Окремого дослідження потребує і система обліку продуктивності праці, якщо в розкритті злочину брали участь працівники міліції різних служб, а також слідчий як самостійно, так і разом з працівниками міліції. Основним показником для обліку роботи кожного працівника має бути те, що він розкрив злочин самостійно або разом з іншими працівниками. При такому обліку кількість фактично розкритих злочинів повинна дорівнювати показникам роботи працівників служб органів внутрішніх справ, що працювали над їх розкриттям. Сьогодні в органах внутрішніх справ іноді відбувається дублювання персонального внеску служб у розкриття злочинів, і якщо їх поєднати разом, то вони можуть перевищити кількість вчинених злочинів, як це не парадоксально.

Показник продуктивності роботи працівників міліції не буде повним, якщо дійсно не враховувати кількість розглянутих заяв і повідомлень про події та злочини й факти профілактики.

Що стосується показників продуктивності роботи працівників міліції, служби боротьби з економічною злочинністю, то основним показником, разом з профілактичною роботою, розглядом заяв та повідомлень про правопорушення, повинна бути кількість виявлених злочинів за відповідними категоріями на одного працюючого співробітника міліції.

3. *Встановлення та відстеження об'єктивності інформації про рівень злочинності та результати роботи міліції за допомогою соціологічних методів*, одним з яких є систематичне (один-два рази на рік) опитування громадян про злочини, що вчинені за видами: проти громадського порядку, моралі, здоров'я населення і т. ін., про реагування органів міліції тощо, яке практикується у деяких країн світу.

Соціологічне опитування громадян доповнюється думками працівників правоохоронних органів, спеціалістів з цього приводу і самих засуджених.

~~~~~~~~~~ ● ● ● ~~~~~~~~~~~~

В.БРИЖКО, *заслужений винахідник республіки,*
лауреат Премії імені Ярослава Мудрого

ДО ПИТАННЯ ЩОДО МІЖНАРОДНИХ СТАНДАРТІВ ЗАХИСТУ ДАНИХ

Створення українського законодавства щодо захисту даних бере свій початок з 1992 року. На той час Закон України "Про інформацію" можна з певністю відзначити, як такий, що випереджає свій час. Необхідно віддати належне його розробникам та законодавцям: коли всі ще не відвикли від того, що буквально все належало всім, вони чітко окремими положеннями прописали у законі про введення права власності на інформацію в країні, а також проголосили її товаром.

Більше того, в Законі вперше пробилися паростки ідей приватності (prіavecy) в частині прав людини щодо захисту своїх персональних даних. Закон відніс до одного з основних видів інформації будь-які відомості про людину та у статті 23 проголосив, що *"забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом"*. Було декларовано право громадян на доступ до інформації про них, що збирається в державних і недержавних організаціях, вказані умови відмови, відстрочки та оскарження задоволення запиту щодо доступу до офіційних документів. Одночасно у статті 37 Закону вказувалось, що *"не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять у собі інформацію, що стосується особистого життя громадян"*.

У 1996 році захист персональних даних отримав закріплення у статті 32 Конституції України: *"Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини"*.
~~~~~~~~~~

Разом з тим, діючі в державі правові положення не в достатній мірі створюють умови гарантованого забезпечення захисту персональних даних. Незважаючи на наявність загальних норм конституційного і цивільного права, інформаційного законодавства та низки інших законодавчих актів, є зрозумілим, що в області захисту персональних даних відсутній ефективно діючий механізм реалізації зазначених прав, що відповідає нормам європейських стандартів. Це знайшло відображення, зокрема, в рішенні Конституційного Суду України 1997 року у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру", який офіційно визнав, що *"механізм зазначеного права належним чином не визначений"*.

Таким чином, є сенс звернутися до загальних європейських принципів та підходів у нормативно-правовому впорядкуванні суспільних інформаційних відносин щодо захисту персональних даних.

Конвенція № 108 Ради Європи від 28.01.1981 року

Закони щодо захисту даних за кордоном почали приймати у 1970-х рр. Головною передумовою їх появи було виникнення ком'ютера, активне поширення автоматизованих баз даних, розвиток телекомунікаційних мереж та, одностайно, потреба у врегулюванні інформаційних відносин стосовно приватного життя людини за умови забезпечення інтересів суспільства і ефективного функціонування держави.

