ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

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

Збірник наукових статей
за матеріалами доповідей учасників
науково-практичної конференції
17 грудня 2015 р.

Львів
2015

УДК 004
ББК 32.973
П 78

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол № 5 від 23.12.2015 р.)

П 78 Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі : збірник наукових статей за матеріалами доповідей науково-практичної конференції 17 грудня 2015 року / упорядник Т. В. Магеровська /. – Львів: ЛьвДУВС, 2015. – 243 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі», що проводилася 17 грудня 2015 р. у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

УДК 004
ББК 32.973

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

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЮРИДИЧНІЙ ПРАКТИЦІ

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

Стрімкий та динамічний розвиток інформаційних відносин у XXI ст. 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», «інформаційна війна», «кіберпростір», «кіберзлочинність», «електронне урядування» тощо.

За таких умов дедалі актуальнішими стають проблеми формування нормативно-правової бази у галузі інформаційних відносин та її подальшого розвитку і удосконалення в умовах європейських інтеграційних пріоритетів України, імплементації норм міжнародного права в інформаційне законодавство

України, а також проблема систематизації національного законодавства у сфері застосування інформаційних технологій.

Після проголошення державної незалежності України розпочалося активне формування системи національного законодавства у сфері інформації та інформаційних технологій. З 90-х рр. ХХст. і до сьогодні прийнято значну кількість законів та інших нормативно-правових актів, що дозволило врегулювати найбільш важливі норми інформаційних відносин та інформаційної діяльності.

Нормативно-правовою основою інформаційних відносини в Україні є ціла низка нормативно-правових актів: Конституція України, закони України «Про інформацію», «Про науково-технічну інформацію», «Про телебачення і радіомовлення», «Про друковані засоби масової інформації (пресу) в Україні», «Про бібліотеки і бібліотечну справу», «Про Національний архівний фонд і архівні установи», «Про інформаційні агентства», «Про телекомунікації», «Про Національну програму інформатизації», «Про концепцію національної програми інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про авторське право і суміжні права», «Про державну таємницю», «Про державну статистику», «Про доступ до судових рішень», «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про рекламу», «Про засади державної мовної політики», «Про Суспільне телебачення і радіомовлення України», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» тощо.

Інформаційно-комунікаційні технології істотно змінили практично всі види суспільних відносин (у науці під цим терміном розуміють всі технології, пов'язані із застосуванням та експлуатацією комп'ютерних систем, використовуваних для збереження, перетворення, захисту, обробки, передачі й одержання інформації). Усі сучасні зазначені технології зорієнтовані на об'єднання в мережі з єдиним програмним забезпеченням, що носить характер глобальної інформатизації.

Початок третього тисячоліття позначився оновленими поглядами світової спільноти в майбуття, визначенням ціннісних властивостей суспільного життя, які характеризують його якість. Світ визнав, що добробут, освіта та здоров'я людини є головними чинниками якості її життя, а якість освіти – основною метою, пріоритетом розвитку суспільства XXI ст. [1, с. 4].

Особливої уваги потребує належна професійна підготовка майбутніх працівників правоохоронних органів України, адже сучасний стан застосування інформаційних технологій у всіх галузях права потребує розширення їх впровадження у правоохоронній діяльності.

Сьогодні неможливо уявити собі ефективну роботу правоохоронних органів з попередження, розкриття та розслідування злочинів, встановлення осіб, які їх вчинили без використання сучасних інформаційних технологій. Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських організацій, а також в оперативно-розшуковій, слідчій та експертній роботі органів внутрішніх справ. Для цього широко застосовуються інформаційні технології та відповідне спеціальне програмне забезпечення.

Стрімкий розвиток інформаційно-комунікаційних технологій створив об'єктивні передумови щодо використання сучасної комп'ютерної техніки в процесі професійної підготовки. На сьогодні комп'ютер та інформаційні технології є не лише предметом вивчення цілої низки навчальних дисциплін, а й засобом здійснення навчальної, наукової і професійної діяльності фахівця, який виконує свої професійні обов'язки в умовах інформаційного суспільства, в якому інформація й технології її опрацювання перетворюються на стратегічний ресурс. Саме тому комп'ютерно-інформаційна підготовка випускника вищого юридичного навчального закладу займає одне з пріоритетних місць у процесі визначення професійної компетентності випускника та його та здатності до здійснення певної професійної діяльності [2, с. 15].

Юрист-правоохоронець – це професіонал, який має фундаментальні та спеціальні юридичні знання, глибоко переконаний у винятковому призначенні права, верховенства права і законності

для суспільства, кваліфіковано користується юридичним інструментарієм при розв'язанні юридичних проблем в ім'я захисту прав і законних інтересів громадян.

Безперечно, професійна діяльність юриста пов'язана з опрацюванням значних обсягів нормативно-правової бази з різних галузей права для аналізу різноманітних нестандартних конфліктів, кваліфікації правопорушень, тих чи інших суперечливих з точки зору чинного законодавства ситуацій. На сьогодні обсяг правової матерії настільки великий, що для оперативного доступу до неї, систематизації, а також своєчасного і коректного використання все більш актуальним стає застосування спеціалізованих інформаційно-технічних і програмних засобів.

Саме для цього призначені комп'ютерні правові системи із законодавства, що знайшли широке розповсюдження у науковій, методичній, навчальній роботі провідних юридичних вищих навчальних закладів та у практичній професійній діяльності фахівців у галузі права. Напрацювання майбутніми правниками стійких навичок роботи з правовими інформаційно-пошуковими системами стало складовою їхньої комп'ютерно-інформаційної підготовки, що дозволяє майбутньому юристу впевнено орієнтуватися у мінливому правовому полі, адекватно реагувати на зміни і доповнення у чинному законодавстві [3, с. 46].

Фахівець-правоохоронець має досконало орієнтуватися в пошукових системах Інтернету, мати здатність швидко знайти необхідну для роботи нормативну базу, а також навички швидкої адаптації до незнайомих йому програм. Також фахівець у сфері юриспруденції має володіти навичками роботи з правовими базами та їх пошуковими системами (наприклад, «Ліга», «НАУ», «Експерт» та ін.). Такі навички є складовими інформаційної культури юриста, тобто такого рівня інформаційної підготовки, який дозволяє не тільки вільно орієнтуватися йому в потрібному інформаційному середовищі, а й брати участь у його формуванні та перетворенні.

Категоріями інформаційної культури особи можна вважати також її вміння формулювати свою потребу в інформації, ефективно здійснювати пошук необхідної інформації в усій сукупності інформаційних ресурсів, переробляти і створювати якісно нову інформацію, вести індивідуальні інформаційно-пошукові

системи, відбирати та оцінювати інформацію, а також здатність до інформаційного спілкування і комп'ютерну грамотність.

Коректне і впевнене володіння комп’ютерними засобами пошуку і зберігання правових матеріалів, навички аналізу нормативно-правових актів на предмет відповідності і придатності для кваліфікації фабул правових задач, підготовка власних документів з використанням знайдених правових інформаційних матеріалів стають невід’ємною складовою професійної діяльності правознавця в умовах інформаційного суспільства.

1. Забезпечення якості вищої освіти: європейський досвід та реалії українського класичного університету: навч. посіб./укл. : Р.І. Петришин, О.Г. Ущенко, М.Г. Іванчук та ін. – Чернівці: Чернівецький нац. ун-т, 2013. – 208 с.
2. Співаковський О.В. Інформаційні технології в юридичній діяльності: базовий курс: [навч. посібн.] / О.В. Співаковський, М.І. Шерман, В.М.Стратонов, В.В.Лапінський. – Херсон: ХДУ, 2012. – 220с.
3. Шерман М.І. Правова інформаційно-пошукова система «ЛІГА: ЗАКОН. Юрист» як засіб комп’ютерної підтримки навчання правових дисциплін / М.І. Шерман // Науковий часопис Національного педагогічного університету ім. М.П. Драгоманова.: Збірник наукових праць. – 2011. – Вип. 11 (18). – С. 46–51.

СИСТЕМА ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ НАРЯДАМИ ПАТРУЛЬНОЇ ПОЛІЦІЇ

Горпинченко Євген Григорович,
інженер сектору зв'язку та телекомунікацій Управління патрульної поліції в м. Львові

Система централізованого управління нарядами патрульної служби (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й поліції.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами поліції для ефективного реагування на повідомлення про злочини та події.

Досягнення зазначеної мети забезпечується виконанням таких завдань:

- оптимізація роботи нарядів поліції, задіяних для охорони громадського порядку в системі єдиної дислокації;
- скорочення часу реагування на повідомлення громадян про злочини та події, попередженню правопорушень й затримання злочинців по «гарячих слідах»;
- здійснення оперативного контролю за своєчасністю і якістю реагування нарядами на злочини та правопорушення, дотриманню законності під час виконання службових обов'язків працівниками поліції.

Скорочення часу реагування на повідомлення громадян про злочини та події відбувається за рахунок оптимізації відповідних інформаційних потоків.

Потоки інформації, які надходять в службу «102», можна оцінити таким чином:

- загальне навантаження на службу «102» – близько 3 тис. викликів на добу;
- середній час дозвону заявника – 3–5 сек.;
- сумарний потік інформації на один пульт – до 280 звернень за добу.

Повідомлення отримані оператором служби «102» оперативно надходять в електронному вигляді до чергового-диспетчера, який:

- своєчасно визначає сили реагування (відповідні патрулі) та координує їх роботу;
- оперативно керує роботою патруля (у автоматизованому голосовому та режимі);
- ретельно контролює роботу патруля на маршруті (якість реагування патруля на повідомлення про злочини та правопорушення).

Організаційно система «ЦУНАМІ» складається з двох рівнів – міський та районний.

До складу міського рівня організаційної структури входять наступні підрозділи.

1. Центр прийняття повідомлень – служба «102».
2. Диспетчерський центр управління (чергові, диспетчери-оператори системи).
3. Центр інформаційно-технічного супроводу системи.
   - 3.1. Геоінформаційна система (електронна карта міста).
   - 3.2. Система супутникового GPS-позиціювання та мобільного комунікаційного обладнання.
   - 3.3. Система відеоспостереження.
   - 3.4. Система колективного відображення.

До складу районного рівня організаційної структури входять наступні підрозділи.

1. Чергові частини районних відділень.
2. Підрозділи громадської безпеки.
3. Мобільні патрульні наряди.
4. Слідчо-оперативні групи.
5. Додаткові сили.

Як свідчить аналіз, в результаті впровадження системи «ЦУНАМІ» досягнуто наступних позитивних зрушень в роботі патрульної поліції:

- з'явилася можливість централізованого управління диспетчерами-черговими всіма нарядами поліції по попередженню правопорушень та розкриттю злочинів по «гарячих слідах». Патрульні наряди, а також слідчо-оперативні групи стали діяти більш узгоджено під єдиним керівництвом і контролем диспетчера-чергового;
- скоротився час прибуття нарядів на повідомлення громадян про злочини і події;
- став можливим якісний контроль за проходженням інформації від служби «102» до конкретного виконавця;
- відбувається об'єктивна реєстрація та безумовне реагування на всі події (унаслідок посилення контролю з боку диспетчерів-чергових за своєчасністю та якістю реагування нарядів на злочини та правопорушення);
- удосконалений контроль за дотриманням маршруту несення служби наряду (система автоматично повідомляє диспетчера про ухилення від маршруту);
- керівники отримали можливість відстежувати рух нарядів за минулий період несення служби. За допомогою системи можливо переглянути траєкторію руху патрулів, адреси перебування, тривалість зупинок на тих або інших ділянках маршруту;
- покращено роботу оперативних служб по розкриттю злочинів. У оперативних працівників з’явилась можливість використовувати під час розкриття злочинів записану відеоінформацію.

Водночас, в інших регіонах України система «ЦУНАМІ» тільки вводиться в експлуатацію.

Реалізація проекту «ЦУНАМІ» в інших регіонах України забезпечить подальший стабільний соціально-економічний розвиток міста, підвищить захист життя, здоров'я, власності громадян від протиправних посягань та ефективність контролю за об'єктами інфраструктури країни.

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ОВС УКРАЇНИ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Дабіжа Дмитро Вікторович,
ад'юнкт кафедри криміналістики та судової медицини
Національної академії внутрішніх справ
Хахановський Валерій Георгійович,
професор кафедри інформаційних технологій
Національної академії внутрішніх справ,
доктор юридичних наук, професор

Стрімкий розвиток останніми роками засобів комп'ютерної техніки та інформаційних технологій у сучасному світі спричинив активне використання у боротьбі зі злочинністю комп'ютерних інформаційних систем. У сучасних умовах діяльності правоохоронних органів спостерігається стала тенденція подальшого збільшення обсягів інформації про причини окремих правопорушень та умови, що сприяють їх вчиненню, про пошук найбільш ефективних форм і методів їх запобігання тощо.

Одним із найважливіших факторів, що визначають успіх й ефективність розслідування, є рівень його інформаційного забезпечення. Цей факт підтверджений практикою боротьби зі злочинністю [1, с. 111].

Згідно із ст. 93 Кримінального процесуального кодексу України, збирання доказів здійснюється шляхом проведення слідчих (розшукових) дій та негласних (розшукових) дій, витребування та отриманняречей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених Кодексом. Крім того, джерелом доказової інформації можуть бути численні інформаційні системи, які містять корисну для розслідування інформацію.

Використання інформаційних систем має наступну мету:

- уніфікація технологічних процедур, збирання, реєстрація, накопичення, опрацювання, систематизація інформації, яка

може бути використана для інформаційного забезпечення аналітичних досліджень, а також для суттєвого зміцнення спроможності органів і підрозділів внутрішніх справ у протидії злочинності та профілактиці, розкритті, розслідуванні кримінальних правопорушень;

- вдосконалення інформаційно-аналітичного та організаційно-технологічного забезпечення оперативно-службової діяльності органів і підрозділів внутрішніх справ України;
- виконання інформаційно-пошукових заходів, що сприяють розшуку, пошуку, відбору необхідної інформації про об'єкти, відомості про які можуть бути отримані з використанням інформаційно-облікових даних;
- забезпечення достовірності, оперативного доступу та збереження інформаційного ресурсу;
- надання оперативним підрозділам, слідчим органів досудового розслідування довідкової та орієнтуючої інформації про об'єкти обліку для використання при проведенні слідчих (розшукових) дій та негласних слідчих (розшукових) дій;
- формування на підставі інформації про об'єкти обліку аналітичних і статистичних звітів та довідок.

Отже, призначення інформаційних систем, крім безпосереднього інформаційно-аналітичного забезпечення, багато в чому орієнтовано на використання їх при проведенні слідчих (розшукових) дій та розслідуванні кримінальних правопорушень. Зазначимо, що розслідування кримінальних правопорушень являє собою процес пошуку, дослідження, та використання довідкової, орієнтуючої, криміналістично значущої інформації, за допомогою якої формується уявлення про об'єкт пізнання. Отримана інформації в результаті проведенні слідчих (розшукових) дій безпосередньо впливає на ситуацію, підтверджуючи або спростовуючи судження відносно відповідного рішення. Особливе значення для встановлення окремих фактів, криміналістично значущої інформації може мати використання сучасних можливостей ІІПС ОВС, яка аналізуючи введену на запит інформацію про певний об'єкт обліку, надасть можливість установити взаємозв'язок з іншими, а також отримати найрізноманітнішу

інформацію. Разом з тим, в процесі формування баз даних, а також використання цієї інформаційної системи під час розслідування виникає, низка проблем, що потребують вирішення.

Одна з проблем полягає у визначенні правового статусу таких систем та інформацією, що в них міститься. Наступна – у об'єктивності та достовірності інформації, що міститься у масивах інформаційних систем.

Крім того, слід зазначити, що поняття криміналістичної інформації не має однозначного визначення. Зокрема, М.В. Салтевський розумів криміналістичну інформацію як відомості про теоретичні основи виникнення слідів злочину, практичні методи та засоби їх використання для розкриття, розслідування та попередження злочинів [2, с. 23].

Р.А. Усмановвизначав криміналістичну інформацію як «зміни, що містять зміст об'єктів, які взаємодіяли у зв'язку з подією злочину» [3, с. 18].

В.І. Галаган під криміналістичною інформацією пропонує розуміти будь-якого роду відомості, які відносяться до події, що розслідується, отримані процесуальним і непроцесуальним шляхом у процесі розслідування злочину слідчим або працівником органу дізнання відповідно до рекомендацій, розроблених криміналістикою, які можуть бути доказами у справі чи сприяти їх отриманню» [4. с. 18].

Є.Д. Лук'янчиков під криміналістичною інформацією розуміє відомості про криміналістично значимі ознаки злочину, які вилучені із залишених ним слідів суто криміналістичними засобами (у тому числі й оперативно-розшуковими), що мають відношення до розкриття, розслідування та запобігання злочинам [5, с.106].

В.В. Бірюков вважає, що криміналістична інформація – це відомості про подію злочину, отримані в результаті його цілеспрямованого пізнання криміналістичними засобами й методами з метою використання в розслідуванні для встановлення механізму та визначення ролі кожного причетного до нього об'єкта, про об'єкти, що складають масиви криміналістичних обліків, а також знання з криміналістики, які створюють умови для виявлення, вилучення й використання вказаних даних у розслідуванні та вдосконаленні науки криміналістики. Іншими

словами, це інформація, призначена сприяти розкриттю злочинів [1, с. 97].

Отже, з метою підвищення рівня ефективності ІІПС ОВС під час розслідування кримінальних правопорушень в умовах нового КПК України потрібне подальше наукове дослідження, предметом якого має бути: використання обліків та автоматизованих інформаційних систем; ґрунтовне вивчення відомостей, що містяться в інформаційних підсистемах ІІПС ОВС з метою їх використання при розслідуванні кримінальних правопорушень.

1. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: Монографія / Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2009. – 664 с.
2. Салтевский М.В. Собирание криминалистической информации техническими средствами на предварительномследствии: Учеб. пособ. – К.: РИО КВШ МВД СССР, 1980. – С. 23.
3. Усманов Р.А. Информационные основы предварительного расследования. – М.: Юрлитинформ, 2006. – С. 18.
4. Галаган В.И. Использованиеследователеминформации на первоначальномэтаперасследования: Автореф. дис. ... канд. юрид. наук. – К.: Укр. акад. внутр. дел, 1992. – С. 18.
5. Лук`янчіков Є.Д. Методологічні засади інформаційного забезпечення розслідування злочинів: Монографія. – К.: Нац. акад. внутр. справ України, 2005.

РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

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

Сучасна державна політика в Україні повинна будуватись на принципах загальнодоступності, прозорості і відкритості для громадянського суспільства. Громіздка інформаційна інфраструктура наявного державного управління потребує істотних змін, їх можна здійснити на основі нових підходів і технологій. У цьому неабияку роль відіграють інформаційно-комунікаційні технології (ІКТ). Використання ІКТ для вдосконалення державного управління, покращення відносин між державою і громадянами, організація електронних форм взаємодії між органами державної влади та органами місцевого самоврядування і фізичними та юридичними особами є одним із пріоритетних завдань побудови інформаційного суспільства в Україні. Хмарні обчислення займають одне з провідних місць у переліку сучасних інформаційних технологічних пріоритетів поряд з віртуалізацією, бізнес-аналітикою і мобільними рішеннями [1, с. 341].

У значній частині правове регулювання відносин, пов'язаних з використанням інформаційно-комунікаційні технології в Україні, у тому числі хмарних, знаходиться в руслі загальносвітових тенденцій. Серед пріоритетних завдань правового регулювання використанням інформаційно-комунікаційні технології в Україні представляється необхідним виділити наукові проблеми до числа яких доцільно віднести визначення та встановлення уніфікованої термінології та закріплення її у відповідних правових дефініціях. Слід визнати, що основним стримуючим фактором при використанні хмарних технологій в діяльності органів державної влади та органів місцевого самоврядування, а також більш широкого розповсюдження хмарних технологій в цілому є недостатнє нормативне правове регулювання питань, пов'язаних з використанням хмарних технологій.

Проект Закон України «Про внесення змін до деяких законів України (щодо обробки інформації в системах хмарних обчислень)» характеризується невизначеністю правовий статус хмарних обчислень, відсутні розмежування вимог до обробки загальнодоступної інформації та інформації, що становить державну або комерційну таємницю тощо [2; 3, с. 10].

Серед правових проблем, пов'язаних з використанням хмарних технологій, слід звернути увагу, що в даний час відсутні нормативні правові акти, що встановлюють основні правила використання хмарних технологій, законодавчо не врегульовані питання забезпечення безпеки та конфіденційності інформації, що передається постачальнику хмарних послуг, не закріплені норми, що визначають адміністративну та цивільно-правову відповідальність постачальника хмарних послуг, а також відповідальність керівників і працівників організацій, що надають хмарні послуги.

Необхідність правового вирішення зазначених проблем пов'язана і з розробкою Державним агентством з питань електронного урядування України єдиної мережі передачі даних для органів державної влади Government Cloud (з англ. «урядова хмара»), створюваної в цілях підвищення якості телекомунікаційних і обчислювальних послуг, що надаються органами влади, а також формування умов, що стимулюють ліквідацію цифрової нерівності.

Видається, що необхідна розробка нормативного правового акту, спрямованого на врегулювання відносин при використанні нових інформаційних технологій, зокрема між провайдерами та споживачами хмарних послуг при передачі інформації постачальнику хмарних послуг, а також стандартів безпеки хмарних технологій, що використовуються органами державної та місцевої влади і органами місцевого самоврядування, а також в міжнародному інформаційному обміні.

У Аналітичній записці Національного інституту стратегічних досліджень при Президенті України «Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики» вказано, що, за підрахунками авторитетної International Data Corporation (IDC), вже у 2015 році до 60 % всіх даних людства зберігатиметься у хмарах [4]. В силу глобальності інформаційного

суспільства та розвитку транскордонних процесів важливим завданням стає забезпечення безпеки персональних даних, що використовуються в різних інформаційних системах і подальше вдосконалення нормативного правового регулювання забезпечення інформаційної безпеки.

У зв'язку з цим слід відзначити значення внесення змін і доповнень до Закону України «Про захист персональних даних» щодо реалізації Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних яка була ратифікована відповідно до Закону України від 06.07.2010 № 2438-VI «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» і впровадження Типового порядку обробки персональних даних затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 [5].

Однак необхідно визнати, що існують проблеми в законодавстві України щодо положень Конвенції Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних пов'язані з визначенням регулятора в даній сфері, а також відсутності диференціації типів персональних даних і відповідного поділу вимог щодо їх обробки. Положення чинного законодавства спрямовані на покаранні за невідповідність вимогам контролюючих органів без урахування реального збитку, нанесеного при допущених порушеннях при обробці персональних даних суб'єкту. Таким чином, представляється необхідним вдосконалення законодавства України щодо відповідності положень Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних, в частині передачі повного обсягу повноважень з регулювання та нагляду за порядком обробки персональних даних одному регулятору.

Водночас передача контролюючих функцій у сфері захисту прав суб'єкта персональних даних в незалежний уповноважений орган (Уповноваженому Верховної Ради України з прав людини) дозволила увійти Україні до складу країн з адекватним захистом прав суб'єкта, оскільки згідно з положеннями Конвенції Ради

Європи про захист фізичних осіб при автоматизованій обробці персональних даних, уповноважений орган не повинен входити в структуру органів виконавчої влади.

Враховуючи багато аспектів проблеми, які вимагають наукових досліджень представляється доцільним виділення інституту персональних даних в окремий міжгалузевий правовий інститут, а також розробка концепції організаційно-правового забезпечення інформаційної безпеки при передачі даних на основі транскордонного електронного документообігу з метою забезпечення безпеки і простору довіри.

Реалізація запропонованого вимагає визначення та систематизації проблем у даній сфері. Виходячи з аналізу практики Європейського Союзу представляється необхідним розробка правового акту, що регулює і роз'ясняє положення Закону України «Про захист персональних даних», аналогічного директивам Європейського Союзу та положенням Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних, а також розробка окремих вимог щодо захисту прав суб'єктів персональних даних для суб'єктів малого та середнього бізнесу.

Заслуговує на увагу питання реалізації принципу мережевий нейтральності. Щоб уникнути використання технічних механізмів та інфраструктури мережі Інтернет з метою недобросовісної конкуренції, що можливого внаслідок відсутності законодавчо закріплених вимог, які забороняють використовувати технічні механізми дискримінації трафіку, контенту, додатків, сайтів, платформ і сервісів представляється необхідним розглянути питання про встановлення обов'язків сторони, відповідальної за передачу або маршрутизацію даних, щодо будь-якого пакета даних, незалежно від контенту, джерела або призначення, сервісу, терміналу або додатку, встановлення заборони дискримінації трафіку або погіршення якості послуг, яке не можна віднести до необхідних технічних вимог для адекватного надання послуг, встановлення заборони на перешкоджання щодо отримання або відправці легального контенту, додатків і сервісів, а так само підключення до мережі пристроїв, що здійснюють крадіжку сервісів або які порушують роботу мережі.

Використання хмарного середовища для реалізації функцій державного управління, розвитку судової системи та деяких

інших проектів сьогодні визначені як пріоритетні завдання тому потрібно законодавче регулювання в даній сфері.

1. Вітер М.Б. Використання хмарних технологій у системі інформаційної взаємодії державних органів / М.Б. Вітер, Х.О. Засадна // Наук. вісник Нац. лісотехнічного ун-ту України. – 2014. – Вип. 24.9. – С. 341-347.
2. Закон України (проект) «Про внесення змін до деяких законів України (щодо обробки інформації в системах хмарних обчислень). [Електронний ресурс]. – Режим доступу: reforms.in.ua/Content/download/Initiatives/.../Cloud _DraftLaw.docx
3. Серенок А.О. Нормативно-правове забезпечення впровадження електронного урядування в Україні: ініціативи президента України / А.О. Серенок // Державне будівництво. – 2015. – № 1. – С. 1-12.
4. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles /1191/#_ftn2
5. Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних». [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/v1_02715-14/paran11#n11

ШЛЯХИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Живко Зінаїда Богданівна,
завідувач кафедри менеджменту
Львівського державного університету внутрішніх справ
доктор економічних наук, професор
Баваровська Олена Богданівна,
викладач Львівського коледжу мясної та молочної
промисловості НУХТ, кандидат економічних наук
Живко Павло Богданович,
магістрант економічного факультету
Львівського державного університету внутрішніх справ

Актуальність та постановка проблематики. Саме суспільство є носієм такої глобальної загрози інформаційній безпеці людини, як інформаційна дискримінація, яка проявляється в розподілі людей на тих, які мають доступ до інформації, і тих, які його не мають. Тому якраз висока інформаційна культура повинна стати перешкодою для розповсюдження інформаційної дискримінації. Ці питання особливо важливі і потребують постійного вивчення та дослідження.

Мета дослідження. Різносторонньо дослідити основні аспекти забезпечення інформаційної безпеки, технічний захист інформаційних ресурсів та нормативне закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки.

Виклад основного матеріалу. Проблеми інформаційної безпеки в загальному випадку можна поділити на два класи: захист інформації (запобігання загроз інформації); захист від інформації (запобігання інформаційних загроз).

Тобто, слід розрізняти два аспекти інформаційної безпеки: технічний і гуманітарний, кожний з яких має зовнішню та внутрішню складові. Обидва ці аспекти перш за все стосуються людини і її інформаційної культури.

Технічний аспект інформаційної безпеки полягає у здатності і вмінні людини передбачати та попереджувати *загрози інформації,* яка циркулює в технічних системах, і загрози самим системам.

Однак, технічний аспект не є головним в структурі інформаційної безпеки. Необхідно забезпечити не лише безпеку *інформації* від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку їх маршрутизації, але й інформаційну безпеку суспільства, попередити негативний вплив на навколишнє середовище, який може мати місце як результат непередбачених видів обробки інформації.

Проблеми захисту від інформації суттєво складніші за проблеми захисту інформації, оскільки загрози від інформації надзвичайно різноманітні, їх вплив не завжди очевидний, він здійснюється навмисно, витончено і підступно, а відвернення цих загроз і нейтралізація вимагають різноманітних неординарних дій.

Загрози інформаційній безпеці – це дія дестабілізуючих факторів, пов'язаних з витоком інформації, її перекручуванням, порушенням законів і норм, що може спричинити потенційні або реальні втрати для організації.

Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

Види загроз інформаційній безпеці підприємства класифікують за такими ознаками**:**

- за місцем виникнення: внутрішні; зовнішні;
- за природою виникнення: політичні; кримінальні; технічні; від особи;
- за ймовірністю виникнення: явні; приховані;
- за наслідками: загальні; локальні;
- за відношенням до людської діяльності: об'єктивні; суб'єктивні (зумовлені діяльністю людини) [1].

Інформаційні загрози є складним ієрархічним утворенням з множиною різнорівневих зв'язків, їх вплив на людину комплексний і різноманітний. Для того, щоб спростити класифікацію і впорядкування, умовно всі інформаційні загрози поділяють на дві категорії:

- *макрозагрози* (загрози, які перебувають в інформаційному просторі суспільства й існують незалежно від психологічних і розумових особливостей конкретної особистості);
- *мікрозагрози* (загрози, які діють на рівні людської свідомості).

До найважливіших об'єктів інформаційних загроз відноситься духовна сфера суспільства, складовими якої є суспільна свідомість, суспільна думка і соціально-психологічний клімат.

Сьогодні в Україні відбувається активне насадження прозахідних цінностей, а значить, формування ідеології, що суперечить національному менталітету, тобто спрямованої на підрив інформаційної стійкості і, відповідно, інформаційної безпеки людини. Тому недаремно точаться гарячі дискусії щодо того, якою має бути сучасна ідеологічна концепція, національна ідея.

Безумовно, формування нової системи цінностей і вироблення ідеологічної системи, спрямованої на її підтримку, є складним завданням, яке вимагає ґрунтовного опрацювання і дослідження. Разом з тим, відсутність такої системи шкодить як інформаційній безпеці окремих громадян, так і безпеці держави загалом. Зазначена ситуація ускладнюється тим, що сама держава відвернулася від інформаційного й ідеологічного захисту своїх громадян. Це ще раз підтверджує необхідність спрямування інформаційної культури на формування інформаційного імунітету особистості, забезпечення її інформаційної стійкості.

Принципове значення для сучасного суспільства має факт існування інформаційної картини світу, тобто нашого уявлення про світ, що формується ЗМІ. І це уявлення є важливішим, ніж сам світ. Віртуальна реальність створена мас-медіа впливає на свідомість та підсвідомість людини.

Одним з найрозповсюдженіших видів інформаційних загроз є так звані *патогенні тексти* [1; 2]. До патогенних відносять тексти і повідомлення, які суперечать діючій ідеологічній системі. Зокрема, у різних системах цінностей патогенними вважаються тексти, що:

а) спрямовані на підрив віри у Бога;

б) на підрив національних та державних інтересів;

в) загрожують суспільній моралі;

г) загрожують глобальній безпеці;

д) мають шкідливий психологічний вплив;

є) призводять до нехтування основними правами і свободами.

Забезпечення інформаційної безпеки держави вимагає вирішення цілої низки ключових проблем:

- розвиток науково-практичних основ інформаційної безпеки, сучасної геополітичної ситуації, що відповідає умовам політичного і соціально-економічного розвитку держави;
- формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки:
- розробка реєстру інформаційного ресурсу;
- розробка регламенту інформаційного обміну для органів державної влади і управління, підприємств;
- нормативне закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки;
- розробка механізмів реалізації прав громадян на інформацію.
- формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни;
- розробка сучасних методів і технічних засобів, що забезпечують комплексне вирішення завдань захисту інформації;
- розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікації;
- дослідження форм і способів цивілізованої дії держави на формування суспільної свідомості;
- комплексне дослідження діяльності персонале інформаційних систем, зокрема методів підвищення мотивації, морально-психологічної стійкості і соціальна захищенність людей, що працюють з секретною і конфіденційною інформацією.

Крім того, до патогенних текстів належать такі, що містять державну та інші види таємниці, втручаються в особисте життя тощо.

Закрити національний інформаційний простір від зовнішнього інформаційного впливу адміністративними заходами неможливо. Його треба оберігати так само, як наземний, повітряний і

морський. Інформаційна безпека України не зводиться винятково до захисту відомостей і даних. На першому місці повинна стояти проблема захисту від інформації. В цьому аспекті необхідно терміново й істотно удосконалити законодавчу базу становлення цивілізованих інформаційних відносин [2; 3].

Найдокладніший перелік можливих загроз інформаційній безпеці країни і засобів їх реалізації завжди буде неповним, бо зміни в суспільних відносинах, розвиток інформаційних технологій та засобів інформатизації спричинюють виникнення нових загроз. Одночасно джерела загроз інформаційній безпеці залишаються досить сталими. До джерел загроз належать:

- недружня політика іноземних держав в галузі глобального інформаційного моніторингу, поширення інформації та новітніх інформаційних технологій;
- цілеспрямована діяльність іноземних спецслужб, політичних та економічних структур;
- злочинна діяльність міжнародних угрупувань, формувань та окремих осіб;
- неправомірна чи протиправна діяльність посадових осіб державних органів, структур, формувань, спрямована проти інтересів України;
- стихійні лиха, катастрофи, збройні конфлікти;
- некерований характер процесу створення інформаційної інфраструктури України;
- недосконалість технічних і програмних засобів й недостатня кваліфікація персоналу інформаційних служб і систем;
- недосконалість, неповнота і неузгодженість з відповідними міжнародними правовими актами чинного законодавства України в інформаційній сфері;
- недостатній розвиток лексикографічної бази української мови і національного лінгвістичного забезпечення інформаційних систем;
- низькі темпи науково-технічного і культурного розвитку суспільства внаслідок економічної кризи або неадекватної внутрішньої політики держави в інформаційній сфері;
- низька правова, організаційна та програмно-технічна забезпеченість в галузі інформаційної безпеки.

Засоби впливу загроз на інформаційну безпеку поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові.

Спроба реалізації загрози називається *атакою*, а особа, яка вчиняє таку спробу, – зловмисником. Потенційні зловмисники називаються *джерелами загрози.*

Здебільшого загроза є наслідком наявності вразливих місць в захисті інформаційних. *Вікно небезпеки* – це проміжок часу від моменту, коли з'являється можливість використовувати слабке місце, і до моменту, коли пропуск ліквідовується. Наявність вікна небезпеки уможливлює успішність атаки на інформаційну систему. За умов помилок в ПО, вікно небезпеки «відкривається» з появою засобів використання помилки і ліквідовується при їх виправленні (тобто при накладенні латок).

Для більшості вразливих місць вікно небезпеки існує декілька днів, інколи – тижнів, бо за цей час повинні статися наступні події:

- мають бути встановлені засоби використання пропуску в захисті;
- мають бути випущені відповідні латки;
- латки мають бути встановлені в інформаційній системі, що захищається [4].

Отже, нові вразливі місця і засоби їх використання з'являються в інформаційних системах постійно, що означає:

1) майже завжди існують вікна небезпеки;
2) відслідковування таких вікон повинне проводитися постійно;
3) випуск і накладення латок має здійснюватися оперативно.

Деякі загрози не можна вважати наслідком якихось помилок або прорахунків – вони існують через саму природу сучасних ІС. Наприклад, загроза відключення електрики або виходу його параметрів за допустимі межі існує через залежність апаратного забезпечення ІС від якісного електроживлення.

Зазвичай, поняття «загроза» в різних ситуаціях трактується по-різному, а саме: для відкритої організації загрози конфіденційності інформації може не існувати – вся інформація вважається загальнодоступною; однак, нелегальний доступ до інформаційних ресурсів є серйозною небезпекою. Тобто, загрози, як і все

в інформаційній безпеці, залежать від інтересів суб'єктів інформаційних відносин та від межі і рівня збитковості (і від того, який збиток є для них неприйнятним).

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ. Слід виходити з того, що необхідно конструювати надійні системи (інформаційної безпеки) із залученням ненадійних компонентів (програм). В принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності на всьому протязі життєвого циклу ІС.

Спроба реалізації загрози називається *атакою*, а особа, яка робить таку спробу, – *зловмисником*. Потенційні зловмисники називаються *джерелами загрози* [1; 3].

Зазвичай, загроза є наслідком наявності вразливих місць в захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки у програмному забезпеченні).

Проміжок часу від моменту, коли з'являється можливість використовувати слабке місце, і до моменту, коли пропуск ліквідовується, називається *вікном небезпеки*. За умови існування вікна небезпеки, можливі успішні атаки на ІС.

Висновки. Найпоширенішими технічними загрозами, характерними для сучасних інформаційних систем є перепади напруги в системах електропередач, відключення енергопостачання тощо. Тому важливо знати як про можливі загрози, так і про вразливі місця, які ці загрози зазвичай використовують, для того, щоб вибирати найбільш економічні засоби забезпечення безпеки. Незнання суті загроз призводить до перевитрат засобів та концентрації ресурсів захисту там, де вони не особливо потрібні, за рахунок ослаблення дійсно уразливих напрямів.

Отже, забезпечення інформаційної безпеки держави вимагає наступних дій: розвивати науково-практичні основи інформаційної безпеки; сформувати законодавчу і нормативно-правову базу забезпечення інформаційної безпеки; розробити механізми реалізації прав громадян на інформацію; розробити сучасні методи і технічні засоби, що забезпечують комплексне вирішення завдань захисту інформації; забезпечити комплексне

дослідження діяльності персоналу інформаційних систем, зокрема методів підвищення мотивації, морально-психологічної стійкості і соціальної захищеності людей, що працюють з секретною і конфіденційною інформацією.

1. Живко З.Б. Правові основи охорони інформації / З.Б. Живко, В.В. Сердюков, О. М. Стаднік, В. О. Хорошко. – [за ред. проф. В. О. Хорошка]. – Вид.2. – К.: Вид. ДУІКТ, 2009. – 335 с.;
2. Живко З.Б. Захист інформації / З. Б. Живко, М. О. Живко. – Конспект лекцій. – Львів: Ліга-Прес, 2009. – 112 с.
3. Живко З.Б. Інформаційна безпека та захист інформації: Навч. посіб. / Живко З.Б., Живко М.О., Босак Х.З. Львів: Ліга-Прес, 2010. – 145 с.
4. Живко З.Б. Захист інформації в управлінні системами економічної безпеки підприємства // Матеріали ІІІ МНПК «Сучасні проблеми інноваційного розвитку держави». – Том 7. Дніпропетровськ: ПДАБА, 2008. – С. 46-47. (108 с.)

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Живко Михайло Олександрович,
головний спеціаліст відділу реєстрації Пустомитівського районного управління юстиції,
кандидат юридични наук
Босак Христина Зіновіївна,
старший слідчий слідчого управління ГУ Національної поліції у Львівській області, кандидат юридични наук
Вольних Анастасія Іванівна,
студентка ІКТА НУ «Львівська політехніка»

Актуальність та постановка проблематики. Інформаційна безпека сьогодні є чи не однією з найпоширеніших проблем як на макро, так і на мікрорівні. Велике значення відіграє висока присутність держави в інформаційному просторі, що не сприяє принципам вільного доступу громадян до джерел інформації. Все це обмежує доступ громадян до отримання повної об'єктивної інформації, що є неправильним і недопустимим в демократичній державі, так як обмежує права громадян щодо інформації, призводить до цілої низки проблем, які потребують дослідження.

Мета дослідження. Дослідити особливості та специфіку забезпечення інформаційної безпеки.

Виклад основного матеріалу. Друковані ЗМІ, книговидання, бібліотечний, архівний та кінематографічний комплекси зазнають скорочення, що не відповідає потребам розвинутих країн і ставить Україну відповідно на нищий рівень від інших розвинутих країн.

Інтернет, мобільний зв'язок знаходяться в кращому стані та доходи наших громадян не дають можливості вільного доступу до них.

Погоджуємося з автором [1], що інформаційна безпека досягається реалізацією єдиної державної політики у цій галузі, яка будується на принципах:

- законності;

- дотримання балансу життєво важливих інтересів держави, суспільства та особистості;
- взаємної відповідальності держави, суспільства та особистості за стан безпеки;
- інтеграції з міжнародними системами забезпечення інформаційної безпеки.

Тобто, державна політика забезпечення інформаційної безпеки країни визначає основні напрямки діяльності органів державної влади у цій галузі. Ці напрямки обумовлені змістом національних інтересів держави, суспільства та особистості. По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [2]. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством [3].

Діяльність держави та її органів у сфері забезпечення інформаційної безпеки є багатогранною: це захист державних секретів, дотримання та охорона конституційних прав громадян в інформаційній сфері тощо. Через те організація діяльності держави у питаннях забезпечення інформаційної безпеки – це послідовний безперервний процес, спрямований на розробку і здійснення правових, організаційних, технічних та інших заходів у цій сфері. Крім цього, інформаційна безпека повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України [1].

Можна стверджувати, що інформаційна безпека передбачає можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й розповсюдження інформації. Поняття інформаційної безпеки держави слід також розглядати у контексті забезпечення безпечних умов існування

інформаційних технологій, які включають питання захисту інформації, як такої інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть вчинити збиток чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Отже, **інформаційна безпека держави** – це стан захищеності інформаційного середовища, що забезпечує умови функціонування держави незалежно від можливих (прогнозованих чи передбачуваних) і реальних внутрішніх і зовнішніх загроз.

В Україні хоча й функціонує система забезпечення інформаційної безпеки та сам розподіл між окремими суб'єктами системи та схеми їх взаємодії потребують вдосконалення.

Інформаційна безпека – це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних стосунків, зокрема власникам і користувачам інформації і підтримуючої інфраструктури [4].

Захист інформації – це комплекс заходів, направлених на забезпечення інформаційної безпеки.

Практично захист інформації відбувається методом підтримання цілісності, доступності, а якщо потрібно – конфіденційності інформації і ресурсів, які використовуються для введення, зберігання, обробки і передачі даних. До основних механізмів безпеки, що забезпечують захист інформаційних ресурсів, належать

- управління доступом;
- протоколювання і аудит;
- ідентифікація та аутентифікація;
- криптографія;
- екранування.

Необхідно звернути увагу на ступінь важливості інформаційних ресурсів, адже саме від цього і залежить необхідний рівень захисту. Інформація, дані та знання, в межах інформаційної економіки є найбільш перспективним товаром, потребують відповідної реклами на конкретних сегментах ринку. При цьому повинна відбуватися класифікація і структуризація інформаційних ресурсів за їх цінністю, що дає можливість регламентувати доступ до них і сформулювати відповідні пропозиції контрагентам. Результатом даного процесу є формування ціни запропонованих інформаційних ресурсів і відкриття споживачам деяких даних, інформації і знань для її підтвердження. Процес ціноутворення для інформаційних ресурсів – достатньо складний, враховуючи конкуренцію джерел інформації, проблеми динаміки її корисності та цінності, велику кількість потенційних загроз несанкціонованого одержання і використання. Умовно загрози можна поділити на випадкові та навмисні.

Навмисні загрози шляхом їх систематичного застосування можуть виконуватися через випадкові або підготовлені атаки несанкціонованими запитами або вірусними програмами.

Наслідки, до яких призводить реалізація загроз – втрата інформації, модифікація (змінення інформації на неправдиву, вона коректна по формі і змісту, але має інше значення) і ознайомлення з інформацією сторонніх.

Результат таких змін може бути непередбачуваний: від невинних непорозумінь до величезних фінансових втрат. Попередження таких наслідків – основне завдання інформаційної безпеки. Для створення засобів захисту інформації необхідно визначити природу загроз, форми і шляхи їх можливого виявлення та здійснення в інформаційній системі.

На сьогоднішній день неможливо уявити будь-яку організацію без електронних даних. Документи та бухгалтерія, рахунки клієнтів та організацій, пошта, рекламна інформація, програми, файли з графічними відео/аудіо даними, корпоративні бази даних тощо – все знаходиться на дисках серверів локальних мереж. Отже, інформація – це свого роду серце, яке забезпечує життєдіяльність корпорацій чи підприємств.

Джефф Хайн, керівник підрозділу професійного обслуговування компанії Berkshire Computer Products (Хопкинтон, шт.

Массачусетс) зауважує, що як не дивно, але більшість компаній досі ставляться до питання створення структури збереження даних зовсім несерйозно – вони просто збільшують кількість серверів та розширюють обсяги дискового простору [5].

Натомість втрата інформації може загрожувати підприємству повним крахом. Така ситуація а області забезпечення інформаційної безпеки потребує нагального вирішення на загальнодержавному рівні.

Правильний з методологічної точки зору підхід до проблем убезпечення інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). *Загрози інформаційній безпеці* – це зворотна сторона використання інформаційних технологій.

З цього положення можна вивести два важливі наслідки:

1. Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно відрізнятися.
2. Інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це принципово ширше поняття. Суб'єкт інформаційних стосунків може постраждати (зазнати збитків і/або отримати моральний збиток) не лише від несанкціонованого доступу, але і від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій (наприклад, учбових) власне захист від несанкціонованого доступу до інформації стоїть по важливості зовсім не на першому місці.

Комп'ютерна безпека (як еквівалент або замінник ІБ) представляється нам дуже вузьким. Комп'ютери – тільки одна з складових інформаційних систем, і хоча наша увага буде зосереджена насамперед на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, насамперед, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно визначення інформаційної безпеки, вона залежить не лише від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий

персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою наказаних нею функцій. Тому зосередимо увагу на тому, що у визначенні ІБ перед іменником «збиток» стоїть прикметник «неприйнятний». Очевидно, застрахуватися від всіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Значить, з чимось доводиться миритися і захищатися слід лише від того, з чим змиритися ніяк не можна. Інколи таким неприпустимим збитком є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше межа (поріг) неприйнятності має матеріальне (грошове) вираження, а метою захисту інформації стає зменшення розмірів збитку до допустимих значень.

Інформаційна безпека – багатогранна, багатовимірна сфера діяльності, в якій успіх може принести лише системний, комплексний підхід.

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів і підтримуючої інфраструктури.

Висновки. Для цього необхідно розробити основні напрямки державної політики в галузі забезпечення інформаційної безпеки, а також заходів і механізмів, пов’язаних з реалізацією політики розвитку і удосконалення системи забезпечення інформаційної безпеки, удосконалюючи форми, методи і засоби виявлення, оцінки та прогнозування загроз інформаційної безпеки, а також систем протидії цим загрозам.

Також необхідно розробити критерії і методи оцінки ефективності систем і засобів забезпечення інформаційної безпеки і сертифікації цих систем і засобів. Необхідним також видається удосконалення нормативної правової бази забезпечення інформаційної безпеки, включаючи механізми реалізації прав громадян на одержання інформації та доступу до неї, форми і способи реалізації правових норм щодо координації діяльності різноманітних підприємств незалежно від форм власності в галузі забезпечення інформаційної безпеки. Щодо економічних методів

забезпечення інформаційної безпеки, то, в першу чергу, необхідно розробити програми забезпечення інформаційної безпеки та визначити порядок їх фінансування, удосконалення системи фінансування робіт, пов'язаних з реалізацією правових та організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків юридичних та фізичних осіб.

1. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук. – [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/ trk/publikacii/satshuk_publ.php
2. Баринов А. Информационный суверенитет или информационная безопасность? / А. Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.
3. Бучило И.Л. Информационное право: основы практической информации / И. Л. Бучило. – М., 2001 – С. 253.
4. Асаул, А. Н, Организация предпринимательской деятельности: учебник / А. Н. Асаул. – СПб.: АНО ИПЭВ, 2009. 336с
5. Смирнов Н. О проблемах хранения корпоративной информации / Н. Смирнов. [Електронний ресурс]. – Режим доступу: http://citforum.ru/cfin/articles/problcorpinf.shtml

НОРМАТИВНО-ПРАВОВІ ЧИННИКИ ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захарова Олександра Василівна,
доцент кафедри криміналістики, судової медицини та психіатрії
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Сеник Святослав Володимирович,
магістрант юридичного факультету
Львівського державного університету внутрішніх справ
Ізьо Марта Ігорівна,
студентка юридичного факультету
Львівського державного університету внутрішніх справ

Питання інформаційної безпеки (ІБ) є надзвичайно важливими та актуальними сьогодні, оскільки вже давно вийшли на одне з перших місць серед інших завдань, які розв'язуються у процесі проектування, створення та використання сучасних інформаційних систем (ІС). Підвищення рівня захищеності інформаційного середовища підрозділів Національної поліції України є, на сьогодні, актуальним завданням. Одними з визначальних, у цьому плані, є нормативно-правові чинники – стандарти, закони, інфраструктурні рішення, бібліотеки кращих практик тощо. Мета в них одна – забезпечити виконання організаційно-технічних заходів з захисту інформації, що дозволить підняти рівень захищеності спеціалізованих ІС.

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

У найбільш загальному вигляді ієрархічну структуру нормативно-правових актів України у галузі технічного захисту інформації обов'язкових до виконання можна подати наступним чином:

- Конституція України;
- Закони України;
- укази та розпорядження Президента України;
- постанови та розпорядження Кабінету Міністрів України;
- нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України;
- міжнародні договори України з питань технічного захисту інформації, згода на обов'язковість виконання яких надана Верховною Радою України.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена чинним законодавством, повинна оброблятися в ІС із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи та отримання атестату відповідності [1]. Така комплексна система захисту інформації повинна забезпечувати безпечність та надійність функціонування ІС і, на переконання авторів, розробляється, впроваджується, функціонує на засадничих принципах політики інформаційної безпеки (ПІБ).

Політика інформаційної безпеки документально описує і регламентує систему управління інформаційною безпекою (СУІБ) в інформаційних систем, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів ISO/IEC 27001:2005, ISO/IEC 17799/2005 [2].

