним шляхом. Враховуючи той факт, що фінансовий моніторинг є відносно новим методом фінансового контролю, на практиці виникає низка проблем в процесі його реалізації. Тому для усунення недоліків здійснення компетентними суб'єктами фінансового моніторингу слід вдосконалити нормативно-правове та організаційне забезпечення такого методу фінансового контрою, що потребує подальшої наукової розробки.

1. [Електронний ресурс]. – Режим доступу: http://www.pravoznavec.com.ua/period/article/3149/%
2. Задоя А. О.Фінансовий моніторинг : перспективи впровадження та проблеми реалізації/А. О. Задоя, І. П. Ткаченко//Економічний вісник НГУ. – 2005. – №2. – С.60-69.
3. Матіос А. В. Актуальні проблеми правового регулювання системи фінансового моніторингу / А. В. Матіос // Публічне право. – 2013. – № 2. – С. 129-133.
4. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»: Закон України від 14.10. 2014 р. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1702-18. – Назва з екрана.

5. Слюсар Б. І. Напрями вдосконалення системи державного фінансового моніторингу / Б.І. Слюсар // Ефективна економіка. – 2011. – №11
6. Смагло О. В. Фінансовий моніторинг та його роль у протидії легалізації доходів, отриманих злочинним шляхом / О. В. Смагло. // Економічні науки. Серія : Облік і фінанси. – 2013. – Вип. 10(1).
7. Сюркало Б. І. Напрями вдосконалення системи державного фінансового моніторингу / Б. І. Сюркало. // Ефективна економіка. – 2011. – № 11.
8. Шиян Д. В. Суб'єкти фінансового моніторингу / Д. В. Шиян // Проблеми і перспективи розвитку банківської системи України. – 2012. – Вип. 36. – С. 303-310.

Акти-дії публічної адміністрації у правоохоронній діяльності: поняття, види і межі їх застосування

Павлович-Сенета Ярина Павлівна,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Сафонова Мирослава Ігорівна,

здобувач ступеня бакалавра факультету № 6 Львівського державного університету внутрішніх справ

Актуальність обраної теми полягає у тому, що здійснення актів-дій прямо впливає на реалізацію прав громадян тієї чи іншої країни. Проблема юридичної оцінки вчинення актів-дій є одним із найважливіших питань, яке гостро постало перед нашим суспільством, адже невиконання чи грубе порушення прав громадян органами публічної адміністрації є підставою для їх захисту та порушення справи в судовому порядку. В процесі вивчення та порівняння вітчизняного та зарубіжного досвіду встановлено, що інститут застосування актів-дії публічної адміністрації є одним із найрозвиненіших в Європі, Україні ж варто приділити більше уваги на його удосконалення.

Визначення поняття «акт-дія публічної адміністрації» різні науковці трактують по-різному. Зокрема, професор Гриценко

зазначає: «Акт-дія *публічної адміністрації* – це офіційне рішення суб'єкта публічної адміністрації, що виконується на основі і у відповідності з нормами адміністративного права у формі певних інтелектуально-вольових і фізичних (вербальних) дій і втілює публічно-владне веління з конкретної юридичної ситуації, спрямоване на регулювання суспільних відносин. Це такий вид дій суб'єкта публічної адміністрації, що не тягне правових наслідків. Його метою є настання фактичного результату» [1, с. 326].

В науці адміністративного права виділяють такі види актів-дій публічної адміністрації:

- організаційно-технічні дії з виділення та виплати бюджетних коштів;
- керування рухом транспортних засобів і пішоходів посадовою особою;
- звернення до громадян з інформацією про настання або можливість настання певних подій, фактів через засоби масової інформації;
- попередження та застереження суб'єктом публічної адміністрації про необхідність вжиття заходів з евакуації громадян у випадку наявності інформації про можливі стихійні лиха;
- вчинення фізичних дій для припинення протиправної поведінки особи;
- подання звітів, запитів;
- прибирання доріг, проведення заходів з благоустрою території;
- відібрання проб продукції на визначення її якості тощо [2, с. 79].

Слід зауважити, що найбільш поширеними серед актів-дій публічної адміністрації є ті, що застосовують в правоохоронній сфері. Наприклад, застосування спеціальних заходів фізичного впливу та спеціальних засобів працівниками правоохоронних органів, регулювання дорожнього руху жезлом або положенням рук, застосування світлових і звукових сигналів на дорозі, перекриття залізничних доріг засобами обмеження руху, та

тимчасова заборона руху автомобілів та інших транспортних засобів.

Варто акцентувати увагу на тому, що перелік побідних актів ніколи не був і не може бути вичерпним. Для того, щоб віднести певну дію до правозастосовного акту треба користуватись визначеним колом критеріїв, адже вони мають, перш за все, діяти у межах правового поля.

Класифікують акти-дії за декількома критеріями: за способом фіксації, за суб'єктами прийняття, за функціями у правовому регулюванні, за юридичними підставами, за значенням у юридичному процесі та за формою зовнішнього вираження. Вони є вербальними актами і застосовується вербальними засобами регулювання, здійснюються усно, тому процесуально не оформлюються. Їх вчиняють посадові особи правоохоронних органів, а також органи з питань охорони здоров'я, прикордонної служби, органи з питань надзвичайних ситуацій, і такі інші. Вони належать до допоміжних актів і поділяють їх на регулятивні і охоронні.

Межі застосування актів-дії залежать від специфіки їх діяльності, необхідності швидкого вирішення ситуації, від потреби доведення змісту акта до відома адресата, а також від особливостей правозастосування. Перелік питань, на які відповідає особа, яка уповноважена приймати рішення про застосування акту-дії, послідовність вирішення цих питань, є схожими в кожному випадку його вчинення.

Завжди вирішуються питання про наявність відповідних фактів, їх юридичної кваліфікації, тощо. Це дозволяє розробити алгоритм, придатний для використання правозастосовувачем, який вчиняє акт-дію. На базі цього алгоритму можна для кожного виду юрисдикційного процесу розробити свій спеціальний алгоритм, який відбуватиме специфіку питань, що вирішуються у даному процесі, і закріпити його у нормативному акті [3, ст.17]

Взагалі, акти-дії застосовуються публічною адміністрацією кожного дня і їх помилкове втілення в життя веде до порушення

прав і свобод людини і громадянина, що прямо заборонено Основним Законом нашої держави, тобто Конституцією. Отже, можна дійти до висновку, що на даному етапі органам влади варто було б зосередити свою увагу на цю проблему.

1. Загальне адміністративне право. підручник / [Гриценко І.С., Мельник Р.С., Пухтецька А.А. та інші]; за заг. Ред.. І.С. Гриценка. – К.: Юрінком Інтер, 2017. –326с.
2. Онови адміністративного права Німеччини: монографія / Л.А Мицкевич. – Красноярск, 2002. – 79с.
3. Правозастосувальні акти-дії в механізмі здійснення функцій органами внутрішніх справ: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: «Теорія та історія держави і права; історія політичних і правових вчень» / О.В Фандалюк – Х: ХНУВВС, 1999. – 17с.

Дискреційні повноваження органів публічної влади в правоохоронній сфері

Павлович-Сенета Ярина Павлівна,

доцент кафедри адміністративно-правових дисциплін факультету №6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Степанова Анастасія Олександрівна,

здобувач ступеня бакалавра факультету №6 Львівського державного університету внутрішніх справ

Законодавець намагається визначити всі форми та методи діяльності органів виконавчої влади. Звичайно, що всі варіанти подій передбачити не можливо. Дискреційні повноваження несуть таку особливу функцію публічної адміністрації, котра залежить індивідуально від конкретної посадової особи чи державного органу.

Дискреційні повноваження – це комплекс прав і зобов'язань представників влади як на державному рівні, так і на регіональному, у тому числі представників суспільства, яких

уповноважили діяти від імені держави чи будь-якого органу місцевого самоврядування, що мають можливість надати повного або часткового визначення і змісту, і виду прийнятого управлінського рішення. Також ця особа може вибирати рішення у передбачених для конкретних ситуацій нормативно-правових актах або схожих документах [1, с. 320].

Це надає можливість представникові влади здійснювати вибір варіанта рішення відповідно до власних міркувань, не обмежуючись чітко визначеним варіантом вирішення для конкретної ситуації. Обмежуючим фактором для рішень представників влади згідно з визначенням дискреційних повноважень є закон і справедливість.

В.І. Ремньов розглядав дискреційні повноваження як право органу державного управління приймати владні рішення на власний розсуд. Розглядаючи ці органи в їх вертикальному підпорядкуванні, він дійшов висновку, що обсяг дискреційних повноважень зменшується зверху донизу. Самі ж дискреційні повноваження є елементом компетенції, і їх використання в рамках закону лише зміцнює законність.

Французький вчений Г. Бребан вважав, що дискреційні повноваження, які означають свободу адміністрації оцінювати ситуації і приймати по них рішення, надають адміністрації простір у здійсненні вибору між вільними рішеннями. Вона вправі діяти або не діяти, а коли діє, то може вибирати один або декілька з можливих варіантів дій [2, с. 208].

Адміністративне законодавство щораз більше розширює обсяг дискреційних повноважень органів виконавчої влади, а різноманітна практика їх виконання нерідко породжує складні ситуації. Проблема встановлення механізмів контролю за реалізацією дискреційних повноважень, особливо, коли вони стосуються сфери охоронюваних Конституцією України прав і свобод громадян. Наприклад, дискреційні повноваження мають місце при ліцензуванні певного виду діяльності, при реєстрації суб'єктів підприємницької діяльності (Закон України «Про підприємництво»), при легалізації громадської або релігійної

організації, коли органи влади підтверджують їх право або відмовляють у наданні такого права. На підставі дискреційних повноважень орган влади обумовлює відмову у видачі громадянинові закордонного паспорта або візи іноземному громадянинові [3, с. 432].

Хоча на загал дискреційні повноваження органів виконавчої влади не можуть ані звужувати, ані розширяти окремі конституційні права і свободи громадян. Вони охороняються Основним Законом держави.

Зарубіжний дослідник А. Барак з цього приводу писав, що вільний розсуд — це повноваженні, надані особі, яка наділена владою, вибирати між двома або більше альтернативами, коли кожна альтернатива законна. Отже, це вибір лише із законних альтернатив. Якщо законна альтернатива відсутня, не може бути мови про розсуд [4, с. 267].

Отже, адміністративний розсуд повністю пов'язаний з правом і не має нічого спільного зі свавіллям як дією на свідоме порушення законодавства. Суть розсуду полягає у вольовому співвіднесенні доцільності і законності. Здійснюючи свою діяльність на їх основі, органи виконавчої влади послуговуються тими формами, які визначає законодавець. Однак не завжди наперед можна обумовити всі форми діяльності, особливо коли ситуація стосується виконання та застосування норм права. Сучасна практика підтверджує, що дискреційні повноваження є законним елементом публічної адміністрації. Вони сумісні з адмініструванням у рамках закону.

Підсумовуючи, можна сказати, що в демократичній, правовій державі взагалі не може йтися про будь-який вільний розсуд, не пов'язаний з правом, і про неконтрольовану діяльність адміністрації. Навіть у тих випадках, коли норма права наділяє орган влади певною свободою в прийнятті рішень, орган у межах цієї свободи є зв'язаним загальнообов'язковим правом, всіма закріпленими в ньому принципами і цінностями.

Окремі висновки цього дослідження можуть сприяти подальшим науковим дослідженням у питаннях проблематики

дискреційних повноважень в діяльності правоохоронних органів, а також використати їх для забезпечення раціонального співвідношення обставин справи з прийняттям правових рішень на власний розсуд.

1. Юридичні терміни. Тлумачний словник / В.Г. Гончаренко, П.П. Андрушко, Т.П. Базова та ін.; за ред. В.Г. Гончаренка. – К.: Либідь, 2003. – 320 с.
2. Таманага Б. Верховенство права: історія, політика, теорія / Б. Таманага; [перекл. з англ. А. Іщенка]. – К. : Вид. дім «Києво-Могилянська академія», 2007. – 208 с.
3. Авер'янов В.Б. Державне управління: проблеми адміністративно-правової теорії та практики. – К.: Юрінком Інтер, 1998.- 432с.
4. Голосніченко І.П. Проблеми адміністративного процесу на сучасному етапі розвитку української держави / І.П. Голосніченко // Актуальні проблеми держави і права. Збірник наукових праць. – Вип. 19 – Одеса: Юридична література, 2003. – 267 с.

Система менеджменту інформаційною безпекою в інформаційних системах

Рудий Тарас Володимирович,

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

Живко Зінаїда Богданівна,

завідувач кафедри менеджменту факультету № 8 Львівського державного університету внутрішніх справ, доктор економічних наук, професор

Руда Ольга Іванівна,

доцент кафедри економіки та економічної безпеки факультету № 8 Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

Інформаційна війна, яку Росія активувала з початком збройної агресії проти України, поставила перед нашою державою нові

здачі у сфері інформаційної безпеки, що зумовлено виникненням актуальних загроз національній безпеці в інформаційній сфері, а також потребою визначення інноваційних підходів до формування та розвитку сучасних систем захисту, включаючи системи менеджменту інформаційною безпекою (СМІБ). Відсутність реально працюючих механізмів координування діяльності та менеджменту у сфері інформаційної безпеки тільки загострюють означені проблеми.

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

Аналіз наявних матеріалів стосовно проблеми захисту інформаційних активів ІС дає змогу виявити недоліки як у методології проектування та функціонування комплексних систем захисту інформації (КСЗІ), так і СМІБ, які суттєво впливають на ефективність функціонування усієї системи безпеки ІС. Серед головних відзначимо: КСЗІ у ІС не враховує динаміки зміни загроз; не забезпечує достатнього рівня стійкості системи захисту інформації (ЗІ) до відмов та відновлення після збоїв; відсутність методик оцінювання ефективності СМІБ; ігнорування вимогами міжнародних стандартів у галузі ЗІ при проектуванні СМІБ.

Метою даного дослідження є обґрунтування пріоритету створення СМІБ в контексті забезпечення захисту інформаційних активів ІС та означити організаційні принципи на основі вимог міжнародних стандартів.

Отже, розвиток і впровадження ІТ у функціонування державних органів влади і, зокрема, Національної поліції України вимагають розв’язання питань захисту інформаційних активів ІС на підставі: Конституції України; Законів України; указів та розпоряджень Президента України; постанов та розпоряджень Кабінету Міністрів України; нормативно-правових актів Служби безпеки України, Державної служби спеціального

зв'язку та захисту інформації (ДССЗТЗІ) України; міжнародних угод України з питань ЗІ, згода на обов'язковість виконання яких надана Верховною Радою України.

Довільна використовувана методологія при проектуванні СМІБ повинна бути сумісною з основними стандартами ISO/IEC серії 27000: 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].

Основним стандартом, на підставі якого можна провести роботи з створення СМІБ є оновлений ISO/IEC 27001:2013, причому це не технічний стандарт, а управлінський. Використання міжнародних стандартів ISO/IEC серії 27000 у СМІБ інформаційних систем подано на рис. 1.

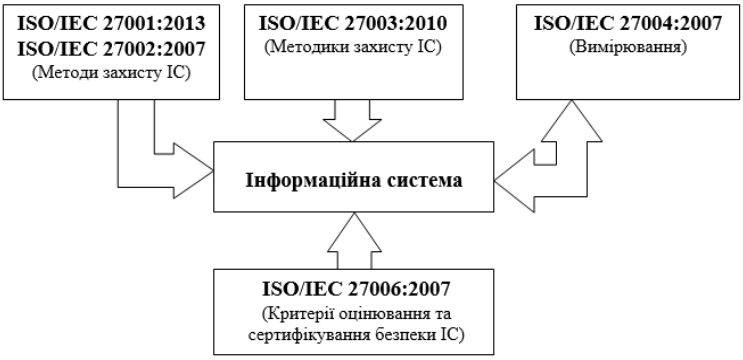


Рис. 1. Використання міжнародних стандартів ISO/IEC серії 27000 у СМІБ інформаційних систем

У відповідності до вимог міжнародних стандартів процес розроблення СМІБ містить такі етапи: планування – забезпечує правильне завдання масштабу СМІБ, оцінює ризики, пропонує відповідний план оброблення цих ризиків; реалізування – впроваджує ухвалені рішення, які були визначені на етапі планування; аналіз захищеності – оцінювання ефективності та надійності функціонування створеної СМІБ, проведення аудиту ІБ, виявлення недоліків; реагування – виконання коригувальних дій з покращення функціонування СМІБ і вимагає первісного інвестування, документування діяльності, формалізування підходу до управління ризиками, визначення методів аналізу.

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

Для процесів СМІБ застосована модель циклічного процесу з використанням принципу управління ІБ, ядро якої становить централізоване адміністрування (враховує специфіку функціонування ІС спеціального призначення – дотримання режиму таємності). Організаційні принципи реалізування СМІБ подано на рис. 2.

Аналіз і оцінювання ризиків, на думку авторів, провадитися за чотирма основними критеріями безпеки: доступність – забезпечення безперервного доступу до інформаційних та апаратних активів ІС, сервісів згідно з наданими працівникам повноваженнями та правами у необхідному обсязі; цілісність – захист точності/коректності та повноти інформаційних активів ІС і методів оброблення інформації; конфіденційність – доступність до інформаційних активів винятково для офіційно авторизованих працівників у мінімально необхідному обсязі; спостережність – забезпечення принципу невідмови від вчинених дій. Тобто, у СМІБ реалізоване жорстке адміністративне керування доступом.

