УДК 342.721:681.3.02

В. БРИЖКО, *кандидат юридичних наук (Ph. D), старший науковий співробітник*

ПРО УПОРЯДКУВАННЯ ЗАКОНОДАВСТВА УКРАЇНИ ІЗ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. *Щодо підсумків, перспектив та пропозицій з нормативно-правового упорядкування відносин у сфері захисту персональних даних.*

На другій рік після “оксамитової революції” 1991 р. Угорщина одним з перших міжнародних актів підписала та ратифікувала Конвенцію Ради Європи № 108 від 28 січня 1981 року “Про захист прав осіб у зв’язку з автоматизованою обробкою персональних даних”. У 1992 р. парламент країни прийняв базовий закон та призначив комісара із захисту персональних даних. Конституційний Суд Угорщини почав розглядати питання, зокрема щодо особистого ідентифікаційного коду [6, с. 146-153; 17].

В Україні стан справ з розв’язанням питань із захисту персональних даних згідно з положеннями європейських стандартів значно скромніший.

Ще у 1994 році була підписана “Угода про партнерство та співробітництво, яка започатковує партнерство між Європейськими Співтовариствами та їх державами-членами, з одного боку, та Україною, з іншого боку”, ратифікована Законом України від 10.11.1994 р. № 237/94-ВР. У 1998 р. затверджена Стратегія інтеграції України до Європейського Союзу (Указ Президента України від 11.06.1998 р. № 615/98), де у п. 4.4. визначались етапи інтеграції щодо захист інформації про особу. Потім була низка незчисленних указів Президента, постанов та розпоряджень КМ України щодо концепцій та програм інтеграції, рішень “круглих столів” та парламентських слухань, а також план Мін’юсту України під назвою “План заходів щодо виконання Плану дій Україна – ЄС на 2005 рік”, що передбачало ратифікацію Конвенції Ради Європи № 108 і Додаткового протоколу до неї 2001 р. з одночасним прискоренням розгляду законів та внесення змін у законодавство, зокрема щодо захисту персональних даних.

На превеликий жаль, за 16 років державотворення питання із запровадження в Україні міжнародних принципів із захисту персональних даних практично не вирішене.

1. Міжнародні стандарти із захисту персональних даних

Рада Європи. У травні 1949 року у Лондоні, виходячи з необхідності зміцнення миру на засадах справедливості та консолідації у співробітництві з гуманітарних питань, що становлять підвалини справжньої демократії, десять країн Європи заснували міжнародну інституцію під назвою “Рада Європи”, яка складається з представників урядів та консультативної асамблеї*.

Метою Ради Європи є досягнення більш тісного єднання європейських країн для збереження та втілення в життя ідеалів і принципів, які є спільним надбанням, а також сприяння економічному та соціальному прогресу, посилення демократичного, соціального та культурного розвитку кожної держави-члена Ради Європи.

© В. Брижко, 2008

* Рада Європи нараховує 40 держав-членів [1]. Усі держави-члени Європейського Союзу [2] (директиви якого мають пріоритет у вирішенні економічних питань) є членами Ради Європи.

Діяльність Ради Європи передбачає вироблення конвенцій та угод, які становлять правову базу для уніфікації (упорядкування) відносин у відповідних сферах суспільного життя. Кожна держава-член Ради Європи зобов’язана здійснити зміни у національному законодавстві та привести його до вимог положень, які є європейськими та, звичайно, міжнародними стандартами.

У 1995 р. Україна приєдналася до Ради Європи. Вручення 09.11.1995 р. ратифікаційних грамот Генеральному Секретарю Ради Європи (рішення Верховної Ради України про приєднання прийнято 31.10.1995 р.) зобов’язало Україну підписати та ратифікувати понад 170 міжнародно-правових актів, з яких у наш час підписано 30, підписано та ратифіковано понад 24 конвенцій (за таких темпів євроінтеграції можна бути впевненим, що років через 50 Україна виконає свої обіцянки світовому співтовариству у повному обсязі).

Першим у світі, головним та єдиним правовим актом, який визначає основоположні, уніфіковані принципи створення національного законодавства країн світу у сфері захисту персональних даних, є Конвенція Ради Європи № 108 “Про захист прав осіб у зв’язку з автоматизованою обробкою персональних даних”, вчинена 28 січня 1981 р. в м. Страсбурзі [3] (далі – Конвенція РЄ № 108). Повне й безпосереднє виконання її правових норм є обов’язковим для усіх держав-членів, що її ратифікували. Координування та нагляд за цією діяльністю покладено на Комісара РЄ із захисту даних, який підпорядкований Генеральному Секретарю Ради Європи.

У 2001 р., з метою приєднання України до Конвенції РЄ № 108 та Додаткового протоколу до неї щодо органів нагляду та транскордонних потоків даних (вчиненого 8 листопада 2001 р. в м. Страсбурзі) нами було здійснено їх переклад з англійської на українську мову, яки отримали офіційне затвердження Міністерства закордонних справ України від 01.07.2002 р.

У серпні 2002 р. українська версія вказаних актів спрямована до Кабінету Міністрів України на предмет її подання до Верховної Ради України для подальшого підпису та ратифікації.

Через три роки, 5 серпня 2005 р., розпорядженням Президента України (№ 1142/2005-рп) Постійного представника України при Раді Європи було уповноважено на підписання від імені України Конвенції РЄ № 108 та Додаткового протоколу до неї від 8.11.2001 р., що у наступному й було зроблено.

З часу підпису вказаних Конвенції та Додаткового протоколу минуло ще два роки. Однак ратифікація зазначених міжнародних актів й досі не відбулася. Головна причина – згідно зі статтею 4 Конвенції РЄ № 108 Верховна Рада України має право її ратифікувати за умов приведення національного законодавства у відповідність з її положеннями. А це передбачає перегляд та корегування усього національного законодавства згідно з міжнародними принципами захисту персональних даних, викладеними у Конвенції РЄ № 108.

Загальносвітова практика запровадження у національне законодавство принципів Конвенції РЄ № 108 здійснюється наступним чином.

Спочатку кожна країна розробляє та приймає базовий закон щодо зазначеної сфери, а потім здійснює корегування усього законодавства на основі його положень. У наступному за галузевим принципом розподілу правових норм за окремими напрямами соціальної та господарської діяльності (з метою врахування особливостей регулювання суспільних відносин у тій чи іншій галузі) здійснюється впровадження рекомендацій Ради Європи, а також положень директив та резолюцій Європейського Союзу.

Згідно зі статтею 13 Конвенції РЄ № 108 та статтею 1 Додаткового протоколу до неї від 08.11.2001 р. нагляд за діяльністю стосовно виконання принципів, які містяться у національному законодавстві, що втілюють принципи міжнародних стандартів, здійснює уповноважений орган із захисту персональних даних, який виконує свої функції у повній незалежності.

Європейський Союз. Заснований у 1957 р. з метою співробітництва з економічних та монетарних питань держав-членів ЄС. Головне завдання – створення “Загального ринку”.

У середині 1990-х рр. ця міжнародна інституція звернула увагу на те, що регуляція економічних питань у державах-членах ЄС одночасно потребує врахування питань нормативного упорядкування відносин із захисту персональних даних. Першим актом з цього була Директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 р. “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” [14, с. 273-293]. У 1997 р. Європейський Парламент (дорадчий орган, члени якого призначаються парламентами) та Рада Європейського Союзу (представляє уряди) прийняли Директиву 97/66/ЄС Європейського Парламенту і Ради від 15.12.1997 р. “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” [14, с. 337-344]. Нагляд за цією діяльності у країнах ЄС здійснює Європейський наглядач із захисту даних.

У зазначених актах було здійснено намагання деталізувати відносини як із захисту персональних даних, так і вільного їх обігу. Враховуючи, по-перше, те, що пріоритети інтересів ЄС мають економічний зміст й тільки вимушено повинні враховувати гуманістичні питання, а по-друге, що будь-яку систему абсолютного захисту створити неможливо взагалі, положення зазначених актів розглядаються як рекомендації щодо їх впровадження до національного законодавства за умов свободи вибору форм і методів та застосування у період від 3 до 12 років з дня їх прийняття.

При цьому слід звернути увагу на строки запровадження у національне законодавство принципів Конвенції РЄ № 108, яки є обов’язковими не тільки для країн Європи, а й для усіх країн світу, яки бажають бути у європейському ринку. Згідно з пунктом 3 статті 22 Конвенції РЄ № 108: *“Для будь-якої держави-члена, яка згодом висловить свою згоду на обов’язковість для неї цієї Конвенції, вона набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи схвалення”* [3].

2. Законодавство із захисту персональних даних в Україні

У зв’язку з поширенням інформаційно-комп’ютерних технологій та мереж, які активно вторгаються у сферу особистого життя кожної людини, у 1986 році було поставлено питання про створення закону України із захисту персональних даних [4; 5].

Після ознайомлення з міжнародно-правовими актами РЄ, ЄС та законодавством провідних країн світу щодо захисту персональних даних [6; 14] стало зрозумілим, що бажання швидко гармонізуватися із законодавством європейських інституцій може бути реалізоване тільки на рівні умоглядних уявлень. Менталітет, соціальні та політико-економічні реалії країни, яка тільки вибирає шлях демократії та верховенства права, не сприяють оперативному вирішенню проблеми. Створення юридичних умов захисту прав та інтересів окремої людини потребує поступової та неспішної роботи за принципом – від головного до детального.

Якщо порахувати кількість нормативно-правових документів, що є чинними тільки в інформаційній сфері та потребують внесення до них змін та доповнень у зв’язку з запровадженням вимог європейського права до захисту персональних даних, то їх кіль-

кість становитиме не менш як 4500 актів. Більш значна цифра виникає, якщо враховувати необхідність внесення змін та доповнень у інші нормативно-правові акти, будь то Цивільний, Господарський, Кримінальний тощо кодекси, або до безлічі чинних у різних галузях господарства підзаконних актів. А врахувати їх є потреба. Хочемо ми того чи ні, немає такої області життєдіяльності людини або діяльності суспільства і держави, яка не потребує корегування відносин згідно з європейськими принципами захисту персональних даних.

У той час було визначено етапи створення та вимоги до законопроекту за умов приведення законодавства України до законодавства європейських інституцій, а саме:

- по-перше. Закон про захист персональних даних повинен бути рамковим, тобто – визначати межи правового регулювання, та – базовим для корегування законодавства за галузями народного господарства;
- по-друге. Так як закон покликаний вирішувати насамперед питання, які безпосередньо стосуються гуманітарних проблем щодо захисту окремої фізичної особи, його основою повинні бути принципи, визначені у відповідному міжнародно-правовому акті щодо гуманітарних питань. У світі таким єдиним правовим актом визнана Конвенція РЄ № 108 та Додатковий протокол до неї від 08.11.2001 р.;
- по-третє. У повсякденному житті фізична особа виступає у двох іпостасях: як “людина” та як “громадянин”. У принципі, для створення умов дійового захисту персональних даних у законодавстві це потребує їх розмежування.

Для створення умов дійового захисту прав “людини” від несанкціонованої комерційної діяльності з даними необхідно долучити безпосередньо її до процесу захисту своїх персональних даних за визначеними законом умовами. Це можливо, якщо надати людині право власності на її персональні дані (до теперішнього часу відповіді на запитання – кому належать персональні дані конкретної особи? – взагалі не маємо). Підкреслимо, зазначене право стосується лише будь-якої комерції з персональними даними фізичних осіб – збирання даних з різних джерел, створення баз персональних даних та їх поширення на комерційних засадах, здійснення чого повинно в обов’язковому порядку враховувати добре відоме оголошення: *“Стій! Приватна власність. Вхід заборонено”.*

Діяльність держави, зокрема функціонування її правоохоронних органів, не є можливою без персональних даних. Для органів влади фізична особа виступає як “громадянин”, використання даних якої повинно здійснюватися лише у межах наданих законом повноважень.

Така постановка справи, з одного боку, надає проекту стрижень (системність, логічність та перспективність), на який, як нитка на веретено, повинні “накручуватися” всі правові формули щодо захисту персональних даних (детальне обґрунтування див. у [6, с. 40-42; 7, с. 169-176; 8, с. 38-42; 9, с. 65-69; 10, с. 66-68; 11, с. 52-53; 12, с. 18-24]), а з іншого – ця новація у повному обсязі відповідає положенню статті 11 Конвенції РЄ № 108 “*Жодне з положень цієї глави* (Глава II – Основоположні принципи захисту даних – від авт.) *не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією*” [14, с. 68];

- по-четверте. Закон повинен мати чіткість у визначеннях видів діяльності та їх узгодженість. Крім цього, закон повинен мати визначення узагальнюючого терміну щодо будь-якої діяльності із захисту персональних даних (у міжнародних стандартах – це “обробка”);
- по-п’яте. Закон повинен бути таким, щоб його положення надавали можливість застосовувати їх до файлів персональних даних у зв’язку з автоматизованої обробкою

даних за умов використання інформаційно-комп’ютерних технологій та мереж як у державному, так й у приватному секторах;

• по-шосте. Закон повинен бути базою для внесення змін та доповнень у галузеве законодавство за умов запровадження до них у наступному відповідних положень Рекомендацій РЄ, а також Директив та Рекомендацій ЄС. Саме їх положення становлять умови деталізації у регулюванні відносин у тій або інший галузі. Виконання цього етапу можна вважати кінцевою метою у створенні правового фундаменту, який спирається на світові принципи приведення усього законодавства із захисту персональних даних в Україні у відповідність до вимог законодавства європейських інституцій;

• по-сьоме. Після введення закону в дію є необхідним запровадження спеціального уповноваженого органу, який повинен відповідати за остаточне приведення галузевого законодавства до європейських стандартів та, у наступному, здійснювати нагляд за діяльністю у сфері захисту персональних даних, що також передбачене європейськими стандартами [5 – 9].

До кінця **1999 р. проект Закону України “Про захист персональних даних” був створений**, пройшов експертизу юристів 11 міністерств і комітетів та завізований їх керівниками (за виключенням Мін’юсту України)*. На той час проект мав 23 редакції, завдяки чому враховано понад 250 зауважень та пропозицій.

Для ознайомлення широкої громадськості з сутністю законопроекту була видана книга “Права человека и защита персональных данных” [7], кошти на яку надала Харківська правозахисна група (Є. Захаров), що могло свідчити про те, що на той час українські представники Гельсінського правозахисного руху претензій до проекту не мали.

У 2000 році проект Закону України “Про захист персональних даних” був спрямований до Кабінету Міністрів України (вих. Держкомзв’язку України від 20 грудня 2000 р. № 9141/17-02-09).

Але у КМ України проект затримали (незважаючи на те, що раніше у профільних відділах його вивчали та претензії не виказували); уряд не виступив ініціатором внесення його до Верховної Ради України. Одна з причин цього – створення іншого, альтернативного законопроекту під назвою “Про інформацію персонального характеру”. Цей проект був внесений головою парламентського Комітету з питань правової політики Верховної Ради України третього скликання, зареєстрований у секторі реєстрації законопроектів апарату Верховної Ради України від 12.11.2001 № 7432 на заміну перероблені першої версії, зареєстрованої від 25.06.2001 № 7432.

Проект неодноразово розглядався в комітетах Верховної Ради України, але так і не був внесений на пленарне засідання. До нього було багато принципових зауважень (зокрема, від Комісара Ради Європи з питань захисту даних доктора Вольтраут Кочі), незважаючи на те, що він перероблявся та перереєстровувався. Остаточне рішення Комітету Верховної Ради України з питань свободи слова та інформації – відхилити та зняти з розгляду. З сутністю деяких зауважень до вказаного законопроекту можна ознайомитися у [15, с. 52-64]. Про що може йти мова, коли автори законопроекту вважають, що така категорія, як “інформація” має “характер”? З будь-якого словника відомо, що останнє поняття властиво біологічним істотам. Використання його у юриспруденції – це помилка “онімії”, коли одне й теж слово позначає різні речі.

Проте, навіть після зняття з розгляду, вищезгаданий проект не тільки перебував на сайті ВР України, у Переліку законопроектів з питань інформаційної політики, що перебувають на розгляді у ВР України, але й був розміщений за № 1 у розділі “Інформаційні

* Зміст проекту та деяка інформація про хід експертизи надана у [13].

ресурси”. У публікаціях ЗМІ та окремих офіційних документах проект також продовжував фігурувати як єдиний та перспективний, наприклад, див. [16].

У січні 2003 р. народні депутати України Родіонов М.К, Ніколаєнко С.М., академіки НАН України Юхновський І.Р., Толочко П.П. та Ситник К.М. виступили з правом законодавчої ініціативи щодо проекту Закону України “Про захист персональних даних (вих. Держкомзв’язку України від 20.12.2000 року № 9141/17-02-09). Законопроект був зареєстрований (від 10.01.2003 р. № 2618), **розглянутий у першому читанні** та **прийнятий за основу** Постановою ВР України від 15.05.2003 р. № 784-IV. Узагальнюючий висновок Головного науково-експертного управління апарату Верховної Ради України: *“За результатами розгляду в першому читанні проект Закону України "Про захист персональних даних” може бути взятий за основу з урахуванням викладених вище зауважень і пропозицій”*.

Згідно з поіменним голосуванням 15.03.2003 р.: **“за” законопроект – 244 депутати**, “проти” – 5 депутатів (О. Каменяш, В. Фіалковський, І. Гаврилюк, Е. Матвейчук, Т. Чорновил), “утримались” – немає, “не голосувало” – 167 депутатів. Рішення прийнято.

Проте, **у 2005 р.** у Міністерстві юстиції України **створюється робоча група**, до якої запросили представників недержавних організацій, що працюють у сфері захисту права на приватність [22]. Група отримала завдання створити альтернативний, але однойменний проект Закону України “Про захист персональних даних”.

Протягом двох років ця група робила проект, але він так і не був внесений до парламенту. Громадська рада з питань інформаційно-комунікаційних технологій у доповіді Президенту України під назвою “Про невідкладні заходи щодо розвитку інформаційного суспільства в Україні” повідомляла: *“Міністерством юстиції України розроблено новий законопроект з аналогічною назвою* (“Про захист персональних даних” – від авт.)*, при цьому ігнорується законопроект № 2618, вже прийнятий Верховною Радою України. Законопроект Міністерства юстиції України розкритикований правозахисниками та професійними організаціями як корупційно-небезпечний та такий, що не відповідає нормам європейського законодавства”*.

16 березня 2006 року Верховна Рада України **у другому читанні** розглянула проект Закону України “Про захист персональних даних” від 10.01.2003 р. № 2618.

За результатами законопроект був **прийнятий в цілому як Закон**. Згідно з поіменним голосуванням: **“за” законопроект – 287,** “проти” – 0, “утримались” – 1, “не голосувало” – 108. Рішення прийнято. Закон набирає чинності з 1 січня 2007 року.

На той час проект враховував уже понад 600 зауважень та пропозицій.

Безпосередньо його підтримали 18 докторів та 19 кандидатів наук.

Але… **11 квітня 2006 року Президент України повертає закон** на доопрацювання. *“Серед недоліків, які унеможливили підписання закону, була концепція права власності особи на власні персональні дані, яка, на думку* (радників – від авт.) *Президента, суперечить Конституції України”* [18].

На наш погляд, по-перше, вищезазначене формулювання не враховує положення статті 11 Конвенції РЄ № 108, яка, хочемо ми того чи ні, буде колись ратифікована Верховною Радою України та стане складовою частиною національного законодавства.

По-друге, слід дивитися у майбутнє щодо електронно-інформаційного простору, де регуляція суспільних відносин має деякий інший зміст та форму, що потребує від юриспруденції нетрадиційних підходів.

По-третє, щоб зрозуміти категорію “права власності особи на особисті персональні дані”, треба просто запитати самого себе: *що ти хочеш – щоб держава монопольно за-*

хищала твої особисті дані (що вона завжди робила, але персональні дані використовують так, як кому та де заманеться), або ти бажаєш отримати реальну юридичну нагоду самому їх захистити від свавілля чиновників та несанкціонованої комерції? Відповідає така постановка питання, зокрема букві та духу статті 3 Конституції України чи ні? Якщо з відповіддю виникають складнощі, пропонуємо звернутися до аргументів, що зазначені, зокрема в [10 – 12; 19; 20].

Повернемось до хронології.

З метою оцінки та врахування зауважень у Верховній Раді України було створено робочу групу. Але ніякої оцінки не було. Було “програмування” у напрямі – *про право власності людини на свої персональні дані не йдеться; персональні дані відносяться до “особистих немайнових прав”.*

Закон доопрацювали (прибрали “право власності людини на саму себе” та збільшили кількість термінів щодо інформатизації), переєстрували та відправили на третє читання.

9 січня 2007 р. Трете читання та **повторне голосування в цілому як Закон** після врахування пропозицій Президента: **“за” законопроект – 329** народних депутати України.

Але… **30 січня 2007 р. Закон знову повертається** до Верховної Ради України з новими зауваженнями – *невідповідність Закону положенням статті 32 Конституції України та міжнародно-правовим актам* [21].

У статті 32 Конституції України мова йде про поняття “конфіденційна інформація про особу” (з англ. confidence – довіра). У законопроекті “Про захист персональних даних” мова йде про поняття “персональні дані” (personal data), обсяг якого більший ніж обсяг поняття “довірча інформація” (“персональні дані” можуть бути довірчі, недовірчі, обмеженої обробки, поширення та використання, таємні тощо). Тільки поняття “персональні дані” застосовують у міжнародних стандартах та у національних законодавствах щодо їх захисту.

Враховуючи курс країни на євроінтеграцію та виходячи з того, що правозастосовна практика повинна орієнтуватися на “букву” положень міжнародних стандартів, стаття 32 Конституції України (до речі, й ЦКУ теж) потребує корегування та приведення у відповідність до термінології, яку застосовують у зазначених стандартах.

Стосовно зауваження щодо *“...невідповідності Закону ...міжнародно-правовим актам”.*

Взагалі не є зрозумілим – яким конкретно положенням міжнародно-правових актів законопроект не відповідає? Зазначена теза не має відповідних посилок та аргументації, що не надає їй логічної завершеності в доказах.

На жаль, подібний стан справ щодо звичайної відсутності аргументів та доказів має та продовжує мати місце всі роки оцінки законопроекту. Так, зокрема, до 2000 р. представники Харківської правозахисної групи не виказували до нього зауважень, навіть надали кошти на видання книги щодо захисту персональних даних [7], а у серпні 2007 р. зазначають, що законопроект *“абсолютно не враховував європейські стандарти із захисту персональних даних, часом плутаючи це з технічним захистом баз даних. У проекті не існувало жодних істотних гарантій збереження приватності в автоматизованих системах. Багато організацій звернулося до Президента з проханням застосувати право вето, що і було зроблено”* [22].

Виникає питання – яку мету може переслідувати зазначене зауваження? Мабуть – появу “панацеї – закону” із захисту персональних даних, яка надасть відповіді на всі ви-

падки життя, передусім щодо необмеженої свободи. Та навряд це можливо. Крім прав особи, є інтереси суспільства та держави, які слід враховувати, а не робити з поняття “свобода” абсолют.

Якщо є бажання “обійняти неосяжне”, то слід просто переписати та консолідувати всі документи Ради Європи та Європейського Союзу щодо захисту персональних даних в один закон. Приблизні розрахунки свідчать про те, що в зазначеній сфері вже є більш як 100 спеціалізованих документів (середня кількість аркушів одного з них – 20-30) не враховуючи інших євростандартів, ще опосередковано стосуються захисту персональних даних. Що це буде за нормативний акт, хто його буде читати та як їм користуватися? – ось у чому питання.

Щодо тезису ХПГ – *“у проекті не враховано питання телекомунікацій”*.

Хто сьогодні може знати, який розвиток матиме так зване е-середовище у майбутньому? Поява нових інформаційно-комп’ютерних технологій, телекомунікаційних засобів чи нових засобів комунікації на базі біо-, біохімічних- (зокрема, на амінокислотах), нанотехнологій, суміші зазначених та невідомих поки що технологій буде завжди вимагати внесення змінам у базовий закон, хоча питання може бути вирішено значно простіше, завдяки змін у галузевому законодавстві, зокрема щодо телекомунікацій.

Тобто мова у нас іде про базовий закон, а опоненти нескінченними зауваженнями за відсутності чіткості уявлення про те, що самі хочуть, схиляють законопроект у бік створення галузевого підзаконного акта.

Усьому свій час. Насамперед необхідно визначитися з принципами та видами діяльності у сфері захисту персональних даних, які затвердить Верховна Рада України. Потім усе інше, зокрема щодо створення механізму реалізації принципів, завдяки діяльності спеціально призначеного органу (нагляду) із захисту персональних даних. Тільки за таких умов можна отримати загальнодержавну системність у роботі щодо приведення законодавства України у відповідність до законодавства співтовариств Європи.

3. Реєстрація та ідентифікація фізичних осіб [*]

Тим часом, без законодавчої бази щодо захисту персональних даних, триває обговорення нормативно-правових актів щодо реєстрації та ідентифікації фізичних осіб [23] і паралельно – реальне створення Єдиного державного автоматизованого реєстру фізичних осіб (далі – ЄДАРФО), а також інших державних реєстрів, що містять персональні дані, зокрема, реєстру виборців. Відповідне розпорядження Кабінету Міністрів України від 03.07.2000 р. № 274 підписав тодішній Прем’єр-міністр В. Ющенко. Виробником ідентифікаційних документів визначався державний поліграфічний комбінат “Україна” як структура Мінфіну.

Незважаючи на відсутність законних підстав (Верховна Рада України протягом минулих років неодноразово відхиляла законопроекти щодо різних єдиних реєстрів[**]), Президент України Л. Кучма указом від 30 квітня 2004 р. № 500 “Про створення Єдино-

[*] Щодо підсумків стану справ впровадження протягом минулих двадцяти років урядами багатьох країн ідентифікаційних карток див. у розділі цього журналу *ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ*: **Заява Комітету Парламенту Канади з питань громадянства та імміграції від 4 жовтня 2003 року: “Національні ідентифікаційні картки (посвідчення особи)”**.

[**] Зокрема, у 2003 р. повідомлялося [//www.rupor.org], Комітет Верховної Ради України з питань державного будівництва та місцевого самоврядування не підтримав законопроект “**Про єдиний реєстр персональних даних**” через відсутність у ньому чіткого визначення прав та обов’язків органів реєстрації персональних даних тощо.

го державного реєстру фізичних осіб” санкціонував створення та ведення такого реєстру. Указом ця діяльність була вже покладена на МВС України на основі Єдиної державної автоматизованої паспортної системи (ЄДАПС), концепція якої була затверджена постановою уряду ще в січні 1997 р.

Для виконання робіт зі створення паспортної системи МВС України визначило приватну компанію – корпорацію “ЄДАПС”. Таким чином, персональні дані, які громадяни України передавали державному органу, потім передавалися приватній структурі. Пізніше керівництво МВС України передало цій приватній структурі також і питання видачі бланків для паспортів, базу даних ДАІ та інші.

Президент України В. Ющенко указом від 10 березня 2005 р. за № 457/2005 анулював попередні рішення Президента Л. Кучми щодо створення Єдиного державного реєстру фізичних осіб (згаданий вище указ від 30 квітня 2004 р.), а разом з тим й наміри запровадити паспорт нового зразка у вигляді пластикової картки на основі ЄДАПС [25].

Проте парламент 15 грудня 2006 р. прийняв у першому читанні проект закону “Про Національний демографічний регістр”[26]. Цей проект є перефразованим прообразом старих проектів законів про ЄДАРФО.

Головна суть цього та попередніх проектів – створення єдиної автоматизованої бази даних про громадян, де б під одним номером (єдиним або універсальним ідентифікатором) збиралася вся інформація про всіх громадян України, що накопичується органами влади та державними установами. Такий підхід може призвести до порушення права на персональні дані. Саме тому, Конституційний суд Угорщини ще в 1991 р. визнав систему з універсальним ідентифікатором антиконституційною. Її не застосовують в жодній розвинутій демократичній країні. Проте Верховна Рада України надала “зелене світло” щодо його створення. Фактично, як видно з попереднього, ця система й так створюється за заочним принципом без жодного належного правового обґрунтування.

На початку 2007 р. Верховна Рада України прийняла закон про державний реєстр виборців. Проект цього закону знаходився в парламенті з лютого 2004 р. Можна вважати, що цей проект є позитивним з точки зору дотримання права на захист персональних даних, хоча й не містить процедури незалежного контролю за використанням цього реєстру.

Президент України доручив Секретарю Ради національної безпеки і оборони України (далі – РНБОУ) підготувати засідання РНБОУ з питань удосконалення роботи, пов’язаної з виготовленням, оформленням і видачею паспортних документів та приведенням їх до міжнародних стандартів системи реєстрації фізичних осіб.

23 лютого 2006 р. за розпорядженням Секретаря РНБОУ було утворено відповідну робочу групу. Такий розвиток подій свідчить про те, що **питання** паспортної системи та **реєстрації осіб віднесено до категорії таких, що впливають на національну безпеку**.

Проте, незважаючи на скасування відповідних указів Президента, МВС України продовжує створювати ЄДАПС. На це виділяються кошти в державному бюджеті, й надалі видаються закордонні паспорти раніше встановленого зразку.