Враховуючи зростаючу активність у використанні сучасних інформаційно-комп'ютерних технологій та мереж і загрозу несанкціонованої автоматизованої обробки персональних даних в умовах різного рівня їх захисту, європейські країни ухвалили Конвенцію № 108 Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" від 28.01.1981 р. Положення Конвенції № 108 Ради Європи зобов'язали країни-учасниці здійснити коригування національних законодавств у частині втілення встановлених нею основних принципів захисту персональних даних. З того часу захист персональних даних виокремився в самостійний вид діяльності.

Сьогодні Конвенція № 108 Ради Європи – головний та єдиний правовий акт, який визначає загальні принципи та підходи до розбудови національних законодавств у зазначеній сфері. Розглянемо його основні вимоги.

Згідно з Конвенцією № 108 Ради Європи держави, які підписали цей документ, зобов'язуються керуватися її положеннями при розгляді питань, пов'язаних із захистом персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах. Кожна держава-член Конвенції № 108 Ради Європи коригує національне законодавство у частині втілення її основних принципів та поставленої мети – забезпечення на території будь-якої держави-члена поваги до прав та основних свобод кожної особи, незалежно від її громадянства або місця проживання. Держава-член Конвенції № 108 Ради Європи має право самостійно визначати категорії персональних даних, які підлягають захисту.

До захисту персональних даних висуваються певні вимоги. Їх отримання та обробка мають здійснюватися законним шляхом. Вони повинні зберігатися та використовуватися у визначених та законних цілях, бути точними та поновлюваними, допускати ідентифікацію фізичної особи. Засоби та заходи, що їх застосовують, повинні передбачати захист персональних даних від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та втрати.

Конвенція № 108 Ради Європи передбачає дуже важливий момент, згідно з яким збирання, накопичення, зберігання і поширення відомостей про фізичну особу може здійснюватися лише з дозволу особи, дані про яку обробляються. Цій особі надано право знати місце роботи та проживання розпорядника бази персональних даних, а також право отримувати відповідні дані без затримок та у зрозумілій формі. У разі відмови зацікавлена особа може звернутися до суб'єкта нагляду за дотриманням законодавства у державі, який повинен забезпечити припинення порушень, зазначених у національному законодавстві.

Виходячи з інтересів суспільства і держави, Конвенція № 108 Ради Європи допускає обмеження у правах фізичних осіб, якщо це стосується державної чи суспільної безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та основних свобод інших осіб.

Взаємодія між державами-членами Конвенції № 108 Ради Європи має здійснюватися за принципами, що не забороняють передачу персональних даних на територію іншої держави-члена за умов забезпечення адекватного захисту даних. Допускається обмеження цієї вимоги у разі, якщо національне законодавство передбачає особливий порядок регулювання та визначення видів персональних даних у зв'язку із специфічністю деяких відомостей, крім випадків, коли законодавство іншої держави-члена має адекватний ступінь захисту.

Держави-члени зобов'язані підтримувати своїх громадян, які проживають за кордоном, і допомагати Уповноваженому органу своєї держави у питаннях захисту персональних даних.

Для захисту персональних даних Конвенція № 108 Ради Європи зобов'язує кожну державу-члена призначити один чи більше уповноважених органів нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи (Комісару Ради Європи по захисту персональних даних). Завдання інституту уповноваженого передбачають створення організаційно-правових умов забезпечення діяльності щодо захисту персональних даних у країні.

Зазначений орган виконує свої функції в повній незалежності, що є елементом ефективного захисту осіб у зв'язку з обробкою їх персональних даних. З цією метою вищезазначений орган нагляду повинен мати, зокрема, повноваження щодо втручання у діяльність, яка пов'язана з обробкою персональних даних.

Він також може брати участь в судовому розгляді або повідомляти компетентні судові органи про порушення законодавства у сфері захисту персональних даних. Уповноважений орган розглядає та приймає рішення щодо заяв будь-якої особи стосовно обробки персональних даних в межах своєї компетенції. Рішення уповноваженого органу можна оскаржити в суді.