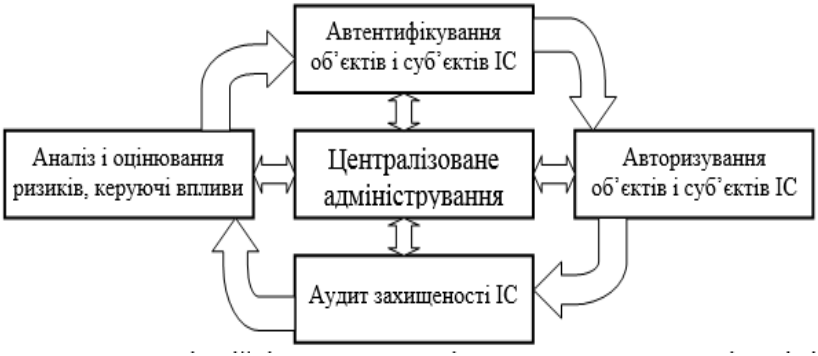


Рис. 2. Організаційні принципи реалізування системи управління інформаційною безпекою

Сформульовані правила фіксуються у відповідних документах (документування процедур – одне з основних вимог стандарту ISO 27001).

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми, навмисними та ненавмисними впливами, елементарною необізнаністю працівників у галузі ІТ необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІБ), яка є базовою частиною загальної СМІБ.

Основна задача СУІБ – якомога швидше відновити роботу сервісів і звести до мінімуму негативний вплив інциденту на роботу ІС для підтримки якості і доступності сервісів на максимально можливому рівні. Штатною вважається робота сервісів, що не виходить за рамки угоди про рівень обслуговування. Згідно з [3] цілі, які ставлять перед СУІБ є такими: відновлення штатної роботи сервісів у найкоротші терміни; зведення до мінімуму впливу інцидентів на функціонування ІС; забезпечення оброблення всіх інцидентів і запитів обслуговування; зосередження ресурсів підтримки ІБ на найбільш важливих напрямах; надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління. Процес управління інцидентами інформаційної безпеки подано на рис. 3.

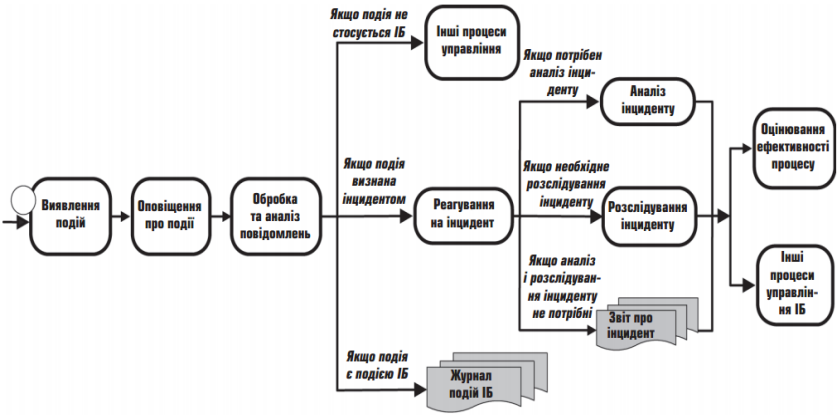


Рис. 3. Процес управління інцидентами інформаційної безпеки

Висновки. Впровадження СМІБ дозволить зменшити інформаційні ризики порушення роботи ІС за рахунок розмежування фізичного доступу та впровадження механізму моніторингу (аудиту) стану ІБ.

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

1. Рудий Т. В. Організаційно-правовий супровід захисту інформаційних систем підрозділів Національної поліції України на основі міжнародних стандартів / Т. В. Рудий, О. В. Захарова, В. В. Сеник, С. В. Сеник, М. І. Ізьо/ Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С.213-225.
2. Рудий Т.В. 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. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В., Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

Інформаційно-аналітичне забезпечення розслідування терористичних актів, з використанням вибухових пристроїв

Савчук Микола Васильович,

здобувач Львівського університету бізнесу та права

Перспективних напрямом підвищення ефективності організації розслідування кримінального провадження терористичних актів, з використанням вибухових пристроїв слід уважати впровадження в даний процес новітніх інформаційних систем і технологій, під якими прийнято розуміти організаційно впорядковану сукупність масивів інформації про об'єкти та інформаційні технології, у тому числі засоби сучасної комп'ютерної техніки, програмне забезпечення й мережі зв'язку, що забезпечують процеси введення, опрацювання та видачі інформації

Процес розслідування, зазначених злочинів пропонує розроблення й використання комп'ютерних програм як підґрунтя інформаційного забезпечення підтримки прийняття рішення слідчим, який здійснює розслідування за конкретним кримінальним провадженням, а саме: про забезпечення такої його інтелектуальної діяльності, як планування, і таких його аспектів, як висунення робочих версій та обрання оптимальних систем слідчих (розшукових) і негласних слідчих (розшукових) дій щодо їх перевірення.

Наприклад, В. В. Бірюков як криміналіст називає це поняття «інформаційне довідкове забезпечення» та вважає, що інформаційно-довідкове забезпечення розслідування злочинів – це окреме криміналістичне вчення, предметом якого є знання про організацію та функціонування інформаційних систем, незалежно від їх основного призначення та відомчої належності,

порядок отримання облікової інформації та особливості її використання в розслідуванні. Разом із визначенням поняття вчення нами сформульовано поняття інформаційно-довідкового забезпечення розслідування злочинів як вид діяльності, що здійснюється працівниками правоохоронних органів [1, с. 9]. В. С. Безрученко визначає це поняття як «інформаційно-аналітичне забезпечення» та зазначає, що інформаційно-аналітичне забезпечення – це сукупність компонентів з організації діяльності щодо виявлення осіб і фактів, які становлять оперативний інтерес, збору, передачі та обробки інформації, аналітичних методів її аналізу, внутрішніх і зовнішніх каналів її транспортування (зв'язків) та, власне, інформацію [2, с. 23].

Авторський колектив (Р. А. Калюжний, В. О. Шамрай, М. Я. Швець та інші) визначають зміст поняття «інформаційне забезпечення» як: – забезпеченість системи управління відповідною множиною інформації; – діяльність, пов'язана із організацією збору, реєстрації, передачі, зберігання, опрацювання і представлення інформації; – діяльність щодо формування цілеспрямованої суспільної і індивідуальної свідомості суб'єктів суспільних відносин щодо управління у конкретній сфері суспільних відносин [3, с. 6–7].

Розслідування терористичних актів, з використанням вибухових пристроїв, як специфічний вид інформаційно-пізнавальної діяльності здійснюється за допомогою відповідних засобів, дослідженню яких приділяється увага і в інших галузях знань.

Інформаційні дані використовуються слідчими процесі ведення кримінального провадження з розслідування терористичних актів, з використанням вибухових пристроїв, які знаходяться у криміналістичних обліках.

Найбільш продуктивними, такими, що відповідають як сучасному стану наукових досліджень, так і потребам судово-слідчої практики, можна визнати інформаційно-довідкову, інформаційно-пошукову, інформаційно-модельну та інформаційно-консультативну системи.

Слідчі звертаються до інформаційно-довідкових обліків (колекції й картотеки), що комплектуються за об'єктами та даними, які безпосередньо не пов'язані з подією злочину та отримані в результаті накопичення відомостей інформаційного характеру. Об'єктами інформаційно-довідкових колекцій і картотек можуть бути зразки різноманітних вибухових виробів.

У межах центральних обліків (ДНДЕКЦ) слідчі можуть звернутися до вибухотехнічного обліку, який функціонує на центральному та обласному рівнях і складається з:

а) оперативно-пошукової колекції вибухових пристроїв та їх залишків;

б) інформаційно-довідкової колекції вибухових пристроїв.

Оперативно-пошукова колекція формується з:

- саморобних і промислових вибухових пристроїв та їх залишків, вилучених під час проведення слідчих (розшукових) дій та оперативно-розшукових заходів;
- саморобних вибухових пристроїв, реконструйованих при проведенні експертиз;
- карток обліку вибухових пристроїв та зарядів вибухових речовин і піротехнічних засобів (вилучених, розряджених або застосованих для вчинення вибухів), складених за висновками експертиз.

До оперативно-пошукової колекції вміщуються саморобні та промислові вибухові пристрої, в яких заряди вибухової речовини та засоби підриву заміщуються інертними, не здатними до вибуху речовинами.

Інформаційно-довідкова колекція формується з:

- боєприпасів і зарядів вибухових речовин промислового виготовлення та їх комплектуючих;
- продукції народногосподарського призначення, що може бути використана для виготовлення саморобних вибухових пристроїв [4, с. 374].

Центральні оперативно-пошукова та інформаційно-довідкова колекції можуть формуватися з об'єктів, які надходили для проведення експертних досліджень до НДЕКЦ перевірка за вибухотехнічним обліком на центральному та обласних рівнях здійснюється за такими позиціями: за місцем та способом вчинення злочину, конструкцією вибухових пристроїв чи їх окремих складових частин і механізмів, маркувальними позначеннями.

Отже інформаційне-аналітичне забезпечення розслідування кримінального провадження терористичних актів, з використанням вибухових пристроїв це специфічний вид діяльності направлений на здобуття слідчим достатньої сукупності актуальної вчасної необхідної інформації яка знаходиться у різних банках даних щодо виду вибухових пристроїв та їх залишків, способів їх застосування тощо.

---

1. Бірюков В. В. Інформаційно-довідкове забезпечення розслідування злочинів : навчальний посібник / В. В. Бірюков ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2009. – 112 с.
2. Безрученко В. С. Напрями вдосконалення інформаційно-аналітичного забезпечення підрозділів податкової міліції. Проблеми удосконалення законодавства і практики протидії злочинності у сфері господарської діяльності : збірник наукових праць за матеріалами Міжнародного науково-практичного семінару; 10 грудня 2009 року / Безрученко В. С. ;Національний університет ДПС України, НДІ фінансового права. – К. : Вік. Прінт, 2009. – 278 с.
3. Семер'янов Д. Я. Інформаційно-аналітичне забезпечення управління підрозділами податкової міліції : дис. кандидата юр. наук : 12.00.07 / Семер'янов Дмитро Якович. – Ірпінь,2004. – 178 с.
4. Міжнародна поліцейська енциклопедія. У 10 т. / Відп. редактори Є.М. Моісєєв, В.Я. Таций, Ю.С. Шемшученко. – К.: Атіка. 2009. – – Т.V. Кримінально-процесуальна та криміналістична діяльність поліцейських організацій. – 1008 с.

Управління ресурсопотоками, що циркулюють у логістичній системі ЗВО

Сватюк Оксана Робертівна,

доцент кафедри менеджменту факультету № 8 Львівського державного університету внутрішніх справ кандидат економічних наук, доцент

Костюк Богдан Володимирович,

здобувач ступеня магістра факультету № 8 Львівського державного університету внутрішніх справ

Сватюк Данило Романович,

здобувач ступеня бакалавра Національного університету «Львівська політехніка»

Відповідно до змін Закону «Про освіту» № 2145-VIII від 05.09.2017 у тексті слова «вищий навчальний заклад» (ВНЗ) в усіх відмінках і числах замінено відповідно словами «заклад вищої освіти» (ЗВО) [1].

Національний інститут стратегічних досліджень обґрунтував тенденції та питання розвитку освіти: 1) децентралізація системи вищої освіти, реальна *автономізація ЗВО* (включно з економічною діяльністю), розвиток приватного сектора галузі вищої освіти з одночасним запровадженням ефективної системи оцінювання якості освіти, на базі незалежних агенцій оцінювання якості; 2) послідовна реструктуризація й оптимізація державного замовлення на підготовку фахівців за участі роботодавців з метою приведення державного замовлення у відповідність до реальних потреб державного і приватного секторів національної економіки; 3) подальший розвиток експортного потенціалу вітчизняної вищої освіти з метою отримання економічних результатів, *прискорення модернізації освіти та посилення впливу і престижу України у світі* тощо [2].

Метою статті є визначення оптимального управління потоками, що циркулюють у логістичній системі ЗВО, де виділяються області максимального зосередження потоків у однакові моменти часу-точки.

При аналізі літератури [3, 4, 6] виділено основні етапи: 1) визначення зв'язку інформаційного потоку з відповідними дохідними та витратними грошовими потоками; 2) обґрунтування дохідних та витратних грошових потоків, що використовувалися до визначення коефіцієнту відповідної інформації; 3) виділення, згідно значень коефіцієнтів, видів інформаційних потоків (вимоги, що надходять від споживачів; замовлення освітніх послуг; інші замовлення, між якими розподіляються менеджерські ресурси). Відповідно, точки інформаційного та фінансового потоків у межах організаційної структури ЗВО зображено на рис. 1.

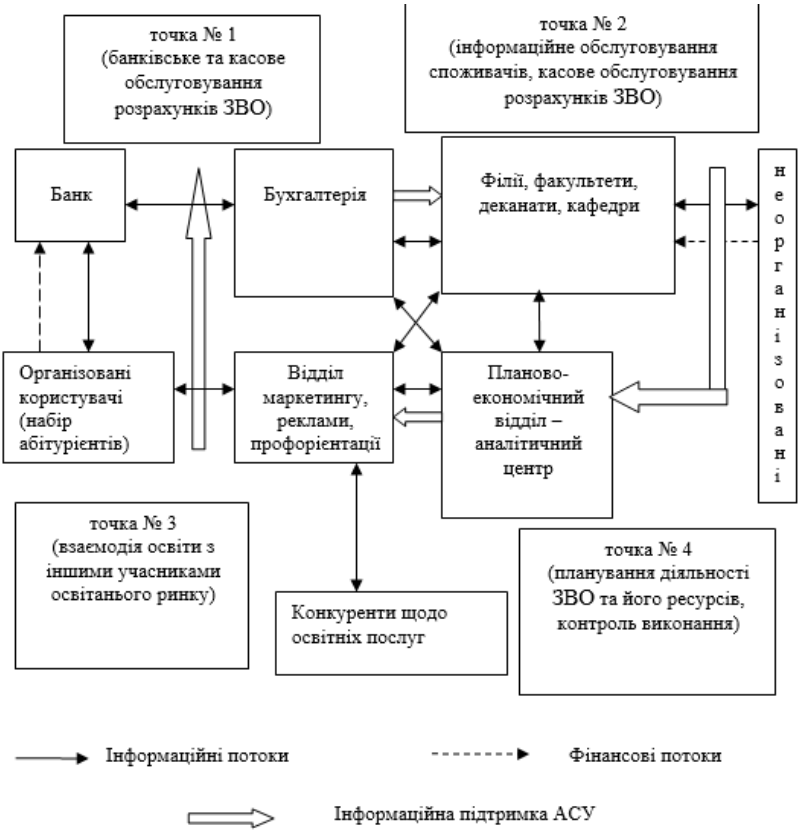


Рис. 1.Формування точок перетину ресурсопотоків у логістичній системі ЗВО. адаптовано за джерелами [4, 6].

У результаті руху інформаційних, фінансових та сервісних потоків у логістичній системі закладів вищої освіти утворюються місця, де концентрація всіх потоків є найвищою. Це так звані *точки закладення ресурсопотоків*. Оскільки всі ресурсопотоки пов'язані та впливають на характеристики один одного, то організація менеджерських впливів на потоки найефективніша у точках їхнього перетину, де одна управлінська дія може бути скерована на зміну параметрів одразу декількох ресурсопотоків. Формування таких точок відбувається невипадково. Прийняті в освіті правила обслуговування, форми та методи розрахунків, характер руху інформації між організаціями, комунальними установами, між учасниками конференції, персоналом, а також внутрішніми службами в процесі обслуговування, природним чином формують склад та параметри точок, визначають їхнє місцеположення відносно до організаційної структури освітнього закладу, до конкретних відділів.

У наслідку суміщення запропонованої структури логістичної системи ЗВО з адміністративною мережею ЗВО були отримані точки перетину ресурсопотоків. Як показав аналіз, усі точки відкриті для постійного менеджерського впливу і саме в них повинні концентруватися головні ресурси управління товариством.

Отже, подано більш детальний аналіз змісту, структури, а також властивостей та рекомендацій кожної з представлених на рис. 1 точок.

Точка № 1 це місце банківського та касового обслуговування розрахунків ЗВО, основу якого являють собою банківські та касові рахунки. Її формування визначається необхідністю здійснення розрахункових та облікових операцій у товаристві. В адміністративній мережі ЗВО вона прив'язана до відділу бухгалтерії, яка відповідає за зв'язок з банком, організацію безготівкових розрахунків з споживачами послуг, підрядниками, веде облік руху готівкових грошових засобів у товаристві. Структуру даної точки утворюють два види потоки – зовнішній та внутрішній. До перших відносяться

зовнішні інформаційні потоки (договори, рахунки, платіжні документи), які обслуговують зовнішні фінансові потоки, що проходять через цей точка та характеризують оплату вже наданих або майбутніх послуг. До внутрішніх потоків належить сукупність вхідних та вихідних з точки потоків документації з елементарних логістичних пунктів (довідки, звіти, форми), що убезпечують інформаційну підтримку інших підрозділів ЗВО.

Наявність двох видів потоків відносно до логістичної системи Публічного акціонерного товариства (ПАТ) визначає змішаний тип даної точки. Крім цього, склад та поточні параметри точки №1 здійснюють безпосередній вплив на точки № 2 та № 3 та опосередкований вплив на точку № 4.

Зокрема, наявний у точці № 1 інформаційний потік про дебіторську заборгованість у будь-якого споживача може генерувати прямі потоки інформації у відділи про призупинку заявок та обслуговування договору. В свою чергу це впливає на параметри грошових показників та планів.

Точка № 2. Його формування характеризується тим, що походження вхідних та вихідних ресурсопотоків визначається безпосереднім контактом відповідних служб ПАТ з споживачами. Це точка інформаційного обслуговування споживачів ПАТ (оплата освітніх послуг), а також касового обслуговування готівкових розрахунків (каси, банкомати). Ця точка перш за все прив’язана до служби прийому та розміщення (яка будучи інформаційним посередником між споживачами та внутрішніми службами ПАТ, виконує функції інформаційного центру), а також до служб надання додаткових освітніх послуг. Структуру точки № 2 складають вхідні інформаційні потоки від споживачів, що обробляються та продовжують рух у різні підрозділи ПАТ. Вхідні грошові потоки від споживачів (готівка та кредитні картки) перетворюються в інформаційні потоки (рахунки, інформація в електронній системі) та направляються для подальшої обробки у точки № 1 та № 3 та опосередковано на точка № 4.