У жовтні 2005 р. МВС подало до Кабінету Міністрів України пакет документів з метою *“зробити картку громадянина України у вигляді пластикової картки із вшитим електронним чіпом, який буде серйозно захищено, і він матиме номер картки, який буде єдиним для використання як у Податковій, так і в Пенсійному фонді. Чіп міститиме всю необхідну інформацію про людину, і, крім того, у цей чіп можна буде ввести інформацію про наявність водійського посвідчення”*.

До цього зазначимо, що у наш час у ЄС та США запроваджуються так звані біометричні паспорти, у яких чіпи (коштує 59 євро [//www.profile.ru]) зберігають, крім звичайної інформації, дані про відбитки пальців і сітківки ока. В одній тільки Великобританії на цю програму витрачено майже мільярд доларів (контрольна система біометрії у ЄС коштує 97 млн. євро). Проте, як повідомляється в [//www.untro.ru], хакер зміг зламати код такого паспорта і скопіювати інформацію на інший чіп, який можна встановити у фальшивому документі. Це може бути свідченням ненадійності технологій та даремності таких паспортів.

До теперішнього часу вказана вище ініціатива МВС України не почала впроваджуватися у повному обсязі, хоча на практиці уже давно реалізується без жодних законів.

На таку ініціативу Українська Гельсінська спілка правозахисників надіслала звернення до Прем’єр-міністра України та розпочала збір підписів громадян під відкритим листом до влади [27]. Правозахисники вимагають врахування наступних важливих для захисту персональних даних моментів щодо:

а) пластикової картки:

- прийняти закон про захист персональних даних;
- виробництвом картки має опікуватися лише державна структура;
- особа повинна мати можливість знати, які її персональні дані містить код картки, та мати можливість їх змінити.

б) ідентифікаційного коду особи:

- різні коди повинні використовуватися окремо, не допускається створення єдиного ідентифікаційного коду для накопичення всієї інформації про особу;
- коди повинні використовуватися лише для тих цілей, для яких вони були створені;
- їх використання повинне бути обумовлене в законі про захист персональних даних.

У наш час основним електронним класифікатором, на основі якого відбувається збір та обробка персональних даних громадян України, є ідентифікаційний код, що надається Державною податковою адміністрацією. Сфера його використання постійно розширюється і виходить далеко за межі тієї мети, з якою він був запроваджений – податковий облік. За відсутності ідентифікаційного коду неможливими є легальне працевлаштування, доступ до пенсійного забезпечення, реалізація права на освіту, отримання стипендій та допомоги з безробіття, оформлення субсидій, відкриття банківських рахунків, реєстрація підприємницької діяльності тощо.

Проте, як стверджують правозахисники [22], сьогодні має місце практика порушення Закону України “Про єдиний реєстр фізичних осіб-платників податків” і використання податкового номера для інших цілей, не передбачених цим Законом.

Процес обробки персональних даних у комерційних цілях усе більше перетворюється на процвітаючий бізнес. Як вже зверталась увага (див. [11, с. 45-48]), за деякими джерелами, **(!) грошовій оборот на світовому ринку персональних даних досягає 3 млрд. доларів на рік.**

Сьогодні відомості про людину збираються й акумулюються різними державними органами (при влаштуванні на роботу, податковими органами, органами внутрішніх справ, органами реєстрації юридичних осіб, при народженні й одержанні у наступному різних документів актів цивільного стану, медичними установами, органами реєстрації прав на нерухоме майно, при створенні приватних підприємств, бюро технічної інвентаризації, комунальними службами та ін.) і приватними структурами (медичні, юридичні організації, стільникові компанії, туристичні фірми, магазини тощо).

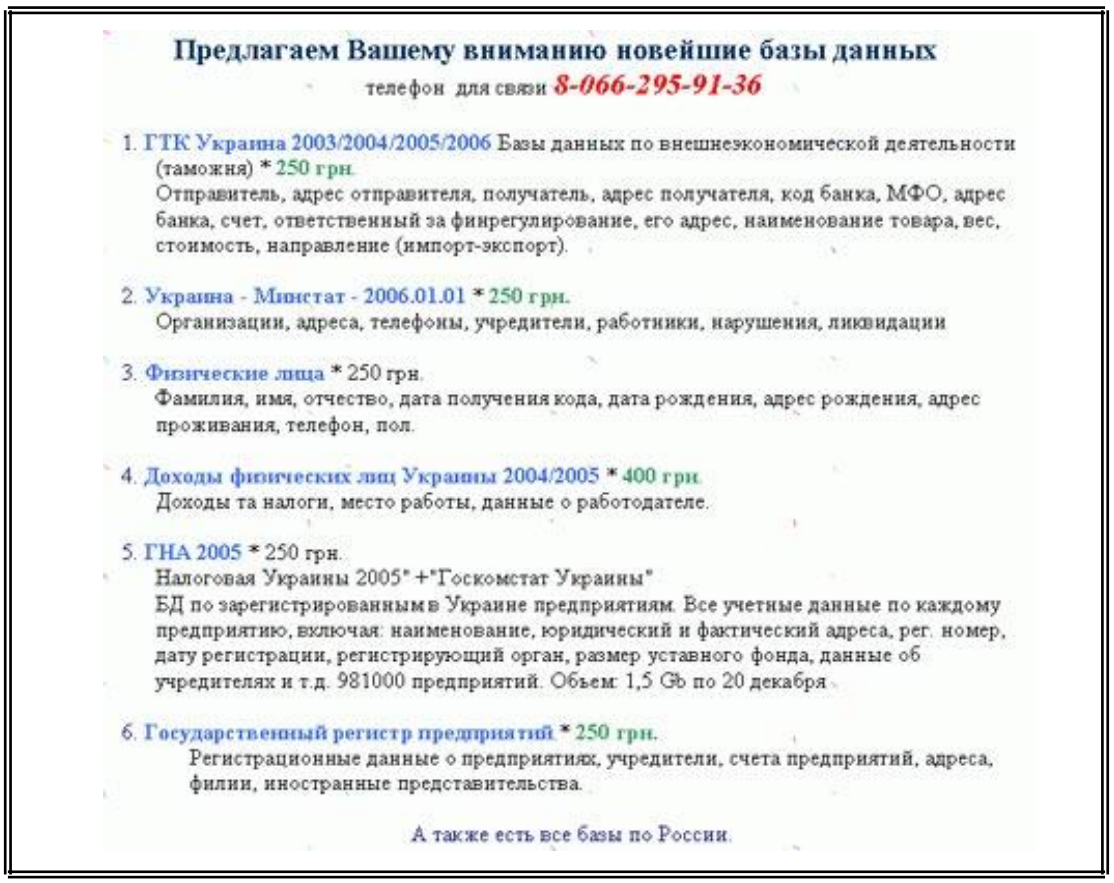
Наприклад, роблячи покупки в Інтернет-магазинах або отримуючи дисконтні картки, споживач повідомляє свої персональні дані. Власники магазинів, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини, навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку. Останнє в умовах ринку – значний важіль у конкурентній боротьбі. Більш того, якщо хтось почав збирати персональні дані, інші вимушені робити теж саме.

Придбати комп’ютерні бази даних, що містять персональні дані, можна на кожному кроці – на ринку, за допомогою різних оголошень, в Інтернеті тощо.

Так у Росії, зокрема пропонуються такі бази даних, власниками яких є державні органи [28]:

Назва бази персональних даних	**Ціна** (руб)
БД “Приватні особи м. Москви та Московської області”	$ 150
БД “Приватні особи Росії та СНД” (включає е-адресу)	$ 200
БД “Фізичні особи Московської області”	1000
БД “Жителі Московського регіону” (повні відомості щодо паспорта)	400
БД “Прописка у м. Москві”	500
БД “Прописка у Московській області”	400
БД “Квартири та їх власники м. Москви”	1000
БД “Приватизовані квартири м. Москви”	400
БД “Експортно-імпортні операції” (товар, вартість, постачальник, споживач тощо)	1400
БД Московської ліцензійної палати (про ліцензії)	400
БД Московської реєстраційної палати (про юридичних осіб і приватних підприємців)	500
БД Московської обласної реєстраційної палати	500
БД Московського земельного комітету	200
БД “ДАІ м. Москви” (повні відомості про автомобілі та їх власників)	500
БД “Посвідчення водія у м. Москва”	500
БД “Посвідчення водія у Московській області”	500
БД “Мобільні телефони Московського регіону”	500
БД “Єдина міська телефонна мережа м. Москви”	500
БД “МГТС 2003” відомості щодо усіх телефонних номерів та абонентів	500
БД “Банки Росії” (усі реквізити)	300

В Україні, для прикладу, маємо таке оголошення [22]:



Предлагаем Вашему вниманию новейшие базы данных

телефон для связи *8-066-295-91-36*

1. ГТК Украина 2003/2004/2005/2006 Базы данных по внешнеэкономической деятельности (таможня) * 250 грн.
   Отправитель, адрес отправителя, получатель, адрес получателя, код банка, МФО, адрес банка, счет, ответственный за финрегулирование, его адрес, наименование товара, вес, стоимость, направление (импорт-экспорт).

2. Украина - Минстат - 2006.01.01 * 250 грн.
   Организации, адреса, телефоны, учредители, работники, нарушения, ликвидации

3. Физические лица * 250 грн.
   Фамилия, имя, отчество, дата получения кода, дата рождения, адрес рождения, адрес проживания, телефон, пол.

4. Доходы физических лиц Украины 2004/2005 * 400 грн.
   Доходы та налоги, место работы, данные о работодателе.

5. ГНА 2005 * 250 грн.
   Налоговая Украины 2005" +"Госкомстат Украины"
   БД по зарегистрированным в Украине предприятиям. Все учетные данные по каждому предприятию, включая: наименование, юридический и фактический адреса, рег. номер, дату регистрации, регистрирующий орган, размер уставного фонда, данные об учредителях и т.д. 981000 предприятий. Объем: 1,5 Gb по 20 декабря

6. Государственный регистр предприятий * 250 грн.
   Регистрационные данные о предприятиях, учредители, счета предприятий, адреса, филии, иностранные представительства.

А также есть все базы по России.

При цьому ДПА, яка адмініструє більшість із цих баз даних, заявляє, що в них не зафіксовано витоку інформації. Проте іншим шляхом, ніж скопіювати цю базу даних у ДПА, отримати такі дані просто неможливо. Тому заперечувати витік інформації в такій ситуації є просто безвідповідальним. Це ж стосується й ДАІ.

За даними СБУ, протягом 2006 року було припинено 28 спроб продажу баз даних державних установ та організацій, які містять конфіденційну інформацію, що належить державі [29]. Більш детальна інформація про ці випадки, зокрема, чи були притягнуті до відповідальності особи та які саме бази даних вони намагалися продати, відсутня.

Висновки та пропозиції.

Щодо перспектив нормативно-правового упорядкування відносин у сфері захисту персональних даних за умов гармонізації положень національного законодавства з положеннями міжнародних стандартів маємо зазначити на необхідності здійснення таких першочергових кроків:

Перше. Ратифікувати Конвенцію Ради Європи № 108 “Про захист прав осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. та Додатковий протокол до неї щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р. Це є можливим лише за умов виконання положення статті 4 Конвенції РЄ № 108, початком чого є прийняття національного базового закону щодо сфери захисту персональних даних.

Друге. Прийняти Закон України “Про захист персональних даних”. Головне в цьому є те, що поки зазначений закон не набере чинності, зупинити несанкціоновану коме-

рцію щодо збору, обробки, поширення і продажу баз персональних даних навряд чи можливо.

Вважаємо, що для остаточного вирішення питання щодо прийняття закону та створення в Україні базових умов із захисту персональних даних необхідно повернутися до редакції законопроекту від 16 березня 2006 р., який був розглянутий Верховною Радою України та прийнятий у другому читанні та в цілому як Закон (текст закону див. у [13]).

Головне у цьому питанні наступне – ми наполягаємо на запровадженні в законодавстві України юридичній категорії “право власності людини на свої персональні дані”. За усі роки (з 1997 по 2007 рр.) від опонентів законопроекту не отримано аргументів, які надали б чітку та однозначну відповідь на запитання – *чому людина не може мати зазначене вище право, яке нами розглядається як “право кожного на самого себе”? і чому пропозиція не відповідає чинній Конституції (зокрема, статті 3), а також правам та основоположним свободам людини і громадянина, які визначені міжнародними стандартами?*

Посилання критики у питаннях захисту персональних даних на так звані “особисті немайнові права” (зокрема, щодо Глави 20 ЦКУ), коли предмет даних (як зазначають опоненти) не має майнового змісту, у сучасних умовах поширеної діяльності з продажу персональних даних не відповідає дійсності. Персональні дані сьогодні збираються, обробляються, продаються та купуються будь-де й, звичайно не санкціоновано.

Теза – *це не може бути (про право людини на свої персональні дані), тому що не було ніколи*, не є аргументом у доказах.

Третє. Створити механізм щодо Уповноваженого органу з питань захисту персональних даних в Україні.

Враховуючи особливості діяльності засобів масової інформації, є необхідність призначення окремого уповноваженого з питань захисту персональних даних у зазначеній галузі.

Четверте. Запровадити у державі Судову палату з питань захисту персональних даних та почати підготовку кваліфікованих фахівців для цієї сфери.

П’яте. Галузеве законодавство із захисту персональних даних має виходити з того, що універсальний ідентифікатор фізичних осіб:

- може бути тільки за галузевою ознакою;
- має використовуватися лише для тих цілей, для яких він був запроваджений.

Шосте. Єдина державна автоматизована паспортна система (ЄДАПС) має запроваджуватися лише на законних підставах з урахуванням положень Конвенції Ради Європи № 108. Виготовленням документів, зокрема, електронних карток, з персональними даними громадян України повинно здійснюватися лише державною структурою.

Сьоме. На наш погляд, практика, коли співробітники міністерств та комітетів розробляють проекти нормативно-правових актів, не відповідає потребам часу. Це має просте пояснення.

Міністерства та комітети – це органи виконавчої влади держави, які вимушені працювати за наказами та в інтересах держави. Держава як “неживе” формування не може бути підзвітне громадянам, і тим більше суспільству. За цим стоїть воля живих суб'єктів, підзвітності яких добитися завжди складно, якщо й неможливо. Тому інтереси окремої людини та суспільства завжди будуть не на передньому плані, які б аргументи навпаки не наводились.

Функції міністерств та ін. органів виконавчої влади не передбачають проведення науково-дослідної роботи щодо юриспруденції. У цьому плані вони виконують експертні та наглядові функції стосовно відповідності положень проектів нормативно-правових актів положенням чинної Конституції.

Розробка законів та підзаконних актів може та повинна здійснюватися тільки в науково-дослідних інститутах, які мають відповідну спеціалізацію або на конкурсній (тендерній) основі між організаціями, які здатні виконати роботу. Але якщо тендери (з анг. слово “тендер” перекладається як “паровозна бочка з водою”) щодо розподілу грошей з держбюджету будуть й надалі мати формальний зміст їх організації, а гроші виділятимуть за політичними або суб'єктивними інтересами (що є поширеною практикою), то “розмішування води у ступі” під прикриттям проведення конкурсного змагання й у подальшому не буде відповідати інтересам як суспільства, так і держави.

Використана література

1. Рада Європи: діяльність та здобутки; Ред. О. Павличенко. – К.: Право, 1999. – 88 с.

2. Європейський Союз: словник-довідник; Ред. М. Марченко. – К.: К.І.С., 2005. – 142 с.

3. Конвенція Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. та Додатковий протокол до Конвенції Ради Європи № 108 від 8 листопада 2001 року. Офіційний переклад з англ. засвідчено МЗС України від 01.07.2002 р. // Правова інформатика. – № 2/2004. – 77-85.

4. *А. Баранов*. Персональные данные: есть ли проблемы? // Зеркало недели, 15.06.1996 р.

5. Защита персональных данных // Деловая Украина, 8.10.1997 р.

6. Защита персональных данных. – К.: Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.

7. Права человека и защита персональных данных. – К., Государственный комитет связи и информатизации Украины, 2000 г. – 280 с.

8. Правовий механізм захисту персональних даних: Монографія. – К.: Парлам. вид-во, 2003. – 120 с.

9. Організаційно-правові питання захисту персональних даних: Дис. …канд. юрид. наук: 12.00.07 – К.: Науково-дослідний центр правової інформатики АПрН України, Національна академія державної податкової служби України, 2004. – 251 с.

10. Інформаційне право та правова інформатика у сфері захисту персональних даних: Монографія; За ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – К.: НДЦПІ АПрН України, 2006 р. – 450 с.

11. До питання економічного аспекту захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-54.

12. До питання е-торгівлі та захисту персональних даних // Правова інформатика. – № 1(13)/2007. – С. 12-25.

13. Про прийняття Верховною Радою України в цілому Закону України “Про захист персональних даних” // Правова інформатика. – № 3(11)/2006. – С. 80-90.

14. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності: Посібник. Кн. 2; За ред. члена-кореспондента АПрН України М. Швеця та к.ю.н. Б.Романюка. – К.: НДЦПІ АПрН України, 2006 р. – 509 с.

15. Про зняття з розгляду Верховною Радою України законопроекту “Про інформацію персонального характеру” // Правова інформатика. – № 2(6)/2005. – С. 52-64.

16. Лист Інституту законодавства Верховної Ради України Голові Комітету Верховної Ради України з питань науки і освіти від 02.11.2004 р. № 22/438-6-2 (додатково від 05.11.2004 р. № 06-6/9-2760), стор. 4.

17. Первые судебные решения о личном идентификационном коде в Венгрии //www.khpg.org/index.php?id=1084718376.

18. Верховна Рада проголосувала Закон “Про захист персональних даних”, ветований Президентом у квітні 2006 року. Інститут Медіа Права, 17.01.2007 //www.telekritika.kiev.ua/articles /138/0/8423/verkhovna_rada_prgolosuvala_pro_zakhist_personalnikh_danikh_vetovanij_prezidento.

19. е-майбутнє та інформаційне право. – К.: НДЦПІ АПрН України. – 2006. – 302 с.

20. е-боротьба в інформаційних війнах та інформаційне право: Монографія. – К.: НДЦПІ АПрН України, 2007 р. – 234 с.

21. //www.gska2.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=27270.

22. //www.khpg.org/index.php?id=1186147137.

23. Щодо реєстрації, ідентифікації фізичних осіб та захисту персональних даних // Правова інформатика. – № 4/2004. – С. 38-48.

25. ДЗГ МВС України в Інтернеті //mvsinfo.gov.ua/official/2005/03/031805_1.html.

26. Проект Закону України від 14.09.2006 р. № 2170. Автори законодавчої ініціативи: В. Цушко, А. Семинога, М. Оніщук та інші.

27. //www.helsinki.org.ua/index.php?id=1130842348.

28. //www.kiev-security.org.ua/box /4/136.shtml.

29. Повідомлення Прес-центру СБУ від 02.10.2006 р. //www.sbu.gov.ua.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 347.82:681.3

В. ЦИМБАЛЮК, *кандидат юридичних наук, старший науковий співробітник,*
директор науково-дослідного центру, професор кафедри конституційного і адміністративного права Інституту повітряного і космічного права Національного авіаційного університету

ДО МЕТОДОЛОГІЇ МІЖГАЛУЗЕВОГО ВЗАЄМОЗВ’ЯЗКУ З ОРГАНІЗАЦІЙНО-ПРАВОВИМ ЗАБЕЗПЕЧЕННЯМ СИСТЕМНОСТІ ІНФОРМАТИЗАЦІЇ

(на прикладі інституціоналізації інформаційних правовідносин у сфері повітряного транспорту)

Анотація. *Про підвищення ефективності правового забезпечення суспільних відносин щодо інформатизації у сфері цивільної авіації.*

Важливим теоретико-прикладним аспектом сучасного правознавства у нашій країні є структуризація нових комплексних галузей права. Необхідність їх виникнення зумовлена бурхливим розвитком відповідних галузей суспільних відносин під впливом нових здобутків науково-технічного прогресу. До нових галузей права, що динамічно почали розвиватися на рубежі XX-XXI століть і які заявили про необхідність їх виділення з традиційних галузей права, можна віднести інформаційне право та повітряне право. Нині вони в України розглядаються як комплексної галузі права, джерелами яких є провідні галузі права – адміністративне, цивільне та кримінальне право, а також ряд інших комплексних галузей права: господарське, екологічне та інші.

У порядку постановки проблеми у загальному вигляді та її зв’язку з важливими науковими і практичними завданнями можна зазначити, що для формування нових галузей права притаманні ряд питань, пов’язаних з їх структуризацією, зокрема на рівні інститутів цих галузей права.

Аналіз останніх досліджень, у яких започатковано розв’язання проблем стосовно питань інституціаналізації інформаційного права та його взаємозв’язку з регулюванням інформаційних відносин у сфері повітряного права, зокрема його складової – авіаційного права та інформаційної безпеки цивільного повітряного транспорту, свідчить, що таких комплексних наукових розвідок не проводилося.

Можливо це зумовлено тим, що повітряне право довгий час розглядалося тільки як інститут такої підгалузі адміністративного права, якою є транспортне право. В Україні на рівні органу державного управління сфера транспорту об’єднана із сферою зв’язку: у Міністерстві транспорту і зв’язку. Нагромадження у цьому міністерстві адміністративних структур усіх видів транспорту і зв’язку в Україні значно стримує його наукову підтримку, зокрема стосовно організації правового забезпечення функціонування повітряного транспорту. Можливо, це є і одним з факторів того, що наука повітряного права розвивалася в Україні досить повільно, що не відповідає потребам практики.

Інституціоналізія повітряного права як комплексної галузі права України передбачає розробку наукового базису концептуальних засад формування в системі цього права, в його особливій (чи спеціальній) частині, інституту правового забезпечення суспільних відносин щодо інформації, інформатизації та інформаційної безпеки у повітряному просторі, у тому числі як підінституту в його складі – правового забезпечення суспільних відносин щодо інформатизації у сфері цивільної авіації.

© В. Цимбалюк, 2008

Виходячи із спільності загального предмета дослідження такої комплексної галузі права, як інформаційне право та специфіки предмета наукового інституту повітряного права – правового забезпечення суспільних відносин щодо інформатизації у сфері цивільної авіації можна стверджуватися, що теорія повітряного права цілком може запозичити окремі методологічні положення у науки інформаційного права та у правової інформатики. Методологічні положення інформаційного права цілком екстраполюються на методологію повітряного права стосовно інформатизації у сфері цивільної авіації.

При цьому пропонується спиратися на результати наукових досліджень, які знайшли відображення у публікаціях українських дослідників сфери інформаційного права, правової інформатики та інформаційної безпеки, зокрема: М.Я. Швеця, Р.А. Калюжного, В.К. Шкарупи, В.М. Брижка, О.А. Баранова, К.І. Бєлякова, В.Д. Гавловського, В.К. Гіжевського, А.І. Марущака та багатьох інших , див., зокрема [1 – 16].

У сучасному науково-практичному, широкому юридичному розумінні інформатизація розглядається комплексно. ***Інформатизація – це множина взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих та інших процесів, які спрямовані на формування умов для задоволення інформаційних потреб громадян, суспільства та держави через створення, застосування і розвиток інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі сучасної електронно-обчислювальної (комп’ютерної) та комунікаційної техніки.***

У вузькому змісті *інформатизація – це багатофункціональна діяльність, спрямована на створення та широкомасштабне застосування в усіх сферах життя суспільства комп’ютерних інформаційних технологій.*

Інформатизація за сутністю є проявом інформатики. Зміст інформатики можна розглядати у декількох аспектах. Серед них пропонується звернути увагу на наступні.

Інформатика: 1) соціально-технічна сфера діяльності, базою якої є здобутки науково-технічного прогресу стосовно створення, обробки, зберігання інформації, а також телекомунікації за допомогою автоматизованих електронно-обчислювальних систем (комп’ютерів) та заснованих на них технологій; 2) наука про системну інформатизацію різноманітних сфер суспільного життя.

Створення, функціонування і розвиток комп’ютерних інформаційних систем у сфері цивільної авіації України є важливої складовою єдиного інформаційного простору України та глобального інформаційного простору. Норми суспільних відносин в інформаційному просторі тісно переплітаються з нормами суспільних відносин, що виникають, здійснюються та припиняються у повітряному просторі.

У контексті положень теорії права можна зазначити, що норми правил поведінки суб’єктів суспільно-технічних відносин у повітряному просторі тісно інтегровані з нормами правил поведінки інформаційних відносин. По суті вони, утворюючи умовно автономну сферу в інформаційному просторі, є виразом окремих правовідносин суб’єктів повітряного простору. Таким чином, можна зазначити, що формування правового забезпечення інформаційного простору у сфері правовідносин, що виникають стосовно повітряного простору в цілому, і суспільних відносин у сфері цивільної авіації є важливими інституціями повітряного права, у тому числі й у контексті підтримки інформаційної безпеки польотів цивільного авіаційного транспорту.

У контексті безпекології інформаційна безпека у сфері авіації є однією з важливих складових безпеки у повітряному просторі, у тому числі щодо об’єктів цивільної авіації.

Однією з важливих сучасних складових формування інформаційної сфери суспільних відносин у повітряному просторі можна вважати правовідносини щодо створення

комп’ютерної інформаційно-аналітичної системи нормативно-правових актів у галузі регулювання діяльності цивільної авіації (ЦА) України. Це необхідно для розроблення і узгодження проектів нормативно-правових актів, зокрема: нової редакції Повітряного кодексу України, Зводу авіаційних правил України (АПУ) та інших у рамках гармонізації нормативно-правової бази України із законодавством про цивільну авіацію і повітряний простір країн Європейського Союзу (ЄС) та інших держав.

Національне законодавство України з питань діяльності ЦА має розвинуту систему правових норм. Але, враховуючи, що в Україні нині активно йде розбудова інформаційного суспільства також, існує нагальна потреба правового упорядкування суспільних відносин стосовно процесів, пов’язаних зі створенням, розвитком і застосуванням комп’ютерних інформаційних систем різного функціонального призначення.

Більш ефективне правове забезпечення суспільних відносин у повітряному просторі, у тому числі інформаційних та пов’язаної з цим наземної інфраструктури, нині можливо із застосуванням сучасних комп’ютеризованих інформаційних систем правової інформації. Це вимагає розроблення основних засад удосконалення правового забезпечення інформатизації, впровадження здобутків інформатики в ЦА відповідно до вимог Конституції України та інформаційного законодавства.

При цьому можна виділити наступні завдання:

- приведення правового забезпечення розробки, впровадження і застосування здобутків інформатики в ЦА у відповідність з чинним інформаційним законодавством України;
- розробка проектів законодавчих актів щодо удосконалення правового забезпечення інформатизації в ЦА;
- науковий супровід процесу їх прийняття в органах державної влади, а також впровадження в життя прийнятих законопроектів, у тому числі через систему вищої освіти;
- створення комп’ютерної інформаційно-аналітичної системи нормативно-правових актів у сфері ЦА з елементом автоматизованої інформаційно-довідкової системи наукових досліджень в галузі повітряного права України та міжнародного повітряного права;
- впровадження зазначеної комп’ютерної інформаційно-аналітичної системи в діяльність структур ЦА, у тому числі через впровадження у навчальний процес, зокрема в Національному авіаційному університеті (як спеціалізованому вищому навчальному закладі, який здійснює цільову підготовку фахівців широкого спектра з вищою освітою для діяльності у сфері правовідносин, пов’язаних з повітряним простором.

Для реалізації зазначеного у Національному авіаційному університеті створено базис науково-навчальної інфраструктури –Інститут повітряного і космічного права.

Підвищення якості комплексного правового забезпечення суспільних відносин у повітряному просторі пропонується, як перший етап, провести через модернізацію науково-навчальної складової. Для цього вже створено певну організаційно-правову основу на рівні Кабінету Міністрів та Міністерства науки і освіти України, а також керівництва Національного авіаційного університету. До реалізації зазначеного як загальнодержавного проекту пропонується залучити керівництво Державного авіаційного агентства та підприємства цивільної авіації України.

Перший організаційно-правовий крок до створення державного програмно-цільового проекту пропонується зробити через реорганізацію Інституту повітряного і космічного права НАУ в науково-навчальний комплекс з виділенням у ньому трьох провідних складових: наукової та двох навчальних. Кожна з цих складових повинна бути інтегрована з відповідними практичними структурами Державного авіаційного агентства.

Для підвищення ефективності функціонування зазначеного науково-навчального комплексу нагальною є реорганізація Науково-дослідного центру Інституту повітряного і космічного права НАУ. В цьому Центрі пропонується визначити і виділити чотири провідні функціональні структури на рівні відділів: відділ повітряного права, відділ екологічного права у сфері повітряного простору, відділ правової інформатики та відділ космічного права. Для залучення висококваліфікованих науковців-правознавців штатну структуру Центру слід визначити відповідно до законодавства України про наукову і науково-технічну діяльність.

