УДК 621.96 (043.2)

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Сергій Філоненко, Валеріан Швець, Ігор Мужик

Обробка персональних даних, яка є обов'язковою для будь-якої установи чи організації, потребує впровадження інформаційних систем обробки персональних даних і, безумовно, їх захисту. Існуючі методи та методики захисту інформації, в переважній більшості, орієнтовані на захист ресурсів корпоративних інформаційних систем. Такі методики не завжди враховують особливі вимоги до даних, що обробляються. Це в повній мірі стосується обробки персональних даних, захист яких передбачений чинним законодавством Розглянуто підходи до захисту персональних даних, які обробляються в автоматизованих інформаційних системах. Наведено класифікацію загроз персональним даним, які можуть виникати при їх обробці в автоматизованих системах. Розглянуто цілі та методи мінімізації таких загроз з урахуванням комплексних заходів захисту персональних даних. Запропоновано шляхи та засоби реалізації методів захисту персональних даних. Визначено пріоритети формування загальної системи захисту персональних даних.

Ключові слова: *персональні дані, захист інформації, інформаційна безпека, інформаційна система обробки персональних даних, захист персональних даних, загрози персональним даним.*

Постановка проблеми. Інформаційні технології мають широке застосування при обробці даних, а також при їх обміні між різними користувачами. Такі процеси охоплюють не тільки окрему організацію або її структури, які виступають у вигляді внутрішніх користувачів, але й зовнішніх користувачів. За таких умов, з урахуванням все більш широкого використання інформаційних технологій, виникають проблеми захисту інформаційних ресурсів, включаючи і дані, що обробляються або передаються. Тому питанням інформаційної безпеки приділяється значна увага.

Безпека інформаційних ресурсів охоплює низку питань, які пов'язані з організаційними заходами, захистом від зовнішніх загроз, захистом від витоку конфіденційної інформації тощо. Слід відмітити, що більшість інформаційних систем безпеки спрямовані на захист від зовнішніх загроз та захист від витоку конфіденційної інформації. Такі системи використовують різні методи захисту, зокрема фільтрацію інформації з аналізом контенту для попередження небажаного розголошення конфіденційної інформації за рахунок публікації файлів, відправки листів, передачі файлів по мережі тощо. Однак, як показують результати досліджень різних центрів [1-5], що працюють у галузі інформаційної безпеки, значна кількість інцидентів, пов'язаних з порушенням інформаційної безпеки, викликана внутрішніми загрозами. Джерелом таких загроз є легальні користувачі інформаційних систем.

Проблема захисту інформаційних ресурсів особливо важлива з точки зору захисту персональних даних. Такий захист передбачає мінімізацію втрат, які виникають при реалізації загроз безпеки персональним даним з відповідними наслідками – фізичної, матеріальної та фінансової шкоди суб'єкту персональних даних. Тому в останній час питанням захисту персональних даних приділяється значна увага у багатьох країнах світу.

Перш за все, це стосується питань розробки систем захисту таких даних, як низки заходів забезпечення захисту персональних даних. У цих питаннях важливе місце займають технічні методи, які повинні включати програмні, апаратні або апаратно-програмні засоби, що виконують функції захисту інформації. Вони повинні будуватися, з урахуванням концепцій захисту персональних даних, відповідно до їх структури, моделей загроз безпеки персональним даним, методів обробки, аналізу і управління даними, структури баз даних тощо. Іншими словами, проблема захисту персональних даних передбачає виконання комплексу організаційних і технічних заходів, що формують структуру системи захисту персональних даних, і які реалізуються у рамках створюваної системи.

Аналіз останніх досліджень. Загрози інформаційній безпеці за своєю актуальністю посідають друге місце серед основних загроз бізнесу, таких як економічна нестабільність, промисловий шпіонаж, викрадення інтелектуальної власності, нанесення шкоди репутації, тощо. Встановлено, що питання внутрішньої безпеки інформаційних систем, зокрема і питання неконтрольованого поширення даних, на поточний час є актуальними [1, 2, 3]. Це викликано стабільно зростаючою кількістю зафіксованих випадків витоку інформації у всіх країнах світу. При цьому 70-90% даних, що втрачаються, складають персональні дані, третина з яких втрачається мережевим шляхом. Приблизно однакові частки втрати персональних даних спостерігаються як за рахунок навмисних дій співробітників компаній, так і через їх необережність.

Серед загроз в інформаційній безпеці виділяють дві групи загроз: внутрішні та зовнішні [1]. До зовнішніх загроз відносять загрози, які виникають та якими керують за межами інформаційних систем (ІС), відносно ресурсів яких вони спрямовані. З точки зору захисту інформації та інформаційних ресурсів перевага приділяється зовнішнім загрозам, тобто боротьбі із зовнішніми загрозами. Практично на усіх підприємствах використовуються програмні та апаратні засоби захисту, які призначені для боротьби із зовнішніми загрозами і досить ефективно їм протистоять. Наприклад, антивірусні та антиспамові системи, системи контролю доступу та між мережеві екрани, IDS/IPS системи тощо.