Як випливає з даних стандартів необхідно оцінити інформаційні активи ІС, розглянути і оцінити специфічні ризики щодо збереження, конфіденційності та цілісності інформації, та на основі цих кроків сформувати ПІБ, яка дозволить уникнути або мінімізувати ризики безпеки.

Метою політики інформаційної безпеки є впровадження та ефективне управління системою забезпечення ІБ, спрямованої на

захист інформаційних активів, забезпечення безперервного функціонування сервісів ІС, мінімізування ризиків ІБ.

Основним завданням впровадження ПІБ є захист інформаційних активів від зовнішніх та внутрішніх, навмисних і ненавмисних загроз. ПІБ розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для зловмисних діянь у разі несанкціонованого доступу.

Аналіз наявних у вільному доступі матеріалів стосовно проблеми безпеки інформаційних активів ІС дає змогу виявити недоліки у методології розроблення ПІБ систем захисту, які суттєво впливають на ефективність їх функціонування. Відзначимо основні з цих недоліків:

- ПІБ системи захисту інформаційних активів ІС не враховує динаміки зміни загроз;
- недостатній рівень стійкості системи захисту ІС до відмов та відновлення після збоїв;
- необхідність зосередження ресурсів підтримки систем безпеки інформаційних активів ІС на найбільш критичних напрямах;
- відсутність ефективних методик попереднього оцінювання ефективності системи безпеки інформаційних активів ІС;
- ігнорування нормативно-правовими аспектами та вимогами міжнародних стандартів у галузі ІБ при проектуванні надійної системи захисту.

ПІБ регламентує управління доступами та паролями, чіткий розподіл ролей та обов’язків, визначення вимог ІБ для кожного активу. Впровадження ПІБ в інформаційні системи забезпечує підтримку рівня безпеки на належному рівні, що у свою чергу передбачає:

- постійне навчання працівників у сфері ІБ;
- проведення контролю безпеки та доступу до ІС;
- управління інцидентами, категоріювання та забезпечення конфіденційності інформації;
- антивірусний захист, резервне копіювання, ліцензійну чистоту програмного забезпечення, вхідний/вихідний контроль за обміном інформацією у ІС;

- забезпечення фізичної безпеки та інших аспектів ІБ.

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 СУІБ. СУІБ дозволяє виявляти, враховувати, реагувати і аналізувати події та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог міжнародних стандартів і галузевих норм.

Управління інцидентами, це важливий процес, який забезпечує можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його усунути.

Основна задача управління інцидентами – 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.

Цілі, які ставлять перед СУІБ є такими:

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

Використовуючи найкращі, перевірені часом напрацювання для оброблення збоїв довільних видів, рішення з управління інцидентами дозволяють використовувати ресурси залежно від пріоритетів оперативної діяльності, управляти рівнями обслуговування, а також краще контролювати роботу ІТ-сервісів.

Для реалізування системи управління інцидентами інформаційної безпеки необхідно виконати такі роботи:

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

У результаті проведених робіт буде запроваджена СУІБ, яка розв'язуватиме наступні задачі:

- оперативний моніторинг стану ІБ в рамках функціонування ІС;
- виявлення, облік, реагування, розслідування та аналіз інцидентів ІБ;
- інформування вищого керівництва про поточний стан ІБ.

Таким чином, необхідно реалізувати комплексний підхід щодо розв'язання наступних задач:

- виявлення, інформування та облік інцидентів ІБ
- реакція на інциденти ІБ, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку;
- аналіз реалізованих інцидентів, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення ІБ в цілому.

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

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

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

Висновки. Ефективність захисту спеціалізованих ІС залежить від прийняття правильних рішень, які підтримують захист, котрий адаптується до постійно змінюваних умов функціонування і, на переконання авторів, розробляється, впроваджується, функціонує на засадничих принципах політики інформаційної безпеки.

При експлуатуванні ІС процес управління ІБ є одним з найважливіших у постачанні даних для аналізу функціонування таких систем, оцінювання ефективності використовуваних заходів, зниження ризиків і планування удосконалення роботи ІС.

1. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник. Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. –Львів: ЛьвДУВС. 2010, – с. 90-97.
2. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.

КОМП'ЮТЕРНІ ЗЛОЧИНИ ЯК СКЛАДОВА ІНФОРМАЦІЙНИХ ЗЛОЧИНІВ

Ковалів Мирослав Володимирович,
завідувач кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, професор
Іваха Валерій Олександрович,
декан факультету заочного навчання цивільних осіб
Львівського державного університету внутрішніх справ,
кандидат юридичних наук

Проект Концепції державної інформаційної безпеки України, одним з призначень якої є звернення уваги органів державної влади, засобів масової інформації, всіх зацікавлених осіб на проблеми підготовки держави, суспільства, особистості до умов життя в інформаційному суспільстві. Відповідно до проекту Концепції головним завданням є забезпечення інформаційної безпеки. У числі основних положень правового забезпечення інформаційної безпеки знаходиться захист законними засобами особистості, суспільства, держави від неправдивої інформації. Реалізація на практиці такого підходу до інформаційної безпеки може здійснюватись виключно за участі всіх суб'єктів інформаційних відносин і за умов ефективної взаємодії держави з громадянським суспільством, приватним сектором і громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту від зовнішніх загроз [1].

Проект Концепції носять програмний характер і задає цілі, досягнення яких є пріоритетним завданням. Вироблення адекватних заходів боротьби з комп'ютерними злочинами знаходиться в їх числі. І хоча багато явищ у сфері комп'ютерних злочинів залишаються невивченими є загальний погляд на способи боротьби з ними. Зокрема, піддаються детальному аналізу поняття комп'ютерної інформації та окремі види комп'ютерних злочинів. Таким чином, у кримінальному праві поняття інформації вивчається, насамперед, у зв'язку з

комп'ютерними злочинами та для визначення заходів боротьби з ними. Це дозволяє вирішити проблему кримінально-правового регулювання інформаційних відносин лише частково. Пов'язано це з тим, що інформаційна безпека, а також захист від неправдивої інформації забезпечуються не тільки заходами боротьби з комп'ютерними злочинами.

Для реалізації положень Концепції необхідний комплексний погляд на інформаційні явища, які підлягають захисту кримінально-правовими засобами.

Інформація як предмет інформаційних злочинів має нематеріальну форму, зберігається на будь-якому матеріальному носії, але не має будь-якого жорстко детермінованого зв'язку з цим носієм. У кримінальному законі такий предмет злочину виражається шляхом безпосередньої вказівки на інформацію, шляхом вказівки на матеріальний носій інформації, а також шляхом згадки документів як інформації, закріпленої на особливому матеріальному носії. Інформаційний вплив як спосіб вчинення інформаційних злочинів може бути направлено на конкретну людину і на невизначене коло осіб.

Під інформацією пропонується розуміти відомості, що передаються між суб'єктами за допомогою сигналів у формі певного коду які представляють собою цілеспрямований управлінський вплив. Закон України «Про інформацію» забороняє розповсюдження окремих видів інформації відносно невизначеного кола осіб [2]. Разом з тим, аналогічне правило щодо конкретних одержувачів інформації відсутнє. Крім цього, в законі відсутнє визначення одного з базових понять інформаційної сфери – поняття інформаційної безпеки. У цьому зв'язку набувають особливого значення дослідження, присвячені вивченню поняття соціальної інформації в кримінальному праві, зокрема, визначенню інформації як предмета злочину.

Інформаційні зв'язки є основою всіх соціальних взаємодій, при дослідженні яких доцільно використовувати інформаційний, системний і організаційний підходи. Будь-які системні або організаційні явища засновані на інформаційних взаємодіях. Вивчаючи основні форми і види інформаційних взаємодій, можна визначити інформаційний простір соціальної системи. Під соціальною інформацією, тобто інформацією яка є об'єктом

інформаційної безпеки, пропонується розуміти відомості, що передаються між суб'єктами за допомогою сигналів у формі певного коду і представляють собою цілеспрямований управлінський вплив. Ці відомості не мають фізичних характеристик, не можуть бути зрозумілі поза інформаційною взаємодією, і здатні породжувати нову інформацію у приймаючого суб'єкта. Інформаційна структура властива будь-яким системам, в тому числі і інформаційній безпеці, яка, у свою чергу, являє собою сукупність елементів які складають систему охоронних норм, кримінального, адміністративного, цивільного і інших галузей права, що беруть участь у регулюванні правовідносин у зазначеній сфері.

Необхідність виділення інформаційних злочинів продиктована зростанням значення інформації і інформаційних процесів в умовах реалізації Угоди про асоціацію України до Європейського Союзу. Особливе значення, у зв'язку з цим, знаходить усвідомлення суті інформаційних процесів у кримінально-правовій сфері [3].

Кримінальне законодавство містить великий масив злочинів, які можуть бути визначені як інформаційні. Під інформаційними злочинами пропонується розуміти суспільно небезпечні протиправні діяння, які заподіюють шкоду суспільним відносинам щодо забезпечення інформаційної безпеки особистості, суспільства і держави, способом вчинення яких є інформаційний вплив або (і) предметом яких є інформація як особливий нематеріальний об'єкт. Відповідно, виділяються два види інформаційних злочинів: злочини, предметом яких є інформація, і злочини, способом вчинення яких є інформаційний вплив.

Додатковим родовим об'єктом, загальним для всіх видів інформаційних злочинів, є суспільні відносини з приводу забезпечення інформаційної безпеки особистості, суспільства та держави. Виділення даного об'єкта обумовлено логікою побудови кримінального закону, в якому розділи присвячені охороні суспільних відносин щодо окремої особистості, суспільства, держави. Це означає охорону інформаційної безпеки особистості, суспільства та держави складами інформаційних злочинів, розташованих у відповідних розділах.

Науково-теоретичною основою вивчення першого виду злочинів, (предметом яких є інформація) способом вчинення яких є інформаційний вплив, поряд з роботами з теорії інформації служать дослідження криміналістів, присвячені різним видам інформаційного впливу, таким, як загроза, шантаж, обман.

Другий вид інформаційних злочинів (злочини, способом вчинення яких є інформаційний вплив), має в якості об'єкта інформаційні відносини, які вивчаються в рамках галузі інформаційного права. Інформаційні злочину в цілому, а також їх окремі групи можуть бути класифіковані за різними підставами що необхідно при оцінці обґрунтованості криміналізації (декриміналізації) інформаційних злочинів.

Загальним моментом, що об'єднує всі інформаційні злочини, є використання в конструкції складів таких злочинів термінів, що позначають різні інформаційні явища. Зазначені терміни повинні вживатися, по-перше, коректно з точки зору теорії інформації, по-друге, одноманітно у всьому тексті кримінального закону. Порушення цих вимог означатиме недотримання таких принципів криміналізації, як відсутність прогалин закону і не надмірність заборони, а також визначеність і єдність термінології. Зокрема, це відносяться до інформаційних і комп'ютерних злочинів, як комп'ютерна інформація та комп'ютер. Термін «ЕОМ», використовуваний в Кримінального кодексу України, не відображає повною мірою сутність означуваного явища і потребує заміни [4].

Особливе місце серед інформаційних злочинів займають комп'ютерні злочини які є видом інформаційних злочинів. Особлива значимість комп'ютерних злочинів серед інших видів інформаційних злочинів обумовлена тим, що вони виділені спеціально для захисту комп'ютерної інформації та інформаційних відносин, у той час як інші інформаційні злочину захищають інформаційні відносини лише опосередковано, мають їх в якості додаткового об'єкта.

Виділяється два поняття комп'ютерних злочинів – у вузькому і широкому значенні. Власне «комп'ютерними» є злочини з першої групи, друга група злочинів обґрунтовано відноситься до «злочинів, що здійснюються з використанням комп'ютера». Під комп'ютерними злочинами доцільно розуміти

суспільно небезпечні протиправні діяння, які мають своїм додатковим родовим об'єктом суспільні відносини щодо забезпечення інформаційної безпеки суспільства, що посягають на нормальний режим зберігання, обробки і передачі даних в комп'ютерах (комп'ютерних системах). Будь-який комп'ютерний злочин має в обов'язковому порядку мати ознаки інформаційного злочину, оскільки поняття інформаційного злочину цілком охоплює поняття комп'ютерного злочину, хоча і не обмежується ім. Специфіка цих злочинів полягає в тому, що вони носять транскордонний характер.

Для успішної боротьби з комп'ютерними злочинами необхідна координація діяльності різних державних органів і уніфікація національного законодавства з законодавством Європейського Союзу. Європейська практика йде по шляху приведення національного законодавства у відповідність до Конвенції Ради Європи про кіберзлочинність [5].

1. Проект Концепції державної інформаційної безпеки України. Офіційний сайт Міністерства інформаційної політики України. 08.06.2015. [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf
2. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради. – 1992. – № 48. – Ст. 650.
3. Угода про Асоціацію між Україною. з однієї сторони. та Європейським Союзом. Європейським співтовариством з атомної енергії і їхніми державами-членами. з іншої сторони Угода про асоціацію України до Європейського Союзу. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/984_011
4. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради. – 2001. – № 25-26. – Ст. 131.
5. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради. – 2006. – № 5-6. – Ст. 71.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ОВС: ЗНАЧЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Комісарчук Юлія Анатоліївна,
доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Жук Андрій Петрович,
курсант
Львівського державного університету внутрішніх справ

На даному етапі розвитку України великого значення набуває впровадження нових інформаційних технологій в діяльність органів державної влади і органів внутрішніх справ (далі ОВС), зокрема. Важко уявити роботу правоохоронних органів під час профілактики, виявлення, розслідування злочинів без використання інформаційних технологій. За допомогою технологій виконується велика кількість інформаційно-аналітичної, статистичної роботи; технології використовує кожен працівник у своїй повсякденній діяльності. Нові українські поліцейські для виконання своїх повноважень формують та використовують інформаційні ресурси, застосовують технічні прилади та технічні засоби, які мають функції фото- і кінозйомки, відеозапису.

Попри важливість використання інформаційних технологій у діяльності ОВС не менш важливим є застосування цих же технологій у навчальному процесі. Молодих спеціалістів потрібно навчати загальним особливостям роботи, правилам користування інформаційними технологіями, які використовуються в ОВС. Знайомство з інформаційними технологіями у процесі навчання сприяє ефективності навчання, більш швидкому освоєнні тих чи інших технологій, які в подальшому будуть використовуватися у практичній діяльності.

Під інформаційною технологією розуміють процес, що використовує сукупність засобів і методів збору, накопичення, обробки і передачі даних (первинної інформації) для отримання

оновлених даних про стан об'єкта, процесу або явища (інформаційного продукту). Цей процес складається з чітко регламентованої послідовності виконання операцій, дій, етапів різного ступеня складності з даними, які зберігаються на комп'ютерах. Основною метою інформаційної технології є обробка первинної інформації з допомогою цілеспрямованих дій та отримання необхідної користувацької інформації, а також отримання та обробка даних для їх подальшого аналізу і прийняття рішень про виконання певної дії.

Інформаційні технології (IT, англ. Information technology, IT) – широкий клас дисциплін та галузей діяльності, що відносяться до технології управління, накопичення, обробки і передачі інформації. Також під інформаційними технологіями розуміються сукупність методів, виробничих процесів і програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збір, обробку, зберігання, передачу і відображення інформації.

Самі інформаційні технології вимагають завчасної складної підготовки, великих початкових витрат і наукомісткої техніки. Їх запровадження має починатися зі створення математичного забезпечення, моделювання, формування інформаційних сховищ для проміжних даних і рішень. Галузь інформаційних технологій займається створенням, розвитком та експлуатацією інформаційних систем. Інформаційні технології мають, ґрунтуватись і раціонально використовувати сучасні досягнення в галузі комп'ютерної техніки та інших високих технологій, новітніх засобів комунікації, програмного забезпечення і практичного досвіду. Вирішувати завдання щодо ефективної організації інформаційного процесу для зниження витрат часу, праці, енергії і матеріальних ресурсів у всіх сферах людського життя і сучасного суспільства. Інформаційні технології взаємодіють, і нерідко входять до сфери послуг, галузі управління, промислового виробництва, соціальних процесів [4, с. 43-44].

Ефективність використання інформаційних технологій в ОВС залежить від матеріально-технічного забезпечення, наявності професійної підготовки, знань та навичок у працівників. Важливою також є нормативно-правова регламентація застосування технологій в ОВС.

Технологічне використання комп'ютера в навчальному процесі розв'язує ряд проблем:

- Освітню: знайомлять студентів з можливостями обчислювальної техніки; прищеплюють їм уміння та навички доцільного її використання; формує уміння користуватись навчальними програмами.
- Педагогічну: допомагає студентові швидко і якісно засвоювати навчальний матеріал; унаочнює навчальний процес; індивідуалізує навчання.
- Організаційну: забезпечує можливість одночасного комп'ютерного тестування усіх студентів; проводить комп'ютерний контроль за якістю роботи та її економний облік [3].

До основних методичних цілей, які найбільш ефективно реалізуються за допомогою використання інформаційних технологій можна віднести наступні:

1. Індивідуалізація і диференціація навчання;
2. Формування культури навчальної діяльності, у т.ч. інформаційної;
3. Розвиток інтелектуального потенціалу курсантів та підвищенні їх мотивації;
4. Формування навичок прийняття рішень у складних ситуаціях;
5. Здійснення контролю і самоконтролю за процесом навчання;
6. Комп'ютерне моделювання процесів і явищ, що вивчаються;
7. Якісно більш високий ступінь візуалізації навчального матеріалу за рахунок використання технології мультимедіа;
8. Реалізація доступу до інформаційних ресурсів незалежно від місця їх розташування, який здійснюється на основі технологій телекомунікації [2].

Практика боротьби зі злочинністю свідчить про суттєву роль системи інформаційного забезпечення ОВС як ланки, що зумовлює ефективність роботи правоохоронних структур. Система інформаційного забезпечення здійснює інформаційну підтримку органів внутрішніх справ у розкритті і попередженні злочинів, розшуку злочинців, надає багатоцільову статистичну, аналітичну та довідкову інформацію.

Досвід використання комп'ютерних інформаційних систем і технологій в правоохоронній сфері свідчить, що основними тенденціями їх розвитку та удосконалення є:

1. Удосконалення форм та методів керування системами інформаційного забезпечення;
2. Централізація та інтеграція комп'ютерних банків даних;
3. Впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних обліків;
4. Розбудова та широке використання ефективних та потужних комп'ютерних мереж;
5. Застосування спеціалізованих засобів захисту та безпеки інформації;
6. Налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні.

---

1. Закон України «Про національну поліцію» [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/580-19
2. Горелов Ю.П. Використання інформаційних технологій в системі підготовки кадрів МВС / Харківський національний університет внутрішніх справ [Електронний ресурс]. Режим доступу: http://essuir.sumdu.edu.ua/bitstream/123456789/28735/1/information.pdf
3. Торубара О.М. Застосування новітніх інформаційних технологій в навчальному процесі вищих навчальних закладів / О.М. Торубара // Вісник Чернігівського національного педагогічного університету. Педагогічні науки. – 2013. – Вип. 108.2. – Режим доступу: http://nbuv.gov.ua/j-pdf/VchdpuP_2013_2_108_20.pdf
4. Андрощук О.В., Кондратенко Ю.В., Головченко О.В., Ворона Т.О., Петрушен М.В. Інформаційні технології та їх вплив на розвиток суспільства / Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.– 2014. – № 1(50). – 157 с.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОВС УКРАЇНИ: СУТНІСТЬ, ЗАВДАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Король Тетяна Олександрівна,
курсант
Львівського державного університету внутрішніх справ
Комісарчук Юлія Анатоліївна,
доцент кафедри кримінального процесу
Львівського державного університету внутрішніх справ
кандидат юридичних наук, доцент

Відповідно до ст. 3 Закону України «Про інформацію», одним з основних напрямів державної інформаційної політики в Україні, сьогодні, є створення інформаційних систем і мереж інформації; розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України. Тому останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, у тому числі в діяльність органів внутрішніх справ (ОВС) України.

Таким чином, на сучасному етапі розвитку України спостерігається необхідність вивчення сутності інформаційного забезпечення органів внутрішніх справ, тому що воно є одним із гарантів та способом забезпечення ефективності боротьби зі злочинністю, захисту прав і свобод українського суспільства в цілому й окремих його членів. Адже не слід забувати давню мудрість: «Попереджений – значить озброєний».

Чим складніші та масштабніші завдання постають перед ОВС, тим відповідно, є вищими критерії оцінювання інформації, яка має безпосереднє відношення до діяльності ОВС: її аналізу та захисту. Захист інформації розглядається як діяльність, спрямована на запобігання витоку інформації з обмеженим доступом (інформації, що складає таємницю), а також на запобігання різноманітного роду несанкціонованих і небажаних умисних

впливів на інформацію та її носії, тобто діяльність, спрямована на захист інформації [1, с. 130].

Інформаційне забезпечення управління ОВС України є одним із провідних питань, що вирішуються на сучасному етапі розвитку правоохоронних органів України.

Постійна циркуляція різноманітної інформації між складовими частинами системи ОВС, між системою ОВС у цілому і її навколишнім середовищем є обов'язковим атрибутом управління органами внутрішніх справ. Тільки завдяки інформаційним процесам може ефективно впливати на зовнішнє її оточення, направляти свою діяльність на успішне вирішення завдань, що стоять перед нею, здійснювати координацію між її складовими частинами.

Інформаційне забезпечення ОВС являє собою органічну єдність роботи щодо визначення змісту, обсягів, якості інформації, необхідної для здійснення управління, а також заходів щодо раціональної організації процесів збирання, систематизації, накопичення та обробки цієї інформації шляхом застосування різноманітних методів, методик і технічних засобів[2, с. 301].

Основними завданнями функціонування системи інформаційного забезпечення ОВС вважаються: забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами ОВС для розкриття, розслідування, попередження злочинів і розшуку злочинців; збір, обробка та узагальнення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної, і контрольної інформації для оцінки ситуації та прийняття обгрунтованих оптимальних рішень на всіх рівнях діяльності ОВС; забезпечення динамічної та ефективної інформаційної взаємодії усіх галузевих служб ОВС України, інших правоохоронних органів та державних установ; забезпечення захисту інформації. Органи внутрішніх справ користуються й іншим інформаційним забезпеченням. За доступністю його можна поділити на відкрите і закрите забезпечення. Відкрите – це забезпечення зовнішнього загального користування, наприклад, обласні адресно-довідкові картотеки (адресні бюро), а закрите – обмеженого користування, наприклад, оперативно-довідкова картотека джерел інформації, призначене тільки для певної категорії працівників, допущених до оперативно-розшукової діяльності. Окремі служби МВС створюють свої специфічні

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

Інформація, необхідна для здійснення управління ОВС, накопичується, обробляється і зберігається в єдиному інформаційному масиві (банку даних). Система інформаційного забезпечення ОВС являє собою сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання та забезпечення загальновизначених та обов'язкових вимог: нормативно-правової бази, організаційно-кадрового забезпечення інформаційних підрозділів, навчання та перепідготовки кадрів; комп'ютерних, програмних, телекомунікаційних засобів та технологій; матеріально-технічного та фінансового забезпечення. Основною метою системи інформаційного забезпечення ОВС України є всебічна інформаційна підтримка діяльності ОВС у боротьбі зі злочинністю на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів. Формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення ОВС, здійснюється згідно з такими принципами: функціонального призначення. нормативно-правової забезпеченості; фактичності даних; доцільності впровадження та експлуатації; нарощення та розвитку [4, с. 173].

Збір інформації для автоматизованого банку даних про об'єкти кримінальної реєстрації здійснюється за допомогою єдиних карток збору інформації усіх рівнів. Важливе місце в системі інформаційного забезпечення управління ОВС займають канали зв'язку і передачі інформації. В даний час в системі ОВС створено телекомунікаційні системи для здійснення зв’язку і передачі інформації з банку даних. Так, для безпосереднього звернення в «АБД Центр» з УМВС областей та міськрайвідділів використовуються підсистема «Телеграф» і підсистема обробки запитів по телефонних каналах зв'язку. Система «Телеграф»

дозволяє проводити обробку запитів в «АБД Центр» за такими напрямками: а) підсистема «Особа»; б) підсистема «Номерні речі»; в) підсистема «Автомобіль». В одному запиті можна перевіряти до 30 осіб, речей, зброї та автотранспортних засобів. Правила набору запитів містяться у відповідних інструкціях, які є у всіх інформаційних управліннях УМВС областей України. Абонентом системи «Телеграф» може стати будь-який орган внутрішніх справ, обладнаний звичайним телеграфним апаратом, персональним комп'ютером із спеціальним адаптером [3, с. 170]. Для здійснення зв'язку і передачі інформації в системі ОВС використовується електронна пошта, телеграф, письмовий зв'язок, особисте звернення працівника ОВС [5, с. 3].

Постійне загострення криміногенного стану в Україні висуває вимоги докорінного поліпшення інформаційного забезпечення діяльності ОВС у боротьбі із злочинністю, створення принципово нової системи, яка має поєднувати всі накопичені та наново створювані масиви оперативно-розшукового призначення в єдину інформаційно-обчислювальну мережу ОВС України.

Отже, процес запровадження в ОВС інформаційних технологій тільки набирає сили і не є досконалим, однак ті позитивні зміни, що відбуваються останнім часом, та визначені перспективні напрямки допоможуть здолати всі перешкоди в інформаційному забезпеченні діяльності органів внутрішніх справ і підвищити ефективність протидії злочинності.

1. Ковалів М.В. Інформаційно-аналітична робота в ОВС // Проблеми інформаційного забезпечення діяльності практичних підрозділів ОВС та впровадження інформаційних технологій в навчальний процес. – Львів, 2004. – С. 126-134.
2. Державне управління: Навч. посіб./Мельник А.Ф., Оболенський О.Ю., Васіна А.Ю., Гордієнко Л.Ю.; За ред. А.Ф. Мельник. – К.: Знання-Прес, 2003. – 343 с.
3. Бандурка О.М. Управління в органах внутрішніх справ України: Підручник. – Харків, 1998. – 780 с.
4. Фролова О.Г. Про сучасне інформаційно-методичне забезпечення управління в ОВС // Держава і право. – К., 2013. – Вип. 13. – С. 171-176.
5. Інформаційні підсистеми ОВС України.– [Електронний ресурс] – режим доступу: http://www. naiau.kiev.ua/biblio/books/Kriminal inform/tema 3/htm.

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ ПІД ЧАС ЗДІЙСНЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Магеровська Тетяна Валеріївна,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук, доцент
Андрухів Євгенія Михайлівна,
студентка юридичного факультету
Львівського державного університету внутрішніх справ

Актуальність обраної теми пов'язана із великою кількістю запитань щодо здійснення органами внутрішніх справ досудового слідства шляхом застосування інформаційних технологій.

Дослідженням даного питання займалося чимало науковців, серед яких: Д.О.Максимус, О.О. Юхно, В.М. Шевчук, І.В. Рогатюк та інші.

Стрімкий розвиток інформаційних технологій розповсюдив свій вплив не лише на окремі сфери життя суспільства, але й на існування людства в цілому. Такий вплив став поштовхом до розвитку всіх можливих видів діяльності з їх подальшим удосконаленням. Кожна країна почала застосовувати дані технології у своїй діяльності, а також впроваджувати їх використання серед відповідних служб, для покращення роботи цих установ, а тим самим і для процвітання країни загалом. Україна теж скористалася даною можливістю розвитку суспільства в усіх можливих сферах своєї діяльності. Застосування інформаційних технологій у роботі органів внутрішніх справ (в нашому випадку під час здійснення досудового слідства) стало лише одним із можливих чинників покращення життя українського народу.

Для початку варто звернути увагу на визначення декількох ключових понять щодо даного питання, а саме: «досудове

розслідування», «досудове слідство» та «інформаційна технологія».

Досудове розслідування – це діяльність спеціально уповноважених органів держави, яка полягає у виявленні злочинів, злочинців, збиранням доказів, обробці доказів, повного дослідження всіх обставин справи. Формами досудового розслідування є : дізнання і досудове слідство. Звернімо увагу на таку форму досудового розслідування як досудове слідство.

Пильгун Н.В., Бородін Є.В. Присяжнюк І.О. у своїй праці «Досудове слідство як основна форма розслідування: питання реформування на сучасному етапі» використали наступне твердження щодо поняття «досудове слідство»: «Досудове слідство є основною формою попереднього розслідування, яка являє собою врегульовану нормами кримінально-процесуального закону діяльність слідчого, пов'язану із збиранням, перевіркою та оцінкою доказів з метою всебічного, повного і об'єктивного встановлення події злочину, винності конкретних осіб у скоєнні злочину та інших обставин, які мають значення для правильного вирішення кримінальної справи.» З даного визначення можна зробити висновок, що досудове слідство базується на збиранні, перевірці доказів, що є достатньо клопіткою роботою, тим не менше, саме сучасні інформаційні технології слугують не лише для покращення діяльності органів внутрішніх справ, але й для суттєвого полегшення їхньої роботи.Тому для кращого розуміння що таке інформаційні технології потрібно звернутися до роботи Андрощука О.В., Кондратенка Ю.В., Головченка О.В., Ворони Т.О. та Петрушена М.В. «Інформаційні технології та їх вплив на розвиток суспільства» де чітко дано визначення поняттю «інформаційна технологія» відповідно до якого інформаційна технологія– це процес, що використовує сукупність засобів і методів збору, накопичення, обробки і передачі даних(первинної інформації) для отримання оновлених даних про стан об'єкта, процесу або явища(інформаційного продукту).

Для проведення слідчої діяльності використовуються різного роду автоматизовані бази даних, що дозволяють пришвидшити пошук потрібної інформації, автоматизовані робочі місця, програмно-технічні комплекси та інші засоби, що в свою чергу і є сучасними інформаційними технологіями.

Під час досудового розслідування за наявності використання інформаційних технологій здійснення роботи органами внутрішніх справ набуває характеру оперативності, що виявляється у швидкому збиранні, аналізі та зіставленні відомостей з різних джерел. Бази даних, які використовуються органами досудового розслідування призначені для представлення інформації, яка вноситься у ці бази даних в хронологічному порядку, за часом надходження або в іншому потрібному в даній ситуації порядку.

Інформаційні технології на досудовому розслідуванні використовуються у таких напрямках: для створення та ведення криміналістичних обліків, користування законодавчою базою даних України, крім того для побудови суб'єктивних портретів злочинців, пошуку відомостей щодо будь-яких потрібних об'єктів по справі.

Згідно із ч.2 ст. 214 КПК України: «Досудове розслідування розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань» ЄРДР виступає інформаційною технологією, яку використовують для введення наступних даних: відомостей про кримінальні правопорушення, рішень за кримінальним провадженням, осіб, які вчинили кримінальне правопорушення. Такого роду реєстрація дозволяє вести зручний облік справ, а також при необхідності і зручний їх пошук. Важливим є той факт, що законодавець визначає обов'язковою умовою внесення відомостей у ЄРДР, так відповідно до ч.3 ст.214 КПК України: «Здійснення досудового розслідування до внесення відомостей до реєстру або без такого внесення не допускається і тягне за собою відповідальність, встановлену законом»

Доречним є також звернути увагу на досвід у сфері застосування інформаційних технологій на досудовому розслідуванні в інших державах. Так, у Грузії, спільним для нашої країни є момент початку досудового розслідування, а саме момент внесення відомостей до єдиного електронного реєстру кримінальних справ. Рогатюк І.В. зазначає, що картка обліку кримінального правопорушення, в яку вноситься наступне: відомості про особу слідчого, який розпочав розслідування, джерело з якого стало відому про факт вчинення правопорушення, відомості про потерпілого та заявника, виклад обставин кримінального правопорушення, попередня правова кваліфікація кримінального

правопорушення є першим документом у даному реєстрі. Слідчий, який веде справу, начальник слідчого відділу а також прокурор можуть як за допомогою стаціонарного комп'ютера, так і за допомогою портативного пристрою шляхом введення спеціального коду та електронного ключа отримати доступ до справи. Такий доступ є швидким, ефективним, а крім того унеможливлює сторонніх осіб ознайомитися з матеріалами справ, що внесені до даного реєстру. Така позиція щодо єдиного електронного реєстру справ Грузії зацікавила і Україну, тому чимало вітчизняних фахівців неодноразово звертали увагу саме на цю державу як на приклад для наслідування, оскільки Грузія теж як і Україна нещодавно проведено реформу у сфері кримінальної юстиції, та прийняла новий КПК для своєї держави.

Застосування інформаційних технологій на досудовому розслідуванні полегшує не лише ведення документації по справах, що знаходяться в правоохоронних органах, але дозволяє ефективно вчиняти певні слідчі дії щодо даних справ. Доречним є звернути увагу на використання правоохоронними органами окремих інформаційних технологій, призначенням яких є встановлення місця знаходження осіб. Відповідно до ч.1 ст. 281 КПК України: «Якщо під час досудового розслідування місцезнаходження підозрюваного невідоме, то слідчий, прокурор оголошує його розшук». Здійснення розшуку передбачає застосування різноманітних способів, методів та засобів для визначення місцязнаходження особи. Традиційні засоби розшуку (такі як, наприклад, опитування родичів, друзів, сусідів розшукуваної особи) все ще використовуються правоохоронними органами, але використання лише їх зменшує оперативність здійснення даної дії. Лисенко О.В. у своїй статті «Використання інформаційних технологій для розшуку осіб, які переховуються від органів досудового розслідування та суду» зазначив наступне: «До сучасних засобів розшуку особи можна віднести алгоритми пошуку загальнодоступної інформації (інформаційних слідів), що залишають персональні комп'ютери, мобільні телефони, комп'ютерні планшети, облікові записи (акаунти) в «Facebook», «Вконтакті», «Skype», «Twitter», «Однокласники» різноманітних блогах та інших інформаційних сервісах.» Використання в наш час комп'ютерних технологій, а разом з цим і комп'ютерної

мережі «Інтернет» робить наше життя більш зручнішим. Соціальні мережі набули свого широкого розповсюдження з 2004 року. Користувачі соцмереж постійно залишають інформацію про своє життя на своїх ж сторінках цих мереж, наприклад, викладаючи відео, фотографії, іншу інформацію про себе. Правоохоронні органи відслідковують таку інформацію щодо розшукуваної особи, що допомагає їм створити певний портрет даної особи та побудувати версії щодо її розшуку, враховуючи вподобання цієї людини, місця проведення нею останньої своєї фото сесії перед зникненням, її переписку з іншими особами, та іншу інформацію, яку розшукуваний залишив в соцмережах. Інформацію отриману вищезазначеним шляхом називають «інформаційними слідами»

Цікавим є той факт, що останнім часом все частіше працівники правоохоронних органів використовують «інформаційні сліди» з метою встановлення протиправної діяльності, пошуку інформації, завданням якої є закликати людей до вчинення у майбутньому певних злочинів, протидії злочинам терористичної спрямованості. Щодо останнього твердження варто звернутися до вище згадуваної праці Лисенка О.В., в якій він зазначає: «Матеріали Служби Безпеки України щодо протидії діяльності терористичних організацій у Донецькій та Луганській областях, де використовувалося інформаційно-аналітичне забезпечення під час проведення Антитерористичної операції дозволило встановлювати місцезнаходження баз терористів, маршрути їх пересування, місця переховування, зміст спілкування між собою».

Збирання інформації про розшукувану особу правоохоронними органами таким шляхом не завжди приводить до бажаного результату. Ускладнюють можливість фіксації працівниками ОВС інформації наступні обставини: адміністратор Інтернет-ресурсу може в будь-який момент змінити зміст інформації, внести неправдиві відомості про себе заплутуючи сліди або видалити таку інформацію з серверу. В такому разі правоохоронним органам варто ретельно перевіряти зібрану інформацію зіставляючи її уже із відомими обставинами по справі.

Розвинені зарубіжні країни використовують інформаційні технології при розшуку з великою інтенсивністю, аргументуючи таке використання збільшенням ймовірності знайдення особи в

найкоротший термін. Лисенко О.В. висвітлив у своїй статті позицію США щодо використання інформаційних технологій в діяльності правоохоронних органів, а саме: «Згідно з опитуванням у США 4 із 5 представників правоохоронних органів використовують можливості соціальних мереж для розшуку осіб, у тому числі тих, які переховуються від слідства та суду. Також згідно з цим опитуванням, роль соціальних мереж для розслідування злочинів та розшуку осіб, на думку опитаних осіб, буде в майбутньому лише зростати, оскільки спостерігається збільшення користувачів таких мереж». Громадяни України теж користуються соціальними мережами, що слугує однією із причин швидшого розкриття злочинності в країні.

В будь-якому випадку, для того аби зібрати інформацію щодо особи яка цікавить правоохоронні органи потрібно мати хоча б мінімальну інформацію про цю особу. Якщо ж правоохоронним органам відома певна інформація щодо розшукуваної особи, наприклад, прізвище, ім'я та по-батькові цієї особи, адреса електронної пошти такої особи, ім'я в сервісі Skype, то така інформація дозволить знайти ще інформацію на дану особу, використовуючи соціальні мережі. Найпростішим способом знаходження такої інформації є введення відомих даних у пошукову систему «Google».

Із збільшенням використання комп'ютерних технологій у роботі органами внутрішніх справ України, комп'ютерна грамотність працівників теж підвищилася, що забезпечує можливість і використання інформаційних технологій. Більше того важливим критерієм при прийнятті на роботу працівників в правоохоронні органи є наявність в них уміння працювати з комп'ютерами. Студенти університетів внутрішніх справ України вивчають роботу з інформаційними технологіями щоб в подальшому в них при роботі не виникало жодних непередбачуваних труднощів. Хахановський В.Г у своїй праці «Наукове забезпечення інформатизації правоохоронної діяльності та підготовка кадрів в інформаційній сфері» зазначив: «25 червня 2013 року виповнюється 25 років з дня заснування першої в системі МВС України кафедри, яка здійснює підготовку кадрів в інформаційній сфері та забезпечує наукову підтримку інформатизації протидії злочинності. Сьогодні кафедра інформаційних

технологій є навчально-науковим структурним підрозділом Національної академії внутрішніх справ та забезпечує проведення навчальної, навчально-методичної, наукової та виховної роботи з метою набуття слухачами, курсантами та студентами спеціальних професійних знань та навичок.» Тобто знання інформаційних технологій є невід'ємною частиною роботи працівників правоохоронних органів.Попри все вищезазначене саме рівень уміння працювати працівників з комп'ютерами залишається однією із основних проблем для впровадження нових інформаційних технологій, адже більшість слідчих України не володіє інноваційними методами отримання інформації. Підготовка з функціонування інформаційних систем, локальних та глобальних мереж зв'язку, організація обробки інформаційних потоків потребує вдосконалення, оскільки без такого вдосконалення досудове розслідування втрачає свою ефективність.

Отже, наявність інформаційних технологій у діяльності органів внутрішніх справ дозволяє збільшити оперативність роботи даних органів, сприяє полегшенню ведення документації, крім того електронне збереження інформації – це один із кращих способів в подальшому і її ефективного використання.

1. Пильгун Н.В., Бородін Є.В., Присяжнюк І.О. Досудове слідство як основна форма розслідування: питання реформування на сучасному етапі // Юридичний вісник. – 2012. – №3. – С.135-139.
2. Організація судових та правоохоронних органів: підручник для студентів юрид. спеціальностей вищих навч. закладів / І. Є. Марочкін, Н. В. Сібільова, В. П. Тихий та ін. За ред. І. Є. Марочкіна, Н. В. Сібільової. — Х.: ТОВ «Одіссей», 2007. — 528 с.
3. Рогатюк І.В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспектива розвитку // Науковий вісник національної академії внутрішніх справ. – 2013. – №3. – С. 312-320.
4. Андрощук О.В., Кондратенко Ю.В., Головченко О.В., Ворона Т.О., Петрушевич М.В. Інформаційні технології та їх вплив на розвиток суспільства // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім.ІванаЧерияховського. – 2014. – №1. – С.42-47.
5. Шевчук В.М. Запровадження сучасних інформаційних технологій для оптимізації слідчої діяльності // Науковий вісник Херсонського державного університету. – 2013. – Випуск 6 Том 2. – С. 149-153.

6. Хахановський В.Г. Наукове забезпечення інформатизації правоохоронної діяльності та підготовка кадрів в інформаційній сфері // Правова інформатика. – 2012. – № 4. – С. 91-93.
7. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (редакція від 16.08.2015) – [Електронний ресурс]. – Режим доступу:http://zakon4.rada.gov.ua/laws/show/4651-17/page7/
8. Лисенко О.В. Використання інформаційних технологій для розшуку осіб, які переховуються від органів досудового розслідування та суду // Науковий вісник національного університету ДПС України (економіка, право). – 2014. – №2. – С.194-201.
9. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій: навч. посіб./ Д.О. Максимус, О.О. Юнхо. – Харків: НікаНова, 2013. – 102с.

ВИКОРИСТАННЯ МЕТОДІВ ЕКСПЕРТНИХ СИСТЕМ ДЛЯ АВТОМАТИЗАЦІЇ РОЗСЕЛЕННЯ ОСІБ У МІСЦЯ ТИМЧАСОВОГО ПРОЖИВАННЯ

Магеровський Дмитро Вікторович,
студент ІКНІ
Національного університету «Львівська політехніка»

У сучасному світі при стрімкому розвитку технологій люди прагнуть автоматизувати практично всі аспекти їх життя. Системи «Розумний дім», автомобілі що не вимагають водія – ці речі вже є реальністю в західних країнах. Тобто такі системи є індивідуальні й працюють на побутовому рівні, не кажучи вже про фірми чи корпорації, для яких автоматизація рутинних дій, що потребують часу більше ніж на те розраховано є звичною вже з десяток років. Проте, у країнах колишнього Радянського Союзу в більшості великих структур, не кажучи вже про індивідуальне, й досі вся робота, що потребує певного простого переліку дій виконується людьми. Перевагою такого підходу є те, що по статистиці відсоток безробіття у країні є меншим. З іншого боку кінцевим продуктом діяльності людини на такій посаді є доволі велика кількість використаного паперу, поява бюрократії, хамства та інших особливостей, притаманних виключно людині через особливості її характеру, фізичний/психічний стан, тощо. Також людина може підробляти вихідні дані у своїх інтересах, або інтересах окремої групи людей. Обабіч цих проблем стоїть проблема повільної обробки даних. В залежності від складності вхідних даних на їх обробку може знадобитися від 10 секунд до кількох хвилин.

Проте окрім власне виробництва, є і інші сфери де застосування автоматизованих експертних систем (тобто систем прийняття рішень) було би доцільне. Однією з таких сфер є поселення людей у гуртожитки та інші місця тимчасового проживання, коли часто місце проживання надається не найбільш потребуючим її людям, через складність використання паперових репозиторіїв

даних важко вести облік порушень, оплати та інших сфер й особливостей конкретного поселення. Створення експертної системи для розселення респондентів у місця тимчасового проживання може зробити прозорим процес власне поселення а також надати можливість адміністрації вчасно та ефективно приймати рішення при фактах порушення умов проживання.

Експертна система. Експертною системою (ЕС) називають систему підтримки прийняття рішень, яка містить знання з певної вузької предметної області, а також може пропонувати користувачу рішення проблем з цієї галузі і обґрунтовувати їх. Вона складається з бази знань, механізму логічного виводу і підсистеми обґрунтувань.

Експертна система акумулює професійні знання керівників і фахівців, використовуючи їх для формування бази знань, яка містить набір взаємопов'язаних правил. При прийнятті рішень стає можливим аналіз наслідків різних рішень у вигляді питань «що буде, якщо...», не витрачаючи часу на трудомісткий процес програмування.

Особливістю сучасних діючих експериментальних експертних систем є їх дуже вузька спеціалізація. Вузька спеціалізація експериментальних експертних систем викликана бажанням зменшити об'єм професійних знань, що закладаються в систему, для спрощення задачі створення цих знань та їх збереження у пам'яті ІС.

Професійні знання передаються експертній системі відповідним спеціалістом, а їх зведення до вигляду, зручного для використання у комп'ютері виконує програміст. Найпоширенішою і природною формою представлення знань у системі є їх запис у вигляді професійних правил або тверджень типу «якщо..., то...». Ліва частина такого правила представляє поєднання фактів або ознак, які характеризують деяку умову, а права частина вказує на дію або висновок, що відповідає наявній ситуації. [1]

При створенні бази знань експертної системи часто використовують нечітку логіку.

Нечітка логіка (від англ. fuzzy logic) як наука була започаткована американським вченим іранського походження Лотфі А. Заде (Lotfi A. Zadeh). На відміну від булевої алгебри, у

котрій існує лише дві величини (0 та 1, правда чи неправда) у нечіткій логіці існують також перехідні величини (стани) [2].

Технології. Зазвичай експертні системи розробляють з допомогою мов C, Perl, Ajax або таких, що найшвидше обробляють інформацію. Проте у випадку систем, що не потребують найбільшої обчислювальної швидкості, допустиме використання засобів розробки з більш зручним функціоналом та уніфікацією.

Для експертної системи поселення у місця тимчасового проживання найдоречнішими технологіями для розробки будуть Microsoft.NET та Java. Обидві технології мають достатню функціональність та широту застосування, що забезпечуватиме простішу й дешевшу підтримку системи, а також спростить додавання нового функціоналу за потреби. Також такі програми можуть виконуватися як на десктопі, так і на веб-сервері, при цьому не потрібно буде великих затрат для оптимізації під ці системи. Внутрішній код завжди виконуватиметься однаково.

На мою думку, оптимальним є використання .Net у зв'язці з MS SQL Server, використовуючи при цьому Entity Framework та мову вбудованих запитів LINQ.

Така зв'язка буде більш функціональною, розробка буде простішою завдяки підтримці середовища розробки Visual Studio як інструментарію для написання алгоритмів майбутньої системи, так і для побудови баз даних і знань. Entity Framework дозволить представити базу даних у вигляді об'єкту класу, що спросить роботу з нею, а LINQ надає можливість написання більш зрозумілих та прозорих запитів, а також спростить їх опрацювання в коді.

Математична модель. Для прикладу буде взято студмістечко Національного університету «Львівська політехніка». Всі числа у моделі надані для наглядності й можуть варіюватися.

Необхідними у ЕС поселення є такі параметри:

- пільги людини, що заселяється. Пільговики мають першочергове право на поселення. Виключення: пільговик прописаний у місті, де розташовані гуртожитки;
- країна проживання. Іноземці заселяються першочергово. Фактично, вважаються пільговиками;

- відстань до населеного пункту, де розташовано гуртожиток. Чим людина далі – тим більше шанс на поселення.

На основі цього можна зробити нечіткі змінні. Нехай візьмемо $M = \{0,1000\}$, де 0 – поселення неможливо, 1000 – поселення 100%. Оскільки пільговики мають також свою чергу, визначимо на пільги 400 балів. І за градацією серйозності пільги начислятимемо бали. На відстань до Львова буде надано 400 балів. Буде 4 градації – близько, середньо, далеко, дуже далеко. За кожну з них начислятиметься певна сума балів. Також враховуватиметься рейтинг абітурієнта або студента, якщо він є резидентом України – 200 балів. При поселенні іноземця йому автоматично буде присвоєно максимальне значення.

Далі сума балів підраховується та ділиться на 1000. Отримується градація, що, в свою чергу, буде поділятися на 4 черги поселень. Так, люди, які, наприклад, набрали коефіцієнт поселення > 0.5 потрапляють в 1 чергу. Далі відбувається вибірка людей на поселення. Така модель дозволить поселити у кращі умови тих, хто їх потребує (при введені градації «крутості» гуртожитка) та, наприклад, поселити у прості кімнати (які оцінені нижче) людей, які мають змогу щодня добиратися додому.

Таким чином, математична модель задачі без урахування якості гуртожитка виглядатиме так:

$$P(пос) = \frac{S_{пільги} + S_{відстань} + S_{рейтинг}}{1000}$$, де P – коефіцієнт, S – кількість отриманих балів.

Приклад реалізації. В якості прикладу буде утворено таблицю бази даних в якій міститимуться головні показники для обчислення коефіцієнту поселення – що напряму впливатиме на відповідність черзі на поселення. Такими сутностями є: відстань від міста де розташоване тимчасове поселення, наявність пільг, при чому самі пільги занесені до бази знань, у процесі підрахунку коефіцієнту беруть участь їх числові коди. Також можна підрахувати рейтинг. На рис. 1 зображено схему БД згенеровану Entity Framework.

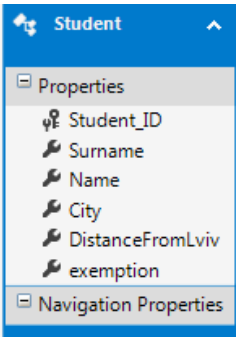


Рис 1. Схема таблиці в представлені Entity Framefork

Базою знань пільг у прикладі виступатиме перелік константних значень – ENUM.

```
enum Exemptions
{
None = 0,
Mountain = 1,
Orpham = 2,
HealthProblems = 3,
Foreigner = 4
};
```

Для наглядного прикладу роботи системи до таблиці буде введено декілька нових значень – студентів з різним місцем проживання та різними пільгами або їх відсутністю (рис. 2).

