Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

68-ма
науково-технічна конференція
професорсько-викладацького складу,
науковців, аспірантів та студентів

Матеріали конференції
(4 – 6 грудня 2013 р.)

Частина ІІІ

СЕКЦІЯ 3
СУЧАСНІ ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ

СЕКЦІЯ 4
ІНФОРМАЦІЙНА БЕЗПЕКА

Одеса 2013

СЕКЦІЯ 4. ІНФОРМАЦІЙНА БЕЗПЕКА

Дрейс Ю.О., Дейсан А.О., Беляк Д.Ю.
Житомирський військовий інститут ім. С.П.Корольова
Державного університету телекомунікацій

ПІДХІД ДО АНАЛІЗУ І ОЦІНКИ РИЗИКІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ДЕРЖАВНИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ

Анотація. Запропоновано підхід до аналізу і оцінки ризиків захисту персональних даних у базах персональних даних, що створюються і обробляються прикладним програмним забезпеченням в державних автоматизованих системах як спосіб формування стандартного профілю захищеності з визначеним набором функціональних послуг та базовим рівнем гарантій.

Актуальність та новизна. З огляду останніх подій, а саме факту несанкціонованого втручання в роботу автоматизованих систем (АС) Міністерства юстиції України через блокування інформації і порушення встановленого порядку її маршрутизації, що призвело до припинення функціонування 12 Державних та Єдиних реєстрів інформаційної мережі [1], виникають питання до належного та гарантованого захисту окремих державних інформаційних ресурсів. Це стосується саме тих ресурсів, які містять дані про фізичних осіб, що обробляються без їх згоди в інтересах національної безпеки, економічного добробуту та прав людини [2], тобто, персональних даних (ПД) (відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована) розпорядником яких є держава. Визначено [2, 3], що ПД, крім знеособлених, за режимом доступу є інформацією з обмеженим доступом, а саме конфіденційною інформацією (КІ) (доступ до якої обмежено її власником). Тому держава, як розпорядник ПД якому за законом [2, 3] надано право обробляти ці дані від імені володільця, повинна не тільки визначати склад цих ПД, мету і процедуру їх обробки, але й забезпечувати захист такої КІ у власних системах [4].

Постановка задачі. Відповідно до вимог [4] захист державних інформаційних ресурсів (у тому числі і КІ, яка містить ПД), що обробляються в АС, повинен відбуватися із застосуванням комплексної системи захисту інформації (КСЗІ). Базовим етапом її побудови є створення політики безпеки, методологія якої включає [5]: розробку концепції інформаційної безпеки в АС, аналіз ризиків; визначення вимог до заходів, методів та засобів захисту; вибір основних рішень для забезпечення інформаційної безпеки; організацію виконання відновлювальних робіт і забезпечення безперебійного функціонування АС; оформлення політики безпеки. Для аналізу ризиків необхідно [5]: визначити базові складові АС та

скласти реєстр ресурсів, що циркулюють і враховуються при аналізі; ідентифікувати загрози об'єктам захисту; оцінити ризики та величину можливих збитків пов'язаних з реалізацією загроз; визначити варіанти і витрати на побудову КСЗІ. Тому, аналіз і оцінка ризиків захисту ПД при розробці КСЗІ для державних АС, де циркулює КІ (така як ПД), що обробляється у базах ПД (БПД) в інтересах визначених законодавством є актуальним науковим завданням.