Використана література

1. *Гавловський В., Кашпур В. Цимбалюк В.* Державно-правове регулювання соціальних інформаційних відносин // Українське право. – 1998. – №1. – С. 173-176.
2. *Гриценко В., Гавловський В., Колпак Р., Цимбалюк В.* Поступ України до інформаційного суспільства (організаційно-правовий аспект). Збірник наукових праць (м. Ірпінь) // Науковий вісник. – 2001. – № 3 (13).– С. 184-187.
3. *Калюжний Р., Гавловський В., Швець М., Цимбалюк В.* Інформаційне законодавство України: концептуальні основи формування // Право України. – 2001. – № 7. – С. 88-81.
4. *Рогатюк І., Середа Г., Цимбалюк В.* Концептуальні засади наукового забезпечення інформатизації прокуратури // Вісник прокуратури. – 2006. – № 5. – С.14-19.
5. *Гуцалюк М., Цимбалюк В., Гавловський В.* Удосконалення інформаційного законодавства як засіб оптимізації протидії комп’ютерній злочинності // Науковий вісник Національної академії внутрішніх справ України. – 2001. – №3. – С.20-24.
6. *Цимбалюк В*. Питання організаційно-правового забезпечення інформатизації як провідного напрямку модернізації державної податкової служби України // Науковий вісник Національної академії державної податкової служби України. – 2004. – № 2 (24). – С. 135-141.
7. *Цимбалюк В.* Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) // Підприємництво, господарство, право. – 2004. – № 3. – С. 88-91.
8. *Цимбалюк В.* Сутність і зміст правової інформатики (методологічний аспект) // Правова інформатика. – 2005. – № 4(8). – С. 18-30.
9. *Цимбалюк В.* Роль правової інформатики у модернізації прокуратури України // Право України. – 2006. – № 11. – С. 73-77.
10. *Цимбалюк В.* Правові аспекти створення єдиної комп’ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю в Україні //Боротьба з організованою злочинністю і корупцією (теорія і практика). – К.: МНДЦ з проблем боротьби з організованою злочинністю РНБО України. – 2006. – № 14. – С.193-200.
11. *Цимбалюк В.* Щодо формування стратегії інформатизації прокуратури України в умовах розвитку інформаційного суспільства // Вісник прокуратури. – 2007. – № 5. – С. 92-99.
12. *Цимбалюк В.* Наукові джерела інформаційного права України // Бюлетень Мін’юсту України. – 2007. – № 5. – С. 28-76.
13. *Цимбалюк В.* Кримінологічний аспект Інтернет-торгівлі // Малий і середній бізнес. – 2007. – №1. – С. 26-33.
14. *Цимбалюк В.* Методологія інформаційного права як комплексної галузі юридичної науки (засадничі, принципові положення) // Правова інформатика. – 2007. – № 3(15). – С. 40-51.
15. *Цимбалюк В.* Інституціоналізація інформаційної безпеки в інформаційному праві України // Бюлетень Мін’юсту України. – 2007. – № 8(70). – С. 45-53.
16. *Шкарупа В. Цимбалюк В.* Застосування положень права щодо формування основ теорії інформаційного права // Правова інформатика. – 2006. – № 3(11). – С. 44- 51.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 341.018

М. РАСКАЛЄЙ, Науково-дослідний інститут фінансового права

ІНФОРМАЦІЙНА ГЛОБАЛІЗАЦІЯ В ГАЛУЗІ ПОВІТРЯНОГО ПРАВА

Анотація. *Щодо розробки та прийняття нового Повітряного кодексу.*

Залежно від рівня соціально-економічного розвитку, географічного розташування, забезпечення територіальної цілісності, національної безпеки та суверенітету, що відображаються у концепції національного інтересу, будується зовнішня політика будь-якої держави. Відстоювати свої національні інтереси, забезпечувати власну національну безпеку – це майже обов’язок кожної держави, яка не має на меті втратити своєї самостійності та незалежності, адже наслідком для держави, яка буде неспроможна відповісти на загрози та виклики, пов’язані з глобалізацією, адекватним чином, може стати неминуче послаблення та деградація цієї держави.

Таким чином, виникає питання: що ж таке глобалізація? Термін “глобалізація” вживається не тільки в економіці, праві, але й у політиці, в суспільному житті та в усьому, що стосується світових процесів, які поширилися і продовжують поширюватися зараз. Проте, не зовсім зрозуміло, що ж таке глобалізація в її первісному значенні.

Єдиного поняття процесу глобалізації не існує. Наука на сьогодні має чимало визначень феномену глобалізації. Коротке, але змістовне, російського вченого М. Чешкова: *“Глобалізація – процес з’єднання різних компонентів людства під час його еволюції на противагу процесу диференціації людства”* [1]. Більш ґрунтовне і придатне для наших цілей – американського дослідника Т. Фридмана, у якого глобалізація – це *“нестримна інтеграція ринків, націй-держав і технологій, що дозволяє індивідам, корпораціям і націям-державам досягати будь-якої точки світу швидше, далі, глибше і дешевше, ніж будь-коли раніше... Глобалізація означає поширення капіталізму вільного ринку практично на всі країни світу. Глобалізація має свій власний набір економічних правил, які базуються на відкритості, дерегуляції й приватизації національних економік з метою зміцнення їх конкурентоспроможності і більшої привабливості для іноземного капіталу”* [2]. Але всі визначення не містять вичерпної характеристики глобалізації і не відповідають на питання, чому саме вона на початку нового тисячоліття стала причиною можливості зіткнення цивілізацій.

Можливо виділити загальні риси цього поняття. Перш за все необхідно зазначити, що глобалізація – це історичний процес, який відбувається впродовж багатьох століть, тобто це реальний процес, який розвивається у всіх галузях суспільного життя. Глобалізація розвивається та має певні мережі: телекомунікації, транспорт, фінанси. Добре, якщо ці мережі впорядковані та контрольовані [3]. Беручи до уваги напрям, що на сьогодні викликає найбільше зацікавлення, можна дати визначення глобалізації як посилення взаємозалежності національних економік та законодавств, переплетення соціально-економічних процесів, що відбуваються у різноманітних регіонах світу і спонукають уряди та юридичних осіб у процесі своєї діяльності до пошуку кращих умов діяльності, цей процес глобалізації є ключем до майбутнього розвитку світової економіки як неминучий процес. Існує точка зору про те, що глобалізація – це процес, направлений та керований, оскільки у ньому є лідери, хтось охоче бере в ньому участь, хтось за це платить, хтось опирається цьому процесу, хтось ним просто користується. Тобто глобалізація є процесом керованим, і успіх у керуванні нею залежить від уміння “сторін” домовлятись між

© М. Раскалєй, 2008

собою. Під “сторонами” в даному випадку розглядаються не держави в цілому, а транснаціональні корпорації (далі – ТНК) як вагомі економічні структури. Подекуди стверджують, що у глобалізації є явний лідер – США, а з цього випливає і ототожнення глобалізації з американізацією. За даними світового банку, 140 країн світу є біднішими, ніж найменша з 29 найбагатших ТНК. Отже, перевагами глобалізації скористалися, головним чином, багаті, бідні стали ще біднішими, залишившись постачальниками сировини та дешевої робочої сили. Так глобалізація виглядає як “змова багатих” для досягнення своїх економічних інтересів (незважаючи навіть на погіршення умов навколишнього середовища) проти решти світу. Саме для більш справедливого розподілу ресурсів та контролю над рухом капіталів (тобто для контролю над діяльністю “багатих”) створюються міжнародні організації (МВФ, СОТ, ООН, Світовий банк). Але неможливо однозначно говорити про роль таких організацій, оскільки вони є породженням глобалізованої економіки. Ці організації, за словами Дж. Штігліца, являють собою “глобальне управління” в своїх інтересах, оскільки переважна більшість учасників економічної діяльності, яких торкаються рішення цих інституцій, позбавлена права голосу, щоб адекватно відповісти на їхні дії. Опоненти глобалізації говорять про те, що, не зважаючи на спроби контролю, цей процес є тенденцією глибоко антидемократичною і експлуататорською за суттю. Протести лунають не тільки з “бідного” світу. Протестують також і у багатому світі, і навіть у американському, де відбувся один з найголосніших протестів – у Сіетлі 1999 року під час саміту СОТ.

У 1980 – 1990-х роках у науці спостерігався розпад біполярної системи світоустрою, перетворення тенденції глобалізації економіки на магістральний напрям розвитку світового господарства, формування “нового світового порядку”, що включатиме не тільки економіку, а й широке коло інших проблем – від глобалізації національних культур до екології та питань безпеки. Однак уже у середині 1990-х років у міру нагромадження різноманітності та варіативності властивостей глобалізаційних феноменів на методологічних підходах до їх пізнання стали позначатися суттєві хиби змістового та формального характеру [4].

Як відзначали з приводу проблем розвитку теорії глобальних змін співробітник Пітсбурзького університету (США) Р. Робертсон та викладач Національного університету Сингапуру Х. Хондкер, попри всі намагання дати визначення глобалізації, досвідчені фахівці з проблем дослідження сучасного світу – як цілісного в історичній перспективі – ледве тямлять, чим вони займаються. Склалася ситуація, коли поняття і теорії, сформульовані в серйозній науці про суспільство, втрачають свою аналітичну цінність.

Стверджується, що глобалізація, наче дев'ятий вал, захльостує планету, руйнуючи при цьому Вестфальсько-Філадельфійську систему як таку, що складається з понад двохсот суверенних держав з усталеним міжнародним правом. Висловлюються також думки, що глобалізація – просто модне слово, яке не має власного змісту. Справа в тому, що від невмілого користування, яке найчастіше йде від нерозуміння явища, термін “глобалізація” ладен перетворитися на “слово-пастку” (Дж. Сарторі), втратити свій первісний зміст та почати відображати щось інше [5].

З іншого боку глобалізація в цілому, як і суто інформаційна глобалізація, розглядається як процес, який шкодить світовому розвитку, збільшує ступінь нерівності серед різних країн, загрожує зайнятості й рівню життя й перешкоджає соціальному прогресу.

За останні декілька років Україна почала прискореними темпами рухатись у напрямі інтеграції з європейськими державами. У тому числі це стосується такої суспільноважливої галузі, як транспортна, зокрема авіаційна. У розвитку зовнішньоекономічних зв’язків та реалізації геополітичного потенціалу України як транзитної держави все бі-

льшого значення набуває авіатранспорт. Темпи зростання ринку пасажирських авіаперевезень залишаються найшвидшими з-поміж усіх видів транспорту. Загалом, за станом на 2007 рік, роботу авіаційної галузі забезпечують 92 авіакомпанії, 42 аеропорти та аеродроми, ДП ОПР “Укравроруx”, а також ряд інших спеціалізованих підприємств [6]. Необхідно зауважити, що як на внутрішніх, так і на міжнародних авіалініях спостерігається зростання обсягів перевезень. На даний час транспортна система України не повною мірою готова до забезпечення перевезень у таких обсягах, насамперед через недостатній розвиток нормативно-правової бази і низький інвестиційний потенціал ТДК (транспортно-дорожнього комплексу), внаслідок чого збільшується зношення технічних засобів, погіршується їх структура, не забезпечується належна безпека руху, зростає негативний вплив діяльності транспорту на навколишнє природне середовище та здоров’я. А якщо взяти до уваги ще й жорстку конкуренцію, яка існує в світі, то неважко помітити, що все це призводить до витіснення українських перевізників з міжнародних ринків транспортних послуг, знижує якість обслуговування вітчизняних підприємств і населення, що в свою чергу створює реальну загрозу економічній безпеці держави. Для створення умов, що сприяють підвищенню конкурентоспроможності національних авіаперевізників та експедиторів на міжнародних і внутрішньому ринках авіатранспортних послуг, необхідно формувати єдине правове поле діяльності підприємств транспорту з урахуванням міжнародних норм шляхом уніфікації національних правових норм з міжнародним транспортним правом щодо перевезень та їх транспортно-експедиційного обслуговування і приєднання України до ряду міжнародних конвенцій та багатосторонніх угод, а також шляхом визначення ефективного механізму входження в міжнародні транспортні організації та активної участі в їх діяльності.

На сьогодні відповідна нормативно-правова база в Україні недостатньо опрацьована, галузь працює переважно за нормативними актами, що були розроблені ще в СРСР. Зрозуміло, що таке становище не тільки стримує інтеграцію України до Євросоюзу, а й заважає національним авіаперевізникам працювати за зрозумілими для всіх правилами та стандартами, що відповідають міжнародним вимогам та повністю покривають діяльність даної галузі. Саме у вирішенні цього питання інформаційну глобалізацію можна розуміти як таку, що несе позитивні результати для розвитку цієї галузі. Більшість наукових досліджень, що провадилися, були спрямовані на аналіз економічних або технічних факторів та шляхів удосконалення української авіаційної галузі. Проте рідко хто зосереджує свою увагу на такому важливому аспекті, як правова основа діяльності авіаційної галузі, інтеграція та погодження зі світовими нормами права.

В загальному вигляді діяльність авіакомпаній регулюється на чотирьох рівнях:

1. На світовому рівні відносини у повітряному сполученні регулюються великою кількістю конвенцій, серед них виділяють такі основні: Чиказька конвенція 1944 р. з 18 додатками; Варшавська конвенція 1929 р.; Гаазький протокол 1955 р.; Монреальська конвенція 1971 р. та Гвадалахарська конвенція 1999 р. Необхідно також зазначити, що діяльність міжнародних організацій у галузі повітряного сполучення (ІСАО, ІАТА) теж має велике значення, оскільки впливає на розвиток відносин у цій галузі шляхом створення нових програм, внесення пропозицій та взагалі здійснення політики в цій сфері.

2. Наступним рівнем, на якому відбувається регулювання авіаційної діяльності, є регіональний. Для вирішення питань, які виникають при здійсненні діяльності в рамках регіонів, було створено регіональні організації цивільної авіації: африканська – АСЕКНА, латиноамериканська – ЛАКАК, центральноамериканська – КОКЕСНА, арабських держав – КАКАС [7].

3. Третім рівнем є двостороннє регулювання (міжурядові угоди).

Саме тут важливого значення набуває питання стосовно вибору виду міжурядових угод. Тут ідеться про визначення найбільш прийнятного для країни шляху розвитку авіаційного сполучення: стандартні угоди чи “відкрите небо”? Вирішення питання лібералізації є дискусійним, оскільки, по-перше, в процесі повітряних перевезень беруть участь три сторони – авіаційна компанія, аеропорти та інші обслуговуючі фірми. По-друге, згідно з угодою про “вільне небо” на сьогодні всі відносини між сторонами набувають іншого вигляду, оскільки, насамперед, більш жорсткою стає конкуренція, і не лише між вітчизняними суб’єктами авіаційних відносин. Таким чином, постає закономірне питання: чи вигідна лібералізація країні в цілому? Чи вигідна вона вітчизняним авіаційним компаніям? Чи вигідна вона аеропортам та іншим обслуговуючим фірмам? Чи виграють від цього національні споживачі, роботодавці та ті, хто бажає отримати роботу?

4. І, нарешті, діяльність в галузі авіації регулюється на території (в межах) певної країни, тобто йдеться про державне регулювання. Активна робота саме на цьому рівні є найбільш актуальним питанням для України.

В умовах існування великої кількості не адаптованих до вимог сьогодення, часто взаємовиключаючих або неповних нормативних актів, які регулюють діяльність авіаперевізників на різних рівнях, вітчизняним компаніям важко працювати. Щоб полегшити діяльність та підвищити їх конкурентоспроможність на міжнародному рівні, необхідно привести національне законодавство в цій галузі у відповідність з міжнародними нормами та стандартами, оскільки існуюча нормативно-правова база, яка регулює відносини авіаційного сполучення та значною мірою впливає на діяльність суб’єктів цих відносин, дуже розрізнена.

Як було вказано у затвердженій Міністерством транспорту та зв’язку України “Концепції розвитку транспортно-дорожнього комплексу України на середньостроковий період та до 2020 року”, інтеграція України в європейську та світову транспортні системи є одним з пріоритетних напрямів розвитку [8]. Для досягнення цієї мети, серед інших, варто визначити і деякі правові заходи: уніфікація національної нормативно-правової бази вітчизняного транспорту і транспортної діяльності в Україні з відповідними міжнародно-правовими нормами; уніфікація національних правових норм з міжнародним транспортним правом щодо міжнародних перевезень та їх транспортно-експедиційного обслуговування і приєднання України до ряду міжнародних конвенцій та багатосторонніх угод.

Більш ніж десять років тому велика кількість держав спрямувала свою діяльність на лібералізацію регулювання міжнародного транспорту, про що свідчить збільшення кількості держав, які беруть участь у діяльності будь-яких механізмів, що забезпечують повний доступ до ринку. Але така лібералізація тягне за собою більш жорсткі умови конкуренції, і, як наслідок, у галузі авіаперевезень відбуваються великі структурні трансформування (утворення альянсів, злиття та придбання компаній). Розглянемо, наприклад, Андську угоду про “відкрите небо” (у 1969 р. п’ять держав Південної Америки у рамках Картахенської угоди утворили так звану “Андську групу”, до якої входили Болівія, Колумбія, Перу, Чилі, яка вийшла з неї у 1976 р., та Еквадор, в 1973 р. до групи приєдналась Венесуела), за якою одним із завдань цієї групи було забезпечення збалансованого та стійкого розвитку шляхом розширення економічної інтеграції та співробітництва [9]. Запланований кінцевий строк утворення вільної торговельної зони в цьому регіоні – 1993 р. За цей час у 1991 році було розпочато здійснення авіатранспортної політики “відкритого неба” на субрегіональній основі. Крім цього, було проведено лібералізацію системи ціноутворення авіакомпаній шляхом введення режиму встановлення тарифів країною початку перевезення. Така політика створила сприятливі умови для стимулювання еко-

номічної діяльності та розширення можливостей комерційних авіакомпаній. Незважаючи на юридичні обов’язки в рамках політики “відкритого неба”, темпи проведення лібералізації мають суттєві відмінності через розбіжності в економічному становищі та у процесі розвитку приватизації. В той час як Колумбія і Венесуела намагалися розвинути процес лібералізації, Перу тимчасово (до 1997 р.) відкликала всі свої зобов’язання у межах програм лібералізації. І все ж таки, незважаючи на значне збільшення обсягу повітряних перевезень, деякі приватизовані національні авіакомпанії у регіоні припинили свою діяльність завдяки великого тиску, який чинять конкурентні авіаперевізники із Сполучених Штатів Америки та Європи. А що відбуватиметься з вітчизняними авіаперевізниками в теперішніх умовах жорсткої конкуренції?

Лібералізація в повітряному сполученні впливає на авіаперевізників по всьому світу. У 2004 р. відбулося злиття французького та голландського національних авіаперевізників, у результаті чого з’явилася нова найбільша в Європі авіакомпанія Air France KLM. Завдяки такому об’єднанню, навіть з урахуванням примусової передачі 94 слотів у день в аеропортах Амстердаму і Парижу конкурентам, витрати було знижено, а прибуток виріс на 20 %. Незважаючи на те, що ціни на нафту значно зросли (до 50$ за баррель), що потягло за собою підвищення цін на авіаційне паливо (до 33 %), а з цього випливає і підвищення вартості квитків, керівництво компанії вважало ці труднощі тимчасовими [10]. Так, у 2006 – 2007 фінансовому році прибуток авіакомпанії зріс на 32,5 %, а вже у I кварталі 2007 – 2008 фінансового року чистий прибуток зріс на 70,1 – до 415 млн. євро порівняно з 244 млн. євро, що були отримані за аналогічний період у минулому році. Ці данні містяться у звіті компанії Air France KLM, яка пов’язує зростання прибутку із скороченням видатків, що здійснювалося з моменту злиття двох компаній у 2004 р., а також із збільшенням пасажиропотоку, що компенсувало підвищення цін на авіаційне паливо[11]. Для розширення кола своїх споживачів авіакомпанії Air France та KLM запустили сервіс мобільної реєстрації на рейси з використанням підтвердження шляхом надсилання SMS-повідомлення. Окрім Air France та KLM, сервис мобільної реєстрації надають тільки декілька компаній у світі, включаючи Air Canada, Southwest та SAS [12].

В жовтні 2007 р. німецька авіакомпанія Lufthansa Cargo, яка займає третю позицію у вантажних авіаперевезеннях (перша належить Air France KLM, а друга – Korean Air), зробила стратегічно важливий крок, зумовлений саме процесом лібералізації, об’єднавшись з Deutsche Post. Нове підприємство з міжконтинентальних вантажних перевезень почне свою роботу у 2009 р. – саме тоді, коли спливає термін дії угоди, за якою співробітництво концернів на трансконтинентальних маршрутах курирує компанія Aerologic. Завдяки цьому альянсу DHL стає більш ефективною, ніж американські служби експрес-доставки. Lufthansa Cargo, в свою чергу, закріплює свої позиції на ринку вантажоперевезень оскільки залучає до співпраці важливого клієнта. Окрім цього, нова авіакомпанія планує своє базування в аеропорту Лейпциг, де DHL має намір побудувати новий міжнародний вантажний термінал. Прогнозується, що все це значно збільшить вантажообіг аеропорту, завдяки чому аеропорт Лейпциг стане одним з трьох найбільших хабів DHL [13].

Отже, можна побачити тенденції до об’єднання авіакомпаній для підвищення їх конкурентоспроможності на ринку в умовах лібералізації. Причому спостерігається не об’єднання компаній-конкурентів, а фінансове об’єднання декількох компаній, які доповнюють одна одну але продовжують діяти під своїми торговими марками, розширюючи свої можливості, зменшуючи витрати та збільшуючи прибутки.

Вітчизняні перевізники без узгодження вітчизняного законодавства з міжнародним, перебуватимуть в складній системі правових відносин, що тягне правову невизначеність.

Ряд претензійних позовів по відношенню до компанії, неузгодженість політики регулювання (взаємодії) між суб’єктами ринку авіаперевезень в кінцевому випадку призводить як до фінансових втрат самих суб’єктів, так і до погіршення їх іміджу.

Тобто глобалізація в цьому питанні може мати позитивні результати тільки в тому випадку, коли йдеться про спрощення системи регулювання відносин повітряного сполучення. А для досягнення цієї мети доцільно було б створити таку інформаційну систему, яка б включала в себе всі нормативні документи, включаючи конвенції, міждержавні угоди, та інші нормативні акти, як зовнішні, так і внутрішні, які стосуються повітряного права. Необхідно сюди додати також судову практику та коментарій щодо застосування таких нормативних актів. Це могло б значно полегшити діяльність суб’єктів авіаперевезень, покращити практику вирішення спорів у судовому порядку і, взагалі, вдосконалити відносини в цій галузі.

Така інформація має цінність ще й тому, що виходячи з подій, які відбуваються у світі останнім часом, вона має більш чітко зорієнтувати вітчизняних авіаперевізників, зайнятих у міжнародних авіаперевезеннях, в особливостях правового режиму “відкритого неба”, а це знання, які мають великий практичний сенс при роботі на ринку перевезень у таких країнах. Крім того, така робота може значно розширити уявлення про діяльність, що проводиться ІСАО в інтересах встановлення загальних техніко-юридичних правил у галузі міжнародної аеронавігації та міжнародного повітряного транспорту.

Це дослідження буде чи не найпершою в Україні спробою комплексного, ґрунтовного та всебічного аналізу впливу норм міжнародного повітряного законодавства на діяльність авіатранспортної галузі в Україні, а також перспектив її подальшої інтеграції до міжнародних організацій та об’єднань, відповідності існуючих нормативно-правових актів міжнародним вимогам та шляхів подальшого розвитку і адаптації української законодавчої бази. Це має велике значення, оскільки в Україні на сьогодні гостро постає питання розробки нового основного нормативного акта, який би займався регулюванням діяльності авіатранспортної галузі. В даному випадку йдеться про розробку та прийняття нового Повітряного кодексу, оскільки чинний не відповідає сучасним вимогам та потребам.

Використана література

1. *Чешков М.* Глобализация: сущность, нынешняя фаза и перспективы // Pro et Contra. – 1999. – С. 114.

2. Friedman Th. Understanding Globalization. The lexus and the Olive Tree. – N. Y., 2000, p. 9.

3. *Парахонський Б.О.* Національні інтереси України (духовно-інтелектуальний аспект). – К.: НІСД, 1993. – 43 с.

4. Стратегії економічного розвитку в умовах глобалізації: Монографія; За ред. д.е.н., проф. Д.Г. Лук’яненка. – К.: КНЕУ, 2001. – 215 с.

5. *Хайек Ф.* Пагубная самонадеянность. – М., 1992. – С. 184-202; Sartori G. The Theory of Democracy Prevised. Chatom Hous.

6. Підсумки роботи за І півріччя 2007 року. Державіаадміністрація // Прес-служба МТЗУ. – 2007. – 18 липня // www.mintrans.gov.ua/mintrans/control/uk/publish/article?art_id=73066&cat_id=42549 – 50 k.

7. *Бордунов В.Д.* Правовой механизм деятельности международных воздушных организаций. – М.: Наука, 1989. – 168 с.

8. Концепція розвитку транспортно-дорожнього комплексу України на середньостроковий період та до 2020 року / Міністерство транспорту та зв'язку України // www.mintrans.gov.ua/mintrans/control/uk/publish/article?art_id=43124&cat_id=42258–148 k.

9. Всемирная авиатранспортная конференция “Проблемы и возможности либерализации” (Монреаль, 2003).

10. Air France и KLM: годовщина брака // www.ratanews.ru/news/news_23052005_20.stm – 51 k.

11. Авиакомпания Air France-KLM увеличила чистую прибыль на 70,1 % // MyForex – Forex portal. – 09.08.2007.

12. Air France и KLM запустили мобильную регистрацию // ITnews.com.ua. – 02.07.07.

13. Соб. инф. и по материалам информагентств. Актуально в мировых компаниях // Комп&ньон. – 2007. – № 39. – С. 14-15.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 004.4:331

С. ШВЕЦЬ, науковий співробітник НДЦПІ АПрН України

ДО ПИТАННЯ УПРАВЛІННЯ ПРОЕКТАМИ

Анотація. *Щодо сутності та змісту управління проектами як напряму професійної діяльності та складової виробничого процесу.*

Одним з аспектів, зумовлених участю України в міжнародному співробітництві, є визнання та широке застосування систем “управління проектами” не тільки як методології й інструменту планування, контролю та координації проектів, але й як сфери активізації професійної діяльності. Нині, на відміну від минулих часів, управління проектами – один з розповсюджених напрямів діяльності, а попит на кваліфікованих керівників проектів на ринку праці перевищує пропозицію.

Поряд із значними змінами в економічному житті країни змінилося й саме поняття “проект”. Раніше під цим терміном розуміли комплект технічної документації та кошторис для, головним чином, будівництва або технічної розробки. Нині проект – це більш широке поняття, яким користуються фінансисти, економісти, політики, юристи, підприємці, які мають на меті втілити в життя наміри із заздалегідь визначеними цілями, вимогами, строками, кошторисом, ризиками та якістю очікуваних результатів. Це і є проекти.

Управління проектами – це система методів і засобів керування, координації зусиль людей із застосуванням досягнень сучасної науки, комп’ютерних технологій для успішної реалізації цілей проекту. На практичному рівні, управління проектом – це дії, спрямовані на вирішення проблем, пов’язаних із затримками, змінами вимог та іншими перепонами, що з’являються в процесі реалізації будь-якого проекту. Основна ж ціль керівника проекту – мінімізація витрат ресурсів на проект та максимізація прибутку від цього. За результатами фінансових та часових витрат та задоволення всіх зацікавлених учасників проекту можна судити, був проект успішним чи ні.

Практично не буває двох однакових проектів. Кожен проект є унікальним за своїми цілями, термінами, ресурсами, фінансами, персоналом. Це складна багатопараметрична задача, що потребує від керівництва прийняття необхідних рішень при повному розумінні наслідків, що вони нестимуть. Для правильної організації проекту та відстежування виконання його етапів часто використовується сітьове планування.

Управління проектом включає в себе процес обмірковування, обговорення та точне формулювання того, що повинно бути досягнуто виконанням проекту; планування послідовних кроків та визначення необхідних для цього людських, інформаційних і матеріальних ресурсів.

Після всебічного обговорення та обміркування керівником проекту складається план. Згідно з цим планом у майбутньому можна буде визначати стан робіт на проекті, перевіряти отримані результати робіт. Також бажано скласти сітьовий графік робіт, що відображає роботи та взаємозв’язки між ними, а також ресурсну гістограму, що є графічним відображенням потреб проекту в тих чи інших ресурсах у певний момент часу. Розклад проекту включає детальний аналіз усіх дій, необхідних для виконання проекту; реалістичні оцінки часу (оптимістичні й песимістичні) на кожен вид діяльності; взаємозв’язок між різними видами робіт. У сукупності ці елементи дають відповідь на наступні запитання:

© С.Швець, 2008

• Що повинно бути зроблено і в який термін?

• Які ресурси: люди, обладнання, матеріали, інформація, енергія, інструменти, споруди, транспорт тощо необхідні для кожного виду робіт? Чи будуть вони в наявності, коли це буде необхідно?

• Скільки коштів необхідно витратити на якому етапі?

• Яка очікувана корисність від виконаного проекту (в грошовому або іншому еквіваленті)?

Якщо відповіді на ці запитання знайдено, то частину роботи – планування – можна вважати виконаною.