У той же час, як показують дослідження [4], за останні роки відбувається зростання витоку інформації за межі захищених ІС. Обсяг такої інформації (даних) постійно зростає. Тому питанням захисту інформації від витоку і впровадженню відповідних засобів і систем приділяється все більша увага. Відома класифікація таких систем з поділом на чотири класи. До них відносяться системи моніторингу та аудиту, системи аутентифікації, засоби шифрування та системи виявлення і попередження витоку інформації.

При проведенні класифікації ІС враховується низка вихідних даних: категорія оброблюваної в ІС інформації (даних), обсяг оброблюваної інформації, задані оператором характеристики безпеки інформації або інформаційних ресурсів, структура необхідної ІС, наявність підключень ІС до мереж зв'язку загального користування або до мереж міжнародного інформаційного обміну, необхідні режими обробки інформації, місцезнаходження технічних засобів ІС тощо. В загальному випадку ІС, що обробляють дані, поділяють на типові й спеціальні. У типових ІС потрібно забезпечити тільки конфіденційність інформації, а в спеціальних – хоча б одну з додаткових функцій безпеки даних – захищеність від знищення, зміни, копіювання тощо.

Існують також інші програмно-апаратні засоби захисту інформації від її витоку, які не можна безпосередньо віднести до наведених вище. Наприклад, засоби блокування зовнішніх носіїв інформації. Такі системи не можуть розпізнавати інформацію за категоріями, не відрізняють інформацію обмеженого поширення від загальної і є реалізацією окремих функцій наведених систем захисту інформації. На сьогоднішній день лише системи виявлення та попередження витоків інформації, так звані DLP-системи, мають найбільше поширення. Вони використовуються для запобігання витоку інформації за межі захищеного простору ІС в реальному масштабі часу на основі фільтрації даних або зовнішніх атрибутів, які супроводжують процес переміщення даних. З даної точки зору можна виділити ряд рішень, наприклад, InfoWatch Traffic Monitor Enterprise, для контролю різних каналів витоку даних [5]; Oracle Information Rights Management, для забезпечення захисту обміну документами [6]. У даних системах також використовуються певні рішення і вони мають певну спрямованість з точки зору захисту даних.

Ключовою функцією DLP-систем є автоматичне виявлення в інформаційних потоках даних обмеженого поширення з використанням спеціальних алгоритмів. Ефективність їх роботи, в першу чергу, залежить від якості виявлення заданої до пошуку інформації в загальному потоці даних. Тому саме методи та алгоритми аналізу інформації є ключовими у роботі подібних систем. Для цього використовуються різні методи, технології та алгоритми. Однак, слід відмітити, в загальному випадку аналіз інформації у таких системах стосується блоків або шаблонів. У той же час, важливим є аналіз інформації, що обробляється в цілому. Це особливо стосується персональних даних (ПД).

Клас спеціальних систем захисту інформації визначають на основі формування моделі загроз, що виникають. Базова модель таких загроз безпеці інформації при її обробці в ІС, як правило, містить єдині вихідні дані, які стосуються призначення самої системи захисту. Наприклад, запобігання перехоплення даних, які передаються по технічних каналах з метою їх копіювання або неправомірного поширення, запобігання несанкціонованого доступу до даних, запобігання деструктивного впливу на інформаційні ресурси ІС тощо. Вихідні данні для визначення актуальних загроз формуються на основі переліку джерел таких загроз, уразливих ланок ІС, переліку технічних каналів витоку інформації тощо. Порядок визначення актуальних загроз безпеці інформації і інформаційним ресурсам передбачає виконання низькі етапів. Наприклад, проведення оцінки рівня вихідної захищеності ІС на основі опитування та аналізу, тобто визначення рівня захищеності – високий, середній, низький; проведення експертної оцінки частоти або імовірності реалізації загроз інформаційної безпеки – малоймовірна, низька, середня, висока; визначення переліку актуальних загроз з застосуванням визначених алгоритмів тощо.

При цьому проводиться і аналіз засобів захисту інформації, включаючи аналіз: шлюзів VPN; антивірусних засобів захисту; засобів виявлення атак IDP/IPS; міжмережевих екранів і систем захисту від витоку конфіденційної інформації тощо. Додатково проводиться аналіз безпеки мережевої інфраструктури: комутаторів; маршрутизаторів; мереж SAN і WLAN тощо. Перелік заходів, що проводяться, не обмежується розглянутими, включаючи і застосування існуючих систем, наприклад, DLP-систем, для вирішення конкретної задачі захисту інформації та інформаційних ресурсів, з урахуванням типу оброблюваних даних. Як видно, при розробці систем захисту інформації і інформаційних ресурсів реалізуються певні підходи. Однак, у кінцевому підсумку, ефективність систем захисту інформації визначається застосованими алгоритмами її обробки та аналізу з отриманням відповідного результату.