Зокрема, наказ на зарахування студента на навчання чи його поновлення, що надійшла до відділу, генерує інформаційні потоки на точці а № 3 (про кількість, термін навчання, тощо – для аналізу можливостей ПАТ у вказаний період та визначення ціни), а також на точка № 1 (для організації розрахункових операцій з обслуговування).

Точка № 3 є ключовим вузлом у якому формується споживацька база ПАТ; готуються, укладаються та обслуговуються договори з надання послуг; розробляється та затверджується тарифний та маркетингові плани. Існування цього точки пояснюється необхідністю взаємодії ПАТ з іншими учасниками ринку освітніх послуг – товариствами, агентами, конкурентами. В адміністративній структурі ПАТ точка № 3 прив'язаний до відділу продажу послуг та маркетингу, а його склад становлять зовнішні інформаційні потоки від організованих споживачів (про стан, динаміку та перспективи розвитку ринку, параметри конкуренції) та внутрішні потоки (про результати роботи, споживчі уподобання, якість обслуговування). Отже, ця точка теж є змішаною і здійснює прямий вплив на всі інші точки. Отже, при використанні інструментів маркетингу, зокрема механізму ціноутворення, можуть бути змінені параметри вхідного потоку з замовлення послуг на точці № 2, обсяги проведення розрахункових операцій на точці № 1 та виконане коригування грошових показників і планів на точці № 4.

Точка № 4. Наявність цього точки визначається необхідністю планування розвитку ПАТ та його ресурсів, проведення аналітичної роботи, здійснення контролю щодо виконання планів, а також можливою зміною показників. Відповідно на точка № 4 приходять потоки інформації про ситуацію та параметри інших точок; ці потоки обробляються та розподіляються у вигляді планів, кошторисів підрозділів тощо. Тому дана точка є внутрішньою та здійснює прямий вплив на всі інші точки.

Отже, на стадії планування ресурсопотоків у точці № 2 відбувається формування заявок на майбутні періоди, виконується завантаження даних до комп'ютерної системи,

визначаються параметри (обсяг потоку, рівень неоплачених послуг). У точці № 3 здійснюється прогноз стану ринку, плануються обсяги сервісних потоків та можливостей ПАТ на наступні періоди, формуються цінові пропозиції на конкретні майбутні періоди, розробляється маркетинговий план.

Таким чином, точкові впливи охоплюють усю організаційно-управлінську структуру ЗВО. Більше того, прямий та тісний характер взаємодії точок №1 та №3 в логістичній діяльності ПАТ доводить необхідність безпосередньої участі відповідних служб в організації та оперативному управлінні всіма логістичними процесами в освіті.

За стратегічного управління та планування всіх процесів потрібною є розробка технології взаємодії представників усіх точкових служб, що дозволить: підвищити ступінь регулювання та узгодженість служб, мінімізувати можливі збої в роботі, ефективніше здійснювати управління ресурсопотоками ПАТ у точках їхнього перетину на кожній стадії логістичного процесу – планування, організування, контролю.

Точка № 4 готує необхідну планову документацію з ресурсопотоків, розраховує потреби грошових та трудових ресурсів, виконує розрахунки собівартості з окремих освітніх продуктів.

На стадії організації ресурсопотоків на точці № 1 обслуговується безготівкові розрахунки, кредитні картки споживачів, виконується обробка звітів касирів, організація бухгалтерського обліку. Точка № 2 здійснює касове обслуговування готівкових розрахунків у освіті, організує рух внутрішніх інформаційних потоків у процесі обслуговування, забезпечує надання додаткових послуг та вирішення поточних питань. У точці № 3 оформлюються договори та угоди, ведеться та оновлюється база даних корпоративних споживачів, застосовуються необхідні маркетингові інструменти до впливу на параметри ресурсопотоків. Аналітичний центр (точка № 4) виконує фінансовий облік, облік робочого часу, що оплачується тощо.

На стадії контролю та обліку ресурсопотоків бухгалтерія (точка № 1) виявляє невідповідності параметрів потоків послуг та пов'язаних з ними грошових потоків, здійснює облік дебіторської та кредиторської заборгованості, проводить фінансово-менеджерський облік. Служби прийому документів (точка № 2) ведуть облік та коригують рівень неявки з різних видів замовлення, складають та оновлюють список постійних споживачів згідно внутрішньо-нормативних документів. Відділ продажу та маркетингу аналізує рекомендації фактичних потоків, послуг за споживачами, здійснює коригування цінової політики, веде аналіз та облік споживчих уподобань, складає звіти про роботу конкурентів. При цьому, аналітичний центр відслідковує відхилення фактичних характеристик ресурсопотоків від планових показників та зміни собівартості послуг, здійснює аналіз діяльності ЗВО.

Знання інформатики та грамотне володіння комп'ютером дають можливість швидко та безпомилково продемонструвати теоретичні припущення у вигляді кількісних і якісних оцінок, а також вміло використати програмні продукти [4].

Рішенням проблем застосування інформаційних технологій може бути економіко-математичний апарат моделювання. Існує ціла низка класичних лінійних та нелінійних математичних моделей, що описують розвиток освіти [5] для подальшого дослідження.

1. Про освіту. Закон України. Відомості Верховної Ради (ВВР), 2017, № 38-39, ст.380. Документ 2145-19, чинний, поточна редакція — Прийняття від 05.09.2017. URL: http://zakon3.rada.gov.ua/laws/ show/2145-19
2. Глобальні тенденції і проблеми розвитку освіти: наслідки для України. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1537/
3. Жданов Б. Новая логика и факторы развития КИС. /Б. Жданов. № 3/2006. с.12-17. URL: http://www.management.com.ua/ims/ ims125.html

4. Економіко-математичне моделювання: Навчальний посібник / За ред. О. Т. Іващука. – Тернопіль: ТНЕУ «Економічна думка», 2008. – 704 с.
5. Меняев М.Ф. Информационные системы и технологии управления организацией : учеб. пособие / М.Ф. Меняев – М. : Изд-во МГТУ им. Н.Э. Баумана, 2010 .— 88 с.
6. Смирнов І.Г. Логістика ресурсної бази туризму в контексті його сталого розвитку / І.Г. Смирнов // Вісник ДІТБ. – 2008. – №12. – С.159-167.

Інформаційні технології у судово-медичній експертній діяльності

Сибірний Андрій Володимирович,

доцент кафедри загальної гігієни з екологією Львівського національного медичного університету ім. Данила Галицького, кандидат біологічних наук, доцент

Сибірна Рома Іллінічна,

професор кафедри психології діяльності в особливих умовах факультету № 7 Львівського державного університету внутрішніх справ, доктор біологічних наук, професор

Формування творчого судово-медичного мислення базується на комплексному використанні як класичних прийомів, так і новітніх інформаційних технологій. Безпосереднє проведення експертного дослідження є безперечною компетенцією експерта. Однак, не применшуючи самостійності експерта, варто вказати на необхідність активної участі у цьому процесі слідчого, зацікавленого в якісному і ефективному проведенні дослідження, використанні новітніх технологій і досягнень науки та техніки, збереженні досліджуваного об’єкта для проведення інших досліджень.

Так, на первинному етапі проведення експертного дослідження слідчий і експерт разом усвідомлюють завдання призначеної експертизи, сутність поставлених перед експертом питань, визначають реальні терміни проведення дослідження, спільно перевіряють матеріали, що надійшли на експертизу, їхнє

упакування. На цій стадії експерт може вказати на недоліки, наявні під час вилучення представлених на дослідження матеріалів, надати консультації щодо їх усунення в роботі з іншими речовими доказами.

Проведення судово-медичної експертизи здійснюється фахівцями державних установ судово-медичних експертиз МОЗ України.

Проведення судово-медичних експертиз може здійснюватися на підприємницьких засадах на підставі ліцензії, що видається МОЗ України [2].

Судово-медична експертиза виконується відповідно до Закону України «Про судову експертизу», згідно з Кримінальним процесуальним кодексом України та іншими законодавчими актами, міжнародними договорами та угодами про взаємну правову допомогу і співробітництво, що регулюють правовідносини у сфері судової медицини, судово-медичної експертизи та судово-медичної експертної діяльності та нормативними документами, затвердженими наказом Міністерства охорони здоров'я України № 6 від 17 січня 1995 року.

Судово-медична експертиза здійснюється на принципах законності, об'єктивності, повноти дослідження та незалежності державними установами – бюро судово-медичних експертиз (Головним та регіональними).

Судово-медична експертиза проводиться з метою дослідження на підставі спеціальних знань матеріальних об'єктів, що містять інформацію про обставини справи, яка перебуває в провадженні органів дізнання, слідчого, прокурора чи суду.

Бурхливий розвиток сучасних інформаційних технологій, як однієї із складових частин науково-технічного прогресу, обумовлений необхідністю отримання і використання інформації у зв'язку з підвищеною діловою активністю у всіх сферах діяльності людини.

Так, у судово-медичній експертній діяльності висока технологічність смартфонів з їх великими екранами (дисплеями)

і наявністю своїх графічних редакторів дозволяє створювати різноманітні схеми і рисунки для ілюстрації пошкоджень чи слідів на тілі людини, її одязі, кістках чи внутрішніх органах. Створений набір малюнків задовольняє практично всі запити судово-медичного експерта при його роботі як на місці пригоди, так і в умовах моргу чи лабораторії [2, 3].

Враховуючи те, що смартфон (комунікатор) є інтегральним засобом отримання і передачі інформації, слід передбачити, що такі функції можуть бути використані і в судовій медицині. Адже комп'ютерні можливості смартфонів повинні підтримувати комп'ютерні технології, які за останні десятиріччя набули свого широкого практичного втілення в судово-медичну практику.

Враховуючи те, що смартфон (комунікатор) є інтегральним засобом отримання і передачі інформації, слід передбачити, що такі функції можуть бути використані і в судовій медицині. Адже комп'ютерні можливості смартфонів повинні підтримувати комп'ютерні технології, які за останні десятиріччя набули свого широкого практичного втілення в судово-медичну практику. Слід врахувати, що смартфон є компактним приладом, наділеним різноманітними функціями як комп'ютера, так і цифрового засобу отримання і передачі інформації, тому особливо корисним може бути при огляді місця пригоди, при проведенні експрес-дослідження поза межами моргу чи судово-медичної лабораторії.

В сучасних смартфонах і комунікаторах реалізовані функції фото- і відеозйомки, тобто вони, водночас, є і камерофонами. Як відомо, якість фото- відеозйомки обумовлена роздільною здатністю матриці (тобто, кількістю пікселів на ній), якістю об'єктива, наявністю чи відсутністю функції автофокуса. Апріорі можна передбачити, що ці функції смартфона можуть бути використані, в першу чергу, при огляді місця події, особливо з метою фіксації плинних процесів, наприклад, зміни трупних плям при натискуванні на них з метою прогнозування часу настання смерті. Однак, такі роботи у доступній нам судово-медичній літературі одиничні, не систематизовані.

Таким чином, смартфон як сучасний високотехнологічний засіб комунікації, отримання і обробки різноманітної інформації, наділений значною кількістю функцій, які могли б бути використані при проведенні судово-медичних експертиз. Однак будь-яких відомостей про можливості використання смартфонів чи комунікаторів у судовій медицині та фаховій літературі нами не знайдено. Цей факт засвідчує актуальність та необхідність пошуків науково обґрунтованих підходів до вирішення проблеми застосування смартфонів у судово-медичній та, відповідно, криміналістичній практиці.

Так, сьогодні розроблені програми та набори рисунків (атласи) можуть бути широко використані в будь-якому бюро судово-медичної експертизи, що має персональний комп'ютер чи сучасний смартфон (комунікатор).

Функція електронної пошти (E-Mail) смартфона дозволяє передачу графічної (фотографії, рисунки, відео-файли) чи текстової інформації на будь-який стаціонарний комп'ютер, що підключений до Інтернет-мережі, або інший смартфон. Все це створює умови для використання широкої мережі передачі інформації між різними підрозділами бюро судово-медичної експертизи.

Відтворення обставин отримання травми можливе при експертному моделюванні процесу в ході проведення судово-медичної експертизи (без участі слідчого), що практикується при виконанні судово-медичних експертиз у відділенні судово-медичної криміналістики (в тому числі й комплексних). Результати відео-зйомки, записані смартфоном, можна переглянути на його екрані за допомогою вмонтованого програвача Real Player. Крім того є можливість перенесення файлу в комп'ютер за допомогою кабелю з'єднання або через бездротову передачу по Bluetooth.

Особливою функцією, яка вмонтована у смартфони, є підготовка і передача текстової інформації.

Важливим завданням є передача експертних документів особі, яка з ними ознайомлюється та їх опрацьовує. Найефективнішим

варіантом є відправка повідомлення по електронній пошті (E-Mail). Широко практикується надсилання «Актів судово-медичних експертиз» чи «Висновків експерта», у випадках, коли до Головного бюро судово-медичної експертизи МОЗ України надходять скерування судово-медичного експерта районного відділення чи обласного бюро судово-медичних експертиз. У Головному бюро виконується дослідження чи експертиза і складений експертний документ необхідно передати замовнику роботи на місця. Як показують результати дослідження, це значно скорочує час від проведення експертизи до його отримання замовником. Слід відзначити, що стримуючим фактором розповсюдження такого способу є відсутність смартфонів чи комунікаторів в обласних бюро судово-медичної експертизи. Такі апарати слід включати у перелік обов'язкового обладнання бюро судово-медичних експертиз [1].

Таким чином, сучасні смартфони (комунікатори) є багатофункціональними, інтегральними і компактними засобами отримання, обробки і оперативної передачі різноманітної інформації. Результати досліджень засвідчують доцільність використання смартфонів у практичній судово-медичній експертизі для виконання цілої низки завдань та відпрацювання за їх допомогою нових способів дослідження об'єктів судово-медичної експертизи.

Поєднання в смартфонах функцій мобільного телефону та комп'ютера, дозволяє складати спеціалізовані комп'ютерні програми діагностичного і довідкового спрямування, які можуть бути використані при проведенні судово-медичних досліджень і експертиз.

Компактність смартфонів, з вбудованим в них судово-медичним програмним забезпеченням, створює ефективну можливість експрес-діагностики стану трупа, ушкоджень, накладень і слідів на місці виявлення трупа або його частин. Адекватність і однозначне сприйняття програм стаціонарним комп'ютером і смартфоном дозволяє їх використання і в стаціонарних умовах роботи експерта - в морзі, чи у відділеннях лабораторії.

Вбудований графічний редактор смартфона забезпечує створення різноманітних схем, малюнків, графіків для формалізації ушкоджень і слідів як на місці події, так і в стаціонарних умовах роботи експерта. Складений атлас рисунків доповнює інформацію про судово-медичну характеристику таких об'єктів, сприяє об'єктивізації самого дослідження.

Цифрова відеокамера сучасного смартфона успішно забезпечує достатню якість фіксації плинних процесів, зокрема, послідовність змін трупних плям, і може бути використана на місці пригоди, при відтворенні обставин і умов спричинення травми та реконструкції події в цілому, експертному моделюванні процесу спричинення травми.

Отримана за допомогою смартфона інформація у вигляді результату роботи комп'ютерної програми, графічного зображення, відео-файла може бути використана в експертному документі. Смартфон, як один із сучасних швидкісних засобів передачі інформації, дозволяє зручно надсилати її для використання на стаціонарному комп'ютері за допомогою вбудованих у ньому засобів. Найбільш ефективною є передача інформації замовнику за допомогою електронної пошти.

1. Шавловський Г.С. Використання смартфонів і комунікаторів в судово-медичній експертизі / Г.С. Шавловський [Електронний ресурс] ... Режим доступу: https://www.kazedu.kz/referat/116104.
2. Інструкція про проведення судово-медичної експертизи: Затверджено наказом Міністерства охорони здоров'я України від 17.01.95 р. № 6.
3. Правила проведення судово-медичних експертиз (досліджень) у відділеннях судово-медичної токсикології бюро судово-медичної експертизи наказ Міністерства охорони здоров'я України від 17 січня 1995 року № 6.

Програмне та інформаційне забезпечення веб-орієнтованої системи автоматизованого дослідження теплових процесів

Синичак Степан Орестович,

здобувач ступеня магістра Національного лісотехнічного університету України

Використання чисельних методів в задачах тепло- і масообміну дозволяє вирішувати багато практичних завдань. Поява високопродуктивної обчислювальної техніки дозволяє в даний час розв'язувати нестаціонарні просторові задачі тепло- і масоперенесення [1].

Метою даної роботи стало розроблення програмного забезпечення для розв'язання задачі теплопровідності чисельними методами, а саме для двовимірного нестаціонарного рівняння теплопровідності проведено дослідження та реалізацію методу скінчених елементів.

Рівняння теплопровідності описує поширення тепла в заданій області простору в залежності від часу. Є параболічним диференціальним рівнянням в часткових похідних. У двовимірному випадку рівняння має вигляд:

$$\frac{\partial u}{\partial t} - \alpha\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2}\right) = f(x, y, t),$$

де a – коефіцієнт температуропровідності, $f(x, y, t)$ – функція теплових джерел, $u = u(x, y, t)$ – шукана функція, що задає температуру в точці з координатами (x, y) в момент часу t [2].

Розроблена програма розв'язує нестаціонарне двовимірне рівняння теплопровідності, використовуючи метод скінченних елементів в просторі і метод ліній в часі із неявним Ейлеровим наближенням для похідної за часом. Обчислювальна область являє собою прямокутник з однорідними граничними умовами Діріхле, прикладеними уздовж границі. Змінна $u(x, y, t)$ обмежується:

$u_t - \alpha(u_{xx} + u_{yy}) = f(x,y,t)$ – всередині моделі. У нашому випадку $f(x,y,t) = 0$;

$u(x,y,t) = g(x,y,t)$ для (x,y) на границі. У нашому випадку задається значення температури;

$u(x,y,t) = h(x,y,t)$ в початковий момент часу, аналогічно задається температура.