Після цього проект можна починати. Бажано мати формальне позначення старту проекту. Можна здійняти прапор або зробити розсилку по електронній пошті до кожного члену команди проекту з привітанням про старт проекту. Прикладом такого старту щодо розроблення проекту Інформаційного кодексу України може слугувати відповідне звернення (див. журнал “Правова інформатика” № 4(16)/2007, стор. 5). Це важливий психологічний крок. Свідомо чи підсвідомо, члени команди тепер знатимуть, що час пішов і кожен день/тиждень зволікань коштуватиме певних матеріальних і моральних втрат. Так само бажано “відмічати” завершення кожного з етапів робіт. Але це вже частина другого етапу проекту – виконання проекту та його контроль.

Послідовне відстежування (моніторинг) виконання робіт забезпечує об’єктивну оцінку поточного стану проекту. Звіти про виконану по проекту роботу дозволяють відокремити реальний прогрес від уявного. Так послідовно враховуються зміни в проекті, поновлюється поточний стан проекту та розробляються нові завдання. Стає можливим об’єктивно констатувати випередження чи відставання від плану. Вище керівництво організації використовує управління проектами в якості інструмента і має точну уяву про те, який стан речей на проекті, які роботи будуть проводитись у майбутньому, на що потрібно звернути увагу і які питання в якій послідовності потребують негайного вирішення. База для прийняття рішень вдосконалюється, а суб’єктивність – зникає або зменшується.

Внесок, що його робить керівник проекту (менеджер проекту), наступний:

• Керує людьми в стресовому середовищі.

• Фокусує загальну увагу на єдиній меті.

• Керує змістом проекту, щоб у результаті мету було досягнуто.

• Постійно змінює навантаження і часові рамки, щоб проект залишався в колії.

• Керує вирішенням проблем. Не обов’язково самостійно вирішує їх, але стежить, щоб їх було адресовано тому, хто їх може вирішити.

• Стежить за наявністю всіх необхідних ресурсів.

• Планує діяльність та стежить, щоб плани виконувались вчасно.

• Знає, що відбувається на різних напрямах, та керує залежностями між різними задачами проекту.

• Ініціює розгляд відкритих, відкладених питань, сприяє однозначній їх трактовці.

• Ідентифікує ризики та робить все можливе, щоб їх уникнути.

Завершальний етап – здача проекту та перехід у безстрокову фазу підтримки. Вміле й ефективне завершення проекту може зробити значний внесок в його успіх. Тому планувати завершальний етап потрібно заздалегідь. Заключне враження від проекту залишається в пам’яті людей. Необхідно підготувати звіт про завершення проекту, в якому повинно бути відображено: що було зроблено добре, що погано, що можливо було б по-

кращити. Така самооцінка необхідна й тим, хто буде втілювати майбутні проекти, і як інструмент самовдосконалення.

Сучасні системи управління проектами в промисловості, економіці отримали широке застосування.

Щодо використання нових підходів управління проектами в галузі держави і права, і зокрема в законотворчому процесі, то в цьому напрямі зроблено перші кроки. Створення і впровадження системи управління проектами в законотворчому процесі є актуальним і потребує активізації.

Використана література

1. //www.marathon.ru/setevoe.html.
2. //www.dvpm.biz/articles/article-10.shtml.
3. //www.pmonline.ru/phparticles/show_news_one.php?n_id=373.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 336.71:681.302

А. НОВИЦЬКИЙ, *кандидат юридичних наук,*
начальник відділу дослідження проблем протидії
податковим правопорушенням
НДЦ з проблем оподаткування
Національного університету ДПС України

ЕЛЕКТРОННІ ГРОШІ – ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОБІГУ В УКРАЇНІ

Анотація. *Щодо проблемних питань правового забезпечення емісії, обігу електронних грошей в Україні, розвитку дозвільної системи застосування засобів обігу електронних грошей; визначення ризиків їх обігу, можливих напрямів правового врегулювання суспільних відносин, пов’язаних із застосуванням електронних грошей.*

Активний розвиток сучасних телекомунікаційних, комп’ютерних технологій привів до розвитку нових суспільних відносин. Перш за все, це надання послуг за допомогою мережі Інтернет. Поряд з наданням послуг виникла необхідність і оплати за ці послуги. Глобальність самої мережі, відсутність кордонів у спілкуванні дещо змінили встановлені правила ведення бізнесу, замовлення послуг та товарів, отримання та оплату. Глобальна мережа надала можливість проводити операції купівлі-продажу, замовлення послуг, не виходячи з дому. Швидкість обробки та передачі замовлень відповідно повинні були підтверджені й оплатою коштами. Виникла необхідність у швидких розрахунках. Готівковий обіг передбачає матеріальне переміщення відповідних купюр чи монет, безготівковий переказ-звернення до відповідного банку, який здійснюватиме переказ, внаслідок цього втрачається оперативність розрахунків. Тому було запропоновано електронний варіант грошей, який можна було б легко і швидко, навіть поза банківською установою, переказати на відповідний рахунок свого контрагента.

В прийнятій 18 вересня 2000 р. Директиві Європейського Парламенту та Ради “Про започаткування та здійснення діяльності установами-емітентами електронних грошей та пруденційний нагляд за ними” зазначено, що для електронної торгівлі, яка швидко розвивається, бажано забезпечити регулятивну основу, що допоможе повною мірою виявити потенційні переваги електронних грошей і, зокрема, уникнути затримки впроваджень технологічних нововведень, а електронні гроші можуть розглядатися як електронний замінник монет і банкнот, який зберігається на електронному пристрої, наприклад, на чіп-картці або у пам’яті комп’ютера, і який, в основному, призначений для здійснення електронних банківських платежів обмеженими сумами [1].

Проблема правового забезпечення існування електронних грошей, різноманітних платіжних систем, що здійснюють свою діяльність в національному сегменті Інтернету визначена окремими органами виконавчої влади України. Так, у листі Держфінмоніторингу України від 2 грудня 2003 р. № 1826/30420-4 “Щодо правомірності використання системи трансферу майнових прав Web Money Transfer суб’єктами підприємницької діяльності”, зокрема, зазначається, що відповідно до Закону України “Про платіжні системи та переказ коштів в Україні” обов’язковою умовою законного проведення розрахунків фізичними та юридичними особами України між собою за допомогою платіжних систем є наявність дозволу або реєстрації [6].

© А. Новицький, 2008

В той же час, Національний банк України в листі № 25-209/1539-8608 від 20 листопада 2003 р. зазначив, що питання емісії та обігу електронних грошей ще не знайшли відображення в законодавчих та нормативно-правових актах унаслідок їх новизни для України. Вбачається реальна необхідність не лише технічної розробки нормативних актів на основі міжнародних рекомендацій, а й вироблення концептуальних підходів щодо реалізації державної грошової політики України.

На підтвердження необхідності нормативного забезпечення даного виду суспільних відносин може слугувати і телеграма Національного банку України № 48-012/29-192 від 10 січня 2006 р., в якій, зокрема, попереджаються всі банківські установи України про загрозу відмивання коштів, здобутих злочинним шляхом клієнтами Інтернет-банкінгу, та рекомендується посилити вимоги до віртуальних клієнтів.

Проблеми правового забезпечення становлення інформаційного суспільства, його окремих елементів, у тому числі й електронної комерції та електронних грошей, вивчали українські вчені: І. Аристова, К. Бєляков, В. Гавловський, Р. Калюжний, М. Швець, В. Цимбалюк та інші. Проте в роботах даних учених не зроблено системного аналізу виникнення та функціонування електронних грошей, правового забезпечення вільного обігу та встановлення спеціальних правил застосування.

Метою статті є дослідження правового забезпечення емісії, обігу електронних грошей в Україні, розвитку дозвільної системи застосування засобів обігу електронних грошей; визначення ризиків їх обігу, можливі напрями правового врегулювання суспільних відносин, пов’язаних із застосуванням електронних грошей.

Інтенсивний розвиток нових інформаційних технологій стає основною рушійною силою економічних та соціальних змін у світі. Завдячуючи цьому, можна стверджувати, що світ вступає в нову стадію свого розвитку – інформаційну. Ми можемо впевнено стверджувати про становлення глобального електронного середовища для економічної діяльності, для виникнення нових суспільних відносин.

Розвиток інформаційного суспільства не може сам по собі здійснюватись завдяки тому, що більшістю розвинутих країн задекларовано про становлення таких суспільних відносин. Йде природний цикл формування відносин, які є класичними для становлення будь-якої форми суспільних відносин. Яскравим прикладом формування інформаційного суспільства є виникнення нового виду платіжного засобу – електронних грошей. Походження грошей взагалі як форми платіжного засобу пов’язують з розвитком товарообмінних операцій, з труднощами, що виникають при безпосередньому обміні продуктами праці. Перші згадки про еквівалент товару, виражений у предметах розкоші – намисто, перли, певні шматки породи, є фактично початком відліку історії грошей. Пізніша їх трансформація в металеві та паперові носії здійснюється до сьогодні. З розвитком техніки поряд з матеріальним засобом забезпечення вартості грошей виникає їх безготівкова форма. Перші перекази грошей телеграфом, міжбанківські безготівкові трансфери, розвиток інших форм передачі інформації про гроші створили платформу для сучасного розуміння феномена “електронних грошей”.

Що ж таке електронні гроші? Відповідно до Європейської Директиви “Про електронні гроші” № 2000/46/ЄС від 18 вересня 2000 р.: “електронні гроші” означають грошову вартість, яку представлено у вимозі до емітента, яка:

а) зберігається на електронному пристрої;

б) випускається для одержання коштів на суму, не меншу за вартість у грошовому вираженні;

в) приймається як засоби платежу за зобов’язаннями іншими, ніж зобов’язання емітента [1].

Великий тлумачний словник сучасної української мови дає наступне визначення: *“електронні гроші – грошові засоби, які використовуються в електронній системі банківських послуг”* [2].

В національній правовій системі нормативне визначення поняття електронних грошей поки що відсутнє, як і правила їх обігу.

Розглянемо загальні функції грошей. Взагалі, гроші – це специфічний товар, що має властивість обмінюватись на будь-який інший товар, тобто є загальним еквівалентом [3]. Їх основні функції полягають у забезпеченні міри вартості, тобто забезпечують вираження і вимірювання вартості товарів, надаючи їй форму ціни; у засобі обміну, де гроші виступають як посередник в обміні товарів і забезпечують їх обіг; як засіб платежу, де гроші обслуговують погашення різноманітних боргових зобов’язань між суб’єктами економічних відносин; як засіб нагромадження та заощадження, де гроші забезпечують нагромадження вартості в її загальній абстрактній формі в процесі розширеного відтворення. Можна з впевненістю сказати, що всі функції грошей властиві і “електронним грошам”.

Виходячи із цих суджень можна зробити висновок, що електронні гроші є результатом еволюції безготівкових розрахунків, які перейшли на більш високий рівень та забезпечуються електронними технічними засобами.

Фактично на даному етапі розвитку техніки можна виділити два способи забезпечення існування та обігу електронних грошей: картковий та занесений в пам’ять електронно-обчислювальних машин (в пам’ять комп’ютера).

Виникла досить парадоксальна ситуація. Постановою Національного банку “Про затвердження Положення про порядок емісії платіжних карток і здійснення операцій з їх застосуванням“ № 137 від 19 квітня 2005 року дано визначення поняття “електронний гаманець”, проте не визначено сутності електронних грошей. Ця постанова регламентує лише один бік обігу електронних грошей – за допомогою платіжних карток, що ж стосується питань, пов’язаних з обігом електронних грошей, які зберігаються в пам’яті комп’ютера, то вони правовою системою України не розглядаються взагалі.

Ініціативи Національного банку України направлені на чітку регламентацію обігу, емісії електронних грошей. І навіть був запропонований проект положення, яким передбачалось введення процедури ліцензування діяльності банків щодо емісії електронних грошей в Україні. Як окреме обмеження щодо обігу електронних грошей для фізичних осіб пропонується встановити максимальну межу для “електронного гаманця” на позначці 1000 гривень, що фактично досить близько до пропозиції Директиви Європейського Парламенту та Ради “Про започаткування та здійснення діяльності установами-емітентами електронних грошей та пруденційний нагляд за ними”, яка передбачає встановлення обмеження на рівні 150 євро [4].

На нашу думку, потрібно на законодавчому рівні визначити суб’єктів правовідносин, пов’язаних перш за все з емісією електронних грошей, з порядком їх обігу та забезпеченням їх легалізації шляхом беззаперечного викупу всіма учасниками фінансово-грошових відносин. Зокрема, в Директиві Європейського Парламенту та Ради “Про електронні гроші” зазначено, що електронні гроші підлягають викупу з метою забезпечення довіри власника, а можливість викупу завжди повинна розумітись як викуп за номінальною вартістю [1].

Перекази коштів у мережі Інтернет не регламентується чіткими правилами чи законами, тому що досить складно визначити юрисдикцію тієї чи іншої норми щодо трансакцій електронних грошей. Переказ може бути проведений з однієї країни в іншу безпосередньо або через посередника і т. д. Проблемність визначення юрисдикції тієї чи

іншої норми досить часто унеможливлює сам факт нормативного врегулювання даних відносин.

Проблемою залишається правове забезпечення переказу коштів за допомогою всесвітніх платіжних систем. Поряд із чіткою регламентацією роботи банківських установ щодо переказу електронних грошей в мережі існують і небанківські платіжні системи, які практично виконують функції банків. Сьогодні в Інтернеті діють сайти, що проводять обмін електронних грошей різних платіжних систем, таким чином виконується функція банку з обміну/продажу різного роду електронної валюти.

Досить проблемним фактом залишається можливість здійснювати будь-які фінансові операції з електронними коштами анонімним контрагентам. У деяких країнах світу встановлені спеціальні обмеження щодо придбання дорогих автомобілів, прикрас, коштовностей (необхідно надати декларацію про законність отриманих доходів). Інтернет дає змогу обійти дані законодавчі обмеження і проводити аукціони та торги анонімно. При цьому переказ грошей також може бути здійснений в мережі, а куплена таким чином коштовна річ буде доставлена покупцю анонімно, що є досить ймовірним способом відмивання коштів здобутих злочинним шляхом.

В даний час нам необхідно говорити про створення спеціальних наддержавних правил поведінки в глобальній мережі Інтернет, які обов’язково були б імплементовані в національні законодавства держав світу і мали б категоріальні норми поведінки, встановлювали б солідарну відповідальність за порушення правил обігу електронних грошей, унеможливлювали б злочинні перекази та відмивання коштів, здобутих злочинним шляхом.

Розвиток науково-технічного прогресу не стоїть на місці. Як ми вже відмічали, є два способи забезпечення існування та обігу електронних грошей: картковий та занесений в пам’ять електронно-обчислювальних машин (в пам’ять комп’ютера). Виникає питання, як кваліфікувати мобільний телефон, за допомогою якого можна робити перерахунки грошей з одного рахунку абонента на інший? Спочатку зазначена послуга операторів мобільного зв’язку надавалась як можливість поповнення рахунку одного абонента іншому.

Проте винахідливі підприємці швидко зорієнтувались у можливостях нового способу забезпечення платежів. Сьогодні в Інтернеті досить часто можна зустріти повідомлення про спосіб оплати за надані послуги через перерахування певної суми коштів за допомогою операторів мобільного зв’язку. Більше того, Київська міська державна адміністрація як перспективний спосіб оплати за паркування автомобілів у місті розглядає саме можливість оплати за дану послугу за допомогою мобільних телефонів. Це є предметом перемов з операторами мобільного зв’язку [5].

Таким чином, мобільний телефон стає інструментом обігу електронних грошей, а оператори мобільного зв’язку перебирають на себе частину функцій банківських установ. Як розглядати мобільний телефон у даних правовідносинах, коли кошти перераховуються з одного абонентського рахунку на інший в якості оплати за певні послуги? Можна стверджувати, що мобільний телефон є лише інструментом доступу до комп’ютера оператора мобільного зв’язку. Проте, з мобільного телефону на комп’ютер передається певний контент інформації, який є збудником для проведення операцій подальшої передачі контенту інформації. Тобто саме з мобільного телефону передається першочергова команда (у вигляді інформації) на проведення операцій з електронними коштами, що знаходяться на абонентному рахунку користувача мобільного телефону. Це не суперечить Закону України “Про платіжні системи та переказ коштів в Україні”, де в статті 14.1, зокрема, зазначено, що спеціальний платіжний засіб може існувати у будь-якій фо-

рмі на будь-якому, крім паперового, носії, що дозволяє зберігати інформацію, необхідну для ініціювання переказу. Проте, даний закон у статті 14.2 встановлює, що спеціальний платіжний засіб має дозволяти ідентифікувати його держателя [7].

Законодавством України не передбачено обов’язковість ідентифікації операторами мобільного зв’язку при реєстрації нового абонента-користувача мобільного зв’язку, крім випадків контрактного обслуговування. Тому можна говорити, що використання мобільного телефону як інструменту платежу можливе лише при контрактному підключенні абонента. Тобто при можливості ідентифікації особи, яка здійснила той чи інший переказ електронних коштів.

Ми можемо констатувати, що інструментом проведення операцій з електронними грошима сьогодні вже є не тільки картки та комп’ютери, а й мобільні телефони як інструменти для проведення фінансових операцій. Тому в нормативній базі, що готується, необхідно передбачити й такі особливості розвитку телекомунікаційних мереж.

Однією з реальних можливостей вирішення проблем забезпечення офіційності обігу електронних грошей може стати прийняття спеціалізованих нормативних документів. У нашій державі ведеться робота над створенням Інформаційного кодексу України. Одним з можливих варіантів правового забезпечення необхідно передбачити в даному законодавчому акті поряд з електронною комерцією, електронним банкінгом чітко визначені елементи обігу, емісії, застосування електронних грошей.

Використана література

1. Директива Європейського Парламенту та Ради “Про започаткування та здійснення діяльності установами-емітентами електронних грошей та пруденційний нагляд за ними” від № 2000/46/ЄС 18 вересня 2000 року //Законодавчі і нормативні акти з банківської діяльності. – 2002. – № 6.

2. Великий тлумачний словник сучасної української мови (з дод. допов. та CD) Уклад. та гол. ред. В.Т. Бусел. – К.-Ірпінь: ВТФ “Перун”, 2007. – 1736 с.

3. Гроші та кредит / М.І. Савлук, А.М. Мороз, М.Ф. Пудовкіна та ін. – К.: Либідь. 1992. – 331 с.

4. Поданева Ю. Выпуск электронных денег хотят ограничить //www.times.liga.net /l_nav_doc2.ns.

5. Парковку в Киеве будут оплачивать с помощью мобильного телефона // АвтоОбоз, 23 жовтня 2007 року // www.auto.oboz.ua/news.

6. Новиков С. WWW-виртуальные деньги: стоит ли связываться? // Контракты. – 2004. – № 14.

7. Закон України “Про платіжні системи та переказ коштів в Україні” № 2346 від 05.04.2001 // www.liga.net

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 343:681.302

Г. УСАТИЙ, *кандидат юридичних наук, доцент,*
Національний університет ДПС України

КРИМІНОГЕННА СИТУАЦІЯ У СФЕРІ ЕЛЕКТРОННОГО БАНКІНГУ

Анотація. *Щодо аналізу негативних тенденції та потреби у створенні національної системи кримінально-правового забезпечення ефективної протидії злочинам у сфері електронного банкінгу.*

Аналіз стану криміногенної ситуації у сфері електронного банкінгу* в Україні свідчить про тісний зв'язок злочинності і її залежності від зростання кількості комп’ютерів, підключених до мережі Інтернет. При цьому, чим більшою є комп’ютеризація сучасного суспільства і, відповідно, питома вага осіб, що мають доступ до глобальної інформаційної мережі, тим більшим є ризик негативного впливу комп’ютерної злочинності на сферу електронного банкінгу.

Серед факторів та обставин, які обумовлюють сучасний стан та тенденції злочинності у сфері електронного банкінгу, можна (з певною часткою умовності) виділити наступні.

По-перше, вразливість комп’ютерних систем (у т. ч. електронних платіжних систем). Сюди можна віднести умисні помилки чи помилки з необережності при розробці програмного забезпечення фінансових установ, а також недостатню активність банків з розробки та забезпечення відповідних заходів по запобіганню зовнішнім атакам та внутрішнім посяганням з боку власних працівників.

По-друге, унікальні особливості кіберпростору надають зловмиснику можливість анонімних дій, адже фактично особа, що вчиняє злочин, знаходиться в реальному світі, а злочинною діяльністю займається у віртуальному. Таким чином, “електронні” сліди злочину вітчизняним правоохоронцям надзвичайно складно виявити, зафіксувати та використати у перспективі в межах досудового слідства.

По-третє, просторовий фактор. Адже нерідко комп’ютерного злочинця і жертву розділяють значні відстані, які не обмежуються кордонами однієї держави. Так, наприклад, злочинець може спочатку зайти у мережу з комп’ютера “І” (Україна) і через комп’ютер “ІІ” Інтернет-провайдера, що розміщений у Російській Федерації, заподіяти майнову шкоду або заволодіти майном шляхом незаконного міжбанківського переказу з комп’ютера “ІІІ” (США).

По-четверте, надзвичайно високий рівень латентності злочинів у сфері електронного банкінгу. Так, за інформацією Української міжбанківської асоціації членів Europay International “ЕМА”, яка виступає профільною міжбанківською установою та координує спільні заходи щодо запобігання неправомірному використанню карток, загальний обсяг шахрайських операцій перевищив в Україні 500.000 доларів США у 2001 році та 1.000.000 доларів США у 2002 р. Це 1 % загального легального обігу карткових операцій, хоча середньоєвропейське значення – 0,3 % обігу. Але офіційні дані банківських структур та самих платіжних систем на декілька порядків нижчі [1].

© Г. Усатий, 2008

* Від ред.: електронний банкінг – це система дистанційного банківського обслуговування клієнта (проведення фінансових операцій (платежів) за допомогою телекомунікаційних каналів (РС-банкінг) і засобів Інтернету (Інтернет-банкінг).

По-п’яте, цьому також сприяє закритість (непрозорість) банківської системи, що дозволяє службовим особам, а інколи навіть і рядовим співробітникам банків вчиняти суттєві зловживання. Керівники кредитних установ (особливо вищої ланки) непідконтрольні практично нікому, окрім засновників банку.

На заваді правоохоронним і контролюючим органам України при проведенні документальних перевірок та ревізій постає правовий інститут банківської (чи комерційної) таємниці. Саме тому можна зрозуміти, чому різноманітні розкрадання у сфері електронного банкінгу вчиняються злочинцями переважно з використанням свого службового становища. Разом з тим, у рекомендаціях ООН з питань формування міжбанківської служби безпеки зазначається, що “для банків життєво важливим є створення механізму ідентифікації особи своїх клієнтів і надання сприяння правоохоронним органам у випадках, коли виникають підозри стосовно тих чи інших вкладів чи операцій. При цьому також необхідне зміцнення механізмів контролю над банківськими операціями і, можливо, навіть централізація такого роду інформації. Державам необхідно заохочувати банки, брати на себе якомога більшу відповідальність за подібний контроль з метою боротьби зі злочинністю” [2].

По-шосте, недоліки у нормативній базі з урегулювання взаємовідносин між господарюючими суб’єктами, у тому числі між банками і їх клієнтами. Відсутність нормативних актів (або їх неналежна якість), що регламентують окремі напрями сфери електронного банкінгу, підсилюється суперечливістю і нечіткістю багатьох законів, інструкцій та розпоряджень, що прийняті поспіхом, без глибинного опрацювання і розуміння сутності проблеми. Так, останніми роками поширеними стають схеми отримання грошових коштів у сфері електронного банкінгу з використанням фіктивних договорів, коли протизаконній діяльності надається формально законний вигляд, що ускладнює втручання та своєчасне реагування на такі факти правоохоронних органів (оскільки взаємовідносини сторін ззовні мають цивільно-правовий чи господарсько-правовий зміст).

Недосконалим, на жаль, у вищезазначеному сенсі є також вітчизняне кримінальне законодавство, яке має суттєві вади та прогалини у забезпеченні ефективної протидії злочинам у сфері електронного банкінгу. Так, ще у 1999 р. Асоціація банків-членів EUROPAY International розробила законопроект, який містив описання складів злочинів у сфері використання банківських платіжних карток. Пропонувалося передбачити покарання за такі діяння: неправомірне використання банківської платіжної картки, її номера, персонального ідентифікаційного коду з метою незаконного отримання доходу або привласнення майна; умисне використання банківської платіжної картки з метою збільшити кредиторську заборгованість, яку особа неспроможна погасити; виготовлення підроблених банківських платіжних карток, їх збут або використання; залучення іншої особи до прийому справжніх або підроблених платіжних карток під час оплати товарів чи послуг з метою незаконного одержання доходу; прийом справжніх або підроблених платіжних карток у рахунок оплати товарів або послуг, якщо особа, яка здійснює такий прийом, знає або підозрює, що картка є підробленою або отримана злочинним шляхом; виготовлення або зберігання інструментів для підробки або копіювання банківських платіжних карток. Під такими інструментами пропонувалось розуміти будь-які матеріали, за допомогою яких можна здійснити штампування, кодування або друкування на платіжних картках [3].

Як бачимо, ухвалюючи Кримінальний кодекс 2001 року, законодавець не сприйняв хоч і не позбавлений недоліків, проте комплексний підхід банкірів у питанні кримінально-правового захисту сфери обігу платіжних карток і обмежився встановленням кримі-

нальної відповідальності лише за підробку таких платіжних інструментів та за деякі дії з ними.

Серед інших умов, що сприяють вчиненню злочинів у сфері електронного банкінгу, російський правник Астапкіна С.М. [4] виділяє наступні:

а) недостатню взаємодію банківських структур і правоохоронних органів. З одного боку, банки зацікавлені, по-перше, не виносити “бруд з хати” (у даному контексті – інформацію про вчинені проти них “пластикові злочини”) з метою запобігання антирекламі і, по-друге, залучати нову клієнтуру будь-якою ціною (у т. ч. і без достатньої її перевірки), з іншого боку – працівники правоохоронних органів нерідко недооцінюють небезпеку даного виду злочинів і навіть не завжди вносять викрадені картки у списки номерних викрадених речей (тому вони, наприклад, не завжди потрапляють у поле зору працівників міліції при обшуку осіб, затриманих за інші правопорушення);

б) халатне ставлення деяких співробітників банків до збереження службової інформації, а також недбале зберігання чи пересилання пластикових платіжних засобів, бланків суворої звітності, наприклад, сліпів (не говорячи вже про умисне співробітництво зі злочинцями);

в) недоліки в організації роботи торговельних підприємств, що приймають до оплати пластикові картки (наприклад, для економії часу на авторизацію касири нерідко розбивають суму покупки на декілька рахунків, кожен з яких не перевищує ліміту, який не потребує авторизації, стаючи фактично спільниками злочинців);

г) економія на засобах захисту пластикових карток;

г') несвоєчасне і неповне використання стоп-листів з метою попередження шахрайства з картками. Затримки у внесенні втраченої чи викраденої картки до списку заборонених до прийому карток (стоп-лист), а також обмежена територіальність дії стоп-листів (з метою економії) дозволять злочинцям використовувати викрадені чи фальшиві (підроблені) картки тривалий час.

Розглядаючи криміногенну ситуацію у сфері електронного банкінгу, не можна оминути увагою відповідні види (класифікацію) злочинів.

Так, виходячи з вищезазначеного можна виділити найпоширеніші види комп’ютерних злочинів:

- несанкціонований доступ;
- пошкодження комп’ютерних даних;
- комп’ютерний саботаж;
- комп’ютерне розкрадання;
- комп’ютерне шахрайство;
- комп’ютерний підлог (підроблення).

Враховуючи специфіку злочинних посягань у сфері електронного банкінгу, доцільним, на нашу думку, вбачається описання у межах статті наступних його видів:

Комп'ютерне розкрадання. Даний вид злочину включає в себе незаконне привласнення чужої інформації, у т. ч. несанкціоноване перехоплення без дозволу і з використанням технічних засобів повідомлень, які надходять в комп'ютерну систему або мережу, що витікають з комп’ютерної системи або мережі або циркулюють у рамках такої системи або мережі.

Предметом даного злочинного посягання є комп’ютерна інформація, яка може включати конфіденційні відомості про її власника, банківські вклади, номери рахунків, кредитних карток і т. д.

Концептуально крадіжка у фізичному світі не відрізняється від крадіжки у віртуальному просторі. Відмінність полягає лише у тому, що власність в останньому випадку

носить віртуальний характер [5]. Особа здійснює злочин, якщо обертає майно у своє володіння або здійснює незаконний контроль над власністю іншого.

Одному з останніх злочинних діянь подібного роду було надано широкого розголосу (резонансу) у зв'язку з арештом у США двох російських громадян-мешканців м. Челябінська О. Іванова і З. Горшкова, які, за даними ФБР США, впродовж 1999-2001 рр. використовуючи персональні комп’ютери, що знаходяться у Челябінську, шляхом сканування здійснювали в Інтернеті пошук компаній, що використовують уразливе з точки зору захисту програмне забезпечення. Виявляючи такі, вони проникали в комп’ютерні системи і брали їх під свій контроль, “викачуючи” всю необхідну інформацію про клієнтів. В окремих випадках вони входили в контакт з компанією – власником інформації, представляючись членами “групи експертів по захисту від хакерів”, і повідомляли, що їм вдалося проникнути у комп'ютери компанії. Потім вони пропонували за плату усунути недоліки і підвищити безпеку комп'ютерної системи [6].