Це в повній мірі відносить і до захисту ПД, які мають визначені особливості, тобто поняття ПД може стосуватися не блоку інформації, а окремих визначень. Для даних такого типу важливим є формування концептуального підходу з визначенням заходів, які необхідно реалізувати при формуванні системи захисту ПД.

Задачі дослідження. У роботі буде розглянуто підходи до захисту персональних даних, які обробляються в інформаційних системах обробки персональних даних. Буде показано, що такі системи повинні входити до складу корпоративних інформаційних систем. Буде наведено класифікацію загроз персональним даним, які можуть виникати при їх обробці в автоматизованих системах, розглянуто цілі та методи мінімізації таких загроз. Буде запропоновано засоби та шляхи впровадження методів захисту персональних даних та розглянуто завдання, які необхідно реалізувати для їх захисту при формуванні та створенні інформаційних систем обробки персональних даних. Буде показано, що попередження несанкціонованого витоку персональних даних мережевими каналами потребує впровадження спеціальних систем виявлення та блокування таких пересилок мережевими каналами.

Особливістю інформації, яка циркулює в інформаційних системах обробки персональних даних (ІСОПД), є її конфіденційність. У відповідності до Закону України "Про захист персональних даних" [7] оператори, які обробляють персональні дані (ПД), зобов'язані вживати необхідних та достатніх заходів щодо обмеження несанкціонованого доступу до ПД, збереження їх цілісності та попередження неконтрольованого поширення. Тому однією з головних задач при роботі ІСОПД є забезпечення та підтримка визначеного рівня інформаційної безпеки їх ресурсів. Рівень безпеки таких систем, згідно [8, 9], визначається ступенем захисту інформації від несанкціонованого доступу до неї, а також захищеністю від втрати та спотворення даних, що обробляються. При цьому забезпечення необхідного рівня безпеки ІСОПД включає комплекс організаційно-технічних заходів, які виключать або суттєво мінімізують можливість несанкціонованого поширення інформації, спотворення або знищення даних.

За своєю структурою ІСОПД є локальними інформаційними системами, до складу яких входять технічні та програмні засоби, які використовуються для обробки ПД. Такі системи не можуть бути відокремлені від корпоративних інформаційних систем (КІС), а повинні бути їх складовою частиною. Це обумовлено рядом причин. По перше, КІС спрямовані на обробку і передачу інформації з об'єднанням всіх структур (підрозділів, служб тощо) її власника в єдиний інформаційних простір. По друге, відокремлення ІСОПД від КІС ускладнює як технічну, так програмну реалізацію процесів обробки інформації. По третє, суттєво збільшуються матеріальні витрати на утримання систем обробки інформації. У випадку відокремлення ІСОПД від КІС виключається можливість спільного використання для обробки ПД апаратних та програмних засобів, а також каналів передачі даних, включених до складу КІС.

У загальному випадку КІС представляє собою територіально розподілений комплекс програмно-технічних засобів (рис. 1), розміщених на усіх рівнях управління структурою установи та об'єднаних між собою каналами передачі даних. До складу таких систем можуть входити локальні інформаційні системи корпоративного центру, територіально рознесених філіалів, в тому числі і закордонних. У своєму складі вони можуть мати зовнішні інформаційні системи. Наприклад, інформаційні системи організацій-партнерів, які мають доступ до інформаційних або технічних ресурсів КІС. Окремі елементи (робочі місця системи) можуть бути мобільними, у тому числі і такими, де буде проводитись обробка даних і, зокрема, персональних.

Для підтримки процесу обробки інформації та забезпечення обміну даними між елементами КІС використовуються канали передачі даних. Такі канали можуть бути захищеними або не захищеними від несанкціонованого доступу до даних, що ними передаються. При цьому мережеві канали передачі

даних можуть бути такими, що контролюються оператором, тобто є власністю або обслуговуються силами установи, власника КІС. Мережеві канали також можуть обслуговуватися іншими установами, тобто використовуються для забезпечення роботи КІС на умовах оренди.

