МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.5

М.Ф. БОНДАРЕНКО, д-р техн. наук, Н.С. ЛЄСНА, канд. техн. наук, О.О. ТКАЧ, В.М. КАРАВАЄВ, О.І. ШУМОВ

ПОЛОЖЕННЯ ПРО ОБРОБКУ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ХНУРЕ

Вступ

Національною доктриною розвитку освіти, затвердженою Указом Президента України від 17.94.2002 р. №347/2002, державною програмою "Інформаційні та комунікаційні технології в освіті і науці на 2006–2010 рр.", затвердженою постановою Кабінету Міністрів України від 07.12.2005р. № 1153, законом України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр." від 09.01.2007 р. та рядом інших нормативних актів. визначено пріоритетні напрями державної політики у галузі інформатизації освіти.

Відповідно до визначених напрямів інформатизації в Харківському національному університеті радіоелектроніки (далі – Університет) впроваджені автоматизовані інформаційні (інформаційно-телекомунікаційні) системи та технології, які забезпечують вирішення завдань обробки та ефективного використання інформації в електронній формі в більшості основних процесів інформаційної діяльності: навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом. Разом із тим, у зв'язку з особливостями використання та розповсюдження інформації, окремі процеси інформаційної діяльності реалізуються не автоматизованими інформаційними технологіями (обробка та використання інформації у формі картотек, архівів, особистих справ, довідників, адресних книг та інших паперових документів без використання комплексів засобів автоматизації).

Суттєвою особливістю певної частини впроваджених в Університеті інформаційних процесів навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом та відповідних інформаційних технологій є використання відомостей про фізичну особу (персональних даних) під час обробки інформації навчального, соціального, фінансового, науково-технічного, адміністративного та іншого характеру.

Враховуючи необхідність застосування сучасних технологій при автоматизованій обробці інформації про особу, а також виникнення загрози для конкретної людини стосовно витоку та несанкціонованого використання персональних даних, багато європейських країн підписали Конвенцію № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [1] та Додатковий протокол до Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [2].

Принципи, що містяться у Конвенції, уточнюються і розширюються в Директиві 95/46/ЕС Європейського парламенту і Ради Європи від 24.10.95 р. "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" [3], в Директиві 2002/58/ЄС Європейського парламенту й Ради Європи від 12.07.2002 р. "Про обробку персональних даних та захист таємниці сектора електронних комунікацій (директива про секретність та електронні комунікації) [4], Директиві 2006/24/ЕС Європейського парламенту та Ради Європи від 15.03.2006 р. "Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та внесення поправок в Директиву 2002/58/ЕС" [5].

У зв'язку з набуттям чинності закону України "Про захист персональних даних" [6] виникла необхідність запровадження єдиного підходу щодо визначення і формування завдань, функцій, підрозділів та окремих посадових осіб, їх повноважень та відповідальності, а також

організації робіт із захисту персональних даних впродовж всіх етапів життєвого циклу інформаційних систем Університету.

З метою вирішення цих питань в Університеті, як передбачено ст. 6. Закону [6], було розроблено "Положення про обробку та захист персональних даних" (далі – Положення), яке регулює діяльність Університету з питань обробки та захисту персональних даних в інформаційних (автоматизованих) системах та в картотеках персональних даних (далі – залежно від контексту викладення використовується узагальнюючий термін – інформаційні системи персональних даних (ІСПДн)).

Положення є офіційним керівним документом Університету, який призначений для керівного складу, фахівців підрозділів захисту інформації та працівників структурних підрозділів, які організують і здійснюють роботи з обробки інформації про фізичну особу (персональних даних) в процесі інформаційної діяльності з навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом.

Положення складається з наступних основних розділів, короткий зміст яких наведений далі.

1. Розділ "Загальні положення"

В розділі визначені мета і призначення документу, галузь застосування, порядок затвердження "Положення ..." і змін до нього, обов'язок уповноважених працівників Університету забезпечити кожному суб'єктові персональних даних можливість ознайомлення з документами й матеріалами, що безпосередньо зачіпають його права й свободи, якщо інше не передбачено законом.