Десятиліття, що минули з часу прийняття Конвенції № 108 Ради Європи, показали, що інститут уповноваженого з питань захисту персональних даних не лише зберігся, а й дістав поширення в усіх західноєвропейських країнах. На даний час уповноважені органи з питань захисту персональних даних діють більше ніж у двадцяти країнах Європи. Їх діяльність свідчить, що вони є ефективним засобом, здатним забезпечити баланс інтересів людини, суспільства і держави. У Німеччинії, наприклад, за його участі вдалося законодавчо оформити право на захист персональних даних як основне право фізичних осіб і розглядати його як конституційну норму.

Директиви Європейського Союзу

Виходячи з економічних інтересів забезпечення вільної трансграничної передачі персональних даних, Європейський Союз у 1995 році ухвалив Директиву 95/46/ЄС "Про захист осіб у зв'язку з обробкою персональних даних і вільного обігу цих даних" , а потім у 1997 році – Директиву 97/66/ЄС "Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі" .

Ці документи деталізують положення Конвенції № 108 Ради Європи та вводять обмеження на передачу даних як у Європу, так і з Європи у країни, де не прийняті закони з адекватним рівнем захисту персональних даних. Вони гарантують країнам, які дотримуються європейського режиму захисту персональних даних, вільний обмін такими даними. Тому, щоб процеси торгівлі не потерпали від європейських вимог щодо захисту даних, країни Сходу (Австралія, Гонконг, Нова Зеландія), Південної Африки, Америки (Канада) тощо прийняли відповідні закони з питань захисту даних. На сьогодні зазначені документи визначають принципи упорядкування інформаційних відносин у сфері захисту персональних даних не лише для європейських, а й для інших країн світу та є міжнародними стандартами. Сьогодні більше 20 країн Європи та 40 країн світу мають закони з питань захисту даних, що відповідають цим стандартам.

Директива 95/46/ЄС "Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних" від 24.10.1995 р. У 1995 році Європейський парламент на підставі положень Договору про заснування Європейського Союзу та висновку Комісії Економічної та Соціальної Ради ЄС ухвалив

Директиву Європейського парламенту та Ради Європейського Союзу 95/46/ЄС "Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних" від 24 жовтня 1995 р.

Головна причина, що спонукала ввести додаткові рекомендації до положень Конвенції № 108 Ради Європи, полягає у тому, що захист персональних даних у країнах здійснювався на різних рівнях регламентації, який надавався національними законодавчими, регулятивними та адміністративними положеннями.

Директива 95/46/ЄС складається з констатуючої частини, 7 розділів та заключних положень. Вона конкретизує європейські принципи та загальні умови обробки персональних даних, умови правової допомоги, відповідальності та санкцій, порядок передачі даних до третіх країн, обумовлює необхідність укладання кодексу поведінки при обробці персональних даних, а також відображає організаційні питання, що пов'язані з правами та обов'язками контрольного (наглядового) органу та консультативної групи у питаннях захисту персональних даних у державах-членах Конвенції № 108 Ради Європи. Згідно з Директивою 95/46/ЄС у Раді Європи створено Комітет по захисту персональних даних, який складається з представників держав-членів Конвенції № 108 Ради Європи.

Констатуюча частина Директиви 95/46/ЄС містить 72 принципи-рекомендації щодо захисту персональних даних. Вона акцентує увагу на те, що системи обробки всіх видів персональних даних призначені сприяти економічному та соціальному прогресу, розвитку взаємовигідного обміну та добробуту людини. Вільний рух товарів, капіталів і послуг, пересування громадян передбачає не лише вільний рух персональних даних, а й забезпечення високого рівня їх захисту у країнах Європейської Співдружності. Цього вимагає збільшення обсягів співробітництва, зростання інформаційних потоків та розширення телекомунікаційних зв'язків.