ДМИТРИЙ-ПК\LOCA...b4 - dbo.Student ДМИТРИЙ-ПК\LOCA...b4 - dbo.Student

Student_ID	Surname	Name	City	DistanceFrom...	exemption
0	Lang	Alex	Lviv	0	3
1	Pow	Dmytro	Slavske	120	1
2	Div	Olexandr	Lviv	0	0
3	Yumba	Tumba	Bangladesh	2300	4
4	Revazov	Jora	Poltava	700	0
NULL	NULL	NULL	NULL	NULL	NULL

Рис. 2. Заповнення БД даними

Після цього за правилом «якщо… то» буде обчисленно коефіцієнт черги поселення респондента (рис. 3).

```
double sum = 0;
 using (var db = new ESLab4Entities1())
 {
 var query = from s in db.Students
 orderby s.Surname
 select s;
 foreach(var stud in query)
 {
```

```
        switch (stud.exemption)
        {
        case 0:
        sum += 0;
        break;
        case 1:
        sum += 150;
        break;
        case 2:
        sum += 600;
        break;
        case 3:
        sum += 350;
        break;
        case 4:
        sum += 600;
        break;
        }
        if(stud.DistanceFromLviv == 0)
        {
        sum += 0;
        }
        else if (stud.DistanceFromLviv > 400)
        {
        sum += 400;
        }
        else
        {
        sum += (int)stud.DistanceFromLviv;
        }
        sum /= 1000;
        Console.WriteLine(«A chanse of {0} {1} to get a settle is {2}»,
stud.Name, stud.Surname, sum.ToString(«0.00»));
        sum = 0;
        }
        }
        }
```

Для прикладу подано такі правила:

1. **Якщо** відстань до місця тимчасового проживання є меншою ніж 400 кілометрів – **то** респонденту начисляється кількість балів що дорівнює даній відстані.
2. **Якщо** відстань до місця тимчасового проживання є меншою ніж 400 кілометрів – **то** респонденту начисляють 400 балів.
3. **Якщо** у респондента наявна пільга *a* – **то** йому начисляють *n* балів.

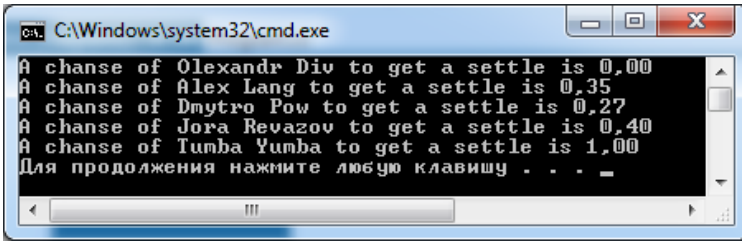


Рис. 3. Розрахунок коефіцієнту черги поселення

Висновок. Алгоритм поселення людей в гуртожиток є доволі простим. Реалізація цього алгоритму для експертної системи поселення у місця тимчасового проживання з допомогою сучасних засобів програмування відповідно також є доволі простою. При цьому адміністрація місця тимчасового проживання отримує перевагу в якості й прозорості обробки даних, а також швидкості представлення готового рішення. Також, це зменшує витрати адміністрації у зв'язку із можливим скороченням людського ресурсу, що відповідав за поселення до автоматизації або розподілом цього ресурсу на інші задачі, що в свою чергу збільшить ефективність роботи. Потенційні поселенці отримують перевагу у прозорості машинного обрахунку, таким чином найбільш потребуючі прошарки матимуть більші шанси на поселення. Тобто скоротиться кількість неправомірних підмін результатів, часу очікування та паперової тяганини, пов'язаної з бюрократичними процедурами.

Таким чином, автоматизація процесів у місцях тимчасових поселень вигідна усім сторонам й бажана для реалізації у поселеннях, в яких людських ресурсів недостатньо для ефективного процесу керування поселенням.

1. http://pidruchniki.com/10811007/informatika/ekspertni_sistemi
2. http://www.znannya.org/?view=fuzzy-logic
3. http://www.victoria.lviv.ua/html/oio/html/theme11.htm

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПОЛІЦІЇ У СФЕРІ ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ НАРКОТИЧНИХ ЗАСОБІВ

Мельник Ольга Миколаївна,
старший науковий співробітник наукової лабораторії
Львівського державного університету внутрішніх справ,
кандидат юридичних наук

Інформаційне забезпечення сил охорони правопорядку є актуальним питанням не тільки для України, але й для багатьох зарубіжних країн, в яких значна увага приділяється створенню і використанню інформаційних систем спеціальної поліцейської діяльності.

Категорія «інформаційне забезпечення» отримала достатній розвиток у межах інформаційного права. Питання інформаційного забезпечення також розглядалося в окремих працях з кримінального процесу, оперативно-розшукової діяльності під час висвітлення пропозицій, спрямованих на підвищення ефективності боротьби зі злочинністю.

Згідно Закону України «Про Національну поліцію» поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень.

Поліція в рамках інформаційно-аналітичної діяльності:

1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями [1].

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності щодо протидії наркозлочинам передбачає вдосконалення системи статистичного обліку і звітності в країні,

інформування про стан, динаміку, структуру наркозлочинів, критеріїв оцінки ефективності діяльності правоохоронних органів, збору необхідної і достатньої інформації для ефективної діяльності суб'єктів профілактики і прийняття відповідних управлінських рішень щодо запобігання цим злочинам [2, с. 390].

Поліція в межах своєї компетенції 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.

Зараз в умовах, коли у світі відбуваються інтенсивні інтеграційні процеси, усі країни зацікавлені в тому, щоб статистичні показники про злочинність, можна було б порівнювати та всебічно її розглядати [3, с. 64].

Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку безвісно зниклих;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв’язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності.

На даний час поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав

доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних.

Загальні принципи побудови системи кримінальної статистики про наркозлочини, та можливість і виправданість застосування тих чи інших технічних засобів та прийомів має спиратись на міжнародні стандарти.

Протидія злочинам у сфері незаконного обігу наркотичних засобів та психотропних речовин засобами оперативно-розшукової діяльності сьогодні потребує застосування знань у сфері інформатики та телекомунікацій. Подальше вдосконалення процесу доказування пов'язано з дослідженням складних залежностей між виникненням інформації про кримінальні правопорушення та події, оперативно-розшуковою тактикою її отримання та процесуальною природою закріплення судових доказів [4, с. 76].

---

1. Про Національну поліцію: закон України від 2015 р. // Відомості Верховної Ради. – 2015 р. – № 40-41. – С. 379.

2. Оперативно-розшукова діяльність органів внутрішніх справ: Загальна частина: підручник; [авт. кол.: Е.О. Дидоренко, І.П. Козаченко, Я.Ю. Кондратьев та ін.] / за заг. ред. Л.В. Бородина. – Луганськ. РВВ ЛІВС, 1999. – Т. 1. – 390 с.
3. Хитра О.Л. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності щодо протидії наркозлочинам, вчинюваних неповнолітніми // О.Л. Хитра / Вісник Львівського державного університету внутрішніх справ (серія юридична) – №1. – 2009 – с.60-68;
4. Михайлецький О.О. Окремі аспекти інформаційно-аналітичного забезпечення підрозділами МВС України у боротьбі з незаконним обігом наркотичних засобів та психотропних речовин // О.О. Михайлецький / Вісник Львівського державного університету внутрішніх справ 9серія юридична) – №1. – 2009. – с. 68-78

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СФЕРІ ФІКСАЦІЙ АДМІНІСТРАТИВНИХ ПОРУШЕНЬ ПРАВИЛ ДОРОЖНЬОГО РУХУ

Мних Сергій Романович,
студент юридичного факультету
Львівського державного університету внутрішніх справ
Неспляк Дмитро Михайлович,
викладач кафедри інформатики
Львівського державного університету внутрішніх справ

Аналізуючи практику європейських країн, з метою ефективного контролю за виконанням водіями транспортних засобів вимог встановлених правил дорожнього руху, використовуються системи автоматичної фото та відео-фіксації правопорушень у сфері безпеки дорожнього руху, це безумовно дуже хороший приклад для законодавчих систем інших європейських країн, включаючи і Україну, яка почала переймати цей досвід.

Серед європейських країн Україна залишається одним з лідерів серед держав із складною ситуацією з дорожньо-транспортними пригодами і травматичними та летальними їх наслідками.

Протягом 2014 року на вулично-дорожній мережі країни сталося понад 153 тис. дорожньо-транспортних пригод, у тому числі 26 тис. з постраждалими, у яких загинуло 4,4 тис. і травмувалось 32,2 тис. громадян. Іншими словами, майже кожні 17 хвилин траплялося ДТП з постраждалими, практично кожні 2 години гинула людина.

За перші 10 місяців 2015 року в Україні сталося 107 324, з них 20 033 ДТП з постраждалими, в яких 25 028 осіб травмовано та 3 124 загинуло, в тому числі постраждало 3 258 дітей до 18 років і 173 дитини загинуло. Проаналізувавши поквартально статистику 2015 року аварійності на дорогах України, можна дійти висновку, що аварійність з кожним кварталом росте, так за перші три квартали 2015 року в Україні сталося 17312 аварій , в них 21708 постраждалі і 2661 загинуло. В першому кварталі

сталося 3914 ДТП в них 4764 людей травмовано і загинуло 672 людей , в другому 5888 ДТП (приріст в 50%), а в третьому 7359 аварій в них 9419 травмовано і 1075 загинуло. Як вбачається з наведених даних приріст ДТП в Україні з певними летальними випадками дуже великий , так приріст між першим і третім кварталом 2015 року становить майже 50% ДТП з летальними наслідками, а скоєних ДТП в третьому кварталі вдвічі перевищує показник першого кварталу. Я вважаю, що ці показники мали б дати відповідним органам певне уявлення про стан ДТП в Україні і здійснювати певні позитивні зрушення в нівелювання цих показників, адже ці показники не просто цифри, а реальний і страшний показник небезпеки людського життя на дорогах.

Аналізуючи вище зазначену інформацію можна дійти висновку, що основними причинами таких авто пригод стали перевищення безпечної швидкості руху (26 % від усіх ДТП з постраждалими), порушення правил маневрування (19,5 %), порушення правил проїзду перехресть (понад 7 %).

Проаналізувавши дані, які зазначає Всесвітня організація охорони здоров'я можна дійти висновку, що щорічно в світі у ДТП гине 1,3 мільйона осіб і 30-50 мільйонів отримують травми. Зараз це друга найпоширеніша причина смертності серед 6-14 річних підлітків та найпоширеніша серед людей у віці 15-44 років і є більш небезпечною ніж малярія, а до 2030 року буде в 2 рази небезпечніше СНІД та в 4 рази небезпечніше туберкульозу. Якщо не вжити жодних заходів, до 2020 року очікується підвищення рівня смертності у ДТП до 80 %.

Для нівелювання показників смертності на дорогах і порушень правил дорожнього руху законодавчим органом України вноситься низка нововведень для забезпечення безпеки дорожнього руху, основну роль яких становлять інформаційне забезпечення руху технічними засобами контролю.

Одним із перших позитивних змін у введенні засобів інформаційних технологій для фіксації фактів адміністративних правопорушень є результати реалізації Концепції першочергових заходів реформування системи Міністерства внутрішніх справ, схваленої розпорядженням Кабінету Міністрів України від 22 жовтня 2014 р. №1118-р, проголошено утвердження принципів верховенства права, неупередженості, доброчесності та додержання прав і свобод людини і громадянина в діяльності органів

внутрішніх справ; наближення стандартів діяльності органів внутрішніх справ до відповідних стандартів правоохоронних органів європейських країн.

Виходячи з пропозицій окремих народних депутатів, вони пропонують внести зміни в Кодекс України про адміністративні правопорушення внести в перелік такі заходи, які спрямовані на досягнення цієї мети, до них належать впровадження захищених засобів відео-фіксації на потенційно критичних об'єктах і автоматичної фіксації порушень у сфері безпеки дорожнього руху.

Нововведення щодо впровадження захищених засобів відео-фіксації на потенційно критичних об'єктах і автоматичної фіксації порушень у сфері безпеки дорожнього руху підтримують усі науковці в галузі адміністративного права з метою запобігання описаним негативним наслідкам, я вважаю, що їх утілення в життя повинно здійснюватися за умови невідкладного приведення національної дорожньої інфраструктури у відповідність до вимог чинних європейських норм і стандартів та на основі обов'язкового врахування не лише досягнутого рівня, а й перспектив розвитку науково-технічного прогресу в Україні та світі, а також наявного негативного досвіду впровадження в діяльність Державтоінспекції сумнозвісних «листів щастя». Також потрібно привести стан доріг у належний стан, адже упровадження нової системи фіксації адміністративних правопорушень технічними засобами повинно передувати належній організації дорожнього руху.

Законодавчий орган України у своїх проектах законопроектів визнає велику роль забезпечення дорожнього руху за допомогою інформаційних технологій фіксації порушень ПДР.

Як визначається законопроектом про внесення змін до Кодексу про Адміністративні правопорушення автоматично фіксуватися будуть порушення швидкісного режиму, проїзд на заборонний сигнал світлофора, виїзд на смугу зустрічного руху, а також порушення правил стоянки та зупинки тощо.

Використовуючи стаціонарні системи застосовуються відповідні дорожні знаки та муляжі для періодичної зміни місця фіксації правопорушень шляхом перестановки приладів у встановлених стаціонарно контейнерах.

Працівники поліції не зупиняють водія, а інформація про порушення автоматично за допомогою технічних засобів обміну інформації і автоматизованої системи документообігу і передається до відповідного підрозділу (центру обробки інформації), обробляється та надсилається власнику транспортного засобу, на якому скоєно правопорушення, відповідне повідомлення. Я вважаю, що ці нововведення містять в собі багато недоліків, тому що ці прилади автоматичної фіксації не фіксують самого водія транспортного засобу, а фіксують номери агрегатів і направляють дані автоматично в базу даних і надсилається не особі , яка керувала транспортним засобом, а власнику транспортного засобу.

Така обробка даних включає в себе фіксацію факту правопорушення, розпізнання номерного знака автомобіля, визначення через відповідні бази даних власника та винесення постанови про розмір штрафу, і це все здійснюється відповідними засобами інформаційних технологій. На мою думку це допоможе об'єктивно фіксувати і оформлювати правопорушення в автоматичному режимі без участі посадової особи.

Автоматичні системи фіксації правопорушень можуть також використовувати і муніципальні органи. При цьому штрафи стягуються до державного бюджету, а у випадку з муніципальними підрозділами – до бюджету відповідної адміністративної одиниці.

Використання сучасних інформаційних технологій, крім фіксації та оброблення інформації про правопорушення, дозволяє також здійснювати сплату накладених штрафів через мережу Інтернет, телефон або електронну пошту.

Я вважаю, що запровадження на території нашої держави автоматичних систем фіксації правопорушень у сфері безпеки дорожнього руху дозволить відповідно до європейських стандартів удосконалити порядок контролю за дотриманням водіями вимог Правил дорожнього руху.

Верховна Рада України ухвалила в першому читанні проект Закону «Про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання відносин у сфері забезпечення безпеки дорожнього руху» (№2562), внесений Кабінетом

Міністрів України. На мою думку це один з найбільш реальних перших кроків в автоматизації системи авто порушень.

Метою даного законопроекту є зменшення кількості ДТП та загиблих і травмованих у них людей шляхом запровадження в Україні ефективного адміністративно-правового механізму притягнення до відповідальності за адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані в автоматичному режимі.

За дане рішення проголосували 247 із 346 народних депутатів, зареєстрованих в сесійній залі.

Верховна Рада України також вирішила, що до другого читання у законопроекті має бути враховано ряд положень проекту закону з цього ж питання під реєстраційним № 2562-1, внесений рядом народних депутатів.

Законопроектом, запропонованим урядом, передбачається запровадження системи автоматичної фотозйомки і/або відеофіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху.

Як зазначається в цих законопроектах, пропонується доповнити Кодекс України про адміністративні правопорушення статтею 14-2, відповідно до якої запроваджується автоматична фото та відео-фіксація низки порушень правил дорожнього руху.

Пропонується законодавчо закріпити норму, згідно з якою відповідальність за правопорушення у сфері забезпечення дорожнього руху, що зафіксовані в автоматичному режимі, нестиме юридична або фізична особа, за якою зареєстровано транспортний засіб.

Фіксація визнаватиметься безумовним доказом вини власника, це може бути як фізична так і юридична особа або особа, яка ввезла транспортний засіб на територію України, якщо вони не доведуть, що транспортний засіб або його номерний знак вибув з їхнього володіння внаслідок протиправних дій інших осіб.

«Відповідальності за адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані в автоматичному режимі» від 16 січня 2014 р. №723-VII : стаття 142 «Відповідальність за адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані в автоматичному режимі». Частиною першою цієї статті визначає,

що адміністративну відповідальність за адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані в автоматичному режимі за допомогою технічних засобів, що дають змогу здійснювати фотозйомку та/або відеозапис без участі оператора, несе особа, за якою зареєстрований транспортний засіб». Спрямованість цього закону полягає в установленні презумпції вини власника транспортного засобу (особи, за якою зареєстровано транспортний засіб) у вчиненні певних адміністративних правопорушень у разі їх автоматичної фіксації і покладенні (фактично перекладанні) на власника обов'язку доводити свою невинуватість у вчиненні адміністративного правопорушення. Її реалізація могла потягнути за собою серйозні порушення прав громадян, зокрема конституційного принципу індивідуальності юридичної відповідальності та презумпції невинуватості; створювала правову невизначеність в установленні суб'єкта, що притягується до відповідальності у цій сфері.

В Україні започаткували введення автоматичної фіксації порушень у сфері безпеки дорожнього руху в розроблених проектів відповідних законів на застарілій нормативно-правовій, технічній і технологічній основі, яка:

1) обмежує перелік учасників дорожнього руху, правопорушення яких є досяжними для автоматичної фіксації, виключно водіями офіційно зареєстрованих транспортних засобів, а коло адміністративних правопорушень, що об'єктивно можуть бути зафіксовані в автоматичному режимі, звужує виключно до: перевищення обмежень швидкості руху транспортних засобів, проїзду на заборонний сигнал регулювання дорожнього руху, порушення правил зупинки і стоянки, а також встановленої для транспортних засобів заборони.

2) передбачає опосередковане ототожнення автомобіля за зафіксованим на фото та відео-зображенні державним реєстраційним номером встановлення за реєстраційними даними ДАІ виключно власників транспортних засобів, які часто навіть не керували цими засобами під час вчинення правопорушення (фактично не були чи не могли бути їх водіями, наприклад, через перебування в іншому місці чи наявність істотних фізичних вад), а у випадку з власниками – юридичними особами взагалі не могли бути водіями

Також здійснюється перелік технічних засобів, що використовуються в підрозділах Державтоінспекції МВС для виявлення та фіксування порушень дорожнього руху відповідним нормативним актом, затвердженим наказом МВС України від 1 березня 2010 р. №33, зареєстрованим у Міністерстві юстиції України 30 березня 2010 р. за №262/17557.

Цим актом зазначається, що до числа спеціальних технічних засобів, які працюють в автоматичному режимі, що мають функції фото і кінозйомки, відеозапису, цим Переліком віднесено виключно:

1) вимірювач швидкості радіолокаційний відеозаписувальний «ВИЗИР» з активованою функцією «автоматичний режим» модифікації «ВИЗИР 03»;

2) вимірювач швидкості радіолокаційний з фото-фіксацією «АРЕНА»;

3) лазерний вимірювач швидкості транспортних засобів «TruCAM»

Законопроектами, які уже були мною зазначенні пропонується цей перелік розширити відповідними новими інформаційними технологіями для фіксації адміністративних правопорушень, такими як: фото та відео зйомка, та автоматичне оброблення і відправлення цих даних у відповідний центр обробки даних.

Виходячи з даних наведених у цій статті, введення в Україні систем автоматичної фіксації порушень правил дорожнього руху за допомогою інформаційних технічних засобів допоможе зменшити показники порушень правил дорожнього руху, та летальних і травматичних наслідків їх порушень завдяки автоматичному надходженні інформації працівникам правоохоронних органів.

Також такі нововведення допоможуть Україні виконати позитивні зобов'язання реалізації підписаних Європейських Конвенції, які є обов'язковими для України на шляху до євроінтеграції.

Я вважаю, що дані інформаційні технології, які пропонуються для введення фіксації адміністративних порушень є шляхом до об'єктивізації оформлень порушень, але існують також і багато недоліків, таких як: – дані інформаційні технології, які пропонуються ввести не зовсім досконалі для фіксації самих

водіїв транспортних засобів, їх можливості обмежені лише в фіксації номерів транспортного засобу; – запровадження і встановлення таких засобів є дуже затратним і потребує велику кількість фахівців у галузі інформаційних технологій.

Можна сказати, що позитивні зрушення у реформуванні правоохоронної системи відбувається, зокрема у автоматизації цієї системи, а також у проектах створення кібер поліції.

1. Кодекс України про адміністративні правопорушення від 6 жовтня 2015 року;
2. Наукова стаття Шепітько В.Ю, Білоус В.В., Використання інформаційних технологій під час автоматичної фіксації порушень у сфері безпеки дорожнього руху;
3. Пояснювальна записка до проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання відносин у сфері забезпечення безпеки дорожнього руху та відповідальності за порушення правил дорожнього руху, що зафіксовані в автоматичному режимі»;
4. Концепція першочергових заходів реформування системи Міністерства внутрішніх справ від 10 грудня 2014 року;
5. Проект Закону «Про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання відносин у сфері забезпечення безпеки дорожнього руху» (№2562) від 06.04.2015р.;
6. Наказ МВС України від 1 березня 2010 р. №33, зареєстрований у Міністерстві юстиції України 30 березня 2010 р. за №262/17557.

МОДЕЛІ ЗМІН В СУСПІЛЬСТВІ НА ОСНОВІ ІНТЕЛЕКТУАЛІЗАЦІЇ

Мойсеєнко Ірина Павлівна,
професор кафедри фінансів
Львівського державного університету внутрішніх справ,
доктор економічних наук, професор

Розвиток великих систем є нелінійним, нестабільним, багатоваріантним та суперечливим процесом, який відбувається під постійним впливом внутрішніх та зовнішніх чинників, що спонукають прилаштовуватись до нових умов шляхом системної трансформації. В сучасних умовах продовження системної кризи в Україні відбувається загострення суспільної, політичної та економічної трансформації, що ускладнюється необхідністю проведення глибоких економічних та соціальних реформ в умовах глобальних викликів. Сучасні системні трансформації є неоднозначними за своїми наслідками, впливають на основи економічної системи, знижують її системну стійкість і супроводжуються кризовими явищами.

Тому актуалізується потреба в ґрунтовному осмисленні сутності, закономірностей розвитку, структурної динаміки та механізмів трансформації економічних систем.

Процес трансформації полягає у зміні компонентів, параметрів, пропорцій та зв'язків економічної системи у процесі переходу в новий якісний стан, під впливом зовнішнього середовища. Трансформаційний процес має динамічну природу, яка виступає, як процес та результат, що призводить до аналізу процесу зміни економічної системи з оцінкою її якісного стану. Ця оцінка системи здійснюється перш за все тоді, коли потрібно підтримати її життєздатність і примноження потенціалу розвитку [1].

Основна увага дослідників, переважно, зосереджується на таких проявах трансформації економічних систем: трансформація від капіталізму до соціалізму, від планової до ринкової економіки; трансформація, обумовлена цивілізаційно-формаційним розвитком. Тому сучасні уявлення про проблематику

економічних трансформацій потребують їх подальшої розробки з урахуванням необхідності міждисциплінарності аналізу (політичні та економічні трансформації). Також нерозв'язаними залишаються питання, пов'язані з пошуком оптимальних шляхів трансформації та прогнозування майбутнього стану економічної системи.

Метою статті є систематизація підходів щодо дослідження динамічних процесів в економіці, де трансформація постає як їх внутрішня і необхідна частина, обґрунтування сутності, причин виникнення та наслідків трансформацій сучасної економічної системи.

Економічну трансформацію, переважно, розглядають як процес внесення нових елементів в модель національної економіки, який призводить до змін існуючої або створення нової [3, 24]. Важливо пам'ятати, що трансформаційні зміни неможливі без докорінної перебудови всіх елементів соціально-економічного укладу суспільства. Ігнорування даної умови призводить до низки проблем сучасної трансформаційної кризи в Україні. (рис 1).

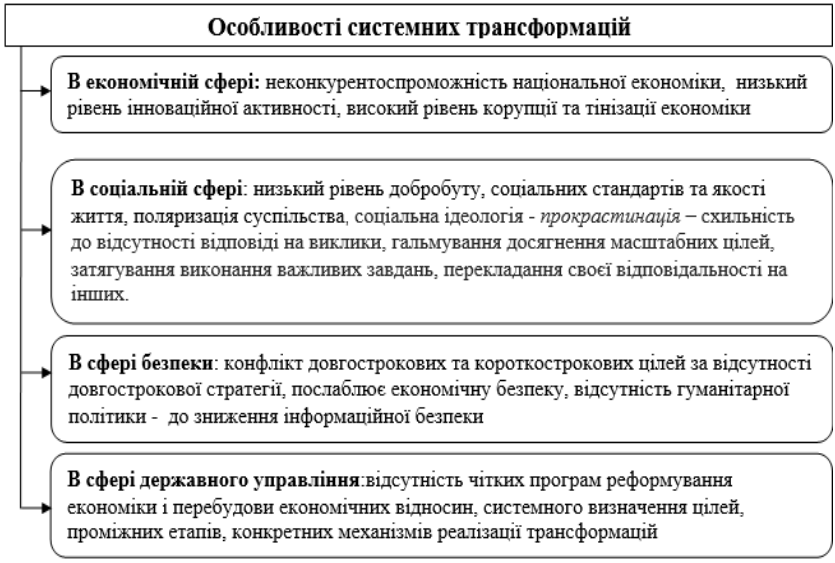


Рис.1 Особливості трансформаційних процесів в Україні розроблено автором на основі джерел [2, 3].

З метою обґрунтування сутності, основних етапів та форм трансформаційних процесів в економічних системах як самостійний напрям досліджень формується економічна транзитологія. Вітчизняні вчені пропонують розглянути економічну транзитологію в таких аспектах: обґрунтування перехідних процесів у країнах, що розвиваються; вирішення проблем і суперечностей транзитивних змін в економічних системах; фрагментація економічної транзитології під впливом економічного розвитку та інституційної парадигми [2, 78-79].

Сучасні науковці пропонують виокремити також наступні підходи до системних трансформацій: модернізаційний, інституціональний, технократично-футурологічний та синергетичний.

Модернізаційний підхід спрямований на усунення структурних диспропорцій, накопичених в період докризового розвитку; цілеспрямоване формування майбутніх структурних характеристик економічної системи на основі врахування майбутніх ризиків. Модернізоване суспільство має комплекс взаємопов'язаних рис, котрі часто розглядають як окремі процеси економічної, політичної, соціальної та культурної модернізації.

Економічна модернізація передбачає інтенсифікацію процесу економічного відтворення, котра досягається завдяки зростанню спеціалізації та диференціації праці, енергетичного устаткування виробництва, перетворення науки на виробничу (економічну) силу та розвитку раціонального управління виробництвом.

Політична модернізація передбачає створення певних політичних інститутів, які мають сприяти реальній участі населення у владних структурах та впливу народних мас на прийняття конкретних рішень. Її складові:наближення до диференційованої політичної структури з високою спеціалізацією політичних ролей та інститутів; посилення ролі держави; розширення сфери дії та посилення ролі законодавчого поля, що поєднує державу та громадян; ослаблення традиційних еліт та їхньої легітимності, посилення модернізаторських еліт.

Соціальна модернізація передбачає формування відкритого суспільства з динамічною соціальною структурою. Її складові:створення суспільства з відкритою стратифікаційною системою та високою мобільністю;складна система соціального

управління (відокремлення інституту управління, соціальних органів управління та самоврядування);виокремлення різноманітних соціальних інститутів. Соціальна модернізація сприяє розвитку громадянського суспільства та соціальної держави[7].

Культурна модернізація передбачає формування високодиференційованої і в той же час уніфікованої культури, що базується на комплексній парадигмі прогресу, удосконалення, ефективності, щастя і природного вираження особистих можливостей і почуттів, а також на розвиткові індивідуалізму.

Інституціональний підхід дозволяє враховувати особливості перехідних економік (необхідність здійснення перетворень у традиційних сферах діяльності, подолання викривлень колишнього режиму, створення нових норм і процедур) [3], а також обґрунтовує можливість реалізації однакових реформ для різних економічних систем.

Увага технократично-футурологічного підходу зосереджена на переході економічних систем до постіндустріальної стадії розвитку, а також проблеми слаборозвинутих держав. Підхід базується на науково-технічній та інформаційно-технологічній революції [6].

Моделі змін в суспільстві на основі інтелектуалізації передбачають використання таких їх різновидів: інституційно-ідеологічна, лідерсько-інноваційна, соціально-партнерська на основі використання інтелектуального, культурного та освітнього потенціалу нації.

Науковці допускають, що основними механізмами реалізації синергетики при виборі та використання різних моделей є процеси інтеграції та диференціації. А здатність економічних систем до саморозвитку є внутрішньо необхідною добровільною зміною, обумовленою її внутрішніми суперечностями, що викликає трансформацію економічної системи [4, 32].

Висновки. Трансформація економічних систем є невід'ємною складовою сучасного глобального світу та рушійною силою його розвитку, проте супроводжується закономірними кризовими явищами. Основними цілями, що об'єктивно обґрунтовують необхідність подальшої трансформації економіки України, є: макроекономічна і фінансова стабілізація; підвищення добробуту народу, зростання витрат на медицину, освіту, відпочинок; підвищення інноваційного потенціалу.

Трансформація економіки України залишається незавершеною, оскільки сформовані державні та ринкові інститути не відповідають сучасним вимогам прозорості, ефективності та результативності, а проведені реформи носять фрагментарний, а не системний характер.

1. Ерохина Е. А. Теория экономического развития: системно-синергетический подход / Е. А. Ерохина [Электронный ресурс]. — Режим доступу : http://ek-lit.narod.ru/eroh/index.html.
2. Дацюк С.Серая Пирамида в стадии завершения
3. С. Дацюк [Электронный ресурс]. — Режим доступу : www.pravda.com.ua/rus/articles/2013/07/15/6994246/view_print/
4. Кухарская Н.А. Сущноть и направления трансформации экономичекого развития Украины в условиях рыночных реформ / Н.А. Кухарская // Економічні інновації . – 2013. Вип. 52. – С. 113- 123.
5. Мельник Л.Г. Теория самоорганизации экономических систем: монография / Л.Г. Мельник . – Сумы: Университетская книга, 2012. – С. 439.
6. Черленяк І.І. Концептуальні проблеми ідентифікації постсоціалістичної трансформації економічної системи України / І.І. Черленяк, О.А. Курей // Економічний часопис – XXI. – 2013. – № 11-12(2). – С. 3-6.
7. Ягельська К.Ю. Місце трансформаційних процесів української економіки в типології економічного розвитку / К.Ю. Ягельська // Європейський вектор економічного розвитку. – 2014. – № 1(16). – С.203-209.
8. Новікова О.Ф. Соціальна орієнтація економіки: механізми державного регулювання: [монографія] / О.Ф. Новікова, С.М. Гріневська, Л.Л. Шамілева. – Донецьк: Ін-т економіки пром-сті, 2009. – 219 с.

ОХОРОНА ІНФОРМАЦІЇ: ПОГЛЯД ЗБОКУ

Мороз Володимир Іванович,
професор кафедри електроприводу і комп'ютеризованих
електромеханічних систем
Національного університету «Львівська політехніка»
доктор технічних наук, професор

Захист інформації, як відомо, має три об'єктивних аспекти: апаратний, інформаційний і програмний. Проте, як стверджують джерела, основний же витік непублічної інформації відбувається внаслідок четвертого, суб'єктивного фактору – людського (організаційного). Так, вважається, що більше половини витоків відбувається саме таким чином, а за неофіційними даними це може бути навіть три чверті всіх витоків конфіденційної інформації.

Як приклад, можна навести типову поведінку комп'ютерних хакерів, які отримують логіни та паролі безпосередньо від користувачів захищених мереж (зокрема, банків), називаючись адміністратором чи працівником служби захисту.

Іншим, актуальним на даний час прикладом є використання за старою звичкою багатьма українськими користувачами російських поштових серверів **mail.ru**, **yandex.ru**, **rambler.ru** для яких **законодавчо** встановлено **повний контроль** російськими спецслужбами. Потрібно теж згадати російські антивіруси Касперського, DrWeb, які непомітно для користувача встановлюють шпигунські модулі в систему [1, 2]. Напевно, не один користувач вже зустрічався з проблемами пересилання електронної пошти на згадані російські сервери, а також незрозумілої поведінки свого комп'ютера у випадку використання російських антивірусів.

Як альтернативу російським поштовим службам можна рекомендувати відповідні сервіси Microsoft і Google, які підтримують і корпоративну пошту, що, наприклад, і зроблено у Львівській політехніці. Потрібно відзначити, що і Microsoft, і Google відмовилися надавати доступ до інформації своїх

користувачів урядам і навіть АНБ США. Полегшити користувачам перехід на ці поштові сервіси дає змогу проста процедура підімкнення та наступного використання згаданих російських поштових скриньок до захищених поштових сервісів Gmail чи Outlook.

Якщо суб'єктивний фактор усунути, залишаються об'єктивні фактори, з яких хотілося б проаналізувати відомі, проте не дуже поширені можливості того, що конфіденційна інформація може «витекти» за дозволені межі.

Апаратний бік захисту інформації

1. Передача інформації між комп'ютерами через оптичний канал: екран + відеокамера.

У даному варіанті джерелом сигналу є дисплей персонального комп'ютера чи ноутбука, через який шляхом відповідної **невидимої оком** модуляції (наприклад, з частотою поновлення екрану 60 Гц і невеликої амплітуди, наприклад, 10% від рівня світіння екрану) передається необхідна інформація. На іншому комп'ютері така інформація зчитується вбудованою камерою чи спеціальним пристроєм, якщо ведеться спостереження зовні.

2. Передача інформації між комп'ютерами через акустичний канал: гучномовець + мікрофон.

У цьому випадку інформація передається акустичним каналом з використанням **нечутної для вуха** частоти (вище 18–20 КГц) з використанням відповідної модуляції, що дає змогу приховати процес шумоподібним сигналом. На іншому комп'ютері ця інформація зчитується вбудованим мікрофоном чи спеціальним спрямованим мікрофоном, якщо ведеться спостереження зовні.

Ще одним, менш відомим фактом є існування в процесорах Intel спеціальної області пам'яті, яка призначена для прошивки новим мікрокодом вже випущених процесорів у випадку виявлення допущених помилок на кристалі. Така заміна прошивки мікрокоду дає змогу не лише виправити помилки у виконанні команд процесора, але «занести» у процесор зловмисний код, який не виявить **ЖОДНА** програма, і цей процес проконтролювати неможливо ніякими засобами.

Інформаційний бік захисту інформації. Звичайно, можна заперечити існування каналу втрати конфіденційної інформації,

посилаючись на відсутність зовнішніх ознак наявності такого каналу – простіше, кажучи, його не виявили. Таку ситуацію можна пояснити як покращенням якості каналу передачі інформації, так і підвищенням її захищеності. З них я відзначу лише два.

- Звуження смуги пропускання каналу.

Звуження смуги пропускання приймача інформації, як відомо, дає змогу покращити співвідношення сигнал до шуму. Звичайно, при цьому знижується швидкість передачі інформації, але якщо потрібно викрасти пароль, то навіть невеликої швидкості цілком достатньо. При цьому рівень передачі сигналу можна вибрати настільки низьким, що для зовнішнього спостерігача він буде непомітним.

- Застосування шумоподібних сигналів.

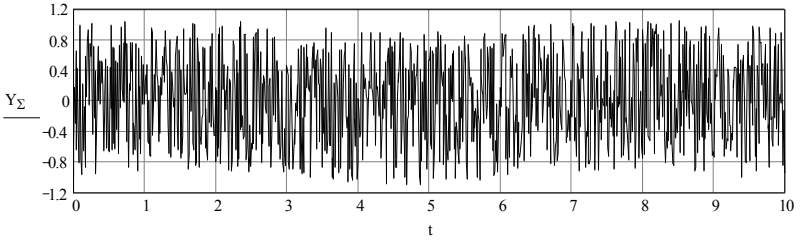
Застосування шумоподібних сигналів (наприклад, коду Баркера [3]) дає змогу приховати факт передачі інформації від користувача через аудіовізуальні чи інші канали комп'ютера. Не знаючи порядку даного коду та частоти його дискретизації такий сигнал практично неможливо виявити, оскільки код Баркера генерує рівномірний шумовий сигнал, який «губиться» на фоні всіх інших сигналів.

- Застосування автокореляційних функцій.

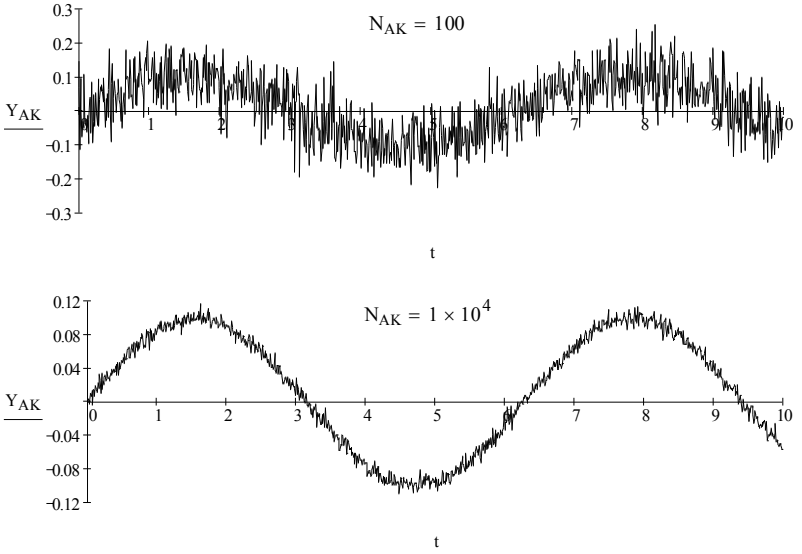
У випадку, якщо рівень корисного сигналу значно поступається шумам і завадам, використання автокореляційних функцій для фільтрації дає змогу виділити необхідну інформацію, щоправда за довший проміжок часу відповідно до кількості усереднень. Простий приклад з використанням синусоїдного сигналу та шуму, який має на порядок більшу амплітуду, показує переваги використання автокореляційної функції для виділення корисного сигналу, що й показано на рисунку для різної кількості усереднень.

Як приклади передачі інформації з дуже низьким рівнем сигналу внаслідок віддаленості можна згадати міжпланетні зонди Pioneer-10, Voyager, New Horizons, час надходження сигналу від яких вже перевищує 20 год. Іншим прикладом є навігаційні системи (наприклад, GPS) – ми не задумуємося над тим, що супутник знаходиться на орбіті висотою понад 20 тис. км і має

потужність передавача 50 Вт, а його сигнал без проблем розпізнають сучасні смартфони чи навігатори без громіздких антен. Це досягається швидкістю передачі інформації приблизно 50 біт за сек.



«Зашумлений» сигнал



Ефект виділення корисного сигналу автокореляцією

Програмний бік захисту інформації. Давнє питання: Windows проти Linux – абсолютного захисту інформації у жодній системі нема, суперечки про переваги чи недоліки тієї чи іншої системи у плані захищеності безпідставні. Яскравим підтвердженням цього є постійна дискусія в Internet стосовно переваг

кожної зі систем, нових вірусів і троянів, які вражають кожну з них. Тут нічого кращого, ніж організаційні заходи не придумати.

На закінчення для ознайомлення пропонується невеликий перелік матеріалів, які пов'язані з проблемою втрати конфіденційної інформації [4–8].

1. Ворона Т. «Лаборатория Касперского» сотрудничает с российскими спецслужбами – Bloomberg [Електронний ресурс] / Т. Ворона. – [Режим доступу до ресурсу]: http://ain.ua/2015/03/20/570795
2. Райбман Н. Bloomberg сообщил об укреплении связей «Лаборатории Касперского» с российской разведкой [Електронний ресурс] / Н. Райбман. – [Режим доступу до ресурсу]: http://www.vedomosti.ru/politics/articles/2015/03/20/bloomberg-soobschil-ob-ukreplenii-svyazei-laboratorii-kasperskogo-s-rossiiskoi-razvedkoi
3. Barker Code [Wikipedia] [Електронний ресурс]. – [Режим доступу до ресурсу]: https://en.wikipedia.org/wiki/Barker_code
4. BadBIOS, или Большие проблемы [Електронний ресурс]. – [Режим доступу до ресурсу]: http://www.3dnews.ru/777783
5. UEFI: хотели как лучше… [Електронний ресурс]. – [Режим доступу до ресурсу]: http://kiwibyrd.org/2013/11/07/1110/
6. Чума на ваши USB [Електронний ресурс] . – [Режим доступу до ресурсу]: http://www.3dnews.ru/825348
7. UEFI как SNAFU [Електронний ресурс]. – [Режим доступу до ресурсу]: http://www.3dnews.ru/908186 або http://kiwi-byrd.org/2015/01/23/151/
8. Карасёв С. Выявлена масштабная кампания кибершпионажа через компьютерные накопители [Електронний ресурс]/ Сергей Карасёв. – [Режим доступу до ресурсу]: http://www.3dnews.ru/909624

ПРОБЛЕМИ І ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Нагачевська Юлія Сергіївна,
доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
кандидат юридичних наук

Інформація – явище незрівнянно більш древнє, ніж сама людина. Уже природа у процесі своєї еволюції передавала закодовану інформацію в рослинах і живих організмах. З перших своїх кроків люди шукають і знаходять нові засоби передачі, збереження та обробки інформації. Однак ніколи раніше людство не накопичувало інформацію й знання настільки стрімкими темпами. Тому закономірним є те, що жодна галузь людської діяльності не зазнала такого розвитку як інформаційні технології. Саме вони були покликані збільшити ефективність та зручність використання різноманітних видів інформації. За останні десятиріччя інформаційні технології зазнали такого глобального поширення, що зараз уже важко уявити життя сучасної людини без них.

Для інформаційних технологій є цілком природним те, що вони застарівають і заміняються новими. Так, наприклад, на зміну технології пакетного опрацювання програм на великий ЕОМ в обчислювальному центрі прийшла технологія роботи на персональному комп'ютері на робочому місці користувача. Телеграф передав усі свої функції телефону. Телефон поступово витісняється службою експресс-доставки. Телекс передав більшість своїх функцій факсу й електронній пошті.

При впровадженні нової інформаційної технології в організації необхідно оцінити ризик відставання від конкурентів у результаті її неминучого старіння, тому що інформаційні продукти, як ніякі інші види матеріальних товарів, мають надзвичайно високу швидкість змінюваності новими видами або версіями. Періоди змінюваності коливаються від декількох місяців до одного року. Якщо в процесі впровадження нової

інформаційної технології цьому фактору не приділяти належної уваги, цілком можливо, що до моменту завершення переходу фірми на нову інформаційну технологію вона вже застаріє і прийдеться вживати заходів щодо її модернізації. Такі невдачі з впровадженням інформаційних технологій звичайно пов'язані з недосконалістю технічних засобів, в той час як основною причиною невдач є відсутність або слабка пропрацьованність методології використання інформаційної технології.

Централізоване опрацювання інформації на ЕОМ обчислювальних центрів були першою історично сформованою технологією. Створювалися великі обчислювальні центри колективного користування, оснащені великими ЕОМ. Застосування таких ЕОМ дозволяло опрацьовувати великі масиви вхідної інформації й одержати на цій основі різноманітні види інформаційної продукції, яка потім передавалася користувачам. Такий технологічний процес був обумовлений недостатнім оснащенням обчислювальною технікою підприємств і організацій у 60-70-і рр.

Переваги методології централізованої технології:

- можливість звертання користувача до великих масивів інформації у вигляді баз даних і до інформаційної продукції широкої номенклатури;
- відносна легкість упровадження методологічних рішень по розвитку й удосконалюванню інформаційної технології завдяки їх централізованому прийняттю.

Недоліки такої методології очевидні:

- обмежена відповідальність нижчого персоналу, що не сприяє оперативному одержанню інформації користувачем, тим самим перешкоджаючи правильності виробітку управлінських рішень;
- обмеження можливостей користувача в процесі одержання і використання інформації.

Децентралізоване опрацювання інформації пов'язане з появою в 80-х рр. персональних комп'ютерів і розвитком засобів телекомунікацій. Вона дуже істотно потіснила попередню технологію, оскільки дає користувачу широкі можливості в роботі з інформацією і не обмежує його ініціатив.

Перевагами такої методології є:

- гнучкість структури, що забезпечує простір ініціативам користувача;
- посилення відповідальності нижчої ланки співробітників;
- зменшення потреби в користуванні центральним комп'ютером і відповідно контролі з боку обчислювального центру;
- більш повна реалізація творчого потенціалу користувача завдяки використанню засобів комп'ютерного зв'язку.

Проте ця методологія має і свої недоліки:

- складність стандартизації через велику кількість унікальних розробок;
- психологічне несприйняття користувачами що рекомендуються обчислювальним центром стандартів у готових програмні продукти;
- нерівномірність розвитку рівня інформаційної технології на локальних місцях, що в першу чергу визначається рівнем кваліфікації конкретного працівника.

Описані переваги і недоліки централізованої і децентралізованої інформаційної технології призвели до необхідності притримуватися лінії розумного застосування і того, і іншого підходу.

Такий підхід назвемо раціональною методологією і покажемо, як у цьому випадку будуть розподілятися обов'язки:

- обчислювальний центр повинен відповідати за створення загальної стратегії використання інформаційної технології, допомагати користувачам як у роботі, так і у навчанні, установлювати стандарт і визначати політику застосування програмних і технічних засобів;
- персонал, який використовує інформаційну технологію, повинен дотримуватися вказівок обчислювального центру, здійснювати розробку своїх локальних систем і технологій відповідно до загального плану організації.

Раціональна методологія використання інформаційної технології дозволить досягти більшої гнучкості, підтримувати загальні стандарти, здійснити сумісність інформаційних локальних продуктів та знизити дублювання діяльності.

Отже, одним із засобів керування розвитком інтелекту і підвищення його організованості на сучасному етапі є інформатизація суспільства, що ґрунтується насамперед на розвитку

інформаційних комп'ютерних технологій. Значення інформаційної технології величезне – вона формує передній край науково-технічного прогресу, створює інформаційний фундамент розвитку науки і всіх інших технологій. Головними, визначальними стимулами розвитку інформаційної технології, є соціально-економічні потреби суспільства, і саме зараз суспільство як ніколи зацікавлене в якомога швидшій інформатизації та комп'ютеризації всіх без винятку сфер діяльності.

Дуже важливою властивістю інформаційної технології є те, що для неї інформація є не тільки продуктом, але і вихідною сировиною. Особлива роль приділяється всьому комплексу інформаційної технології і техніки в структурній перебудові економіки убік наукоємності. Більш того, інформаційна технологія є свого роду перетворювачем всіх інших галузей господарства, як виробничих, так і невиробничих, основним засобом їхньої автоматизації, якісної зміни продукції і, як наслідок, їх переходу частково або цілком у категорію наукомістких. Пов'язаний з цим і працезаощаджувальний характер інформаційної технології, що реалізується, зокрема, у керуванні багатьма видами робіт і технологічних операцій.

Безсумнівною перевагою інформаційної технології є те, що вона сама створює засоби для своєї еволюції. Формування системи, що саморозвивається найважливіший підсумок, досягнутий у сфері інформаційної технології.

Таким чином, усі вищевикладені риси інформаційної технології вказують на те, що вона й у майбутньому залишиться самим перспективним видом технології, що допомагає людині впевнено крокувати шляхом прогресу.

1. Макарова Н. В., Матвєєва Л. А., Бройдо В. Л. Підручник «Інформатика», М.: «Фінанси та статистика», 1997 р.
2. Багриновський К.А., Хрусталєв Е.Ю. «Нові інформаційні технології», М.: «ЭКО», 1996 р.
3. Крилов І. В. «Інформаційні технології: теорія і практика», М.: «Центр», 1996 р.
4. Малиновський Б.М. «Історія обчислювальної техніки», К.: «Лотус», 1995 р.
5. Кондрашова С.С. Учбовий посібник «Інформаційні технології в управлінні», К.: МАУП. 1998 р.

ТЕХНОЛОГІЯ HIBERNATE РОБОТИ З БАЗАМИ ДАНИХ

Неспляк Дмитро Михайлович,
викладач кафедри інформатики
Львівського державного університету внутрішніх справ
Магеровський Дмитро Вікторович,
студен ІКНІ
Національного університету «Львівська політехніка»

Дані є основою практично для будь-якого проекту. На основі вимог до програмної системи будується модель даних. Надалі саме з даною моделлю працює програма, вводиться деяка інформація, здійснюються обчислення, формуються звіти і т. д. У процесі розвитку програмних систем проектуються і використовуються різні системи управління базами даних (СУБД) – ієрархічні, реляційні, об'єктні та ін.

На практиці найбільшу популярність отримали саме реляційні моделі баз даних, хоча в сучасних методологіях програмування найбільшу популярність отримало об'єктно-орієнтоване програмування. Для стикування даних технологій розроблено безліч технологій, специфікацій та фреймворків для маппінга об'єктів на таблиці реляційних баз даних. Java розробникам доступно безліч технологій для роботи з даними. Це може бути просто сереалізація об'єктів, JDBC, JDO і безліч інших. Але кожна з них має ряд переваг і недоліків. Серіалізація (Serialization) є вбудованим механізмом зберігання і передачі об'єктів в Java. Проте для практичної роботи з даними даний підхід мало придатний, оскільки потрібно витягувати і зберігати весь граф об'єктів, що ускладнює роботу з великими обсягами даних. Java Database Connectivity (JDBC) Application programming interface (API) розроблявся для роботи з реляційними базами даних. Мінусом даної технології є відсутність механізмів проекції реляційних даних на об'єкти, що істотно збільшує обсяг коду для даного перетворення. Специфікація Java Data Objects (JDO) на поточний момент є однією з найбільш прогресивних і

дозволяє використовувати не тільки реляційні, а й об'єктні сховища даних. Java Persistence API (JPA) [1, 2, 3, 5, 6, 7] поєднує в собі простоту серіалізації об'єктів з можливістю роботи з даними на рівні об'єктно-орієнтованої моделі. При цьому залишається можливість комбінування доступу до даних як в JDBC [4, 8] на рівні реляційних даних, що інколи дозволяє досягати більшої продуктивності і гнучкості в порівнянні з JDO.