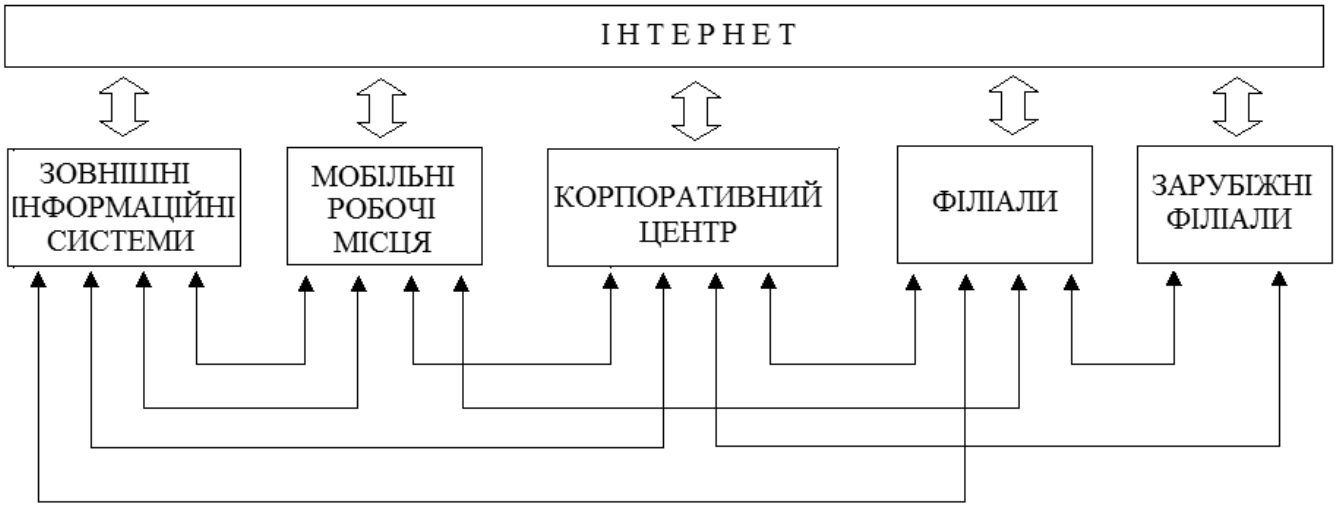

Рис. 1. Структура організації корпоративної інформаційної мережі

З огляду на економічну доцільність, досить часто для обміну інформацією між елементами КІС використовуються системи передачі даних загального користування, наприклад, інтернет. У цьому випадку, використання таких каналів суттєво знижує захищеність даних, що обробляються КІС. До таких даних, безумовно, має доступ широке коло користувачів. При цьому практично відсутні гарантії щодо безпеки передачі даних через мережу Інтернет. Тому питання використання таких каналів і забезпечення рівня захищеності даних, включаючи і ПД, є проблемою структур, які забезпечують роботу КІС, тобто є проблемою організацій, установ тощо.

Виходячи з структури КІС, з урахуванням структури їх програмних і технічних засобів у випадку обробки даних можливо виділити наступні загрози інформаційній безпеці (рис. 2):

Загрози, які пов'язані з перехопленням даних у каналах передачі інформації. Такі загрози можуть бути спрямовані на обмеження передачі інформації, її спотворення, копіювання, неправомірне поширення чи не законне використання.

Загрози, які пов'язані з несанкціонованим, у тому числі і випадковим, доступом до ресурсів КІС. Такі загрози можуть бути спрямовані на знищення, спотворення, копіювання чи неправомірне поширення даних. Крім того такі загрози можуть мати деструктивний вплив на елементи самої КІС.

Загрози, які пов'язані з несанкціонованим, навмисним чи випадковим, поширенням даних легальними користувачами КІС через мережеві канали, у тому числі і відкриті канали передачі даних. Такі загрози можуть бути спрямовані на копіювання, неправомірне поширення даних чи не законне їх використання.

Загрози, які пов'язані з втратою мобільних засобів збереження чи обробки інформації. Такі загрози можуть бути спрямовані на знищення, спотворення, копіювання чи неправомірне поширення даних.

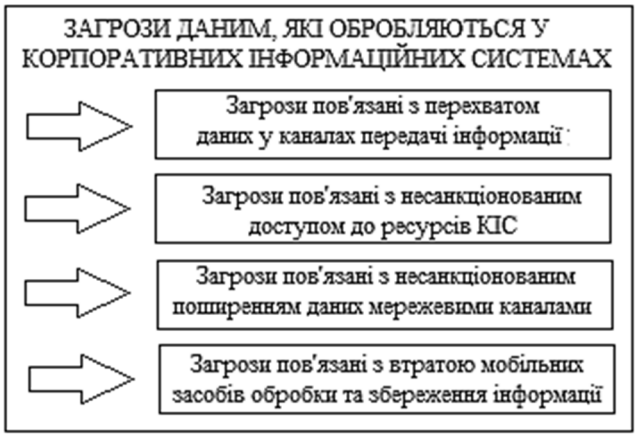

Рис. 2. Загрози даним, які обробляються в КІС

Згідно наведеної класифікації загроз, порушниками інформаційної безпеки, у тому числі і безпеки ПД, можуть бути як фізичні особи, так і організації. У залежності від прав доступу до ресурсів КІС порушник може бути зовнішнім або внутрішнім, який безпосередньо або за допомогою технічних чи програмних засобів намагається отримати доступ до інформації (інформаційних ресурсів). Порушниками інформаційної безпеки можуть бути і легальні, зареєстровані у системі, користувачі, які внаслідок умисних або необережних дій

створюють загрози інформаційній безпеці. Мотивами їх дій можуть бути помста, отримання матеріальної винагороди, хуліганські дії, самоствердження тощо. За результатами дій таких порушників, як ненавмисних так і свідомих, може бути порушена інформаційна безпека (безпека інформаційних ресурсів).