Основні кроки алгоритму [3]:

- Тріангуляція області. Обчислювальна область спочатку покривається прямокутним масивом точок nx на ny, створюючи (nx-1)*(ny-1) прямокутних субелементів. Кожен субелемент розділений на два трикутники, створюючи в загальній складності 2*(nx-1)*(ny-1) геометричних «елементів». Кожен трикутник визначається не тільки трьома кутовими вузлами, а й трьома додатковими серединними вузлами. Якщо ми врахуємо ці додаткові вузли, то в області тепер є всього (2*nx-1)*(2*ny-1) вузлів.
- Вибір базисних функцій трикутних елементів.
- Обчислення матриць жорсткості і вектора навантажень для скінченних елементів.
- Ансамблювання. Ансамблювання – це побудова матриці жорсткості для всієї області з матриць жорсткості одного скінченного елемента. При ансамблюванні матриці використовується нумерація вузлів розбиття області, нумерація вершин скінченних елементів (трикутників) і матриця жорсткості одного елемента.
- Задання граничних умов. Граничні умови представлені у вигляді умов Діріхле.
- Обчислення глобальних матриці жорсткості і вектора навантажень.
- Розв’язування СЛАР і отримання кінцевого результату.

Для розроблення графічного інтерфейсу програми було вирішено скористатись методами візуального програмування і класами бібліотеки Windows Forms. На рисунку 1 показано головне вікно програми.

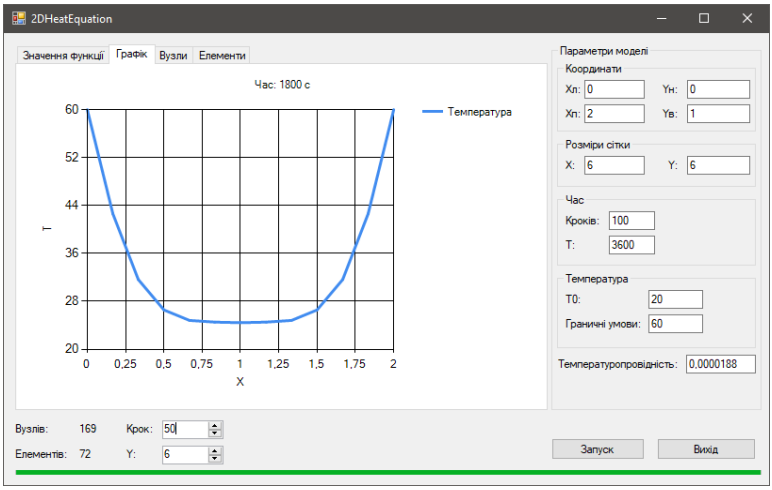


Рис. 1. Головне вікно програми

Як бачимо, інтерфейс програми дозволяє настроїти основні параметри моделі, такі як координати системи, розміри сітки, час і кількість кроків моделювання, початкову температуру і граничні умови, а також коефіцієнт температуропровідності. Кнопка «Запуск» починає моделювання. У нижньому лівому куті вікна візуалізації виводяться числові характеристики сітки – кількість вузлів та елементів. На вкладці «Значення функції» відображаються значення функції (температури) в кожному вузлі. На наступній вкладці виводиться графік температури по X на вибраному кроці при певному значенні Y. Значення кроку та Y регулюється, при цьому значення функції та графік візуалізуються динамічно. На наступних вкладках виводяться координати вузлів та нумерація вузлів для кожного елемента відповідно. Крім візуалізації, програма зберігає в файли списки вузлів та елементів, а також розв’язки задачі на кожному кроці для подальшої роботи в інших програмних комплексах.

Отже, в ході роботи було виконано аналіз предметної області, вибраних технологій та засобів проектування. Результатом є програмна реалізація методу скінченних елементів для розв’язування нестаціонарного рівняння теплопровідності в двовимірному просторі.

Обчислювана область представлена прямокутником із заданими координатами. Є можливість гнучкої настройки моделі за допомогою додаткових параметрів. Результати роботи програми виводяться у графічне вікно з одночасним записом в файли. Користувач має змогу переглянути результати моделювання на кожному кроці, а також характеристики побудованої сітки — кількість і координати всіх елементів. Програма розроблена мовою програмування C# середовищі Microsoft Visual Studio 2017.

1. Крайнов А.Ю., Миньков Л.Л. Численные методы решения задач тепло- и массопереноса : учеб. пособие. – Томск : STT, 2016. – 92 с.
2. Уравнение теплопроводности [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Уравнение_теплопроводности
3. Метод скінченних елементів [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Метод_скінченних_елементів

Використання технічних засобів у дистанційному досудовому розслідуванні

Сокиран Федір Михайлович,

професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент

В листопаді 2012 року набрав чинності новий Кримінальний процесуальний кодекс України від 13 квітня 2012 р. № 4651-VI підписаний Президентом України 13 квітня 2012 року.

Основним завданням нового Кримінального процесуального кодексу України є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до

відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура.

Новий КПК містить чимало нововведень, і в першу чергу покликаний зрівняти права та обвинувачення в кримінальному процесі.

Одним із таких новаторських є положення нового КПК, що передбачають можливість проведення досудового розслідування дистанційно, використанням сучасних телекомунікаційних можливостей, наприклад відеоконференції.

Так, відповідно до ст. 232 КПК запроваджено можливість проведення допиту, впізнання у режимі відеоконференції під час досудового розслідування.

Допит осіб, впізнання осіб чи речей під час досудового розслідування можуть бути проведені у режимі відеоконференції при трансляції з іншого приміщення у випадках:

- неможливості безпосередньої участі певних осіб у досудовому провадженні за станом здоров'я або з інших поважних причин;
- необхідності забезпечення безпеки осіб;
- проведення допиту малолітнього або неповнолітнього свідка, потерпілого;
- необхідності вжиття заходів для забезпечення оперативності досудового розслідування;
- наявності інших підстав, визначених слідчим, прокурором, слідчим суддею достатніми.

Рішення про здійснення дистанційного досудового розслідування приймається слідчим, прокурором, а в разі здійснення у режимі відеоконференції допиту згідно із статтею 225 КПК (допит свідка, потерпілого під час досудового розслідування в судовому засіданні) – слідчим суддею з власної ініціативи або за клопотанням сторони кримінального

провадження чи інших учасників кримінального провадження. У разі, якщо сторона кримінального провадження чи потерпілий заперечує проти здійснення дистанційного досудового розслідування, слідчий, прокурор, слідчий суддя може прийняти рішення про його здійснення лише вмотивованою постановою (ухвалою), обґрунтувавши в ній прийняте рішення. Рішення про здійснення дистанційного досудового розслідування, в якому дистанційно перебуватиме підозрюваний, не може бути прийнятим, якщо він проти цього заперечує.

Використання у дистанційному досудовому розслідуванні технічних засобів і технологій повинно забезпечувати належну якість зображення і звуку, а також інформаційну безпеку. Учасникам слідчої (розшукової) дії повинна бути забезпечена можливість ставити запитання і отримувати відповіді осіб, які беруть участь у слідчій (розшуковій) дії дистанційно, реалізовувати інші надані їм процесуальні права та виконувати процесуальні обов'язки, передбачені КПК.

Крім, того, з метою забезпечення оперативності кримінального провадження, чинний КПК дає можливість слідчому, прокурору проводити опитування в режимі відео- або телефонної конференції. Підставами для цього є знаходження особи у віддаленому від місця проведення розслідування місці, хвороба, зайнятість чи інші причини, з яких особа не може без зайвих труднощів прибути своєчасно до слідчого, прокурора.

У результаті проведення опитування з використанням відео- та телефонної конференції, уповноважена особа складає рапорт, у якому зазначає дату та час опитування, дані про особу опитуваного, дані про те, яким чином була підтверджена особа опитуваного, ідентифікаційні ознаки засобу зв'язку, що використовувався опитуваним, а також обставини, які були ним повідомлені.

Обов'язкової фіксації опитування за допомогою технічних записів аудіо- та відеозаписи не передбачається, вона проводиться в разі потреби. Визначення необхідності фіксації – це виключна компетенція слідчого, прокурора, тоді як право

опитуваного заявити таке окреме клопотання або самому використовувати такі засоби в новому КПК не передбачено.

Резюмуючи вищезазначене, слід сказати, що можливість проведення дистанційного досудового розслідування із застосуванням допомогою відео-, телефонної конференції є закономірним кроком по впровадженню в кримінальний процес сучасних технологій зв'язку та фіксації інформації. Це дозволяє заощаджувати сили, час і кошти всіх учасників досудового провадження.

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI // Відомості Верховної Ради України. – 2013. – № 9-10, № 11-12, № 13. – Ст. 88.
2. Кримінальний процесуальний кодекс України. Науково-практичний коментар / За заг. ред. професорів В.Г. Гончаренка, В.Т. Нора, М.Є. Шумила. – К.: Юстиніан, 2012. – 1224 с.
3. Михальчук Т.В. Особливості проведення окремих слідчих (розшукових) дій у режимі відеоконференції / Т. В. Михальчук // Криминалистика и судебная експертиза. – 2013. – Вип. 58(1). – С. 138-144.

Окремі аспекти застосування законодавства про доступ до конфіденційної інформації

Тимчишин Тарас Михайлович,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. У свою чергу, інформація з обмеженим доступом за своїм правовим режимом поділяється на таємну і конфіденційну.

Проте різні закони дають не однакове визначення конфіденційної інформації.

Згідно з ч.1 ст. 7 Закону «Про доступ до публічної інформації» конфіденційна інформація − це інформація, доступ до якої

обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [1].

В свою чергу ч. 2 ст. 21 Закону «Про інформацію», за якою конфіденційною є інформація про фізичну особу незалежно від відповідного її волевиявлення [2].

Для усунення колізії наведених норм суди повинні застосовувати положення частини четвертої ст. 9 Кодексу адміністративного судочинства України, за якою у разі встановлення невідповідності закону Конституції України суд застосовує правовий акт, який має вищу юридичну силу, тобто Конституцію України, а саме положення про те, що інформація про особу є конфіденційною, крім окремо визначених [3].

Виходячи з положень Закону «Про доступ до публічної інформації», Закону «Про інформацію» та ст. 32 Конституції України конфіденційна інформація може поширюватись у таких випадках:

- коли особа самостійно встановила випадки (порядок, умови), коли ця інформація може поширюватись;
- коли особа у відповідь на прохання/пропозицію дає згоду на використання своїх конфіденційних даних. При цьому використання таких даних третьою особою здійснюється лише за згодою власника конфіденційних даних;
- коли закон чітко дозволяє певним суб'єктам отримувати та використовувати конфіденційну інформацію без згоди особи;
- коли розголошення конфіденційної інформації відповідає суспільному інтересу і право громадськості знати цю інформацію переважає шкоду, яку може бути завдано особі поширенням її конфіденційної інформації.

Необхідно зауважити, що вказане положення ч. 1 ст. 7 Закону Про доступ до публічної інформації не передбачає можливості для суб'єктів владних повноважень відносити інформацію до конфіденційної. Такі суб'єкти можуть лише обмежувати доступ

до інформації шляхом віднесення її до службової або таємної відповідно до закону.

Розпорядники інформації, такі як суб'єкти владних повноважень, що є юридичними особами, що фінансуються з державного чи місцевих бюджетів, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди − лише в інтересах національної безпеки, економічного добробуту та прав людини.

Такі положення узгоджуються з положеннями ст. 32 Конституції України, відповідно до якої не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Інформація може бути поширена за умови, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Вбачається, що з урахуванням положень Закону «Про доступ до публічної інформації» та Конституції України, інтереси громадськості, у яких конфіденційна інформація може бути поширена, є лише інтереси національної безпеки, економічного добробуту та прав людини.

Такий підхід також відповідає ст. 8 Конвенції про захист прав людини і основоположних свобод, відповідно до якої втручання у право на приватність особи можливе, якщо воно ґрунтується на законі, переслідує легітимну мету та є необхідним у демократичному суспільстві [4].

У ст. 12 Загальної декларації прав людини 1948 року встановлено, що ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист законом від такого втручання або таких посягань [5].

Також у ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 року визначено, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції; органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб [6].

Осторонь також не лишився Міжнародний пакт про громадянські і політичні права 1966 року де в п. 1 ст. 17 встановлено, що ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію [7].

Таким чином, відмова у надати інформації є вмотивованою у разі, якщо розпорядник в листі вказує, якому саме з інтересів загрожує розголошення інформації, що запитується, та в чому полягає істотна шкода цим інтересам від її розголошення, або чому шкода від оприлюднення такої інформації переважає право громадськості знати цю інформацію в інтересах національної безпеки, економічного добробуту чи прав людини.

1. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI / [Електронний ресурс]. – Режим доступу: http: http://zakon2.rada.gov.ua/laws/show/2939-17
2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12
3. Кодекс адміністративного судочинства від 06.07.2005 № 2747-IV / [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2747-15
4. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 / [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/995_004

5. Загальної декларації прав людини від 10.12.1948 / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_015
6. Конвенції про захист прав людини і основоположних свобод від 04.11.1950 / [Електронний ресурс]. – Режим доступу: http:// http://zakon2.rada.gov.ua/laws/show/995_004
7. Міжнародний пакт про громадянські і політичні права від 16.12.1966 / [Електронний ресурс]. – Режим доступу: http:// http://zakon3.rada.gov.ua/laws/show/995_043

Розробка фотоконтролера для безпеки особи (на прикладі виявлення несанкціонованого проникнення і мінування автомобіля)

Хомин Оксана Йосипівна,

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

Смичок Василь Дмитрович,

старший викладач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук

Протягом останніх років все більше ми чуємо про замінування та вибухи автомобілів цивільного населення, працівників правоохоронних органів, військовослужбовців ЗС України і т. п. Злочинці використовують як відомі, так і нові і перспективні матеріали і технології в якості вибухових речовин і методів їх приведення в дію «активації». Однією з причин неможливості попередження злочину є відсутність інформації про несанкціоноване проникнення і можливе мінування автомобіля.

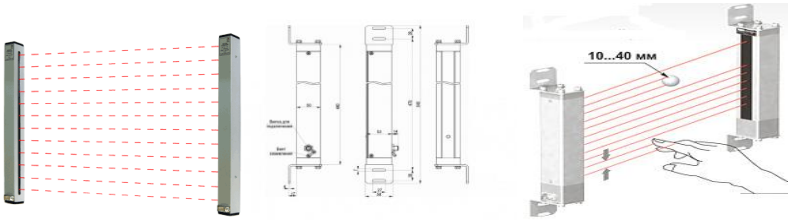
Проблема мінування автомобіля стала важливою умовою забезпечення безпеки особи тому, що її вирішення, в основному, залежить від зусиль самої особи, яка користується транспортним засобом. Після серії зухвалих вбивств за допомогою замінування автомобіля, вважаємо, забезпечення безпеки особи є вкрай актуальним.

Незважаючи на багатий і добрий досвід отримання інформації щодо проникнення (з можливим замінуванням), як в Україні так і закордоном (існують сотні типів систем безпеки – сигналізації) питання залишається відкритим. Володіючи сучасними інформаційними технологіями та електронним обладнанням можна забезпечити користувача автомобіля інформацією про несанкціоноване проникнення і можливе мінування автомобіля [1].

Актуальність теми спонукає авторів продовжити дослідження та запропонувати теоретичну розробку алгоритмічного електронного засобу виявлення несанкціонованого проникнення і можливого мінування на прикладі автомобіля. В даному випадку дослідження стосується оптичних методів та способів захисту від проникнення, а саме встановлення фотобар'єра [2, 3].

Принцип роботи та технічні характеристики сучасних фотобар'єрів дозволяють забезпечити надійною інформацією на стоянці про «небажані, або випадкові» проникнення до автомобіля, що дозволить попередити можливість його мінування.

Ми розглянемо фотобар'єр серії PJ2, що складається із світлових завіс безпеки. Це оптоелектронне обладнання, яке містить стійки із багатопроменевою системою джерела інфрачервоного випромінювання та приймача власного випромінювання Рис. 1 а, б, в).



а) *б)* *в)*

Рис.1 а, б, в). Конструкція стійки багатопроменевого випромінювача і приймача (а, б), та принцип роботи світлової завіси (в)

На рис. 1 а, б, в показана структура і принцип дії типового фотобар'єра на прикладі серії PJ2, де: а) випромінювач і приймач фотобар'єра, б) принцип побудови випромінювача,

приймача і захисного ковпака та принцип роботи і передачі променів досліджуваного фотобар'єра в).

Схема підключення типового фотобар'єра показана на Рис. 2. На рисунку видно, що для роботи в штатному режимі необхідною умовою являється підключення точки – 2 інфрачервоного (ІЧ) приймача із точкою – 2 (ІЧ) передавача.

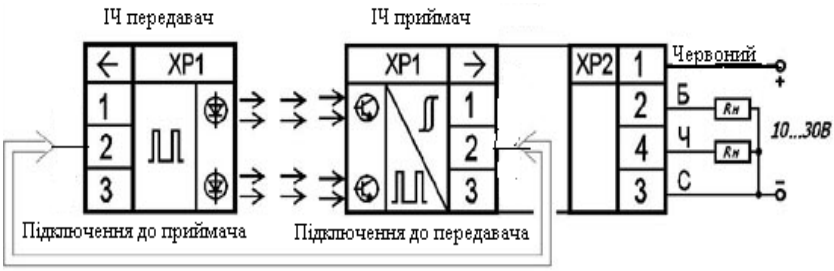


Рис. 2. Схема підключення (ІЧ) приймача з (ІЧ) передавачем та електроживлення

Принцип роботи фотобар'єра полягає у наступному:

1. Захисна зона (в даному випадку автомобіль) знаходиться між інфрачервоним випромінювачем 1 та приймачем 2 розробленого бар'єра.