У ФБР США вважають [7], що заарештовані мають відношення до сотень злочинів, зокрема до справи про розкрадання 15700 номерів кредитних карт компанії з виконання грошових переказів “Western Union” (Денвер, США). У вересні 2000 року та 17 травня 2001 р. у справі відбулися судові слухання. У жовтні 2001 р. Горшков визнаний судом винним за 20 пунктами висунутого проти нього обвинувачення.

Поширеними є випадки, коли злочинець копіює інформацію і забирає копію, залишаючи оригінальну версію законному власникові. У цих випадках жертва часто навіть не знає про злочин, що відбувся. Проте їй заподіяна шкода, яка залежить від характеру власності і, відповідно, кваліфікуватиметься, наприклад, як порушення авторських прав.

Деякі фахівці виділяють окремий вид комп'ютерної крадіжки – крадіжку комп'ютерних послуг. Наприклад, у традиційному сенсі згідно з § 223.7 Типового кримінального кодексу США особа здійснює крадіжку послуг, якщо “шляхом обману або загрози або шляхом пред'явлення фальшивих знаків або інших засобів з метою уникнути платежу за послугу отримує послуги, які свідомо для неї можуть бути надані тільки за умови відшкодування” [8]. У фізичному світі це може бути праця, професійна послуга, перевезення, послуги з телефонного зв'язку, обслуговування в готелі, ресторані, допуск на виставки, користування транспортом або іншим рухомим майном. У віртуальному світі можна вкрасти час користування мережею Інтернет, комп'ютерний час. Правопорушник, у якого немає законного права на використання послуг і який діє з метою позбавлення законного власника власності, таким чином позбавляє жертву цієї власності.

Основними прийомами вчинення злочинів при цьому, на думку Н. Ахтирської [9], можуть бути наступні:

- вилучення засобів обчислювальної техніки, яке здійснюється з метою отримання системних блоків, окремих вінчестерів чи інших носіїв інформації, що містять у пам’яті установчі данні про клієнтів, вкладників, кредиторів банку. Такі дії можуть здійснюватись шляхом викрадення і самі по собі містять склад злочину звичайних, “некомп’ютерних” злочинів;
- перехоплення (негласне отримання) інформації служить для отримання певних відомостей про клієнтів, вкладників, кредиторів банку. Воно може здійснюватися з використанням методів і апаратури аудіо-, візуального і електромагнітного спостереження. Об'єктами, як правило, є канали зв'язку, телекомунікаційне устаткування, службові приміщення для проведення конфіденційних переговорів, паперові і магнітні носії (у тому числі і технологічні відходи);

• несанкціонований доступ до засобів обчислювальної техніки, тобто активні дії по створенню можливості розпоряджатися інформацією без згоди власника, що здійснюється з використанням наступних основних прийомів:

1) “за дурнем” – фізичне проникнення у виробничі приміщення. Зловмисник чекає у закритого приміщення, тримаючи в руках предмети, пов'язані з роботою на комп'ютерній техніці (елементи маскування), поки не з'явиться хто-небудь, що має легальний доступ до нього, потім залишається тільки увійти всередину разом з ним або попросити його допомогти занести нібито необхідні для роботи на комп'ютері предмети.

Інший варіант – електронне проникнення у засоби обчислювальної техніки – підключення додаткового комп'ютерного терміналу до каналів зв'язку з використанням шлейфу “шнурка” у той момент часу, коли законний користувач короткочасно покидає своє робоче місце, залишаючи свій термінал або персональний комп'ютер в активному режимі;

2) “за хвіст” – зловмисник підключається до лінії зв'язку законного користувача і терпляче чекає сигналу, що позначає кінець роботи, перехоплює його на себе, а потім, коли законний користувач закінчує активний режим, здійснює доступ до банківської системи; подібними властивостями володіють телефонні апарати з функцією утримання номера, що викликається абонентом;

3) “комп'ютерний абордаж” – зловмисник вручну або з використанням автоматичної програми підбирає код (пароль) доступу до банківської системи з використанням звичайного телефонного апарату;

4) “неспішний вибір” – зловмисник вивчає і досліджує систему захисту, використовувану у банківській комп'ютерній системі, її слабкі місця, виявляє ділянки, що мають помилки або невдалу логіку програмної будови, розриви програми (пролом, люк), і вводить додаткові програми, що вирішують доступ;

5) “маскарад” – зловмисник проникає в банківську комп'ютерну систему, видаючи себе за законного користувача із застосуванням його кодів (паролів) та інших ідентифікуючих шифрів;

6) “містифікація” – зловмисник створює умови, коли законний користувач банківської системи здійснює зв'язок з нелегальним терміналом, будучи абсолютно упевненим у тому, що він працює з потрібним йому законним абонентом. Формуючи правдоподібні відповіді на запити законного користувача і підтримуючи його помилки якийсь час, зловмисник здобуває коди (паролі) доступу або відгук на пароль;

7) “аварійний” – зловмисник створює умови для виникнення збоїв або інших відхилень у роботі засобів обчислювальної техніки банківської комп'ютерної системи. При цьому включається особлива програма, що дозволяє в аварійному режимі діставати доступ до найбільш цінних даних. У цьому режимі можливе “відключення” всіх наявних у банківській комп'ютерній системі засобів захисту інформації, що полегшує доступ до них зловмисника.

Комп'ютерне шахрайство. Відповідно до рекомендацій Ради Європи даний злочин включає введення, зміну, стирання або поглинання комп’ютерних даних чи комп'ютерних програм або інше втручання у процес обробки даних, що завдає іншій особі економічного збитку або веде до втрати її майна, з метою отримання незаконної економічної вигоди для себе або на користь іншої особи. Аналізуючи даний вид злочину у сфері комп'ютерної інформації, слід відокремлювати його від шахрайства, здійсненого з використанням комп'ютера як інструменту, а інформаційного простору – як середовища скоєння злочину.

Здійснюючи комп’ютерне шахрайство, правопорушник несанкціоновано або з дозволу втручається у процес належного функціонування обробки даних комп'ютером таким чином, що це призводить до наслідків, що підпадають під визначення шахрайства.

Так, згідно з § 263а Кримінального кодексу ФРН під комп'ютерним шахрайством розуміється діяння, що полягає у завданні шкоди чужому майну через дію на результат обробки даних шляхом неправильного створення програм, використання неправильних даних або неправомочного використання даних чи іншого впливу на результат обробки даних з наміром отримати для себе або третьої особи майнову користь [10].

В одному з відомих випадків у 1997 – 1998 рр. громадянин Ш., знаходячись за місцем свого проживання, за допомогою програми згенерував номер кредитної картки платіжної системи VISA. Знаючи адресу електронного магазину “PC Teach” в Інтернеті, він провів замовлення різних товарів на суму понад 20 тисяч доларів США, ввівши магазин в оману відносно своєї платоспроможності шляхом надання відомостей про номер кредитної картки [11], що був згенерований ним.

Широко поширені схеми обману людей за допомогою таких електронних звернень або повідомлень через Інтернет, як пропозиції про продаж акцій за привабливою ціною; інвестиції у нерухомість в іноземній державі; надання позик на умовах, що забезпечують винятково високу норму прибутку; передоплата недостатньо ретельно охарактеризованих товарів або запрошення приєднатися до фінансової піраміди. Комп'ютер у таких випадках використовується як допоміжний інструмент для скоєння злочину, а віртуальне середовище є альтернативою фізичного світу, в якому також можна здійснити аналогічні операції. Правопорушник використовує Інтернет або будь-яку іншу мережу, щоб спілкуватися з потенційними жертвами не безпосередньо, а віртуально, свідомо убезпечивши себе, приховавши свою особу. Спілкування може відбуватися за допомогою вебсайтів або електронної пошти. Шахраї переконують переслати грошові кошти на їх адресу в обмін на послуги, які вони ніколи не нададуть.

У останньому випадку це не комп'ютерне, а традиційне шахрайство, де комп'ютер – тільки інструмент для скоєння злочину, оскільки немає безпосередніх маніпуляцій з комп'ютерною інформацією. В цьому випадку повинні застосовуватися традиційні норми, що стосуються шахрайства.

На основі узагальнення і аналізу судово-слідчої практики способи здійснення шахрайства з платіжними картками представляється доцільним класифікувати на п'ять основних груп [12]:

1. Способи шахрайства з використанням підробленої платіжної картки. При скоєнні злочинів можливо використання як підроблених платіжних карток (матеріальна підробка), так і платіжних карток, належно виготовлених, але які містять помилкові відомості (інтелектуальне підроблення). Виготовленням підроблених платіжних карток визнається як їх повне відтворення, так і часткова підробка (наприклад, зміна реквізитів – номери рахунку, підписи, перекодування інформації на магнітному носієві). Способи їх виготовлення такі: поліграфічний, репрографічний, анастатичний, малюванням і комбінований.

2. Способи шахрайства з використанням сліпів (квитанції електронного терміналу). Підроблені сліпи для здійснення злочину можуть бути отримані при виробництві несанкціонованих відбитків як із справжньої, так і з підробленої платіжних карток. Сліпи виготовляються шахраями за допомогою набірних друкарських форм або шляхом застосування підроблених кліше з використанням інформації із справжніх пластикових карток.

3. Способи шахрайства, реалізовані з використанням слабких місць технології обробки платежів за платіжними картками. Це способи, засновані на недосконалості каналів зв'язку між торговими точками і банками, а також на непрофесіоналізмі працівників

торгівлі, що оформляють платежі по картці. У зв'язку з тим, що для скоєння злочинів вказаними способами необхідний значний обсяг знань, спеціальні технічні засоби, а сам процес здійснення розкрадання досить тривалий (час на розшифровку і перекодування інформації) і трудомісткий, випадки скоєння таких злочинів зустрічаються рідко.

4. Способи шахрайства з використанням справжньої платіжної картки, законно або незаконно отриманої злочинцями. Сюди можна віднести: овердрафт з шахрайським використанням платіжної картки, передачу картки шахраям її власником за певну винагороду, отримання платіжних карток у банках по викрадених документах з подальшим перевищенням ліміту кредитування, операції з краденою або втраченою карткою.

5. Способи шахрайства з використанням інформації про платіжну картку у сфері телекомунікацій. Найбільш латентний і небезпечний спосіб скоєння злочинів у сфері обороту платіжних карток – це скоєння злочинів через всесвітню мережу Інтернет. Проблема полягає у тому, що більшість співробітників СБУ і МВС, зокрема слідчих підрозділів, мають дуже узагальнене уявлення про комп'ютерні технології, навіть на рівні користувачів, тому їм складно використовувати у доведенні роздруківки з рядом IP-адрес. Крім того, несанкціоновані проникнення в комп'ютерні мережі можуть мати дуже обширну географію, і тому локалізувати місце скоєння злочину практично неможливо. Хакер, що знаходиться в Україні, може, наприклад, розплатитися з американським магазином платіжною карткою громадянина Італії, що відкрив рахунок в австралійському банку.

Комп'ютерний підлог (підроблення). Комп'ютерний підлог (підроблення) – це всілякі маніпуляції, що включають введення, зміну, стирання або поглинання комп'ютерних даних чи комп'ютерних програм з метою здійснення фальсифікації у класичному сенсі.

Коли питання не стосуються обробки комп'ютерних даних, як у випадку з підробкою, комп'ютер використовується як інструмент для зміни або створення фальшивого письмового або електронного документа. Об'єктивний бік злочину становить зміна, створення, доповнення, випуск, передача і збут фальшивих документів, записів, чеків, кредитних карток та інших предметів.

У зв'язку з цим слід підкреслити суміжність віртуальних і традиційних форм шахрайства і комп’ютерного підлогу (підроблення). Перший з них стосується декількох форм шахрайства у зв'язку з телекомунікаційними послугами. У таких випадках злочинець намагається отримати послуги без оплати за допомогою технічних маніпуляцій з пристроями або електронними елементами пристроїв. Така поведінка зазвичай криміналізується за допомогою конкретних кримінально-правових положень, проте у ряді випадків її можна віднести до категорії, відповідної класичним положенням, що характеризують шахрайство чи комп’ютерний підлог (підроблення). Друга група пов'язана із зловживанням платіжними документами. Злочинець, здійснюючи махінації з електронною банківською карткою або використовуючи підроблені картки чи помилкові коди, намагається отримати незаконну фінансову вигоду. Такі діяння можуть охоплюватися конкретними кримінально-правовими положеннями або класичними положеннями, що характеризують шахрайство і комп’ютерний підлог (підроблення), до яких можуть вноситися поправки.

В якості **висновків** можна зазначити наступне.

Проаналізовані негативні тенденції засвідчують, що вже зараз суспільство і держава відчувають нагальну потребу створення національної системи кримінально-правового забезпечення ефективної протидії злочинам у сфері електронного банкінгу, їх запобігання та криміналістичного захисту банківської (грошової) системи не лише від “традиційних” злочинних посягань у сфері власності, господарської діяльності тощо, але й від

новітніх, вкрай складних та надзвичайно досконалих способів шахрайства, які безпосередньо пов’язані з науково-технічним прогресом у цій галузі (у т. ч. злочини з використанням пластикових карток).

Використана література

1. Бутузов В.М., Василинчук В.І., Шеломенцев В.П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: Навчальний посібник. – К.: Типографія ТОВ “СТ-Стиль”, 2006. – С. 45.

2. Практические меры борьбы с организованной преступностью / Материалы семинара ООН. – Суздаль, 21-25 октября 1991. – С. 31.

3. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика: Монографія. – К.: Юридична практика, 2003. – С. 78.

4. Астапкина С.М., Максимов С.В. Криминальные расчёты: уголовно-правовая охрана инвестиций. – М., 1995. – С. 80-82.

5. Brenner S.W. California Criminal Law Review. 2001, vol. 4.

6. Russian National Arrested and Indicted for Penetrating U.S. Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers // Press Release for Immediate Release. U.S. Department of Justice, United States Attorney, District of Connecticut. 2001, May 7.

7. Садчиков А. Как ФБР устроило “подставу” хакерам Леше и Васе // Комсомольская правда. 2001, 24 мая; Георгиев В. Судебные слушания в Сиэтле по делу челябинских хакеров состоялись, но решение пока не оглашено // Урал-Пресс. 2001, 23 мая; Трудолюбов М. Хакеров выловили на приманку // Ведомости. 2001, 25 апреля; Куклев С. Агент Мадлер поймал хакера Иванова // Челябинский рабочий. 2001, 25 апреля.

8. Примерный уголовный кодекс США. – М.: Прогресс, 1969. – С. 153.

9. Ахтырская Н. Способы хищений в банковских информационно-вычислительных системах // Компьютерная преступность и кибертерроризм: Сб. научных статей. – Запорожье, 2004. – Вып. 1. – С. 117.

10. Уголовный кодекс ФРГ / Пер. с нем. – М.: Зерцало, 2000.

11. Кесарева Т.П. Криминальная паутина. Мошенничество в системе электронной торговли через Интернет // Интерпол в России, 2000. – № 3. – С. 26-27.

12. Реуцкий А.В. Способы совершения мошенничества с платёжными карточками // Відповідальність за злочини у сфері господарської діяльності: Матер. НПК. – Х., 2006. – С. 197-198.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 681.3.06

В. ХАХАНОВСЬКИЙ, *кандидат юридичних наук, доцент*
В. КОРЗУН, ад’юнкт Київського національного університету внутрішніх справ

ГЕОІНФОРМАЦІЙНА СИСТЕМА ЯК СКЛАДОВА ЄДИНОЇ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПРАВООХОРОННИХ ОРГАНІВ

Анотація. *Щодо можливостей та перспектив використання геоінформаційних систем у правоохоронній сфері.*

Сучасні інформаційні технології широко впроваджуються практично в усі сфери життєдіяльності, у тому числі – у правоохоронну сферу. Так, відповідно до Указу Президента України “Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю” від 31.01.2006 р. № 80/2006, Наказу МВС України від 07.06.2006 р. № 571 “Про затвердження Програми створення інтегрованої інформаційно-пошукової системи органів внутрішніх справ України” [1 – 2] та інших нормативно-правових документів в Україні здійснюється інформатизація правоохоронної діяльності.

Створення інтегрованого банку даних правоохоронних органів передбачає комплексне застосування як внутрішньовідомчих, так і зовнішніх інформаційних ресурсів, а також різноманітних комп’ютеризованих інформаційних систем. Однією з найперспективніших систем у цьому комплексі є геоінформаційна система (далі – ГІС), яка являє собою ефективний інструментарій для аналізу взаємодії об’єктів та пов’язаних з ними подій у рамках чітко визначених територіальних меж і часових інтервалів.

Вважається, що першу ГІС було створено у кінці 1960-х рр. Міністерством оборони США. На початку 1970-х рр. з’явилось так зване комп’ютерне картографування. Точки, лінії та об’єкти на карті були представлені множиною координат X,Y. Ці дані можна було виводити на плоттер у різноманітних шкалах і проекціях. На початку 1980-х рр. з’явилися системи управління просторовими базами даних, призначені для зв’язування комп’ютерного картографування з традиційними системами управління базами даних. В цих системах можна було, вказавши місце на карті, отримати певну інформацію або, задавши ряд умов, отримати результат у вигляді карти. З’явилося інтегроване середовище – дані дистанційного зондування, цифрова карта висот, доріг, рослинності та ін., які співіснували в рамках однієї системи. Удосконалювалося обладнання для дигиталізації, з’явилися нові моделі сканерів тощо. Виявилося, що ГІС дозволяють по-іншому дивитися на світ, на багато процесів, що відбуваються у ньому.

Геоінформаційні технології сьогодні застосовуються в різноманітних галузях. Це, зокрема: геоінформаційний пакет для багатоцільового використання різними службами міста (ГІС-Київ); системи для газової, нафтової та вугільної промисловості; геоінформаційні пакети банку цифрової геологічної інформації; системи для ведення кадастру земель, промислових риб, для маркетингових досліджень, для відображення зон проходження радіохвиль; геоінформаційна система аналітичного забезпечення процесу управління територією тощо. Про це йдеться у наукових публікаціях, зокрема, А. Витюка, А. Волосовича, Є. Карякіна, П. Косецького, П. Марченко, В. Шемета та ін. [3 – 5].

Застосуванню ГІС у правоохоронній сфері присвячені роботи О. Барладіна, В. Васюніна, М. Водова, Г. Пухова та інших [6]. Це, зокрема, системи для аналізу даних про викрадений автотранспорт, зброю, про злочинців, для забезпечення безпеки дорожнього

© В. Хахаовський, В. Корзун, 2008

руху, а також ГІС для підвищення ефективності діяльності чергових частин. Саме на останніх ГІС зупинімось докладніше.

Відомо, що діяльність чергових частин спрямована на оперативне збирання, обробку і формування даних про оперативну обстановку на території. На жаль, сьогодні у більшості чергових частин такі операції поки що не автоматизовані, що, безперечно, знижує оперативність реагування ОВС на заяви і повідомлення.

Головними вимогами, які пред’являються до автоматизованого робочого місця (далі – АРМ) оперативного чергового, є: висока оперативність реагування на повідомлення про злочини і події; автоматизація процесів їх реєстрації, отримання довідкової інформації; формування і передача інформації; володіння інформацією про оперативну обстановку в районі, місті чи області у близькому до реального часу масштабі.

Слід зазначити, що головним напрямом вдосконалення роботи оперативного чергового є автоматизація найбільш трудомістких, рутинних операцій: реєстрація повідомлень, робота з базами даних, просторова локалізація злочинів і подій. Реалізація цих вимог досягається шляхом автоматизації запису повідомлень на цифровий магнітофон, визначення номера і відображення місця розташування на плані міста (а також на плані району у збільшеному масштабі).

Значний досвід використання ГІС-технологій має ГУВС м. Санкт-Петербург, де з кінця 1990-х років використовується типове АРМ оперативного чергового міліції (розробка Центру “Севзапгеоинформ”. ГІС дозволяє приймати і реєструвати дані, що надходять телефонними каналами, відображати розташування джерела повідомлення на електронній карті, видавати наявні дані про джерело, документувати отриману інформацію. Можна використовувати базові електронні карти і наносити на них необхідну оперативно-службову інформацію (зокрема, про маршрути патрулів). Кожній записаній в базі даних фонограмі відповідають поля з текстовою інформацією.

Окремо слід відзначити геоінформаційну систему для аналізу даних ОВС України, розроблену Інститутом передових технологій (м. Київ, директор інституту О.В. Барладін), яка являє собою комплекс АРМів, призначених для реалізації аналітичних і оперативних завдань органів внутрішніх справ.

До складу системи входять такі функціональні модулі:

- бази даних підвідомчої території;
- сервер оперативної буферної бази даних;
- оперативного керування ситуацією на підвідомчій території з АРМ оперативного чергового і АРМ збирання інформації та обліку подій;
- реєстрації, відображення та аналізу в реальному режимі часу з АРМ щойно отриманої інформації про події, вчинені злочини та правопорушення.

Останній модуль надає можливість аналізувати події і приймати рішення відразу після надходження інформації з місця події. Для АРМ оперативного чергового створено спеціальну базу даних з системами аналізу інформації, при роботі з якою фіксується інформація про склад чергової групи.

Для реєстрації подій та правопорушень розроблена спеціалізована форма (див. Рис. 1).

Для територіальної прив’язки подій передбачена зручна форма реєстрації адреси подій. За першими літерами назви вулиці (чи населеного пункту) здійснюється автоматична вибірка в алфавітному порядку. Вибір однієї з них запускає модуль виводу номерів будинків для певної вулиці. Іноді адреса місця події може бути вказана помилково чи неповно. В такому разі система здійснює пошук найближчої адреси на основі аналізу наявної інформації. Крім того, АРМ оперативного чергового має в своєму складі систему формування звітів про події, зареєстровані за певний період.

Більш детальне опрацювання інформації передбачено безпосередньо черговим із застосуванням електронної карти ділянки міста, яка підпорядкована певному ОВС. За адресою на електронну карту автоматично подається позначення певного правопорушення, що дає змогу оперативно скласти план дій, а в разі необхідності передати ситуацію на загальноміську електронну карту. Звітом чергового може бути роздруківка з електронної карти ділянки міста, де подано позначення вчинених (розкритих) правопорушень і відповідних дій групи за період чергування.

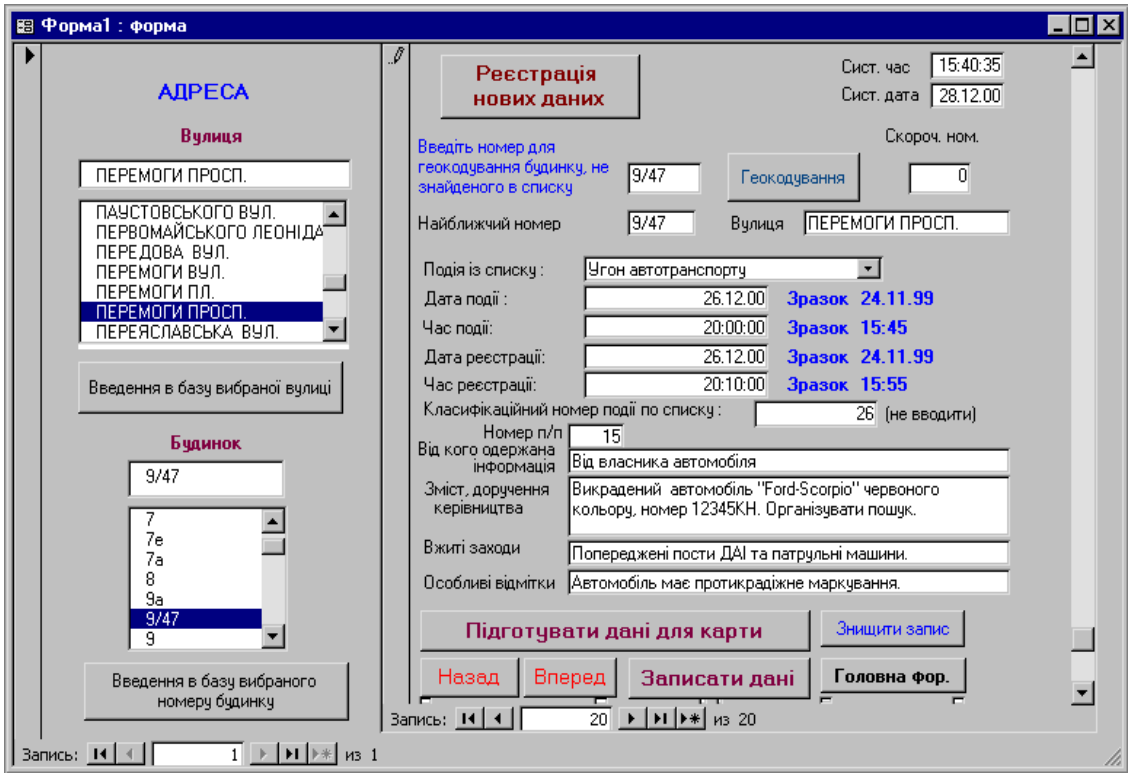


Рис. 1. Спеціалізована форма для реєстрації подій та правопорушень

Інформація подається на електронній карті, де зображено усі проїзди й будинки тощо, а може й бути узагальнена на електронній карті міста в цілому. Такий територіальний розподіл передбачає подання інформації по районах міста. У такому вигляді можна подати й зведену оперативну інформацію по місту за тиждень, місяць, квартал, рік тощо. Зведена інформація відображається на електронній карті міста з її адміністративним розподілом з урахуванням типу подій.

Для обробки та нанесення відповідних характеристик на електронну карту використано робочу базу даних ГУ МВС України в м. Києві, яка постійно поновлюється. Аналіз карти дає можливість відслідковувати тенденції правопорушень певного виду в районах міста з метою попередження злочинів з урахуванням виду злочинів та місць їх найчастішого вчинення.

Електронна карта (див. Рис. 2) містить різнобічну інформацію про правопорушення та їх розкриття. Території районів відображені різною інтенсивністю кольору. Кількість зареєстрованих правопорушень відображена у вигляді кругових діаграм, в яких кожному виду правопорушення відповідає сектор певного кольору. В лівій частині вікна подано пояснення належності кольорів секторів до різних правопорушень. Діаметр кругової діаграми пропорційний загальній кількості зареєстрованих правопорушень, а розмір сектору – кількості правопорушень певного виду.

Інтенсивність забарвлення кожного району є теж інформативною характеристикою – вона відповідає відсотку розкриття злочинів. Ліва частина вікна вміщує легенду карти, де подано систему якісних та кількісних показників розкриття злочинів.

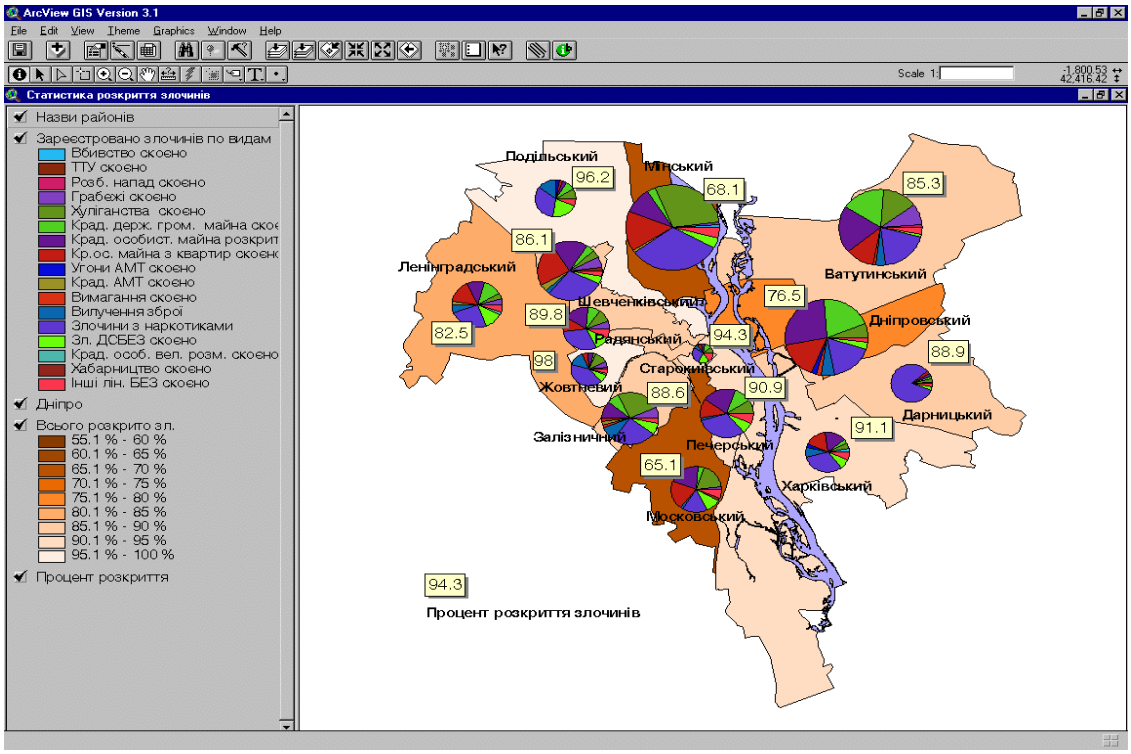


Рис. 2. Електронна карта з інформацією про правопорушення
та їх розкриття по районах міста

Висновки. Досвід використання ГІС свідчить, що сучасні інформаційні технології мають значну перспективу для вдосконалення діяльності чергових частин. Подальше застосування ГІС у правоохоронній сфері відбувається за такими напрямами:

- стеження за переміщенням службового автотранспорту на карті в реальному масштабі часу;
- формування і відображення оперативної обстановки;
- візуалізація плану місця події, його аналіз при виникненні складної ситуації;
- визначення оптимального маршруту руху автомобіля слідчо-оперативної групи до місця події, до найближчих лікарень тощо;
- підвищення ефективності управління силами і засобами;
- аналіз криміногенної обстановки на території за звітній період і у поточний час.