2. Розділ "Суб'єкти відносин, пов'язаних із персональними даними"

В розділі відповідно до ст. 2 і 4 Закону [6] наводиться перелік юридичних та фізичних осіб, які пов'язані із обробкою персональних даних в ІСПДн Університету, а саме:

1) МОН України – власник баз персональних даних відомчих інформаційних систем, компоненти яких впроваджені в Університеті за наказами Міністерства (системи "Освіта", "Конкурс", "Реєстр докторів наук та професорів" та ін.). МОНУ затверджує мету обробки персональних даних у базах даних цих систем, встановлює склад цих даних та процедури їх обробки;

2) Органи державної влади та органи місцевого самоврядування (Податкова адміністрація, Пенсійний фонд та ін.) – власники баз персональних даних державних інформаційних систем, компоненти яких впроваджені в Університеті, до повноважень яких відповідно до закону належить здійснення обробки та захисту персональних даних, затвердження мети обробки персональних даних у базах даних цих систем, встановлення складу цих даних та процедур їх обробки;

3) Харківський національний університет радіоелектроніки, якій є:

– власником баз персональних даних власних інформаційних підсистем, що впроваджені в Університеті за наказами ректора, який затверджує мету обробки персональних даних у базах даних цих підсистем, встановлює склад цих даних та процедури їх обробки (підсистеми "Університет", "Приймальна комісія", "Відділ кадрів професорсько-викладацького складу", "Профком студентів" та ін.);

– розпорядником баз персональних даних інформаційних підсистем, компоненти яких впроваджені в Університеті за наказами МОН України, законів та нормативно-розпорядчих документів органів державної влади та органів місцевого самоврядування (податкові органи, пенсійні фонди, органи соціального страхування, органи статистики та ін.);

4) Уповноважені працівники Університету – посадові особи (проректори, керівники структурних підрозділів) й працівники структурних підрозділів Університету, яким наказом ректора надано право здійснювати обробку персональних даних в інформаційних системах персональних даних Університету;

5) Суб'єкти персональних даних в Університеті – фізичні особи (носії персональних даних), які передали на обробку, як на добровільній основі, так й у рамках виконання вимог законів та нормативно-правових актів, свої персональні дані Університету, у тому числі: наукові й науково-педагогічні працівники, студенти, здобувачі вчених ступенів, аспіранти й докторанти, абітурієнти, слухачі курсів й окремих освітніх програм, інші особи, що надають персональні дані Університету;

6) Уповноважений державний орган з питань захисту персональних даних – Державна служба з питань захисту персональних даних – центральний орган виконавчої влади, до повноважень якого належить захист персональних даних, що утворюється відповідно до законодавства;

7) Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, власника чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій власником чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону (юридичні й фізичні особи, які звертаються до Університету за одержанням необхідних відомостей про фізичну особу – суб'єкта персональних даних і користуються ними без права передачі й розголошення).

В розділі також визначаються функції та повноваження окремих посадових осіб і підрозділів щодо організації, планування, координації робіт з обробки та забезпечення захисту персональних даних в ІСПДн Університету.

3. Розділ "Поняття й склад персональних даних"

В розділі наведений семантичний аналіз правових аспектів визначення терміну "персональні дані" ст. 2 Закону "Про захист персональних даних" [6].

Зазначено, що суб'єктом персональних даних фізична особа стає з моменту, коли з'являється можливість її ідентифікації, тобто встановлення тотожності або можливість відокремлення від інших на підставі збігу характеристик. Ідентифікація може бути проведена за однією унікальною особистою характеристикою індивідуальності або за комбінацією кількох загальних і особистих характеристик особи. Ідентифікація особи можлива безпосередньо (пряма) або опосередковано (непряма). Наводяться приклади прямої та непрямої (опосередкованої) ідентифікації.

Наведено, що для визначення того, чи можна особу конкретно ідентифікувати (встановити), повинні враховуватися всі засоби, використання яких власником бази персональних даних чи якою-небудь іншою особою імовірно очікувати для ідентифікації цієї особи. Таким чином, визначення вичерпного переліку характеристик індивідуальності, які однозначно кваліфікують відомості як персональні дані, залежить від кількості можливих засобів ідентифікації фізичної особи в конкретній інформаційній системі персональних даних.