2. Інфрачервоний світловий потік направлений від випромінювача на приймач створюючи, таким чином, підконтрольну площину Рис 3.

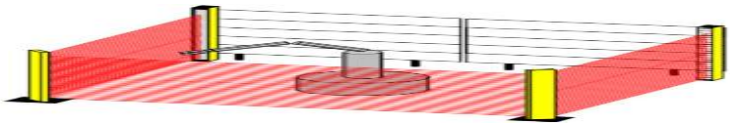


Рис 3. Приклад: підконтрольна площина (по периметру) багатопроменевого (ІЧ) фотобар'єра серії PJ2

3. Висота контрольованої зони у даному випадку суттєвого значення немає, але обмежена лише конструктивними особливостями і можливістю її встановлення (Рис. 1 б.). В залежності від рівня необхідної безпеки може становити від 4 до 124 промені, крок (віддаль) між променями можливо, також

змінювати з кроком 10–20 або 40 мм. Це мінімальна віддаль яку можна контролювати. По дальності дії (відстань між стійками (Рис. 1 а.) можна змінювати (в залежності від конфігурації), але з кроком не більшим від 10,0 м. (Рис. 1 в.)

Недоліком у використанні такого багатопроменевого фотобар'єра являються саме контактне підключення стійки багатопроменевого випромінювача і приймача, які, як відомо, є демаскуючим елементом невидимих (ІЧ) променів.

Враховуючи демаскуючі фактори в стаціонарному режимі роботи фотобар'єрів, а також відсутність інформації про несанкціоноване наближення до автомобіля та контроль його стану, виникає необхідність розробки іншого типу – фотоконтролера.

Фотоконтролер дозволить вирішити проблему з якою зустрічається кожен водій – забезпечити себе інформацією про несанкціоноване проникнення і можливе мінування автомобіля в період відсутності стаціонарного контролю, в режимі експлуатації і в місцях не передбачених і не обладнаних штатними та стаціонарними засобами безпеки.

Запропонований авторами пристрій за своїм принципом роботи фотоконтролера так само, як і фотобар'єри базується на передачі і прийомі інфрачервоних імпульсів та реєстрації проникнення в площину контролю.

Особливість принципу роботи фотоконтролера полягає у тому, що пропонований пристрій реєструє «розсіяне» світло (ІЧ) променів з одного місця. Рис.4.

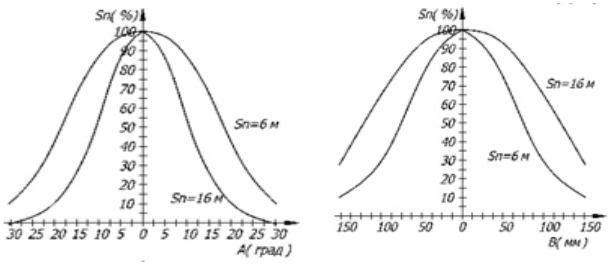
Рис.4. Принцип роботи фото контролера

Отже, кожна зацікавлена в своїй безпеці особа має можливість взяти під контроль свій автомобіль в зручному для неї місці. При умові, що фотоконтролер розміщено тактично правильно (відповідно до умов експлуатації), власник отримує необхідну йому інформацію про рівень безпеки свого автомобіля. Така інформація дає можливість заповнити часові проміжки відсутності контролю над автомобілем.

Авторами теоретично розроблено модифікацію фотомагнітного контролера, який при необхідності встановлюється на даху кузовної частини автомобіля. На Рис. 5 (а, б) показана апертура фотопроменів на відстані 16 та 6 м.

На Рис 5 видно дальність дії і кут розгортки діаграми (16 і 6 м), які дозволяють взяти під інформаційний контроль 5/6 частин периметру автомобіля і частину прилеглої до нього території.

Перевагою даного фотоконтролера є те, що він утворює об'ємний безперервний інфрачервоний фон по всьому об'єму автомобіля на відміну від багатопроменевого фотобар'єру, який підконтрольною утворює лише площину по периметру встановлення стійки передавачів та приймачів.



а *б*

Рис 5 Апертури фото променів

Висновок: Автори дослідження провели аналіз методів фотобар'єрного захисту, сенсорів існуючих інформаційних систем та методів виявлення і фіксації проникнення (замінувань). В результаті дослідження зроблено висновок, що станом на даний час актуальною є проблема створення не

стаціонарного, а портативного, переносного і бажано малогабаритного автомобільного детектора наявності факту (злісного) наближення, або проникнення в автомобіль.

1. Смичок В.Д., Хомин О.Й. Розробка алгоритмічного електронного засобу виявлення замінування автомобіля як засіб забезпечення безпеки. // Збірник тез Міжнародної науково-практичної конференції «Теорія та практика протидії злочинності в сучасних умовах. 10 листопада 2017 р Львів. с.225-227.
2. Хорев А. А. Методы и средства поиска электронных устройств перехвата информации / А. А. Хорев. – М. : МО. – 1998. – 224 с.
3. Горбачев А. А. Признаки распознавания нелинейных рассеивателей электромагнитных волн / А. А. Горбачев, А. П. Колбанов, С. П. Тараканков, С. В. Ларцов, Е. П. Чигин // Нелинейный мир. – 2004. – № 5-6. – с. 301-309.

Модернізація систем наведення озброєння броньованих машин на основі застосування енергетично оптимізованого асинхронного електроприводу

Шабатура Юрій Васильович,

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

Вільман Ігор Михайлович,

здобувач ступеня бакалавра Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

На сьогоднішній день основним видом озброєння підрозділів силових відомств України за фізичним принципом функціонування є вогнепальна зброя. Ефективність застосування даної зброї перш за все визначається швидкістю і точністю її наведення на ціль. Для здійснення наведення зброї, яка встановлена на броньованих машинах широко застосовуються електромеханічні приводи. Дані приводи, як правило

виконуються на основі використання двигунів постійного струму. Такі двигуни повністю забезпечують необхідну точність і швидкість наведення озброєння, однак поряд цим вони мають і ряд недоліків. Зокрема, електродвигуни постійного струму через наявність щітково-колекторних вузлів потребують періодичного огляду та чистки таких вузлів, а при значному зносі необхідно виконувати заміну щіток. Також необхідно враховувати і ту обставину, що ці вузли є джерелом радіозавад. Це знижує надійність такого приводу і відповідно усієї боєготовності броньованої машини. Крім того двигуни постійного струму є менш енергетично ефективними в порівнянні з асинхронними двигунами (АД).

Вимога максимальної енергетичної ефективності і надійності в експлуатації електроприводу систем наведення озброєння броньованих машин дозволяє сформулювати ряд основних принципів щодо його модернізації:

- електропривод систем наведення озброєння броньованих машин при модернізації доцільно виконувати регульованим на основі системи «тиристорный регулятор напруги – асинхронний двигун», побудованої на основі використання силових тиристорів;
- мінімізацію втрат в електроприводі слід виконувати за рахунок погодження навантаження та напруги двигуна приводу систем наведення;
- для зменшення витрат на модернізацію електроприводів систем наведення озброєння броньованих машин можливе збереження основного силового електрообладнання;
- систему контролю і управління модернізованим електроприводом доцільно виконати на базі мікропроконтролера, що дозволить узгодити керування електроприводом системи наведення озброєння броньованих машин з існуючими комп'ютерними системами керування рухом і вогнем броньованих машин.

Виходячи з принципів маловитратної модернізації, досліджені існуючі електроприводи, які побудовані за системою «тиристорний регулятор напруги – асинхронний двигун», та дозволяють

підвищити енергетичні характеристики роботи недовантаженого асинхронного двигуна за різними критеріями мінімізації втрат електричної енергії.

Оптимізувати втрати у електроприводі можливо за рахунок підтримання швидкості обертання АД на рівні оптимального ковзання *Sопт*. При мінімізації втрат електроприводу оптимальне ковзання *Sопт* визначається відповідно з формулою:

$$S_{\text{опт}} = \frac{R_2\sqrt{\left(\frac{x^2}{R_\mu}+R_1\right)/(R_2+R_1)}}{X_{\text{к.з.}}},$$

де R_1 і R_2 – активний приведений опір статора та ротора АД відповідно; R_μ – активний опір контуру намагнічування АД; X_{μ}, $X_{к.з.}$ – реактивний опір контуру намагнічування та короткого замикання АД відповідно.

При максимізації коефіцієнту потужності асинхронної машини значення оптимального ковзання *Sопт* буде визначатися відповідно до формули:

$$S_{\text{опт}} = \frac{R_2\left(R_1+\sqrt{R_1^2+X_\mu X_{\text{КЗ}}}\right)}{X_\mu X_{\text{КЗ}}}.$$

Найбільш раціональним методом оптимізації для електроприводу системи наведення озброєння броньованих машин, при якому не виникає потреба у використанні додаткових давачів для вимірювання швидкості є критерій мінімуму струму статора АД. Для кожного значення моменту опору навантаження при постійній швидкості обертання існує оптимальний режим роботи, який характеризується мінімальним струмом споживання АД. Це дозволяє мінімізувати втрати електричної енергії в електроприводі на основі АД за рахунок контролю лише двох параметрів – струму і напруги.

Співставлення різних критеріїв мінімізації та способів керування приводять до висновку щодо доцільності розробки

функціональної схеми енергоресурсозберігаючого електроприводу системи наведення озброєння броньованих машин, яка включає в себе регулятор на нечіткій логіці (фаззі регулятор). Зображення запропонованої функціональної схеми наведено на рисунку 1.

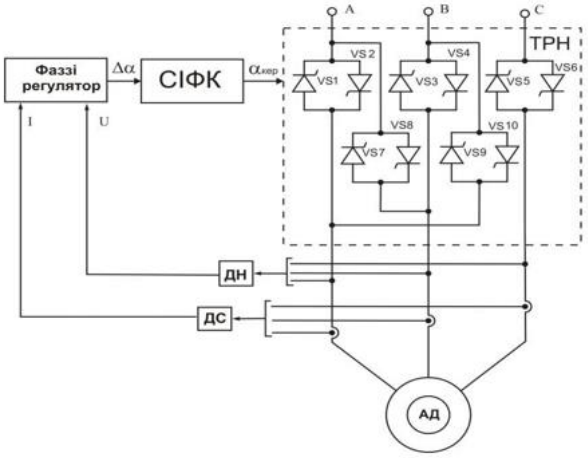


Рис.1. Запропонована функціональна схема електроприводу.

На наведеній схемі використані наступні позначення: СІФК – схема імпульсно-фазового керування тиристорами; ДН – датчик напруги; ДС – датчик струму; ТРН – тиристорний регулятор напруги.

Використання нечіткої логіки в керуванні електроприводами дає можливість будувати енергоефективні системи без застосування громіздкого математичного опису режимів роботи електромеханічних систем. Електропривод ТРН-АД є нелінійною системою із взаємозв'язаними електромагнітними процесами в обмотках АД, тому врахування впливу електрорушійної сили у безструмових інтервалах на напругу та струм в сусідніх фазах ускладнює розрахунок. Нечіткі моделі є значно простішими для апаратної реалізації порівняно з класичними алгоритмами керування.

Для практичного здійснення алгоритму пошуку мінімуму струму статора АД згідно з його U-подібними

характеристиками, фаззі регулятор повинен оцінювати зміну струму ΔI та напруги ΔU на кожному кроці розрахунку для чого запропонована структурна схема (рис. 2) до якої введено блоки одиничної дискретної затримки z^{-1} для розрахунку вхідних значень фаззі регулятора ΔI та ΔU та значення корегування кута керування тиристорами Δα.

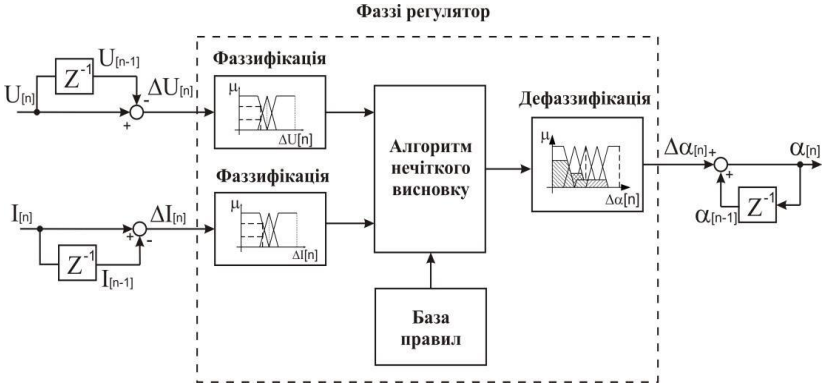


Рис.2. Структурна схема фаззі регулятора.

Найбільш важливою частиною даного регулятора, яка забезпечує «інтелектуальне» прийняття рішення є база правил. Вона розробляється виходячи із задачі оптимізації енергоспоживання електроприводу шляхом знаходження мінімуму струму статора на основі залежності струму статора АД від напруги.

На завершення необхідно зазначити, що дана система є системою підпорядкованого управління нижнього рівня, яка забезпечує мінімізацію енергетичних втрат при виконанні задачі наведення озброєння, при цьому вирішення задач досягнення необхідної точності і швидкості наведення забезпечується системою верхнього рівня управління.

1. Изосимов Д.Б., Козаченко В.Ф. Алгоритмы и системы цифрового управления электроприводами переменного тока //Электротехника. 1999. №4. с.41-51.

2. Хашимов А.А. Энергосберегающие системы автоматизированного электропривода переменного тока //Электротехника. 1995. №11. с.34-39.
3. Луговой А.В. К теории энергосбережения средствами промышленного электропривода// Электротехника. 1999. № 5. с. 62-67
4. Браславский И.Я. Энергосберегающий асинхронный электропривод: учеб. пособие для студ. высш. учеб. заведений / И.Я. Браславский, З.Ш. Ишматов, В.Н. Поляков; под ред. И.Я. Браславского. М.: Издательский центр «Академия», 2004. – 256 с.

Програмно-технічна модернізація двигунів внутрішнього згоряння спецтехніки та зразків озброєння військової техніки

Шабатура Юрій Васильович,

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

Гера Володимир Ярославович,

ад'юнкт Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Повноцінне функціонування силових структур держави в сучасну епоху неможливе без застосування різноманітних засобів пересування серед яких найбільш поширеними є автомобілі. Автомобільна техніка застосовується як при виконані спеціальних завдань так і у повсякденній діяльності підрозділів. Основою енергетичної системи більшості сучасних автомобілів є і очевидно ще досить довго залишатиметься – двигун внутрішнього згоряння (ДВЗ).

Це достатньо складний пристрій, який після свого винайдення за два з половиною століття постійно удосконалювався. Для тривалої і надійної роботи двигуна вкрай необхідне якісне змащування його робочих поверхонь, які зазнають великих механічних і теплових навантажень перебуваючи в обертальному або ковзному контакті під час відносного руху.

Оптимальне змащування забезпечує збереження ресурсу робочих деталей, очищення і відведення механічних відпрацьованих домішок та часткове охолодження двигуна. Усі вище зазначені функції в ДВЗ виконує система його змащування.

На даний час двигуни внутрішнього згоряння, які використовуються в спецтехніці, зразках озброєння та військової техніки, які знаходяться в експлуатації в силових відомствах держави, оснащуються механічними системами змащування. Механічна система змащування є доволі простим, надійним і достатньо ефективним вирішенням задачі змащування двигуна, однак вона не позбавлена ряду недоліків. В основі цієї системи змащування ДВЗ лежить використання обладнана механічного (шестирінчастого) масляного насосу, який приводиться в рух безпосередньо від колінчастого валу, таким чином продуктивність такого насосу пропорційно залежить від частоти обертів колінчастого валу двигуна. Як показали проведені дослідження такі системи змащування не в спромозі забезпечити оптимальний режим змащування ДВЗ в широкому діапазоні зміни навантажувальних та температурних режимів роботи двигуна.

Однією з найгостріших проблем, яка потребує вирішення це «холодний пуск» ДВЗ. Після тривалої зупинки двигуна масло з робочих поверхонь механічних зчленувань, в тому числі і найбільш відповідальних, які зазнають найбільших механічних навантажень, стікає під дією сили тяжіння, тим самим залишаючи робочі деталі без достатньої кількості масла. Таким чином, перші робочі ходи багатьох вузлів ДВЗ проходять в умовах гострої «масляної недостатності» внаслідок чого надмірні витрати енергії потребуються для запуску двигуна і відбувається інтенсивне зношування відповідальних вузлів, це приводить не тільки зменшення надійності і ресурсу двигуна, але і до погіршення його експлуатаційних характеристик. Приведені аргументи добре ілюструються наведеним на рис. 1 графіком.

Наступна проблема, яку в принципі не може вирішити механічна система змащування, це необхідність для забезпечування оптимального режиму змащування, за умови зміни в широкому діапазоні температури та в’язкості моторного

масла, забезпечувати нелінійну зміну тиску масла в залежності від навантаження двигуна.

Рис 1. Залежність тиску масла від кількості обертів колінчастого валу ДВЗ.

Експерименти і практичний досвід переконливо засвідчують, що під час запуску в холодному двигуні в'язкість масла є високою, внаслідок цього тиск масла в двигуні росте, однак на робочих поверхнях багатьох відповідальних вузлів його ще недостатньо, це призводить до погіршення роботи ДВЗ в цілому, а також при цьому відбувається інтенсивне зношування деталей. Апроксимація експериментальних даних відображена на рис. 2.