Розглянуті питання в повній мірі відносяться і до ПД. З урахуванням можливих видів загроз щодо безпеки ПД та вимог законодавства до їх обробки, у рамках КІС необхідно впроваджувати інформаційну систему, яка буде спрямована на обробку ПД, тобто ІСОПД. З метою встановлення необхідного рівня захищеності ПД розробка та впровадження таких систем потребують використання різних методів забезпечення безпеки ПД. До таких методів необхідно віднести адміністративно-правові, організаційно-технічні та економічні методи (рис. 3). Розглянемо ці методи окремо та визначимо шляхи їх застосувань для формування безпеки ПД при їх обробці у КІС, у складі якої створюється ІСОПД. При цьому необхідно врахувати, що відповідно до встановлених чинних вимог ІСОПД повинна забезпечити обробку ПД, як автономно, так і у складі інформаційно-телекомунікаційної системи із застосуванням засобів захисту даних під час їх обробки [10].

Рис. 3. Методи забезпечення безпеки ПД

До адміністративно-правових методів можна віднести норми чинного законодавства та підзаконних актів, організаційно-розпорядчі документи виконавчих та наглядових органів державної влади. Такі документи встановлюють правила обробки ПД, закріплюють права та обов'язки сторін інформаційних відносин, що виникають в процесі обробки даних. Крім того вони визначають відповідальність за порушення порядку обробки та збереження ПД. Застосування таких документів є основою для розробки відомчих правил та норм обробки ПД, які повинні бути стримуючим фактором на шляху реалізації загроз ПД потенційними порушниками. До основних напрямків застосування організаційно-правових методів захисту на рівні КІС і ІСОПД можна віднести:

– розробку та вдосконалення політики інформаційної безпеки в частині, що стосується обробки ПД, а також розробку та корегування супроводжуючих її документів;

– визначення порядку реалізації процесів обробки ПД;

– визначення персональної відповідальності за порушення норм та правил безпечної обробки ПД;

– призначення та підготовку відповідальних осіб за організацію та реалізацію процесів обробки ПД, а також заходів з забезпечення їх безпеки;

– контроль за дотриманням користувачами ІСОПД норм та правил безпечної їх обробки;

– проведення аналізу ефективності та необхідної достатності вжитих заходів щодо безпеки обробки ПД, а також розробку пропозицій щодо вдосконалення таких заходів.

Адміністративно-правові методи є основою для розробки організаційно-технічних методів захисту ПД, які повинні охоплювати всі ресурси КІС та ІСОПД: апаратні засоби обробки інформації та управління системою, канали передачі даних та канали міжсистемного управління, алгоритми обробки інформації, алгоритми управління системами та захистом інформаційних ресурсів, апаратно-програмні засоби обробки інформації та підтримки встановленого рівня інформаційної безпеки тощо. Ресурсом реалізації таких методів є апаратні, програмні та апаратно-програмні засоби ІСОПД. Впровадження організаційно-технічних методів повинно бути спрямовано на вирішення наступних задач:

– попередження несанкціонованого доступу до технічних та інформаційних ресурсів ІСОПД;

– попередження несанкціонованого поширення даних технічними каналами;

– недопущення несанкціонованого впливу на ресурси ІСОПД, результатом якого може бути знищення чи спотворення даних, пошкодження чи зміна алгоритмів обробки ПД тощо;

– своєчасне виявлення фактів несанкціонованого втручання в роботу ІСОПД;

– забезпечення можливості відновлення ПД після їх зміни чи знищення в результаті несанкціонованого доступу, а також відмов у роботі програмно-технічних ресурсів системи обробки даних;

– проведення обліку ресурсів, що підлягають захисту та контролю за дотриманням рівня захищеності ПД.

Економічні методи забезпечення безпеки ПД полягають у формуванні фінансових заходів розробки програм з забезпечення та підтримки необхідного рівня безпеки ПД, а також у розробці та впровадженні заходів заохочень і стягнень за дотримання чи порушення порядку безпечної обробки ПД.

Слід зауважити, що впровадження методів забезпечення безпеки ПД повинно носити попереджувальний характер. На рівні оператора обробки ПД методи їх захисту в ІСОПД реалізуються шляхом проведення організаційних, технічних та технологічних заходів. Організаційні заходи визначають порядок роботи персоналу з експлуатації ІСОПД та обробки даних, порядку застосування інформаційних технологій, впровадженню заходів з підтримки ІСОПД в робочому та захищеному стані, а також порядок проведення аналізу захищеності системи обробки ПД. Технічні заходи орієнтовані на управління та підтримку в робочому стані технічних засобів, які забезпечують обробку ПД та захищений режим їх аналізу. Технологічні заходи полягають у забезпеченні реалізації функцій та алгоритмів роботи ІСОПД, технологій обробки ПД та захисту ресурсів системи.