На поточний момент існує безліч реалізацій специфікації JPA, як комерційних, так і вільних з відкритим вихідним кодом (open source).

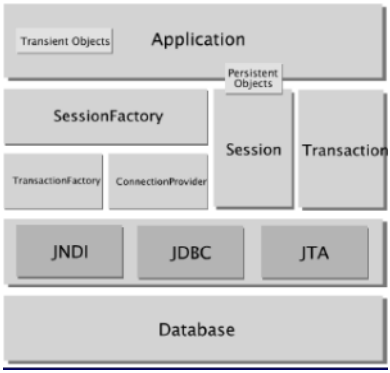


Рис. 1 Архітектура Hibernate

На рис 1 зображена схема, що показує комплексну архітектуру Hibernate. Приведемо деякі визначення об'єктів, які зображені на ній.

Прикладна програма (Application) – складається з усіх написаних користувачем Java файлів та інших ресурсів.

Перехідні об'єкти (Transient Objects) – примірники довгоживучих класів, які в даний час не пов'язані з сесією. Вони, можливо, були ініціалізовані у прикладній програмі і ще не збережені, або ж вони були ініціалізовані закритою сесією.

Постійні об'єкти (Persistent objects) – короткоживучі, однопоточні об'єкти, що містять постійний стан і бізнес-функції. Вони пов'язані тільки з однією сесією. Після того, як сесія закрита, вони будуть відокремлені і вільні для використання в будь-якому протоколі прикладного рівня (наприклад, в якості об'єктів передачі даних).

SessionFactory – потокобезпечний, незмінний кеш скомпільованих відображень для бази даних. Фабрика для сесії і клієнт для ConnectionProvider, SessionFactory може містити додатковий кеш даних, який використовується повторно між операціями в процесі.

Сессіея (Session) – Однопотоковий, короткоживучий об'єкт, що представляє взаємодію між прикладною програмою і постійною пам'яттю. Він служить обгорткою для JDBC з'єднання і також є фабрикою для Transaction. Сесія містить обов'язковий кеш першого рівня постійних об'єктів, який використовується для навігації по об'єктному графу або пошуку об'єктів за ідентифікатором.

TransactionFactory – фабрика для примірників Transaction. Інтерфейс не відкритий для програми, але може бути розширений або реалізований розробником.

ConnectionProvider – фабрика і пул JDBC з'єднань. Інтерфейс абстрагує додаток від основного джерела даних або диспетчера драйверів. Він не відкритий для програми, але може бути розширений або реалізований розробником.

Трансакція (Transaction) – однопоточний, короткоживучий об'єкт, який використовується додатком для вказівки atomic змінних роботи. Він абстрагує додаток від основних JDBC, JTA або CORBA трансакцій. Сесія може охоплювати кілька трансакцій в деяких випадках. Тим не менш, розмежування транзакцій, яке також використовується в основах API або Transaction, завжди обяв'язкове.

Hibernate є інструментом об'єктно-реляційного відображення для Java з відкритим вихідним кодом. Він надає фреймворк для відображення об'єктно-орієнтованої моделі даних в традиційні реляційні бази даних. Hibernate не тільки піклується про відображення класів Java в таблиці БД (і типів даних Java в типи даних SQL), але також забезпечує запит даних і пошукові засоби і може значно скоротити час розробки який витрачається на ручне написання SQL і JDBC коду.

Зіставлення Java-класів з таблицями БД здійснюється за допомогою конфігураційних XML файлів, або за допомогою Java анотацій. Забезпечуються можливості по організації відносини між класами один-до-багатьом і багато-до-багатьох. На додаток

до управління асоціацією між об'єктами, Hibernate може також управляти рефлексивними відносинами, де об'єкт має зв'язок один-до-багатьох з іншими екземплярами свого типу.

Інтерфейс JPA (Java Persistence API) надає можливість зберігати об'єкти. Hibernate є однією з реалізацій JPA. Існує також можливість анотувати класи використовуючи JPA анотації, однак без реалізації нічого не зміниться. JPA – це керівні принципи, які повинні дотримуватися або реалізовуватися, в той час як Hibernate це код, який відповідає API і забезпечує приховування функціональності.

При використанні Hibernate з JPA ми насправді використовуємо реалізацію JPA. Перевагою цього є те, що існує можливість поміняти Hibernate на будь-яку іншу реалізацію JPA специфікації. При використанні Hibernate безпосередньо, ми замикаємося в реалізації, тому що інші ORMs (Object-relational mapping) можуть використовувати не такі методи / конфігурації та анотації, внаслідок чого існує можливість просто переключитися на інший ORM.

Отже, використання Hibernate дозволяє швидко та ефективно працювати з базами даних використовуючи переваги об’єктно-орієнтованого програмування що є особливо зручно на етапі відлагодження та підтримки прикладних програм.

1. Cameron Wallace McKenzie Hibernate Made Easy: Simplified Data Persistence with Hibernate and Jpa (Java Persistence API) Annotations // Pulpjava. – 2008. – 442 pages
2. Christian Bauer, Gavin King Hibernate in Action // Manning Publications. – 2004. – 400 pages
3. Christian Bauer, Gavin King Java Persistence with Hibernate // Manning Publications. – 2006. – 904 pages
4. George Reese Database Programming with JDBC and Java // O'Reilly Media. – 1997. – 237 pages
5. James Elliott Hibernate: A Developer’s Notebook // O'Reilly Media. – 2004. – 192 pages
6. James Elliott, Timothy M. O'Brien, Ryan Fowler Harnessing Hibernate // O'Reilly Media. – 2008. – 382 pages
7. Madhusudhan Konda Just Hibernate // O'Reilly Media. – 2014. – 140 pages
8. R. M. Menon Expert Oracle JDBC Programming // Apress. – 2008. – 744 pages

ПРОБЛЕМІ ПИТАННЯ, ПОВ'ЯЗАНІ ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ПРИ ЗВЕРНЕННІ ДО СУДУ

Паращук Лідія Ярославівна,
ст.викладач кафедри електромеханіки та електроніки
Національної академії сухопутних військ імені гетьмана
Петра Сагайдачного,
кандидат технічних наук
Бесага Ірина Василівна,
студентка юридичного факультету
Львівського державного університету внутрішніх справ

На зміну некомпактним дискетам прийшли портативні засоби зв'язку, ноутбуки, флеш-носії, які уже не є чимось незвичним для більшості з нас, ми використовуємо їх як в роботі, так і в побуті. Не новина наразі і електронний підпис, можливість використання якого нарівні з власноручним встановлена законами, постановами та іншими підзаконними нормативними актами.

Так, правовому регулюванню даного питання присвячено велику кількість нормативних актів, зокрема Закон України «Про електронний цифровий підпис», Закон України «Про електронні документи та електронний документообіг» та значну кількість підзаконних нормативно-правових актів.

Стаття 1 Закону України «Про електронний цифровий підпис» встановлює, що Електронний цифровий підпис (ЕЦП) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Оригіналом електронного документа вважається електронний примірник з електронним цифровим підписом автора.

Формування ЕЦП створюється згідно з асиметричним алгоритмом RSA і відбувається за наступною схемою. Клієнт звертається в Центр сертифікації ключів для їх отримання. Придбавальник в одному сеансі генерує пару ключів: особистий (секретний) і відкритий (прилюдний). Особистий передається у вигляді файлу клієнтові, який зберігає цей ключ в таємниці. Відкритий ключ підписується сертифікатом ЦСК і передається також у вигляді файлу. Відкритий ключ знаходитиметься в сховищі відкритих ключів і клієнт може вільно поширювати його серед своїх кореспондентів. При відправці свого документа в суд чи державні органи або іншому кореспондентові, клієнт «підписує» файл своїм особистим ключем, тобто ставить контрольну суму (алфавітно-цифрову послідовність) у файл і пересилає його. Отримавши файл, кореспондент, маючи відкритий ключ клієнта, за певним алгоритмом самостійно розраховує контрольну суму. При збігу контрольної суми, що знаходиться у файлі, і розрахованої кореспондентом отриманий файл вважається автентичним.

Використання ЕЦП стало нормою та широко застосовується у всіх сферах суспільного життя, починаючи від посвідчення договорів і закінчуючи електронними позовними заявами. За загальним правилом, вироблення та використання ЕЦП є правом особи і призначено для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів, ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Проте законодавством передбачені певні винятки. Так, для поміщення судового рішення до Єдиного державного реєстру судових рішень необхідне його скріплення електронним цифровим підписом особи. При виконанні даної дії застосовуються сукупність програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів, а саме: перенесення інформації з паперових носіїв у електронні, використовуючи системи ЕЦП та занесення її у автоматизовану систему збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень.

Питання обов'язковості застосування ЕПЦ часто є причинами судових спорів. Останні підлягають поділу на такі категорії:

1. Поміщення судового рішення до Єдиного державного реєстру судових рішень (Рішення Ради суддів загальних судів від4 квітня 2013 року №26).

Ч. 2 ст. 2 Закону України «Про доступ до судових рішень» *усі судові рішення є відкритими та підлягають оприлюдненню в електронній формі не пізніше наступного дня після їх виготовлення і підписання*. В абз. 3 п. 1.2 Інструкції про порядок реєстрації, обліку та зберігання електронних копій судових рішень, що підлягають внесенню до Єдиного державного реєстру судових рішень, що кореспондується з положеннями Постанови Кабінету Міністрів України від 25.05.2006р. №740, *електронна копія судового рішення – складений в суді у вигляді електронних даних ідентичний судовому рішенню за документарною інформацією та реквізитами електронний документ, засвідчений електронним цифровим підписом особи, що підписала зазначене рішення, який може бути перетворений електронними засобами у візуальну форму.*

Згідно ст.12 Порядку ведення Єдиного державного реєстру судових рішень, затвердженим постановою Кабінету Міністрів від 25.05.2006р. №740, суди надсилають адміністраторові Реєстру копії всіх судових рішень *виключно в електронній формі з використанням електронного цифрового підпису, що передує видачі копії судового рішення.* З цього випливає, що електронна копія судового акту набуває офіційного статусу лише після застосування особою, що ухвалила рішення, електронного цифрового підпису. Тобто суддя, який ухвалив рішення, зобов'язаний володіти ЕЦП.

Існує ще одна проблема пов'язана з поміщенням документів до ЄДРСР. Вона полягає у недосконалому інтерфейсі програми. Харківською правозахисною групою було проведено дослідження, за результатами якого були встановлені недоліки,серед яких неможливість перегляду всіх рішень конкретного суду. Допускається пошук лише певного виду судового акту за один конкретний рік. Що виключає можливість перевірки виконання суддями покладених на них обов'язків, зокрема щодо внесення судового акту в ЄДРСР.

2. Справи щодо використання ЕЦП, які стали причиною звернення до суду (Рішення № 904/8641/13).

3. Справи щодо систематичного несвоєчасного внесення до ЄДРСР копій судових рішень; про внесення до Єдиного державного реєстру судових рішень електронної копії ухвали ; невнесення ухвал про відкриття провадження у справі по яких рішення винесено та включено до ЄДРСР тощо. Як приклад можна навести ухвали суду № 754/3157/15-к та № 813/3649/13-а.

4. Справи, які залишаються без розгляду чи руху внаслідок недотримання учасниками спору вимог законодавства про застосування ЕЦП. Це зокрема справи щодо подання позовних заяв, апеляційних скарг у електронній формі (ухвала суду № 127/6586/14-а), представництва на основі довіреностей із застосуванням ЕЦП (ухвала № 35/904/80/20133а), заяви про відмову від позовних вимог (ухвала суду № 908/1982/15-г), клопотання про розгляд справи за відсутності позивача(№ 2а-11617/10/2670), заяви та клопотання про вчинення інших процесуальних дій (ухвала № 914/2310/15).

Головним аргументом у останній категорії справ виступає те, що суд не має можливості перевірити автентичність електронних підписів, оскільки не являється суб'єктом у даному колі відносин. Це випливає із ст. 2 ЗУ «Про електронний цифровий підпис», де суб'єктами правових відносин у цій сфері виступає: підписувач; користувач; центр сертифікації ключів; акредитований центр сертифікації ключів; центральний засвідчувальний орган; засвідчувальний центр органу виконавчої влади або іншого державного органу; контролюючий орган.

Також відповідно до ст. 4 Закону України «Про електронний цифровий підпис» використання ЕЦП не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі. Таким чином, навіть за умови, що довіреність чи заява підписана електронним цифровим підписом, це не виключає її підписання в письмовій формі. Ч.1ст. 119 ЦПК передбачено, що позовна заява подається в письмовій формі. Аналогічні твердження містяться і у ч. 1 ст. 54 ГПК, ст.105 КАСУ тощо.

Уникнути цих проблем стало можливим після введення системи обміну електронними документами, передбаченого

Наказом від 07.09.2012 № 105 Про реалізацію пілотного проекту щодо обміну електронними документами між судом та учасниками судового процесу. Останній передбачає проведення обміну електронними документами між судом та учасниками судового процесу. Документи можуть бути подані користувачем до суду і надіслані йому судом в електронному вигляді лише після реєстрації в Системі, розміщеної на офіційному веб-порталі судової влади України. При реєстрації користувач надає зразок (сертифікат) ЕЦП, який буде застосовуватися під час листування з судами у Системі з використанням електронної адреси.

Підписання електронного документа ЕЦП унеможливлює внесення змін до структури документа, що є як перевагою, так і недоліком. Виключається можливість нанесення реквізитів у процесі роботи з документом, наприклад, резолюцій, грифу погодження, затвердження і направлення його до справи тощо.

Ще одним цікавим аргументом виступає твердження в ухвалі суду щодо другої виділеної категорії справ 813/3649/13-а «оскільки даний спір не належить розглядати як в порядку адміністративного судочинства так і такий не підлягає розгляду судами України, а відтак, слід відмовити у відкритті провадження у адміністративній справі». При цьому у цій ж ухвалі, суд визнав, що «електронна копія судового рішення надсилається до Реєстру суддею, який ухвалив (постановив) судове рішення та є нічим іншим, як процесуальною дією головуючого у справі судді при здійсненні ним правосуддя». Відповідно до ст. 55 Конституції України кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб. Оскарження дій чи бездіяльності судді при здійсненні ними правосуддя, які пов’язані з підготовкою, розглядом справ або іншими процесуальними діями, здійснюється шляхом подання апеляційних та касаційних скарг на рішення судді у встановленому процесуальним законом порядку, що є загальною гарантією при здійсненні судочинства. Тому згадане твердження суду у даній ухвалі є неточним: справа не підсудна адміністративним судам, але немає обмежень щодо цивільного чи господарського оскарження у порядку апеляції чи касації.

У зв'язку з тим, що в даній сфері важливу роль відіграє і людський фактор, варто звернути увагу можливість створення і рекомендації для реалізації програми адаптації персоналу до роботи з електронним цифровим підписом. У такій програмі слід передбачити можливість забезпечення безпеки носія електронного цифрового підпису, що безпосередньо пов'язано з впливом людського фактора, так як недотримання встановлених правил може призвести до значних матеріальних витратах на відновлення функціональності всієї інформаційної системи. Це пов’язано, зокрема, з тим, що єдиний недолік ЕЦП в порівнянні із звичайним підписом в тому, що не можна з такою ж впевненістю визначити, хто саме підписав документ.

Як висновок необхідно зазначити, що існує необхідність зміни законодавчого підходу щодо кола суб’єктів у сфері використання ЕЦП, забезпечення можливості перевірки судом автентичності ЕЦП на документі та удосконалення системи електронного документообігу з використанням ЕЦП в останніх. Доцільним було б також передбачити розроблення ЕЦП не для всього файлу, а для окремих фрагментів документа з метою включення можливості внесення реквізитів у процесі роботи з документом.

1. Конституція України Верховна Рада України; Конституція, Закон від 28.06.1996 № 254к/96-ВР
2. Про доступ до судових рішень Верховна Рада України; Закон від 22.12.2005 № 3262-IV
3. Про електронний цифровий підпис Верховна Рада України; Закон від 22.05.2003 № 852-IV
4. Про затвердження Інструкції про порядок виготовлення, надсилання, реєстрації, обліку та зберігання на паперових носіях та в електронному вигляді копій судових рішень, що підлягають внесенню до Єдиного державного реєстру судових рішень Наказ Державна судова адміністрація України 14.05.2008 р. N 37
5. Наказ Державної судової адміністрації України «Про реалізацію пілотного проекту щодо обміну електронними документами між судом та учасниками судового процесу» від 07 вересня 2012 року № 105
6. Порядок ведення державного реєстру судових рішень, затверджений Постановою Кабінету міністрів України від 25.05.2006р. за № 740

7. Положення про автоматизовану систему документообігу суду, Рада суддів України, рішення від 26 листопада 2010 року N 30
8. Хілінський А. Електронний цифровий підпис (у запитаннях і відповідях) / А. Хілінський // Секретарь-референт, №1,2011 [Електронний ресурс]. – Режим доступу :http://www.trainings .ua/article/2113.html
9. Богдан Бондаренко, Юлия Ращупкина Анализ работы Единого государственного реестра судебных решений, 6 травня 2009.
10. Лаба О. В. До визначення переваг електронного діловодства) /О. В. Лаба // Вісник Харківської державної академії культури. – 2012. – Вип. 38. – С. 95-101.[Електронний ресурс] Режим доступу: http://nbuv.gov.ua/j-pdf/hak_2012_38_12.pdf
11. Котлярова М. Ф. Проблемы практического применения электронной цифровой подписи в РФ на современном этапе/ М. Ф. Котлярова // Всероссийский научно-практический журнал «История, философия, экономика и право» – 2/2014.[Електронний ресурс] Режим доступу: http://ифэп.рф/2-2014/6.pdf
12. Филенко Е. Н. Проблемы использования электронной цифровой подписи / Е. Н. Филенко // «Трудовое право», 2007, N 11. [Електронний ресурс] Режим доступу: http://www.center-bereg.ru/h1601.html
13. Левшаков, С.Ф. Проблеми становлення інфраструктури електронних цифрових підписів у банківській системі України /С.Ф.Левшаков // Вісник Української академії банківської справи. – 2010. – № 2 (29). – С. 80-85.

ОКРЕМІ ПРОБЛЕМИ ВИКОРИСТАННЯ МОБІЛЬНИХ ТА ІНТЕРНЕТ-ТЕХНОЛОГІЙ У НАДАННІ КОМЕРЦІЙНИХ ПОСЛУГ

Протиняк Андрій Андрійович,
студент економічного факультету
Львівського державного університету внутрішніх справ
Сеник Володимир Васильович,
завідувач кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Рудий Тарас Володимирович,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Сьогодні Інтернет, мережеві і мобільні технології стали невід'ємною частиною ведення комерційної діяльності. Дані технології у бізнесі підтримуються:

1. Наявністю глобальних і локальних мереж фіксованого та мобільного зв'язку, а також протоколів обміну між ними.
2. Існуванням глобальної всесвітньої мережі Інтернет, створеної мільйонами Веб-серверів, що розташовані по всьому світу.
3. Стандартизацією мережевого та периферійного обладнання, а також його інтерфейсів, запитів та протоколів обміну інформацією.
4. Розвитком виробництва товарів та послуг у напрямку запровадження високих технологій.
5. Розвитком ідеології бізнесу у напрямку застосування мобільних та інтернет-технологій.
6. Наявністю споживацьких запитів на застосування інтернет-технологій.

Сьогодні для ведення комерційної діяльності використовується достатньо багато різноманітних відомих мобільних та

інтернет-сервісів. До таких, наприклад, належать WWW (World Wide Web), електронна пошта (e-mail), Skype, GSM, GPS тощо.

Як приклад широкого застосування даних технологій, окрім інтернет-магазинів, можна привести: системи бронювання залізничних та авіаквитків; технології дистанційного банківського обслуговування, відомого під поняттям інтернет-банкінг; контроль за пересуванням автотранспорту на основі супутникової системи GPS; використання GSM-контролерів під час створення і використання охоронних систем та багато інших.

Однак, застосування мобільних та інтернет-технологій у комерційній діяльності стримується багатьма факторами. Розглянемо деякі з них з точки зору споживача.

Основним стримуючим фактором під час купівлі товарів через Інтернет є те, що інтеренет-сайти можуть надати лише формальні і візуальні дані про товар (ціна, технічні характеристики, вигляд). Купуючи такі товари у реальному магазині покупець використовує і іншу інформацію, наприклад, оцінку матеріалу виробу, порівняння з подібним товаром. Окрім цього, якщо говорити про віртуальне представлення товару, то часто в інтернет-магазинах продаються товари, які реально не відповідають своєму представленню на сайті, оскільки під час фотозйомки використовувалось додаткове освітлення або товар представляється у найвигіднішому ракурсі.

Стосовно продовольчих товарів справи значно складніші, оскільки під час їх замовлення покупець повинен переконатися у багатьох споживацьких властивостях продукту. Все це призводить до того, що через Інтернет продаються стандартні продовольчі та виробничі товари, наприклад, книжки, напої відомих брендів, інші товари, купівля яких не пов’язана з певним споживацьким ризиком. Однак, слід зазначити, що в Україні існує ряд успішних інтернет-сервсів з продажу товарів, наприклад, «Rozetka» [1].

Що стосується реалізації послуг через Інтернет, то тут ситуація цілком впорядкована. Існує цілий ряд послуг, реалізація яких з використанням Інтернету достатньо відпрацьована. До таких послуг необхідно в першу чергу віднести бронювання місць у готелі [2], продаж залізничних квитків [3], замовлення екскурсійних турів [4]. Проблеми, що можуть виникнути під час

використання таких сервісів, як правило, залежать у відсутності зворотного зв'язку з постачальником послуг. Так, окремі необачні дії можуть призвести до необхідності повернення квитків.

Складні споживацькі товари, наприклад, смартфони, потребують перевірки своїх споживацьких властивостей, наприклад, швидкості роботи в Інтернеті, час реагування дисплея тощо. Оскільки у протилежному випадку їх купівля може принести споживачу не лише моральну, але і матеріальну шкоду у вигляді відсутності необхідних функціональних властивостей.

Необхідно зазначити, що існує ряд послуг, використання яких через мережу Інтернет у повному обсязі скоріш за все буде неможливим. До таких послуг слід віднести, наприклад, послуги туристичних компаній. Тут, щоб не бути розчарованим у послузі, клієнту необхідний безпосередній контакт з постачальником послуг чи його представником. З іншого боку, Інтернет, у даному випадку, необхідний для перевірки якості даної послуги. Тим не менше, спроби розвивати інтернет-технології у цьому напрямку ведуться постійно. Прикладом є корисний для споживачів сайт [5].

Окремою проблемою є низька технічна та програмна продуманість деяких сайтів.

Як стримуючі фактори у застосуванні безпосередньо мобільних інтернет-технологій, необхідно виділити:

- високі тарифи операторів мобільного зв'язку на трафік;
- відсутність покриття GSM-мережами окремих територій;
- низьку якість зв'язку та повільну роботу каналів передачі даних;
- складність самих мобільних технологій, наприклад, розуміння того, яким чином, який саме пристрій, з якою конфігурацією і операційною системою доцільніше використовувати для доступу до мережі Інтернет.

Як стримуючий потенційних споживачів фактор, який відноситься до інтернет-технологій у цілому, необхідно відзначити можливість втрати та розкриття клієнтської інформації внаслідок різноманітного мобільного та інтернет-шахрайства, а також певну організаційну та технічну слабкість захисту комп'ютерних систем постачальників товарів і послуг по відношенню до різних хакерських атак.

Вказані проблеми, які відносяться безпосередньо до мобільних інтернет-технологій, пов'язані з тим, що дана технологічна галузь переживає потужний період розвитку і в ній немає постійних технологічних та програмних рішень.

1. Интернет-супермаркет Rozetka [Электронный ресурс]. – Режим доступа: URL: www.rozetka.com.ua/
2. Bookin.com [Електронний ресурс]. – Режим доступу: URL: http://www.booking.com/
3. Tickets.ua [Електронний ресурс]. – Режим доступу: URL: http://gd.tickets.ua/
4. Час на мандри [Електронний ресурс]. – Режим доступу: URL: http://timetotravel.in.ua/
5. Сеть агентств горящих путевок [Электронный ресурс]. – Режим доступа: URL: http://www.hottour.com.ua/

ЗАХИСТ СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ АУДИТУ БЕЗПЕКИ В УМОВАХ ТРАНСФОРМАЦІЇ МВС

Руда Ольга Іванівна,
доцент кафедри економіки та економічної безпеки
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент
Протиняк Діана Андріївна,
студентка економічного факультету
Львівського державного університету внутрішніх справ

На поточний момент, коли обсяги інформації, що циркулює, обробляється та накопичується у сучасних інформаційних системах (ІС), стрімко збільшуються, питання захисту інформації стає особливо актуальним. В умовах розвитку та впровадження технології систем з відкритою архітектурою, яка вирізняється складною взаємодією ІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (мобільність) та іншими особливостями, питання захисту інформації набуває все більшої ваги.

На даний момент ще не сформовано усталеного визначення аудиту інформаційної безпеки (ІБ). У подальшому ми пропонуємо під поняттям аудиту ІБ розуміти системний процес отримання об'єктивних якісних і кількісних оцінок заходів безпеки, процесів та процедур відповідно до визначених критеріїв та показників безпеки, вимог міжнародних стандартів, чинного законодавства України, відомчих нормативно-правових актів.

Процедура аудиту ІБ дозволяє керівництву отримати об'єктивну інформацію про стан захищеності ІС. Однак, як показує практика, керівництво і особовий склад найчастіше розуміють суть цієї послуги по-різному.

Метою публікації є детальне класифікування послуг різних видів аудиту, обґрунтування особливостей та головних критеріїв раціонального вибору і застосування різних видів аудиту ІБ інформаційних систем в умовах трансформації МВС.

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

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

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

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

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

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

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

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

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

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

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

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

На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент ІС, які беруть участь у найбільш важливих процесах передавання, зберігання та оброблення інформації. Застосування аналізу рівня критичності інформаційних потоків дає можливість реалізувати систему захисту, яка відповідає принципу розумної достатності.

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

Аудит на відповідність стандартам. Суть даного виду аудиту найбільш наближена до тих формулювань, які існують у фінансовій сфері. При проведенні даного виду аудиту стан системи захисту ІС порівнюється з прийнятим абстрактним описом, який подається у міжнародних стандартах.

Організаційно-правова структура інформаційного аудиту системи ІБ у ІС формується відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: 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 управління ІБ.

Офіційний звіт, підготований у результаті проведення даного виду аудиту, включає наступну інформацію: ступінь відповідності ІС обраним стандартам; ступінь відповідності власним внутрішнім вимогам в області ІБ; кількість і категорії отриманих невідповідностей і зауважень; настанови з побудови або модифікування системи ІБ, що дозволяють привести її у

відповідність з даним стандартом; докладне посилання на основні документи, включаючи політику інформаційної безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які запроваджені у ІС.

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

Як висновок відзначимо, що при плануванні перевірки стану системи ІБ важливо не тільки точно вибрати вид аудиту, виходячи з потреб і можливостей, але і не помилитися з вибором виконавця.

1. Рудий Т.В. Захист інформаційних систем підрозділів МВС / Т.В. Рудий, Я.Ф. Кулешник, О.В. Омельяненко, О.О. Логінова / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 14 грудня 2011 р. – Львів: Львівський державний університет внутрішніх справ, 2011, с. 58-64.
2. Рудий Т.В. Управління безпекою в інформаційних системах МВС / Т.В. Рудий, Я.Ф. Кулешник, І.М. Ганич, І.В Бичинюк / Науковий вісник Львівського державного університету внутрішніх справ, №1(47), – Львів. 2011. – С. 382-392.
3. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк. – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.
4. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник, А.Т. Рудий / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. – Львів: ЛДУВС. 2010, – с. 90-97.

РОЗРОБЛЕННЯ АЛГОРИТМУ ШИФРУВАННЯ ДАНИХ SVABOM

Соколов Володимир Степанович,
магістрант кафедри програмного забезпечення
Національного університету «Львівська політехніка»
Грицюк Юрій Іванович,
професор кафедри програмного забезпечення
Національного університету «Львівська політехніка»
доктор технічних наук, професор

Вступ. На даний час симетричні алгоритми шифрування є одним з інструментів, що успішно забезпечують криптографічний захист інформації протягом тривалого періоду часу. На одному з конкурсів [2] було відзначено алгоритм «Калина» як алгоритм-прототип блокового симетричного шифрування, однак як стандарт шифрування він не був прийнятим. У зв'язку з цим залишається відкритим питання про прийняття нового стандарту шифрування для України на заміну ДСТУ ГОСТ 28147:2009.

Для підвищення криптостійкості алгоритмів потрібно використовувати нові методики, такі як ключі змінної довжини, змінна кількість раундів чи неповні (урізані) раунди [2]. Однак, оскільки для всіх наявних алгоритмів шифрування, котрі добре себе зарекомендували, прораховані всі деталі, ми не можемо змінити їх структуру з використанням нових методик без погішення криптостійкості чи інших параметрів алгоритму [1].

Отже, актуальність цієї роботи визначається розробленням нового симетричного блокового алгоритму з підвищеною криптостійкістю.

Загальна характеристика алгоритму Svabom. Алгоритм Svabom є симетричним блоковим алгоритмом з деякими особливостями роботи.

По-перше, алгоритм опрацьовує блоки вхідних даних різного розміру. Блок подається квадратною матрицею розміром $N \times N$, $\forall N \bmod 16 = 0$, тобто можливі блоки 16×16 байт, 32×32 байти, 128×128 байт та більші. На даний час найчастіше

використовують блоки розміром 256 біт, тобто 16 байт (4×4 байти). Від обраного розміру блоку значно залежить надійність алгоритму та його швидкодія, а також розмір вихідного файлу. Наприклад, якщо обрати блок 256×256 байт, тобто 65536 байт = 64 Мб, то швидкість формування матриці перестановки буде набагато більша, ніж для блоку в 256 байт, а також вихідний файл може бути більший, ніж вхідний на 64 Мб – 1 байт.

По-друге, алгоритм є гнучким в плані налаштування співвідношення надійності та швидкодії. Це реалізується за допомогою розміру складових елементів ключа BlendKey, від котрих залежить тривалість процесу формування матриці змішування даних, або за допомогою змінної кількість раундів шифрування блоку. Обидва способи дають змогу налаштовувати потрібну надійність та швидкодію алгоритму шифрування даних.

Складові ключа алгоритму Svabom. Ключ для даного алгоритму складається з шести компонент: BlockSize; WhiteData; Blendkey; FibonacciMatrix; Chmode; RoundTrans. Розглянемо детальніше кожен пункт.

BlockSize – це нульова складова ключа, котра відповідає за поділ його на блоки. В ключі це відображається цілим числом N, $\forall N \bmod 16 = 0$, тобто N = 16, 32, 48 … Саме від BlockSize залежатиме криптостійкість алгоритму та істотно залежатиме процес формування матриці перестановки. Рекомендується використовувати блоки з BlockSize не менше 128 (16 Кб).

WhiteData – це перша складова ключа, яка вона відповідає за «відбілювання даних». Тобто реалізується початкова перестановка стовпців. В ключі це відображається як N чисел від 0 до N-1, з котрих буде формуватися матриця перестановки стовпців. Цей процес не істотно впливає на криптостійкість алгоритму та швидкість шифрування.

Blendkey – це основна складова алгоритму, котра відповідає за створення матриці змішування даних. В ключі це відображатиметься набором чисел (рекомендується від 17 до 33) + дата час у форматі YY.MM.DD.HH.MM.SS, котрі відповідають за номери наборів чисел в файлі з Blendkey наборами. Номер файлу обирається залежно від дати та часу. Для кожного проміжку часу актуальним є тільки один файл. Як обиратимуться

часові проміжки та який саме файл обиратиметься на даному проміжку – визначатиме окрема служба, котра немає нічого спільного з алгоритмом. Перші числа в Blendkey обиратимуть набори чисел, що використовуватимуться для створення матриці перестановки, останнє число – це кількість чисел з останнього набору, що будуть використовуватися. Наприклад, послідовність чисел «125065237125» означає, що треба використати 125-ий та 065-ий набори повністю та ще 125 чисел з 237-ого набору. Це дає змогу значно ускладнити роботу алгоритму, оскільки для розміру блоку в 64 Кб існує $128^2! \approx 10^{61936}$ варіантів матриці перестановки. Складність алгоритму AES, (брутфорсу – перебору) становить $2^{256} \approx 10^{77}$.

FibonacciMatrix – складова алгоритму, яка відповідає за розроблення матриці Фібоначчі для отримання шифротексту. В ключі це відобразиться одним числом від 000 до 100, (рекомендується 014 та більше). Власне все буде відбуватися приблизно в такій послідовності:

1) блоки вхідних даних розміром $N \times N$ діляться на $N/16$ матриць розміром $N \times 16$;

2) з матриць розміром $N \times 16$ утворюються матриці розміром $N \times 8$ методом конкатенації байт по вертикалі;

3) матриці розміром $N \times 8$ перемножуються на матрицю Фібоначчі розміром 8×8 певного порядку (до 100);

4) знаходження залишку від ділення елементів матриць на число 65536 (2 байти);

6) розширення матриць розміром $N \times 8$ до матриць розміром $N \times 16$.

Chmode – це складова, що відповідає за підстановку. В ключі відображається одним числом від 000 до 2^{32}. На основі цього числа будуть формуватися байтові словники. Далі буде за словником відбуватися заміна даних. Процес потоковий і значно швидкий. Рекомендується вмикати для всіх задач, де шифруватимуться не текстові дані.

RoundTrans – це складова, що відповідає за кількість раундів шифрування, яка в ключі відображається набором нулів та одиниць. На кінець кожного раунду, залежно від того 0 чи 1, в поточній позиції RoundTrans матриця буде (або ні) повернена на 90^o, після чого всі описані вище дії будуть проводитися заново.

Хоч в RoundTrans можна записувати довільну кількість раундів, від 8 до 32, однак цей параметр значно впливає на швидкість шифрування.

Кожна складова алгоритму, окрім RoundTrans, залежно від складності задачі може бути вимкнена. Це вплине на швидкодію та криптографічну стійкість алгоритму. На практиці це означає, що можна відбілювати дані, множити їх на матрицю Фібоначчі та виконувати підстановку з допомогою Chmode, а можна використати матрицю змішування та множення на матрицю Фібоначчі. В обох випадках відрізнятиметься швидкість шифрування тексту та криптостійкість алгоритму. Це дає змогу алгоритму гнучко налаштовуватися на найрізноманітніші задачі, тобто такі, що потребують як швидкого шифрування, так і високого рівня складності криптоаналізу.

Розшифрування відбувається таким аналогічно, як і шифрування, однак в зворотному порядку та з незначними змінами.

Приблизна складність брутфорсу алгоритму Svabom. Ключ алгоритму складається з шести компонент. Розглянемо складність алгоритму при BlockSize = 128, тобто при розміру блоку 16 Кб. За таких умов у Whitedata буде 128 елементів, кожен з яких від 0 до 127 без повторень. Це можна записати формулою P(Whitedata) $\approx 3.8 \cdot 10^{215}$.

Наступна компонента алгоритму є Blendkey. Рекомендується від 17 до 33 параметрів. Тобто у нас буде від 16·128–127=1921 до 32·128–0=4096 елементів від 0 до 127. Це можна записати формулою P(Blendkey) $\sum_{i=1921}^{4096} 128^i$ $128^i \approx 1{,}3 \cdot 10^{8631}$. Отже, дана складова алгоритму дає змогу не перейматися за стійкість до підбору ключа методом грубої сили (брутфорс).

Наступною складовою алгоритму є компонента Fibonacci Matrix. Рекомендується використовувати від 14-ої до 100-ої степені матриці Фібоначчі. Тому P(FibonacciMatrix) = 86. Однак ця складова алгоритму так змінює байти вихідного повідомлення, що кожен байт в рядку вхідних даних впливає на кожен байт в рядку вихідного повідомлення. Причому, чим ближче байт знаходиться до лівої сторони матриці, тим більше він впливає, і, відповідно, чим ближче до правої сторони – тим менше.

Ще одною складовою є компонента Chmode. В цій складові алгоритму використовується тільки 2^{32} словників, декотрі з яких

у теорії можуть бути ідентичними, тому P(Chmode)<= 2^{32}. Дана складова алгоритму відповідає за підстановку даних, тому немає сенсу створювати надто багато словників з врахуванням того, що вони динамічно генеруються в процесі роботи алгоритму і цей процес потребує затрат процесорного часу. Взагалі для алфавіту з 128 символів можна створити 128! словників.

Наступною складовою алгоритму є компонента RoundTrans. На цьому етапі матриця повертається або не повертається на 90^o наліво та починається новий раунд алгоритму. Раундів рекомендується використовувати від 8 до 32. Кількість раундів істотно не впливає на складність брутфорсу (24 варіанти), однак поворот матриці на 90^o вліво дає змогу ускладнити криптоаналіз іншими підходами. Так відбувається ще один етап відбілювання з допомогою WhiteData.

Ще раз відбувається перестановка на етапі Blendkey. Повторно відбувається множення на матрицю Фібоначчі, однак якщо в попередньому раундів кожен елемент в рядку вхідного тексту впливав на значення кожного елемента в рядку вихідного тексту, то після повороту кожні рядки стали стовпцями, а стовпці – рядками, тому вже кожен елемент стовпця вхідних даних впливає на кожен елемент стовпця вихідних даних. Таким чином для того, аби кожен байт блоку вхідних даних впливав на кожен байт блоку вихідних даних, потрібно аби відбувся поворот тільки один раз, а якщо таких поворотів буде 4, то кожен елемент вхідної інформації у блоці буде майже рівномірно впливати на елементи вихідної інформації у блоці.

Також у новому раундів відбудеться знов заміна даних з допомогою динамічно згенерованих словників. Так відбудеться багатокрокова заміна даних і, якби дані не змінювалися на етапі множення на матриці Фібоначчі, то можна було б говорити про недоцільність повторного використання динамічно згенерованих словників.

Загальна криптографічна стійкість алгоритму Svabom методом грубої сили становить:

P(Svabom) = P(Whitedata)×P(Blendkey)×P(Chmode) ≈

≈ $3.8 \cdot 10^{215} \times 1.3 \cdot 10^{8621} \times 2^{32} \approx$ **$2.1 \cdot 10^{8856}$**

Отже, алгоритм Svabom з розміром блоку 16 Кб істотно складніший при брутфорсі, ніж більшість відомих досі широкому загалу алгоритмів. На 97.4% складність алгоритму Svabom забезпечується за допомогою матриці перестановок, яка формується на етапі оброблення Blendkey.

Висновки: Отже, алгоритм Svabom є новим криптостійким алгоритмом, який шифрує дані блоками більшими, ніж прийнято використовувати в симетричних алгоритмах. Розмір блоку може бути змінений залежно від постановки задачі. Це вплине на межі складності криптоаналізу.

Даний алгоритм складається з 6 складових BlockSize, WhiteData, Blendkey, FibonacciMatrix, Chmode, RoundTrans, кожна з яких немає особливої складності в реалізації, однак всі разом вони доповнюють одна одну і разом виходить доволі складний для криптоаналізу алгоритм.

Для брутфорсу даного алгоритму потрібно перебрати $2.1 \cdot 10^{8856}$ варіантів за умови, що використано ключ з рекомендованими параметрами. Складність брутфорсу можна дещо збільшити, однак, враховуючи сучасний розвиток комп'ютерної техніки, це не є доцільним. Інші методи криптоаналізу даного алгоритму поки що не досліджені.

1. Білан С.М. Підвищення криптостійкості та швидкодії алгоритму Blowfish у каналах передачі даних / С.М. Білан, І.М. Шварц // Реєстрація, зберігання і обробка даних : зб. наук. праць. – 2005. – Т. 7, № 1. – С. 97-102.
2. Олешко О.І. Методи прискореного криптоаналізу БСШ на основі аналізу показників стійкості зменшених моделей прототипів : автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.21 – системи захисту інформації / О.І. Олешко; ХНУРЕ. – Харків, 2010. – 24 с.
3. Казимиров О.В. Методи та засоби генерації нелінійних вузлів заміни для симетричних криптоалгоритмів : автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.21 – системи захисту інформації / О.В. Казимиров; ХНУРЕ. – Харків, 2010. – 20 с.

КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

Тележенко Богдан Олександрович,
студент Сумської філії Харківського національного університету внутрішніх справ
Чередниченко Віталій Борисович,
старший викладач кафедри соціально-економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ

Передача службової інформації по каналах зв'язку супроводжується її захистом, причому тим потужнішим, чим більшу шкоду може принести її перехоплення. Особливої актуальності набуває проблема конфіденційності при проведенні спецоперацій, при бойових зіткненнях, таємних акціях, тощо. Зважаючи на зростаючі можливості злому кодів – ефективним засобом слід вважати маскування самого факту передачі певного повідомлення.

Стеганографічні методи (*Steganographia,* «тайнопис») направлені на збереження в таємниці самого факту передачі прихованої інформації. При цьому корисні дані непомітно «вбудовуються» у інше повідомлення – фотографію, аудіо- файл, текст, тощо.

Криптографічні методи шифрують інформацію, але не приховують факт передачі захищених даних, тому наявність зашифрованого повідомлення викликає до нього негайний інтерес.

Часто стеганографію застосовують одночасно з методами криптографії, що підвищує ступінь захисту повідомлення.

Елементами стеганосистеми є стеганоконтейнер, стеганоканал, стеганоключ.

Контейнер – будь-яка інформація, що використовується для приховування таємного повідомлення. Заповнений контейнер (стегоконтейнер) містить таємне послання, а у порожньому вона відсутня.

Стеганографічний канал (стегоканал) – слугує для передачі стегоконтейнера.

Стеганоключ – секретний ключ, потрібний для приховування стегоконтейнера. Ключі в стегосистемах бувають двох типів: секретні та відкриті [1].

Комп'ютерна стеганографія є найбільшою гілкою загальної стеганографії та бурхливо розвивається в останні роки. Вона використовує комп'ютерні технічні платформи, програмні засоби, а також канали електронного зв'язку. Її звичайно поділяють на цифрову, лінгвістичну та квантову.

Цифрова стеганографія – це спосіб приховування даних, коли необхідна інформація вбудовується у мультимедійні та інші цифрові файли, а внесені нею зміни знаходяться нижче типового порога чутливості людини. Приховування даних у *зображеннях* здійснюється наступними методами: 1) заміни найменш значущого біта, 2) псевдовипадкового інтервалу, 3) псевдовипадкової перестановки, 4) блокового приховування, 5) заміни палітри, 6) квантування зображення, 7) вбудовування в канал синього кольору зображення, яке має {R,G,B} кодування.

Приховування даних *в частотній області зображення* створюється методами: 1) заміни величин коефіцієнтів дискретно косинусного перетворення (ДКП), 2) вбудовування цифрового водяного знаку, 3) вбудовування даних в ДКП коефіцієнти. Приховування даних в *аудіосигналах* здійснюється такими методами: 1) кодування найменш значущих біт, 2) фазовое кодування, 3) розширення спектру, 4) приховування з використанням ехо-сигналу [2].

Лінгвістична стеганографія – це методи приховування інформації у текстовому файлі. Її синтаксичні методи полягають у зміні пунктуації, стилю або структури тексту. Семантичні методи використовують таблицю синонімів. Методи довільного інтервалу використовують: заміни інтервалу між реченнями, зміни кількості пробілів у кінці текстових рядків, зміни кількості пропусків між словами вирівняного за шириною тексту. Одним з лінгвістичних методів є умовне письмо. До нього відносять: жаргонний код, геометричну систему, нульовий шифр і шифр «решітка». Жаргонний код передбачає використання не привертаючих увагу слів, які мають зовсім інше реальне значення,

а текст складається так, щоб виглядати максимально логічно та правдоподібно. Жаргонні коди включають в себе таємну термінологію або звичайну розмову, яка передає особливий зміст внаслідок того, що ключ відомий тільки відправнику та одержувачу. При застосуванні геометричної системи мають значення слова, розташовані на сторінці в певних місцях або в точках перетину геометричної фігури заданого розміру. Нульовий шифр приховує повідомлення відповідно до певного, заздалегідь підготовленого, набору правил (наприклад, «прочитайте кожне п'яте слово» або «врахуйте третю букву в кожному слові»). Шифр «решітка» застосовує шаблон, який використовується для приховування повідомлення-контейнера. Слова, які з'являються в отворах шаблону, є прихованим повідомленням. Іншу категорію лінгвістичних методів становлять семаграми – таємні повідомлення, в яких значеннями шифру є будь-які символи (крім літер і цифр). Наприклад, ці повідомлення можуть бути передані в малюнку, що містить крапки і тире для читання за кодом Морзе, або обумовлені зміни у дизайні веб-сайту, ледь помітні зміни в розмірі або інтервалі шрифту, додавання додаткових пробілів, різних завитків у буквах тексту, тощо [1].

Квантова стеганографія є синтезом квантової фізики та класичної теорії інформації, вона порівняно молода та перебуває у стані розвитку. Можна сказати, що квантова стенографія є значно стійкішою за інші методи, насамперед тим, що перехопити і декодувати конфіденційну інформацію, закодовану такими методами, теоретично неможливо (теоретико-інформаційна стійкість) [1].

Використання методів комп’ютерної стеганографії значно підвищує ступінь захисту конфіденційної інформації, яка передається по каналах зв’язку, від несанкціонованого доступу або спотворення.

---

1. Стасюк О.І., Гнатюк С.О та ін. Сучасні стеганографічні методи захисту інформації // Захист інформації. К. НАУ. – 2011. – №1. С. 1-7.
2. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с. (Укр. мов.)

ОКРЕМІ ТЕРМІНОЛОГІЧНІ ПРОБЛЕМИ, ЩО ВИНИКАЮТЬ В ПРОЦЕСІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Хахановський Валерій Георгійович,
професор кафедри інформаційних технологій
Національної академії внутрішніх справ,
доктор юридичних наук, професор

Проблемам інформаційного забезпечення правоохоронної діяльності було присвячено значна кількість робіт, серед яких слід відзначити праці таких вчених, як В. П. Бахін, Р. С. Бєлкін, В. В. Бірюков, В. Д. Гавловський, В. І. Галаган, В. М. Глушков, В. Г. Гончаренко, А. В. Іщенко, Р. А. Калюжний, Н. І. Клименко, В. Є. Коновалова, І. І. Котюк, В. С. Кузьмічов, В. К. Лисиченко, В. Г. Лукашевич, Є. Д. Лук'янчиков, Ю. О. Мазниченко, Д. Й. Никифорчук, В. О. Образцов, Ю. Ю. Орлов, М. А. Погорецький, М. С. Полевой, О. Р. Росинська, М. В. Салтевський, М. Я. Сегай, М. О. Селіванов, В. М. Смаглюк, В. В. Тіщенко, М. Я. Швець, В. Ю. Шепітько, М. Є. Шумило та інші.

Однією з нагальних проблем інформаційного забезпечення є термінологія, яка використовується при розгляді цього питання. Нажаль, часто визначення, поняття та терміни використовуються на власний розсуд авторів, без урахування чинної нормативно-правової бази тощо.

До згадуваних понять слід віднести, зокрема такі: «інформаційна система», «інформаційна підсистема», «інформаційно-аналітична система», «банк даних», «база даних». Так, Інтегровану інформаційно-пошукову систему ОВС України нерідко продовжують називати Армором. Розглядаючи у різні часи ці поняття, ми зазначали, що автоматизація аналітичної роботи на сучасному етапі розвитку інформаційних технологій передбачає використання інтелектуальних програмних систем, серед яких найбільш розповсюдженими є експертні системи [1]; [2]; [3].

Крім того, часто використовується поняття «автоматизоване робоче місце (АРМ). Останнім часом їх іноді називають комп'ютеризованими робочими місцями (КРМ), аби підкреслити домінуюче значення саме комп'ютера. На наш погляд, КРМ є поняттям більш вузьким, ніж АРМ. Комп'ютеризованими робочими місцями може бути оснащений, зокрема, комп'ютерний клас. Крім того, абревіатура АРМ усталена та, як правило, не викликає різночитань, тоді як «КРМ» може трактуватися зовсім інакше.

Останнім часом в правоохоронних органах розроблено та застосовується низка автоматизованих робочих місць: АРМи слідчого, експерта-криміналіста, оперативного працівника, тощо. Але здебільшого вони являють собою автоматизовані інформаційно-довідкові системи.

З нашого погляду, повноцінний АРМ, зокрема, слідчого має забезпечувати такі можливості:

- реєстрацію та облік кримінальних правопорушень;
- облік рішень у кримінальних справах, рішень щодо осіб, які проходять у справах, слідчих доручень;
- контроль термінів виконання рішень, слідчих доручень;
- контроль термінів розслідування;
- ведення довідників працівників, кримінальних проваджень;
- підготовку процесуальних документів;
- підготовку статистичних довідок роботи слідчого підрозділу;
- пошук інформації у базах даних;
- захист інформації від несанкціонованого доступу [4]; [5].