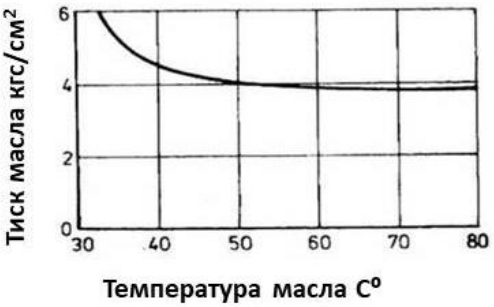


Рис. 2. Залежність тиску масла від температури

Графічне відображення зміни коефіцієнта тертя відповідно до умов зміни режимів змащування в ДВЗ показано на діаграмі Герсі-Штрібека, яка наведена на рис. 3.

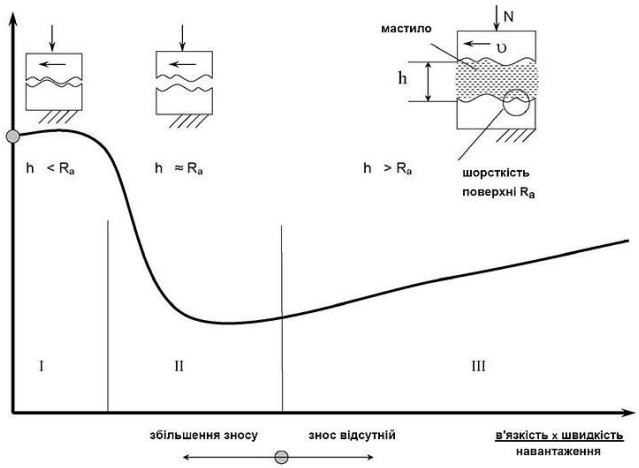


Рис. 3. Діаграма Герсі-Штрібека

На даній діаграмі можна чітко виділити три режими змащування: гідромеханічний, граничний, змішаний.

При граничному режимі змащування (область I) поверхні деталей контактують між собою. Знос деталей є максимальним.

При гідродинамічному режимі змащування (область III) поверхні деталей повністю роз'єднані шаром масла. Тертя між ними зумовлене об'ємними властивостями. Знос деталей відсутній, але відбуваються перевитрати моторного масла.

При змішаному режимі змащування (область II) ділянки робочих поверхонь двигуна знаходяться між режимами гідродинамічного та граничного режиму змащування. Відстань між поверхнями є порівнювана до величин їх шорсткості. Цей режим і є оптимальним режимом змащування ДВЗ.

Для забезпечення оптимального режиму змащування ДВЗ запропонована керована мікроконтролером електромеханічна система змащування, яка завдяки програмному забезпеченню є адаптивною і здатною до самонастроювання з врахуванням усіх умов експлуатації і факторів впливу. Структурно-функціональна схема запропонованої системи наведена на рис. 4.

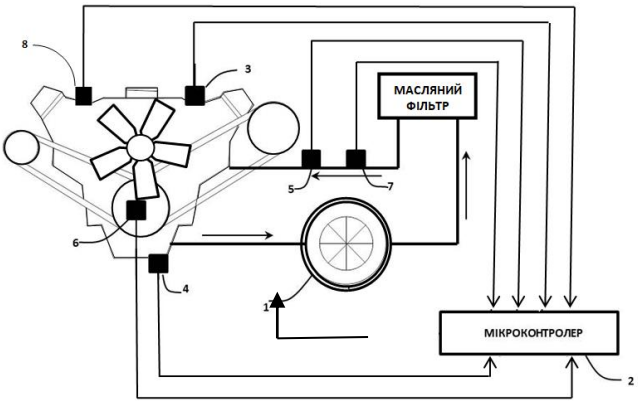


Рис. 4. Електромеханічна система змащування ДВЗ

Застосування даної системи не потребує значних змін в конструкції двигуна автомобіля. Пропонується на штатному місці замірного щупа для визначення рівня масла встановити додаткову масляну магістраль, яка буде з'єднана з електричним масляним насосом (1), роботою даного насосу буде керувати мікроконтролер (2), який отримуватиме інформацію про фізико-механічні властивості масла за допомогою сенсорів: температури (3), густини (4), якості масла (5), навантаження двигуна (6), тиску масла (7), кількості обертів колінчастого валу двигуна (8). Мікроконтролер на основі об'єктивної інформації з сенсорів завдяки інтелектуальному програмному забезпеченню буде здійснювати управління електричним масляним насосом таким чином, щоб постійно забезпечувати оптимальний для двигуна змішаний режим змащування.

Таким чином використання програмно керованої мікроконтролерної електромеханічної системи змащування двигуна внутрішнього згоряння значно підвищить надійність, економічність і ефективність в процесі запуску, роботи і зупинки двигуна внутрішнього згоряння і збільшить ресурс його експлуатації, а також призведе до покращення технічних характеристик в роботі двигуна, та до зменшення витрати пального і масла.

1. Альмеев Р.И., Денисов А.С. Анализ влияния параметров системы смазки на режим работы подшипников коленчатого вала при холодном пуске двигателя // Научно-техническое творчество: проблемы и перспективы: сб. статей IV Всерос. науч.-техн. конф.-семинара: в 2 ч. Ч. 2. Самара: Самар. гос. техн. ун-т, 2009. С. 35-46.
2. Аулін В.В. Вплив режимів тертя в основних сполученнях деталей на механічні втрати в ДВЗ / В.В. Аулін, С.В. Лисенко, О.В. Кузик // Вісник інженерної академії України. – 2011. – № 2. – С. 200-204.
3. Аулін В.В. Дослідження властивостей моторної оливи в процесі експлуатації дизелів / В.В. Аулін, С.В. Лисенко, О.В. Кузик // Конструювання, виробництво та експлуатація с/г машин : загальнодержавний міжвідомчий науково-технічний збірник. – Кіровоград : КНТУ, 2009 р. – Вип.39. – С. 274-280.

Модернізація системи наведення артилерійського озброєння самохідної гаубиці 2С3М на основі застосування методів математичної обробки сигналів кутовимірювальних сенсорів

Шабатура Юрій Васильович,

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

Снітков Костянтин Ігорович,

ад'юнкт Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

Самохідні артилерійська установка (САУ), у порівнянні з причіпною гарматою володіє підвищеною бойовою ефективністю за рахунок збільшення рухомості, маневреності, а також постійної та швидкої готовності до відкриття вогню, що досягається за рахунок застосування електроприводу системи наведення гармати. Разом з тим інформацію про поточний стан електроприводу, зокрема, узгодження прицілу та гармати, надається від давачів зворотних зав'язків, які на сьогоднішній день є примітивними та недостатньо прецизійним враховуючи сучасний розвиток електроніки та техніки.

За положення ствола, узгодженого з установками прицілу відповідає вузол узгодження, який призначений для забезпечення візуального контролю встановлення ствола на кут підвищення, що відповідає установкам прицілу. Вузол узгодження складається із: вузла індукційного давача; вузла механічного дублера; щитка узгодження.

Вузол індукційного давача призначений для узгодження положення ствола з кутом підвищення, який установлений на прицілі. Він має статор, жорстко зв'язаний з головною віссю прицілу, та ротор, який має кінематичний зв'язок із вузлом гарматної частини.

При введенні в приціл кутів підвищення разом із головною віссю прицілу повертається статор індукційного давача відносно ротора, внаслідок чого в обмотках ротора наводиться ЕРС – сигнал неузгодженості, величина якого залежить від кута повороту статора, а фаза – від напрямку повороту.

При наведенні ствола у вертикальній площині повертається ротор індукційного давача відносно статора, і коли їх обмотки займуть одна відносно іншої початкове положення, індукується ЕРС згідно з [1] приблизно стає рівною нулю, тобто сигнал неузгодженості зникне про що свідчить трьохлампова індикація на щитку узгодження.

Відомо, що індукційні давачі, які використовуються в даних системах характеризуються значною похибкою яка сягає 3÷5 кутових хвилин. Дана похибка визначається внаслідок значного рівня шумів та залишковим гістерезисом. В зв'язку з цим наведення гармати буде відбуватись з відповідною похибкою, що в свою чергу призведе до відхилення польоту снаряду при пострілі. Для прикладу, відповідно до таблиць стрільб [2] виконання пострілу на повному заряді на дальність 4000 м на неузгодженому стволі гармати із прицілом, попадання снаряду в цілі відбудеться з характерною похибкою розмах якої може сягати близько 100м. Для узгодженості ствола гармати з прицілом необхідно виконувати їх вивірку після кожного здійснення маршу та пострілу. Проведення вивірки прицілу з

стволом гармати потребує спеціальних приладів, інструментів та затрати часу. Для зменшення часу та уникнення використання спеціальних приладів для приведення гармати в готовність до пострілу необхідно модернізувати дану систему.

Модернізацію даної системи можна здійснити різними методами, одним з яких є отримання високоточного вихідного сигналу з давача кута, а оцифрований його сигнал надасть змогу отримувати кутове положення ствола у реальному часі.

Одним із варіантів отримання високоточного сигналу, є застосування у даних системах оптичного енкодера, або магнітного енкодера. Оптичний енкодер перетворює рух в цифрові значення. Кожне кутове положення перетворюється на виході як цифрове значення. Завдяки цим значенням можна визначити кутові переміщення і визначити положення. Але попри всі переваги, енкодер має ряд недоліків, які ускладнюють його використання в системах озброєння та військовій техніці. Зокрема їх робота при занадто важких зусиллях які впливають на вал, не допускається наявність вологості при експлуатації, малий діапазон робочих температур, чутливість до вібрації, ударів або інших фізичних впливів, висока вартість давача. Недоліки пов'язані із використанням магнітного енкодеру розглянуті [3].

На підставі вищенаведеного доцільно продовжувати використання індукційного електромеханічні перетворювача із застосуванням математичною обробкою його сигналу з переходом до цифрової системи вимірювання.

Для переходу до цифрової системи вимірювання пропонується спрощена структурна схема, яка показана на рис. 1.

На схемі позначено ADC – *m*-канальний аналого-цифровий перетворювач (АЦП) розрядністю *na* з частотою вибірок *fg*; 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*о кожен; D – цифровий детектор фази за значеннями величин *c* і *s* (ЦДФ); G – генератор опорних імпульсів частоти *fg* для синхронізації роботи блоків ADC і FCS.

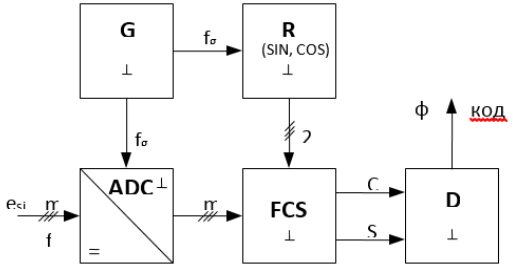


Рис.1 Структурна схема переходу до цифрової системи вимірювання

Функціонування запропонованого вторинного перетворювача сигналу ВП відбувається таким чином: «оцифровані» з частотою *fg* 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 наведені [4]. ЦДФ за одним з відомих алгоритмів визначає фазу хвильового пакета прямої послідовності сигналів e_{si} , яка є носієм інформації про кутове положення ротора давача кута 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.

Використання індукційного давача із застосуванням математичних методів обробки його сигналів при модернізації систем вертикального наведення гармати 2С3 забезпечить точність позиціювання даної системи на рівні десятків і навіть одиниць кутових секунд, що призведе до підвищення точності адаптації гармати з установками прицілу.

Отримання оцифрованого вихідного сигналу про значення кута наведення надасть можливість замінити щиток узгодження, який сигналізує узгодження гармати з установками прицілу за допомогою контрольних лам на сучасний цифровий дисплей, та дозволить визначення позиціювання ствола у реальному часі,

що зробить можливим адаптацію ствола з сучасними приладами управління вогнем (балістичним калькулятором, електронним планшетом з програмним забезпеченням типу ГісАрта, АрміяSOS) та значно підвищать бойову ефективність при виконанні вогневого завдання.

1. Артилерійське озброєння і боєприпаси: навчальний посібник /А. Й. Дерев'янчук, М.Б. Шелест. – Суми: Вид-во СумДУ, 2010. – 415с.
2. Міністерство оборони України, таблиці стрільби для рівнинних і гірських умов 152 – мм самохідної гаубиці 2С3 (2С3М, 2С3М1).
3. IV-а Міжнародна наукова конференція «Вимірювання, контроль та діагностика в технічних системах» Збірник тез доповідей Вінниця 2017р. С 112-2.
4. Глинченко А.С. и др. Цифровые методы измерения сдвига фаз. – Новосиб.: Наука, Сиб.отд., 1979 - 136 с.
5. 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.

Інформаційна технологія попередження надзвичайних ситуацій у будівлях з дерев′яними несучими конструкціями на основі аналізу їх акустичних сигналів

Шабатура Юрій Васильович,

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

Стась Стефан Володимирович,

аспірант Національного лісотехнічного університету України

Однією із найбільш динамічно розвинених індустрій сьогодення є індустрія будівництва та промислового виготовлення

предметів і об′єктів як зовнішнього так і внутрішнього інтер′єрів приміщень і будівель. Незважаючи на те, що основною тенденцією цієї індустрії є широке використання штучних матеріалів, проте найкращими з точки зору ергономічних і екологічних характеристик залишаються вироби і матеріали з деревини. Саме тому деревина і понині є основним матеріалом для виготовлення предметів внутрішнього інтер′єру будівель, зокрема меблів, крім того, вона часто використовується і для виготовлення різного роду будівельних конструкцій, наприклад, каркасів дахів, сходів і т. д. А в порівняно недалекому минулому деревина була одним з основних будівельних матеріалів. У більшості будівель споруджених у першій половині минулого століття і раніше з деревини були виготовлені усі елементи несучих конструкцій і міжповерхові перекриття. Таким чином від збереження міцності дерев'яних елементів несучих конструкцій залежить надійність і безпека експлуатації великої кількості нині існуючих будівель, тому розроблення технологій, методів і засобів, які дозволяють об'єктивно оцінювати їх стан є важливою і актуальною задачею.

Питанню безпеки експлуатації будівель з дерев'яними елементами несучих конструкцій, які іноді мають біля ста і більше років експлуатації приділяється велика увага. Особливо актуальним це питання є для міст у яких є багато старовинних історичних споруд. Зокрема, до таких міст в Україні в першу чергу відноситься старовинний Львів.

Деревина є органічним матеріалом, тому крім природних процесів старіння вона нерідко зазнає пошкодження від різного роду біологічних чинників: гризунів, комах, черв'яків, грибків та бактерій. На даний момент основним методом оцінки стану і міцності дерев'яних будівельних конструкцій є експертна оцінка фахівцями, які окрім візуального огляду здійснюють лабораторне дослідження зразків деревини будівельних конструкцій. Це дуже затратний і довготривалий метод, крім того він не завжди може бути застосований, оскільки чимало елементів дерев'яних несучих конструкцій часто залишаються просто недоступними для візуального огляду і фізичного контакту.

Основною ідеєю, яка покладена в основу розробленої інформаційної технології аналізу і оцінки стану дерев'яних елементів будівельних конструкцій лежить використання явища емісії акустичних сигналів в'язко-пружним матеріалом деревини при виникненні у ній механічних напружень, пошкоджуючій дії комах і гризунів, а також виникнення сигналів-відгуків, як результатів дії на дерев'яні конструкції дозованих тестових механічних ударів.

Запропонована інформаційна технологія базується на використанні експертних систем для проведення інтелектуального аналізу акустичних сигналів елементів дерев'яних конструкцій. Причому аналіз проводиться з використанням бази знань в якій враховується вид деревини, форма елементів деревних конструкцій, тип і спосіб кріплення цих елементів, призначення і вид самої дерев'яної конструкції, її приблизний вік та інші класифікаційні ознаки.

Програмне забезпечення розробленої технології передбачає використання самовдосконалюваних програмних продуктів, які використовують нечіткий логічний висновок і нейронні мережі, а також можливість мережевого доступу до системи управління базами даних (СУБД).

Виконані дослідження дозволили з'ясувати цілий ряд характерних особливостей проходження і виникнення акустичних сигналів у деревині.

До основних звукових властивостей деревини належать: швидкість поширення звуку, акустичний опір, логарифмічний декремент затухання коливань, звукопроникність, звукопоглинання, резонансну властивість. Нижче в таблицях наведені типові значення зазначених властивостей для найбільш пошите них в Україні видів деревини.

Середні значення швидкості розповсюдження звуку при продольних коливаннях для кімнатно-сухої деревини

Порода	Модрина	Сосна	Ялина	Дуб	Ясен	Береза
Швидкість звуку, м/с	4930	5360	5630	4720	4730	5530

Величина акустичного опору для кімнатно-сухої деревини

Порода	Модрина	Сосна	Ялина	Дуб	Ясен	Береза
$R \cdot 10^{-5}$ Па $\cdot$ с/м	33	28	31	30	28	29

Логарифмічний декремент коливань деревини

Порода	Волога W, %	Вид коливань	Декремент коливань $\delta \cdot 10^4$ Нп	Автор
Сосна	7	Гнучнкі	207	В.Д. Нікішов
Ялина	8	Гнучкі	173-307	І.І. Пищик
Ясен	12	Продольні	330	А.М. Боровиков
Бук	12	Продольні	366	Н.Н. Дулевслький
Береза	7	Гнучкі	272	В.Д. Нікішов
Клен	8	Гнучкі	219-377	І.І. Пищик
Тополя	12	Гнучкі	288	Й. Беничак

*Нп – «непер» – відношення двох фізичних величин, натуральний логарифм якого рівний одиниці

Дослідження деревини, підтвердили відому закономірність про збільшення швидкості поширення звуку з підвищенням густини. Аналіз результатів досліджень показує, що з збільшенням густини збільшується швидкість звуку в продольному напрямку. Збільшується і динамічний модуль гнучкості деревини, розрахований на основі швидкості проходження звукових коливань через досліджуваний зразок:

$$E_\partial = C^2 \rho ,$$

де С – швидкість звуку в продольному напрямку, м/с; ρ – густина деревини, кг/$м^3$.

Результати експериментів, які підтверджують такі висновки наведені на рисунку 1.

Загальна структура програмного забезпечення, яке реалізує запропоновану технологію наведена на рисунку 2 у вигляді UML діаграми компонентів.