Відмітимо, що захист ПД проводиться з метою мінімізації втрат, як безпосередніх так і опосередкованих, що можуть виникнути внаслідок реалізації загроз таким даним. При формуванні єдиної системи захисту ПД в ІСОПД необхідно вирішувати низку взаємопов'язаних задач (рис. 4):

– управління доступом;

– забезпечення конфіденційності, цілісності, достовірності та доступності даних;

– забезпечення безпечного міжмережевого та міжсистемного обміну даними;

– своєчасне виявлення вторгнень та забезпечення антивірусного захисту;

– проведення аудиту та реєстрації подій, які мають місце при обробці ПД;

– контроль за переміщенням ПД за межі захищеної інформаційної системи.

У межах вирішення цих задач передбачається забезпечення доступу до інформації зареєстрованим користувачам інформаційної системи, протидіючи при цьому несанкціонованому доступу до ресурсів системи. В основу управління доступом повинно бути покладено авторизацію (ідентифікацію та аутентифікацію) суб'єкта, а також розмежування доступу.

Як відомо, до систем управління доступом входять засоби забезпечення/обмеження доступу до ІСОПД та засоби підтвердження достовірності суб'єкта, що звертається до ресурсів системи обробки ПД. Під авторизацією розуміють визначення суб'єкта (наприклад, шляхом введення імені) і перевірка достовірності пред'явлених ідентифікаційних даних (наприклад, введення паролю). Можливі і інші, більш ефективні, методи ідентифікації, наприклад, за біометричними ознаками або іншими носіями аутентифікуючої інформації. Розмежування доступу до даних та засобів ІСОПД повинно забезпечуватись виконанням алгоритмів, які

дозволять надавати доступ до ресурсів ІСОПД визначеним суб'єктам. Для забезпечення розмежування доступу необхідно встановлення несуперечливих правил доступу до інформаційних ресурсів та подальша реалізація їх на програмному рівні.

Ці правила можуть бути оформлені у вигляді матриці доступу, яка визначає відповідність суб'єктів та їх прав на виконання тих чи інших дій над ресурсами ІСОПД.

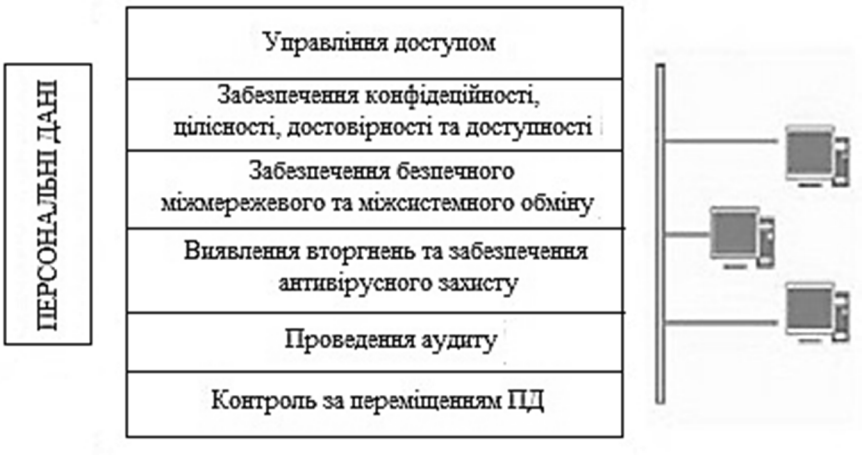

Рис. 4. Формування єдиної системи захисту ПД

З точки зору вирішення задачі обмеження доступу актуальними є заходи з фізичного захисту приміщень, об'єктів та засобів ІСОПД. Охорона, впровадження спеціального обладнання контролю доступу та правильно організований режим доступу мінімізують можливість проникнення та перебування сторонніх осіб у місцях проведення робіт з обробки ПД.

Наступною задачею є забезпечення цілісності (достовірності) як даних, так і програмного забезпечення ІСОПД, у тому числі і засобів захисту інформації. З цим завданням тісно пов'язані антивірусний захист та аудит Важливість цих складових системи захисту обумовлена тим, що довільну ІСОПД неможливо вважати абсолютно захищеною системою. У зв'язку з цим необхідно вести протоколи доступу до даних та інших подій, які мали місце у межах системи, та використовувати спеціальне програмне забезпечення, яке може своєчасно виявляти та блокувати процеси, які не передбачені у роботі системи. Крім функцій реєстрації на засоби аудиту може бути покладено виконання наступних функцій:

– накопичення інформації для розробників з метою виявлення і подальшого усунення можливих шляхів обходу систем захисту;

– збір даних для керівництва і адміністратора з безпеки про співробітників, що намагаються обійти систему захисту;

– збір даних про спроби злому системи захисту.