Отже, належно організоване автоматизоване робоче місце може бути суттєвим чинником підвищення ефективності інформаційного забезпечення процесу розслідування. Разом з тим, на наш погляд, АРМ не може бути відокремленим від криміногічних, криміналістичних, оперативних та інших обліків правоохоронних органів. Тобто АРМ слідчого має бути підключеним до корпоративної мережі ОВС України та використовуватися у комплексі із застосуванням новітніх досягнень у сфері високих технологій: цифрова фотографія, цифровий звуко- та відеозапис, геоінформаційні системи, мобільний зв'язок та сучасні GPS-технології тощо. При цьому разом із отриманням інформації із

спеціалізованих обліків при розкритті та розслідуванні злочинів доцільно використовувати інформацію з глобальної мережі Інтернет. Практика окремих підрозділів ОВС свідчить, що досить часто порівняння інформації із цих, на перший погляд, несумісних джерел, надіє нову інформацію про злочинну подію.

1. Хахановський В. Г. Термінологічні та організаційні аспекти створення інформаційно-аналітичної системи ОВС України / В. Г. Хахановський, В. М. Смаглюк // Правова інформатика. – 2006. – № 1 (9). – С. 42–44.
2. Задорожній Ю. О. Інформації багато не буває / Ю. О. Задорожній, В. Г. Хахановський // Бюлетень з обміну досвідом роботи. – № 178. – 2009. – С. 19–42.
3. Хахановський В. Г. Автоматизація інформаційно-аналітичної роботи: досвід зарубіжних та вітчизняних правоохоронних органів / В. Г. Хахановський // Право і суспільство. – 2011. – № 2. – С. 27–29.
4. Хахановський В. Г. Перспективи використання АРМ слідчого / В. Г. Хахановський // Бюлетень з обміну досвідом роботи. – № 179. – 2009. – С. 74–82.
5. Хахановський В. Г. Проблеми теорії і практики криміналістичної інформатики, монографія, – К. : Вид.Дім «Аванпост-Прим», 2010. – 382 с.

СУЧАСНІ РЕАЛІЇ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ДІЯЛЬНОСТІ ЮРИДИЧНОЇ ОСОБИ

Хитра Олександра Леонтіївна,
доцент кафедри адміністративного права та адміністративного процесу
Львівського державного університету внутрішніх справ,
кандидат юридичних наук

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

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

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

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

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

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

- розголошення (зайва балакучість співробітників) – 32%;
- несанкціонований доступ шляхом підкупу і схиляння до співробітництва з боку конкурентів і злочинних угруповань – 24%;

- відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14%;
- традиційний обмін виробничим досвідом – 12%;
- безконтрольне використання інформаційних систем – 10%;
- наявність передумов виникнення серед співробітників конфліктних ситуацій – 8% [1].

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

Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать:

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

Неформальними каналами поширення інформації є:

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

Як правило, причиною розголошення конфіденційної інформації є:

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

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

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

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

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

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

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

- недостатнє знання працівниками підприємства правил захисту комерційної таємниці і нерозуміння (або непорозуміння) необхідності їх ретельного дотримання;
- використання не атестованих технічних засобів обробки конфіденційної інформації;
- слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та інженерно-технічними заходами;

- плинність кадрів, у тому числі які володіють інформацією, що становить комерційну таємницю.

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

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

До таких способів відносяться:

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

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

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

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

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

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

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

---

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

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РОБОТІ СИЛОВИХ СТРУКТУР УКРАЇНИ

Цибуляк Богдан Зеновійович,
професор кафедри електромеханіки та електроніки,
Національної академії сухопутних військ імені гетьмана
Петра Сагайдачного,
кандидат фізико-математичних наук, доцент

Україна сьогодні знаходиться у складній ситуації, оскільки ще не вийшовши з економічної кризи доводиться вирішувати ряд складних задач: проведення антитерористичної операції на Сході нашої держави, запровадження системних політичних, економічних, соціальних реформ, а також реформи в системі цивільної та військової освіти тощо. Особливе місце у цьому переліку займає питання якнайшвидшого вирішення питання збройного протистояння на східних рубежах країни. Понад річний досвід проведення АТО показує, що перемогу отримає той, у кого буде найтехнологічніше озброєння, високий рівень підготовки бійців Збройних сил України, національної гвардії, добровольчих батальйонів. Особливе місце при цьому виділяється питанням інтеграції й взаємодії різних підрозділів, тилових служб, медичному забезпечення та ін. Вирішенню цієї задачі суттєво може посприяти впровадження та розвиток інформаційних технологій у силових структурах держави.

У сучасних умовах збройна боротьба ведеться із застосуванням високоточної зброї, високоефективних засобів розвідки й ураження, навігації і зв'язку, з різким збільшенням розмаху і швидкоплинності операцій, інформаційного навантаження органів управління, істотним підвищенням ролі інформаційної складової в процесах управління, крім того, набуває особливої актуальності проблема підвищення ефективності управління військами (силами) і на передній план висуваються оперативність і якість управління.

Комплексне вирішення таких різнопланових, проте взаємопов'язаних задач можливе не лише через створення баз даних

окремих галузей, а й побудова Єдиної автоматизованої системи управління, яка здатна проводити аналіз, обробку навіть різнопланових даних, розв'язувати питання логістики, планування, прогнозування, а також інтегруватися із сучасними потужними системами підтримки прийняття рішень [1].

Аналіз етапів використання інформаційних технологій у збройній боротьбі, за досвідом передових країн світу, свідчить про постійне зростання впливу інформаційного фактора на хід і результат воєнних дій. Характерними з цієї точки зору є такі фактори:

- постійне зростання кількості засобів обчислювальної техніки, задіяної на етапах планування операцій і під час прийняття управлінських рішень у ході операцій;
- подальша мініатюризація обчислювальних систем, їх використання практично в усіх зразках озброєння та бойової техніки, аж до особистої зброї та спорядження особового складу;
- поступова інтеграція на основі глобальних інформаційних технологій систем розвідки, управління та ураження в єдиний контур, що охоплює угруповання від підрозділу (одиниці бойової техніки) до вищого командування;
- поява перших зразків так званої керованої зброї – якісно нових зразків високоточної зброї, заснованої на використанні інформаційних технологій, що спільно з системами розвідки й управління дозволяє знищити будь-який об'єкт у будь-який точці планети;
- формування концепції інформаційних (інформаційно-ударних) операцій і перші спроби її реалізації;
- сприйняття інформаційної інфраструктури противника як об'єкта цілеспрямованого впливу (ураження або використання у власних інтересах);
- використання глобальних інформаційних ресурсів для інформаційної підтримки воєнних дій;
- проведення інформаційних операцій традиційними та зовсім новими засобами – зброєю на нових фізичних принципах (електромагнітною, психотропною, геофізичною), засобами програмно-математичного впливу;

- зростання ролі імітаційного моделювання під час планування операцій та у процесі ведення бойових дій; подальша інтеграція засобів штучного інтелекту в інформаційні системи воєнного призначення.

Україна зараз має шанс здійснити революційний прорив у модернізації військової техніки та озброєння, підвищення рівня кожного бійця Збройних сил України, національної гвардії та командування згідно сучасних світових стандартів. Проте для впровадження інформаційних технологій та систем підтримки прийняття рішень у силові відомства України потрібно першочергове вирішення ряду проблемних питань:

- розробка та вдосконалення існуючої нормативно-правової бази у збройних силах щодо створення, модернізації та функціонування інформаційних ресурсів і продуктів;
- створення інформаційно-аналітичних органів, що дозволяли б провести інтеграцію різних структур та підрозділів Збройних сил України;
- розробка єдиної системи стандартів та сертифікатів щодо програмного і апаратного забезпечення, засобів зв'язку та систем кодування інформації у Збройних силах України;
- розбудова інтегрованого банку даних як елемента загальнодержавної інформаційної структури із необхідними засадами доступу, зберігання та резервного копіювання;
- необхідність підготовки кваліфікованих фахівців для роботи в сучасних інформаційно-аналітичних системах;
- недостатність фінансування для впровадження інформаційних технологій у силові відомства України;
- відсутність чіткого плану та комплексного підходу в організації досліджень щодо вирішення проблем створення системи інформаційного забезпечення Збройних сил України.

Саме вирішення останнього з переліку питань дало би відповідь на більшість існуючих проблем і суперечностей щодо побудови інформаційного суспільства країни в цілому. Цьому в значній мірі може посприяти аналіз досвіду таких розвинених країн, як США, ЄС, Японія [2]. Проте економіки цих країн володіють вільними засобами для підтримки процесів інформатизації і розвитку інформаційно-комунікативної структури, існують державні стратегії і програми щодо побудови в них

інформаційного суспільства – в Україні всього цього практично поки що не існує. Проте варто відзначити високий рівень системи загальної освіти, не повністю втрачений науковий потенціал у сфері техніки, цікаві теоретичні розробки світового рівня в галузі інформатики. Розвиток вітчизняних телекомунікацій всіх видів відбувається випереджаючими темпами у порівнянні з іншими сферами економічної діяльності, що дозволяє розраховувати на успішне формування інфраструктури інформаційних і комунікаційних послуг.

Крім того, рік військових дій на Донбасі не тільки вивів українську армію з летаргічного сну, але і дав поштовх до розвитку високих оборонних технологій. Вітчизняні виробники активно зайнялись проектуванням розробкою та виготовленням широкого асортименту артилерійського озброєння, засобів зв'язку, автоматизованого управління, боєприпасів, безпілотних розвідувальних літальних апаратів. Але головним напрямком стали інтелектуальні новації, які, в першу чергу, покликані зберегти життя українським військовим.

Сучасні війни – це війни високих технологій, стверджують експерти. У нашої країни з'явився реальний шанс зайняти лідируючі позиції в даному напрямку. Доводять це нові розробки українських підприємств, що представлялись на XII Міжнародній спеціалізованій виставці «Зброя і безпека – 2015», яка цього року виявилась наймасштабнішою за усі 11 років її існування.

Одним із прикладів, який викликав великий інтерес з боку Міністерства оборони, ЗСУ і Національної гвардії є розроблений бойовий модуль «Десна» [3], оснащений принципово новою системою наведення, стабілізації та управління озброєнням. Модуль, що встановлюється на легкоброньовану техніку (типу БМП і БТР, катери і стаціонарні вогневі точки). Особливістю даної розробки є поява у ньому інтелектуальної складової, чого ніколи не було в існуючих рішеннях. Однією з українських компаній було створено універсальне програмне забезпечення та електроніку для нового модуля, які дозволяють вести бій, управляти вогнем з укриття і одночасно з декількох точок.

Універсальність системи управління модулем полягає в тому, що її функціонал можна постійно вдосконалювати, додаючи нові властивості відповідно до потреб армії. У

перспективі система дозволить обмінюватися даними про ведення бою як в підрозділах, так і в масштабі всієї армії.

Завдяки цьому суттєво зріс рівень безпеки обслуговуючого персоналу. У вежі без людини, як у аналогічних розробках типу «Парус», щоб зробити перезарядку, бійцю потрібно вийти на броню – є вірогідність його ураження. Тут же не потрібно цього робити. Якщо закінчиться боєкомплект, можна заряджати його зсередини, у тому числі, якщо сталася осічка.

Бойовий модуль призначений для ураження броньованих цілей, вогневих точок, живої сили противника і стрільби по повітряних цілях (типу «завислий вертоліт»). Новація забезпечує спостереження за навколишньою місцевістю, надводною і береговою обстановкою у денних і нічних умовах, автосупровід цілі, вимір кутових координат і дальності вибраної цілі для ураження. Крім того, система проста в управлінні і не вимагає спеціальних навичок від солдатів. Пульт управління в експлуатації нагадує звичайний ігровий джойстик. Кожна кнопка на пульті відповідає вибраній зброї. На монітор виводиться інформація про боєкомплект, кількість відстріляних снарядів і залишок боєкомплекту.

Тому розроблення нової концепції та побудованої на її основі комплексної програми інформатизації силових структур України, які, з одного боку, мають відповідати реаліям сьогодення, а з іншого – відображати стратегічні напрямки впровадження інформаційних технологій у збройну боротьбу, сформульовані на основі загальносвітових тенденцій є на сьогодні пріоритетним напрямком розвитку України.

1. Пермяков О.Ю., Солонніков В.Г., Прібилєв Ю.Б. та ін. Використання інформаційних технологій та застосування космічних систем в інтересах військ (сил): підручник. – К. : НУОУ ім. Івана Черняховського, 2014. – 208 с.
2. Пожуєв В.І. Особливості переходу україни до інформаційного суспільства // Гуманітарний вісник ЗДІА. – 2012, № 50. – С. 5-20.
3. Інформаційні технології на службі в армії / Електронний ресурс. http://www.ukrinform.ua/rubric-other_news/1889046-informatsiyni_tehnologiii_na_slugbi_v_armiii_2099730.html

ДЕЯКІ ПИТАННЯ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Чередниченко Віталій Борисович,
старший викладач кафедри соціально–економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ

Використання інформаційно-комунікаційних технологій вимагає застосування потужних засобів інформаційної безпеки при передачі документів по каналах зв'язку. Відомо, що найбільш надійним засобом захисту даних при мережевому обміні є електронний цифровий підпис (ЕЦП). Недосконалість захисту даних може нанести непоправної шкоди. Як негативний приклад можна навести факт розголошення в Інтернеті персональних даних про особовий склад бойової частини Національної гвардії МВС.

У даній роботі розглядаються деякі проблеми застосування цифрового підпису в Україні та напрямки їх подолання з метою гармонізації з вимогами Європейського союзу.

Використання ЕЦП внормовано документами ООН та стандартами Євросоюзу [1]. В Україні також було створено законодавчу базу ЕЦП [2]. Ця галузь пройшла етап становлення та перебуває у стані активного розвитку. Так, на 1.01.2015 р. в Україні функціонує 18 акредитованих та 7 зареєстрованих центрів сертифікації ключів (ЦСК). За даними Центрального засвідчувального органу (ЦЗО) Міністерства юстиції України акредитованими центрами сертифікації протягом 2014 р. сформовано 3,3 млн. сертифікатів відкритих ключів, та надано 38, 7 млн. послуг фіксування часу, що набагато більше за попередній рік [3].

Як позитивний приклад, можна навести впровадження Державною фіскальною службою (ДФС) України сервісу для підприємців «Електронний кабінет платника податків», який впроваджено з 01.01.2014 р. Вже з 1 січня 2015 року податкові накладні складаються виключно в електронній формі та підлягають обов'язковій реєстрації в Єдиному реєстрі податкових накладних ДФС.

Національна Система ЕЦП поки відстає від світового рівня розвитку (за деякими оцінками на 8 – 10 років [4]. Так, європейська бізнес-модель ЕЦП реалізує три види кваліфікованих підписів, вона є кваліфікованою інфраструктурою відкритих ключів (Qualified public key infrastructure, QPKI). Недолік прийнятої в Україні інфра-структури PKI – реалізація тільки одного, найпростішого різновиду підпису [5].

Для часткового подолання цієї проблеми Акредитований центр сертифікації ключів ДФС з 1.01.2014 р. перейшов на одночасне використання двох посилених сертифікатів ключів ЕЦП (згідно наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 р. №739 «Про затвердження Вимог до форматів криптографічних повідомлень»).

Ще одним недоліком НС ЕЦП є невизначеність механізмів внутрішньої крос-сертифікації ключів різних Центрів Сертифікації. В Україні згідно ДСТУ 4145 + ГОСТ 34.311 реалізований найпростіший неінтероперабельний варіант ЕЦП з єдиним комплектом підписів, що не допускає контрпідписи. У результаті клієнти вимушені використовувати ключі розрізнених систем ЕЦП, що стримує розвиток процесів електронної взаємодії [5].

Також НС ЕЦП позбавлена зовнішньої інтероперабельності зважаючи на негармонізований з нормативами Євросоюзу алгоритм підписання, який не забезпечує взаємодію з міжнародно визнаними криптографічними алгоритмами. НС ЕЦП також не готова до визнання сертифікатів ключів, виданих за межами України, тобто нездатна до зовнішньої крос-сертифікації з будь-якою державою [6].

Слід вказати на існуючі проблеми процесу акредитації центрів сертифікації ключів (ЦСК). Перевірці експертною комісією ЦЗО підлягає програмно – технічний комплекс (ПТК) і його компоненти та компетентність персоналу ЦСК, але не оцінюються функціональність і результативність ПТК, тобто кінцевий результат. Також в Україні порушено принцип незалежності експертів – оцінювачів, оскільки де-факто технічний нагляд проводить контролюючий орган. Вкрай негативним є використання суб'єктивного критерію «позитивних експертних висновків», який неможливо виміряти або описати. У

Євросоюзі така процедура оцінки відповідності максимально формалізована і виконується он-лайн по Інтернету. Для довіри іноземних партнерів Центральному засвідчувальному органу України необхідно розробити і впровадити он-лайн методику акредитації ЦСК, можливо, з використанням розробленого в Україні тестового стенду [7].

Також експерти виділяють ряд загроз, що виникають при багаторічному зберіганні електронних документів. До таких загроз можна віднести: зміну технологій і стандартів ЕЦП; відсутність гарантій доступності сертифіката ключа в довгостроковій перспективі; зміну програмно-апаратних платформ кожні 2-3 роки; компрометацію секретного ключа або технологій ЕЦП. Наслідок – відсутність гарантії того, що через декілька років можна довести юридичну правомочність електронного документа через неможливості використання старих засобів перевірки ЕЦП [6].

Велика розповсюдженість мобільних пристроїв (смартфони, планшетні ПК, тощо) вимагає розробки та унормування процедур використання таких пристроїв користувачами ЕЦП. Бажано стандартизувати наступні процедури:

а) Локальне підписання, при якому підпис створюється з використанням ключа, що зберігається на мобільному пристрої.

б) Дистанційне підписання, при якому підпис створюється з використанням ключа, який зберігається на віддаленому сервері.

в) Процедури перевірки ЕЦП з використанням мобільного пристрою [8].

Держспецзв'язку у 2014 р. прийнято два нових національних стандарти криптографічного захисту інформації. Один з них – ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування», вводиться в дію 1 квітня 2015 року. Другий – ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». Введення в дію нових національних стандартів дозволить більш надійно захищати системи, засоби і протоколи криптографічного перетворення інформації, що розробляються в Україні, у тому числі у сфері електронного цифрового підпису. Це відповідає вимогам Європейського Союзу, а нові криптографічні алгоритми підтримують довжину ключа від 128 до 512 бітів, що відповідає світовому рівню.

Висновок. Зважаючи на вищевикладене можна вважати, що основними задачами впровадження в Україні надійних механізмів довіри в НС ЕЦП є: гармонізація національних процедур ЕЦП з міжнародними стандартами, запровадження крос-сертифікаційних механізмів у політику підпису, реалізація прозорої он-лайн процедури акредитації ЦСК, тощо.

Можна стверджувати, що застосування ЕЦП для захисту службової інформації при її передачі по каналах зв'язку має перспективи у системі МВС України.

1. Чередниченко, В. Електронний цифровий підпис – міжнародні правові аспекти [Текст] / В.Б.Чередниченко // Електроніка та системи управління, Київський національний авіаційний університет. – 2008. – №3(17). – С. 84-87.
2. Чередниченко, В. Електронний цифровий підпис у правовому полі України [Текст] / В. Б. Чередниченко // Системи обробки інформації. – 2009. – № 7(79). – С. 123-124. [Харківський університет повітряних сил ім. І.Кожедуба]. – ISBN 1681-7710.
3. Кількість сформованих сертифікатів відкритих ключів та послуг фіксування часу в Україні за 2014 рік. [Електронний ресурс] Режим доступу: http://czo.gov.ua/news.
4. Клімушин П.С. Механізми забезпечення довіри в національній системі електронних цифрових підписів [Текст] // Теорія та практика державного управління. зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2013. – Вип. 2 (41). с.51-58.
5. Кузнецов О. О. Захист інформації в інформаційних системах [Текст] : навч. посіб. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король ; Харк. нац. екон. ун-т. – Х. : Вид-во ХНЕУ, 2011. – 512 с.
6. Горбенко Ю. І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика [Текст] : монографія / Ю. І. Горбенко, І. Д. Горбенко // Харк. нац. ун-т радіоелектрон., Інт. інформ. технологій. – Х. : Форт, 2010. – 593с.
7. Мелащенко А.О. Национальная система электронных цифровых подписей как открытая система [Текст] / А. О. Мелащенко, О. Л. Перевозчикова // Кибернетика и системный анализ, изд. Ин-т кибернетики НАНУ. – 2011. – № 5. – С. 180-188
8. Сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі / Ю. І. Горбенко, К. В. Ісірова // Теоретичні та прикладні аспекти побудови програмних систем TAAPSD'2014: матеріали XI Міжнародної наукової конференції, м. Київ, 15-17 грудня 2014 р. / – К. «Авангард», – 2014. с.75-79.

ДОСВІД США В ГАЛУЗІ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Чистоклетов Леонтій Григорович,
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, професор

Розкриваючи питання щодо інформаційно-правового забезпечення безпеки суб'єктів господарювання, не можна обминути проблематичність існування на сьогодення законодавства України з питань забезпечення національної безпеки, яке є у значній мірі застарілим, а закладені у ньому норми щодо взаємодії та координації органів державної влади і силових структур як у мирний час, так і в кризові періоди, не враховуючи особливості нового типу агресії, у ході якої широко використовується не лише традиційні військові операції, а й різноманітні невоєнні сили та засоби боротьби. Крім того, правові акти у цій сфері містять низку неузгодженостей, підходи до визначення певних термінів мають бути переглянутими, потребують запровадження сучасні механізми управління загрозами національної безпеки [1].

Зважуючи також на сьогоднішні події, пов'язані з безпекою життєдіяльності в світі, а саме з терористичними актами у Франції в листопаді 2015 року, директор Центру досліджень тероризму з Collegium Civitas Кшиштоф Лідель створення польської доктрини інформаційної безпеки вважає підтвердженням серйозності намірів Варшави протистояти інформаційним загрозам. За його словами, до створення такого документу польську владу підштовхнули події в Україні. Як зазначає експерт: «Я думаю, що конфлікт в Україні дуже добре показує те, як виглядає інформаційна боротьба в контексті пропагандистської та психологічної боротьби, тому що з самого початку цей конфлікт в Україні був дуже старанно підготований Росією» [2].

Таким чином, враховуючи проблематику створення та розвитку в Україні інформаційно–правового забезпечення безпеки суб'єктів господарювання, яка є складовою національної

безпеки, цілком логічно звертатися до відповідного позитивного зарубіжного досвіду. Зокрема, значний інтерес становить досвід США, які мають найбільш детально розроблене законодавство в царині регулювання приватного підприємництва і є одним з лідерів у сфері недержавної правоохоронної діяльності.

Питання, що мають відношення до проблеми вивчення досвіду США в сфері інформаційно–правового забезпечення безпеки суб'єктів господарювання, доволі широко висвітлені в літературі. Проте в українській юридичній науці ми не знайшли спроб узагальнення цього досвіду, та ще й в аспекті виявлення тих його складових, які становлять найбільший інтерес з погляду потреб вітчизняної теорії та практики її забезпечення безпеки суб'єктів господарювання. Звідси актуальність даної розвідки.

Огляд досвіду США в сфері інформаційно–правового забезпечення безпеки суб'єктів господарювання розпочнемо з виділення таких моментів:

- відсутність федерального закону про приватну охоронно-розшукову діяльність зумовила істотні розбіжності в її правовому регулюванні на рівні окремих штатів [3, с. 274];
- широкого розвитку отримали програми взаємодії поліції з недержавною системою безпеки. Уже в 1999 році в країні налічувалося понад 600 таких програм [4]. Про їх ефективність свідчить, зокрема, те, що, якщо в 1991 році відбулось 9381 банківське пограбування, то у 2011 році – 5014, а відсоток втрат від злодійства та інших злочинів у торгівлі зменшився: від 1,79 % в 1991 році до 1,41 % у 2012 році [5];
- на ЦРУ покладений обов'язок захищати інтереси й забезпечувати безпеку американських корпорацій за кордоном;
- від початку 1990-х років Державний департамент і сотні корпорацій США почали регулярно обмінюватися інформацією щодо загроз підприємницькій діяльності американських громадян за межами США [6, с. 42–43].

Уперше у США в 1906 р. був прийнятий закон про захист інформації, на сьогодні, вже майже 500 законодавчих актів, що регулюють питання захисту інформаційної безпеки (ІБ), протидії комп'ютерним злочинам. Політика ІБ США формується на 2 рівнях.

На процедуриому рівні визначаються безпосередньо заходи щодо забезпечення ІБ суб' єкта господарювання. До них вони

відносять управління персоналом, фізичний захист і планування роботи. На програмно-технічному рівні здійснюється захист устаткування програмних засобів та інформаційних ресурсів. Реалізується це за допомогою сервісів безпеки: 1) ідентифікація та аутентифікація; 2) розмежування доступу; 3) протоколювання й аудит; 4) шифрування; 5) забезпечення цілісності; 6) екранування; 7) забезпечення доступності; 8) забезпечення стійкості.

Наступний аспект інформаційно–правового забезпечення безпеки діяльності суб'єктів господарювання в США, до якого хотілось би привернути увагу, пов'язаний з реакцією американських законодавців на занепокоєння, яке виникло в американському суспільстві в середині XX ст. у зв'язку з істотним посиленням ролі міністерств і адміністративних агентств (урядових інституцій, які мають більш вузьку спеціальну компетенцію, ніж міністерства, можуть видавати нормативні акти, що мають силу закону, стежити за їх виконанням та розв'язують в адміністративних судах конфлікти, що виникають на цьому ґрунті) [7, с. 99–100; 8, с. 212]. Уже в 1960 – ті роки Конгрес прийняв серію законів, спрямованих на відкритість цих державних органів [7, с. 104]. Зокрема, у 1966 році був прийнятий Закон про свободу інформації, який зобов'язав розкривати певні категорії справ будь-якій особі за її вимогою [7, с. 104]. У 1976 році ухвалено Закон про відкрите прийняття рішень, відповідно до якого будь-яке засідання колегії агентства (за певними винятками) повинно бути відкритим для громадського нагляду [7, с. 104–105].

У 1980 році Конгрес прийняв Закон про гнучке регулювання, який передбачив необхідність з'ясування державними органами наслідків запровадження для малих підприємств нових правил ще до встановлення останніх, щоб забезпечити вибір найменш обтяжливих засобів регулювання [7, с. 105]. У 1990 році ухвалено Закон про переговорний процес при створенні нормативних актів, який дозволив міністерствам і відомствам при підготовці нормативних актів вести попередні переговори із представниками тих сфер або галузей, яких стосуються ці акти [7, с. 105].

Надзвичайно важливим з погляду забезпечення транспарентності урядової діяльності, а тому й з точки зору гарантування безпеки суб'єктів господарювання в США було прийняття в цій країні Закону про електронний уряд, яке сталося 2002 року [8, с. 218].

Таким чином, слід констатувати, що з погляду вирішення проблем вдосконалення інфомаційно–правового забезпечення безпеки суб'єктів господарювання в Україні доволі значний інтерес становить досвід США в царині адміністративно–правового захисту прав власності, організації взаємодії суб'єктів недержавного сектора безпеки з державними органами, забезпечення транспарентності урядової діяльності, доступу до інформації, яка належить адміністративним органам. Уважаємо також за потрібне вказати на актуальність для вітчизняної теорії та практики недержавної правоохоронної діяльності глибокого аналізу переваг і недоліків характерної для США децентралізації її правового регулювання.

1. Висновки і рекомендації щодо внесення змін до Закону України «Про основи національної безпеки України» – Режим доступа: http://www.niss.gov.ua. /articles/1775 .
2. Польща почала писати доктрину інформаційної безпеки – Режим доступа: http://osvita.mediasapiens.ua/media_law/government/polscha_pochala _pisati_doktrinu_informatsiynoi_bezpeki/.
3. Чередниченко О.Ю. Проблемні питання детективної (розшукової) діяльності в Україні, історія розвитку, світовий досвід, ринок приватної детективної (розшукової) діяльності / Чередниченко О.Ю., Чередниченко А.О. // Вісн. економіки трансп. і пром-сті. – 2014. – № 45. – С. 272–280. – Режим доступу : http://nbuv.gov.ua/j-pdf/Vetp_2014_45_62.pdf.
4. Прыгунов П. Об охранном законодательстве различных стран мира / П. Прыгунов // Best of security. – 2007. – № 4–6. – Режим доступа: http://dailyold.sec.ru/dailypblshow.cfm?rid=34&pid=19152.
5. Роль частной охраны в борьбе с преступностью в США // Охрана предприятия. – 2013. – № 5. – Режим доступа: http://www.amulet-group.ru/page.htm?id=1885.
6. Зеркалов Д.В. Экономическая безопасность: моногр. / Д.В. Зеркалов. – К.: Основа, 2011. – Режим доступа: http://zerkalov.kiev.ua/sites/default/files/ekonomicheskaya_bezopasnost.pdf.
7. Шумилов В.М. Правовая система США : учеб. пособие / В.М. Шумилов. – 2-е изд., перераб. и доп. – М. : Междунар. отношения, 2006. – 408 с. – Режим доступа: http://library.nulau.edu.ua/POLN_TEXT/UP/SHUMILOV_2006.pdf.
8. Административное право зарубежных стран: учебник / под ред. В.Я. Кикотя, Г.А. Василевича, Н.В. Румянцева. – М.: ЮНИТИ-ДАНА; Закон и право, 2012. – 431 с. – Режим доступа : http://www.twirpx.com/file/1466921/.

ОСНОВНІ НАПРЯМИ ТА ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ ЛАТВІЇ

Чумак Володимир Валентинович,
провідний науковий співробітник відділу організації наукової роботи Харківського національного університету внутрішніх справ, кандидат юридичних наук

Сучасні соціальні, економічні, політичні зміни, які відбуваються в державі, відображаються в діяльності органів державної влади, в тому числі й поліції, впливають на їх реформування та модернізацію [1, с. 87].

Сьогодні у Міністерстві внутрішніх справ України відбуваються системні реформи, що мають на меті перетворення його на правоохоронне відомство європейського зразка, діяльність якого ґрунтується на підтримці громадськості, забезпеченні прав і свобод людини та громадянина, захисті інтересів держави від протиправних посягань [2, с. 145].

Ефективне виконання завдань, покладених на поліцію, неможливе без створення належного механізму управління. Його розробка та оптимізація мають спиратися на науковий підхід, а також враховувати позитивний зарубіжний досвід діяльності поліції.

Це пояснюється як процесами інтеграції законодавства, активною міжурядовою координацією заходів протидії правопорушенням, так і обміном досвіду проведення конкретних профілактичних заходів. Більшою мірою це стосується країн-членів Євросоюзу, хоча в кожній країні все ж таки залишаються специфічні риси з огляду на особливості їх розвитку, правові традиції, ментальність і ступінь активності громадян [3, с. 75–76, 4, с. 166].

У цьому аспекті важливим та актуальним є дослідження завдань діяльності поліції у сучасних умовах та їх відповідальність міжнародним стандартам, внесення пропозицій щодо удосконалення законодавства, яке регулює діяльність поліції.

В Україні окремі аспекти діяльності поліції в України уже стали предметом дослідження в наукових працях як вітчизняними, так і зарубіжних вчених, серед яких варто відзначити

О. М. Бандурку, Д. М. Бахраха, Ю. П. Битяка, С. М. Гусарова, А. С. Васильєва, С. В. Додіна, С. В Ківалова, В. К. Колпакова, О. Т. Корнійчук, А. Т. Комзюка, Р. С. Мельника, В. П. Науменко, А. П. Павлова, П. В. Пашка, О. С. Проневича, К. К. Сандровського, О. Ю.Синявську, С. С. Терещенка, С.О. Юніна тощо.

Даними авторами зроблено значний внесок у науку адміністративного права, зокрема, при дослідженні діяльності поліції в зарубіжних країнах, проте питання щодо основних напрямків діяльності поліції Латвії все ж висвітлено недостатньо, в існуючих наукових працях указані питання досліджувались фрагментарно або в рамках ширшої правової проблематики без комплексного підходу.

За чисельністю персоналу поліція Латвії традиційно посідає одне з провідних місць серед органів виконавчої влади Латвії.

Зазначимо, що у ст. 1 закону «Про поліцію» Латвійської Республіки, поліція, це озброєні, воєнізовані державні та місцеві поліцейські, чий обов'язок полягає в захисті життя, здоров'я, прав і свобод громадян, власності, інтересів суспільства і держави від злочинних та інших протиправних посягань [5].

Слід зазначити, що відповідно до ст. 3 закону «Про поліцію» на поліцію в Латвійській Республіці покладанні наступні завдання:

- забезпечення індивідуальної та громадської безпеки;
- запобігання кримінальним злочинам та іншим правопорушенням;
- розкриття злочинів розшук осіб які вчинили кримінальні злочини;
- надання допомоги установам та приватним особам щодо захисту своїх прав та інші.

Забороняється залучати поліцію виконувати інші завдання, ніж ті, що передбачені в латвійському законодавстві.

Підкреслимо, що діяльність поліції в Латвійській Республіці регулюється Конституцією Латвії, міжнародними договорами, Законом про поліцію, іншими нормативно-правовими актами Латвії, а також рішеннями органів місцевого самоврядування якщо вони не суперечать законам Латвійської Республіки.

Ніхто не має права втручатися в діяльність поліції, коли вони виконують свої обов'язки, о крім осіб, які уповноважені законом.

Слід наголосити, що діяльність поліції в Латвійській Республіці здійснюється відповідно до принципів законності, гуманізму, права людини, соціальної справедливості та прозорості.

Поліція захищає права і законні інтереси громадян, незалежно від їх національності, соціального, фінансового та іншого стану, расової та національної належності, статі і віку, освіти та мови, ставлення до релігії, політичних або інших переконань.

Працівники поліції діють в інтересах національних і місцевих органів влади, а також громадян [5].

Отже, зазначимо, що вивчення досвіду державного управління поліцією зарубіжних країн має не тільки теоретичне, але й практичне значення в аспекті впровадження в діяльність правоохоронних органів України сучасних форм і методів діяльності. Але під час здійснення реформування правоохоронних органів України без сумніву мають враховуватися, насамперед, національні особливості і запозичати із зарубіжного досвіду необхідно лише найефективніші важелі управлінської діяльності, спрямовані на вдосконалення функціонування поліцейських інститутів.

1. Комзюк В. Т. Завдання та принципи діяльності митних органів України та спеціалізованих митних установ / В. Т.Комзюк / Право і безпека. – 2012. – № 1. – С. 86 – 90.
2. Ратушняк В. І. Завдання та структура підрозділів міліції (поліції) громадської безпеки України та інших країн СНД: порівняльно-правовий аналіз / В. І. Ратушняк // Вісник ХНУВС. – 2012. № 4 (59). – С. 145 – 156.
3. Ответственность за должностные преступления в зарубежных странах / Ф. М. Решетников (отв. ред.). – М. : Юрид. лит., 1994. – 128 с.
4. Григоренко І. А. Зарубіжний досвід протидії службовим зловживанням та корупції в діяльності поліції / І. А. Григоренко І. А // Юридичний часопис національної академії внутрішніх справ. – 2014. – № 1. – С. 164 – 175.
5. Par policiju Latvijas Republikas likums Izdevējs: Augstākā PadomeVeids: likumsPieņemts : закон Латвійської Республіки від 04.06.1991 [Електронний ресурс]. – Режим доступу: http://likumi.lv/doc.php?id=67957. – Закон Латвійської Республіки про поліцію від 04.06.1991

ДОСВІД США У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шишко Валерій Валерійович,
доцент кафедри теорії та історії держави і права
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Шишко Валерій Йосипович,
старший викладач кафедри інформатики
Львівського державного університету внутрішніх справ

Як відомо, Сполучені Штати Америки є однією з перших країн, які розпочали процес інформатизації. Інші промислово розвинені країни світу, зрозумівши перспективність і неминучість цього процесу, вельми швидко зорієнтувались і почали нарощувати темпи впровадження комп'ютерів та засобів телекомунікацій.

У період з 1967 року до сьогодні в США прийнято цілу низку законів, що створюють основу для формування та проведення єдиної державної політики забезпечення інформаційної безпеки з урахуванням інтересів національної безпеки держави. Це закони «Про свободу інформації» (1967 р.), «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про комп'ютерні зловживання та шахрайство» (1986 р.), «Про безпеку комп'ютерних систем «(1987 р.) та інші.

Необхідно визнати, що забезпечення інформаційної безпеки в Україні, насичення усіх сфер життедіяльності новими технологіями, розвиток приватного бізнесу тощо відбувається поки що при мінімальному нормативно-правовому забезпеченні.

Авторитетний американський соціолог і футуролог Елвін Тофлер у своїй праці «Третя хвиля», досліджуючи питання розвитку інформації та техніки і їх роль у соціальних перетвореннях, доводить теорію «інформаційного суспільства», яку, по суті, можна вважати різновидом теорії постіндустріалізму, основи якої заклали американські соціологи З.Бжезинський та

Д.Белл. Дослідники дають різні визначення інформаційного суспільства, але сходяться в головному: інформація в інформаційному суспільстві стає домінуючою цінністю; «генерування, обробка і передача інформації стали фундаментальними джерелами продуктивності і влади» [1, С. 4].

Американським компаніям та університетам належить більша частина світових патентів у сфері інформаційних технологій. У середині 1990-х років у США були зосереджені 426 із 816 світових інформаційних банків даних із науково-технічних дисциплін і 716 із 1035 наявних у світі баз даних із економічних дисциплін. Найближчими роками США залишаться найбільшим у світі ринком програмного забезпечення [2, с. 34].

США, як одна з найбільш інформаційно розвинутих країн, однією з перших зіткнулися з проблемою забезпечення приватності особистого життя та економічної безпеки своїх громадян. Мільйони американців уже стали жертвами кіберзлочинців: їх приватне життя порушується, їх особисті дані викрадаються, їх гаманці спорожняються і все життя перевертається догори дном. За даними дослідження групи ЛЮ, тільки останніми двома роками кіберзлочинність коштувала американцям 8 млрд. доларів [3, с. 16].

У серпні–жовтні 2008 року хакери отримали доступ до електронної пошти і низки файлів передвиборної кампанії Барака Обами, включаючи документи, що розкривають політичні позиції та плани поїздок. Штабістам довелося тісно співпрацювати з Центральним розвідувальним управлінням (ЦРУ), Федеральним бюро розслідувань (ФБР) США, наймати консультантів для відновлення систем [3, с. 16]. За оцінками спеціалістів, упродовж одного року, по всьому світу кіберзлочинці крадуть інтелектуальну власність в середньому на суму до $ 1 трлн [4].

Економічне процвітання Америки в XXI столітті залежатиме від кібербезпеки. Тепер очевидно, що кіберзагроза – це одна з найсерйозніших економічних і національних проблем цієї держави.

Нині Сполучені Штати Америки, як і більшість країн Заходу, зіткнулися з необхідністю удосконалення, з одного боку, функціонування державного апарату, а з іншого – за допомогою

адміністративно-правових засобів забезпечення інформаційної безпеки, що спричинено справжньою революцією у сфері комунікацій та інформаційних технологій, яка призвела до виникнення низки абсолютно нових неврегульованих правом суспільних відносин.

У травні 2009 року при федеральному уряді США була створена Єдина Рада з національної безпеки, однією з основних функцій якої є нагляд за реалізацією політики кібербезпеки. У Білому Домі створено також новий відділ, яким керує Координатор з кібербезпеки [5], який підпорядковується безпосередньо президенту. Слід підкреслити важливість функцій, які виконуються на цій посаді: це інтеграція і злагоджена робота всіх аспектів політики кібербезпеки в галузі управління; тісна співпраця з офісами Білого Дому, а також координація дій у відповідь у випадку надзвичайних подій або нападів. З метою посилення федерального складника політики зміцнення інформаційної безпеки Координатор з кібербезпеки також є членом Ради Національної безпеки, а також членом Національної економічної ради.

Загалом, останнім часом спостерігається різке збільшення кількості хакерських атак в усьому світі. Зокрема, за підрахунками McAfee, за рік кількість нових шкідливих програм зросла на 500%. Так у липні-серпні 2014 року хакери отримали доступ до даних 83 млн. клієнтів одного з найбільших американських банків JPMORGAN CHASE. Хоча найцінніше – паролі, номери рахунків і номери соціального забезпечення – не потрапило хакерам у руки, але за допомогою витягнутої інформації у них з'явилася теоретична можливість пройти ідентифікацію особи. На думку фахівців, метою злому був продаж отриманих даних третім особам; вони, в свою чергу, могли потім використовувати її для просунутих індивідуалізованих форм фішингу, які складно розпізнати навіть уважному користувачеві. В атаці звинуватили деяких російських хакерів, які нібито мали зв'язки з урядом країни [6].

Під час опитування 54% менеджерів вищої ланки визнали, що очолювані ними об'єкти вже постраждали від великомасштабних кібератак із боку організованих злочинців, терористів та окремих держав. Окрім того, 37% респондентів повідомили про те, що минулого року через скорочення корпоративних

бюджетів ситуація з кібербезпекою погіршилася. Сорок відсотків опитаних очікують у новому році великого інциденту в сфері кібернетичної безпеки. Середня величина прогнозованих збитків від простою, викликаного збоєм у роботі ІТ-систем, становитиме близько 6,3 мільйона доларів на день. При цьому 45% керівників уважають, що відповідальність за запобігання такими атаками повинні нести регіональні або місцеві органи влади [7, с. 27].

На Всесвітньому економічному форумі в Давосі генеральний секретар Міжнародного телекомунікаційного союзу Хамадун Туре наголосив, що сучасний світ має потребу в договорі, який міг би запобігти прийдешній світовій кібервійні. Директор із досліджень і стратегії корпорації Microsoft Крейг Манді як рішення запропонував ввести обов'язковий документ для Інтернет-користувачів – аналог водійських прав. «Проблема в тому, що люди не розуміють масштаби і загрозу злочинної діяльності в Інтернеті», – заявив він [8, с. 63].

Адміністрація Барака Обами заявила, що здійснюватиме новий комплексний підхід до забезпечення безпеки цифрової інфраструктури Америки. Надалі американська цифрова інфраструктура – мережі та комп'ютери – розглядатимуться так, як вони повинні розглядатися – як стратегічний національний актив. Захист цієї інфраструктури, у тому числі адміністративно-правовими засобами, буде пріоритетом національної безпеки.

Отже, впровадження нової стратегії інформаційної безпеки Бараком Обамою у США свідчить про зростаючу роль впливу цієї сфери людської діяльності на забезпечення стабільного функціонування державного апарату в одній з найбільших країн світу.

Таким чином, з уваги на досвід США, вітчизняні органи державної влади повинні взяти під регулюючий контроль побудову національної інформаційної інфраструктури. Ситуація ускладнюється ще і тим, що впровадження ІТ в нашій державі супроводжується залежністю від їхньої захищеності. Ключові програмно-апаратні засоби інформаційно-комунікаційних систем розробляються за межами України, тому наша країна позбавлена можливості доступу до їх технічних характеристик.

Сьогоднішній день демонструє, що нехтування питанням безпеки національного інформаційного простору може дуже болісно закінчитися для держави. Найсерйозніша війна зараз перемістилась з площини прямої військової агресії до інформаційної площини, і саме збереження українського інформаційного простору, українських, не лише державних, а взагалі українських телеканалів, радіоканалів є для держави і в цілому для всієї країни принциповою позицією, питанням, яке неможливо віддавати на відкуп кому завгодно.

1. Кастельс Мануель. Информационная епоха: экономика, общество и культура / Пер. С англ., под науч. ред. О.И. Шкаратана. – М., 2000. – С. 4.
2. Роговской Е. Развитие информационного сектора США к началу XXI века / Е. Роговский. – США–Канада. – 2002. – № 4. – С. 32–37.
3. AIG Technology Report 2007–2008: Readiness for the Networked World Center for International Development at Harvard University, March 2009. – P. 14–18.
4. WIPO 2008 Report [Електронний ресурс] / WIPO Site. – Режим доступу: http://www.wipo.int/meetings/en/archive.jsp.
5. Barack Obama Speech, March, 13, 2009 [Електронний ресурс] / Barack Obama Site. – Режим доступу: http://my.barackobama. com/ page/ content/ofasplashbsignon/.
6. Найгучніші хакерські атаки минулого року. – Режим доступу: http://basicgroup.ua/naiguchnishi-khakerski-ataky-mynulogo-roku.
7. Даниелова А. Основные направления информатизации американского общества / А. Даниелова // США–Канада. – 2009. – № 5. – С. 25–29.
8. Шершнёв Е. Информатизация общества и экономики США / Е. Шершнёв // США–Канада. – 2008. – № 1. – С. 61–65.

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

ПРИСТРОЇ АКУСТИЧНОГО КОНТРОЛЮ ІНФОРМАЦІЇ

Вишня Володимир Борисович,
професор кафедри інформатики та інформаційних технологій в діяльності ОВС Дніпропетровського державного університету внутрішніх справ,
доктор технічних наук, професор
Прокопов Сергій Олександрович,
старший викладач кафедри інформатики та інформаційних технологій в діяльності ОВС Дніпропетровського державного університету внутрішніх справ

Сьогодні у навчальних закладах МВС України курсантам, студентам та слухачам викладаються вибіркові дисципліни «Інформаційна безпека», «Основи інформаційної безпеки». Мета включення цих дисципліни до навчального плану полягає в тому, щоб дати майбутнім юристам і правоохоронцям знання, уміння та навички користування комп'ютерною технікою з елементами інформаційної безпеки, з засобами і заходами захисту інформації при виконання завдань в професійній діяльності.

Тому, не зайвою для них буде інформація, підібрана авторами із відомих джерел, про окремі існуючі спеціальні технічні пристрої прослуховування та збору інформації, зокрема їх типи, технічні характеристики та способи застосування.

Викладення матеріалу почнемо з *спрямованих мікрофонів***.**

Звичайні мікрофони здатні реєструвати людську мову на відстані, що не перевищує декількох десятків метрів. Для збільшення дистанції, на якій можна робити прослуховування, практикують застосування спрямованого мікрофона.

Іншими словами, цей пристрій збирає звуки тільки з одного напрямку, тобто має вузьку діаграму спрямованості. Такі пристрої широко застосовуються не тільки в розвідці, але і журналістами, мисливцями, рятувальниками і т. ін.

Можна виділити два основних типи спрямованих мікрофонів: з параболічним відбивачем та резонансний мікрофон.

*Мікрофон з параболічним відбивачем***.** У мікрофоні з параболічним відбивачем власне мікрофон розташований у фокусі параболічного відбивача звуку.

Спрямований параболічний мікрофон з підсилювачем AD-9 концентрує звуки, що йдуть, і підсилює їх. Простий у звертанні і настроюванні. У комплект входить мікрофон, підсилювач, кабель і головні телефони. Електроживлення – від батареї 9В.

Випускаються кілька моделей. Загальним у конструкції всіх цих мікрофонів є наявність рукоятки пістолетного типу, параболічного відбивача діаметром близько 40 див і підсилювача. Діапазон сприйманих частот складає від 100-250 Гц до 15-18 кГц. Усі мікрофони мають автономне живлення і мають рознімання для підключення до магнітофона. Гостра «голчаста» діаграма спрямованості дозволяє при відсутності перешкод контролювати людську мову на відстані до 1200м. У реальних умовах (в умовах міста) можна розраховувати на дальність до 100м.

*Резонансний мікрофон***.** Резонансний мікрофон заснований на використанні явища резонансу в металевих трубках різної довжини. Наприклад, в одній з модифікацій такого мікрофона використовується набір з 37 трубок довжиною від 1 до 92 см.

Звукові хвилі, що приходять до приймача по осьовому напрямку, приходять до мікрофона в однаковій фазі, а з бічних напрямків (через відмінну швидкість поширення звукових хвиль у металі, а також різної довжини трубок) – виявляються зрушеними по фазі.

З погляду схованого контролю звуку застосування спрямованих мікрофонів утруднено через найчастіше неприйнятні

їхні габарити і джерела акустичних перешкод. Крім того, для того, щоб не бути прослуханим в автомобілі, досить просто підняти скло.

Лазерні мікрофони. У тому випадку, якщо ви підняли скло в автомобілі чи закрили кватирку, може бути використаний лазерний мікрофон. Перші їхні зразки були прийняті на озброєння американськими спецслужбами ще в 60-і роки минулого сторіччя.

Як приклад, визначимо лазерний мікрофон HP-150 фірми «Hewlett-Packard» з дальністю дії до 1000м. Він сконструйований на основі гелій-неонового чи напівпровідникового лазера з довжиною хвилі 0,63 мкм (тобто у видимому діапазоні; сучасні пристрої використовують невидимий ІЧ діапазон).

Промінь лазера, відбитий від скла приміщення, у якому ведуться переговори, виявляється промодульованим звуковою частотою. Прийнятий фотоприймачем відбитий промінь детектирується, звук підсилюється і записується. Приймач і передавач виконані роздільно, мається блок компенсації перешкод. Вся апаратура розміщена в кейсі і має автономне живлення. Подібні системи мають дуже високу вартість (більш $10000) і, крім того, вимагають спеціального навчання персоналу та використання комп'ютерної обробки мови для збільшення дальності.

Існує досвідчена вітчизняна система ЛСТ-ЛА2 з дальністю знімання менш 100м і досить скромною вартістю. Слід зазначити, що ефективність застосування такої системи зростає зі зменшенням освітленості оперативного простору.

Гідроакустичні датчики. Звукові хвилі поширюються у воді з дуже невеликим загасанням. Гідроакустики ВМФ навчилися прослухувати шепіт у підвідних човнах, що знаходяться на глибині десятків метрів. Цей же принцип можна застосовувати, використовуючи рідину, що знаходиться в системах водопостачання і каналізації. Таку інформацію можна перехоплювати в межах будинку, але радіус прослуховування буде дуже сильно залежати від рівня шумів, особливо у водопроводі. Переважно використовувати датчик, встановлений у батареї опалення. Ще більш ефективним буде використання гідроакустичного передавача, встановленого в батареї приміщення, що прослухується.