Виклад основного матеріалу. На сьогодні існує багато засобів, що використовуються для аналізу і оцінки ризиків, основаних на положеннях нормативних документів (стандартів, методик [5]) і реалізованих прикладними програмними рішеннями. Слід відмітити, що в основному для аналізу і оцінки ризиків використовують статистичні дані про інциденти та загрози інформаційної безпеки. Однак в багатьох країнах (у тому числі і в Україні) відсутня відповідна державна політика відносно застосування такої статистичної інформації, особливо щодо порушень у сфері захисту ПД у БПД, що обробляються в АС. Наразі ведеться лише практика державної реєстрації БПД [2] та встановлено типовий (мінімальний) перелік робіт (Типовий порядок [6]), які необхідно реалізувати володільцю ПД під час організації заходів, зокрема, із захисту ПД. Цей Типовий порядок [6] передбачає застосування ІТС/АС мережевого захисту від несанкціонованого доступу під час обробки ПД (міжмережеві екрани, системи виявлення втручань, засоби створення VPN, засоби оцінки захищеності) [7], впровадження процедур авторизації користувачів, забезпечення антивірусного захисту, а також використання технічних засобів безперебійного живлення елементів АС, яка здійснює обробку ПД. Остаточний вибір конкретних заходів захисту, технічних рішень та стандартів, якими необхідно керуватися, архітектури ІТС та АС залишається в межах компетенції володільця ПД разом з безпосередньою оцінкою ризиків порушень безпеки даних, тобто захисту ПД. Слід зазначити, що Типовим порядком [6] взагалі не передбачається застосування засобів захисту ПД при її обробці у БПД в АС. Це, на нашу думку, суперечить існуючим вимогам нормативно-правового забезпечення (статей 8 та 9 [4]) щодо умов обробки та захисту інформації, що є власністю держави, або інформації з обмеженим доступом в системах, а також наукового обґрунтування (табл.1 [8]) варіантів застосування атестованої КСЗІ за показниками {форма _власності, режим_доступу}.

Таблиця 1

		Режим доступу	
		відкрита інформація	інформація з обмеженим доступом
Форма власності	державна	атестовану КСЗІ треба застосовувати завжди	атестовану КСЗІ треба застосовувати завжди
	недержавна (приватна)	застосування атестованої КСЗІ не вимагається	атестовану КСЗІ треба застосовувати тільки тоді, коли захисту цієї інформації вимагає закон

Тому, запропоновано базовий підхід до аналізу і оцінки ризиків захисту ПД у БПД (на етапі проектуванні КСЗІ – розробки політики безпеки), що створюється і обробляється прикладним програмним забезпеченням в державних АС. Підхід має стандартну типову структуру і реалізується виконанням наступних 6 етапів:

Етап 1. Ідентифікація складу і змісту ПД, мети та засобів обробки БПД в АС.

До складу і змісту ПД відносяться: прізвище, ім'я, по батькові; дата і місце народження; відомості про освіту; ідентифікаційний код; відомості з військового квитка, водійських прав, свідоцтва про народження (одруження тощо) та інші дані (видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе).

До засобів обробки БПД в АС відносяться такі прикладні програмні продукти як: 1С, «Парус», «Кадри», «Працівники», а також MS Excel, MS Word, MS Access та ін.

Метою обробки ПД у БПД, наприклад «Працівники», є: 1) забезпечення реалізації трудових, соціально-трудових відносин, відносин у сфері управління персоналом,

військового обліку; адміністративно-правових відносин; відносин у сфері бухгалтерського і податкового обліку; 2) забезпечення національної безпеки, економічного добробуту та прав людини; захист прав і свобод фізичних осіб, ПД яких обробляються, чи прав інших суб'єктів відносин, пов'язаних із ПД, а також з метою боротьби із злочинністю; забезпечення суб'єктів відносин, пов'язаних із ПД, зведеною знеособленою інформацією щодо ПД згідно закону.

Етап 2. Аудит застосованих механізмів безпеки, а саме: 1) наявність згоди суб'єкта ПД на обробку ПД в АС; 2) ідентифіковано володільця чи розпорядника БПД, третю особу (місце знаходження, форма власності тощо) та встановлено Типовий порядку обробки ПД у БПД; 3) отримано Свідоцтво про реєстрації БПД уповноваженим органом з питань захисту ПД у Державному реєстрі БПД; 4) призначено відповідальну особу за обробку та захист ПД або створено службу захисту інформації (з обов'язками захисту ПД); 5) застосовано систему управління (менеджменту) інформаційною безпекою або атестовану КСЗІ з реалізованим стандартним профілем х.КЦ.х, х.КД.х, х.КЦД.х (за довідковим додатком А., п.А.1 [9]). Встановити наявності функціональних послуг критеріїв [9]: конфіденційності {КА, КВ}, цілісності {ЦА, ЦВ}, доступності {ДС}, спостережності {НР, НИ, НО, НВ, НА, НП, НК}.

Етап 3. Визначення загроз захисту ПД при обробці БПД в АС. Перелік можливих загроз визначається існуючими методиками аналізу і оцінки ризиків інформаційної безпеки [5] і може доповнюватись самостійно.