Найбільш важливими рекомендаціями Директиви 95/46/ЄС є такі:

* обробка персональних даних має здійснюватися лише за згодою зацікавленої фізичної особи. Під обробкою персональних даних слід вважати будь-які дії чи сукупність дій, які здійснюють чи не здійснюють за допомогою автоматизованих систем. Обробка включає збирання, реєстрацію, накопичення, зберігання, модифікацію, комбінування, компіляцію, поширення та будь-яку іншу форму дій, що дозволяють мати доступ до персональних даних, а також їх блокування та знищення на носіях інформації;
* фізична особа має бути повідомлена про факт обробки її персональних даних під час їх реєстрації, крім випадків, що передбачені законодавством;
* фізична особа має право знати про передачу її персональних даних третім особам, а також – точну та повну інформацію про обставини такої передачі;
* право доступу до персональних даних не повинно завдавати шкоди комерційній таємниці та правам інтелектуальної власності;
* стосовно до доступу та окремих обов'язків з обробки персональних даних держава-член має право встановити виключення з правил, які зазначені у Директиві 95/46/ЄС, виходячи з інтересів національної безпеки, оборони, охорони порядку, найважливіших економічних чи фінансових інтересів, проведення досліджень, встановлення нових юридичних процедур та переслідування порушень професійних норм поведінки;
* захист персональних даних передбачає використання технічних та організаційних заходів з моменту створення системи обробки;
* відповідальним за обробку персональних даних та їх передачу в електронний спосіб є особа, яка обробляє дані, а не особа, яка надає послуг з передачі даних. Особа, яка надає послуги зв'язку, несе відповідальність за додаткову та необхідну для функціонування засобів зв'язку обробку персональних даних;
* національне законодавство повинно передбачати відповідальність суб'єктів відносин, пов'язаних з обробкою персональних даних, за невиконання вимог щодо захисту персональних даних згідно з чинними нормами як приватного, так і публічного права;
* держави-члени зобов'язані забезпечити заходи для повного виконання рекомендацій Директиви 95/46/ЄС. Національне законодавство не повинно містити правові норми, які б сприяли

зниженню рівня захисту, а навпаки, повинно мати за мету забезпечення підвищення рівня захисту персональних даних.

В інтересах економічної та інформаційної безпеки допускається впровадження норм, які встановлюють нові методи обробки персональних даних, не передбачених Директивою 95/46/ЄС, та надають можливість обробки звукових чи образотворчих персональних даних, а також – спостереження відеокамерами.

Для звукових та образотворчих даних принципи Директиви 95/46/ЄС застосовуються тоді, коли має місце їх автоматизована обробка або ці дані розміщені (будуть розміщені) у сховищах з вільних до них доступом. Ці принципи необхідно узгоджувати з нормами, що визначають свободу слова при забезпеченні журналістських, літературних чи мистецьких цілей, насамперед в аудіовізуальному секторі.

Забороняється здійснювати обробку персональних даних:

* якщо обробка не відповідає цілям, для яких збиралися дані, насамперед цілям, пов'язаним з виборами, коли відсутні правові норми, що встановлюють гарантії їх захисту;
* коли персональні дані можуть заподіяти шкоду правам людини та основним свободам, приватному життю інших осіб;
* коли персональні дані пов'язані виключно з особистими інтересами та справами домашнього господарства (особисте листування, ведення списків та ін.).

У Директиві 95/46/ЄС зазначено, що іноземна особа має дотримуватися національного законодавства про захист персональних даних тієї держави, на території якої вона перебуває. При цьому захист юридичних осіб не є предметом Директиви 95/46/ЄС.

Забороняється здійснювати передачу персональних даних до третьої країни, якщо її законодавство не надає адекватний рівень захисту даних. Однак можуть бути встановлені обмеження цієї заборони, наприклад, коли зацікавлена особа дала на це свою згоду або коли мається на меті вирішення проблем великого суспільного значення, таких як проблеми оподаткування, страхування, переслідування злочинців тощо.

Принципи Директиви 95/46/ЄС не застосовують для захисту анонімних чи окремих даних, що розташовані у неструктурованих (згідно з визначеними критеріями) папках та обробляються в ручний спосіб.