НВЧ і ІЧ передавачі. Для підвищення скритності в останні роки стали використовувати інфрачервоний канал. Як передавач звуку від мікрофона використовується напівпровідниковий лазер. Як приклад розглянемо пристрій TRM-1830. Дальність дії складає 150 м вдень, та 400 м уночі, час безупинної роботи – 20 годин. Габарити не перевищують 26х22х20 мм. До недоліків подібної системи можна віднести необхідність прямої видимості між передавачем і приймачем та вплив перешкод. Найгучніша справа з застосуванням ІЧ каналу – Уотергейт.

Підвищити скритність одержання інформації можна також за допомогою використання каналу НВЧ діапазону (більш 10 ГГц). Передавач, виконаний на діоді Ганна, може мати дуже невеликі габарити. Забезпечується дальність більш 100 м. До переваг такої системи можна віднести відсутність перешкод, простоту і відсутність у даний час ефективних засобів контролю. До недоліків варто віднести необхідність прямої видимості, хоча й у меншому ступені, тому що НВЧ сигнал може обгинати невеликі перешкоди і проходить (з ослабленням) крізь тонкі діелектрики, наприклад, штори на вікнах.

Стетоскопи. Стетоскоп являє собою вібродатчик, підсилювач і головні телефони.

Вібродатчик спеціальною мастикою прикріплюється до стіни, стелі і т. ін. Розміри датчика, на прикладі пристрою DTI, складають 2,2х0,8 см, діапазон частот – 300-3000 Гц, вага – 126 г, коефіцієнт підсилення – 20000.

За допомогою подібних пристроїв можна здійснювати прослуховування розмови через стіни товщиною до одного метру. Стетоскоп може оснащуватися провідним, чи радіо іншим каналом передачі інформації. Основною перевагою стетоскопа можна вважати труднощі виявлення, тому що він може встановлюватися в сусідніх приміщеннях.

Існують стетоскопи, у яких чуттєвий елемент, підсилювач і радіопередавач об'єднані в одному корпусі. Вони мають дуже невеликі габарити і дозволяють не тільки прослухувати розмови через стіни, віконні рами, двері, але і передавати інформацію по радіоканалу. Мають високу чутливість і забезпечує гарну розбірливість мовного сигналу. Як правило робоча частота складає 470

МГц. Дальність передачі – до 100 м. Час безупинної роботи – 24 год, розміри – 40х93 мм.

Більшістю фахівців прогнозується постійний ріст випадків застосування стетоскопів, що насамперед порозумівається зручністю застосування подібної техніки, а також тим, що їх надзвичайно важко знайти.

На останнє розглянемо, яким чином можна підключитися до телефонної лінії і здійснити запис переговорів. У технічному плані найпростішим способом є контактне підключення.

Можливо тимчасове підключення до абонентської проводки за допомогою стандартної «монтерської трубки». Однак підключення такого типу легко виявляється за допомогою найпростіших засобів контролю напруги телефонної мережі. Зменшити ефект спадання напруги можна шляхом підключенням слухавки через резистор 0,6-1,0 КОм. Підключення здійснюється за допомогою дуже тонких голочок і тонких, проводів, що прокладаються в якій-небудь існуючій чи виготовленій щілині. Щілина може бути зашпакльована і пофарбована так, що візуально визначити підключення дуже важко.

Відомий спосіб підключення до ліній зв'язку апаратури з компенсацією спадання напруги. Істотними недоліками контактного способу підключення є порушення цілісності проводів і вплив підключеного пристрою на характеристики ліній зв’язку. З метою усунення цього недоліку застосовується індуктивний датчик, виконаний у виді трансформатора. Існують також датчики, принцип роботи яких заснований на ефекті Холу.

Вартість подібних пристроїв коливається від $20 до $250. Як записуючі пристрої застосовуються стандартні диктофони, спеціальні мініатюрні типу OLIMPUS L-400, а також стаціонарні багатоканальні диктофони, як, наприклад, АД-25-1. Часто прослуховування організовано так, що магнітофон включається з появою сигналу в лінії. Мініатюрним магнітофоном можна вважати модель N2502, рекламовану як магнітофон, що неможливо знайти за допомогою сучасних детекторів записуючої техніки. У цьому магнітофоні маються гнізда для підключення зовнішнього мікрофона, пульта дистанційного управління і головних телефонів.

Як правило, спеціальні багатоканальні магнітофони для запису телефонних переговорів використовуються в складі спеціальної апаратури для контролю особливо режимних робіт. У цьому випадку використовуються спеціальні прийоми, що дозволяють по ключових словах переривати чи записувати телефонну розмову. Такий акустичний контроль може бути організований за допомогою наявних на ринках зарубіжних країн спеціальних багатоканальних магнітофонів, призначених для стаціонарного запису телефонних переговорів і розрахованих на значну кількість (від 10 до 100) каналів.

РОЗРОБКА МОДЕРНІЗОВАНОЇ АВТОНОМНОЇ РЕПРОДУКЦІЙНОЇ УСТАНОВКИ «ЕЛЬ-М2»

Зачек Олег Ігорович,
доцент кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Під час здійснення слідчо-криміналістичної діяльності інколи виникає необхідність здійснити копіювання документів. Не завжди є можливість використати ксерокопіювальне обладнання. А зйомка документів фотоапаратом з рук не може забезпечити необхідної якості зображення через неоднозначне позиціонування документа та незадовільне освітлення. Для вирішення цього питання було розроблено модернізовану автономну репродукційну установку «Ель-М2». Ця установка може бути використана для отримання якісних фотокопій документів за допомогою цифрового фотоапарата з метою подальшого їх зберігання в електронних накопичувачах або оперативного пересилання через інформаційні мережі до конкретного споживача.

Відома репродукційна установка «С-64» («Ель») [1]. Вона відноситься до засобів фіксації візуальної інформації ОВС [2]. Установка призначена для оперативного отримання фотокопій документів розмірами 68×90 мм, 120×160 мм, 180×240 мм та 240×320 мм на стандартну 35-мм фотоплівку з розміром кадру 18×24 мм. За допомогою даної установки фотозйомка документів може бути виконана з малими затратами часу. Недоліком цієї установки є використання плівкового фотоапарата і двох ламп розжарювання потужністю 150 Вт в освітлювачах, що не відповідає сучасним вимогам інформаційного забезпечення та енергозбереження.

Творчим колективом була створена модернізована автономна репродукційна установка «Ель-М» [3]. Основним недоліком даної конструкції є використання енергоощадних люмінесцентних ламп, які потребують живлення змінною напругою 220 В, споживають значно більше електроенергії у порівнянні зі

світлодіодними лампами, забезпечують менший світловий потік та характеризуються низькою надійністю і довговічністю.

Наш творчий колектив поставив перед собою завдання модернізувати цю установку відповідно до вимог часу з найменшими затратами коштів на її вдосконалення.

Поставлене завдання досягається створенням модернізованої автономної репродукційної установки «Ель-М2», яка оснащена світлодіодними лампами з потужним світловим потоком, які живляться від вбудованої акумуляторної батареї, під'єднаної до зарядного пристрою, що підключається до зовнішнього джерела змінної напруги. Зовнішній вигляд модернізованої автономної репродукційної установки «Ель-М2» у складеному (транспортному) вигляді показано на рис. 1.

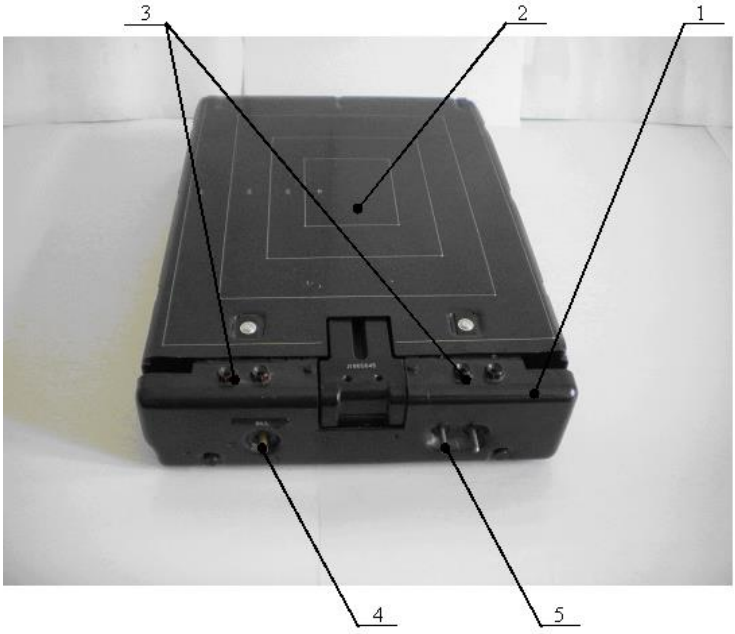


Рис. 1. Модернізована автономна репродукційна установка «Ель-М2» у складеному (транспортному) вигляді.

Основою установки є корпус 1, закритий кришкою 2 і обладнаний рознімами 3 для підключення освітлювачів, вимикачем 4 живлення, рознімом 5 для підключення кабеля живлення

та заряджання акумулятора від зовнішнього джерела змінної напруги.

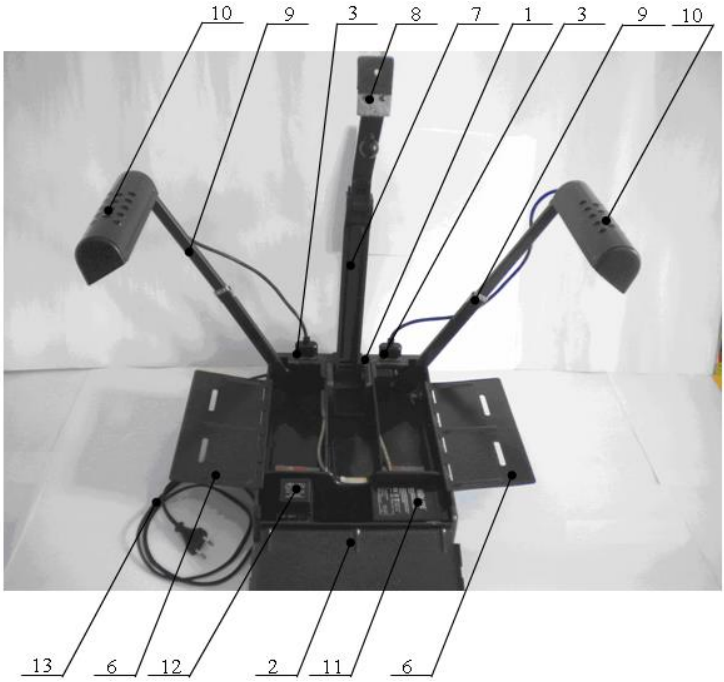


Рис. 2. Модернізована автономна репродукційна установка «Ель-М2» у розкладеному стані без фотоапарата та з відкритим корпусом.

Модернізована автономна репродукційна установка «Ель-М2» у розкладеному стані без фотоапарата та з відкритим корпусом показана на рис. 2. Установка містить корпус 1, до якого шарнірно закріплені верхня кришка 2 та бічні кришки 6, рухома опора 7 (з можливістю фіксації у певних положеннях) з універсальним кронштейном 8 для кріплення цифрового фотоапарата довільної моделі та дві рухомі фіксовані у певних положеннях телескопічні штанги 9, до яких шарнірно закріплені освітлювачі 10 зі світлодіодними лампами з потужним світловим потоком, підключеними через розніми 3 до вбудованої акумуляторної батареї 11, під'єднаної до зарядного пристрою 12, що підключається до зовнішнього джерела змінної напруги через кабель живлення 13.

Модернізована автономна репродукційна установка «Ель-М2» у розкладеному (робочому) вигляді з цифровим фотоапаратом 14 показана на рис. 3.

Рис. 3. Модернізована автономна репродукційна установка «Ель-М2» у розкладеному (робочому) вигляді з цифровим фотоапаратом.

У режимі автономної роботи установки акумуляторна батарея 11 (див. рис. 2) повинна бути заряджена, для чого підключають кабель живлення 13 до розніму 5 (див. рис. 1) і під'єднують його на визначений час до зовнішнього джерела змінної напруги. Робота установки у стаціонарному режимі відбувається при постійно підключеному кабелі живлення 13 до зовнішнього джерела змінної напруги.

Перед початком роботи установки (див. рис. 2) відкривають верхню кришку 2 корпуса 1 і бічні кришки 6, піднімають та фіксують у необхідному положенні опору 7 з універсальним кронштейном 8, до якого прикріплюють цифровий фотоапарат 14 (див. рис. 3), розкладають і фіксують телескопічні штанги 9 з

освітлювачами 10, закривають бічні кришки 6 та верхню кришку 2, підключають освітлювачі 10 до рознімів 3 та включають вимикач 4 живлення, встановлюють на верхній кришці 2 документ і фотографують його. З цифрового носія фотографія документа може бути перенесена на ЕОМ або інший довільний накопичувач інформації і, за необхідності, оперативно передана через дротовий чи бездротовий Інтернет до конкретного адресата. Після завершення роботи необхідно вимкнути вимикач 4 живлення, від'єднати освітлювачі 10 від рознімів 3, від'єднати цифровий фотоапарат 14 від універсального кронштейна 8, відкрити верхню кришку 2 корпуса 1 та бічні кришки 6, скласти опору 7 і телескопічні штанги 9 з освітлювачами 10, закрити бічні кришки 6 та верхню кришку 2.

На модернізовану автономну репродукційну установку «Ель-М2» творчим колективом отримано патент України на корисну модель [4]. Розробки в даному напрямі є перспективними і будуть продовжуватись.

1. Сеник В.В. Засоби фіксації зображення в оперативно-розшуковій діяльності і тактика їх використання у попередженні та розкритті злочинів. – Львів, 2001.
2. Керницький І.С., Щур Б.В., Мовчан А.В., Хараберюш І.Ф., Слижук В.М., Шевченко О.М., Сеник В.В., Зачек О.І. Спеціальна техніка. Підручник. (Затверджено МОН України як підручник для студентів вищих навчальних закладів. Лист № 1/11-10079 від 02.11.2010 р.).– Львів: ЛьвДУВС, 2010 р.–356 с.
3. Цимбалюк М.М., Керницький І.С., Зачек О.І., Григоришин О.М., Слижук В.М., Сеник В.В. Патент України на корисну модель № 85789 «Модернізована автономна репродукційна установка «Ель-М», виданий згідно заявки № u 2013 08469 від 05.07.2013 р. – 4 с.
4. Керницький І.С., Зачек О.І., Сеник В.В. Патент України на корисну модель № 101757 «Модернізована автономна репродукційна установка «Ель-М2», виданий згідно заявки № u 2015 03724 від 20.04.2015 р. – 4 с.

GSM-ТЕХНОЛОГІЇ В ОХОРОННИХ СИСТЕМАХ

Кулешник Ярко Федорович,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент
Рудий Тарас Володимирович,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Охорона власності вимагає крім вирішення організаційних питань ще й застосування надійних каналів зв'язку. Можливе Інтернет-підключення від одного з провайдерів. Але за містом стабільність мереж доступу недостатньо висока, щоб довірити їм безпеку свого житла. І справа тут навіть не в провайдерах, а в особливостях розміщення обладнання. Тому постає питання використання сучасних альтернативних видів охоронних систем, зокрема *GSM-сигналізації.*

Сама проблема носить більше економічний чи технічний характер ніж науковий, тому широкого обговорення в науковий колах поки що не набула. В той же час раціональний і економічно обгрунтований підхід до захисту нерухомості вимагає від власників сучасних знань про можливості охоронних систем, зокрема на основі застосування *GSM-технологій*.

Мета даної публікації полягає у тому, щоб окреслити організаційно-технічну сторону застосування *GSM-сигналізації*. Разом з тим, відзначимо, що це є всього лише спроба відкрити для користувачів новий сучасний вид охоронних систем.

Захист власності, а особливо приватної, у наш час залишається злободенним питанням. В охороні нуждаються приватні будинки, гаражі, магазини, кафе, готелі та ін. Власники повинні чути і бачити що робиться в тому чи іншому місці в момент вторгнення щоб моментально відреагувати.

У битву за своє місце на ринку охоронних систем увірвалась і gsm-сигналізація. Очевидно, що ці охоронні сигналізації швидко виштовхнуть з арени класичні пультові охоронні системи.

У зв'язку з розвитком GSM-зв'язку з'явився новий і зараз найпоширеніший спосіб сповіщення, контролю і управління віддаленими об'єктами, такими як приватний будинок, міська квартира, заміська дача, офіс, гараж та ін. (стаціонарними і рухливими).

Простота і комфорт системи GSM-охорони полягає в її гнучких налаштуваннях під особисті запити будь-якого користувача. Принцип дії базується на швидкому сповіщенні факту злому.

За останні два роки об'єми продажів GSM-сигналізацій ростуть по експоненті. Все більше устаткування робиться в Україні, все більше приватних охоронних підприємств переходять на пультове і об'єктове устаткування використовуючі GSM-канал для охорони майна.

Причини швидко зростаючої популярності GSM-сигналізацій наступні:

- величезні зони охоплення GSM-мереж. Ще ні одна радіосистема не покрила такі ж простори і площі, як мережі стільникового зв'язку.
- низькі ціни на послуги стільникових операторів і як наслідок цього доступність широким верствам населення.
- простота використання. Для монтажника системи досить тільки приїхати на об'єкт і встановити охоронну панель з GSM модулем або GSM-сигналізацію.
- додаткові сервіси. Сервіси стільникових операторів розширюють можливості GSM-сигналізацій, наприклад передача *sms* власникові.
- охоронні підприємства отримують низьку вартість ПЦН, оплачуючи тільки те, що дійсно необхідно, не треба купувати частоти і ретранслятори.
- низька ціна в порівнянні з УКВ передавачами.

Якщо об'єкт, що охороняється, невеликий, Ви програмуєте свій мобільний номер телефону, і сигналізація дзвонить на нього та посилає тривожні повыдомлення з позначкою зони, що спрацювала.

Така функція потрібна і в тій ситуації, якщо зона охорони великих розмірів і на ній постійно знаходяться охоронці. Записавши свій телефон і службовий у охорони, Ви будете в курсі подій, які з'являються у Вас на об'єкті, у зв'язку з тим що gsm-сигналізація подзвонить і пришле *sms* на усі телефонні номери, які в неї записані.

На сьогоднішній день GSM мережі досить надійні, але, якщо є побоювання щодо цього, то варто вибрати сигналізацію, що дозволяє встановити дві SIM картки. Краще, якщо це будуть SIM карти двох різних операторів, в такому випадку надійність системи підвищується.

Основні напрями застосування GSM сигналізації:

- віддалений контроль заміського будинку або квартири – у складі системи «Розумний будинок» або окремих елементів таких як аудіо/відеоконтроль, сповіщення і управління електроприладами;
- GSM облаштування захисту від затоплення – для управління електровентилями і сповіщення користувача;
- GSM пристрої, орієнтовані на ПЦН приватних фірм позавідомчої охорони, – як альтернативний канал охорони;
- системи контролю автотранспорту при грузо/пасажироперевезеннях – в якості GPS/GSM трекерів для визначення місцезнаходження;
- видалений GSM контроллер автомобіля – в якості протиугінної сигналізації, як незалежною, так і разом з штатною;
- супутникові автономні GPS/GSM системи контролю автотранспорту при викраденні і визначенні місцезнаходження;
- термінали прийому платежів – для передачі даних з POS-терміналів і банкоматів, а також сповіщення при їх зломі і знеструмленні;
- кавові та ін. апарати – для передачі даних стану апарату, сповіщення при зломі і знеструмленні;
- GSM системи управління рекламними установками – для передачі даних про стан рекламної установки і управління режимами роботи;
- GSM системи контролю доступу і обліку робочого часу – для передачі інформації;

- системи управління температурним режимом в теплицях – для видаленого контролю і регулювання температурного режиму;
- GSM системи передачі ТБ-сигналу – для сповіщення диспетчерських служб про аварії, що виникають з ефірним устаткуванням;
- холодильне і морозильне устаткування – для видаленого контролю і регулювання температурного режиму.

Сфер застосування GSM сигналізації багато і величезні перспективи розвитку GSM.

Рекомендації по підбору GSM-сигналізації :

- GSM-сигналізації складається з двох частин, контрольної панелі і GSM-модему. Сигналізація, що купується, має бути єдиною, вона не повинна складатися з пристроїв від різних виробників. Тому що виріб в цілому не проходив вихідний контроль і може бути взагалі не сумісним з цією панеллю;
- якість GSM-сигналізації має бути підкріплена сертифікатами;
- в GSM-сигналізаціях повинні використовуватися промислові GSM-модеми і модулі. Трубки стільникових телефонів не придатні для використання в охоронних приладах;
- виріб не має бути зібраний кустарним способом і повинне складатися з хорошої елементної бази.

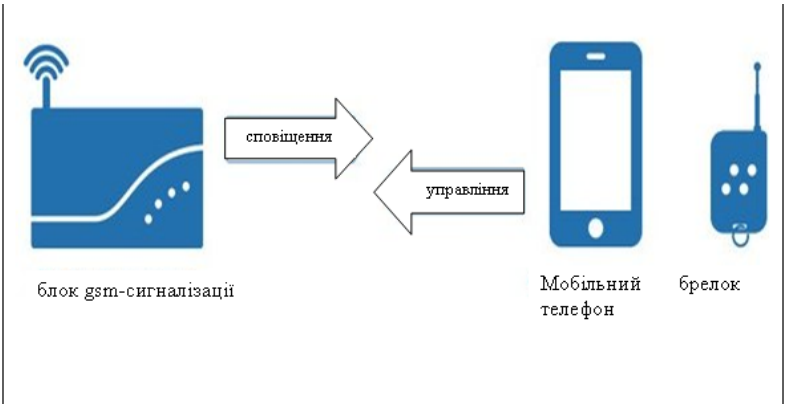
Деякі особливості використання:

- запасу маленьких батарейок у центральному блоці вистарчає на пару років;
- сама автономна сигналізація може працювати 7-10 діб;
- у всіх давачах для комфорту є налаштування чутливості до 15 та 20 кілограм, що запобігає випадкове спрацьовування давача на домашніх тварин.

Gsm-сигналізацію можна встановити декількома способами: дротяним, безпровідним і комбінованим, при чому, безпровідна сигналізація коштує значно дорожче ніж аналогічна дротова.

У загальному випадку процес використання GSM-сигналізації можна представити наступною схемою (рис. 1). У результаті спрацювання дротових чи бездротових давачів сигнал від центрального блоку GSM-сигналізації через антену сповіщає, шляхом sms-повідомлення або телефонного дзвінка на мобільний

телефон, власника нерухомості про несанкціоноване проникнення в приміщення. Власник може відключити gsm-сигналізацію за допомогою мобільного телефону чи брелка, або звернутися при необхідності до відповідних органів для надання термінової допомоги.



Мал. 1. Загальна схема застосування GSM-сигналізації.

Таким чином, необхідність встановлення сигналізації нам очевидна, канал зв'язку теж відомий – це GSM мережа будь-якого мобільного оператора. На сьогоднішній день GSM мережі досить надійні, але, якщо є побоювання щодо цього, то варто вибрати сигналізацію, що дозволяє встановити дві SIM картки.

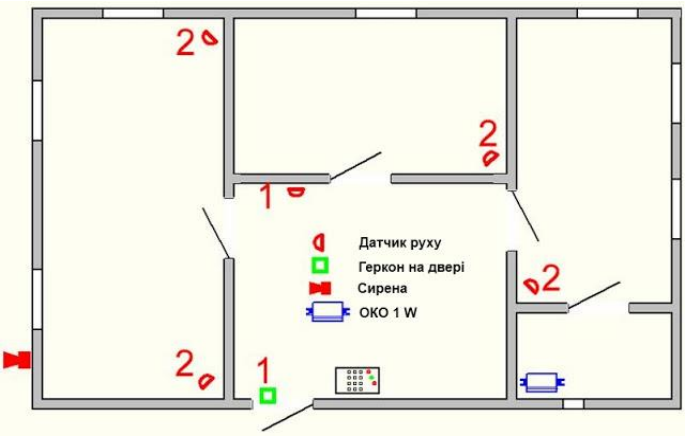
З чого почати?

Почати слід з визначення кількості приміщень та дверей, які повинні знаходиться під охороною. Для забезпечення надійного захисту будинку бажано розмістити сповіщувачі (давачі) у всіх приміщеннях, де є вікна, через які в будинок можуть проникнути зловмисники та на вхідних дверях.

Для того, щоб більш практично розглянути питання інсталяції та налаштування – наведемо приклад невеликої дачі з поясненнями по програмуванню контроллера, підключенню ІЧ-давачів руху і т. ін. Будь-яка справа починається з плану, наш план поверху з місцями всановлення давачів зображений на малюнку 2.

На плані бачимо прихожу, одну житлову кімнату зліва, ще одна житлова кімната попереду вас, кухня праворуч, і невелика

комора поруч. Розбиваємо приміщення і давачі, встановлені в них на умовні «зони». При дротовому варіанті кожна зона підключається на свій шлейф. На плані є герконовий давач, ІЧ-давачі, і клавіатура введення коду зняття і постановки під охорону.Також слід подумати, де буде розташовуватися світлозвукова сирена (оповіщувач). Її доцільно встановити на вулиці. Хоч даний пристрій і призначений для експлуатації поза приміщеннями, слід все ж захистити його від дощу і снігу. У нашому випадку зовнішню сирену ми розміщуємо на стіні будинку, на висоті 4-8 метрів. Першою зоною у нас позначено два давачі: герконовий на двері і в цьому ж приміщенні ІЧ-давач руху. Робиться це для надійності. Більшість проникнень відбуваються через вхідні двері. Навіть якщо зловмисникові вдасться заблокувати геркон на дверях, ІЧ-давач зробить свою справу. Тому розташовуємо його навпроти вхідних дверей, на висоті приблизно 2м від рівня підлоги. Другою зоною позначені дві кімнати і кухня. Звичайно, Ви можете зробити з цього варіанта і три зони. Все залежить від того, наскільки зручно по будинку прокладати кабель. Саму GSM сигналізацію і блок живлення з акумулятором розташуємо в коморі. Це ускладнить знаходження і знищення системи сигналізації до того моменту, коли відбудеться оповіщення всіх телефонних номерів внесених в систему.



Мал. 2. План поверху з наведеними місцями встановлення складових gsm-сигналізації.

Отже, на вхідні двері встановимо магнітоконтактний давач. Він складається з магніту і геркона – при віддаленні магніту контакти в герконі розімкнуться, що і будемо використовувати для охорони відкриття вхідних дверей. Давачі (сповіщувачі) бувають накладні і врізні, дротовими і бездротовими. На металевих вхідних дверях не бажано використовувати герконові давачі. У нашому прикладі (будинок дерев'яний) використаємо врізний дротовий давач, зображений на малюнку 3, 4.

Що таке ІЧ-сповіщувач і чому він комбінований? Сповіщувач – це пристрій (датчик), котрий посилає сигнал тривоги блоку сигналізації, який в свою чергу повідомляє власника житла про несанкціоноване проникнення. ІЧ означає, що давач реєструє зміни інфрачервоного випромінювання, яке ще називають тепловим.

Мал. 3. Герконові дротові накладний та врізний давачі.

Мал. 4. Бездротові ІЧ-давачі.

Господар і зловмисник тут не вийняток, є джерелом інфрачервоного випромінювання, яке і реєструє давач. До речі, домашні тварини також є джерелами інфрачервоного випромінювання. Про них виробники подбали окремо: сповіщувачі не реагують на домашніх тварин менше певної маси. Комбінованим сповіщувач називається тому, що крім реєстрації інфрачервоного випромінювання, він реагує на звук розбиття скла.

Тепер перейдемо до того, як ми будемо ставити і знімати з охорони. Варіантів є декілька: користуючись додатковими радіобрелками з приймачем, електронними ключами (iButton), електронними картками (Proximity), встановивши додаткову клавіатуру для набору секретного коду постановки-зняття і нарешті просто керуючи постановкою-зняттям з мобільного телефону. Тут потрібно відзначити, що кожен з варіантів має свої плюси і мінуси. В першу чергу залежить від кількості користувачів і скільки разів на день буде ставитися і зніматися об'єкт з охорони. На заміській дачі для відвідування на вихідні – цілком підійде варіант управління з мобільного з доставкою підтверджуючого повідомлення *sms* на один або два телефони господарів. Для варіанта квартири, коли користувачів 2-3-4 чол, і *sms* в день може відправлятися чимало, *sms* будуть суттєво відволікати увагу, та й вимагатимуть регулярного поповнення сімкарти. Варіант управління за допомогою клавіатури, брелків і електронними ключами (картами) майже рівноцінний, за винятком того, що брелки та електронні ключі (карти) потрібно брати з невеликим запасом, і в разі втрати швидше за все буде потрібно спочатку витерти з пам'яті пристрою всі брелки та ключі, а потім заново записати нові. Для клавіатури тут найпростіше: просто змінити на новий код і повідомити його користувачам системи. Але якщо Вам все таки зручно користуватися електронними ключами (iButton) або електронними картами (Proximity), то Вам буде потрібно модулі контролю доступу зі зчитувачем електронних ключів або карт.

Висновки. Раціональний і економічно обгрунтований підхід до захисту нерухомості вимагає від власників сучасних знань про можливості охоронних систем, зокрема на основі застосування GSM-технологій. Професійно спланувавши організаційно-технічну сторону впровадження GSM-сигналізації Ви самостійно можете вибрати та встановити необхідну вам сигналізацію зекономивши при цьому значну частину власних коштів та отримаєте неабияку насолоду від творчості.

1. www.signalizacia.com.ua
2. www.ohrana.ua
3. www.gsmohrana.com.ua
4. www.bezpeka.kiev.ua
5. www.bezpeka-shop.com

ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ЗАСОБІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОГО ПОРЯДКУ, ПРОВЕДЕННЯ МАСОВИХ ЗАХОДІВ

Нагачевський Сергій Володимирович,
заступник декана юридичного факультету Львівського державного університету внутрішніх справ,
кандидат юридичних наук

Проблеми припинення порушень громадського порядку при проведенні масових заходів є актуальними і характерними для поліції всіх країн світу. Україна не є винятком. Особливого значення набула ця проблема в останні 10 років незалежності і демократичних перетворень у державі. Це і демонстрації різних партій, акти протесту перед спорудами Верховної Ради України, Кабінету Міністрів, дії опозиції біля пам'ятника Т. Г. Шевченку, які було продовжено біля будівлі МВС України, створення наметового містечка на майдані Незалежності, мітинги про набуття статусу державної іншими мовами, протистояння при проведенні виборчої кампанії у східних і західних регіонах України, а також з випадки терористичних дій. Подібні дії контролюються ОВС і спрямовані на вирішення проблем для забезпечення громадського порядку (ГП) та громадської безпеки (ГБ). Для нейтралізації лише перелічених загроз та мінімізації їх наслідків працівники ОВС мають бути добре підготовленими, володіти відповідними тактичними прийомами та засобами, досягати майстерності у максимально ефективному їх застосуванні. В якості засобів активної оборони: спеціальні, як правило, хімічні сполуки за ГОСТ 12.1.004-76, що застосовуються у вигляді аерозолю або рідини, що швидко випаровується. При розпиленні у повітрі вони впливають на дихальні органи людини, її слизову оболонку та шкіру. У спеціальній літературі ці подразнюючі речовини отримали назву іритантів, летальна дія для яких нехарактерна та можлива лише при потраплянню в організм людини доз, які значно перевищують допустимі норми, в десятки, а то й сотні разів [2]. Найбільш для цього придатні

речовини, що мають неприємний або нестерпний запах. Проведені дослідження показують, що існує низка речовин з надзвичайно нестерпним запахом, які класифіковані у такому порядку: королівський дракон, скунс, тхір тощо. Відповідно до вимог, що висуваються до таких речовин, вони не повинні призводити до тілесних ушкоджень, подальших фізичних ускладнень здоров'я, людини, а головне, її психічних розладів та впливу на клітковому рівні. Такі речовини у припустимих концентраціях (К), відповідно до санітарних норм, містять складові, що викликають короткочасну сльозогінну дію, пригнічення фізичних реакцій у людей, нудоту, або навпаки, неусвідомлене, несподіване здійснення природних функціональних реакцій. Нині іританти використовуються в АГ, що приведені у роботі авторів [1; 2]. На практиці для зазначених цілей використовують 'Ц-хлорацетофенон та інші речовини ГДК впливу якого складає не більше 0,3, що вимагає подвійного захисту. Пристрої для застосування СЗ нами класифікуються за трьома видами: аерозольні, струменеві рідинні та піноутворюючі [1]. Збільшення правопорушень ГП при проведенні масових заходів вимагає застосування нових методів, форм і засобів впливу на громадян порушників. Такими засобами прогнозування призупинення масових порушень ГП є застосування стандартних балонів-генераторів до 100 мл, що містять подразнюючі газоподібні суміші. їх застосування пов'язане зі станом атмосфери і можливістю створення високої концентрації в повітрі зони руху порушників проведення масових заходів. Недоліком вказаної тактики застосування є нетривала дія таких генераторів, (приблизно 35-45 с), але це дозволяє створити короткочасну перепону, яка не є стабільною і не дає можливості стримати натовп надовго. Можливим є застосування у таких ситуаціях і генераторів обсягом 25 л, але на їх застосування потрібен спеціальний дозвіл через ймовірність створення у зоні порушення громадського порядку високої концентрації тазу подразнюючої дії, що перевищує допустимий рівень гранично допустимої концентрації. Це вимагає створення генераторів з меншим за 25 л обсягом, наприклад, від 0,4 до 2 літрів, якими можуть бути озброєні працівники ОВС і використовувати їх залежно від ситуації та оперативної обстановки. Аналогічний показник, за визначенням Шостака

В.В., «запас безпеки» важливий і для іритантів, особливо у разі застосування під час масових порушень ГП при одночасному впливі на людей різної статі, віку, ваги, з різним станом здоров'я. Хіміко-фізіологічні показники препаратів подразнюючої дії, їх концентрації тощо, що впливають на організм людини, приведені в роботі авторів статті [1].

Підсумовуючи викладене, на снові проведених досліджень можливо зробити наступні висновки. Застосування аерозольних генераторів при проведенні працівниками ОВС заходів по забезпеченню охорони громадського порядку, за рахунок гнучкої тактики, можуть мати більші можливості і бути більш ефективними, ніж це викладено в існуючих нормативних документах.

Вдосконалення тактики застосування аерозольних генераторів для підвищення ефективності дії досягається шляхом застосування аерозолів з меншою концентрацією з тим же ефектом дії. Наприклад, при застосуванні хлораценофену той самий ефект дії досягається застосування дибензоксазепину з концентрацією ГДК меншою в ЗО разів. Підвищений ефект дії аерозольних генераторів, для створення «газової перепони» перешкоджаючій руху порушникам громадського порядку, досягається запропонованим розпилюванням «методом ланцюжка» за рахунок створення стійкого рівномірного розподілення згінного аерозолю. За таких умов, а також з зарахуванням тактики застосування, зменшується ризик ураження з перебільшенням ГДК як для порушників громадського порядку, так і для працівників ОВС. Як правило, застосування сльозогінного газу вимагає використання міліцією спеціальних засобів індивідуального захисту.

Засобами доставки аерозолю в місця створення аерозольної, газової перепони можуть стати точні інноваційні дистанційні системи на основі безпілотних літальних апаратів.

---

1. Шиян В. Д. Тактика застосування аерозольних генераторів при проведенні заходів забезпечення громадського порядку / В. Д. Шиян // Сучасна спеціальна техніка. – 2009. – № 2. – С. 16-26.
2. Шиян В. Д. Тактика застосування іритантів працівниками ОВС / Василь Шиян, Ігор Сторожук // Честь і закон. – 2010. – № 2. – С. 75-80.

ЕЕЛЕКТРОННІ КАРТИ В СИСТЕМІ МОНІТОРИНГУ ТА ПРОГНОЗУВАННЯ СТАНУ ВОДНИХ РЕСУРСІВ

Стадник Мирослава Євгенівна,
заступник декана економічного факультету
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент
Стадник Ольга Володимирівна,
магістрант економічного факультету
Львівського державного університету внутрішніх справ

Для забезпечення необхідною оперативною інформацією усіх існуючих на сьогоднішній день рівнів управління водними ресурсами: державного, басейнового та територіального, уникаючи дублювання представлених даних, для створення єдиного цілісного наочного територіального відображення стану водойм, інтенсивності використання водних ресурсів, джерел їх забруднення, прогнозування виникнення надзвичайних ситуацій виникає необхідність у застосуванні електронних карт для впровадження високоефективної трирівневої геоінформаційної (ГІС) системи моніторингу та прогнозування стану водних ресурсів з врахуванням їх взаємодії з природним та антропогенним середовищем.

Геоінформаційна система виступає дієвим інструментом в управлінні, зокрема, водними ресурсами як в масштабах усієї країни, так і окремих територій чи басейнів рік. Геоінформаційна система управління водними ресурсами за основну мету має спостереження, обробку, збереження в єдиній інформаційній базі даних моніторингу водойм з прив'язкою до території і врахуванням її природно-кліматичних особливостей та господарської діяльності людини.

У національній програмі інформатизації ГІС розглядається як сучасна комп'ютерна технологія, що дає можливість поєднати модельне зображення території (електронне відображення карт, схем, космо- та аерозображень земної поверхні) з інформацією

табличного типу (різноманітні статистичні дані, списки, економічні показники тощо) [3].

Сучасна професійна ГІС – це універсальна «клієнт-серверна» система, що має засоби створення і редагування електронних карт, виконання різноманітних вимірювань і розрахунків, оверлейних операцій, побудови тривимірних моделей, обробки растрових даних, засоби підготовки графічних документів, а також зручні інструментальні засоби для роботи з базами даних. Наявні розвинені засоби редагування векторних і растрових карт місцевості і нанесення прикладної графічної інформації на карту. Підтримка декількох десятків різних проекцій карт і систем координат [2, с. 128].

Засобом візуалізації (наочного відображення) інформації в ГІС є електронні карти, які за допомогою виділень і символів відображають в просторі і часі в будь-якому масштабі необхідну інформацію, що оперативно оновлюється і представляється в електронному вигляді чи на папері (рис. 1).

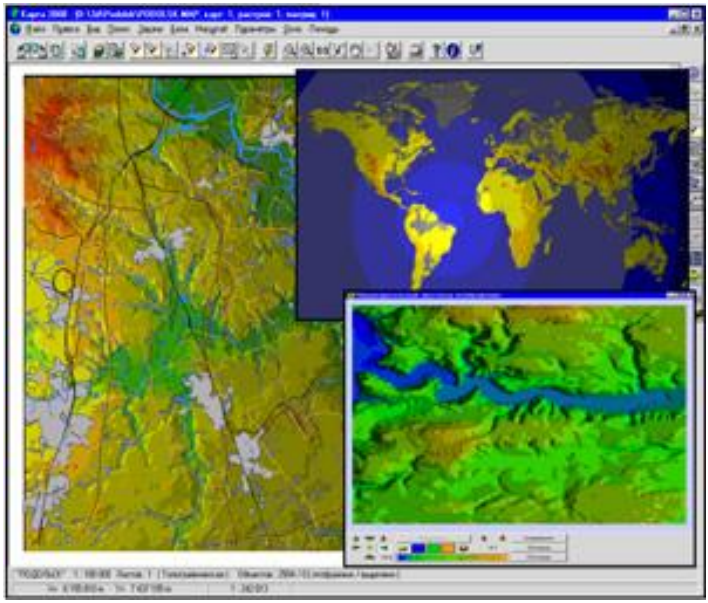


Рис. 1. Приклад тривимірної моделі місцевості

Використання електронних карт забезпечує легке і швидке копіювання даних і поширення їх по локальних та глобальних інформаційних мережах.

Для побудови електронних карт застосовують спеціальну систему умовних знаків, які мають свої особливості і відрізняються від традиційних паперових карт рядом ознак. До основних з них можна віднести: нижча роздільна здатність сучасних пристроїв відеовідображення, ніж у технологій друку на твердій підкладці, та ширшими графічними можливостями в галузі анімації.

Оскільки роздільна здатність дисплеїв часом має певні обмеження, то виникає потреба у спрощенні умовних знаків, тобто використовувати графічні образи з меншою кількістю деталей. Також статичне зображення паперових карт вже не задовольняє потреби дослідників, тому почали застосовувати анімацію (миготіння) для позначення окремих об'єктів аналізу (результатів пошуку).

До переваг сучасних електронних карт слід віднести їхню більшу деталізацію порівняно з паперовими, можливість зміни масштабу, швидкого пошуку необхідних даних, їх оновлення, обміну інформацією між рівними ланками управління. Такі карти легко розповсюджувати, тиражувати, вони не зношуються.

На сучасних електронних картах відображають просторову та атрибутивну інформацію. Для цього застосовуються дві моделі даних: векторні і растрові.

Растрові зображення будують за допомогою точок різних кольорів або пікселів (тобто мінімальних ділянок зображення, кожна з яких має власне положення та колір), які розміщені на правильній сітці.

Якість растрового зображення залежить від розміру зображення (кількості пікселів по горизонталі та вертикалі) та кількості кольорів, які можна задати для кожного пікселя. Растрові, зображення дуже чутливі до зміни масштабу. При зменшенні растрового зображення декілька сусідніх точок поєднуються в одну, тому відбувається неврахування дрібних деталей зображення. При збільшенні зображення збільшується розмір кожної точки та має місце ступінчатий ефект, який можна побачити, не придивляючись. Важливою характеристикою растра є його

роздільна здатність, тобто кількість пікселів на одиницю довжини [1].

При векторній побудові електронних карт відображення інформації подають як сукупність геометричних примітивів (точок, ліній, кривих, полігонів), точок, що можна описати за допомогою математичних рівнянь. Електронні карти будуються як набір кординат, векторів і інших чисел, що характеризують примітиви, з яких вони складаються. Примітиви, у свою чергу, зображаються на основі ключових точок, що визначаються у вигляді набору чисел, а вже програма відтворює зображення шляхом з'єднання ключових точок [1]. Векторні моделі побудови електронних карт надають більші можливості для їх редагування: масштабування, повертання, деформування.

Кожна із зазначених моделей має свої переваги і недоліки, а також призначення. Тому залежно від потреби і типу даних використовують одну із них.

Основою побудови електронних карт та ефективної роботи ГІС є формування та управління базами даних. «Базою даних у ГІС називають сукупність просторових і семантичних (змістовних) даних, що організовані згідно із загальними принципами опису, зберігання і маніпулювання даними, незалежно від тематичного спрямування прикладних програм» [4].

Сучасні системи управління базами даних (СУБД) сприяють зберіганню, структуруванню та керуванню значними обсягами інформації з метою прийняття певних управлінських рішень. Вони забезпечують користувачеві просте і доступне використання необхідної інформації і не вимагають від нього глибоких знань організації баз даних. У короткі строки вони надають користувачам відповідних рівнів необхідну інформацію, за потреби згруповану певним чином, відображає взаємозв’язки між різними параметрами (ґрунт, рельєф, водні ресурси, ступінь забруднення довкілля, обсяги промислового виробництва на певній території тощо).

Сучасний досвід застосування геоінформаційних технологій для управління водними ресурсами, їх позитивні та негативні характеристики переконують, що для підвищення ефективності їх використання необхідна співпраця економістів, програмістів,

фізиків, хіміків, біологів тощо. Таким чином застосування ефективної геоінформаційної системи забезпечить усі рівні управління водними ресурсами необхідною доступною повною оперативною аналітичною наочно відображеною інформацією про реальний та прогнозний стан водних ресурсів і дозволить приймати вчасні рішення щодо його покращення й попередження забруднення водойм і виникнення стихійних лих.

1. Лыбак Т. М. Все к уроку : Компьютерная графика : Учеб. пособие / Т.М. Лыбак. – [Электронный ресурс] – Режим доступа : http://navigator.rv.ua/index.php?option=com_content&view=article&id=4106:2013-07-01-13-25-20&catid=86.
2. Мельник Т.П. Применение ГИС для потребности предупреждения стихийных гидрологических явлений / Т. П. Мельник // Вестник Харьковского национального университета. – 2012. – № 1037. – С. 125-132.
3. О национальной программе информатизации [Закон Украины]// [Электронный ресурс] – Режим доступа : http://zakon1.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80
4. Шевчук В.Я. Экологическое управление : Учебник / В. Я. Шевчук, Ю. М. Саталкин, Г. О. Белявский и др. – К. : Либедь, 2004. – 432 с.

ОПТИМІЗАЦІЙНА МОДЕЛЬ ЗАДАЧІ ПЛАНУВАННЯ ЛОГІСТИЧНИХ ПЕРЕВЕЗЕНЬ

Федорчук Євдоким Никифорович,
Національний університет «Львівська політехніка»,
кандидат технічних наук, доцент
Федорчук Юрій Євдокимович,
аспірант Львівської комерційної академії

Логістичні задачі планування ресурсів для перевезень є актуальними економічними та технічними задачами як для звичайних перевезень, так і для перевезень із зони стихійного лиха, надзвичайних ситуацій, у практиці підготовки військових операцій [1, 2].

Пропонується модель для задачі планування у формі задачі оптимізації [3]. Є ряд маршрутів, для яких є відомою орієнтовна кількість пасажирів для одноразового перевезення. Необхідно розрахувати кількість транспортних засобів різного типу для перевезення потрібної кількості людей на кожному маршруті. Математична постановка такої задачі має вигляд. Знайти

$$\min \Phi = \left(\sum_{i=1}^{m} k_i n_i - N_z \right)^2 \qquad (1)$$

де: m – задана кількість типів транспорту в парку транспорту; n_i – задана місткість окремого засобу(автомобіль, автобус); k_i – кількість одиниць окремого засобу; N_z – задана кількість пасажирів на маршруті. Обмеження задачі включають обмеження на існуючу кількість типів транспорту:

$1 <= k^i <= k^i{}_{max}$; $i \in [1, m]$.

Добуток $k_i n_i$ у виразі (1) дає допустиму кількість пасажирів, яку може перевозити k-одиниць окремого типу транспорту. Ці машини можуть входити в парк із m-типів транспорту. Вважається, що парк машин сформований на основі політики власників парку.

Розв'язок задачі дає $k^{опт}$ – необхідну кількість одиниць кожного типу транспорту, задіяних у перевезеннях вибраного маршруту.

Розглянута задача є неперервною багатокритеріальною задачею оптимізації. При різних початкових значеннях ***к*** можливі варіанти рішень, відмінних за сумарною кількістю одиниць транспорту. Це дає змогу обрати оптимальний варіант – транспортний кластер для маршруту. Дана задача орієнтована на пошук у базі транспортних одиниць. Вважається, що база є наявною в інформаційній системі організації, що займається перевезеннями.

Алгоритми вирішення описаної задачі є відомими. Вони реалізовані в багатьох програмних засобах Matcad, Matlab, Excel. Нами обрана система Excel, в якій легко реалізувати базу даних транспортного парку і обчислити рішення задачі оптимізації за допомогою процедури «Пошук рішення». Для автоматизації її виклику написаний скрипт мовою VBA, який приєднується до книги системи Excel і слугує інтерфейсом користувача для виконання різних розрахунків.

В табл. 1 подано дані про обрану авторами структуру транспортного парку та результати оптимізації. Подано: зображення, місткість окремої одиниці, наявна кількість одиниць. В табл. 2 подано результати моделювання для 4-х варіантів маршрутів із заданою кількістю перевезень. Похибка обчислень є малою, що свідчить про доцільність застосування пропонованої моделі для логістичних задач.

Табл. 1. Парк транспортних засобів

№	Тип	Марка	Місткість, чол	Наявні в парку
1		Газ-3204	18	14
2		Лаз-5269	90	2

3		«Богдан» А-064	17	15
4		Богдан» А-069	18	2
5		«Богдан» А-091	21	13
6		ЛАЗ-1414	38	18
7		ЛАЗ-5207	36	29
8		ГАЗ-3321	11	37
9		А-092 «Богдан»	27	31

10		ЛАЗ Лайнер-10	36	29

Табл. 2. Результати моделювання перевезень

№ п/п	Типи транспорту	Задані значення			
		1500	2000	3000	4000
1	Газ-3204(14)	4	7	9	13
2	Лаз-5269(2)	2	1	1	2
3	«Богдан» А-064(16)	2	7	9	12
4	«Богдан» А-069(2)	2	2	2	2
5	«Богдан» А-091(13)	5	5	10	12
6	ЛАЗ-1414(18)	8	8	18	18
7	ЛАЗ-5207 (29)	7	13	17	25
8	ГАЗ-3321(37)	3	3	6	7
9	А-092 «Богдан»(31)	6	9	13	18
10	ЛАЗ Лайнер-10(29)	8	14	17	26
11	Обчислені значення	1500	1968	2976	3969
12	Похибка обчислень, %	0	1.6	0.8	0.775

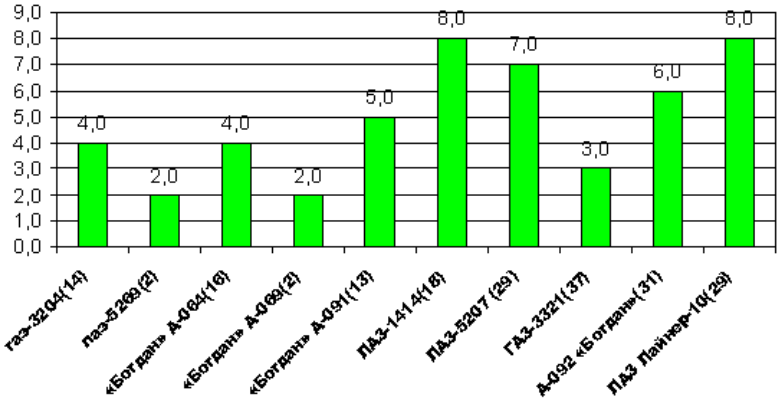


Рис.1. Транспортний кластер для маршруту на перевезення 1500 пасажирів

Застосування пропонованої моделі (1) для задачі планування дозволяє автоматизувати її вирішення. Результати вирішення

задачі дають можливість приймати рішення про способи обслуговування маршрутів на основі наявного парку транспорту. Оскільки рішення задачі можуть містити багато варіантів, то вони можуть розглядатись як кластери, обчислені за однаковим критерієм-кількістю перевезень. Автоматизація вирішення даних задач дає змогу формалізувати процес планування. Економічний ефект полягає у автоматизації рутинних робіт з перебору великої кількості варіантів задачі.