Таким чином, апробовані на прикладі м. Києва АРМ оперативного чергового і АРМ узагальнення статистики правопорушень та їх розкриття придатні для використання в ОВС України.

Використана література

1. Указ Президента України “Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю” від 31 січня 2006 р. № 80/2006.

2. Наказ МВС Україн “Про затвердження Програми створення інтегрованої інформаційно-пошукової системи органів внутрішніх справ України” від 07.06.2006 р. № 571.

3. *Марченко П.Б., Волосович А.Э., Косецкий П.И.* Особенности внедрения ГИС-технологий. Материалы НТК “Приборостроение-96”, часть 1. – Винница-Судак, 1996. – С.117.

4. *Волосович А.Э.* Тенденции развития ГИС. Материалы конференции “Теория, технология, внедрение ГИС”, ГИС-Форум-97. – К.: ГИС-ассоциация Украины, 1997. – С. 14-15.

5. *Витюк А., Карякин Е., Шемет В.* Инструментальная геоинформационная система “МАПАв” для Windows. Материалы конференции “Теория, технология, внедрение ГИС”, ГИС-Форум-97. – К.: ГИС-ассоциация Украины, 1997. – С. 74-75.

6. *Пухов Г.Г., Водов М.А., Васюнин В.С.* Опыт и перспективы применения ГИС в ГУВД Санкт-Петербурга и Ленинградской области //www.dataplus.ru/Industries/2MVD/5_guvd.htm.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 343.985.7

О. ВОЛКОВ, ад’юнкт Київського національного університету внутрішніх справ

ДО ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ПРАВООХОРОННИХ ОРГАНІВ ПО БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Анотація. *Щодо організації навчального процесу з підготовки фахівців правоохоронних органів для протидії злочинності в сфері інформаційних технологій; представлені форми підготовки, методика закріплення практичних навичок.*

Актуальність проблеми, яка подається до розгляду, полягає в належній забезпеченості відповідними фахівцями правоохоронних органів та їх підготовки в сфері протидії несанкціонованому втручанню за допомогою шкідливих програмних засобів в електронно-обчислювальні машини (комп’ютери), автоматизовані системи, комп’ютерні мережі та мережі електрозв’язку, а також в комплектації таких органів фахівцями в сфері інформаційних технологій та захисту інформації. Вирішення проблеми підготовки фахівців і комплектування правоохоронних органів певною мірою задовольнить потреби як науки (теоретичні розробки захисту інформації), так і практики (захист інформації як предмета злочинного посягання) та буде сприяти підвищенню ефективності захисту інформації в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах та мережах електрозв’язку, ефективного викриття, документування, розкриття та розслідування злочинів у цій сфері. Розробка практичних дієвих заходів щодо протидії проявам злочинної діяльності в сфері інформаційних технологій і адекватного реагування на такі злочини є важливим завданням сьогодення.

Мета цієї публікації – висвітлення результатів наукових досліджень стосовно підготовки спеціалістів для правоохоронних органів по боротьбі зі злочинами в сфері інформаційних технологій.

Дослідженням питання підготовки фахівців у сфері інформаційних технологій приділяється увага у наукових статтях, періодичних наукових виданнях та монографіях. Безпосередньо цю проблеми вивчали: Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Іщенко А.В., Цимбалюк В.С., Белкін Р.С., Хахановський В.Г., Біленчук П.Д. та інші вчені, які займалися розробкою питання протидії кіберзлочинності. Незважаючи на розгляд даної проблематики з боку вчених, автором публікації пропонується свій погляд та пропозиції щодо конструктивного вирішення проблеми комплектації правоохоронних органів фахівцями.

У відомчих вищих навчальних закладах системи МВС на даний час розроблені і активно вивчаються слухачами та курсантами навчальні програми з розслідування комп’ютерних злочинів. Донецький інститут внутрішніх справ, що є навчальним закладом саме такого спрямування [7], проводить навчання співробітників МВС з розслідування злочинів у сфері інформаційних технологій [8], а також організації оперативно-розшукової роботи на основі інформаційних технологій [9]. У Харківському національному університеті внутрішніх справ у цьому плані фахівцям після закінчення навчального закладу видають два дипломи про вищу освіту за спеціалізаціями: “правознавство” – “слідчо-криміналістична” і “захист інформації з обмеженим доступом та автоматизація її обробки – організація захисту інформації”.

Слід відмітити навчальні дисципліни у вищому державному навчальному закладі

© О. Волков, 2008

МВС України IV рівня акредитації (Київський національний університет внутрішніх справ) на здобуття юридичної освіти за спеціальністю “правознавство” (7.060101). Цей заклад актуалізував навчальний процес, і слухачам слідчої спеціалізації пропонувалося здобуття знань, пов’язаних з інформаційною безпекою: інформатизація управління в ОВС (108 годин); комп’ютеризовані інформаційні системи правоохоронних органів та інформаційна безпека (72 години); криміналістична інформатика (108 годин). В цьому ж навчальному закладі за спеціальністю “управління у сфері правопорядку” (8.000004) освітньо-професійної програми підготовки магістрів пропонується курс: криміналістична інформатика (27 годин).

Певної підготовленості слідчих підрозділів вимагають і відомчі нормативні акти МВС України. Так слідчий повинен не лише вміти ефективно працювати з організаційною, криміналістичною, спеціальною технікою і засобами зв’язку [10], а й знати та дотримуватись заходів інформаційної безпеки. На жаль в цьому документі не вказано не тільки про впровадження в практичну діяльність слідчих підрозділів таких специфічних програмних засобів, як АРМ “Слідчий” чи АРМ “Керівник слідчого підрозділу”, а й про навчання користування розробками щодо інформаційної безпеки. Практичну цікавість слідчих підрозділів в цьому плані викликають не вищезазначені програмні засоби, які б значно спростили роботу слідчого і керівника слідчого підрозділу, а програмні засоби “підтримки прийняття рішень” в конкретних ситуаціях. В теоретичному ж плані про ці розробки слідчим відомо лише з оглядових відомчих джерел та лекційних занять, практично ж вони не використовуються через їх ненадходження в практичні підрозділи районних відділів області.

В слідчому відділенні, де працює автор, проводиться робота по спрощенню документообігу процесуальних документів, які складаються під час розслідування кримінальних справ. В цьому напрямі проведена робота по створенню бази стандартних процесуальних бланків розроблених ГСУ МВС України [11], яка заповнюється в програмі Microsoft Office Excel по кожній кримінальній справі. Спрощення роботи при використанні цієї бази даних полягає в напівавтоматичному заповненні процесуально значущих фактів, обставин та подій по кожній кримінальній справі. Після закінчення проведення досудового розслідування по кожній кримінальній справі залишається повне наглядове провадження в електронному вигляді бази даних а не окремих процесуальних документів. В цій же програмі співробітниками СУ УМВС розроблені бланки та логіка до заповнення місячних та квартальних звітів СЛ та СЛМ, які певною мірою полегшують роботу при складанні звітності керівників слідчих підрозділів.

У структурі Державного департаменту боротьби з економічною злочинністю МВС України створено спеціальний підрозділ по боротьбі з правопорушеннями у сфері інформаційних технологій. В Державному науково-дослідному експертно-криміналістичному центрі створено відділ криміналістичних комп’ютерних досліджень з проведення таких експертиз. З 2007 р. відповідно до Закону України “Про Державну службу спеціального зв’язку та захисту інформації України” від 23 лютого 2006 року завдання, пов’язані із захистом інформації (зокрема, участь у формуванні та реалізації державної політики у сфері захисту інформаційних ресурсів, створення та розвиток систем технічного та криптографічного захисту інформації), вирішуватиме Державна служба спеціального зв’язку та захисту інформації України. В системі МВС аналогічні функції покладені на Департамент документального забезпечення та режиму. Один з напрямів діяльності цього департаменту – захист інформації технічними засобами, зокрема убезпечення комп’ютерного обладнання від несанкціонованого втручання [12].

Діяльність щодо спрощення роботи, пов’язаної з документообігом, ведеться і в самому центральному апараті МВС. Так в 2006 р. фахівці Департаменту документального забезпечення та режиму почали працювати над впровадженням електронного документообігу по Міністерству внутрішніх справ у цілому та в регіонах аби повністю позбутися паперової частини діловодства. Відбулася презентація програмних продуктів трьох фірм, які брали участь в розробці цього проекту. Спільно з Департаментом інформаційних технологій розроблені технічні вимоги і завдання до такого програмного комплексу. У системі буде задіяний центральний апарат, далі електронний зв'язок сягатиме обласних управлінь і далі райвідділів міліції.

Для об’єднання всіх канцелярій в самому центральному апараті міністерства в одну систему необхідно створити 150 робочих місць. Взагалі ж по Україні впровадження комп’ютерного документообігу потребує відповідного сертифікованого оснащення разом з програмним забезпеченням, а також додатково 1500 фахівців [13].

Відповідно до Закону України “Про основи національної безпеки України” [14] наша держава реалізує комплексну програму по усуненню загроз національній безпеці в різних сферах, в тому числі й в інформаційній. Пріоритетним напрямом цієї діяльності є комп’ютерна злочинність та комп’ютерний тероризм. Без сучасного захисту інформації в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах та мережах електрозв’язку не може бути забезпечена національна безпека нашої держави.

У зв’язку з цим постає проблема не тільки браку самих знань, а й кадрового забезпечення підрозділів професіоналами. Відомчі навчальні заклади системи МВС України проводять підготовку фахівців правоохоронних органів у сфері боротьби з кіберзлочинністю. Але така підготовка не повною мірою відповідає потребам сьогодення та оперативної обстановки в регіонах.

Проблеми вищої освіти в Україні з підготовки фахівців у сфері інформаційних технологій неодноразово досліджувались у фахових виданнях. Це і низька заробітна плата професорсько-викладацького складу, практична відсутність матеріального забезпечення навчального процесу, дефіцит сучасної навчальної літератури, відірваність від світових джерел наукової інформації у сфері боротьби з кіберзлочинністю. Вихід з такої ситуації вбачається в розробці загальнодержавної програми підготовки фахівців. На думку інших дослідників, основним недоліком процесу підготовки фахівців називається відсутність єдиної стратегії боротьби з цими злочинами та безсистемність в організації процесу підготовки та перепідготовки кадрів у цій сфері [15].

Підготовку фахівців у сфері інформаційних технологій необхідно продовжувати у напряму реформування діяльності відомчих закладів освіти МВС України з підготовки та перепідготовки фахівців: оперативних співробітників, слідчих, експертів. Постійно проводити перегляд навчальних планів, введення таких предметів, як правова інформатика та інформаційне право, а також нових спеціалізацій з інформаційно-аналітичного забезпечення діяльності ОВС, захисту відомчої інформації і боротьби з кіберзлочинністю. Освітньо-професійні плани навчання повинні входити до затверджених галузевих стандартів вищої освіти, тобто визначення сучасних напрямів підготовки фахівців по боротьбі з кіберзлочинністю.

Такий фахівець повинен мати належну підготовку не тільки з юридичних дисциплін, а й природничо-наукових: фізики, математики, інформатики, достатніх для розв’язання завдань у сфері боротьби з комп’ютерною злочинністю, знання обчислювальних середовищ, прикладних програм, технічних аспектів організації захисту інформації.

Метою курсу спеціальних дисциплін професійної підготовки є формування не тільки практичних навичок, а й професійного світогляду фахівця з інформаційної безпеки: систематичне, теоретичне і практичне опанування класифікації шкідливих програмних засобів, слідову картину такої злочинної діяльності, мотивів, способів захисту інформації, виявлення каналів несанкціонованого проникнення за допомогою шкідливих програмних засобів, встановлення особи злочинця, класифікація методів і способів заміни, знищення, блокування, перехоплення, копіювання комп’ютерної інформації та комплексне вивчення такої злочинної діяльності.

Для практичного закріплення теоретичних знань курс дисципліни супроводжується розрахунковими та курсовими роботами, проектами, ціллю яких є вироблення практичних навичок проектування і розроблення систем захисту в сучасних умовах. При цьому необхідно звертати увагу саме на вивчення практичних навичок, що є результатом теоретичної підготовки.

В цьому плані в навчальних закладах системи МВС є плідні напрацювання. На кафедрі військового тилу Академії ВВ МВС було створено лабораторію автоматизації. На її базі в 1998 р. створено окремий підрозділ – інформаційно-обчислювальний центр (ІОЦ). У його структурі три відділення: програмного забезпечення, технічного обслуговування обчислювальної техніки та інформаційного забезпечення. В Академії налічується 208 ПЕОМ, з яких 128 використовуються у навчальному процесі. Обладнано 12 навчальних комп’ютерних класів, створено локальну мережу з доступом до Інтернету.

У повсякденній діяльності Академії використовуються програмні продукти, створені власними фахівцями: веб-сторінка Академії, АРМ “Оперативний черговий”, АРМ “Матеріальні цінності тилу”, АРМ “Автотранспорт”, АРМ “Оповіщення”, електронний каталог методкабінету, програми “Грошове забезпечення офіцерів, прапорщиків та курсантів”, “Розкладка продуктів”, “Система обліку успішності”, “Система тестування”, “Система створення екзаменаційних білетів”. У грудні 2005 року було розроблено та впроваджено автоматизовану систему навчальних матеріалів “АСУНМ” [16].

Дещо по-іншому поставлена робота прокуратур районів області. Так, широкого поширення знайшла інформаційно-аналітична система “Прокурор”, призначена для складання та автоматизованої обробки статистичних звітів в органах прокуратури України. В районних прокуратурах Чернігівської області в практичному користуванні знаходиться база даних нормативних документів “Нормативні акти України” (розробник ЗАТ “Інформтехнологія”); внесення змін до нормативних актів проводиться регулярно і дане питання стоїть на контролі обласної прокуратури. Широке застосування необхідним програмним продуктом районних прокуратур тісно пов’язано з належним забезпеченням комп’ютерним обладнанням, комп’ютерними мережами, розмножувальною апаратурою [17]. Керівний апарат обласної прокуратури усвідомлює необхідність впровадження сучасних інформаційних технологій. Тому що, як наголошується іншими дослідниками, розвиток підсистеми інформаційної безпеки є важливою складовою стратегії системної інформатизації прокуратури України [18].

Використання інформаційних технологій проводиться не тільки в практичній роботі а й у навчальному процесі при підвищенні кваліфікації прокурорсько-слідчих кадрів Академії прокуратури України. Зокрема, матеріальна база навчального закладу дає змогу ефективно проводити навчання з використанням сучасних технічних можливостей: новітніх засобів електронного зв’язку, сучасної комп’ютерної і оргтехніки, передового програмного забезпечення [19]. Сучасні навчальні аудиторії і відповідне їх оснащення повною мірою дають змогу слухачам засвоювати необхідні знання.

Ефективною робота прокуратур районів буде лише при використанні можливостей комп’ютерних правових програм, впровадженні сучасних технологій отримання, обробки, зберігання і систематизації інформації. Наявна технічна база дає змогу постійного поновлення комп’ютерних правових програм, ведення картотеки нормативних актів, автоматизації обробки статистичної інформації [20]. Використання засобів електронного зв’язку в прокуратурах має певну специфіку (насамперед це пов’язано з захищеністю цих каналів) і вимагає від прокурорських працівників вмінь та навичок користування засобами інформаційної безпеки і каналами електронного зв’язку. Прикладом організації таких мереж може стати електронна мережа, якою користуються органи внутрішніх справ. Це віртуальна комп’ютерна мережа, яку на правах оренди ВАТ “Укртелеком” (монополіст усіх дротовних телекомунікацій) виділяє УМВС по областях. Тобто за договором акціонерне товариство виділяє свої канали зв’язку для користування ОВС. Така мережа має свої як переваги, так і недоліки. Основною перевагою в цьому плані є захищеність каналів зв’язку від несанкціонованого втручання як самими технічними засобами ВАТ “Укртелеком”, так і технічним персоналом УМВС області, рух всієї інформації в мережі знаходиться під контролем співробітників відділу інформаційних технологій.

У сучасних умовах співробітники правоохоронних органів не можуть достатньою мірою тримати в полі зору всі технічні нововведення, що стрімко розвиваються в інформатиці. Готуючи таких співробітників, одним з основних завдань, на нашу думку, є відслідковування новітніх інформаційних технологій, розробка нових методик захисту інформації з застосуванням таких методик на практиці.

Недоліком у розробці методик інформаційної безпеки є те, що методика розкриття та розслідування злочинів, документування, проведення експертиз після проведення необхідних досліджень і обґрунтувань втрачає свою актуальність та своєчасність застосування. Це пов’язано певним чином з так званим феноменом “старіння інформації”, а також з тим, що такі методики розробляються як наслідок злочинної діяльності, а тому самі злочинні прояви (так як це і є новітні інформаційні технології, які на півкроку попереду навіть найсучасніших систем захисту та методик розслідування цих злочинів) можуть ще не мати ефективної протидії. Виходом із цієї ситуації може бути постійний аналіз злочинних проявів у сфері інформаційних технологій, дослідження властивостей та функцій шкідливих програмних засобів, вивчення практичного досвіду фахівців зарубіжних країн у сфері розслідування та проведення комп’ютерних експертиз, вивчення слідової картини, залишеної шкідливим програмним засобом унаслідок несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж та мереж електрозв’язку. Дослідження процесу створення шкідливих програмних засобів їх використання, розповсюдження і збуту, криміналістичне забезпечення практичної діяльності може набувати форму обзорів, довідок, методичних рекомендацій, довідникових посібників.

Автором з метою з’ясування рівня інформаційної культури було проведено анкетування співробітників районного відділу внутрішніх справ України. В результаті 88,8 % опитаних працівників ОВС зазначили, що не мають досвіду роботи в розкритті і розслідуванні злочинів, пов’язаних з виготовленням, розробкою, поширенням і збутом шкідливих програмних засобів. Цей стан речей може засвідчувати, що такий вид злочинів не має широкого поширення або ж високий ступінь його латентності. На думку автора, така ситуація склалася внаслідок масового поширення різного роду програмних систем захисту (антивіруси, фаєрволи, програмні комплекси, спрямовані на виявлення шкідливих програмних засобів і процесів, що загрожують стабільності і функціональності інформаційних систем). Та недостатня правова освіченість користувачів електронної ін-

формації про захист їх інтересів з боку держави і про кримінальну відповідальність за створення, використання, розповсюдження і збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку [22], приводить до латентності такого виду злочинів у силу ряду причин. В практичному аспекті кожен з користувачів персональним комп’ютером неодноразово зустрічався з тими чи іншими шкідливими програмними засобами, а звернення з цього питання в правоохоронні органи носять поодинокий характер.

Під час вивчення результатів опитування бралися до уваги фактори, які зумовлюють низьку ефективність діяльності правоохоронних органів у цій сфері. Опитані респонденти зазначили кілька, на їх думку, суттєвих факторів:

- відсутність знань, розуміння технологічного процесу роботи комп’ютерів (55,5 %);
- відсутність розроблених сучасних методик виявлення та розслідування створення, використання, розповсюдження і збуту шкідливих програмних засобів (50 %);
- новизна таких злочинів, недостатня обізнаність про способи їх вчинення (44,4 %);
- недостатня професійна компетентність та неукомплектованість оперативних працівників (38,8 %).

Опитані співробітники РВ УМВС (100 %) зазначили про необхідність спеціального вивчення тактики злочинців щодо створення, використання, розповсюдження і збуту шкідливих програмних засобів. Результат відповідей саме на це питання свідчить про практичну зацікавленість правоохоронців у вивченні тактики протиправної діяльності з метою ефективної протидії таким злочинним проявам. 94,4 % опитаних повідомили про недостатність методичних рекомендацій, оглядів, літератури стосовно боротьби з шкідливими програмними засобами, призначеними для несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Про недостатність розроблених методик може свідчити те, що Головним слідчим управлінням в 2002 р. розроблена методика “Розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” [22], якою до даного часу користуються практичні працівники. Сучаснішими розробками ця методика не поновлювалась, не говорячи про надходження інших методик у сфері інформаційних технологій в практичні підрозділи.

При з’ясуванні у працівників ОВС джерела інформації про злочини в сфері інформаційних технологій 72,2 % опитаних відповіли, що цим джерелом є обмін досвідом і знаннями з колегами, і лише 22,2 % вказали на службову підготовку і підвищення кваліфікації. Ця проблема не є новою для МВС, і питанням її вирішення постійно приділяється увага. З метою виправлення ситуації, яка склалася в практичних підрозділах ОВС, запроваджено практику цільових виїздів до головних управлінь, УМВС з метою перевірки фахових знань співробітників у цій сфері та надання практичної допомоги. Аналогічну роботу проведено в ряді структурних підрозділів центрального апарату МВС. Проведено семінари та навчальні збори з працівниками служб та іншими підрозділами щодо поліпшення діяльності по захисту інформації і каналів зв’язку [12].

Іншим напрямом виходу з цієї ситуації є налагодження зв’язків навчальних закладів МВС з практичними органами. Цей процес повинен бути двостороннім із взаємною зацікавленістю як навчальних закладів, так і замовників-спеціалістів. Цікавим прикладом зворотного зв'язку у навчанні може бути Прикарпатський юридичний інститут Львівського державного університету внутрішніх справ. Потреби практики активно вивчаються у вигляді: проведення курсів підвищення кваліфікації працівників різних служб, а також керівників міськрайвідділів. При навчанні практичних співробітників

вивчаються і в подальшому враховуються побажання щодо корисності і своєчасності наукових розробок. Узагальнення таких пропозицій проводиться шляхом анкетування [23]. Десь в чомусь схожа підготовка слідчо-прокурорських працівників Академією прокуратури України, яка проводиться на високому професійному рівні співпраці з Академією правових наук та іншими науковими і навчальними закладами України, країн СНД та ЄС [24]. Така діяльність провідного навчального закладу прокуратури налагоджена і розвивається у сфері наукових досліджень, видавничої діяльності, обміну досвідом з підвищення кваліфікації та підготовки кадрів прокурорських працівників.

Підготовка фахівців, які протистоять кіберзлочинності повинна проводитись з урахуванням міжнародного досвіду зарубіжних правоохоронних органів, досягнень у протидії такого виду злочинів. Накази Генеральної прокуратури України чітко зазначають міжнародне співробітництво в роботі органів прокуратури, мета якого – удосконалення механізмів та процедур надання правової допомоги й обміну досвідом, встановлення й розвиток контактів з компетентними установами іноземних держав і міжнародними організаціями [25]. Практичний бік цього співробітництва реалізується у вигляді зустрічей, переговорів, конференцій, семінарів, реалізації проектів і програм співпраці.

Вивчивши потреби практики, вищі навчальні заклади повинні мати сучасні навчальні програми для слідчих, оперативних та експертних підрозділів, готувати фахівців відповідно до державного замовлення цим органам. Необхідно уважно вивчати вимоги підрозділів, що ведуть боротьбу з несанкціонованим втручанням в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж та мереж електрозв’язку. Необхідність підготовки фахівців у сучасних умовах полягає в тому, що сама сфера інформаційних технологій розвивається стрімкими темпами, розробляються та впроваджуються нові системи для передачі даних, технічні стандарти та інше.

Крім цього, при підготовці фахівців необхідно звертати увагу і на зміни законодавства в даній сфері. Відповідно до ст. 35 Європейської конвенції про кіберзлочинність від 23 листопада 2001 р. ратифікованої Верховною Радою України 7 вересня 2005 р. необхідно створити спеціальний орган, який зміг би координувати роботу щодо протидії кіберзлочинності для цілодобових контактів з метою надання негайної допомоги в розслідуванні чи переслідуванні кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосується кримінального правопорушення [26]. При створенні такого органу знову таки постає проблема наповнюваності його необхідними фахівцями для забезпечення виконання покладених функцій.

Такий погляд ученого на розроблювану програму, пов’язану з протидією злочинності в сфері інформаційних технологій, вимагає від вищих навчальних закладів підготовки фахівців як в кількісному, так і в якісному співвідношенні. Оперативно реагуючи на потреби цих органів, на думку автора, можливе створення індивідуальних планів підготовки слухачів та курсантів останніх курсів на замовлення практичних органів.

Певну увагу в цьому необхідно приділяти організації практики слухачів та курсантів таких підрозділів. Така практика повинна бути тісно пов’язана з місцем розподілу молодих фахівців, що дасть змогу випускнику після закінчення вищого навчального закладу усвідомити застосування цих практичних навичок під час навчання. Перебуваючи на переддипломній практиці, майбутній фахівець об’єктивно оцінює фахову підготовку та свої якості в майбутній практичній діяльності.

Зрозуміло, що керівники таких підрозділів хочуть мати добре підготовленого спеціаліста і, бажано, з досвідом оперативної роботи за фахом. Але такими випускники стають лише після тривалої роботи протягом 2 – 3 років під наглядом досвідчених кері-

вників. Тобто досвід приходить тільки з практичним застосуванням теоретичних знань, і найпростіший шлях отримання кваліфікованих працівників – через переддипломну практику та стажування на посаді.

Накази МВС України з метою підвищення фахового рівня слідчих системи МВС України регламентують різні види навчання. В контексті розгляду проблемного питання, пов’язаного з відсутністю розробленої методики запобігання такого виду злочинам, як створення, використання, розповсюдження і збут шкідливих програмних засобів, слід звернути увагу на такий вид навчання, як перепідготовка, підвищення кваліфікації, функціональна підготовка [27]. Цей вид навчання проводиться у вищих навчальних закладах МВС України, інститутах, на факультетах, курсах підвищення кваліфікації і перепідготовки інших міністерств і відомств, в училищах професійної підготовки ГУМВС, УМВС, ГУДСО, навчальних центрах підготовки, за місцем роботи.

Певна відмінність існує у навчанні прокурорсько-слідчих кадрів. Так якісне навчання цих кадрів закріплене наказами Генеральної прокуратури України [28] і зобов’язує щоквартально проводити навчально-методичні семінари, висвітлення в фахових виданнях позитивного досвіду розслідування окремих категорій злочинів, використання можливостей судових експертиз та інших проблемних питань.

Вищі ж навчальні юридичні заклади при підготовці кадрів для прокуратур розробляють навчальні програми з урахуванням практичних потреб прокурорсько-слідчої практики [29].

На думку автора, необхідно підняти статус магістра. Фактично на сьогодні склалася ситуація, що слухачі та курсанти не мають бажання продовжувати навчання в магістратурі і вважають за краще швидше закінчити вищий навчальний заклад у якості спеціаліста. Це пов’язано з тим, що немає різниці у фахових знаннях при отриманні диплома спеціаліста чи магістра і з відсутністю зацікавленості практичних підрозділів у фахівцях з повною вищою освітою. На даний час намічені перспективи розв’язання цієї проблеми, в результаті приєднання України до Булонського процесу та використання в навчальному процесі перспективної кредитно-модульної технології.

В практичній діяльності правоохоронних органів, що протидіють злочинності в сфері інформаційних технологій, позитивні результати показали фахівці, що навчались у вищих навчальних закладах України, які готують спеціалістів для радіоелектронної промисловості, таких як Національний технічний університет України “КПІ”, Харківський державний технічний університет радіоелектроніки, Львівський національний університет, Одеський національний політехнічний університет, Севастопольський національний технічний університет, Державний університет інформаційно-комунікаційних технологій та ін. Підготовка фахівців проходить із спеціалізованим вивченням технологічних і технічних питань захисту інформації та протидії несанкціонованому втручанню в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Тому є сенс в підготовці магістрів і спеціалістів, які мають юридичну освіту, у цих вищих навчальних закладах за державним замовленням правоохоронних органів з урахуванням специфіки подальшої професійної діяльності. Цей процес з боку держави необхідно взяти під контроль та належним чином організувати, викликаючи зацікавленість в подальшому навчанні у магістратурах за вузькопрофільною спеціалізацією.

Актуальною проблемою в підготовці спеціалістів, що займаються боротьбою із злочинністю у сфері інформаційних технологій, є збереження та поповнення викладацьких кадрів, підтримання їх на належному професійному рівні. Не останнє місце в матеріально-технічному забезпеченні навчального процесу займає поповнення таких кафедр талановитою молоддю, створення умов для їх ефективного навчання в сфері інформа-

ційних технологій, належне забезпечення кафедр та навчальних аудиторій комп’ютерною технікою, підвищення заробітної плати викладацькому складу відповідно до професійних здобутків, якостей з підготовки та проведення навчального процесу.