До типових загроз захисту ПД, БПД та АС відносяться: несанкціонований доступ (збирання, видалення, пошкодження, модифікація, поширення тощо); блокування інформації і порушення встановленого порядку її маршрутизації; збій у роботі обладнання та внутрішня відмова АС; неналежна передача ПД третій особі; інші можливі загрози.

Етап 4. Визначення величини можливого збитку від втрати ПД (чи БПД в АС). Величина нанесених збитків може визначатися як кількісними так і якісними показниками, оцінка яких проводиться за існуючих шкалами відомих методик [5], що характеризують матеріальну чи моральну шкоду, шкоду національній безпеці, порушення прав людини тощо.

Етап 5. Оцінка ризиків захисту ПД. Визначається як функція ймовірності реалізації певної загрози до виду і величини завданих збитків (шкоди) при наявності вразливостей та ступеню їх прийнятності для експлуатації АС. Ризик є величиною кількісною або якісною.

Етап 6. Керування ризиком та досягнення необхідного рівня гарантій захисту ПД. Переглядається сукупність заходів, що проводяться протягом всього життєвого циклу АС щодо оцінки ризику, вибору, реалізації і впровадження заходів (механізмів) захисту ПД, БПД та АС, що спрямовані на досягнення прийнятного рівня залишкового ризику. Проводиться необхідне інформування про можливість втрати ПД уповноваженому державному органу з питань захисту ПД. Вживаються додаткові методи забезпечення захисту ПД (обов'язкові чи вибіркові), засоби технічного та криптографічного захисту інформації (шифрування даних) для досягнення міри впевненості, що АС коректно реалізує політику безпеки.

Висновок. Запропоновано базовий підхід до аналізу і оцінки ризиків захисту ПД як етапу побудови КСЗІ при необхідному її застосуванні в державних АС, де циркулює інформація з обмеженим доступом – конфіденційна інформація (персональні дані).

Список літератури:

1. Повідомлення для ЗМІ від 4.10.2013 / Прес-центр СБ України, офіційний сайт // [Режим доступу]: http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=120192&cat_id=120209

2. Про захист персональних даних / Верховна Рада України; Закон від 01.06.2010 № 2297-VI {редакція від 09.06.2013} // [Електронний ресурс. – Режим доступу]: http://zakon4.rada.gov.ua/laws/show/2297-17/page

3. Про доступ до публічної інформації / Верховна Рада України; Закон від 13.01.2011 № 2939-VI {редакція від 09.06.2013} // [Електронний ресурс. – Режим доступу]: http://zakon4.rada.gov.ua/laws/show/2939-17#n87

4. Про захист інформації в інформаційно-телекомунікаційних системах / Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР {редакція від 30.04.2009} // [Електронний ресурс. – Режим доступу]: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Анализ и оценивание рисков информационной безопасности / [Корченко А.Г., Архипов А.Е., Казмирчук С.В.]. – К.: ООО «Лазурит-Полиграф», 2013. – 275с.

6. Про затвердження Типового порядку обробки персональних даних у базах персональних даних / Мін'юст України; Наказ, Порядок від 30.12.2011 № 3659/5 {редакція від 09.08.2013} // [Електронний ресурс. – Режим доступу]: http://zakon4.rada.gov.ua/laws/show/z0001-12/paran46#n46

7. Мервінський О. Деякі практичні аспекти реалізації заходів захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах / О. Мервінський, М. Щербак // «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», сайт науково-технічного збірника НТУУ «КПІ», Випуск – 25, 2013 // [Електронний ресурс. – Режим доступу]: http://pnzzi.kpi.ua/25/25_p33.pdf

8. Аналіз імперативності норм застосування комплексних систем захисту інформації в системах, що обробляють відкриту інформацію, яка є власністю держави / В.В. Мохор, О.О. Бакалинський, О.М. Богданов // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України. – К.: ІПМЕ ім. Г.Є.Пухова НАН України, 2009. – Вип.52 // [Електронний ресурс. – Режим доступу]: http://archive.nbuv.gov.ua/portal/natural/znpipm/2010_52/20.pdf

9. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформаційних від несанкціонованого доступу / НД ТЗІ 2.5-005-99 // [Електронний ресурс. – Режим доступу]: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id=89734