1. Левковець П.Р. Управління перевезеннями вантажів і логістика / П.Р. Левковець, Д.Л. Товкун. – К. : Вид-во НТУ, 2002. – 146 с.
2. Крикавський Є.В. Логістика в стратегії економічного розвитку / Є.В. Крикавський. – Львів: Вид-во НУ «Львівська політехніка», 2002. – 67 с.
3. Федорчук Є.Н. Алгоритми і технології пошуку кластерів на основі оптимізаційних критеріїв для товарних баз даних / Є.Н. Федорчук // Вісник Національного університету «Львівська політехніка». – Сер.: Комп'ютерні системи проектування. Теорія і практика. – Львів : Вид-во НУ «Львівська політехніка». – 2007. – Вип. 591. – С. 48-52.

МІЖНАРОДНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ НАСЕЛЕННЯ В СФЕРІ КОНТРОЛЮ ЗА ЗАСТОСУВАННЯМ ВОГНЕПАЛЬНОЇ ЗБРОЇ

Хомин Оксана Йосипівна,
професор кафедри соціальних дисциплін
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент

Для забезпечення безпеки населення у населених пунктах від можливого несанкціонованого використання зброї в багатьох містах світу використовують засоби, що дозволяють вчасно реагувати на певні дії. Як приклад, розглянемо систему ShotSpotter, що використовується в США та визначимо її ефективність та вкажемо на необхідність використання в роботі органів внутрішніх справ України.

Зазначимо, що питанням адекватного реагування за допомогою технічних засобів на постріли в населених пунктах займаються спеціалісти ще з часів Першої світової війни в Європі та США.

Рис. 1. Принцип встановлення системи Shot Spotter в населеному пункті.

В багатьох місцях правоохоронні органи стикаються з проблемою, удосконалення оперативності реагування на застосування зброї. В зв'язку з тим, що придбати зброю можна у багатьох країнах легально, вона стала доступною широким масам населення. Ця обставина і є вагомою причиною того, що працівники

поліції мають більш відповідально ставитися як до попередження злочину, так і до боротьби зі злочинцями, що незаконно її застосовують. При цьому, одним з найскладніших завдань з якими зустрічаються поліцейські є миттєве виявлення, розпізнавання типу вогнепальної зброї, встановлення її місця несанкціонованого використання.

Застосування технічної системи збору інформації типу ShotSpotter дозволяє департаменту поліції використовувати свої існуючі ресурси більш стратегічно. Це дає можливість добиватися кращих результатів у забезпеченні безпеки населення певного населеного пункту.

За принципом своєї роботи дана система використовує два методи виявлення, розпізнавання та становлення місця пострілу.

1. Базисний метод пеленгації звукових хвиль. Використовує стаціонарні пости мікрофонів. Недоліком цього методу є відбиті сигнали від будинків у великих містах.

   На рисунку 1 зображено принцип встановлення системи ShotSpotter та показано особливості виявлення та дислокації порушника-стрілка за допомогою чотирьох сенсорів-реєстраторів.
2. Роізницево-часовий метод пеленгації моменту пострілу. Використовує стаціонарні пости мікрофонів та камер відеоспостережень. Недоліком цього методу є те, що зброя, яка вистрелила, повинна попасти в поле огляду камери.

Стаціонарний пост (Рис.2.) ShotSpotter збору інформації про порушення громадської безпеки укомплектований звуковим сенсором та сенсором відеореєстрації пострілу.

Рис.2. Стаціонарний пост ShotSpotter збору інформації.

ShotSpotter постійно вдосконалюється і є новітньою технологією забезпечення безпеки населення.

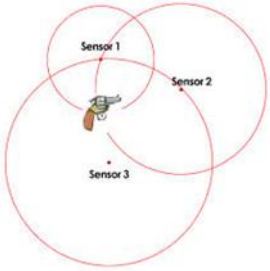


Рис. 3. Реєстрація звуку пострілу трьома сенсорами

В сучасних умовах складність роботи поліції полягає в тому, що в населених пунктах населення використовує різного роду світлові піротехнічні засоби, які видають звуки дуже подібні до вистрілу з вогнепальної зброї. На певній відстані, особливо в міській місцевості, де звукові сигнали мають можливість відбиватися від будівель відрізнити окремі піротехнічні засоби від одиночного вистрілу з вогнепальної зброї без спеціальних технічних засобів, навіть досвідченому поліцейському не завжди вдається, а с особливо, коли час в оперативних умовах є обмежений.

Система ShotSpotter складається з встановлених декількох (не менше трьох Рис.3.) мікрофонів та відеокамер, що дозволяють провести моніторинг звукових хвиль та виокремити постріли з вогнепальної зброї від інших подібних їм за звучанням звуків за допомогою розробленого алгоритму та відповідного програмного забезпечення.

Рис. 4. Прийнята та зареєстрована інформація системою ShotSpotter.

На Рис.4. і 5. зареєстрований і розпізнаний звуковий сигнал пострілу із автоматичним розпізнаванням виду зброї, встановленням адреси, координат на карті, дати та часу з точність до долі секунди.

Рис.5. Під час прийняття оперативного рішення.

В разі фіксування ShotSpotter-ом стрілянини інформація передається до моніторингового центру збору інформації, яка працює в цілодобовому режимі в містах. Результати передаються до відома місцевим поліцейським (Рис.6.). Вся процедура займає приблизно 30 секунд. Це набагато швидше, ніж можлива інформація надходить від випадкових свідків, що можуть подзвонити набравши 911, а отже поліцейський відділок може отримати інформацію значно швидше, оскільки все відбувається в автоматичному режимі.

Рис. 6. Під час чергування отримана інформація про постріл з фіксуванням його місця на карті.

Таким чином автоматизовані системи збору оперативної інформації широко використовують в багатьох розвинених країнах. Система ShotSpotter застосовується приблизно десять років в міських районах з високим рівнем злочинності і поблизу військових баз, в США і в інших країнах.

В США задумуються про впровадження цієї системи в школах та інших закладах, де може бути стрілянина.

Представники компанії, що випускають ShotSpotter стверджують, що система гарантує анонімність приватного життя, через кожні два дні система стирає дані реєстрації. Поліцейські підрозділи в США сподіваються, о застосування системи технології безпеки ShotSpotter – протягом найближчих десятиліть стане звичайним явищем, як пожежна сигналізація та системи пожежогасіння сьогодні. Беручи до уваги військові дії на сході нашої держави, варто було б застосовувати подібну систему забезпечення безпеки населення.

1. Офіційна веб-сторінка [Електронний ресурс]. – Режим доступу: http://www.shotspotter.com/technology
2. [Електронний ресурс]. – Режим доступу: http://www.policemag.com/channel/technology/news/2015/01/30/shotspotter-technology-in-six-new-cities-to-detect-gunfire.aspx
3. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=DBHsPwb7pmk
4. [Електронний ресурс]. – Режим доступу:http://sanfrancisco.cbslocal.com/tag/shotspotter/
5. [Електронний ресурс]. – Режим доступу:http://www.shotspotter.com/
6. [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/200850/

НОВИЙ ПІДХІД ДО ВИРІШЕННЯ ЗАДАЧІ ЕНЕРГЕТИЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТА РОЗВІДУВАЛЬНО-НАВІГАЦІЙНИХ ЗАСОБІВ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ

Шабатура Юрій Васильович,
завідувач кафедри електромеханіки та електроніки
Національної академії сухопутних військ
імені гетьмана Петра Сагайдачного,
доктор технічних наук, професор
Куценко Богдан Анатолійович,
курсант Національної академії сухопутних військ
імені гетьмана Петра Сагайдачного

Вогневе ураження живої сили і техніки противника або правопорушника є останнім аргументом в протистоянні сторін. Тому, ще задовго до цього, а особливо під час нанесення вогневих ударів особливу роль відіграють інформаційно-комунікативні та розвідувально-навігаційні дії, метою яких є збереження життя і здоров'я мирного населення, особового складу, а також військової техніки та озброєння, цивільних споруд і майна мирних громадян.

Традиційно задача енергозабезпечення підрозділів вирішується шляхом використання наступних джерел живлення: первинних джерел в основу дії яких покладені хімічні процеси, вторинних джерел на основі АКБ різноманітних конструкцій; також використовують енергоперетворення за рахунок згоряння палива у двигунах внутрішнього згорання, а саме як різноманітні мобільні бензинові та дизель генератори спеціального призначення, так і автомобільні електрогенератори.

В артилерійських підрозділах від цих принципів енергозабезпечення не відходять і по сьогодні.

«Бог війни», – саме така назва закріпилася за артилерією.

Вона актуальна і зараз, адже під час ведення бойових дій близько 85% вогневого ураження противника припадає саме на підрозділи артилерії та частково авіації.

Засобом ведення вогню в артилерії є гармати, різноманітність яких за своїми тактико-технічними характеристиками досить велика, – від причіпних гармат до ракетних систем залпового вогню. Сьогодні бойові дії на сході нашої країни показують, що причіпній артилерії відводиться важлива роль. Причіпним гарматам надають більшу перевагу в плані простоти обслуговування та надійності на полі бою. Але надзвичайно актуальним і в повній мірі невирішеним залишається питання живучості як самих причіпних артилерійських систем, так і в першу чергу військовослужбовців бойової обслуги самої гармати. Вищезгадане питання в повному обсязі пов'язане з енергопостачанням. Для прикладу, в самохідних артилерійських установках це питання не виникає, адже там енергопостачання відбувається від базового шасі. Виникає логічне питання: що робити з причіпними гарматами, які не мають свого джерела енергії?

Якщо подивитись на гармату, як на теплову машину, виявляється, що коефіцієнт корисної дії такої машини всього лише 30 – 35%. Решта енергії просто вивільняється в навколишнє середовище. Щоб якимось чином використати цю енергію потрібно зважати на те, що вивільнення цієї енергії відбувається імпульсно за досить короткий проміжок часу, окрім того пристрої для перетворення даної енергії не повинні знижувати тактико-технічні характеристики гармати.

Тому для вирішення проблеми енергопостачання причіпних гармат пропонується комплексна система термоелектричного та електромеханічного енергоперетворення. Термоелектричне перетворення буде відбуватись на основі ефекту Пельт'є. За допомогою елементів Пельт'є ствол гармати буде охолоджуватись, що дозволить забезпечувати стабілізацію початкової швидкості снаряда, відповідно частина теплової енергії згоряння порохових газів, яка спричиняє нагрівання ствола буде перетворюватись в електричну. Для другої складової комплексної системи пропонується за допомогою лінійного генератора з постійними магнітами здійснити перетворення механічної енергії відкату ствола в електричну, що в свою чергу буде частково гасити відкат

гармати при пострілі і тим самим питання постійного відновлення налаштувань прицільних пристроїв після пострілу буде вирішено.

Запропонований підхід дозволить отримувати значний обсяг електроенергії від кожного пострілу гармати і використовувати її в корисних цілях.

Створення комплексної системи термоелектричного та електромеханічного енергоперетворення, дозволить забезпечувати живленням інформаційно-комунікативні та розвідувально-навігаційні засоби артилерії навіть, якщо звичні джерела енергії вийшли з ладу, а в деяких випадках і на постійній основі, а це забезпечить надійність в плані енергозабезпечення і однозначно матиме вплив на підвищення живучості як особового складу, так і техніки. Деталі даної системи будуть розглянуті у доповіді.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ВІДНОВЛЮВАНОЇ ЕНЕРГЕТИКИ

Шабатура Юрій Васильович,
професор кафедри інформаційних технологій
Національного лісотехнічного університету України,
доктор технічних наук, професор
Мочернюк Юрій Миколайович,
магістрант Національного лісотехнічного університету
України

Розвиток індустрії та технологій призводить до виснаження ресурсного потенціалу планети, що накладає нові обмеження сферу енергетики. Зокрема виникає потреба у введенні в експлуатацію відновлюваних джерел енергії, які дають виграш з точки зору економіки та екології. Проте не слід забувати про перевагу, яку пропонує альтернативна енергетика у вигляді децентралізації джерел енергії, що дозволяє успішно підвищити ефективність роботи служб безпеки, поліції, військових відділів.

Метою доповіді є аналіз інформаційних технологій та їхнього впливу на енергетичну безпеку при використанні відновлюваної енергетики, що дозволяє не лише підвищити ефективність роботи служб безпеки в мирних час, а й покращити функціонування таких органів впродовж військового стану.

Успішна реалізація завдання вимагає використання аналітичних методів, що необхідні для аналізу наявних можливостей та перспектив в області локального програмного забезпечення, мережевого програмного забезпечення, хмарних обчислень, апаратних засобів та комплексних рішень.

Результатами проведених досліджень є зведення наявної інформації до кількох основних раціоналізованих рішень, котрі дозволять підвищити енергетичну безпеку з використанням відновлюваних джерел енергії.

Перед визначенням переваг при застосуванні інформаційних технологій в даній сфері, слід звернути увагу на доступні види альтернативних джерел енергії. До основних джерел відновлюваної енергетики відносять енергію вітру, енергію сонячного світла, гідроенергію, енергію приливів та відливів, енергію хвиль, біоенергетику та геотермальну енергію. З огляду на географічні фактори для нас найбільший інтерес матиме вітрова енергетика, сонячна фотоенергетика, сонячна теплова енергетика та біоенергетика. Кожна з цих галузей має значні перспективи для розповсюдження в Україні. Саме тому при розгляді інформаційних засобів слід орієнтуватись на ці категорії в області енергетики.

На практиці більшість альтернативних джерел енергії донедавна розглядалися суто на механічному рівні без застосування інформаційних технологій з метою оптимізації їх використання. Такий підхід дозволяв успішно контролювати процеси перетворення енергії в межах однієї чи декількох споруд. Проте при плануванні та розробці глобальних систем цей підхід вичерпував свої можливості. Виникали проблеми у вигляді складності контролю, передачі енергії, збереження та аналізу статистичної інформації і т.п. Тому набув поширення підхід до локалізованого керування системами на базі альтернативних енергетичних рішень. Ця методологія розпочала перехід в глобалізовані рішення на базі хмарних технологій, та інтернету речей (Internet of Things – IoT). В області відновлюваної енергетики цей підхід і є найбільш перспективним. Його ідея полягає в тому, що більшість вузлів технологічних процесів та оточуючих предметів були оснащені вбудованими мікрокомп'ютерами та наборами сенсорів. Таким чином в них з'явиться можливість отримувати, аналізувати, обробляти та передавати оброблену інформацію централізованим вузлам, які можуть бути частинами більших мереж з основним обчислювальним вузлом. Більше того в таких пристроїв з'явиться можливість координувати свою діяльність на основі отриманої інформації з хмарних датацентрів. Одним з прикладів таких систем на побутовому рівні є концепція «розумного будинку», так поширеного у країнах Європи. Подібним чином такі системи можна адаптувати

до потреб відновлюваної енергетики. Для втілення такого підходу у реальність існує цілий ряд технологій. Сюди слід віднести:

- Сенсори – використовуються для відслідковування зміни параметрів навколишнього середовища чи стану певного елемента.
- RFID (Radio-Frequency Identification) – чипи, GPS-модулі, NFC (Near Field Communication) – чипи, QR-коди. Ці технології слугують для ідентифікації певних об'єктів, аналізу їхнього стану.
- Для обробки інформації, отриманої з сенсорів використовуються недорогі та економні вбудовані комп'ютери. Одним з найпопулярніших рішень в цій сфері є лінійка Raspberry Pi на базі архітектури ARM.
- Засоби для обміну інформацією: бездротові мережі.
- Хмарні операційні системи реального часу.
- Датацентри для обробки, збереження отриманої інформації та формування статистики.

Реалізація систем на основі IoT стає реальною завдяки розвитку інформаційної індустрії, виникнення нанотехнологій, вдосконалення напівпровідникового технологічного процесу. Це призводить лише до позитивних результатів на зразок економічного росту, підвищення швидкодії обчислювальних пристроїв, збільшення швидкості передачі даних, пропускної здатності та покращення енергозбереження.

Поява хмарних технологій дозволила також збільшити роль клієнтів в мережевих технологіях, таким чином реалізуючи принцип децентралізації. З точки зору безпеки таких підхід є досить цінним.

Ще одним важливим кроком, який фігуруватиме в еволюції IoT для сфери відновлюваної енергетики це залучення розширеної аналітики для аналізу наявної інформації та покращення результатів діяльності таких систем, а також технології машинного навчання. Реалізація власної екосистеми в цій сфері може бути вельми затратним процесом з фінансової точки зору, проте ця сфера ще досить молода і перспективи її значні. Окрім того, на ринку присутні деякі цілісні рішення від деяких компаній. Явними лідерами в цій сфері є такі компанії як Intel, Cisco та ARM.

Практична цінність роботи полягає в пропозиції інформаційних засобів, котрі дозволять оптимізувати роботу органів внутрішніх справ в сфері енергетичної безпеки та вирішити ряд проблем пов'язаних з енергетичною кризою та екологічним занепадом.

1. [Електронний ресурс]. – Доступний з http://www.uiis.com.ua /sunenergy/photo_electric_systems/70/
2. [Електронний ресурс]. – Доступний з https://en.wikipedia.org/wiki /Renewable_energy
3. [Електронний ресурс]. – Доступний з https://uk.wikipedia.org/wiki /Сонячна_енергетика
4. [Електронний ресурс]. – Доступний з http://www. renewableenergyworld.com/articles/2015/09/the-future-of-the-internet-of-things-in-renewable-energy0.html
5. [Електронний ресурс]. – Доступний з https://en.wikipedia.org/wiki /Internet_of_Things

ІНФОРМАЦІЙНА СИСТЕМА АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ ТА АНАЛІЗУ АТМОСФЕРНОЇ ДИНАМІКИ З ВРАХУВАННЯМ ЛАНДШАФТУ ТЕРИТОРІЇ

Шабатура Юрій Васильович,
професор кафедри інформаційних технологій
Національного лісотехнічного університету України,
доктор технічних наук, професор
Шевчук Роман Васильович,
магістрант Національного лісотехнічного університету
України

Атмосферні явища представляють собою важливий елемент погоди: від того чи йде дощ або сніг, чи відмічається туман або пилева буря, чи бушує заметіль або гроза, в значній мірі залежить як сприйняття поточного стану атмосфери живими створіннями (людина, тварини, рослини), так і вплив погоди на розміщені під відкритим небом машини і механізми, будівлі, дороги.

Роль атмосферних явищ і кліматичних факторів у формуванні мікроклімату житлових і промислових будівель, а також оцінка їхнього впливу на живих створінь і будівлі завжди вважалась важливим питанням. Дослідження аеродинаміки будівель має велике значення для розрахунку і оцінки впливу будівлі на аеродинаміку інших будівель на території її розміщення, а також для проектування вентиляції будівлі. Аналіз атмосферної динаміки, а саме вітрових потоків на забудованій території також дозволяє визначити місця у яких утворюються снігові замети, місця скупчення легких відходів антропогенного та природнього походження і місця розсіювання шкідливих речовин навколо будівель промислового типу, що дає можливість передбачити безпечне і оптимальне місце для побудови нових будівель довільного типу, місця розміщення пішохідних доріжок і забезпечення безпечних умов для переміщення і перебування людей.

Метою роботи є комп'ютерне моделювання і аналіз впливу вітрових потоків на формування снігових заметів і легких

відходів різного типу походження на заданій забудованій території. Моделювання вітрових потоків надає можливість контролювати місця їх скупчення шляхом встановлення різного виду загороджень, спеціальних конструкцій чи снігозатримних насаджень які дозволять унеможливити або мінімізувати снігозанесення у небажаних місцях.

В роботі було використано моделювання з використанням сучасних пакетів для обчислювальної аеродинаміки які дозволяють достовірно відтворити моделі реальних об'єктів і реалістично відтворити вітрову динаміку навколо них. Розроблена інформаційна система має наступний принцип роботи:

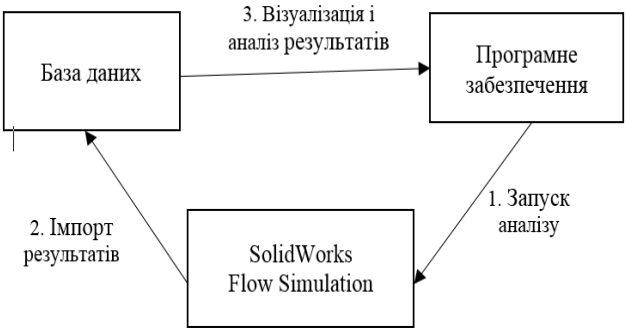


Рис.1. Схема принципу роботи розробленої інформаційної системи.

Вітрові потоки які утворюються навкруги будівель є дуже турбулентними і складними. Фундаментальні рівняння які відповідають руху стійких, нестисливих і турбулентних потоків є усередненням між рівняннями Нав'є-Стокса і рівнянням неперевності і можуть бути виражені наступним чином:

$$\frac{dU_i}{dx_i} = 0$$

$$U_j \frac{\partial U_i}{\partial x_i} = -\frac{1}{\rho}\frac{\partial P}{\partial x_i} + \frac{\partial}{\partial x_j}[v\left(\frac{\partial U_i}{\partial x_j} + \frac{\partial U_j}{\partial x_i}\right) - \overline{u'_i u'_j}$$

Турбулентні напруження $\overline{u'_i u'_j}$ є важливими термінами, що відповідають за турбулентну дифузію і вони повинні бути визначені для повноцінності даної турбулентнії моделі. Вони враховують додаткові втрати і перерозподілення енергії в турбулентному потоці. В використаному для моделювання

програмному забезпеченні – SW FlowSimulation використовуються рівняння Нав'є-Стокса усереднені по Рейнольдсу – RANS[3].

Результатом проведених дослідження є приклад моделювання певної забудованої території і аналіз впливу вітрових потоків поруч з цими будівлями для передбачення місць утворення снігових заметів і легких відходів природнього та антропогенного походження.

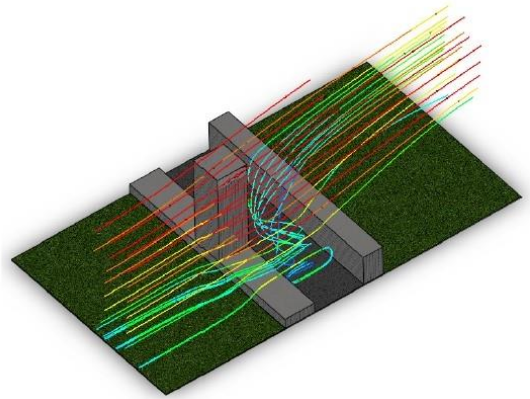


Рис.2 Візуалізація вітрових потоків навколо будівлі

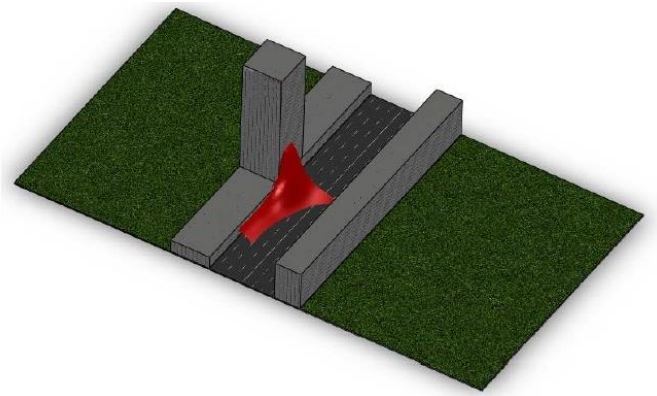


Рис.3 Місце найбільш ймовірного скупчення отримане за допомогою діаграми ізоповерхонь

У підсумку можна зробити висновок про те, що комп'ютерне моделювання вітрових потоків навколо будівель на заданій

території дозволяє отримати корисні і реалістичні результати які допомагають прогнозувати місця утворення і розміщення снігових заметів, місць накопичення інших легких відходів антропогенного та природнього походження, місця розсіювання шкідливих речовин навколо будівель промислового типу, а також дає можливість впливати на формування місць їх утворення шляхом встановлення спеціальних конструкцій і відповідно дає можливість передбачити безпечне і оптимальне місце для побудови нових будівель довільного типу, місця розміщення пішохідних доріжок і забезпечення безпечних умов для переміщення і перебування людей.

1. Реттер Э. И., Стриженов С. И. Аэродинамика зданий. М., 1968.
2. Launder, B.E. and Spalding, D.B. (1974), «The Numerical Computation of Turbulent Flows», Computer Methods in Applied Mechanics and Engineering.
3. [Електронний ресурс] – Доступний з http://ru.wikipedia.org/wiki/RANS.

РОЗДІЛ 3.
НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ ПРОЦЕСІ

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛІЗОВАНИХ СИСТЕМ НАВЧАННЯ НА ЗАНЯТТЯХ З ІНОЗЕМНОЇ МОВИ

Бондаренко Вікторія Анатоліївна,
доцент кафедри іноземних мов
Львівського державного університету внутрішніх справ,
кандидат юридичних наук

Учені багатьох країн світу приділяють особливу увагу галузі сучасних технологій та розробляють нові концепції їх використання у процесі навчання, що зумовлює підвищений інтерес до практики вивчання іноземних мов. Відомий психолог О. Тихомиров [1] визначає, що використання комп'ютерної техніки викликано суспільними потребами, але і при комп'ютеризації насамперед йдеться про людину та суспільство, в якому вона знаходиться.

На думку Г. Козлакової [5], термін «Інтелектуалізовані системи навчання» (ІСН) використовується серед пізнавальних наук і означає звернення до комп'ютерних програм, які можуть навчати інтелектуально. Проте слід зазначити, що термін ІСН має певні обмеження: чинна ІСН не виявляє тих якостей, які має найкращий репетитор-людина. Незважаючи на слово «інтелектуалізована» у назві системи і високу мету її призначення, нинішні ІСН більш скромно і просто розглядаються як розробки з використанням комп'ютерних технологій (КТ) для конкретизації або формалізації теорії навчання, а також як експериментальні засоби для вивчення природи процесів навчання і викладання.

Бужиков Р. відзначає,що інтелектуалізовані системи навчання – це системи індивідуально орієнтованої навчальної діяльності, які пов'язані зі швидким розвитком штучного інтелекту або «інтелектуальним продуктом людської діяльності» та сучасними інтерактивними методами навчання. «Інтелектуальний продукт людської діяльності» – це таке розмаїття виражальних засобів аудіовізуальних джерел інформації, як відеокурси, педагогічне програмне забезпечення (ППЗ), електронні видання, Internet-технології, що дають змогу використовувати їх потенційні можливості для створення зорових, слухових та зорово-слухових образів як основи для формування чітких уявлень і наукових понять [2].

О.Тихомиров вважає, що використання інтелектуалізованих систем навчання як засобу пізнання людини означає появу нових форм мислення, мнемічної, творчої діяльності, що можна розглядати як фактор історичного поступу психічних процесів людини. Застосування ІСН сприяє формуванню таких якостей, як потяг до експериментування, гнучкість, увага. При цьому створюються можливості нового нетрадиційного сприймання фактів, встановлення зв'язків між новою та старою інформацією.

Інтелектуалізовані системи навчання надають принципово нові можливості для організації та подання навчального матеріалу. Це пов'язано з появою лазерних відео-дискових програвачів, цифрових синтезаторів звуків, графічних редакторів, екологічних екранів з високою чіткістю зображення. Прорив через комп'ютеризацію різноманітних видів діяльності, викликаний розвитком Multimedia-технологій (графіка, анімація, фото, відео, звук, текст в інтерактивному режимі роботи), створює інтегроване інформаційне середовище, в якому користувач набуває нових можливостей.

Зрозуміло, що застосування ІСН у навчальному процесі призвело до зміни засобів організаційних форм навчання. Є можливість використання, залежно від бажання студента, різних електронних довідників, ілюстративного матеріалу, методичних порад. Можна всіляко варіювати самостійну діяльність студента; включення його в процес мислення та засвоєння нових знань відбувається за умов безпосереднього спілкування з комп'ютером; існує можливість візуалізації не тільки безпосередньо

отриманого результату, а й всього ходу мислення; інтелектуалізовані технології можна використати в різних формах управління навчальною діяльністю. Саме штучний інтелект може виступати як пасивним елементом, так і активним, все залежатиме від того, яку роль для нього відведено користувачем; виникають різні нові форми організації навчання: дистанційне навчання, електронні конференції, електронна пошта. Звідси виникають питання, пов'язані з комп'ютерною грамотністю, яка включає в себе знання нових інформаційних технологій та їх функціонування; умови більш ефективного застосування інтелектуалізованих технологій; обов'язкове знання мережі Інтернет та уміння працювати в ній; вміння застосовувати комп'ютери в усіх галузях людської діяльності; знання алгоритмічних мов та уміння їх практичного застосування; уміння працювати з програмними продуктами, в тому числі і з текстовими редакторами; знання архітектури комп'ютера.

У сучасних умовах інтелектуалізації усіх сфер людської діяльності перед фахівцями у галузі навчання іноземних мов, які завжди сприймали різного роду технічні засоби як органічну складову процесу викладання, постають нові завдання. В.Ізвозчиков [3], зокрема, відмічає, що використовуючи ЕОМ, мовознавець може автоматизувати трудомісткі, але найнеобхідніші для його наукової і навчальної діяльності операції. Укладання словників, алфавітних і частотних, підготовка дидактичного матеріалу для навчання орфографії, пунктуації, лексиці, граматиці – це вже зараз може взяти на себе ЕОМ. Для вивчення мов розроблено системи обробки текстів. Посилюється мотивація навчання – студент не боїться зробити помилку, оскільки комп'ютер відразу ж показує її, а тому можна більш уваги приділити смисловим та стилістичним моментам при написанні певних робіт.

Використання ІСН сприяє реалізації найважливішої вимоги комунікативної методики – вдосконалення процесу оволодіння іноземною мовою. Великою перевагою ІСН є їх емоційний вплив на студентів, що спонукає спрямовувати увагу на формування особистісного ставлення до побаченого. Успішне досягнення такої цілі можливе лише за умови систематичної роботи з формування основ інформаційної та духовної культури молоді.

У процесі викладання іноземних мов широко вживається педагогічна технологія, яка розкриває можливості використання

(hypermedia), запропонованці мультимедійним комп'ютером, з одночасним доступом до будь-якої кількості текстів, графічної інформації, аудіо-, фото-, та відеофайлів. Ця технологія знімає проблему поєднання відео з іншими засобами: вся інформація може бути представлена на одному екрані. Цифрове відео розкриває перед користувачами ще більші можливості: кожен кадр може бути легко вибраний та опрацьований, окремі уривки – детально розглянуті, візуальна інформація – ретельно проаналізована. Таким чином, мультимедійний комп'ютер одночасно надає доступ до різноманітних вправ і різних додаткових матеріалів. Виконуючи вправи, студенти можуть використовувати субтитри, транскрипції, словники, а також файли з додатковою інформацією культурного, історичного, лінгвістичного характеру. Застосовуючи цю технологію, можна самостійно й легко обрати потрібний рівень мовної підтримки, мати доступ до великої кількості джерел, що дають додаткову інформацію, використовувати інтерактивну відеорозповідь, котра стимулює їх до використання власного мовного досвіду. Отже, відео має великий вплив на мотивацію навчання, оскільки підвищує активність студентів, спонукає їх до використання засвоєного мовного матеріалу в конкретних комунікативних ситуаціях. Викладачі іноземної мови можуть використовувати цю технологію для створення завдань з різних видів мовленнєвої діяльності.

Бужиков Р. пропонує використовувати різноманітні завдання для навчання читання, письма, аудіювання, говоріння [2].

Для навчання читання можна створити вправи з формування лексичних і граматичних навичок читання та розвитку вмінь читання; давати відповіді на запитання вчителя щодо основного змісту тексту та його деталей; підбирати з кількох малюнків ті, які ілюструють провідну думку тексту; складати план тексту; виконувати письмовий переклад тексту і порівнювати його з ключем; виконувати тести.

Для навчання письма можна складати вправи на формування мовленнєвих навичок письма та розвиток вмінь письма: давати відповіді на запитання щодо змісту тексту, складати запитання і план до тексту, робити переказ за планом; писати резюме до тексту і його переказ; описувати малюнок, складати

діалог за темою. Доцільно розробити вправи на трансформацію мовного зразка і на підстановку.

Для навчання аудіювання можна розробити комунікативні вправи на аудіювання текстів з метою одержання інформації, вправи на аудіювання повідомлень, запитань, вправи на контроль розуміння прослуханого тексту.

Для навчання говоріння – вправи з формування вмінь діалогічного та монологічного мовлення.

Нові технології створили базис для докорінних змін у педагогічних і освітніх методиках. Навчання за підтримкою ІСН надає додаткову цінність освіті, забезпечує швидку взаємодію і зворотній зв'язок, моделювання в реальному масштабі часу, пошук інформації та її подання у зручній для розуміння і обробки формі. Зв'язок через Інтернет дає можливість студентам співпрацювати з колегами, іншими людьми під час вивчення і вирішення конкретних проблем, у дослідженні нових засобів зв'язку і доступу до інформації, у розвитку навичок групової наукової і професійної діяльності. ІСН надають можливість широко розповсюджувати співробітництво в навчанні як на рівні студентів, так і на рівні взаємодії викладача зі студентом.

1. Специфика психологических методов в условиях использования компьютера / Арестова О.Н., Бабанин Л.Н., Войскунский А.Е. / Под ред. О. К. Тихомирова; МГУ им. М. В. Ломоносова, Фак. психологии. – М. : Изд-во МГУ, 1995. – С. 109.
2. Бужиков Р. П. Педагогічні умови застосування інноваційно-комунікаційних технологій на заняттях з іноземної мови на економічних факультетах / Р. П. Бужиков // Вища освіта України. – 2006.— № 1 (додаток). – С. 134–141.
3. Дидактические основы компьютерного обучения: Межвуз. сб. научн. тр./ ЛТИ им. А. И. Герцена; Редкол.: В.А. Извозчиков (отв. ред.) и др. – Л., 1989. – 204 с.
4. Жовнірук З. Л. Застосування комп'ютерних технологій на заняттях з іноземних мов у вузі / З. Л. Жовнірук, Г. Т. Ісаєва // Лінгвометодичні концепції викладання іноземних мов у немовних вищих навчальних закладах України. – К., 2003. – С. 244–251.
5. Козлакова Г. О. Інформаційне програмне забезпечення дистанційної освіти: зарубіжний і вітчизняний досвід. Монографія / Г. О. Козлакова. – К. : Просвіта, 2002. – 231с.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ВИКЛАДАННІ СОЦІАЛЬНИХ ДИСЦИПЛІН У ВИЩІЙ ШКОЛІ

Йосифович Данило Ігорович,
завідувач кафедри соціальних дисциплін
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент
Ревак Ірина Олександрівна,
професор кафедри соціальних дисциплін
Львівського державного університету внутрішніх справ,
кандидат економічних наук, доцент

Інформатизація суспільства – це глобальний соціальний процес, особливість якого полягає в тому, що домінуючим видом діяльності в сфері суспільного виробництва є збирання, нагромадження, продукування, оброблення, зберігання, передавання та використання інформації.

Значення інформатизації важко переоцінити, адже саме вона сприяє забезпеченню національних інтересів, розвитку наукомістких виробництв та високих технологій, зростанню продуктивності праці, підвищенню комп'ютерної грамотності, розвитку інтелектуального потенціалу та вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства; розвитку культури спілкування тощо.

Виникнення та розвиток інформаційного суспільства припускає широке застосування інформаційно-комунікаційних технологій (ІКТ) в освіті, зокрема при викладанні соціальних дисциплін, що визначається багатьма чинниками.

По-перше, впровадження ІКТ в сучасну освіту суттєво прискорює передавання знань і накопиченого технологічного та соціального досвіду людства не тільки від покоління до покоління, а й від однієї людини до іншої.

По-друге, сучасні ІКТ, підвищуючи якість навчання й освіти, дають змогу людині успішніше й швидше адаптуватися до навколишнього середовища, до соціальних змін. Це дає кожній

людині можливість одержувати необхідні знання як сьогодні, так і в економіці знань.

По-третє, активне й ефективне впровадження інформаційних технологій при викладання соціальних дисциплін є важливим чинником створення нової системи освіти, що відповідає вимогам інформаційного суспільства і процесу модернізації традиційної системи освіти.

У вищій освіті інформатизація відкриває доступ до світових інформаційних ресурсів; зменшує залежність викладання і навчання від місцезнаходження учасників процесу; прискорює глобалізацію; сприяє удосконаленню форм і змісту навчального процесу, підвищенню ефективності засвоєння навчального матеріалу та індивідуалізації навчання, інтеграції навчальної, дослідницької та виробничої діяльності; значно збільшує обсяг ресурсів, якими студенти можуть користуватися за межами аудиторії; сприяє підвищенню мотивації до навчання та розвитку креативного мислення. Інтерактивність і мультимедійна наочність сприяють кращому представленню, і, відповідно, кращому засвоєнню інформації при викладання соціальних дисциплін.

Водночас у науково-методичній літературі недостатньо уваги приділяється питанням, що стосуються критеріїв визначення доцільності використання ІКТ при викладанні соціальних дисциплін в цілому, або під час вивчення окремих тем. На практиці ІКТ безпосередньо використовуються на різних етапах підготовки та проведення навчальних занять. Викладачам соціальних дисциплін доволі часто доводиться адаптувати різні навчальні посібники до конкретних умов навчання та освітніх потреб слухачів, а також розробляти власні навчальні матеріали для практичного застосування студентами засвоєних знань. Сучасні комп'ютерні технології дають змогу не лише виконувати ці завдання ефективніше, а й створювати навчальні та методичні матеріали різного ступеня складності, починаючи від розробки навчальних і робочих програм та завершуючи проблемними та проектними завданнями, створенням веб-сторінок. дистанційних курсів тощо. Переважна більшість матеріалів створюється за допомогою спеціалізованих освітніх електронних ресурсів та комп'ютерних програм загального призначення.

Сучасний етап розвитку педагогічних технологій обумовлений багатьма чинниками, серед яких можна виділити: широке розповсюдження складних професійно-орієнтованих інформаційних систем, що постійно удосконалюються; швидке поширення та проникнення ІКТ у всі сфери діяльності.

Сучасні інформаційно-комунікаційні технології передбачають використання педагогічних програмних засобів, які можуть містити такі модулі: електронна бібліотека, електронний підручник, посібник, електронний довідник, тренажерний комплекс (комп'ютерні моделі, конструктори й тренажери), електронний лабораторний практикум, комп'ютерна тестуюча система тощо.

Суть інформатизації освіти складають структуризація професійних знань в заданих предметних областях і забезпечення вільного доступу студентів до баз даних. Процес навчання має бути спрямованим не на вміння працювати з певними програмними засобами, а на технології роботи з різною інформацією: аудіо- та відео-, графічною, текстовою, табличною. Важливо, щоб навчальні програмні продукти не перетворювались на аналоги існуючих підручників. Особливо доцільним є використання інформаційних технологій для вивчення процесів і явищ, які не піддаються візуальному дослідженню.

Використання засобів електронної комунікації є особливо цінним для вивчання соціальних дисциплін завдяки залученню до навчального процесу комунікації в реальних умовах. Варто зазначити, що загальнодоступні засоби електронної комунікації (чати, форуми, електронна пошта тощо) широко використовуються у навчальних цілях, водночас спеціалізовані комунікаційні освітні ресурси надають безпечне, недоступне для сторонніх осіб освітнє середовище. Віртуальні навчальні середовища, або системи управління навчальними курсами, зазвичай орієнтовані на універсальні освітні задачі й потреби навчального закладу в цілому. Саме ці ресурси є найдорожчими освітніми продуктами. Одне з таких навчальних середовищ — MOODLE (http://moodle.org), яке надає змогу вирішувати такі питання: створення навчальних курсів, завдань та вправ шляхом використання власних програмних засобів навчання, а також матеріалів, створених за допомогою інших програм (наприклад, SMART Notebook); управління

навчальною діяльністю учня; контроль виконання студентом завдань; створення умови для навчального спілкування тощо.

Разом з позитивними рисами інформатизації освіти, зокрема при викладанні соціальних дисциплін (підвищення ролі знань, глобалізація свідомості тощо), активно досліджуються і негативні (залежність від Інтернету, послаблення соціальних зв'язків та посилення соціальної відокремленості) соціокультурні умови і наслідки інформатизації. Загалом інформатизація освіти викликає інформаційне перевантаження, сприяє формуванню компонентів інформаційної диспозиції, інтерналізації (засвоєння цінностей до такої міри, що вони визначають поведінку особистості) та екстерналізації інформаційних цінностей. Внаслідок цього може виникнути новий тип відчуження, а саме відхід людини від реальності та занурення у віртуальний світ; підвищення рівня агресії через вплив агресивних комп'ютерних ігор; соціальну самоізоляцію адепта мережі, створення комп'ютерних вірусів, хакерство тощо.

Отже, при викладанні соціальних дисциплін використання сучасних інформаційних технологій забезпечує:

- інтеграцію – процес створення системи випереджаючої освіти;
- поєднання класичних принципів фундаментальної підготовки з ефективними сучасними інноваційними освітніми моделями;
- модифікацію змісту діяльності викладача, що передбачає високий рівень відповідної підготовки та створення у вищих навчальних закладах потужної інформаційної інфраструктури з розвиненим інформаційно-комп'ютерним навчальним середовищем;
- зміну парадигми освіти від «освіти на все життя» до «освіти протягом життя»;
- аксіологічний (ціннісний) підхід, зокрема, до оцінювання знань;
- творчий похід до навчання: нові знання повинні створюватися спільно, а не просто «передаватися» студентам від викладачів;
- глобальний підхід до навчання – спільні інтереси, допитливість і прагнення вчитися сприяють розширенню знань тих, хто навчається.

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РОЗПОДІЛЕНОЇ БАЗИ ДАНИХ «БОТАНІЧНИЙ САД НЛТУ УКРАЇНИ»

Коширець Світлана Іванівна,
доцент кафедри інформаційних технологій
Національного лісотехнічного університету України,
кандидат технічних наук
Бичинюк Ігор Васильович,
викладач кафедри інформатики
Львівського державного університету внутрішніх справ
Бичинюк Оксана Василівна,
магістрант Національного лісотехнічного університету
України

Актуальність роботи. Для ведення колекційного фонду ботанічного саду, зокрема Національного лісотехнічного університету України, існують програмні продукти, які дозволяють виконувати деякі операції з даними, крім того, вони не розраховані на віддалений доступ і можуть використовуватись лише однією людиною одночасно. Тому актуальною є розробка бази даних та користувацького додатку, які б дозволяли, використовуючи можливість клієнт-серверних баз даних, здійснювати доступ до віддаленого серверу, що містить потрібну інформацію, опрацьовувати її та здійснювати візуалізацію за певними критеріями, виводити статистичні дані, уникнувши некомп'ютеризованого опрацювання інформації. Базуючись на вищесказаному, актуальним є розроблення математичного і програмного забезпечення розподілених баз даних «Ботанічний сад НЛТУУ»

Об'єкт дослідження – колекційний фонд Ботанічного саду державного значення Національного лісотехнічного університету України.

Предмет дослідження – способи та методика ведення каталогів рослин колекційного фонду, з метою їх доповнення, коригування та візуалізації потрібних даних, способі введення

обліку продажів та статистичних даних бухгалтерією саду, способи обробки інформації двома відділами одночасно.

Мета роботи (проекту) – побудова розподіленої бази даних для колекційного фонду Ботанічного саду державного значення Національного лісотехнічного університету України. Дана база даних та користувацький додаток можуть бути використані як працівниками ботанічного саду, бухгалтерії так і в навчальному процесі студентами відповідних спеціальностей.

Математична модель. Прибуток є одним з основних фінансових джерел розвитку даного ботанічного саду, науково-технічного удосконалення його матеріальної бази та всіх форм інвестування. Він служить джерелом сплати податків. Враховуючи значення прибутку, вся діяльність відділу бухгалтерії спрямована на те, щоб забезпечити зростання його величини або принаймні стабілізувати її на певному рівні. Для ведення обліку продажу саджанців, доцільно дослідити можливі значення прибутку на найпростішій моделі:

$$p \circ Q - Q \circ V - F = C, \qquad (1)$$

де p – ціна; Q – обсяг продажу; V – змінні витрати на одиницю продукції; F – фіксовані витрати; C – прибуток. Тут ціна виступає в ролі операційної змінної, тобто ми маємо можливість змінювати її.

Алгоритм реалізації. Було ознайомлено з методикою ведення колекційного фонду працівниками ботанічного саду НЛТУУ [1] та ведення звітів відділом бухгалтерії. Розроблено модель бази даних та фізично реалізовано її на платформі MySQL [2, 3], яка містить таблиці, пов’язані реляційним зв’язком, та заповнена достовірною інформацією, згідно вимог спеціалістів даного профілю (рис. 1).

Для реалізації бази даних вибрано СУБД MySQL, дана база є розподіленою, володіє всіма необхідними функціями для адміністрування [4], основною перевагою є її некомерційність, що значно розширює можливість використання розробленого додатку.

Розроблено сайт (рис. 2), що дозволяє доповнювати, коригувати та видаляти дані таблиць, візуалізовано дані за різними критеріями пошуку як однієї, так і багатьох таблиць,

пов'язаних між собою реляційним зв'язком, створювати звіти на основі оновлених даних [5].

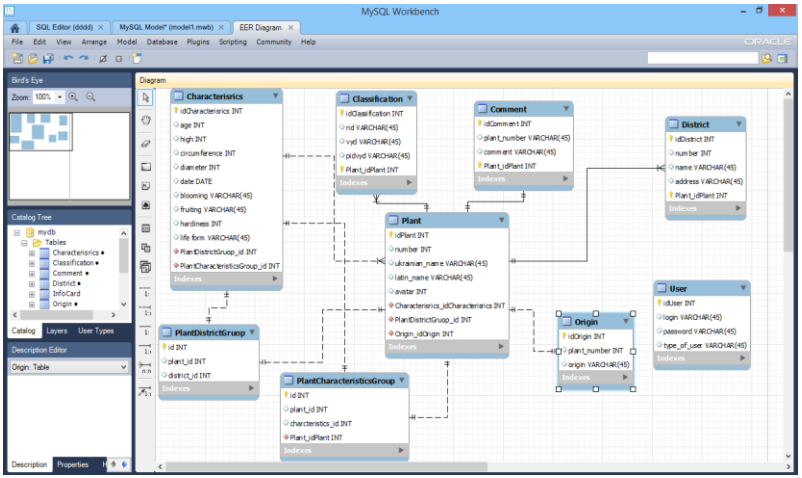


Рис. 1. – ER діаграма бази даних

Доступ до даних здійснено згідно привілеїв. Розроблено чотири рівні користувачів: адміністратор, працівник ботанічного саду, працівник відділу бухгалтерії та користувач.

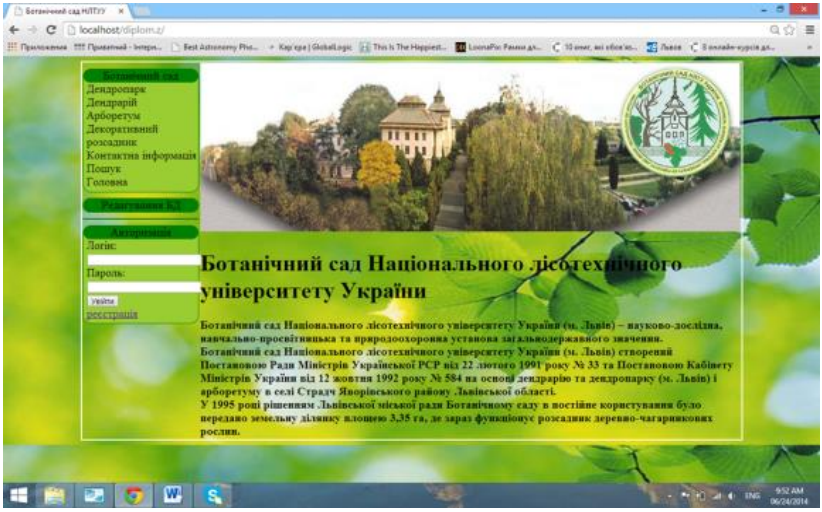


Рис. 2. Головна сторінка сайту

Основна сторінка дозволяє активувати основні функції сайту відповідно до типу користувача. Вони поділені на три блоки: «Ботанічний сад» – дає змогу візуалізувати інформацію про складові частини ботанічного саду (дендропарк, дендрарій, арборетум, декоративний розсадник), «Бухгалтерія» – дозволяє вести облік продажу саджанців та створення звітів на основі оновлених даних, «Редагування бази даних» – надає змогу отримати оновлені дані Колекційного фонду Ботанічного саду НЛТУУ, підтримувати таблиці в актуальному стані.