Зазначено, що конкретний склад та зміст персональних даних в кожній ІСПДн Університету визначається її функціональним призначенням, складом і змістом даних її інформаційного забезпечення, категоріями суб'єктів персональних даних і затверджується ректором Університету відповідно до положень законів, нормативно-правових актів в галузі трудових цивільно-правових відносин і освіти України, міжнародних угод та нормативно-розпорядчих документів МОН України.

З метою визначення методів і способів захисту інформації, необхідних для забезпечення безпеки персональних даних проводиться категоріювання персональних даних, що обробляються, та класифікація інформаційних систем на етапі їх створення або в ході експлуатації (для раніше введених в експлуатацію і (або) модернізованих інформаційних систем). Порядок проведення класифікації інформаційних систем персональних даних визначається нормативними документами Державної служби з питань захисту персональних даних.

У відповідності із визначенням терміну "персональні дані", особливих вимог до їх обробки, що визначені в законі [6], та ступенем можливих негативних наслідків для фізичної осо-

би у випадку порушення заданої характеристики їх безпеки в інформаційних системах Університету, запропоновані чотири категорії персональних даних.

В розділі наведені узагальнені переліки персональних даних (в т.ч. по категоріям), що сформовані на підставі складу та змісту персональних даних, що визначені у законах та інших нормативно-правових актах України в області трудових відносин й освіти, нормативних й розпорядницьких документах МОН України, наказах ректору Університету.

Також в розділі для кожної категорії суб'єктів персональних даних Університету наведений базовий склад документів, у яких містяться персональні дані.

Далі в розділі зазначено, що відповідно до законів [6, 9] персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом (далі – ІзОД), якій за своїм правовим режимом надано статус конфіденційної.

4. Розділ "Принципи обробки персональних даних"

Відповідно до вимог закону [6] в розділі визначені наступні принципи, яких слід дотримуватися при обробці персональних даних в ІСПДн Університету:

– законності (легітимності) цілей і способів обробки;

– відповідності цілей обробки персональних даних;

– законності персональних даних (дані повинні бути отримані на законних підставах й оброблені сумлінним і законним способом);

– адекватності й релевантності персональних даних (склад та зміст даних мають бути відповідними та ненадмірними стосовно визначеної мети їх обробки);

– якості даних (дані мають бути точними, достовірними, у разі необхідності вчасно оновлюватися);

– анонімності (дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються);

– строковості обробки даних (дані обробляються у строк, не більший ніж це необхідно відповідно до їх законного призначення за винятком випадків, установлених законами України);

– гарантії безпеки (дані повинні бути захищені від випадкового або несанкціонованого знищення або випадкової втрати, а також несанкціонованого доступу, зміни або поширення);

– приватності суб'єкта персональних даних (обробка даних грунтується на основі дотримання особистих прав суб'єктів персональних даних);

– правоздатності суб'єкта персональних даних (суб'єкт персональних даних Університету, якому належать відповідні персональні дані, є їх власником, який у повному об'ємі реалізує немайнові права володіння, користування, розпорядження цими даними);

– правоможності власника бази персональних даних (Університет як власник та розпорядник баз персональних даних виконує функцію володіння цими даними й має повноваження розпорядження ними в межах, установлених законодавством України).

5. Розділ "Загальні правила обробки персональних даних"

В підрозділах цього розділу відповідно до вимог закону [6] визначені цілі, основні положення і умови обробки персональних даних. Наведені правила використання, збирання, накопичення та зберігання в інформаційних (автоматизованих) системах (підсистемах) Університету і в картотеках персональних даних, зміни і доповнення, знищення, поширення персональних даних.

6. Розділ "Права та обов'язки суб'єктів персональних даних та Університету"

В розділі відповідно до вимог Конституції [7] та законів [6, 9] визначені права та обов'язки фізичних осіб, які є суб'єктами персональних даних, та юридичної особи – Університету, як власника баз персональних даних.

7. Розділ "Порядок доступу до персональних даних"

В розділі відповідно до вимог закону [6] наведено порядок:

– доступу працівників Університету до персональних даних суб'єктів;

– доступу до персональних даних інших суб'єктів відносин, пов'язаних із персональними даними;

– відстрочення або відмова у доступі до персональних даних;

– оскарження рішення про відстрочення або відмову в доступі до персональних даних

– оплати доступу до персональних даних.