У даній структурі за оброблення HTTP запитів від клієнтської сторони відповідає файл views.py. Так як система реалізована з допомогою фреймворку Django, а він в свою чергу в плані структури відповідає шаблону MVC (Model-View-Controller).

Пошук аудіо реалізує модуль findsound. Основним файлом цього модулю є файл який так і називається – findsound.py. Він надає API модулю для пошуку аудіо і для додавання нових записів до бази даних. Далі розташовуються компоненти, які реалізують алгоритм вирішення задачі ідентифікації аудіозапису за зразком.

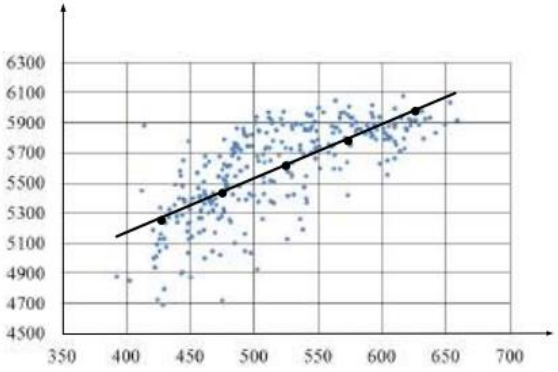


Рис. 1. Вплив густини деревини сосни на швидкість проходження звуку

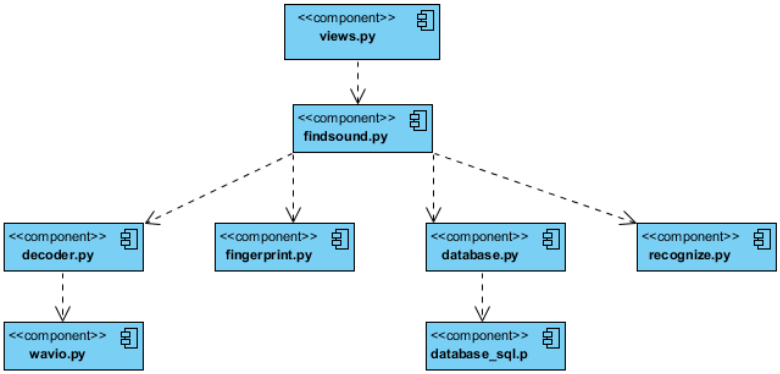


Рис. 2. UML діаграма компонентів програмного забезпечення розробленої інформаційної технології.

У підсумку потрібно зазначити, що практичне застосування запропонованої технології дозволить отримати багато цінних результатів лише після проходження нею надзвичайно відповідального періоду «навчання», що дозволить їй отримати

цінний досвід багатьох експертів і практичні знання стосовно особливостей акустики різних будівельних конструкцій. Окрім чисто інформаційного і програмного аспектів даної технології важливе значення має і технічний аспект її забезпечення первинною акустичною інформацією. Сюди відносяться акустичні сенсори, їх розміщення і забезпечення акустичного контакту з деревиною, а також пристрої подачі в дерев'яні елементи несучих конструкцій тестових сигналів збудження.

1. Рощина С.И. Особенности технической эксплуатации зданий и сооружений: учеб. пособие / С.И. Рощина, М.В. Лукин, М.С. Лисятников / Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2014. – 119 с.
2. Chubinsky A.N., Okuma Motoaki, Sugiyama Junji. Observation on the Deformation of Wood Cells in the Gluing process of Veneer //Bulletin of the Tokyo University Forests-Tokyo: Tokyo University, 1990. №82. P.131-135.

IP-системи у відеотехнологіях безпеки

Шишко Валерій Валерійович,

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

Фірман Володимир Михайлович,

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

Шишко Валерій Йосипович,

старший викладач кафедри інформатики Львівського державного університету внутрішніх справ

Системи відеоспостереження (англ. Closed-circuit television, CCTV) – це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. обладнання),

призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах.

Першу систему відеоспостереження було встановлено фірмою Siemens AG на випробувальному стенді VII у Пенемюнде, Німеччина 1942 року для спостереження за запуском ракети V-2.

У США перша телевізійна система комерційного спостереження, яка називалася Vericon стала доступною 1949 року. Про Vericon відомо дуже мало, за винятком того, що її було оголошено як систему, яка не потребує дозволу уряду. Пізніше, Марі Ван Бріттан Браун винайшов систему домашньої безпеки – патент було видано 1969 року. Система Брауна являла собою набір з 4-а очками і камерою, яка могла ковзати вгору і вниз, щоб подивитися крізь кожне з них. Система містила, також пристрій, що дозволяв домовласнику використовувати телевізор для перегляду людини у дверях і можливості почути її голос.

Відеоспостереження сьогодні є невід'ємним елементом будь-якої сучасної системи безпеки. Основні завдання, розв'язувані за допомогою відеоспостереження:

- *візуальний контроль ситуації на об'єкті, що охороняється* – надає інформацію на пост спостереження в мультиекран (в режимі очікування) або в повноекранному режимі (зображення від однієї телекамери на весь екран) в режимі реального часу. Це забезпечує можливість прийняття оперативних рішень, адекватних конкретній ситуації;
- *можливість організації безперервного відеозапису* відеоспостереження на цифровий відеореєстратор або комп'ютерну систему – дозволяє документально підтвердити факт порушення і надає можливість для проведення ефективного аналізу кожної ситуації;
- *виконання функцій охоронної сигналізації* при використанні детекторів руху відеокамер або зовнішніх охоронних датчиків і інформованість оператора системи про виникнення тривоги в контрольованій зоні з допомогою світлового та звукового сигналу оповіщення. При цьому спрацьовування

детектора руху може автоматично активувати запис для повної реєстрації тривожної ситуації, запускатися один з безлічі сценаріїв реакції системи – запуск виконавчих механізмів, зміна режиму роботи компонента системи, запуск інших програм або ж комбінація всіх цих подій.

На поточний момент серед систем відеоспостереження особливе місце займають системи IP-спостереження, які дозволяють встановлювати відеоконтроль за об'єктами будь-якої складності, а робота на ньому оперативного персоналу не вимагає високої кваліфікації. Такі системи не потребують прокладання додаткових ліній зв'язку, передача даних відбувається за мережевої інфраструктури, побудованої на протоколі IP. Контроль і адміністрування системи здійснюється з будь-якого комп'ютера, що має доступ в мережу і спеціальне програмне забезпечення.

Мережеві камери існують на ринку вже достатньо довго. Перша з них була випущена компанією Axis в 1996 году. Якість зображення в перших мережевих камерах значно поступалася професійним аналоговим камерам. Їх розглядали виключно як дещо екзотичне і використовували тільки у WEB-додатках для передачі відео по локальним мережам і Internet. IP-камери розроблялись з урахуванням переваг мережевих технологій і Internet для роботи з цифровим зображенням в нових прикладних областях і не позиціонувались як камери для систем відео нагляду і безпеки. Але з плином часу мережеві IP камери суттєво змінилися.

Відеоспостереження на базі IP-технологій здійснюється на базі стандартної мережної архітектури – локальної мережі Ethernet. Фактично користувач отримує розподілену цифрову систему охоронного відеоспостереження, яка дозволяє застосовувати для аналізу і обробки даних сучасні інформаційні технології. Ключовим елементом мережі IP-відеоспостереження є мережева (IP) відеокамера, яка має об'єктив, оптичний фільтр, ПЗЗ-матрицю, вбудований мікропроцесор для оцифровування/стиснення відеозображення в різних форматах (найчастіше в H.264, MPEG-4 або M-JPEG), мережевий контролер для

підключення в мережу Ethernet і інші елементи. Потужність процесора визначає продуктивність і швидкість передачі відеопотоку по мережі. По ряду характеристик, таких як тип матриці, чутливість, настройки зображення (баланс білого, АРУ, гамма-корекція і ін.), IP-камери можна порівняти з аналоговими, однак наявність мережевого інтерфейсу і додаткових процесорів дозволяє їм виконувати відеоаналіз, масштабування зображення, накладення на нього титрів і передачу цифрового відео на великі відстані та ін. Найголовніше, що кожна мережева відеокамера має свою власну IP-адресу, обчислювальні функції і вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій. На відміну від аналогової відеокамери, IP-камера не потребує прямому підключенні до комп'ютера або до будь-яким іншим апаратних або програмних засобів. Її підключення може здійснюватися як за допомогою дротового з'єднання (по мідним проводам або оптичному волокну) так і бездротового (Wi-Fi, GPRS/EDGE, 3G, супутниковий зв'язок тощо). Таким чином, досягається повна або часткова мобільність користувача, який здатний стежити за віддаленими об'єктами практично з будь-якої точки земної кулі.

Основні переваги відеоспостереження на основі IP-камер:

- Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з комп’ютера, мобільного телефону тощо), та здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.
- Спрощена установка при малих витратах на монтаж – мережеві відеосистеми IP не вимагають прокладки додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої системи охорони об'єкта або за допомогою бездротових технологій.
- Якість відеозображення – в сучасних IP-системах застосовується формат MPEG-4, який дозволяє більш ефективно використовувати ресурси мережі в порівнянні з форматом M-JPEG. Оцифровування зображення відбувається у самій камері, що надає можливість розвантажити центральне

обладнання системи та зайняти його вирішенням інших насущних задач.

- Можливість передавати по одному кабелю не тільки відео, але і звук, а також управляти і керувати IP-камери. В аналогових системах передача звука можлива тільки по виділеним аудіолініям, окремим від каналів передачі відео. Мережеві камери вирішують цю проблему, опрацьовуючи аудіоінформацію безпосередньо в камері, синхронізуючи її з відео чи навіть об'єднуючи в той же відеопотоку, і потім посилаючи по мережі для контролю і запису. Звуковий канал може використовуватися як в одному, так і в двох напрямках, що дозволяє не тільки отримувати, а й передавати звук на об'єкт.
- Застосування цифрових камер дозволяє відмовитись від використання черезстрокової розгортки і, як наслідок її – деінтерлейсінгу.
- Мережеві камери можуть приймати та опрацьовувати сигнали тривоги, що надходять з датчиків, і управляти зовнішніми виконавчими пристроями через цифрові порти вводу-виводу.
- Гнучкість і масштабованість систем IP відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю та дистанційного керування без прив'язки до відстані.
- Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.
- Використання Хмарного спостереження. Хмарне відеоспостереження це інтернет-сервіс, який дозволяє зберігати, переглядати і зберігати відеозаписи з відеокамери, встановленої у користувача завдяки підключенню через Інтернет до серверів, що зберігають дані. Хмарне відеоспостереження все більше набирає популярність, і цьому є логічне пояснення: замість покупки клієнтом купи всяких компонентів системи відеоспостереження, при Хмарному сервісі у клієнта повинна бути тільки камера – все інше забезпечує Хмара за символічну плату. Це дійсно дуже вигідно.

Водночас масове застосування IP-систем стримує декілька причин.

1. Якість зображення.

Якщо не використовується стиснення, то можна отримати вражаючі цифри. Так якщо у пристрою є буфер на один кадр, то при стандартному розмірі кадра 768x576x2, отримуємо розмір кадра рівний 885 Кбайт! В секунду знімається 25 кадрів (живе відео), тобто 2 Мбайт/с або 177 Мбод! В даний час тільки гігабітний Ethernet або мережі на основі оптоволоконних з'єднань здатні забезпечувати обмін на таких швидкостях.

Обмеження пропускної здатності каналів зв'язку призводять до застосуванню алгоритмів стискання зображення з невідновною втратою якості або зниження швидкості відео потоку (до 1-3 кадрів/с) при збереженні якості. При цьому зображення губить придатність для систем розпізнавання обличь або автомобільних номерів.

При цьому, якщо в системі застосовується JPEG-стиснення при розмірі одного кадра 50 Кбайт і швидкості запису 25 кадрів/с отримуємо потік 1250 Кбайт/с або 10 Мбод. Локальні мережі, що використовують технологію Fast Ethernet, справляються з таким об'ємом трафіка, але для Ethernet мереж, яких пропускна здатність на порядок нижче, таке навантаження вже може представляти деяку загрозу.

2. Якість матриці і оптики в самих IP-відеокамерах. Виробники, намагаючись зробити IP-камери дешевшими і універсальними, встановлюють середні по всім параметрам матриці, які призводять до «сліпоти» камери вночі і її перевантаження при денному світлі.

3. Складності з інтеграцією камер різних виробників в систему з програмним забезпеченням третіх виробників. Вся множина аналогових камер має, як мінімум, один інтерфейс – композитний відеосигнал, який підтримується будь-яким обладнанням. В цифровому світі все більш складно. Багато виробників підтримують всі протоколи передачі даних, але ретельно приховують алгоритм кодування зображення, вимуу-

шуючи клієнтів користуватися тільки їх утилітами перегляду або архівування зображення.

Як зазначалось вище, при організації передачі відеоінформації через Internet, основною проблемою являється вибір пропускної здатності каналу зв'язку і вибір якості зображення. Для фахового вирішення цих проблем доцільно застосовувати спеціалізоване програмне забезпечення. Серед програм щодо розрахунків подібних параметрів виділяється хорошою ефективністю програма Axis Design Tools – зручний і багатофункціональний калькулятор, що застосовується для розрахунків при побудові системи відеоспостереження з камерами і відеосерверами Axis.

Висновки

1. Системи IP-відеоспостереження дозволяють просто масштабуватися. Вони надають можливості використовувати більш рентабельні рішення, такі як стандартні сервери для запису і збереження відеоданих.
2. При використанні системи IP-відеоспостереження є можливість вибору програмного забезпечення, створеного для управління відео і забезпечення необхідної аналітичної підтримки.
3. Системи IP-відеоспостереження дозволяють організовувати децентралізовану обробку і збереження інформації.
4. Системи IP-відеоспостереження легко реконфігуруються і переносяться, що заважає потенційним зловмисникам легко віднаходити слабкі місця в системі.
5. В цілому, мережеві системи відеоспостереження знаходять все ширше застосування для віддаленого контролю стану об'єктів, що не вимагають запам'ятовування і аналізу дрібних деталей зображення.

1. Абуталимов З. TRASSIR Cloud: как избежать лишних затрат на видеонаблюдение? / Системы безопасности. – 2016. – № 1 (127) – С. 33.
2. Алтуев М. Искусство управления огромным потоком событий видеоаналитики / Системы безопасности. – 2016. – № 1 (127) – С. 112-113.

3. Новичихин А., Антюшин С., Артюхов В. Системы хранения данных: потребности распределенных систем видеонаблюдения / Системы безопасности. – 2016. – № 1 (127) – С. 58-59.
4. Йоханссон А. Управление видеонаблюдением в эпоху мобильного Интернета /
5. // Системы безопасности. – 2016. – № 1 (127) – С. 108-111.
6. Лаппенкупер Д. Построение стабильных систем машинного зрения на базе камер USB 3.0 / Системы безопасности. – 2016. – № 3 (129) – С. 96-97.
7. Полл Н., Лисновский М. Облачные подходы к видеохранилищам, или Следуя тренду C2B-Shifling / Системы безопасности. – 2016. – № 2 (128) – С. 118-119.
8. Маликов А. Выбор IP-решений: анализ критерия цена/качество / Системы безопасности. – 2016. – № 4 (130) – С. 44-46. – 3 рис.
9. Петренко С. Безопасность систем безопасности. Защита информации IP-видеонаблюдения / Системы безопасности. – 2016. – № 4 (130) – С. 42-43.
10. Чернов А. Простая инсталляция систем видеонаблюдения: полезные инструменты от AXIS Communications / Системы безопасности. – 2016. – № 2 (128) – С. 111.

Правовий режим персональних даних як інформації обмеженого доступу

Ярема Оксана Григорівна,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Єсімов Сергій Сергійович,

доцент кафедри адміністративно-правових дисциплін факультету № 6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Категорія правового режиму використовується як універсальна для опису численних правових явищ. З її допомогою описується не тільки нормальна життєдіяльність або нормальний стан об'єкта права, а й вводяться виключення із загальних правил у вигляді його спеціальних або особливих режимів.

Винятковість правового режиму може бути спочатку вказана в законі, як, наприклад, в законах про надзвичайний і воєнний стан. У досить великій кількості випадків описується основний – загальний правовий режим, або режим звичайного стану, а виключення або відступу від нього будуть розглядатися як особливі або спеціальні режими.

В юридичній літературі виділяють два основних підходи до розуміння терміна «правовий режим». Перший підхід розглядає правовий режим як особливий порядок правового регулювання, що виражається в певному поєднанні юридичних засобів і створює бажаний соціальний стан і конкретні умови для задоволення інтересів суб'єктів. З точки зору цього підходу можна вести мову про галузеві, міжгалузеві правові режими.

Другий підхід домінує в адміністративно-правовій науці і відноситься, в першу чергу, до характеристики «адміністративно-правових режимів», визначаючи їх як комплекс суспільних відносин певного виду діяльності, закріплений юридичними нормами і забезпечений сукупністю організаційних засобів.

Виділення правового режиму обумовлено: по-перше, особливою спеціальної значимістю суспільних відносин, їх специфічними цілями та завданнями; по-друге, використанням особливих принципів, форм і методів діяльності, що відбиваються в системі прав і обов'язків суб'єктів.

Варто звернути увагу, що законодавство та практика йде по шляху застосування режимів не тільки до сфери державного управління або опису державного стану, але швидше розглядає правові режими як щось універсальне. По суті, слід говорити про формування особливого режимного підходу в вивченні права і правових явищ.

Особливо це справедливо в ситуаціях, що вимагають специфічного і особливого підходу до регулювання тих сфер, регулювання яких може виявитися неефективним в загальному порядку. Ще однією особливістю правових режимів найчастіше є їх комплексний характер. У конструюванні таких режимів

беруть участь норми декількох галузей права (адміністративного, конституційного і ін.), вони зачіпають різні за характером права і обов'язки суб'єктів режимного регулювання. Комплексний характер правових режимів дозволяє об'єднати і адаптувати правові засоби та методи впливу до конкретних суспільних відносин.