Директива 95/46/ЄС зобов'язує створити в кожній державі уповноважений орган нагляду та забезпечення захисту персональних даних, який розглядається як найважливіший елемент захисту прав людини та основних свобод. Орган нагляду повинен мати у своєму розпорядженні необхідні для виконання своїх функцій засоби і повноваження щодо розслідування, насамперед, скарг, поданих до нього чи до суду.

Директива 95/46/ЄС також зобов'язує держави розробляти кодекси поведінки для осіб, які здійснюють обробку персональних даних.

Для держав-членів встановлені конкретні терміни реалізації положень Директиви 95/46/ЄС:

* термін 3 роки від дати набрання чинності положень національного права, прийнятими на виконання Директиви 95/46/ЄС, для приведення національного законодавства у відповідність з її вимогами;
* термін 12 років від дати набрання чинності положень національного права, прийнятими на виконання Директиви 95/46/ЄС, для завершення створення національної системи електронного документообігу щодо персональних даних.

Директива 97/66/ЄС від 15.12.1997 р. та рекомендації Ради Європи від 09.12.1997 р. щодо захисту персональних даних у телекомунікаційному секторі. Дотримуючись проголошеного Конвенцією № 108 Ради Європи та Директивою 95/46/ЄС секторального принципу захисту персональних даних, Європейський парламент ухвалив 15 грудня 1997 р. Директиву 97/66/ЄС "Про обробку персональних даних та захист прав осіб у телекомунікаційному секторі".

Директива 97/66/ЄС має більш вузьку сферу застосування порівняно з Директивою 95/46/ЄС та конкретизує обробку даних операторами під час надання телекомунікаційних послуг,

зокрема за допомогою мережі Інтернет. Її рекомендації спрямовані на захист користувачів від спаму (нав'язливої реклами) та визначають гарантії таємниці зв'язку.

У своєму повідомленні до Директиви 97/66/ЄС Європейська комісія зазначала: "*Унікальною особливістю Інтернет є те, що він одночасно функціонує як засіб розповсюдження інформації та як засіб комунікації. У будь-який час споживач може за бажанням отримати інформацію та забезпечити її ретрансляцію третім особам. Таким чином, Інтернет принципово відрізняється від традиційних засобів інформування, у тому числі від традиційних телекомунікаційних мереж*".

Детальному забезпеченню права на захист персональних даних у телекомунікаційних мережах присвячені рекомендації Ради Європи.

У вступі Рекомендацій від 9 грудня 1997 р. "Основні напрями захисту прав фізичних осіб у зв'язку з обробкою персональних даних в інформаційних супермагістралях" зазначається, що "*документ призначається для організації практичної діяльності користувачів та провайдерів послуг мережі Інтернет (поняття "провайдер послуг Інтернет" використовується у якості загального поняття, що включає різні інстанції провайдерів, доступ провайдерів мереж, провайдерів електронної дошки оголошень, магістральних провайдерів, провайдерів інформаційного змісту)*".

Звертаючись до фізичних осіб, рекомендації вказують, що "*використання мережі Інтернет покладає відповідальність за кожну вашу дію, що піддає ризику конфіденційність приватного життя. Тому важливо діяти таким чином, щоб було забезпечено захист персональних даних та зберігалися добрі стосунки з іншими*".

Рекомендації вказують, що захист персональних даних є фундаментальним правом, яке слід захищати законодавством. Кожному повинно бути відомо про його права та обов'язки щодо обробки та використання персональних даних.

Далі рекомендації звертають увагу користувачів та провайдерів послуг на особливості використання системи Інтернет.

Користувачі Інтернет мають враховувати таке:

Інтернет не є безпечною мережею. Слід використовувати всі засоби для захисту персональних даних, такі як законодавством дозволене шифрування конфіденційної електронної пошти, а також паролі доступу до персонального комп'ютера.

Після кожної операції на вузлах Інтернет, які були відвідані, залишаються "сліди". Ці "електронні сліди" можуть бути використані для збирання різних відомостей щодо відвідувача. Якщо дозволено законом, необхідно використовувати псевдонім, при цьому ідентифікуюча інформація буде відома лише провайдеру послуг Інтернет.