8. Розділ "Захист персональних даних"

Персональні дані належать до окремих видів інформації, необхідність захисту якої визначено законодавством [6].

Розділ включає такі підрозділи: цілі захисту персональних даних, об'єкти захисту, принципи забезпечення безпеки персональних даних, загальний порядок організації захисту персональних даних в Університеті, захист персональних даних у інформаційних (автоматизованих) системах (підсистемах) Університету, захист персональних даних в картотеках персональних даних

В підрозділі *"Цілі захисту персональних даних"* відповідно до Конституції [7] та чинного законодавства [6, 8, 9] визначені головна мета та основні цілі захисту персональних даних суб'єктів захисту.

В підрозділі *"Об'єкти захисту"* відповідно до законів України [6, 9, 10] та постанови КМ України [11] наведені об'єкти захисту в ІСПДн Університету:

В підрозділі *"Принципи забезпечення безпеки персональних даних"* наведені наступні принципи системно-концептуального підходу забезпечення безпеки персональних даних в ІСПДн Університету:

1) Законності. Уповноважені працівники Університету повинні бути освідомленні про відповідальність за правопорушення в області захисту інформації в ІСПДн (ст. 330, 363, 363-1 та інші статті Кримінального Кодексу України) [12];

2) Відповідальності Університету перед зовнішніми сторонами. Згідно з Законом України "Про захист інформації в інформаційно-телекомунікаційних системах" [10] Університет повинен забезпечити адекватний захист цієї інформації і несе відповідальність за порушення конфіденційності, цілісності та доступності персональних даних під час їх обробки засобами системи;

3) Системності та комплексності. Захист повинен здійснюватися ешелоновано на основі комплексного застосування методів та засобів захисту інформації, взаємодії всіх елементів та служб Університету;

4) Своєчасність. Розробка системи захисту повинна вестися паралельно з розробкою й модернізацією самої ІСПДн. Це дозволить урахувати вимоги безпеки при проектуванні архітектури й, в остаточному підсумку, створити більш ефективну (як по витратах ресурсів, так і по стійкості) захищену систему;

5) Безперервність захисту;

6) Економічна доцільність (порівнянність можливого збитку й витрат);

7) Обов'язковість й ефективність контролю;

8) Науково-технічна обгрунтованість і реалізуємість;

9) Спадкоємність і безперервність удосконалення;

10) Спеціалізація й професіоналізм. Експлуатація цих заходів і засобів повинна здійснюватися професійно підготовленими посадовими особами Університету;

11) Взаємодія й координація – при забезпеченні безпеки персональних даних взаємодія із Держслужбою з питань захисту персональних даних, Держспецзв'язком України, МОН України й іншими зацікавленими органами виконавчої влади, а також з підприємствами й

організаціями, що залучаються для виконання робіт із забезпечення безпеки персональних даних.

Підрозділ *"Загальний порядок організації захисту персональних даних в Університеті"* встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в інформаційних (автоматизованих) системах та в картотеках персональних даних, основні з яких наведено нижче.

Захист персональних даних в Університеті від незаконної обробки, а також від незаконного доступу до них здійснюється відповідно до вимог Конституції України [7], закону України "Про захист персональних даних" [6], інших законів та нормативно-правових актів, міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, приписів Державної служби з питань захисту персональних даних, нормативно-розпорядчих документів Держспецзв'язку, МОН України та інших органів державних влади, уповноважених в області захисту інформації, а також затверджених положень й інструкцій Університету.

Захист персональних даних є однією із складових частин управлінської, наукової та навчальної діяльності щодо забезпечення безпеки інформації і являє собою сукупність організаційних і технічних заходів, які ґрунтуються на вищевикладених принципах.

Згідно закону [6] державна політика з питань захисту персональних даних реалізується Державною службою з питань захисту персональних даних у взаємодії з іншими центральними та місцевими органами державної виконавчої влади. Забезпечення захисту персональних даних у базах персональних даних в електронній формі та у формі картотек покладається на власника цих баз.