Висновки.

1. Реалії сьогодення вимагають від держави вжити своєчасні й адекватні заходи з протидії злочинності в сфері інформаційних технологій. Суттєвим кроком у цьому напрямі може стати розробка і прийняття загальнодержавної програми підготовки таких фахівців.

2. На належному рівні забезпечити навчальний процес для таких фахівців. Це і матеріальне забезпечення майбутніх фахівців сучасною навчальною літературою не тільки вітчизняних, а й зарубіжних авторів. Забезпечення інформацією щодо передових інформаційних технологій та розробок у сфері захисту інформації. Забезпечення доступу до зарубіжних джерел наукової інформації.

3. Залучати до підготовки таких фахівців як досвідчений професорсько-викладацький склад, так і практичних співробітників. Організація поповнення кафедр молодими спеціалістами, що мають як теоретичні, так і практичні напрацювання в цій сфері. Забезпечення гідної оплати їх діяльності та матеріального забезпечення.

4. Моніторинг навчальних планів, інформаційно-аналітичного забезпечення навчального процесу саме з урахуванням розвитку інформаційних технологій, напрямку злочинних проявів та протидії такій злочинності. Спрямувати таку підготовку на вивчення не тільки в гуманітарній а й в природничо-науковій сфері, тобто не тільки технічне виявлення слідової картини, а й профілактике кіберзлочинів.

5. Стимулювати в процесі навчання майбутніх фахівців такий вид практичної діяльності як розрахункові, курсові роботи та проекти захисту інформації, метою яких є саме закріплення практичних навичок. Постійно проводити відслідковування розробок і здобутків сучасної радіоелектроніки, комп’ютерних технологій у формі обзорів, довідок, методичних рекомендацій, довідникових посібників.

6. Спрямувати таку підготовку не тільки на вміння застосування здобутих практичних навичок, а й на формування професійного світогляду майбутнього фахівця.

7. Організація навчального процесу повинна відповідати потребам практичних правоохоронних органів, готувати фахівців відповідно до державного замовлення та потреб сьогодення з урахуванням передових інформаційних технологій, що розвиваються стрімкими темпами. За необхідності впровадити в навчальний процес індивідуальних планів підготовки на замовлення практичних органів.

8. Для здобуття необхідних практичних навичок майбутні фахівці повинні проходити переддипломну практику та стажування на посаді безпосередньо в тому практичному органі, за направленням якого вони навчали і в подальшому будуть працювати.

9. Приєднання України до Булонського процесу, впровадження європейських стандартів вищої освіти у вітчизняних навчальних закладах значно змінять ставлення до професійної вищої освіти, підвищать статус магістрів, рівень і якість отримуваних знань.

Використана література

1. *Сандул І.* В мережі // Кореспондент. – 2006. – № 30/219. – С. 45.

2. *Романюк Б.В., Гавловський В.Д., Гуцалюк М.В.* Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Практичний посібник. – К., 2004. – С. 144.

3. //www.cybersecurity.ru.

4. *Р.Семеха.* Проблема міжнародного масштабу // Міліція України. – № 5(119)2007. – С. 7.

5. //www.ukranews.com.

6. *Львовски М.* Два самых крутых крымских хакера учились еле-еле, но украли семь месяцев интернет-времени // Сегодня, 14.04.2005 р. – С. 23.

7. *Титунина Е.В.* Донецке готовят киберполицейских // Центр исследования компьютерной преступности //www.crime-research.ru/news/16.02.2005/1813.

8. *Маклаков Г.Ю., Рижков Є.В.* Методологічні підходи до вдосконалення підготовки кадрів ОВС з урахуванням розвитку інформаційних технологій // У кн.: Проблеми правознавства та правоохоронної діяльності: Зб. наукових статей: Вид-во ДІВС МВС України. – 2001. – № 2. – С. 121-133; *Маклаков Г.Ю., Рыжков Э.В.* Методология подготовки кадров МВД с учетом развития современных информационных технологий // В кн.: Информационные технологии и информационная безопасность в науке, технике и образовании “ИНФОТЕХ-2002”: Материалы Международ. науч.-практ. конф. (30 сентября – 5 октября 2002 г., Киев-Севастополь): НТО РЭС Украины, 2002. – С. 109-110.

9. *Маклаков Г.Ю., Рыжков Э.В.* Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий // У кн: Використання сучасних досягнень криміналістики у боротьбі зі злочинністю: Матеріали міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (Донецьк, 12 квітня 2002 року). – Донецьк: ДІВС, 2002. – С. 19-29; *Маклаков Г.Ю.* Возможности современных информационных технологий при проведении криминалистических исследований и экспертиз // У кн: Використання сучасних досягнень криміналістики у боротьбі зі злочинністю: Матеріали міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (Донецьк, 12 квітня 2002 року). – Донецьк: ДІВС, 2002. – С. 342-355.

10. Наказ МВС України № 160 від 20.02.2006 р. (додаток № 6).

11. Зразки бланків процесуальних та інших документів у кримінальній справі: Практичний посібник; Під редакцією В.І.Захарова. – К., 2002 р.

12. *Стешенко Л. Гончаров О.* Канцелярія без стосів паперу: мрія чи реальність? // Іменем Закону. – 2007 р. – № 10. – С. 6-7.

13. Там же. – С. 6-7.

14. Закон України від 19.06.2003 р. № 964-IV “Про основи національної безпеки України”.

15. Підготовка фахівців у сфері інформаційної безпеки: стан в Україні. К.І. Бєляков, В.Д. Гавловський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2005. – № 12 //mndc.naiau.kiev.ua/Gurnal/12.htm.

16. *Романчук П.* Інформаційні технології: від джерел до сучасності // Іменем Закону. – 2007. – № 18-19. – С. 20.

17. Наказ № 7 гн ГП України від 22.04.2004 року “Про організацію роботи з питань правового забезпечення в органах прокуратури”.

18. *Цимбалюк В.* Щодо формування стратегії інформатизації прокуратури України в умовах розвитку інформаційного суспільства // Вісник прокуратури. – 2007. – № (71). – С. 97.

19. Наказ № 2/3 гн ГП України від 30.09.2004 р. “Про вдосконалення організації роботи щодо підвищення кваліфікації прокуросько-слідчих кадрів в Академії прокуратури України”.

20. Наказ № 1/3 гн ГП України від 19.09.2005 р. “Про організацію роботи з питань первинного обліку, ведення статистичної звітності в органах прокуратури та нагляду за обліком злочинів”.

21. Закон України “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” // Відомості Верховної Ради України. – 2005. – № 6. – Ст. 261-262.

22. Збірник методичних рекомендацій з питань розкриття та розслідування злочинів слідчими та оперативними працівниками ОВС; За редакцією П.В. Коляди. – К., 2002. – С.101-127.

23. *Голинський І.* Наука зайняла свою нішу в інституті // Міліція України. – 2007. – № 4. – С. 24-25.

24. Наказ № 2/3 ГП України від 11.11.2005 р. “Про внесення змін до наказу від 30 вересня 2004 р. № 2/3 гн” (п. 6.2).

25. Наказ № 8 гн ГП України від 26.12.2005 р. “Про організацію роботи органів прокуратури України у галузі міжнародного співробітництва і правової допомоги“ (п.п. 2.2).

26. *Гуцалюк М.В.* Міжнародне співробітництво щодо протидії злочинам у сфері інформаційних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2003. – № 8. – С. 97-104.

27. Наказ МВС України № 1444 від 25.11.2003 р. “Про організацію професійної підготовки осіб рядового і начальницького складу органів внутрішніх справ України”.

28. Наказ № 4 гн ГП України від 19.09.2005 р. “Про організацію прокурорського нагляду за додержанням законів органами, які проводять дізнання та досудове слідство” (п.п. 1.3; 11, 16).

29. Наказ № 2/4 гн ГП України від 8.10.2004 р. “Про вдосконалення організації роботи з добору абітурієнтів для вступу до базових вищих навчальних закладів” (п. 1.4).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

неофіційний переклад

Заява Комітету Парламенту Канади з питань громадянства та імміграції від 4 жовтня 2003 року

“НАЦІОНАЛЬНІ ІДЕНТИФІКАЦІЙНІ КАРТКИ (ПОСВІДЧЕННЯ ОСОБИ)”

Ця письмова заява є наслідком зустрічі між Прайвесі Інтернешнл (Privacy International) і Комітетом Парламенту Канади з питань громадянства та імміграції (далі Комітет), що відбулася за зверненням Комітету 24 червня 2003 року у Лондоні (Велика Британія).

Прайвесі Інтернешнл переконливо рекомендує Комітету підходити до проблеми ідентифікаційних карток з великою пересторогою. Багато які з умов, що пред’являються для технології на основі карткової системи не можуть бути підтримані. Обґрунтування руху у напрямку до цієї картки може в окремих випадках робитися з добрими намірами, але здається, що воно засновується більше на емоціях і балаканині, аніж на вірогідному дослідженні.

Біометрична система, запропонована для формування ідентифікаційної бази для картки, не має успішного зразку будь-де у світі. Свідчення дослідників стверджують, що багато з заяв, зроблених біометричною промисловістю, є неправдивими. Насправді, архітектура біометрії, яку уявляють собі деякі прихильники канадської схеми, є повністю шахрайською.

Вартість системи ідентифікаційних карток, разом з відповідними реєстраційними процедурами, інфраструктурою технологій, узгодженням приватного і публічного секторів і рівнобіжних систем буде значно більшою від неофіційних оцінок, що поширюються на даний час. Базуючись на кошторисах Великої Британії, Європи і Південно-Східної Азії, ми оцінюємо, що канадська система, на момент повного завершення, коштуватиме 7 мільярдів канадських доларів.

Загроза приватності, що виникає в результаті впровадження національної ідентифікаційної системи, не може бути переоцінена. Ідентифікаційні картки в канадському (суспільному) оточенні, імовірніше за все, порушуватимуть Хартію прав і свобод. Картка істотно порушить приватність і принципи захисту даних, передбачені в канадському праві.

У дослідницькій літературі відсутні жодні докази для того, щоб встановити, що ідентифікаційні картки зменшують загрозу тероризму чи зменшують сферу злочинності. Насправді, впровадження ідентифікаційної картки потягне створення нової низки правопорушень і внесе цілком реальну загрозу зростання злочинності в значній кількості областей.

Ідентифікаційна картка, запропонована для Канади, передбачає концепцію зведених чи “об'єднаних” ресурсів даних. Такий стан створює серйозну загрозу безпеці даних. Видається неминучим, що дані будуть загублені, перекручені, видозмінені чи незаконно використані. Доступ великої кількості агенцій до даних значно підвищує імовірність неналежного використання інформації або через розкриття, спричинене корупцією, або через недоліки у безпеці.

Короткий огляд

Протягом минулих двадцяти років уряди багатьох країн впроваджували національні ідентифікаційні картки. Прихильники таких систем наводили усе більше і більше доказів на користь прийняття поєднання усесторонньої інформації про особу та біометричного ідентифікатора, на кшталт сканування райдужної оболонки чи відбитків пальців. Велика Британія і Канада, на даний час, розглядають такі системи, у той час як Бельгія і Китай знаходяться на перших стадіях впровадження ідентифікаційних карток.

Формулювання обґрунтування схем ідентифікації значно відрізняється, але звичайно стосується кількох усвідомлюваних переваг, зокрема, зменшення шахрайства, зростання адміністративної ефективності і боротьби з незаконною імміграцією.

Разом з тим часто наводиться зауваження, що карткова система може слугувати каналом “побудови нації”, завдяки чому можуть бути посилені єдність і національна ідентичність. Ці інтуїтивні зауваження не мають жодного відношення до формулювання обґрунтування карток. У цьому сенсі картка може виступати ініціативою, в основі якої лежить націоналізм.

Опікування ідеєю про ідентифікаційні картки здійснюється з невеликою кількістю доказів, що підлягають вимірюванню, стосовно вимог, які пред’являються до карткової системи. Припущення, наприклад, що національна картка може поліпшити методи правоохоронної діяльності, знизити рівень незаконної імміграції, зменшити шахрайство, допоможе національної безпеці чи покращить адміністративну ефективність, є суто інтуїтивним. Існує небагато, якщо вони взагалі є, доказів того, що карткова система може досягти цих цілей.

Основну причину такої ситуації слід шукати в типі націоналізму, згаданому раніше. Країни, на кшталт Малайзії, Китаю, Сінгапуру та Індонезії, відкрито сприяють цим карткам як засобу встановлення національного “членства” і єдності. Торік у Великій Британії ця позиція була виражена проурядовим парламентарієм, доктором Ніком Палмером, який сказав на публічній зустрічі, присвяченій ідентифікаційним карткам, що він відчуває, що ідентифікаційна картка може створити “зв'язок” поміж усього населення. Карткова система часто носить назву чи символ країни (як, наприклад, вже не чинна картка Австралії і картка Ківі).

Біометрична система, запропонована для канадської картки, є необґрунтованою в своїй основі. Китай недавно відмовився від розміщення відбитків пальців на своїх ідентифікаційних картках через нездоланні технічні проблеми [1], тоді як Британська фінансова група “Nationwide” цього року відмовилась від планів запровадити зняття відбитків пальців і сканування ока на заміну PIN-коду [2].

Американські експерти з безпеки Пітер Нойман і Лаурі Вейнстейн відзначали: *“Вважається, що унікальні ідентифікаційні картки часто підробляються. Діє велика кількість груп підробників ідентифікаційних карток, як для кримінальних, так і для терористичних цілей. До цього часу кожна спроба посилити захист посвідчень особи від підробки була скомпрометована. Крім того, зловживання з боку утаємниченої особи – особливий ризик будь-якої інфраструктури посвідчень особи”.*

“Віра в те, що національні ідентифікаційні смарт-картки можуть забезпечити незаперечну біометричну відповідність без некоректних підтверджень або заперечень, є помилковою. Крім того, такі системи усе ще будуть “проламуватися”, а злочинці і терористи, щодо яких ми найбільше стурбовані, знайдуть спосіб експлуатувати їх, використовуючи фальшиве відчуття безпеки таким чином, що картки забезпечуватимуть їхню власну перевагу – фактично ставлячи нас у меншу безпеку в результаті цього” [3].

Існують також істотні загрози безпеці, що виникають як результат системи ідентифікації, заснованої на біометричних характеристиках. Експерт з комп'ютерної безпеки Брюс Шнеєр (Bruce Schneier) застерігає: *“Обробка біометричних характеристик також має свої недоліки. Уявіть собі, що Аліса використовує відбиток свого великого пальця для біометрії, а хтось вкраде цифровий файл. Що тепер? Це не цифрове посвідчення, коли певна довірена третя особа може видати їй інше. Це – її великий палець. Вона має їх тільки два. Як тільки хтось вкраде ваші біометричні характеристики, вони залишаться вкраденими на все життя; не існує жодного способу повернутися до безпечної ситуації”* [4].

Ця заява обговорює значення і ризики, пов'язані з національними ідентифікаційними картками, із спеціальним посиланням як на біометричну, так і на інформаційну відповідність. Цей документ оцінює аргументи, що просувають використання цієї технології, і вагу цих доказів з юридичної, соціальної і технічної перспективи.

Ключові питання і засади

Пропозиції щодо впровадження урядових систем ідентифікаційних карток викликають суперечності в усьому світі. Парламенти Великої Британії і Канади на даний час розглядають національні схеми, результатом яких була б комплексна обов'язкова система ідентифікації. Австралія, Нова Зеландія і Сполучені Штати також мудрують з цією ідеєю, але зустрічають жорст-

кий політичний опір. Країни, що розвиваються, нестримно поспішають запровадити системи ідентифікації, тоді як у всій Європі уряди досліджували можливість розширення функціонування ідентифікаційних карток. Усі такі ініціативи зустрілися з непередбаченими і надзвичайно складними юридичними, технічними та організаційними проблемами.

Такі заходи завжди породжували дебати щодо їхнього потенційного впливу на приватність і громадянські права. Незважаючи на те, що вони є вирішальними, наслідки технології набагато істотніше і стосуються куди ширшої сфери. В своїй сутності, ці системи незмінно прокладають шлях до приєднання до управління і розвитку комплексного зв’язку між публічним і приватним секторами інформаційних систем.

Більше ніж протягом двох десятиліть дискутувалась аргументація: громадянські свободи проти ідентифікаційних карток. Правозахисники послідовно доводили: мало того, що такі ініціативи перетворять нації на більш авторитарні суспільства, але вони назавжди істотно змінять відносини між громадянином і державою, природу уряду і характер нації.

Цей глибокий вплив є неминучим, оскільки сучасні ідентифікаційні картки – не просто шматочок пластмаси. Це видима складова надзвичайно складної мережі інтерактивної технології, що об’єднує найбільш інтимні характеристики особи з державним механізмом. Це також засіб, через який, теоретично, може бути як спрощено, так і розширено юридичні і адміністративні повноваження уряду.

Майже кожна національна ідентифікаційна карткова система, впроваджена протягом останніх п'ятнадцяти років, містила три компоненти, які потенційно можуть зруйнувати свободу особи і приватність. Спочатку кожен громадянин може бути зобов'язаний здати відбитки пальців чи візерунок сітківки до національної бази даних. Ця інформація об'єднується з іншими персональними даними на кшталт раси, віку і місця проживання. Фотографія довершує досьє. Тоді, для того, щоб надати картці необхідної юридичної ваги, її впровадження повинно супроводжуватися суттєвим зростанням поліцейських повноважень. Органи влади, зрештою, вимагатимуть картку в широкому колі випадків, і люди будуть змушені підкоритися. Найбільш істотною, а разом з тим найбільш тонкою складовою є той факт, що картка і її кодова система згодом формуватимуть адміністративну основу для пов’язування інформації між усіма відомствами. Код, врешті-решт, є найбільш потужним елементом системи.

Для такої системи, пов'язаної десятками тисяч пристроїв для читання карток з центральною базою даних, звичайною справою є проблема підроблених карток. Технологічний розрив між урядами й організованою злочинністю тепер звузився до такого ступеня, що бланки навіть найбільш захищених карток стають доступними через тиждень після їхнього офіційного представлення. Злочинці і терористи можуть насправді пересуватися більш вільно і більш безпечно з декількома підробленими індивідуальностями, ніж вони могли б це робити в країні із численними формами посвідчення особи.

Для того, щоб упевнитися, що люди є саме тими, за кого вони себе видають, картки нового покоління на кшталт представлених торік у Малайзії містять чіп з біометрією – відсканові відбитки пальців, рук чи візерунок сітківки – власника. Картка і палець поміщені в пристрій читання – і особу “підтверджено”. Органи влади мають доступ до детальнішої персональної інформації, що зберігається на чіпі, для того, щоб підтвердити особу власника. Цей процес підтвердження може бути застосований на вулиці, в аеропортах, школах, банках, басейнах чи приміщеннях офісів. Для того, щоб картки слугували меті боротьби з тероризмом і крадіжкою ідентичності, вони повинні б використовуватися як механізм підтвердження багато разів на день, у незчисленних випадках.

Цей тверезий висновок рідко наводиться урядом. Натомість, такі ініціативи м'яко замасковані під виглядом картки громадянина, які забезпечують право на соціальні послуги і допомогу і які спрощують ведення справ особи з урядом. П'ять років тому, після останніх дебатів у Великій Британії щодо ідентифікаційних карток, уряд спокійно поховав такі пропозиції, коли виявив, що картка коштуватиме на мільярди фунтів більше, ніж очікувалось, робить небагато для запобігання злочинам, і може, на завершення, стати надзвичайно непопулярною ініціативою [5].

В останніх двох випадках, коли концепція ідентифікаційної картки була серйозно поставлена у Великій Британії, стало зрозуміло, що підтримка ідентифікаційних карток, в кращому випадку, є неоднорідною. Востаннє щодо цього висловилася (злочин був проблемою, що обговорювалась) навіть Асоціація керівників поліції (Association of Chief Police Officers), яка стверджувала, що картка матиме невеликий вплив на злочинність і може зашкодити стосункам між поліцією і громадськістю.

Це правда, що часи і обставини змінюються, але якщо ідентифікаційна картка п’ять років тому була непрацездатною, чому вона працюватиме зараз? Коротка відповідь на це питання полягає в тому, що на той час вона не могла працювати, доки не було додано біометричні характеристики, і вся система не отримала змогу діставати підтвердження через національну базу даних. Тоді, це – не картка: це – національна інфраструктура спостереження.

Посвідчення особи можуть також робити свій внесок у зростання рівня тероризму і злочинності. Торік у Нью-Джерсі було обвинувачено 36 осіб за їхню участь в злочинній організації, що випускала тисячі підроблених ліцензій водіїв. Також було заарештовано вісім осіб з персоналу Відділу транспортних засобів Нью-Джерсі.

Для країни, у якій ліцензія водія є найближчим відповідником до ідентифікаційної картки (національні картки завжди були неприйнятні для Конгресу), арешти викликали досить широке занепокоєння. Речник Відділу кримінальної юстиції Нью-Джерсі сказав “Нью-Йорк Таймс”, що місця для стоянки автомобілів Відділу транспортних засобів, принаймні у шістьох округах, були подібні на “барахолку незаконних документів”. Особи з персоналу підрозділу у окрузі Вейн отримали від 50 до 100 доларів за кожну з приблизно 3000 ліцензій.

Корупція зсередини – це кара для уряду, яку не насмілюються називати. Тепер, незважаючи на свій намір підсилити захист ліцензій водіїв, США зневірились у чесності своїх первинних засобів ідентифікації. Корупція в подібному масштабі оточує більшість офіційних схем ідентифікаційних карток. Високий попит і величезні інвестиції злочинців спокушають посадових осіб обходити чи порушувати правила прийнятності. Те ж саме є неминучим у Канаді та інших країнах.

Досвід у Нью-Джерсі – один з багатьох факторів, що повинні стримати щенячий ентузіазм будь-якого уряду щодо потенційних переваг ідентифікаційної карти. Міністри уявляють інструмент, який приборкає незаконну імміграцію, усуне злочини і шахрайство, зменшить ухиляння від податків і перешкодить тероризму. У дійсності, вони розпочали проект, що може значно посилити і ускладнити ці проблеми.

Розглянемо практичну сторону. Яким чином пересічний громадянин йтиме до одержання ідентифікаційної картки? І яким чином це відрізнятиметься від способу, яким злочинець, терорист чи незаконний іммігрант одержуватиме її?

Протягом років західні уряди, в усіх своїх консультаціях з цього центрального пункту, грали у мовчанку. Будь-яка ідентифікаційна картка, імовірно, видаватиметься особі на персональному інтерв'ю, можливо, подібному до процесу одержання Номера Соціального Страхування чи ліцензії водія Нью-Джерсі. Претендент може прийти на зустріч з нижчою посадовою особою, яка механічно запитає щодо двох форм ідентифікаційної картки і доказу місця проживання. Претенденту задали б кілька стандартних питань, після чого ідентифікаційна картка може бути формально видана.

Якщо перед цим вони могли принести копію свідоцтва про народження мертвої людини, і, можливо, ліцензію водія і номер рахунку в банку, тепер злочинці володітимуть основною ідентифікаційною карткою, яка не задає жодних запитань. Можливо, навіть більше, ніж однією такою ідентифікаційною карткою.

Ідентифікаційна картка, зрештою, є тільки збільшенням високої цінності первинних документів особи, представлених її власником. Адміністрація США мала можливість пересвідчитися, що саме тут міститься фундаментальний недолік у понятті безпомилкової ідентифікаційної картки.

Після нападу на США 11 вересня ФБР оголосило, що принаймні четверо з повітряних піратів одержали чинні ліцензії водіїв США. Для Відділу транспортних засобів Вірджинії, приче-

тність якого до цього було виявлено, це був один з найсерйозніших моментів протверезіння у його тривалій історії. Органи влади Вірджинії розпочали шалену перевірку своїх процедур подання заявок, але повідомили, що існує досить мало можливостей запобігти цій проблемі.

Точно так само як усі, хто видає такі картки в усьому світі, відділ ліцензування не мав жодного вибору, крім того як покладатися на стандартні документи щодо особи, дійсність яких важко визначити. Як тільки претендент отримав НСС, паспорт, свідоцтво про народження і, можливо, рахунок в банку, усі критерії для видання ліцензії буде виконано. Що ще може зробити орган влади, щоб встановити право на ліцензію?

Одна проблема для вірджінських органів ліцензування, якої неможливо уникнути, полягала в тому, що в реальному світі одна основна форма посвідчення особи використовується для того, щоб отримати іншу форму посвідчення особи. Дві форми посвідчення особи ведуть до надання третьої. І так далі. У вільному суспільстві існує межа щодо ступеня, до якого уряд може поставити вимогу особи щодо розкриття цих документів.

Все ж таки органи ліцензування Вірджинії “накрутили хвоста” своєму персоналу, застерігаючи їх бути особливо допитливими при роботі із заявами. *“Не дратуйте наших клієнтів,* – порадило вище керівництво, – *але зробіть усе, що ви можете, щоб встановити потенційних терористів і незаконних мігрантів”*. За винятком деяких незначних змін, процедура авторизації зберігається як і раніше, з тією відмінністю від попередньої, що, безсумнівно, фальсифікація посвідчень особи коштуватиме дорожче.

А якщо заявники не мають необхідних документів? Який це подарунок у пошуку зайвих грошей для корумпованих державних службовців чи персоналу за контрактом! Корупція серед чинів державних службовців є фактом життя. Після двохлітнього слідства Незалежна Комісія Нового Південного Уельсу проти корупції в Австралії засвідчила у 1992 році, що корупція в державній службі досягла “пропорцій епідемії і ендемії”.

Ще більше погіршить перспективу схеми ідентифікаційних карток сценарій, за яким до вирішення цієї проблеми буде залучено приватну компанію, або, навіть ще гірше, її буде “скинуто” на вже перевантажену урядову агенцію.

Уряди можуть дозволити собі ігнорувати загрозу корупції серед чинів організації, що розглядається, однак банки не настільки наївні. Вони застосовують «модель загрози», що передбачає рівень корупції персоналу від одного до двох відсотків.

Навіть без перспективи офіційної корупції технологічний розрив між урядами й організованою злочинністю тепер звузився до такого ступеня, що навіть бланки найбільш захищених карток доступні через кілька тижнів після їхнього представлення. Злочинці і терористи можуть, насправді, рухатися вільніше і безпечніше з декількома підробленими “офіційними” індивідуальностями, ніж будь-коли в країні, використовуючи багаторазові форми посвідчень «низької вартості», на кшталт свідоцтва про народження.

Злочинне використання підроблених ідентифікаційних документів не обов'язково включає використання методів підробки. У 1999 році у Великій Британії колишній державний контролер був обвинувачений в одержанні до 500 паспортів на фальшивих осіб. Шахрайство було просто результатом маніпулювання під час процедури первинного документування.

Доцільно розглянути деякі неминучі формули, що застосовуються всупереч правилам економіки чорного ринку. Кожен раз, коли уряди намагаються запровадити ідентифікаційну картку, в основі завжди лежить мета усунення фальшивої індивідуальності. Чим вище “цілісність” (надійність і точність) картки, тим більшою є її цінність для злочинців і незаконних іммігрантів. Картка, що має високу цінність, притягує значно більші інвестиції у корупцію та підробку. Рівняння просте: вища цінність посвідчення особи дорівнює інтенсивнішій злочинній діяльності.

Коли такі схеми впроваджуються в поточній суспільній атмосфері, неминучими є три результати. Перший: високо захищена ідентифікаційна картка стане внутрішнім паспортом, необхідним в безлічі ситуацій. Не виходьте зі свого дому без неї. Другий: мільйони людей будуть страждати від серйозних незручностей щороку, через загублені, вкрадені чи пошкоджені картки або – через ще більш потенційно руйнівну причину – через відмову карткових комп'ютерних систем чи біометричних машин зчитування. Нарешті, як свідчить дослідження Прайвесі Інтер-

нешнл, картки будуть неминуче використані для зловживання з боку посадових осіб, які використовуватимуть їх як механізм для упередження, дискримінації чи переслідування. Цей останній пункт був сформульований Високим Судом Великої Британії у 1954 році, коли він визнав незаконними ідентифікаційні картки воєнного часу.

Інші країни також дійшли такого висновку. Жодна країна загального права не запроваджувала ідентифікаційних карток. Коли у 1986 році в Австралії було запропоновано національну картку, ця ідея була квапливо переглянута після найбільшої у сучасній історії суспільної опозиційної кампанії. Громадськість Нової Зеландії відповіла з подібною енергією, тоді як Сполучені Штати традиційно виступають проти національних карток.

Їхні побоювання добре обґрунтовані. Зокрема, за минулі вісімнадцять місяців національні лідери в обох півкулях з дивним смакуванням стверджували, що прагнення до більш безпечного суспільства повинно спонукати до переоцінки особистих свобод і приватності. Іншими словами, йдеться про встановлення істотного розширення повноважень держави щодо здійснення контролю за всіма громадянами і зміщення балансу на користь всебічного спостереження за населенням. Саме ідентифікаційна картка стала найбільш виразним проявом цього прагнення до більшого спостереження.