З останнім завданням, що вирішується системою аудиту, тісно пов'язана система блокувань і оповіщень. Мова в даному випадку йде про те, що у разі виявлення спроб несанкціонованого доступу до даних або порушення норм політики безпеки система автоматично оповіщає адміністратора з безпеки про таку подію. Крім цього, вона може в автоматичному режимі або по команді аудитора блокувати робоче місце, з якого виявлені порушення, або блокувати подальшу роботу користувача, який порушує правила безпеки. Також можливе блокування конкретних інформаційних об'єктів, якщо виявлено їх пошкодження або спотворення.

Вирішення наведених задач мінімізує загрози, пов'язані з несанкціонованим доступом до ресурсів ІСОПД, та частково загрози, пов'язані з несанкціонованим поширенням даних. У разі використання відкритих мережевих каналів передачі суттєво зростає загроза втрати та несанкціонованого поширення ПД такими каналами. Мінімізація загроз, пов'язаних з перехопленням даних у відкритих каналах передачі може проводитись шляхом кодування (шифрування) даних. З метою мінімізації загроз, пов'язаних з несанкціонованим поширенням ПД необхідно впроваджувати спеціальні системи виявлення та блокування таких даних у мережевих каналах. Проблема впровадження зазначених систем полягає у тому, що мережевими каналами ПД дані можуть передаватися легально, як необхідний елемент процедури їх обробки, так і не легально, в наслідок їх помилкової пересилки або умисних протиправних дій порушника. При цьому ПД можуть передаватися мережевими каналами як зовнішніми порушниками, які тим чи іншим шляхом проникли до системи, так і легальними, зареєстрованими у системі, користувачами.

Тому з метою мінімізації загроз, пов'язаних з несанкціонованим поширенням ПД мережеими каналами при їх обробці ІСОПД, доцільним є використання спеціальних систем виявлення таких пересилок у мережених каналах та їх блокування. При цьому зазначені системи повинні у автоматичному режимі визначати чи проводиться виявлена пересилка ПД у межах встановленого алгоритму обробки даних, чи є такою, що не передбачена встановленим процесом обробки ПД.

Висновки: Розглянуто підходи до захисту персональних даних, які повинні оброблятися в інформаційних системах. Показано, що інформаційна система обробки персональних даних повинна входити до складу корпоративної інформаційної системи. Наведено класифікацію загроз персональним даним, які можуть виникати при їх обробці в автоматизованих системах. Розглянуто цілі та методи мінімізації загроз персональним даним, що можуть виникати при обробці їх в автоматизованих інформаційних системах. До таких методів віднесено адміністративно-правові, організаційно-технічні та економічні методи. Запропоновано засоби та шляхи впровадження адміністративно-правових, організаційно-технічних методів мінімізації загроз інформаційній безпеці у інформаційних системах обробки персональних даних. Розглянуто завдання, які необхідно реалізувати для захисту персональних даних при формуванні та створенні інформаційних систем обробки персональних даних. Наведено шляхи їх вирішення для мінімізації загроз, пов'язаних з несанкціонованим доступом та несанкціонованим поширенням даних. Показано, що попередження несанкціонованого витоку персональних даних мережевими каналами потребує впровадження спеціальних систем виявлення та блокування таких пересилок мережевими каналами. Для цього необхідно розробляти алгоритми аналізу потоків даних у мережевих каналах передачі направлених на виявлення персональних даних у загальному потоці даних, визначення правомірності виявленої пересилки та обробки таких даних.

ЛІТЕРАТУРА

[1]. Исследование текущих тенденций в области информационной безопасности бизнеса, 2012. Результаты исследования. Лаборатория Касперского, Москва, 2012. http://www.kaspersky.ru/other/custom-html/brfwn/Bezopasnost_Screen.pdf

[2]. 2010/2011 Computer Crime and Security Survey. Computer Security Institute, 2012. http://gatton.uky.edu/faculty/payne/ACC324/CSISurvey2010.pdf

[3]. Global Information Security Survey. Ernst&Young. http://engweb.info/courses/ens/extra/GISS%20report_final.pdf.

[4]. Глобальное исследование утечек корпоративной информации и конфедициальных данных 2012. Аналитический центр InfoWatch, 2012. http://www.slideshare.net/malvvv/info-watch-globaldataleakagereport2012

[5]. DLP-система InfoWatch Traffic Monitor Enterprise. InfoWatch, 2012. http://www.infowatch. ru/products/traffic_monitor_enterprise.

[6]. Защита корпоративного контента на основе Information Rights Management. http://www.oraclepro.ru/download/archive/almaty-2011/almaty-04.pdf.

[7]. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI (Редакція станом на 09.06.2013).

[8]. НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" від "28" квітня 1999 р. № 22.

[9]. НД ТЗІ 1.1-002-99 "Класифікація автоматизованих систем і стандартні функціональні захищеності оброблюваної інформації від несанкціонованого доступу" від "28" квітня 1999 р. № 22.