Враховуючи наявність у складі ІСПДн Університету як компонентів відомчих та державних інформаційних систем, так і власних інформаційних підсистем, забезпечення захисту персональних даних відповідно до закону [6] покладається:

– на МОН України як власника баз персональних даних відомчих інформаційних систем, компоненти яких впроваджені в Університеті за наказами Міністерства (системи "Освіта", "Конкурс", "Реєстр докторів наук та професорів" та ін.);

– органи державної влади та органи місцевого самоврядування (Податкова адміністрація, Пенсійний фонд та ін.), як власників баз персональних даних державних інформаційних систем, компоненти яких впроваджені в Університеті;

– Університет, що є власником баз персональних даних власних інформаційних підсистем, які впроваджені в Університеті за наказами ректора.

Безпека персональних даних при її обробці в ІСПДн Університету досягається шляхом виключення несанкціонованого, в тому числі випадкового, доступу до персональних даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій.

При обробці персональних даних в інформаційних (автоматизованих) системах та картотеках персональних даних Університету має бути забезпечено:

а) проведення заходів, спрямованих на запобігання несанкціонованого доступу до персональних даних і (або) передачі їх особам, які не мають права доступу до такої інформації;

б) своєчасне виявлення фактів несанкціонованого доступу до персональних даних;

в) недопущення впливу на технічні засоби автоматизованої обробки персональних даних, в результаті якого може бути порушено їх функціонування;

г) можливість негайного відновлення персональних даних, модифікованих або знищених внаслідок несанкціонованого доступу до них;

д) постійний контроль за забезпеченням рівня захищеності персональних даних.

Безпека персональних даних при їх обробці в інформаційних системах Університету забезпечується за допомогою систем захисту персональних даних, що включають організаційні заходи та засоби захисту інформації (у тому числі криптографічні засоби, засоби запобігання несанкціонованому доступу, програмно-технічним впливам на технічні засоби обробки пер-

сональних даних), а також інформаційні технології, що використовуються в інформаційній системі.

Роботи з забезпечення безпеки персональних даних при їх обробці в інформаційних системах Університету є невід'ємною частиною робіт щодо створення інформаційних систем. Витрати, пов'язані із здійсненням заходів щодо захисту персональних даних, включаються до загального кошторису на створення ІСПДн.

Під організацією захисту персональних даних при їх обробці в ІСПДн Університету розуміється формування сукупності заходів, що здійснюються на всіх стадіях життєвого циклу систем, узгоджених за метою, завданням, місцем і часом, спрямованих на запобігання (нейтралізацію) і протидії загроз безпеки персональних даних, на відновлення нормального функціонування ІСПДн після нейтралізації загроз, з метою мінімізації як безпосереднього, так і опосередкованого збитку від можливої реалізації таких загроз.

Заходи щодо організації робіт із захисту персональних даних є складовою частиною комплексу робіт із захисту конфіденційної інформації в Університеті і мають деякі особливості при організації та проведенні заходів, які зумовлені чинним законодавством у сфері захисту персональних даних.

Також в підрозділі наведений загальний порядок організації робіт із захисту персональних даних в ІСПДн Університету та вимоги до розміщення і фізичному захисту приміщень та обладнання ІСПДн.

Підрозділ *"Захист персональних даних у інформаційних (автоматизованих) системах (підсистемах) Університету"* у доповнені до загального порядку організації захисту персональних даних в Університеті встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в інформаційних (автоматизованих) системах (далі – автоматизовані ІСПДн), основні із яких наведені нижче.

Забезпечення захисту персональних даних в автоматизованих ІСПДн Університету повинне здійснюватися відповідно до загальних вимог та організаційних засад, що визначені міжвідомчими "Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [11], нормативними документами Державної служби з питань захисту персональних даних та відомчими нормативно-розпорядчими документами МОН України.

Обробка конфіденційних персональних даних в автоматизованих ІСПДн Університету повинна здійснюватися з використанням захищеної технології, яка спрямована на забезпечення режиму безпеки.

Під режимом безпеки розуміється установлений відповідно до вимог законодавства єдиний порядок забезпечення захисту конфіденційної інформації, який визначає сукупність правових, організаційних (адміністративних), інженерно-технічних заходів, заходів контролю за дотриманням цього порядку тощо, а також правила застосування програмно-апаратних засобів захисту інформації.