Ще однією підставою є її вартість. П'ять років тому уряд Великої Британії оцінив, що повна вартість виробництва і управління карткою становитиме 20 фунтів стерлінгів на особу. Базова вартість біометричної картки в наші дні вимагатиме щонайменше 45 фунтів. В цілому витрати становлять більше двох мільярдів фунтів стерлінгів. Це число потроїться, коли ми врахуємо вартість модифікації комп'ютерної системи, реєстрацію біографічних даних і узгодження з приватним сектором. Уповноважений з питань приватності Канади нещодавно оцінив, що вартість національної картки в його країні становитиме близько п'яти мільярдів канадських доларів. Базуючись на даних Великої Британії і Європи, Прайвесі Інтернешнл оцінює вартість канадської картки в більш ніж 7 мільярдів доларів.

Ідея щодо національної ідентифікаційної картки приваблива на поверхні, але багато країн виявили, що технологія створює більшу кількість проблем, ніж вирішує. Ідентифікаційні картки завжди служили в ролі емоційної політичної відповіді на кризу, але швидкий огляд країн, у яких в недалекі часи було впроваджено ідентифікаційні картки, свідчить, зазвичай, про виникнення низки непередбачених адміністративних і соціальних труднощів. Таїланд, який впровадив свою першу ідентифікаційну картку у 1989 році, після всіх цих років усе ще продовжує згладжувати фундаментальні проблеми.

Жоден уряд все ще не здатен назвати будь-яку країну, де присутність картки утримала б терористів. Для того, щоб досягти такого результату, уряд вимагав би заходів, неймовірних у вільному суспільстві.

Уряди, таким чином, зустрілися з важким вибором. Або вони впроваджують біометричну картку з високим ступенем захисту, що кине виклик кожному принципу свободи, або вони впроваджують картку з низьким чи середнім рівнем захисту, яка буде незабаром доступна злочинцям і терористам на чорному ринку.

Біометричний обман

Усі незалежні дослідницькі студії висунули на перший план величезну прірву між умовами, заявленими біометричними продавцями, і результатом контрольного тестування.

Нещодавнє дослідження Міністерства оборони США виявило, що розпізнавання райдужної оболонки досягло більшого успіху, ніж більшість технологій, але заявка одного виробника на похибку у 0,5 % помилкової ідентифікації, роздулось до 6 % під час іспитів Міністерства оборони [6].

Доповідь, видана Головною лічильною палатою США (US General Accounting Office) в листопаді 2002 року [7], повідомила про те, що найбільша система сканування райдужної оболонки на даний час використовує тільки 30000 записів. Така маленька система діє зовсім іншим чином, ніж система, у яку залучено мільйони чи десятки мільйонів записів.

Головна лічильна палата застерегла, що “невідомо”, яким чином працюватиме система з багатьма мільйонами записів. В доповіді Національного Інституту Науки і Техніки (the National Institute for Science and Technology) [8] робиться висновок, що через недостатню кількість записів і даних неможливо визначити, чи є розпізнавання райдужної оболонки точним способом ідентифікації.

Фундаментальною проблемою для точного функціонування біометрії залишається співвідношення між унікальними біометричними характеристиками особи і кількістю інших ідентичностей, з якими вони співставляються. Це питання простої математики. Якщо біометричне сканування ока чи відбитків пальців один-до-одного відповідає такому ж скануванню, записаному на картку, шанс точної відповідності надзвичайно високий. Похибка може бути встановлена на дуже чутливому рівні (скажімо, плюс-мінус один відсоток). Однак, якщо результат сканування ока співставляється із, скажімо, сотнею інших ідентичностей (відповідність “один до багатьох”), похибка повинна бути збільшена. Інакше, випадки помилкового відхилення будуть неприпустимі. Якщо сканування ока співставляється з національною базою даних, як це запропонували прихильники канадської системи, похибка буде настільки великою, що зробить систему нічого не вартою.

Саме тому математично і технічно неможливо побудувати і використовувати національну базу даних біометричних ідентичностей без того, щоб неминуче не створити помилкове відхилення майже в кожному випадку, коли особа використовує цю систему.

Співставлення даних з елементів схеми ідентифікаційних карток

Автоматизований розподіл даних між організаціями може спричинити суттєвий ризик для осіб, надійності інформації, професійної ефективності і чесності, репутації організації і суспільства в цілому [9].

Співставлення даних серед численних агенцій є складною і часто недосяжною метою. Успішна програма співставлення, що включає численні джерела, вимагатиме високочутливого і строгого поєднання основних умов. Серед них – точна структура визначень, архівна чи альтернативна система підтримки однакової цілісності і набір взаємопов’язаних кодів і методів, які гарантують, що інформація не буде зруйнована чи видозмінена.

Може бути гарантовано, що загроза надійності даних помітно збільшиться, коли програми співставлення розвиватимуться у напрямі від простої компанії до численної корпорації. Можна рівною мірою гарантувати, що програма відповідності послідовно зазнаватиме невдачі, якщо вона базуватиметься на логічно виведених чи “м'яких” елементах даних.

Протягом кількох років організації були зациклені на ідеї зведених чи “об'єднаних” ресурсів даних. Це становить серйозну загрозу безпеці даних. Також представляється неминучим, що дані будуть загублені, перекручені, видозмінені чи стануть об’єктом зловживання. Доступ численних агенцій до вразливих даних значно збільшує потенціал неправильного використання інформації завдяки розголошенню внаслідок корупції або через “дірку” в безпеці.

Загроза безпеці зростає по експоненті відповідно до розширення кількості використання даних поза джерелом “першого покоління”. Просте партнерство двох агенцій, що включає необроблені “тверді” дані, зберігає більший шанс підтримки його безпеки і цілісності. Надійність даних значно зменшується, а загрози її безпеці значно збільшуються з кожним новим застосуванням даних.

Агенції, що використовують систему відповідності різних джерел, можуть зіштовхнутися з істотним інформаційним перевантаженням. Це особливо має місце у справах щодо здоров'я, соціальної допомоги і захисту дітей, там, де потреба підкріпляти, підтверджувати і відсіювати дані для визначення правильності ідентичностей і подій може створити значну загрозу і більш серйозне робоче навантаження, ніж те, яке існує в неавтоматизованій системі.

Співставлення даних також створює загрозу внутрішньому розвитку організацій. Це особливо має місце в сферах діяльності, що вимагає постійних змін і оцінювання, на кшталт тієї, яка існує в сферах освіти і здоров’я. Режим співставлення може стати центром тяжіння, гальмуючи

процес розвитку і створюючи непотрібні загрози стабільності організаційних відносин і обґрунтованості процедур.

Ідентифікаційні картки і крадіжка ідентичності

На перший погляд, видається логічним доводити, що високоінтегрована система ідентифікації допоможе побороти крадіжку ідентичності. Існує, однак, суттєвий масив доказів для того, щоб продемонструвати, що встановлення централізованої ідентифікації може збільшити кількість випадків крадіжки ідентичності.

Найяскравіший приклад такого зв’язку існує в Сполучених Штатах, де НСС став центром ідентифікації і центральним контрольним пунктом реєстру і зв’язку з ідентичністю. Одержання НСС особою передбачає єдиний інтерфейс для взаємодії цієї особи з величезною кількістю приватних і державних організацій. Отже, рівень крадіжки ідентичності в США є непропорційно високим.

Ця ситуація застосовна, однаково, в Австралії, де впровадження Номера Податкового Досьє також збільшило сферу поширення крадіжок ідентичності понад рівень, засвідчений у Великій Британії та інших країнах, в яких відсутня така централізована кодова система.

Ключовий елемент, що сприяє крадіжці ідентичності, – широка доступність центрального номера, пов'язаного з набором персональної інформації. Організації захисту споживачів у США нещодавно розкритикували Комітет Сенату з банківської справи за провал впровадження заходів, спрямованих на цілковиту зміну цієї тенденції. Спілка Споживачів доводить, що крадіжка ідентичності продовжуватиме зростати, поки зв’язки між НСС і публікацією персональних деталей у секторі фінансів не будуть зменшені [10].

Вартість

Наші оцінки загальної вартості Канадської національної ідентифікаційної картки засновані на цілій низці критеріїв. Вони включають (однак не обмежуються):

- створення повної інфраструктури інформаційних технологій;
- вартість самих карток, враховуючи, за оцінкою, три заміни картки протягом життя;
- узгодження публічного і приватного секторів;
- навчання;
- процедури реєстрації біографії;
- встановлення альтернативних і архівних систем;
- механізм зчитування картки;
- умови співставлення даних;
- витрати, що стосуються регулюючих процедур;
- експлуатаційні витрати, включаючи обслуговування і діяльність інфраструктури;
- витрати на додатковий персонал;
- систему співставлення даних, яка пов’язана з реєстрацією карткової системи.

У своїх недавніх консультаційних документах щодо впровадження “Карт управомочування” уряд Великої Британії оцінив, що базова вартість смарт-карток з біометричними даними коштуватиме приблизно 3,2 мільярди фунтів (7,2 мільярда канадських доларів).

Це число повинне бути скореговане з тим, щоб відобразити менше населення Канади (приблизно 50 відсотків населення Великої Британії). Слід додати межу в 10 відсотків, представлену менш сприятливим обсягом економіки.

Таким чином, за британськими параметрами офіційних базових оцінок, канадська картка коштуватиме 4 мільярди канадських доларів.

Однак, оцінки Великої Британії не включають низку ключових витрат, а саме:

- вартість трьох замін картки протягом життя;
- узгодження з приватним сектором;
- повну вартість процедур реєстрації біографії;
- встановлення альтернативних і резервних систем;

• витрати стосовно регулюючих процедур.

Найбільш точні витрати на узгодження приватного сектору були вирахувані Австралійськими індустріальними групами (Australian industry groups), які оцінили, що витрати на узгодження з приватним сектором складуть, принаймні, п'ятдесят відсотків від повної експлуатаційної вартості карткової системи.

Архівні системи, що були б потрібні як основний модуль карткової системи, додадуть до повної вартості ще двадцять відсотків.

Компонент додаткових карток і заміни карток включатиме витрати, які становитимуть приблизно тридцять відсотків від вартості початкової реєстрації і вартості управління.

Разом з іншими категоріями, ці результати в сукупності складають 7 мільярдів канадських доларів для національної ID системи.

---

[1] //www.news.bbc.co.uk/1/hi/technology/3003571.stm.

[2] //www.silicon.com/news/500013/1/6129.html

[3] Ризики Національних посвідчень особи; Communications of the ACM No 44, 12 грудня 2001 //www.csl.sri.com/users/neumann/insiderisks.html.

[4] Біометрія: використання і зловживання; Communications of the ACM, № 42; 8 серпня 1999 //www.csl.sri.com/users/neumann/insiderisks.html.

[5] //www.privacyinternational.org/issues/idcard/index.html.

[6] //www.news.bbc.co.uk/1/hi/technology/3003571.stm.

[7] Повідомлення Генеральної лічильної палати США щодо безпеки кордону //www.gao.gov/new.items/d03546t.pdf .

[8] //www.itl.nist.gov/iad/894.03/NISTAPPNov02.pdf.

[9] *Роджер Кларк.* Комп’ютерна відповідність урядових агенцій: невдача аналізу вартість/вигода як механізму управління //www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html.

[10] Заява Союзу Споживачів //www.consumersunion.org/pub/core_financial_services/000407.html.

Переклад з англійської Р. Тополевського
//“Свобода Висловлювань і Приватність” • 2004 • 01, 10.09.2004

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

До відома читачів

ШАНОВНІ ЧИТАЧІ !

Науково-дослідний центр правової інформатики Академії правових наук України (НДЦПІ АПрН України) разом з апаратом Верховної Ради України, Верховним Судом України, МВС України та іншими органами державної влади і місцевого самоврядування здійснює планові науково-дослідні роботи та розробки за господарськими договорами й зовнішньоекономічними контрактами правових проблем щодо сфери інформації, інформатики та інформатизації, які спрямовані на побудову в Україні е-середовища.

За результатами робіт за 2001 – 2007 роки НДЦПІ АПрН України на базі аналізу й узагальнень, систематизації міжнародної та вітчизняної практики, оцінки тенденцій, що намітилися, розробив та видав ряд матеріалів, які мають теоретичне та практичне значення у зв’язку з проблемами нормативного упорядкування суспільних інформаційних відносин щодо інформаційної, економічної, фінансової, банківської, технологічної, освітянської, культурної, виробничої, правоохоронної та іншої діяльності.

Результати досліджень будуть корисними для студентів, аспірантів юридичних та інших навчальних закладів при вивченні проблем у галузі інформації, інформатики, інформатизації та інформаційного права, а також при розробці науково-практичних посібників та рекомендацій щодо боротьби з комп’ютерними правопорушеннями в умовах просування країни до інформаційного суспільства.

Перелік основних результатів науково-дослідної роботи та видань НДЦПІ АПрН України

№ з/п	Назва, автор (колектив авторів), видання	Проблематика дослідження	Тип видання
Видання 2002 – 2003 років			
1	***Інформатизація, право, управління: організаційно-правові питання*** / Р. Калюжний, О. Крупчан, В. Гавловський, М. Гуцалюк, В. Цимбалюк, М. Швець; За ред. М. Швеця, О. Крупчана. – К.: АПрН України, 2002.	Про інтегровану систему інформаційно-аналітичного забезпечення	Монографія, 191 с.
2	***Інформаційне суспільство. Дефініції***… / В. Брижко, В. Цимбалюк та ін.; За ред. М. Швеця та Р. Калюжного. – К.: “Інтеграл”, 2002.	Щодо термінів та понять у інформаційній сфері	Словник, 220 с.
3	***Правова інформатика*** / М. Швець, В. Брижко, Р. Калюжний, Ю. Клімашевська, Л. Задорожня та ін.; За ред. М. Швеця та Р. Калюжного. – К.: ІВА, 2003.	Про інформатизацію законотворчої, правоохоронної, судочинної діяльності	Монографія, 168 с.
4	***Вступ до інформаційної культури та інформаційного права*** / В. Цимбалюк, В. Брижко, Р. Калюжний, М. Швець та ін. – К.: ІВА, 2003.	Щодо теорії інформаційної культури	Монографія, 240 с.

5	***Правовий механізм захисту персональних даних*** / В. Брижко; За ред. М. Швеця та Р. Калюжного. – К.: Парлам. вид-во, 2003.	Про упорядкування відносин у сфері персональних даних	Монографія, 124 с.
6	***Інформаційно-пошукова система “Законодавство”***: Посібник. – К.: НДЦПІ АПрН України, 2003. – 103 с.	База даних на CD-ROM (понад 210 тис. документів)	
7	***Інформаційно-пошукова система “Термінологія законодавства”***: Посібник. – К.: НДЦПІ АПрН України, 2003. – 25 с.	База даних на CD-ROM (понад 36 тис. термінів)	
8	***Автоматизоване робоче місце “Кримінолога-аналітика”***: Посібник. – К.: НДЦПІ АПрН України, 2003. – 25 с.	База даних на CD-ROM	
9	***Пошукова система “Дисертаційні дослідження”***. – К.: НДЦПІ АПрН України, 2003.	База даних на CD-ROM	
Видання 2004 року			
10	***Тезаурус EUROVOC***: ***автоматизована інформаційно-аналітична система порівняння законодавства України із законодавством країн ЄС;*** За ред. академіка НАН України В. Тація та академіка АПН України В. Зайчука. – К.: Парлам. вид-во, 2004.	Українська версія тезауруса EUROVOC Європейського парламенту, що визнаний міжнародним стандартом	Посібник, 383 с.
11	***Системна інформатизація законотворчої та правоохоронної діяльності;*** Під науковим керівництвом та редакцією В. Дурдинця та В. Зайчука. – К.: Парлам. вид-во, 2004.	Про запровадження інформаційних систем і технологій	Монографія, 520 с.
12	***Системна інформатизація виборчих і референдумних процесів в Україні*** / В. Фурашев, М. Коваль, С. Маглюй. – К.: Парлам. вид-во, 2004.	Про запровадження інформаційних систем і технологій	Монографія, 608 с.
13	***Основи інформаційного права України*** / В. Цимбалюк, В. Гавловський та ін.; За ред. М. Швеця, Р. Калюжного. – К.: Знання, 2004.	Щодо проблем інформаційного права	Навчальний посібник, 274 с.
Видання 2005 року			
14	***Правова інформатика*** / М. Швець, В. Брижко, Л. Задорожня, Ю. Клімашевська, В. Фурашев, В. Хахановський, В. Цимбалюк та ін. – У 2-х т. – К.: Парлам. вид-во, 2005. – Т. 1.	Про інформатизацію законотворчої, правоохоронної, судочинної діяльності	Підручник, 416 с.
15	***Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє*** / В. Фурашев, Д. Ланде, О. Григор’єв, О. Фурашев. – К.: “Інжиніринг” 2005.	Про питання побудови електронного інформаційного суспільства в Україні	Монографія, 164 с.

16	***Питання вдосконалення законодавства України у сфері інформації та інформатизації*** / Л. Задорожня, М. Коваль, В. Брижко; За ред. члена-кореспондента АПрН України М.Я. Швеця. – К.: “Футарі-Прінт”, 2005.	Щодо аналізу та гармонізації законодавства України із законодавством ЄС	Додаток до журналу “Правова інформатика”, 31 с.
17	***Комплексне порівняльно-правове дослідження відповідності законодавства України законодавству Європейського Союзу у сфері захисту персональних даних*** / М. Швець, В. Брижко, В. Цимбалюк, М. Гуцалюк, Б. Раціборинський. – К.: НДЦПІ АПрН України, 2005.	Про концептуальні, правові, організаційні підходи до створення єдиної системи захисту персональних даних в Україні	Звіт про науково-дослідну роботу, 509 с.
18	***Інформаційне право та правова інформатика у сфері захисту персональних даних*** / В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець; За ред. д.е.н., професора, члена-кореспондента Академії правових наук України М. Швеця. – К.: НДЦПІ АПрН України, 2005.	Про стан законодавства щодо захисту персональних даних у країнах ЄС та вирішення зазначеної проблеми в Україні	Монографія, 451 с.
Видання 2006 року			
19	***Становлення правової інформатики в Україні***: *до 35-річчя інформаційної служби ОВС України та 5-ої річниці з дня створення Науково-дослідного центру правової інформатики Академії правових наук України*. – К.: НДЦПІ АПрН України, 2006 //*www.bod.kiev.ua*.	Про результати досліджень, впроваджені проекти, періодичні публікації та видання (бібліотеки) на CD-ROM	Буклет, 8 с.
20	***Бібліотека баз даних і знань у галузі держави і права.*** – К.: НДЦПІ АПрН України, 2006.	База даних на CD-ROM	
21	***Тезаурус “Судова практика”.*** – К.: НДЦПІ АПрН України, 2006.	База даних на CD-ROM	
22	***е-майбутнє та інформаційне право*** /В. Брижко, В. Цимбалюк, М. Швець, Ю. Базанов; За ред. д.е.н., професора, члена-кореспондента АПрН України М. Швеця. – 2-е вид., доп. – К.: НДЦПІ АПрН України, 2006	Про стан і перспективи державної інформаційної політики та системної інформатизації	Наукове видання, 234 с.
23	***Програмно-апаратний комплекс інформаційної підтримки прийняття рішень*** / Ланде Д.В., Фурашев В.М., Григор’єв О.М. – К.: “Інжиніринг”, 2006.	Про теоретичні та практичні питання побудови електронного суспільства в Україні	Науково-методичний посібник, 48 с.
24	***Системна інформатизація законотворчої та правоохоронної діяльності*** / Керів. авт. кол. Швець М.Я.; За ред. В. Дурдинця, О. Зайчука, В. Тація. – К.: “Навчальна книга”, 2005.	Про впровадження та використання інформаційних систем і технологій	Наукове видання, 639 с.

25	***Нормативно-правові засади системної інформатизації інформаційно-аналітичного забезпечення здійснення процедур виборчих і референдумних процесів*** / В.М. Фурашев. – К.: НДЦПІ АПрН України, 2006.	Про нормативно-правові засади для інформаційно-аналітичних систем і технологій щодо проведення виборів і референдумів	Монографія, 144 с.
26	***Системна інформатизація правоохоронної діяльності.*** – У 2-х кн.; За ред. В. Дурдинця та М. Швеця // Упорядники: М. Швець, В. Брижко, Б. Романюк, В. Цимбалюк. – К.: НДЦПІ АПрН України, 2006. *Інформаційне забезпечення та переклад*: Ю. Базанов, Віра Брижко, Т. Шиманська, О. Гладківська, В. Гавловський, М. Гуцалюк, О. Лебединська, С. Антоненко, С. Швець, Л. Хоровицька, А. Мельник, Д. Юзова.	*Книга 1* – про стан та напрями розвитку інформатизації в ОВС України *Книга 2* – переклади стандартів Ради Європи та Європейського Союзу у сфері захисту персональних даних	Монографія, кн.1 - 290 с. кн.2 - 509 с.
	Видання 2007 року		
27	***Правова інформатика.*** – 2-е вид. доп. та перероб; За редакцією В. Дурдинця, Є. Моісеєва та М. Швеця. – К.: ТОВ “ПанТот”, 2007 р. *Авторський колектив*: М. Швець, В. Брижко, В. Фурашев, Б. Раціборинський, М. Целуйко, В. Цимбалюк, Г. Середа, І. Рогатюк, Ю. Кліма-шевська, В. Хахановський, Л. Задорожня.	Про побудову, впровадження та використання інформаційних систем і технологій у законотворчій, правозастосовній, правоохоронній та право освітній діяльності	Підручник, 524 с.
28	В.М. Брижко, М.Я. Швець, В.С. Цимбалюк. ***Е-боротьба в інформаційних війнах та інформаційне право;*** За ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. – К.: НДЦПІ АПрН України, 2007 р.	Про застосування інформаційної зброї, захист інформаційних ресурсів, кодифікацію інформаційного законодавства України	Монографія, 234 с.
29	***Організаційно-правові основи протидії податковим та суміжним правопорушенням у сфері електронного банкінгу***: Збірник матеріалів науково-практичного круглого столу. – Ірпінь-Київ: Національний університет державної податкової служби України, НДЦПІ АПрН України, 2007.	Доповіді та наукові статті учасників науково-практичного “круглого столу”	Додаток до журналу “Правова інформатика”, 82 с.
30	***Системна інформатизація правоохоронної діяльності;*** За ред. В. Дурдинця, М. Швеця. – К.: НДЦПІ АПрН України, 2007 р.	Про перспективи та напрямі розвитку системної інформатизації в ОВС України	Підручник, 382 с.

31	Фурашев В.Н., Ландэ Д.В., Брайчевский С.М. ***Моделирование информационно-электоральных процессов.*** – К.: НИЦПИ АПрН Украины, 2008 г.	Про моделювання поведінки електоральних груп	Монографія, 182 с.
Видання 2008 року			
32	В. Брижко, Ю Базанов, М. Швець. ***Електронний банкінг у контексті захисту персональних даних***; За ред. члена-кореспондента АПрН України М.Швеця. – К.: НДЦПІ АПрН України, 2008 р.	Про стан та перспективи упорядкування інформаційних відносин	Наукове видання (за матеріалами НДР), 141 с.
33	***Малий словник термінів інформаційного права України*** / Укладачі Калюжний Р.А., Марущак А.І., Петров О.Г., Юзова Д.В. – К.: НДЦПІ АПрН України, 2008.	Щодо змісту деяких термінів та понять	Додаток до журналу “Правова інформатика”, 48 с.

Якщо Вас, шановні читачі, зацікавило те або інше видання, звертайтеся за адресою:

01032, м. Київ, вул. Саксаганського, 110-В,
Науково-дослідний центр правової інформатики
Академії правових наук України.

Тел.: ***234-94-56; тел./факс: 234-55-60***
e-mail: ***bib_rada@i.kiev.ua***

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Про редакційну колегію:

Голова редакційної колегії – **М.Я. ШВЕЦЬ,** доктор економічних наук, професор, член-кореспондент АПрН України, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, лауреат Премії ім. Яр. Мудрого; *заступник голови* – **В.М. БРИЖКО,** кандидат юридичних наук (Doctor of Philosophy), старший науковий співробітник, заслужений винахідник республіки, лауреат Премії ім. Яр. Мудрого;

Науковці з юридичних наук: **В.Д. ГАВЛОВСЬКИЙ,** кандидат юридичних наук, старший науковий співробітник, лауреат Премії ім. Яр. Мудрого; **А.П. ЗАКАЛЮК,** доктор юридичних наук, професор, академік АПрН України, заслужений діяч науки і техніки України; **Р.А. КАЛЮЖНИЙ,** доктор юридичних наук, професор, лауреат Премії ім. Яр. Мудрого; **О.Л. КОПИЛЕНКО,** доктор юридичних наук, професор, академік АПрН України; **В.В. КОСТИЦЬКИЙ,** доктор юридичних наук, професор, член-кореспондент АПрН України, заслужений юрист України; **О.Д. КРУПЧАН**, кандидат юридичних наук, член-кореспондент АПрН України; **О.В. ПЕТРИШИН,** доктор юридичних наук, професор, академік АПрН України; **М.Я. СЕГАЙ,** доктор юридичних наук, професор, академік АПрН України; **В.П. ТИХИЙ**, доктор юридичних наук, професор, академік АПрН України; **В.Г. ХАХАНОВСЬКИЙ,** кандидат юридичних наук, доцент; **В.С. ЦИМБАЛЮК,** кандидат юридичних наук, старший науковий співробітник, лауреат Премії ім. Яр. Мудрого;

Науковці з економічних наук: **С.М. БЕЗРУТЧЕНКО**, кандидат економічних наук, **І.Б. ЖИЛЯЄВ**, кандидат економічних наук, **Л.М. ЗАДОРОЖНЯ,** кандидат економічних наук, доцент, заслужений економіст України; **С.В. ЛИХОСТУП,** кандидат економічних наук; **Б.Л. РАЦІБОРИНСЬКИЙ,** кандидат економічних наук, старший науковий співробітник;

Науковці з технічних та математичних наук: **О.А. БАРАНОВ,** кандидат технічних наук, лауреат Державної премії України в галузі науки і техніки; **О.В. ГЛАДКІВСЬКА,** кандидат фізико-математичних наук; **І.О. ЗДЗЕБА,** лауреат Державної премії України в галузі науки і техніки, лауреат Премії ім. Яр. Мудрого; **І.В. СЕРГІЄНКО,** доктор фізико-математичних наук, професор, академік НАН України.

- ✓ Редакційна колегія не завжди поділяє погляди авторів публікацій.
- ✓ Статті видаються в авторській редакції. Можливо внесення змін редакційного змісту без узгодження з автором.
- ✓ Якщо кількість матеріалу однієї статті перевищує 10 стор., редакція залишає за собою право на його скорочення.
- ✓ Листування з читачами – тільки на сторінках журналу.
- ✓ Автор безкоштовно отримує 1 прим. номера журналу, в якому надрукована його стаття. В разі додаткової потреби примірників необхідно за свій рахунок замовити в редакції їх певну кількість.

==========

Адреса редакції: 01032, м. Київ-32, вул. Саксаганського, 110-В.
Тел.: 234-94-56, 246-48-58; тел./факс: 234-55-60; e-mail: *bib_rada@i.kiev.ua*.
Розрахунковий рахунок: № 35224002002155, банк: УДК у м. Києві,
МФО 820019, код ЄДРПОУ 25959933.

Свідоцтво про державну реєстрацію журналу: серія КВ № 8254 від 22.12.2003 р., видане Державним комітетом телебачення і радіомовлення України.

Виготовлено з оригінал-макета НДЦПІ АПрН України в друкарні ТОВ “ПанТот”
01103, м. Київ, бул. Др. Народів, 28; тел. 239-10-49; e-mail: *poligraf@ndei.kiev.ua*

==========

ШАНОВНІ ДРУЗІ !

Журнал “Правова інформатика” видається у двох варіантах – паперовому та електронному.

Паперовий варіант тиражується в обмеженому обсязі.
Телефон для довідок: **234-94-56**.

Для ознайомлення зі скороченим змістом матеріалів пропонуємо відвідати сайт Науково-дослідного центру правової інформатики Академії правових наук України: ***www.bod.kiev.ua*** або безпосередньо – електронну версію журналу: ***www.bod.kiev.ua/jurnal.***

Електронний варіант на CD-ROM, крім повного змісту журналу, містить **інформаційно-пошукову систему “Законодавство” з базами даних:**

- БД “Законодавство України” – понад 210 тис. документів;
- БД “Термінологія законодавства України” – понад 36 тис. термінів;
- БД “Законопроекти” – понад 19400 документів;
- БД “Судова практика” – понад 9300 документів;
- БД “Міжнародні документи” – понад 12 тис. документів;
- БД “Київ” – понад 13700 документів;
- БД “Крим” – понад 15900 документів;
- Міжнародний багатомовний тезаурус ЄС “EUROVOC”;
- Інформація про дослідження з проблем держави і права.

Замовити передплату на електронний варіант журналу “Правова інформатика” та вказані бази даних можна за телефоном: 234-55-60.

Для передплатників журналу встановлення та обслуговування баз даних здійснюється з активованим щоденним поновленням по e-mail або FTP – за пільговими цінами.