Необхідно надавати провайдеру послуг Інтернет чи будь-якій іншій особі лише ті персональні дані, які слугують потребам забезпечення комунікації.

Адреса електронної пошти також є персональними даними і може бути використана з різною метою. Адреса електронної пошти чи інші відомості персонального змісту можуть бути включені до різних каталогів чи списків користувачів. Користувач Інтернет-послуг повинен запитувати про призначення каталогів та вимагати виключення своїх персональних даних з них, якщо не бажає у них фігурувати. Необхідно бути уважним та обережним з веб-вузлами, які вимагають надання більше відомостей, ніж це необхідно для доступу до вузла.

Слід пам'ятати, що користувач Інтернет-послугами може нести юридичну відповідальність за персональні дані, які приймає та передає третім особам. Поширення даних зі злим наміром може завдати шкоди з юридичними наслідками.

Провайдер послуг Інтернет несе відповідальність за правильне використання персональних даних. Час від часу варто з'ясовувати в нього: які персональні дані він збирає, зберігає і поширює, яким чином і з якою метою. Він зобов'язаний виправляти дані, якщо вони помилкові, чи знищити їх, якщо вони надлишкові чи застаріли.

У тому випадку, коли споживач не вдоволений способом, яким провайдер послуг Інтернет збирає, зберігає та поширює персональні дані і він не змінює цей спосіб, необхідно перейти до іншого провайдера.

Перед передачею персональних даних в іншу країну варто перевіряти її юридичний статус (наприклад, одержати консультацію про ратифікацію країною Конвенції № 108 Ради Європи). Якщо країна не ратифікувала Конвенцію, може знадобитися, щоб одержувач, якому надають персональні дані, дав свою згоду на укладення спеціального договору про захист персональних даних, рівень якого повинен бути адекватним вимогам національного законодавства.

Для *провайдерів послуг Інтернет* рекомендації із захисту даних наступні.

Необхідно використовувати всі доступні процедури і нові технології, що забезпечують захист персональних даних.

Необхідно інформувати користувачів про ризики, яким вони можуть піддаватися при використанні мережі Інтернет, перед тим як вони підписалися на послуги чи почали користуватися Інтернет-послугами.

Необхідно надавати користувачам можливість застосування ними псевдоніма і інформувати про технічні засоби захисту, можливості шифрування, що підвищують безпеку передачі персональних даних у мережі.

Не читайте, не змінюйте і не знищуйте повідомлення. Не дозволяйте нікому чинити будь-який вплив на зміст повідомлень. Це може здійснюватися тільки державним органом, що уповноважений на це законом. Сприяйте державним органам у встановленні походження зловмисних і образливих повідомлень, а також інформуйте їх про порушення законодавства про захист персональних даних.

Збирайте і зберігайте персональні дані користувачів тільки у випадках, якщо це вкрай необхідно. Не зберігайте персональні дані довше, ніж це потрібно для досягнення мети обробки (наприклад, не слід зберігати рахунки довше визначеного терміна, якщо це не передбачено податковим, цивільним чи карним законодавством).

Провайдер може використовувати персональні дані для реклами тільки у випадку, якщо на те не має заперечення відповідної особи і за умов додержання зазначеної мети використання.

Перед тим, як користувач починає користуватися послугами вузла провайдера, при запиті з його боку, варто інформувати його про те, які персональні дані обробляються, яким чином, з якою метою і як довго. За вказівкою користувача Інтернет-послугами негайно виправляйте його помилкові персональні дані чи знищуйте їх, якщо вони надлишкові чи застаріли.

Перед опублікуванням персональних даних на вашому веб-вузлі варто звернутися до національного законодавства для визначення правомірності публікації даних і врахувати, що публікація може порушувати конфіденційність особистого життя інших осіб, а також може бути заборонена законодавством.

Перед передачею персональних даних в іншу країну варто перевірити юридичний статус країни та адекватність заходів захисту персональних даних.

Забезпечення захисту персональних даних можна здійснити шляхом використання механізму зворотного зв'язку з органом відповідальним за нагляд і контроль захисту персональних даних в країні, та іншими органами виконавчої влади.