В підрозділі наведено вимоги щодо забезпечення захисту персональних даних в автоматизованих ІСПДн Університету відповідно до постанови КМ України [11].

Організація та порядок проведення робіт із створення комплексної системи захисту інформації в автоматизованих ІСПДн Університету повинні здійснюватися відповідно до вимог НД ТЗІ 3.7-003-05 [13].

Порядок створення КСЗІ в автоматизованих ІСПДн є єдиним незалежно від того, створюється КСЗІ в системі, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту персональних даних або модернізації вже створеної КСЗІ.

Обробка персональних даних в автоматизованих ІСПДн дозволяється тільки після завершення робіт з створення КСЗІ, проведення випробувань та оцінки рівня захищеності інформації на відповідність вимогам нормативних документів системи ТЗІ, за результатами якої Держспецзв'язком або уповноважені ним органи надають атестат відповідності.

Дозвіл на експлуатацію автоматизованої ІСПДн надається наказом ректора Університету на підставі атестату відповідності та отримання документу про реєстрацію баз персональних даних у державному реєстрі Державної служби з питань захисту персональних даних.

Вибір і реалізація методів і способів захисту інформації в автоматизованих ІСПДн здійснюються на основі визначених загроз безпеки персональних даних (моделі загроз) і в залежності від категорії персональних даних, класу інформаційної системи, визначених відповідно до порядку, встановленого нормативними документами Державної служби з питань захисту персональних даних і Держспецзв'язку України.

В КСЗІ автоматизованої ІСПДн в залежності від класу системи та виходячи із загроз безпеки персональним даним, структури системи, наявності міжмережевої взаємодії і режимів обробки персональних даних з використанням відповідних методів і способів захисту інформації від несанкціонованого доступу повинні реалізовуватися функції управління доступом, реєстрації та обліку, забезпечення цілісності, аналізу захищеності, забезпечення безпечної міжмережевої взаємодії і виявлення вторгнень.

Також в підрозділі наведено основні методи і способи захисту персональних даних від несанкціонованого доступу в локальних автоматизованих ІСПДн та систем, які мають підключення до телекомунікаційних мереж загального користування, відомчих або інформаційних систем загального доступу (в т.ч. Internet).

Підрозділ *"Захист персональних даних в картотеках персональних даних"* встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в картотеках персональних даних.

В інших розділах Положення визначені:

– організація контролю за додержанням законодавства у сфері захисту персональних даних;

– порядок взаємодії з Державною службою з питань захисту персональних даних;

– відповідальність за порушення законодавства про захист персональних даних;

– порядок та джерела фінансування робіт із захисту персональних даних;

– положення та вимоги при міжнародному співробітництві відповідно до закону [6].

Список літератури: 1. *Конвенція* №108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних.– Страсбург, 28.01.2001 р. Офіційний переклад. (ратифікована Законом України №2438-VI від 06.07.2010 р.). 2. *Додатковий* протокол до Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних.– Страсбург, 08.11.2001 р. Офіційний переклад. (протокол ратифіковано Законом України № 2438-VI від 06.07.2010р.). 3. *Директива* 95/46/ЕС Європейського Парламенту та Ради Європи від 24.10.1995р. "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних". 4. *Директива* 2002/58/ЄС Європейського парламенту та Ради від 12.07.2002 р. "Про обробку персональних даних та захист таємниці сектора електронних комунікацій (директива про секретність та електронні комунікації). Офіційний переклад Мін'юсту України. 5. *Директива* 2006/24/ЕС Європейського парламенту та Ради Європи від 15.03.2006 р. "Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та внесення поправок в Директиву 2002/58/ЄС". 6. *Закон* України "Про захист персональних даних". 7. *Конституція* України (із змінами). 8. *Цивільний* кодекс України (із змінами). 9. *Закон* України "Про інформацію" (із змінами). 10. *Закон* України "Про захист інформації в інформаційно-телекомунікаційних системах" (із змінами). 11. *Постанова* Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 р. №373. 12. *Кримінальний* кодекс України (із змінами). 13. *НД ТЗІ 3.7-003-05* Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 12.08.2011