Правовий режим інформації, включаючи інформацію обмеженого доступу, характеризується: системністю використовуваних засобів; наявністю специфічних прийомів правового регулювання; систематизацією норм за ознакою об'єкта; створенням умов для досягнення заданого стану об'єкта; комплексністю режиму як відображення комплексності об'єкта; обумовленістю режиму специфічністю груп суспільних відносин, і необхідністю використання особливого підходу до регулювання там, де використання загального підходу неефективно або недоцільно.

Наявність цих характеристик можна простежити щодо правового режиму персональних даних, який слід розглядати як різновид особливого правого режиму інформації – режиму інформації обмеженого доступу.

Безпосередньо розгляд правового режиму персональних даних як інформації обмеженого доступу доцільно почати з визначення його чітких меж, перш за все щодо загального правового режиму інформації обмеженого доступу. Персональні дані самі по собі не є інформацією обмеженого доступу, і їх конфіденційність припускається. Як наслідок, правовий режим персональних даних в цілому має складну структуру, обумовлену специфікою об'єкта регулювання.

Можна виділить дві основні складові цього режиму: правовий режим загальнодоступних персональних даних, який лежить в сфері загального правового режиму інформації, тобто режиму загальнодоступної інформації; правовий режим персональних даних обмеженого доступу, який лежить в сфері спеціальних правових режимів інформації, тобто в сфері правового режиму інформації з обмеженим доступом, який може бути розділений

на декілька складових: персональні дані, що охороняються в режимі державної таємниці; персональні дані обмеженого доступу, оброблювані в режимі архівної інформації (наприклад, у контексті Закону України від 09.04.2015 № 316-VIII «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років»); персональні дані, що охороняються в режимі особистої, сімейної таємниці, таємниці приватного життя (тобто без передачі відомостей третім особам, що не є конфіденційною інформацією); конфіденційні персональні дані, щодо яких спеціальним законом встановлюється вимога про дотримання їх конфіденційності.

Незважаючи на таку складну структуру, можна говорити, що певний інтерес представляє остання категорія, яка може бути охарактеризована як персональні дані, що охороняються в умовах правового режиму конфіденційності персональних даних як інформації обмеженого доступу у межах Закону України від 01.06.2010 № 2297-VI «Про захист персональних даних».

Правовий режим інших категорій, хоч вони і є різновидами інформації обмеженого доступу, не орієнтований спеціально на захист персональних даних як обмеженою в доступі інформації і не виділяє їх в загальному масиві охороняється на умовах цього режиму інформації. Винятком можна назвати персональні дані, що становлять особисту, сімейну таємницю і таємницю приватного життя, які самі по собі не можуть бути не прив'язані до конкретного індивіда. У цьому випадку законодавче регулювання будується виключно на визнання у індивіда права на ці види таємниць і можливості їх самостійної охорони і як наслідок мінімального обсягу нормативних положень, що забезпечує велику особисту свободу та відповідає ідеї природних прав. У даному випадку суть у визначенні прав індивіда в разі передачі інформації про себе третім особам.

Саме довірча передача інформації індивідом іншій особі, тобто оператору або оброблювачу, обумовлює її захист у межах спеціального правового режиму конфіденційних персональних даних. Це підкреслено у Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональ-

них даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [1].

Правовий режим конфіденційності персональних даних включає дві основні складові: загальний правовий режим конфіденційності персональних даних і правовий режим персональних даних визначених ст. 5 Закону України від 01.06.2010 № 2297-VI «Про захист персональних даних».

Що стосується основних елементів і структури правового режиму інформації, і персональних даних зокрема, то тут можна відзначити деякі розбіжності в думках. С. Брайчевський досліджуючи інформаційні потоки та інформаційні об'єкти зазначає, що термін «інформаційний об'єкт» за поширеною думкою слід вважати невдалим уже хоча б тому, що те, що він означає, насправді має в собі цілком виразний елемент суб'єктності, і саме це і робить його цікавим. Однак іншого терміна досі запропоновано не було, і ми будемо користуватися ним, усвідомлюючи всю його відносність [2, с. 134].

З погляду на позицію вказаного вченого, правовий режим можна визначити як сукупність правових норм, що стосуються певного об'єкта врегульованих правом суспільних відносин, включаючи його нормативне визначення і обов'язкові правові приписи про порядок або правила використання даного об'єкта та про відповідальність за їх недотримання.

У контексті дослідження М. Мільман, можна зробити висновок, що правовий режим інформаційного об'єкта повинен, складатися з норм, що регулюють три основних складових: порядок створення об'єкта, порядок його передачі і отримання (включаючи встановлення режиму вільного або обмеженого доступу), питання захисту прав суб'єкта щодо даного об'єкта Крім цього правовий режим може включати і інші (необов'язкові елементи): норми, що регулюють цивільно-правовий обіг об'єкта та інші питання [3, с. 26].

У дійсності правовий режим конкретного різновиду інформації спочатку має свій об'єкт. Такий режим може бути встановлений законом щодо певного виду інформації, як, наприклад, у випадку з персональними даними законодавчо встановлюється відповідний режим, припускаючи, що такий різновид інформації існує. Дія правового режиму може бути поширене на ту чи іншу інформацію, як, наприклад, у випадку з комерційною таємницею, коли її власник має право виконати запропоновані законом дії та поширити на неї режим комерційної таємниці.

З огляду на сказане, найбільш раціональним доцільно визнати виділення основних структурних елементів правового режиму, які притаманні всім правовим режимам інформації: цільове призначення режиму; об'єкт правового регулювання; правове становище суб'єктів правового режиму; комплекс способів правового регулювання та засобів юридичного впливу.

---

1. Наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних». [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/v1_02715-14/paran215#n215
2. Брайчевський С.М. Інформаційні потоки та інформаційні об’єкти / С.М. Брайчевський // Інформація і право. – 2012. – № 2 (5). – С. 133-138.
3. Мільман М. Проблеми оборотоздатності інформаційних об’єктів особистих немайнових прав / М. Мільман // Підприємництво, господарство і право. – 2016. – № 6. – С. 23-28.

Зміст

Розділ 1. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ, ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ, ЇХ ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ТА КОМПЛЕКСНОМУ ПІДХОДІ ДО ПРОБЛЕМ ДЕРЖАВНОЇ БЕЗПЕКИ 3

Бабецький Р. В. Інформаційне забезпечення захисту свідків, які беруть участь у кримінальному судочинстві 3

Бесчастний В. М., Назимко Є. С., Волобуєва О. О. Інформаційне забезпечення протидії злочинності як копмлексний підхід до державної безпеки 7

Бобонець М. М., Рвачов О. М. Особливості використання працівниками Національної поліції України нагрудних відеокамер.... 13

Бондаренко В. А. Методи розмежування доступу до інформаційних ресурсів у базах даних органів МВС 17

Вишня В. Б. Удосконалення зв'язку в системі управління нарядами патрульної служби Національної поліції України 23

Гула Л. Ф. Оптимізація інформаційно-аналітичного забезпечення оперативних підрозділів у протидії злочинам, що вчиняються організованими злочинними групами 27

Дронюк І. М., Кліщ Ю. І. Моделі, засоби збору та опрацювання параметрів трафіку телекомунікаційних мереж 31

Дуфенюк О. М. Як технологія 3D сканування змінює якість розслідування кримінальних правопорушень 35

Зачек О. І., Козаченко В. В. Програмне забезпечення для кримінального аналізу..... 40

Калиновський О. В., Школьніков В. І. Використання методів групування та кластеризації в NodeXL під час здійснення кримінального аналізу..... 45

Комiссарчук Ю. А., Карандюк О. М. Проблеми застосування інформаційних технологій правоохоронними органами України: історичний аспект.....49

Комiссарчук Ю. А., Моняков М. М., Дмитришин О. О. Перспективи розвитку інформаційних технологій у діяльності органів Національної поліції України 53

Кубрак В. П. Питання інформаційно-аналітичного забезпечення діяльності правоохоронних органів 56

Кудінов В. А. Проблема оцінки якості спеціального програмного забезпечення інформаційних систем Національної поліції.....61

Кунтій А. І. Незаконне розповсюдження медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів мережі Інтернет: питання спеціальних експертиз 65

Лепеха О. М., Кондратюк О. В. Використання інформаційних технологій для визначення місцезнаходження об'єкта 69

Мирошниченко В. О., Бакало В. О. Розслідування комп'ютерних злочинів.....73

Пахомов В. Б., Кавун С. В. Аналіз актуальності інформаційних технологій у правоохоронній діяльності.....77

Поляк С. П. Проблеми інформаційно забезпечення діяльності підрозділів карного розшуку в процесі протидії втягненню неповнолітніх у з лочинну діяльність.....81

Проць І. М., Кузьмочка Ю. В. Правовий захист інформації...85

Сеник С. В. Історичні етапи становлення інформаційної діяльності Національної поліції України 88

Узлов Д. Ю., Струков В. М. Сучасні інструментальні засоби кримінального аналізу.....91

Хахановський В. Г. Особливості огляду місця події за фактами вчинення злочинів, спосіб вчинення яких пов'язаний з використанням комп'ютерної та телекомунікаційної техніки.....95

Чистоклетов Л. Г., Хитра О. Л., Шишко В. Й. Сучасні проблеми інформаційно-правового забезпечення особистої безпеки працівників органів правоохоронної діяльності 100

Danuta Kaźmierczak. Learning Management Systems for Homeland Security Training 105

Kuck Jerzy, Grzegorz. Strategy for computerization of organizations, institutions functioning in defense and security..110

Kuck Jerzy, Grzegorz. Identification and optimization of processes for defense and security purposes.....121

Kuck Jerzy, Grzegorz. Identification of products as the foundation of information systems operating in defense and security.....137

Pieronkiewicz Jarosław. Cybersecurity – the most popular methods of cyberattacks 147

Розділ 2. НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ 155

Гавриш О. С. Використання безкоштовних програмних засобів.....155

Грицюк Ю. І., Бучковська А. І. Візуалізація експертного оцінювання якості програмного забезпечення з використанням полярних діаграм.....160

Замула А. О., Кашура Г. К. Система дистанційного навчання – сучасна педагогічна технологія для правоохоронних органів 167

Зачко О. Б., Головатий Р. Р. До проблеми створення внутрішньої наукометричної бази ВНЗ.....172

Коваль С. О., Соколовський Я. І. Розроблення програмно-алгоритмічного забезпечення інтелектуальної системи «Розумна кафедра».....177

Комісарчук Ю. А., Загацький В. В. Застосування інформаційних технологій правоохоронними структурами України та ВНЗ зі специфічними умовами навчання: проблеми та реалії життя.....180

Кулешник Я. Ф., Ізьо М. І. Використання класичних статистичних методів для аналізу валідності та дискримінативності результатів тестування 184

Левус Є. В., Бода О. Б. Алгоритм оцінювання якості машинного перекладу англо-української мовної пари 193

Мельничин А. В. Використання системи візуалізації 3D об'єктів у навчальному процесі 198

Прокопов С. О. Використання пошуку інформації з відкритих джерел мережі Інтернет у навчальному процесі Дніпропетровського державного університету внутрішніх справ. 202

Рижков Е. В. Досвід запровадження проекту «ЛІНІЯ-102» у Дніпропетровському державному університеті внутрішніх справ 205

Савайда О. І. Методологія застосування інформаційних технологій у ВНЗ із специфічними умовами навчання 212

Сватюк О. Р., Миронов Ю. Б., Миронова М. І. Оцінювання ефективності дистанційного навчання 215

Світличний В. А. Деякі методологістичні аспекти підготовки кадрів для підрозділів кіберполіції в Україні 219

Сеник В. В. Роль викладання комп'ютерного аналізу даних у підвищенні професійної підготовки фахівців для підрозділів Національної поліції України 222

Сибірна Р. І., Хомів О. В. Інформаційні системи у наукових розробках працівників ОВС 226

Тулупов В. В., Пересічанський В. М. Проблемні питання розробки та впровадження компонентів інформаційних технологій у освітньому процесі 234

Розділ 3. СУЧАСНІ ПІДХОДИ ВПРОВАДЖЕННЯ ІТ-ТЕХНОЛОГІЙ В АКТУАЛЬНІ СФЕРИ НАУКОВОЇ ТА ПРАКТИЧНОЇ ДІЯЛЬНОСТІ 238

Ангеленюк А.-М. Ю. Використання інформаційних технологій під час досудового розслідування 238

Бортник Н. П., Єсімов С. С. Адміністративно-правове регулювання інформаційного забезпечення діяльності МВС України в сфері міграції.....244

Гаврильців М. Т. Державна інформаційна політика та проблеми інформаційного забезпечення відкритості державної влади в Україні.....249

Герич А. І., Процах Н. П. Проектування та дослідження ВЕБ-орієнтованої системи приватних оголошень на базі 3 LAYERED ARCHITECTURE.....254

Глинський Я. М., Ряжська В. А. Відеоресурс як темотвірний елемент методичної системи навчання.....258

Горлатий Р. М., Головатий А. І. Автоматизоване проектування та моделювання руху дискової фрикційної муфти засобами SOLIDWORKS API та SOLIDWORKS SIMULATION.....264

Дендюк І. М., Дендюк М. В., Процик Ю. С. Система класифікації наукових статей.....267

Дідик Х. І., Пасічник С. Б., Неспляк Д. М., Тучапський Р. І. Використання MapReduce для обробки великих об'ємів даних.....271

Дмитрик Ю. І., Гарват Т. В. Щодо проблем використання даних ДНК-аналізу під час розслідування злочинів.....274

Доліновський Ю. С. Інформаційне забезпечення виявлення злочинів, що вчиняються під час публічних закупівель у сфері охорони здоров'я.....277

Іванців В. І., Шабатура Ю. В. Використання мікроконтролера ARDUINO.....281

Кавун С. В., Ломакіна В. В. Тренди кібербезпеки.....285

Кавун С. В., Шмаков В. В. Розробка пристрою екстреної допомоги співробітнику МВС.....288

Кириченко К. В., Рвачов О. М. Деякі особливості використання відеокамер у діяльності правоохоронних спецпідрозділів.....291

Ковалик П. А. Програмне та алгоритмічне забезпечення інформаційної системи розпізнавання зображень нейронними мережами 294

Ковалів М. В., Хіміч А. М. Реалізація права на доступ до інформації за інформаційним запитом 297

Комісарчук Ю. А., Багин С. С. Інформаційні технології в забезпеченні безпеки бізнесу 302

Курносов М. В., Крошний І. М. Автоматичне проектування та моделювання теплового двигуна із зовнішнім підводом тепла засобами SOLIDWORKS API, SOLIDWORKS SIMULATION 306

Лук'янова Г. Ю. Захист інформаційного суверенітету як складова політики національної безпеки України 309

Магеровський Д. В., Магеровська Т. В., Пелех Я. М., Гошко З. О. Використання засобів Motion Capture для створення симуляторів допиту свідка 314

Павлова Н. В., Матвійчук І. В. Проблеми реалізації фінансового моніторигу в Україні 320

Павлович-Сенета Я. П., Сафонова М. І. Акти-дії публічної адміністрації у правоохоронній діяльності: поняття, види і межі їх застосування 324

Павлович-Сенета Я. П., Степанова А. О. Дискреційні повноваження органів публічної влади в правоохоронній сфері 327

Рудий Т. В., Живко З. Б., Руда О. І. Система менеджменту інформаційною безпекою в інформаційних системах 330

Савчук М. В. Інформаційно-аналітичне забезпечення розслідування терористичних актів, з використанням вибухових пристроїв 336

Сватюк О. Р., Костюк Б. В., Сватюк Д. Р. Управління ресурсопотоками, що циркулюють у логістичній системі ЗВО 340

Сибірний А. В., Сибірна Р. І. Інформаційні технології у судово-медичній експертній діяльності 347

Синичак С. О. Програмне та інформаційне забезпечення веб-орієнтованої системи автоматизованого дослідження теплових процесів.....353

Сокиран Ф. М. Використання технічних засобів у дистанційному досудовому розслідуванні.....356

Тимчишин Т. М. Окремі аспекти застосування законодавствапро доступ до конфіденційної інформаці інформації.....359

Хомин О. Й., Смичок В. Д. Розробка фотоконтролера для безпеки особи (на прикладі виявлення несанкціонованого проникнення і мінування автомобіля).....363

Шабатура Ю. В., Вільман І. М. Модернізація систем наведення озброєння броньованих машин на основі застосування енергетично оптимізованого асинхронного електроприводу.....368

Шабатура Ю. В., Гера В. Я. Програмно-технічна модернізація двигунів внутрішнього згоряння спецтехніки та зразків озброєння військової техніки 373

Шабатура Ю. В., Снітков К. І. Модернізація системи наведення артилерійського озброєння самохідної гаубиці 2С3М на основі застосування методів математичної обробки сигналів кутовимірювальних сенсорів 378

Шабатура Ю. В., Стась С. В. Інформаційна технологія попередження надзвичайних ситуацій в будівлях з дерев′яними несучими конструкціями на основі аналізу їх акустичних сигналів.....382

Шишко В. В., Фірман В. М., Шишко В. Й. IP-системи відеотехнологіях безпеки.....387

Ярема О. Г., Єсімов С. С. Правовий режим персональних даних як інформації обмеженого доступу.....394

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ СТРУКТУРАМИ УКРАЇНИ ТА ВИЩИМИ НАВЧАЛЬНИМИ ЗАКЛАДАМИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Збірник наукових статей за матеріалами доповідей Міжнародної науково-практичної конференції
22 грудня 2017 р.

Відповідальний за випуск В. В. Сеник
Упорядник Т. В. Магеровська
Комп'ютерна верстка Т. В. Магеровська

Опубліковано в авторській редакції

Підписано до друку 10.01.2018 р.
Формат 60х84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк. 23,7
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.