Щодо практичних кроків у адаптації законодавства України в сфері захисту персональних даних до міжнародних стандартів, то вже виконана відповідна підготовча робота.

На виконання Указу Президента України від 06.12.2001 № 1193/2001 "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" та Доручення Кабінету Міністрів України від 23.01.02 № 17884/1 щодо завершення вирішення питання підписання від імені України Конвенції № 108 Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" 1981 року здійснено переклад з англійської українською мовою та офіційне засвідчення Міністерством закордонних справ України тексту зазначеної Конвенції.

Та сама робота була проведена щодо Додаткового протоколу від 08.11.2001 року до Конвенції № 108 Ради Європи, який зобов'язує створити в державі один (або більше) уповноважений орган нагляду, відповідальний за забезпечення захисту персональних даних.

Усе складнішим і мобільнішим стає суспільне життя. Все частише воно використовує різні електронні засоби та інформаційні ресурси. Відомості щодо людини, як найбільш чутлива, делікатна і важлива для неї інформація, займають особливе місце в суспільних інформаційних відносинах. Від розуміння цього багато в чому залежить спокій і благополуччя як окремої людини, так і забезпечення інтересів суспільства та ефективного функціонування органів влади.

Використана література

1. Конституція України. Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. – К.: Офіційне видання Верховної Ради України. 1996.

2. Закон України "Про інформацію" від 02.10.1992 р. № 2657–XII.

3. Конвенція № 108 Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних". Страсбург, 28.01.1981 р. // www.convention.coe.int/treaty/en/Treaties/Html/108.htm. Офіційний переклад; засвідчено МЗС України від 01.07.2002 р.

4. Додатковий протокол до Конвенції № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо уповноважених органів нагляду та міждержавних інформаційних потоків. Страсбург, від 08.11.2001 р. // www.conventions.coe.int/treaty/en/Treaties/Html/181.htm. Офіційний переклад; засвідчено МЗС України від 01.07.2002 р.

5. Директива 95/46/ЄС Європейського парламенту та Ради Європейського Союзу "Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних" від 24.10.1995 р. // www.evropa.eu.int /ISPO/legal/en/dataprot/directiv/directiv.html.

6. Директива 97/66/ЄС Європейського парламенту та Ради Європейського Союзу "Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі" від 15.12.1997 р. // www.evropa. eu.int/ISPO/legal/en/dataprot/protection.html.

О.БАЗАНОВ, студент 4 курсу Національного технічного університету "Київський політехнічний інститут "

ІНФОРМАЦІЙНА СИСТЕМА АНАЛІЗУ ДАНИХ ЩОДО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ОБ'ЄКТІВ

Останнім часом успіхи в галузі технічного і математичного забезпечення ЕОМ обумовили різке впровадження обчислювальної техніки майже в усі сфери людської діяльності. Зараз терміни "інформаційно-аналітична система", "база даних" та "система управління базами даних" зрозумілі не тільки фахівцям комп'ютерної галузі. Нам важко уявити, як можна швидко і якісно обробляти великі об'єми інформації без допомоги комп'ютера. Часи, коли обробка будь-якої інформації велася вручну, можна назвати середньовіччям.

Згідно зі ст. 3 Конституції України – *"Людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю"* [1, – С. 3]. При цьому, з часів початку конституціоналізму починається історія розвитку теорії держави і права, яка заснована на існуючих природних законах. Англійський юрист Д.Локк вперше визначив положення про те, що не тільки право на життя і право на свободу, але й право на володіння майном є природними правами людини [2, – С. 25]. У сучасному світі право на життя, на свободу та недоторканність власного майна вважаються найголовнішими для людини.

Правоохоронні органи, що покликані охороняти громадян від злочинних зазіхань, повинні миттєво реагувати на протиправні дії, в них має бути дуже великий об'єм інформації для того, щоб швидко і точно аналізувати будь-яку ситуацію, робити відповідно тільки правильні висновки. Без автоматизованих засобів збирання, аналітико-синтетичної обробки даних у роботі сучасних правоохоронних органів усе вищезгадане просто неможливе. Зазначене потребує створення відповідних автома-