Крім підтримання таблиць в актуальному стані, передбачено і створення звітів на основі оновлених даних (рис. 3). Бухгалтерський відділ має доступ до певної інформації, на основі якої складаються звіти про продаж саджанців.

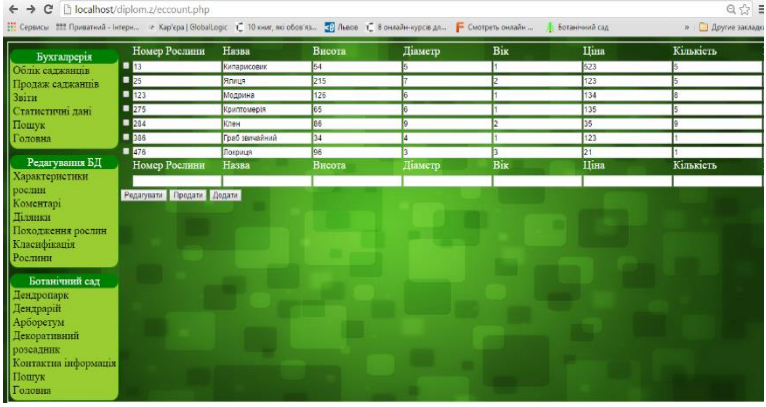


Рис. 3. Форма для підтримання даних таблиць в актуальному стані та створення звітів

Передбачено багатопотоковість, що дозволяє одночасний доступ до даних працівниками різних відділів. Працівники Ботанічного саду та відділу бухгалтерії, мають одночасний доступ до даних та можуть створювати звіти, на основі оновленої інформації. Розроблена програма є працездатною і апробованою на віддаленому кафедральному сервері, «хмарі» (рис. 4).

Використання хмарного сервісу дало змогу перенести обчислювальні ресурси й дані на віддалений сервер, що забезпечило швидку обробку даних без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури.

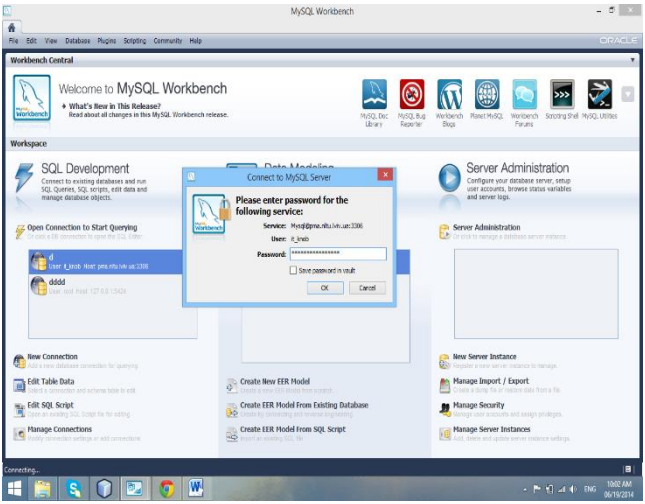


Рис. 4. Підключення до віддаленого сервера

Розроблена база даних та користувацький додаток можуть бути використані як працівниками ботанічного саду та відділу бухгалтерії, так і в навчальному процесі студентами відповідних спеціальностей.

1. Третяк П.Р. Каталог рослин Ботанічного саду Національного лісотехнічного університету України / П.Р. Третяк / Довідн. Посібник. – Львів: НЛТУ України, 2006. – 40с.
2. Кузин А.В. Базы данных: учебное пособие для вузов / А.В. Кузин. – М: Академія, 2005. – 320с.
3. Пасічник В.В. Організація баз даних та знань / В.В. Пасічник, В.А. Резніченко /. – Київ: BHV, 2006. – 383с.
4. Хомоненко А. Работа с базами данных / А. Хомоненко, С. Ададуров/. – С.Петербург: БХВ-Петербург, 2006. – 478с.
5. http://www.botsad.nltu.edu.ua/.

ОСОБЛИВОСТІ ВИВЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ НОВОЇ ПАТРУЛЬНОЇ СЛУЖБИ МВС УКРАЇНИ

Кудінов Вадим Анатолійович,
начальник кафедри інформаційних технологій
Національної академії внутрішніх справ
кандидат фізико-математичних наук, доцент

Міністерство внутрішніх справ (далі – МВС) України з січня 2015 року здійснює низку заходів щодо відбору та підготовки фахівців для нової патрульної служби МВС України в різних містах країни [1]. Так, зокрема, з січня по червень 2015 року такі заходи були проведені в м. Києві.

Під час навчання відібрані слухачі також вивчали навчальну дисципліну «Інформаційні технології» обсягом 10 н.г. Вона передбачає проведення одного лекційного та трьох практичних занять, а також іспиту. Мета дисципліни – навчити слухачів використовувати можливості сучасних інформаційних технологій у діяльності патрульної служби. Для проведення занять з цієї дисципліни були залучені фахівці у галузі інформаційних технологій Національної академії внутрішніх справ (далі – НАВС), Департаменту інформаційно-аналітичного забезпечення (далі – ДІАЗ) МВС України [2], Управління інформаційно-аналітичного забезпечення (далі – УІАЗ) ГУМВС України в м. Києві, які пройшли співбесіду з організаторами проекту по створенню нової патрульної служби МВС України.

Тематичний план дисципліни передбачає вивчення слухачами таких тем: 1. Система централізованого управління нарядами патрульної служби («ЦУНАМІ»). 2. Підготовка патруля до роботи у системі «ЦУНАМІ». 3. Управління станом виконання завдання патрулем. 4. Робота патруля з базами даних.

Для зазначених тем фахівцями ДІАЗ МВС України були розроблені мультимедійні презентації. Враховуючи відведений час та кількість слухачів в групах, іспит проводився з використанням комп’ютерних тестів, які були сумісно розроблені фахівцями НАВС, ДІАЗ МВС України та УІАЗ ГУМВС України в м. Києві.

Іспитовий білет з дисципліни **«Інформаційні технології»** (практика)

Варіант №

Група №: Дата: Прізвище: Ім'я: По батькові:

БЛОК № 1

	К-ть балів:	Отримано:
1. Налаштування планшета:	6	
2. Форма реєстрації патруля:		
Позивний: *Завдання*		
Авто: *Завдання* д/н: *Завдання*	6	
Телефон: *Завдання*		
Всього:	12	

БЛОК № 2

	К-ть балів:	Отримано:
1. Виконання патрулем завдання, яке надане диспетчером-черговим:	5	
2. Самостійне встановлення та виконання патрулем завдання:	5	
3. Перевірка патрулем журналу виконаних завдань:	2	
Всього:	12	

БЛОК № 3

Робота з картою патрулів:		К-ть балів:	Отримано:
1. Завдання	Відповідь:	6	
2. Завдання	Відповідь:	6	
	Всього:	12	

Продовження

БЛОК № 4

Робота патруля з програмою «Карта»:					К-ть балів:	Отримано:
1. Завдання	Відстань:		Час:		6	
2. Завдання	Відстань:		Час:		6	
				Всього:	12	

БЛОК № 5

Робота патруля з базами даних:			К-ть балів:	Отримано:
База даних «Особа»:				
1. Завдання	Відповідь:		2	
2. Завдання	Відповідь:		2	
База даних «Номерні речі»:				
1. Завдання	Відповідь:		2	
2. Завдання	Відповідь:		2	
База даних «Угон»:				
Завдання	Відповідь:		2	
База даних «Посвідчення водія»:				
Завдання	Відповідь:		2	
		Всього:	12	

Підпис слухача: **Всього балів за іспит:** 60

У подальшому для слухачів груп додаткового набору у серпні 2015 року до патрульної служби МВС України фахівцями кафедри інформаційних технологій НАВС були розроблені іспитові білети з дисципліни «Інформаційні технології» для оцінювання їх практичних навичок роботи на мобільному логістичному пристрої (планшеті) та зі спеціалізованим програмним забезпеченням. У листопаді 2015 року мною дані іспитові білети були успішно впроваджені у навчальний процес. Коротко опишемо особливості їх використання.

Кожному слухачу під час іспиту видається планшет та іспитовий білет, в якому він спочатку заповнює свої дані та ставить підпис. Шаблон бланку іспитового білету зображений на рисунку. Він складається з п'яти блоків завдань, кожний з яких оцінюється 12 балами.

У першому блоці слухачу необхідно виконати відповідні налаштування мобільного логістичного пристрою для його роботи та зареєструвати патруль у спеціальній формі реєстрації з урахуванням завдань. Результати показати викладачу.

У другому блоці слухачу необхідно здійснити виконання патрулем завдання, яке надається диспетчером-черговим через викладача, потім самостійно встановити собі завдання та здійснити виконання його патрулем, переглянути журнал виконаних патрулем завдань. Результати показати викладачу.

У третьому блоці слухачу необхідно виконати два завдання за допомогою карти патрулів. Результати записати до іспитового білету.

У четвертому блоці слухачу необхідно виконати два завдання за допомогою програми «Карта». Результати записати до іспитового білету.

У п'ятому блоці слухачу необхідно виконати два завдання у базі даних «Особа», два завдання у базі даних «Номерні речі», одне завдання у базі даних «Угон», одне завдання у базі даних «Посвідчення водія». Результати записати до іспитового білету.

Після виконання всіх завдань слухачі надають свої іспитові білети викладачу, який їх перевіряє з використанням таблиці відповідей та виставляє відповідні бали. Потім він отримані підсумкові бали переносить до іспитової відомості.

Для успішного виконання слухачами вище наведених завдань викладачем відповідним чином проводяться заняття. Так, зокрема, на практичних заняттях слухачі обов'язково мають можливість на планшеті самостійно виконати типові завдання з кожного блоку іспитових білетів.

Необхідно відмітити, що слухачі вивчають бази даних «Особа», «Номерні речі» та «Угон», які входять до складу Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України [3], але інформація надається їм в обмеженому вигляді.

Слід висловити подяку керівництву УІАЗ ГУМВС України в м. Києві Замислову О.С. та Андрєєву М.В., які безпосередньо провели для викладачів НАВС лекційні та практичні заняття по роботі з системою «ЦУНАМІ» на базі Центру прийняття повідомлень – служби «102» в м. Києві.

Таким чином, станом на сьогодні навчальна дисципліна «Інформаційні технології» забезпечена всіма необхідними навчально-методичними матеріалами для успішного засвоєння слухачами можливостей сучасних інформаційних технологій у діяльності патрульної служби. При цьому існує можливість оцінити їх теоретичні знання та практичні навички роботи.

Враховуючи те, що набір до нової патрульної служби МВС України сьогодні здійснюється в багатьох містах країни, вважаю, що вище наведені особливості вивчення інформаційних технологій під час підготовки фахівців для нової патрульної служби будуть корисними для всіх викладачів з навчальної дисципліни «Інформаційні технології» та слухачів.

---

1. Про затвердження Положення про патрульну службу МВС: Наказ МВС України від 02 липня 2015 року № 796.
2. Про затвердження Положення про Департамент інформаційно-аналітичного забезпечення МВС України: Наказ МВС України від 29 квітня 2011 року № 174.
3. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: Наказ МВС України від 12 жовтня 2009 року № 436.

ОСОБЛИВОСТІ НАПИСАННЯ НАУКОВО-ДОСЛІДНИЦЬКИХ РОБІТ З ІНФОРМАТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Мельничин Андрій Володимирович,
доцент кафедри теорії оптимальних процесів, заступник декана факультету прикладної математики та інформатики Львівського національного університету імені Івана Франка,
кандидат технічних наук, доцент

На сьогодні інтенсифікація діяльності суб'єктів навчання у процесі модернізації школи та переходу від традиційних форм організації процесу навчання до впровадження інноваційних технологій зумовлює пошук нових підходів до організації роботи з обдарованою молоддю.

Виявлення і підтримка обдарованих дітей, залучення інтелектуально й творчо обдарованої учнівської молоді до науково-дослідницької та експериментальної роботи, формування активної громадянської позиції учнів, виховання в них самостійності, наполегливості, вміння формувати й обстоювати власну думку, є пріоритетним завданням педагога.

Головним завданням кожного учня, що виявив бажання займатися наукою, є участь у конкурсах різного рівня, на яких юні дослідники представляють свої перші наукові досягнення. Конкурси проводиться з метою духовного, творчого, розумового розвитку дітей країни, виховання їх у дусі патріотизму й демократичних цінностей, створення умов для формування інтелектуального потенціалу нації.

Основним завданням педагога-керівника у процесі написання науково-дослідницької роботи є організація творчого процесу так, щоб розвинути дослідницький потенціал учнів, ознайомити їх із правилами виконання й написання власних наукових робіт. Головне, щоб ще у шкільні роки діти навчилися ретельно проводити дослідження, оволоділи складними методами опрацювання результатів і переконалися, що справжня наука не може бути надуманою, а її результати завжди опираються на дійсно доведені факти.

Хотілося б, щоб для створення наукової атмосфери учні могли обмінюватися досвідом роботи, публікувати результати досліджень і через пресу чи спеціальні видання ознайомлюватися з діяльністю інших юних дослідників. Безперечно, що вдало підібрані та узагальнені матеріали мали б успіх серед учителів і учнів.

Науково-дослідницька робота – самостійно виконане учнем наукове дослідження за визначеною структурою, яке передбачає: розкриття сутності й стану наукової проблеми, обґрунтування актуальності обраної теми, визначення мети, завдань, об'єкта і предмета дослідження, опрацювання наукової та науково-методичної літератури, отримання результатів, а також формулювання власних висновків. Головними критеріями оцінки науково-дослідницької роботи є її актуальність, наукова новизна, теоретичне і практичне значення отриманих результатів. У процесі науково-дослідницької діяльності учні опановують способи та методи наукового пізнання світу, поглиблюють знання з базових навчальних дисциплін, отримують нові знання, не включені до шкільної програми.

Основними завданнями відділення комп'ютерних наук є залучення молоді до науково-дослідницької та технічно-творчої діяльності, спрямування її уваги на наукові проблеми сьогодення, пропаганда досягнень у галузі науки і техніки в Україні та світі.

Працюючи над науково-дослідницькою роботою, учні вчаться опрацьовувати наукову літературу, набувають навичок критичного відбору й аналізу необхідної інформації, виконують наукову, дослідницьку, експериментальну, конструкторську роботу. Таким чином, учень розвивається як дослідник, а в подальшому – і як науковець.

Тематика науково-дослідницьких робіт може бути або довільною, або ж запропонованою керівником. Робота за змістом і формою повинна бути науковою, актуальною, оригінальною, самостійною, з елементами новизни.

Як і кожне наукове дослідження, науково-дослідницька робота учнів є унікальною і має свою специфіку. Її деталі завжди потрібно узгоджувати з науковим керівником.

При виборі теми дослідження слід керуватись такими критеріями, як:

- оригінальність – не повторювати вже існуючі наукові ідеї;

- актуальність – необхідність такої розробки для потреб розвитку науки й галузі, іншими словами, чи потрібне вивчення цієї проблеми для суспільства і чи таке вирішення може бути досягнуто на основі дослідження;
- новизна – уточнення окремих понять з огляду на нові наукові дані, нові підходи в дослідженні явищ, процесів; вирішенням проблем, які до того не були з'ясовані;
- перспективність – можливість застосовувати роботу або її окремі результати в майбутньому;
- тематична спрямованість – відповідність роботи напрямку досліджень у конкретній галузі.

Мета наукової роботи – це запланований кінцевий результат, який має бути відображений у висновках наукової роботи. Мета дослідження конкретизується в завданнях, що формулюються у вигляді низки конкретних кроків, адже опис їхнього виконання має становити зміст розділів наукової роботи. Сформульовані завдання мають розкривати зміст теми наукової роботи.

Отже, мета дослідження може трактуватися як стратегія всієї наукової роботи, а завдання – як тактика для досягнення цієї мети.

Важливе місце у процесі виконання науково-дослідницької роботи займає робота над теоретичною частиною. В цій частині перед учнем ставиться доволі непросте завдання – наукове обґрунтування власної концепції вирішення досліджуваної проблеми.

У роботі над теоретичною частиною дослідження передбачається обґрунтування вибору теми, предмета й об'єкта наукового дослідження, визначення завдання наукової роботи, визначення актуальності, ступеня наукової новизни, значущості теми дослідження.

У теоретичній частині також проводять математичні розрахунки, які слугують фундаментальною базою для перевірки або підтвердження власної концепції.

Якісно провести дослідну роботу – передусім, вивчити і проаналізувати раніше опубліковані роботи за темою дослідження. Результати досліджень із різних наук і галузей життєдіяльності відображені у різних видах наукових робіт: монографіях,

наукових статтях, тезах, рефератах, дисертаціях, наукових доповідях, звітах тощо.

Завершальним етапом роботи над теоретичною частиною є аналіз одержаного наукового матеріалу. Він передбачає:

- обґрунтування вибору теми наукової роботи;
- визначення доцільності наукової роботи (актуальність, новизна ідеї, науковість, практична значимість, соціальна та господарська значимість);
- аналіз рівня розробки проблеми та її стану на момент дослідження;
- визначення ступеня новизни теми дослідження;
- обґрунтування вибору предмета й об'єкта дослідження.

Отже, написання учнями своїх перших наукових робіт — це шлях до створення кращих можливостей для самореалізації обдарованих дітей, формування атмосфери наукового спілкування, а якісна своєчасна допомога керівника-педагога — запорука успішної роботи учнів на науковій ниві.

1. Буйницька О. П. Інформаційні технології та технічні засоби навчання : навч. посіб. / О. П. Буйницька. – К. : Центр учбової літератури, 2012. – 240 с.
2. Концептуальні засади діяльності та розвитку Малої академії наук України / Л. І. Ковбасенко, С. О. Лихота, І. М. Шевченко ; за заг. ред. О. В. Лісового. – К. : ТОВ «Праймдрук», 2012.
3. Мельничин А.В. Вступ до науково-дослідницької роботи : методичні вказівки до написання та захисту науково-дослідницьких робіт з інформатики / А. В. Мельничин, І. А. Лема. – Львів : Видавництво «Львівської політехніки», 2014. – 112с.
4. Романчиков В.І. Основи наукових досліджень : навч. посібник / В. І. Романчиков. – К. : Центр учбової літератури, 2007. – 254 с.

ЗАСТОСУВАННЯ ІНТРОФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ВПЛИВУ НА ВИРІШЕННЯ КОНФЛІКТІВ У ДІЯЛЬНОСТІ ОВС

Рак Ольга Юріївна,
доцент кафедри журналістики та засобів масової комунікації
Національного університету «Львівська політехніка»,
кандидат наук із соціальних комунікацій, доцент

Психологія комунікаційного спілкування займає особливе місце у житті людини, зокрема професійної діяльності ОВС, як шлях до вирішення конфліктів, а саме для налагодження різного роду відносин та стосунків із соціумом. Мова та мовлення як комунікаційно-психологічний аспект впливу на соціум у розв'язанні конфліктів дозволяють пізнавати світ, збагачувати розумові здібності, накопичувати знання, аналізувати, синтезувати та прогнозувати різні спектри розвитку подій.

Конфлікт є тим психолого-соціально-комунікаційним явищем [1], який відтворює людські відносини вербально-дедуктивного типу спілкування, що задовольняє процеси потреб, можливостей, адаптації, конкуренції людини у життєвій конфронтації досягаючи певного комунікаційно-психологічного досвіду (зрілості). В середовищі найкращий і найефективніший спосіб подолання конфліктів є інформаційне знання та його накопичення, оскільки мова, слово має інтроформаційно-психологічну символьно-знакову дію, яка має в своїй складовій цілу низку значень. Кожне символьне значення несе поняттєву рису характеру та впливу. Отримавши готове знакове слово ще не означає, що воно сприйнялося соціумом, що досягло свого позитивного результату. Це не завжди так, оскільки для цього необхідно застосувати позитивний інтроформаційний (несиловий) підхід у вирішенні конфліктів в діяльності ОВС.

Важливим фактором у вирішенні конфліктів працівника ОВС із соціумом є забезпечення соціально-психологічного клімату

спочатку у внутрішньому, а потім у зовнішньому середовищах, який варто використовувати з метою та самоціллю впливу на підсвідомість, інтелектуальне бачення, спілкування та поведінку.

В період психологічної та інформаційної війн, на сьогоднішній день у конфліктному спілкуванні актуально використовувати метод вербалізації як комунікативно-психологічний кібернетичний підхід, що управляє настроями, аудиторією і створює увагу з боку внутрішнього та зовнішнього турбулентного (бурхливого) середовища і формує розуміння цінностей людських відносин.

Для правоохоронця важливим є просторове бачення, працювати не тільки на основі теоретичної і практичної бази знань (досвіду), але й на почуттях інтроформаційно-психологічного міжособистісного контакту, що вимагає рутинної інтелектуальної праці.

У практичній діяльності для працівників ОВС важливим є застосування інтроформаційно-комунікаційних технологій впливу на вирішення конфліктів, що включать:

- природний талант комунікативного спілкування;
- психологічна стриманість у контролюванні емоціями;
- психологічна адаптація;
- розум та уявно-просторове бачення;
- спрямованість на вивчення потреб, мотивів та на очікуваний результат;
- мисленнєво-когнітивне бачення та вміння аналізувати (прогнозувати);
- інтуїтивне відчуття;
- предметно-інтелектуальні знання;
- процес постійного пошуку пізнання;
- право на використання правових можливостей та власних професійних здібностей;
- почуття духовного і матеріального;
- володіння вербальним, вербально-дедуктивним та невербальним манерами спілкування;
- комунікативна компетентність: знать, розуміти, використовувати, аналізувати, синтезувати та оцінювати ситуацію;
- кар'єрна метаспрямованість як шлях до самовдосконалення.

У конфліктному процесі важливим є володіти нормою комунікаційно-соціальною компетентністю [3;5], оскільки вона забезпечує вміння виходити з конфліктних ситуацій, розуміти, вирішувати та вдосконалювати комунікаційно-конфліктний досвід, аналізувати та вчитися адаптуватись до різних життєвих моментів, синтезувати та практично реалізувати знання та навики набуті в оптимізованому інформаційному просторі.

Комунікаційний професіоналізм працівника ОВС забезпечить йому рису лідерства і образ «мети» та «результату» [4]. Через мовлення використанням методів та підходів із основ теорії несилової взаємодії правоохоронець зможе здійснити багато неможливого можливим, оскільки за своєю властивістю інформаційно-комунікаційно-психологічний вплив включає в себе елементи максимального перепрограмування коректування свідомості соціумом, його розуму та поведінки.

Комунікативна мова за своєю властивістю, в умовах інтроформаційної взаємодії, наділена високою емоційною культурою, тональністю, історичністю, розумом та психологічною змістовністю.

Під впливом двох середовищ: внутрішнього і зовнішнього впливів у працівника ОВС формуються компоненти особистісного поля у комунікаційно-конфліктному спілкуванні, що виступають ядром теорії інтроформаційної (несилової) взаємодії у своїй діяльності, а тому за перспективу мали б розвиватися такі особисті якості: міжособистісний вплив, прогнозоване бачення, контактна психолого-комунікаційна взаємодію з соціумом, пізнавальний психологічний вплив, толерантна увага та культура, а також вміння використовувати комунікаційно-регулювальну рівновагу, практичний досвід у вирішенні конфліктів, акторську здібність та управлінські знання з психології впливу у доланні конфліктних бар'єрів.

Здатність інтелектуально-толерантно-культурно вести переговори у професійні діяльності – це і є мистецтво на основі набутого досвіду і знань у вмінні переконувати, знаходити компроміс, досягати згоди і ефективно налагоджувати стосунки, що і є основою методології теорії несилової інтроформаційної взаємодії.

Сьогодні правоохоронця необхідно розглядати як інтелектуально-логічну ланку складу мислення, що живе у вирі постійного

спілкування та інформаційного потоку (позивного і негативного), під постійним впливом інформаційного процесора Природа [5], в цьому є процес зміни соціального життя. Вищий рівень інтелектуального соціального спілкування [2] з соціумом базується на толерантних відносинах, етикетних, культурних цінностях, традиціях та основних підходах із методології теорії несилової взаємодії. Поняття відповідальність та компетентність до справи є складовими толерантно-інтелектуального виховання, основаною на взаємодії інтелектуального розуму та бачення для досягнення прогресивних успіхів у розвитку держави та професійної діяльності працівників ОВС.

В процесі набутих професійних знань, працівник ОВС зуміє досягти акмеологічну точку комунікаційного професіоналізму.

1. Ложкін, Г.В. Психологія конфлікту: теорія і сучасна практика: навчальний посібник / Г.В. Ложкін, Н.І. Пов'якель. – К.: ВД «Професіонал», 2007. – 416 с.
2. Рак, О.Ю. Інтелектуально-конфліктний мотив уваги як психологічне явище вищого рівня комунікативного спілкування у процесі соціалізації / О.Ю. Рак // Актуальні проблеми психології: зб. наук. праць Інституту психології ім. Г.С. Костюка. – К.-Алчевськ: ДонДТУ – 2014. – Том 1. – Вип. 40. – С. 170-174.
3. Сусська, О.О. Інформаційне поле особистості. Формування інформаційного вибору в умовах сучасного соціокультурного середовища: Монографія / О.О. Сусська. – К.: ДАКККіМ. – 188 с.
4. Чічановський, А.А. Інформаційні процеси в структурі світових комунікаційних систем: підручник / А.А. Чічановський, О.Г. Старіш. – К.: Грамота, 2010. – 568 с.
5. Тесля Ю.Н. Введение в информатику Природы: Монография /Ю. Н. Тесля. – Киев: Маклаут, 2010. — 256 с.

СИСТЕМА УПРАВЛІННЯ ВНЗ ТА ЛОГІСТИЧНИМИ ПОТОКАМИ

Сватюк Оксана Робертівна,
доцент кафедри менеджменту
Львівського державного університету внутрішніх справ,
кандидат економічних наук
Сало Юрій Васильвич,
магістрант економічного факультету
Львівського державного університету внутрішніх справ
Стебелко Олег Іванович,
магістрант економічного факультету
Львівського державного університету внутрішніх справ

Для сучасного етапу розвитку національної економіки характерним є переважання сфери виробництва над сферою послуг. Проте у багатьох розвинутих країнах саме сфера послуг має найбільшу частку у валовому національному продукті де зайняте населення. Динаміка розвитку галузей сфери освіти в Україні показує пріоритет цього напряму в національній економіці. [2]

В *освітньому бізнесі під логістикою* розуміють методи та способи управління інформаційними та фінансовими потоками, які необхідні до надання освітніх послуг оптимальним чином. Потоки клієнтів, які є головним видом потоків в логістиці освітніх послуг і для яких власне створені та функціонують освіти різноманітних спеціальностей, видів та розмірів, в освітньому бізнесі відображуються у вигляді їхньої інформаційної та фінансової проекції, тобто інформаційних та фінансових потоків [1]. І в цьому полягає характерна особливість логістики освітніх послуг та її відмінність від логістики освіти. Пов'язане це з тим, що ресурсна база освіти для прийому студентів суворо обмежена акредитацією як в кількісному, так і у вартісному плані. Тому головними характеристиками потоку населення стають його інформаційні та фінансові показники, тобто потоки, які генеруються потоком студентів. Тому, логістична система

управління освітнім господарством, є структурованою адаптивною системою, яка складається з елементів, з'єднаних у процесі управління сервісними та супутніми їм фінансовими та інформаційними потоками.

Інформаційні потоки в логістиці освітніх послуг поділяються на внутрішні та зовнішні. Перші викликані інформаційним обміном між співробітниками закладу, другі – надходять від суб'єктів ринку. В межах польових маркетингових досліджень було виявлено, що най об'ємними та най значимими зовнішніми інформаційними потоками є ті, що надходять від споживачів (вимоги щодо наявності державних місць, стипендій, рівня акредитації, якості освітніх послуг тощо). Інформація, що надходить від споживачів, здійснює вагомий вплив на параметри внутрішніх потоків. Інші зовнішні інформаційні потоки чинять коригуючу дію. Внутрішні інформаційні потоки поділяють на три види: 1) «горизонтальний» інформаційний обмін між керівниками різних підрозділів, що включає документацію для прийняття управлінських рішень; 2) «вертикальний» обмін інформацією між керівництвом та співробітниками, що визначає потоки організаційно-розпорядницької документації; 3) обмін інформацією між клієнтами та працівниками ВНЗ в межах обслуговування. До основних характеристик зовнішніх та внутрішніх потоків інформації відносять те, що перші є не підконтрольними підприємству, вони є первинними та впливають на характеристики внутрішніх потоків; а другі – можуть управлятися керівництвом освітнього закладу. При формуванні моделі організації управлінських впливів на інформаційні потокові процеси керуються наступними засадами:

1) зовнішні інформаційні потоки впливають на управління внутрішніми;

2) характеристики всіх інших потоків ресурсів залежать від інформаційних ;

3) інформаційні потоки ранжуються та визначаються способи дії на кожний рівень ієрархії з акцентом на потоки від споживачів;

4) адекватна реакція керівництва на зміну параметрів потоків інформації визначає можливості ефективного функціонування ВНЗ.

Визначені такі особливості вхідних фінансових потоків: по-перше, вони є наслідком відповідних вхідних інформаційних потоків; а по-друге, вони первинні по відношенню до відповідних сервісних потоків. Ще одна особливість фінансових потоків – це їх орієнтованість, за якою виділяють дохідні та витратні потоки. Основу перших становлять платежі від кількості наявних студентів, служби харчування, надання додаткових послуг. Основу витратних фінансових потоків складають виплати заробітної платні працівникам, податкові відрахування, оплата комунальних послуг. Оскільки логістичні потоки в освітньому закладі є взаємозалежними, то для побудови логістичної системи управління ВНЗ необхідно виявити їх кореляцію (рис.1, розроблений на основі [2]. Відповідні дослідження охопили декілька етапів. На першому – визначався зв'язок інформаційного потоку з відповідними дохідними та витратними фінансовими потоками. Під час другого – значення дохідних та витратних фінансових потоків використовувалися до визначення коефіцієнту відповідного інформаційного потоку. На третьому – згідно значень коефіцієнтів були виділені наступні види інформаційних потоків: а) вимоги, що надходять від споживачів; б) замовлення освітніх служб; в) інші замовлення, між якими розподіляють управлінські ресурси.

До інформаційних потоків, що надходять від споживачів, відносять вимоги щодо цінової політики ВНЗ; фаховості персоналу; відповідності спеціальностей на факультетах, показники рівня акредитації ВНЗ. На підставі визначення інформаційних, фінансових та сервісних потоків у освіті будується організаційна структура логістичної системи. До її внутрішнього середовища належать чотири підсистеми, до зовнішнього – організовані та неорганізовані споживачі, банки, освіті-конкуренти та посередники. Джерелами всіх фінансових та більшої частини інформаційних потоків є студенти. Логістичні потоки, що виникають між ВНЗ та студентами, накопичуються та перерозподіляються посередниками (банками). Обслуговування інформаційно-фінансових потоків між елементами зовнішнього та внутрішнього середовища логістичної системи ВНЗ здійснюють банківські установи. Інформаційна взаємодія чотирьох підсистем внутріш-

нього середовища визначає логістичну діяльність ВНЗ. Основними функціями підсистеми 1, що відповідає за створення та підтримку логістичних каналів зв'язку з об'єктами зовнішнього середовища, є: а) вибір каналів та оптимізація процесу вибору ВНЗ; б) розробка фінансової стратегії стимулювання суб'єктів освітнього бізнесу; в) оптимізація руху потоку ресурсів у комунікаційній діяльності ВНЗ.

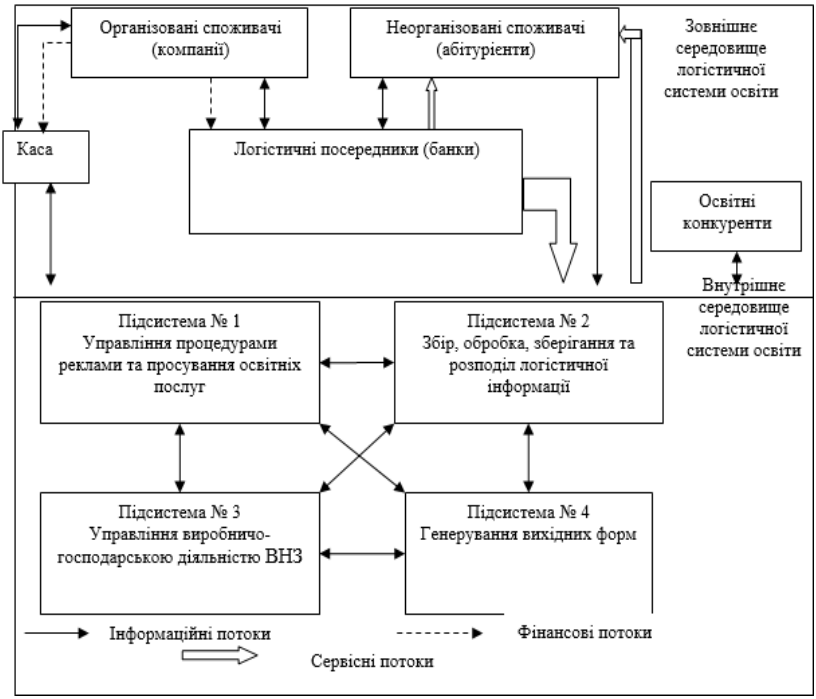


Рис. 1. Організаційна структура логістичної моделі системи управління ВНЗ.

До основних функцій підсистеми 2, що управляє зовнішніми та внутрішніми потоками інформації, належать: а) визначення каналів збору маркетингової інформації; б) прогнозування потоку ресурсів; в) оптимальне використання інформаційних технологій у ВНЗ та оптимізація внутрішнього документообігу. Основними функціями підсистеми 3, що впливає на параметри внутрішніх ресурсів ВНЗ з метою їхньої оптимізації, є: а) форму-

вання ефективної системи управління; б) планування номенклатури освітніх послуг; в) розробка цінової стратегії; г) планування використання ресурсів. У переліку основних функцій підсистеми 4 знаходяться: а) обробка даних; б) їх розподіл у формі звітів для користувачів.

З метою оптимального управління потоками, що циркулюють у логістичній системі ВНЗ виділяються області максимального зосередження потоків у однакові моменти часу-вузли. Варіант поетапного планування діяльності вузлових служб ВНЗ рекомендується до використання при розробці нових освітніх продуктів та програм, стимулюванні діяльності агентів ринку освітніх послуг, розробці спеціальних програм підвищення кваліфікації, вдосконаленні систем якості, розробці системи заохочування персоналу тощо.

1. Кузьмін О. Є. Керівництво організацією / О. Є. Кузьмін – Львів: НУ «ЛП» Інтелект-Захід, 2008. – 244с. 2.Ларрреше Ж.К. Система оценки эффективности маркетинговой деятельности [Електронний ресурс] – Режим доступу: http://www.elitarium.ru/2006/03/17/sistema_ocenki_jeffektivnosti_marketingovojj

ЩОДО НЕОБХІДНОСТІ РОЗРОБКИ ТА ЗАПРОВАДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИЗНАЧЕННЯ РЕЙТИНГУ НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ У ЛьвДУВС

Сеник Володимир Васильович,
завідувач кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Важливим фактором вищої освіти, що впливає на рівень підготовки курсантів та студентів, є професійний рівень знань і компетентність науково-педагогічних працівників. Оцінка ефективності викладацької діяльності є обов'язковою умовою, яка забезпечує функціонування системи управління якістю освіти, а також дозволяє проводити моніторинг, контролювати зміни якісного складу, кадрового потенціалу, активність за різними напрямками педагогічного навантаження, ефективність праці, виявляти та підтримувати позитивні тенденції у роботі науково-педагогічних працівників.

Сучасні вимоги до вищої освіти в Україні, запровадження нових інноваційних технологій у вищих навчальних закладах встановлюють високі вимоги до кваліфікації науково-педагогічних працівників. В залежності від того, чи відповідає науково-педагогічний працівник вимогам сьогодення, залежить рівень підготовки бакалаврів, спеціалістів та магістрів, тобто підготовка висококваліфікованих кадрів для держави.

Разом з тим, практика оцінки діяльності науково-педагогічних працівників, що склалася сьогодні, далека від досконалості, оскільки немає чітких критеріїв і часто орієнтується на суб'єктивний та узагальнюючий підхід. Сьогодні вже нікого не повинні влаштовувати розпливчаті формулювання, якими описують якісні характеристики педагогічної діяльності. У даний час є необхідність запровадження прозорих і зрозумілих кількісних параметрів, що характеризують науково-педагогічну діяльність та не залежать від суб'єктивних факторів.

Формування ефективно працюючого викладача – гарантія якості навчального процесу, які надають ВНЗ студентам. Інструментом, у даному випадку, може виступати «рейтинг науково-педагогічного працівника», який також може бути інструментом як для моніторингу педагогічної діяльності ВНЗ, так і для прийняття управлінських рішень керівництвом навчального закладу з організаційної, фінансової і кадрової політики [1].

Технічне завдання щодо розробки системи формування рейтингу науково-педагогічного працівника повинно враховувати те, що в основі системи оцінки діяльності закладені очевидні і загальноприйняті показники, які загальні для всіх, та показники, які залежать від факультету і профілю діяльності викладача. Рейтинг, як система оцінки за формальними показниками, повинен мати переваги – прозорість оцінки, простоту реалізації і неможливість довільно завищувати чи понижувати оцінку.

На даний час у багатьох вищих навчальних закладах вже запровадженні рейтингові методики оцінки науково-педагогічних працівників. На основі аналізу досвіду запровадження і функціонування таких систем у Львівському державному університеті внутрішніх справ та Національному університеті «Львівська політехніка» можна зробити висновок, що загальними можуть бути загальноприйняті показники, однак варіативні критерії, які залежать від специфіки ВНЗ також мають важливий вплив. При цьому, в залежності від мети рейтингу, реалізовуються різні підходи, а в кінцевому випадку – оцінка діяльності науково-педагогічних працівників.

Аналіз методик розрахунку рейтингу науково-педагогічних працівників показує, що рейтингова система повинна враховувати значну кількість показників діяльності викладачів, таких як: науковий ступінь, вчене звання, членство в академіях, обсяг аудиторного та навчального навантаження, підготовка та видання підручників, посібників, методичних матеріалів, статей, монографій, участь у конференціях, семінарах тощо. Так, у Львівському державному університеті внутрішніх справ рейтинг науково-педагогічного працівника враховує 90 критеріїв, які охоплюють загальні відомості про науково-педагогічного працівника, навчальну, методичну, наукову роботу, роботу з курсантами та студентами тощо.

У зв’язку з великою кількістю і значимістю показників, що враховуються у формуванні рейтингу, очевидним є необхідність

розробки автоматизованої системи формування рейтингу науково-педагогічних працівників із врахуванням специфіки діяльності вищого навчального закладу.

При цьому, для усіх показників необхідно максимально правильно розрахувати коефіцієнти (з врахуванням їх значимості), на основі чого буде проводитись розрахунок рейтингу. Також необхідно прагнути до того, щоб рейтинг був визначальним фактором оцінки діяльності кожного викладача.

Інструментом з реалізації формування рейтингу науково-педагогічних працівників може стати автоматизована інформаційна система, адже вона дозволить реалізувати ряд можливостей:

- формування і актуалізація рейтингу в режимі on-line, що досягається організацією введення показників ефективності та результатів діяльності науково-педагогічного працівника безпосередньо ним. Це сприяє актуалізації інформації на поточний час, а також значно скорочує затрати часу та людських ресурсів на формування і наповнення бази даних системи;
- можливість проводити аналіз з візуалізацією статистичних і аналітичних даних рейтингу (створення звітів, у тому числі у вигляді таблиць, графіків, гістограм).

На основі введених даних, підрозділ, який адмініструватиме систему, повинен мати можливість переглядати результати діяльності не лише окремих науково-педагогічних працівників, але й кафедри чи факультету в цілому. Така можливість дозволятиме приймати управлінські рішення керівникам різних рівнів: кафедри, факультету, університету, що сприятиме ефективнішому використанню людських ресурсів і розподілу фінансових. Загалом університет отримає можливість формувати звіти як по окремому підрозділу, так і по кожному науково-педагогічному працівнику.

Розробка, запровадження і активне використання такої автоматизованої системи оцінки ефективності діяльності науково-педагогічних працівників дозволить підвищити якість управління як окремими підрозділами, так і ВНЗ в цілому, а також дозволить об’єктивно оцінити діяльність кафедр і науково-педагогічних працівників з метою прийняття управлінських рішень.

---

1. Гуров В.Н., Резванова И.Ю. Оценка деятельности преподавателей в контексте качества работы вуза // Наука. Инновации. Технологии. – 2010. – №1. – С. 29-33.

ШЛЯХИ ВДОСКОНАЛЕННЯ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ

Фірман Ігор Володимирович,
старший оперуповноважений з особливо важливих справ
Департаменту внутрішньої безпеки МВС України

Стержнем забезпечення функціонування життєдіяльності держави є її правове поле в основі якого закладено верховенство права, гарантоване Конституцією України.

Держава функціонально здійснює,через правоохоронні органи, забезпечення та реалізацію державної політики, щодо гарантованого Конституцією України права громадян.

Повсякденне правове супроводження забезпечення реалізації конституційних прав громадян, правоохоронні органи здійснюють через свої структурні підрозділи. Цей якісний правовий сервіс безпосередньо залежить від фаховості наповнення функціональних структурних правоохоронних органів підготованими спеціалістами з різних галузей.

Основним постачальником кадрового забезпечення правоохоронних органів, зокрема для органів внутрішніх справ, є відомчі вищі навчальні заклади. Така відомча підпорядкованість дає можливість швидкого, термінового реагування на необхідні зміни у підготовці фахівців, особливо для оперативних служб. У той же час навчання майбутніх правоохоронців тісно пов'язано і залежить не тільки від матеріально-технічної і наукової бази, а і від фаховості, рівня підготовки та практичного досвіду науково-педагогічного складу.

Важливим у цьому питанні є залучення до викладацької роботи на постійній основі працівників органів внутрішніх справ з належним досвідом роботи. Так оправданою нормою, щодо добору кадрів викладацького складу для відомчих навчальних закладів у свій час була вимога колишнього МВС СРСР, яка на наш погляд є актуальною і нині, це призначення на посади викладацького складу співробітників ОВС з стажем практичної служби не менше 5 років.

Це дозволяло залучати до навчального процесу тільки фахівців у яких уже було сформовано професійний закал і акумульовано інтуїтивний досвід роботи правоохоронця. Такий практичний досвід дозволяє особливо при викладанні прикладних дисциплін творчо поєднувати теорію і практику. Подання навчального матеріалу викладачем-практиком проходить шляхом інтегрування теоретичних викладок крізь матрицю алгоритму дій правоохоронця у певних конкретних обставинах.

Професійний досвід фахівця-практика дозволяє йому на викладацькій роботі скеровувати навчальне навантаження на курсантів через призму сприйняття ним самим важливості та необхідності понять знати і вміти. Таке моделювання функціональної залежності знань та вмінь щодо практичної потреби дозволяє формувати якісного спеціаліста-правоохоронця.

Нагромадження знань та практичних вмінь поліцейськими особливо у застосуванні спеціальної техніки, інформаційних технологій для профілактики і розкриття злочинів є одним із пріоритетних напрямків у підготовці. Левова частка злочинів розкривається з застосуванням ОТЗ.

ЗМІСТ

Розділ 1. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПОЛІЦІЇ 3

Гаврильців М.Т. Застосування інформаційних технологій у юридичній практиці 3

Горпинченко Є. Г. Система централізованого управління нарядами патрульної поліції 8

Дабіжа Д. В., Хахановський В. Г. Проблеми застосування інформаційних систем ОВС України під час розслідування кримінальних правопорушень 11

Єсімов С.С. Розвиток правового регулювання використання хмарних технологій 15

Живко З.Б., Баваровська О.Б., Живко П.Б. Шляхи протидії загрозам інформаційній безпеці 20

Живко М.О., Босак Х.З., Вольних А.І. Удосконалення системи забезпечення інформаційної безпеки 28

Захарова О.В., Сеник С.В., Ізьо М.І. Нормативно-правові чинники формування політики інформаційної безпеки 35

Ковалів М.В., Іваха В.О. Комп'ютерні злочини як складова інформаційних злочинів 41

Комісарчук Ю.А., Жук А.П. Інформаційні технології в діяльності ОВС: значення та перспективи розвитку 46

Король Т.О., Комісарчук Ю.А Інформаційне забезпечення ОВС України: сутність, завдання та перспективи розвитку ..50

Магеровська Т.В., Андрухів Є.М. Роль інформаційних технологій у діяльності органів внутрішніх справ України під час здійснення досудового розслідування 54

Магеровський Д.В. Використання методів експертних систем для автоматизації розселення осіб у місця тимчасового проживання 62

Мельник О.М. Інформаційно-аналітична діяльність поліції у сфері протидії незаконному обігу наркотичних засобів.....69

Мних С.Р., Неспляк Д.М. Сучасні інформаційні технології в сфері фіксацій адміністративних порушень правил дорожнього руху 74

Мойсеєнко І.П. Моделі змін в суспільстві на основі інтелектуалізації 82

Мороз В.І. Охорона інформації: погляд збоку 87

Нагачевська Ю.С. Проблеми і перспективи використання інформаційних технологій.....92

Неспляк Д.М., Магеровський Д.В. Технологія Hibernate роботи з базами даних.....96

Паращук Л.Я., Бесага І.В. Проблемі питання, пов'язані із використанням електронного цифрового підпису при зверненні до суду 100

Протиняк А.А., Сеник В.В., Рудий Т.В. Окремі проблеми використання мобільних та інтернет-технологій у наданні комерційних послуг.....107

Руда О.І., Протиняк Д.А. Захист спеціалізованих інформаційних систем на базі аудиту безпеки в умовах трансформації МВС 111

Соколов В.С., Грицюк Ю.І. Розроблення Алгоритму шифрування даних Svabom 116

Тележенко Б.О., Чередниченко В.Б. Комп'ютерна стеганографія та захист інформації.....122

Хахановський В. Г. Окремі термінологічні проблеми, що виникають в процесі інформаційного забезпечення правоохоронної діяльності 125

Хитра О.Л. Сучасні реалії та загрози інформаційній безпеці в діяльності юридичної особи 128

Цибуляк Б.З. Застосування інформаційних технологій у роботі силових структур України 133

Чередниченко В. Б. Деякі питання функціонування електронного цифрового підпису.....138

Чистоклетов Л.Г. Досвід США в галузі інформаційно-правового забезпечення безпеки суб'єктів господарювання 142

Чумак В.В. Основні напрями та особливості організації діяльності поліції Латвії.....146

Шишко В.В., Шишко В.Й. Досвід США у сфері інформаційної безпеки.....149

Розділ 2. ПРОБЛЕМИ ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА ПРОГРАМНО-ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПОЛІЦІЇ 154

Вишня В.Б., Прокопов С.О. Пристрої акустичного контролю інформації.....154

Зачек О.І. Розробка модернізованої автономної репродукційної установки «Ель-М2».....160

Кулешник Я.Ф., Рудий Т.В. GSM-технології в охоронних системах 165

Нагачевський С.В. Застосування спеціальних засобів для забезпечення громадського порядку, проведення масових заходів.....173

Стадник М.Є., Стадник О.В. Еелектронні карти в системі моніторингу та прогнозування стану водних ресурсів 176

Федорчук Є.Н., Федорчук Ю.Є. Оптимізаційна модель задачі планування логістичних перевезень.....181

Хомин О.Й. Міжнародний досвід забезпечення безпеки населення в сфері контролю за застосуванням вогнепальної зброї 186

Шабатура Ю.В., Куценко Б.А. новий підхід до вирішення задачі енергетичного забезпечення інформаційно-комунікаційних та розвідувально-навігаційних засобів артилерійських підрозділів.....191

Шабатура Ю.В., Мочернюк Ю.М. Застосування інформаційних технологій для підвищення енергетичної безпеки при використанні відновлюваної енергетики 194

Шабатура Ю.В., Шевчук Р.В. Інформаційна система автоматизованого проектування та аналізу атмосферної динаміки з врахуванням ландшафту території 198

Розділ 3. НАУКОВО-МЕТОДИЧНІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ ПРОЦЕСІ 202

Бондаренко В.А. Застосування інтелектуалізованих систем навчання на заняттях з іноземної мови 202

Йосифович Д.І., Ревак І.О. Використання інформаційних технологій при викладанні соціальних дисциплін у вищій школі 207

Коширець С.І., Бичинюк І.В., Бичинюк О.В. Математичне та програмне забезпечення розподіленої бази даних «Ботанічний сад НЛТУ України» 211

Кудінов В.А. Особливості вивчення інформаційних технологій під час підготовки фахівців для нової патрульної служби МВС України 216

Мельничин А.В. Особливості написання науково-дослідницьких робіт з інформатики та інформаційних технологій 221

Рак О.Ю. Застосування інтроформаційно-комунікаційних технологій впливу на вирішення конфліктів у діяльності ОВС ..225

Сватюк О.Р., Сало Ю.В., Стебелко О.І. Система управління ВНЗ та логістичними потоками 229

Сеник В.В. Щодо необхідності розробки та запровадження автоматизованої системи визначення рейтингу науково-педагогічних працівників у ЛьвДУВС 234

Фірман І.В. Шляхи вдосконалення підготовки фахівців для правоохоронних органів 237

НАУКОВЕ ВИДАННЯ

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

Збірник наукових статей
за матеріалами доповідей
науково-практичної конференції
17 грудня 2015 р.

Відповідальний за випуск В.В. Сеник
Упорядник Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська

Опубліковано в авторській редакції

Підписано до друку 23.12.2015 р.
Формат 60×84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк.14,1
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.