[10]. Типовий порядок обробки персональних даних у базах персональних даних затв. наказом №3659/5 від 30.12.2011 Міністерства юстиції України.

REFERENCES

[1]. Study of Current trends in security business newsletter, 2012. Results of the study. Kaspersky Labs, 2012. http://www.kaspersky.ru/other/ custom-html/brfwn/Bezopasnost_Screen.pdf.

[2]. 2010/2011 Computer Crime and Security Survey. Computer Security Institute, 2012. http://gatton.uky.edu/faculty/payne/ACC324/CSISurvey2010.pdf

[3]. Global Information Security Survey. Ernst&Young. http://engweb.info/courses/ens/extra/GISS%20report_final.pdf.

[4]. Global Study of Leaks of Corporate Information and Confidential Data, 2012. Research Center. InfoWatch, 2012. http://www.slideshare.net/malvvv/info-watch-globaldataleakagereport2012.

[5]. DLP-system InfoWatch Traffic Monitor Enterprise. InfoWatch, 2012. http://www.infowatch.ru/products/traffic_monitor_enterprise.

[6]. Protecting corporate content-based Information Rights Management. http://www.oraclepro.ru/download/archive/almaty-2011/almaty-04.pdf.

[7]. Law of Ukraine " On Personal Data Protection " from 01.06.2010 № 2297 -VI (Edition on 09.06.2013).

[8]. TPI 1.1-002-99 "General Provisions Concerning the protection of Information from Unauthorized Access in Computer Systems" April, 28, 1999 number 22.

[9]. TPI 1.1-002-99 "Classification of Automated Systems and Standard Functional Security of Information Processed from Unauthorized Access" April, 28, 1999 № 22.

[10]. Typical Procedure for the Processing of Personal Data in the Personal Data Databases approved by Decree № 3659/5 dated 30.12.2011 Ministry of Justice of Ukraine.

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных, процесс, который есть обязательным для любого учреждения или организации, требует внедрения информационных систем обработки персональных данных и, безусловно, их защиты. Существующие методы и методики защиты информации, в подавляющем большинстве, ориентированны на защиту ресурсов корпоративных информационных систе. Такие методики не всегда учитывают особые требования к данным, которые обрабатываются. Это в полной мере касается обработки и персональных данных, защита которых предусмотрена действующим законодательством. Рассмотрены подходы к защите персональных данных, обрабатываемых в автоматизированных информационных системах. Приведена классификация угроз персональным данным, которые могут возникать при их обработке в автоматизированных системах. Рассмотрены цели и методы минимизации угроз на основе комплексных мер защиты персональных данных. Предложены пути и средства реализации методов защиты персональных данных. Определены приоритеты формирования общей системы защиты персональных данных.

Ключевые слова: персональные данные, защита информации, информационная безопасность, информационная система обработки персональных данных, защита персональных данных, угрозы персональным данным.

DATA PROTECTION IN THE PERSONAL DATA PROCESSING

Processing of personal data, which is obligatory for any institution or organization, requires implementation of personal data processing information systems and definitely their security. The majority of existing information security methods and techniques is focused on the security of corporate information systems resources. Such techniques do not always take into account the special requirements for data processing. This fully applies to the processing of personal data protection, the security of which is provided by the current legislation. Approaches to the protection of personal data processed in automated information systems were discussed. The classification of threats to personal data that may occur when processing them in automated systems was brought. We considered the aims and methods of minimizing such threats including comprehensive measures to protect personal data. The ways and means of personal protection methods of personal data were considered. The priorities of forming the overall personal data protection system were defined.

Keywords: the personal data, priv, informative safety, informative system of processing of the personal data, protection of the personal data, threat to the personal data.

Філоненко Сергій Федорович, доктор технічних наук, професор, професор кафедри інформаційних технологій Національного авіаційного університету.
E-mail: fils01@mail.ru

Филоненко Сергей Федорович, доктор технических наук, профессор, профессор кафедры информационных технологий Национального авиационного университета.

Filonenko Serhiy, Dr Habil, Professor, Department of Information Technology National Aviation University.

Швець Валеріан Анатолійович, кандидат технічних наук, доцент, завідувач кафедрою засобів захисту інформації Національного авіаційного університету.
E-mail: hvan@nau.edu.ua

Швец Валериан Анатолиевич, кандидат технических наук, доцент, заведующий кафедрой средств защиты информации Национального авиационного университета.

Shvets Valerian, Ph.D., Associate Professor, Head of Department of Information Protection of National Aviation University.

Мужик Ігор Мирославович, старший викладач кафедри засобів захисту інформації Національного авіаційного університету.
e-mail: myzhuk@mail.ru

Мужик Игорь Мирославович, старший преподаватель кафедры средств защиты информации Национального авиационного университета.

Muzhyk Igor, a senior lecturer in information security National Aviation University.