© Filonenko S., Muzhik I., Nimchenko T. Personal data leakage prevention system for network channels // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 279-285.

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY & PROTECTION FROM IDENTITY THEFT

СИСТЕМА ПОПЕРЕДЖЕННЯ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ МЕРЕЖЕВИМИ КАНАЛАМИ

Сергій Філоненко, Ігор Мужик, Тетяна Німченко

Національний авіаційний університет, Україна

ФІЛОНЕНКО Сергій Федорович, д.т.н.

Рік та місце народження: 1954 рік, м. Ечміадзін, Вірменія.
Освіта: Київський політехнічний інститут.
Посада: директор Інституту інформаційно-діагностичних систем.
Наукові інтереси: діагностика технологічних процесів та об'єктів, автоматизовані діагностичні системи.
Публікації: 250 наукових праць.
E-mail: fils01@mail.ru

МУЖИК Ігор Мирославович

Рік та місце народження: 1958 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет.
Посада: заступник директора Інституту інформаційно-діагностичних систем.
Наукові інтереси: автоматизація обробки інформації.
Публікації: 11 наукових праць.
E-mail: myzhuk@mail.ru

НІМЧЕНКО Тетяна Василівна, к.т.н.

Рік та місце народження: 1980 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет.
Посада: доцент кафедри засобів захисту інформації.
Наукові інтереси: діагностика технологічних процесів та об'єктів.
Публікації: 103 наукові праці.

Анотація. *Витік інформації, зокрема персональних даних, мережевими каналами є актуальною проблемою інформаційної безпеки. З огляду на це, у статті розглянуто методи мінімізації загроз персональним даним. Розглянуто завдання, які необхідно реалізувати для захисту персональних даних при формуванні та створенні систем захисту інформаційних ресурсів. Наведено шляхи їх вирішення з метою мінімізації загроз персональним даним. Показано, що попередження несанкціонованого витоку персональних даних мережевими каналами потребує впровадження спеціальних систем виявлення та блокування таких надсилань мережевими каналами. Створено систему виявлення та попередження витоку персональних даних мережевими каналами. В основу роботи системи покладено особливі вимоги до управління персональними даними. Застосування такого підходу дозволяє виявляти персональні дані у мережевому потоці, проводити ідентифікацію дозволених та недозволених надсилань таких даних мережевими каналами та попереджати їх несанкціоноване поширення мережевими каналами.*

Ключові слова: *персональні данні, мережеві канали, інформація, захист, системи захисту, витік інформації, система попередження витоку даних.*

Постановка задачі

Інформаційні технології мають широке застосування при обробці даних, а також їх обміні між різними користувачами. Такі процеси охоплюють не тільки окрему організацію або її структури, що виступають у вигляді внутрішніх користувачів, але й зовнішніх користувачів, які проводять обробку даних поза межами захищеної інформаційної системи (ІС). За таких умов, з урахуванням все більш широкого застосування інформаційних технологій, виникають проблеми захисту інформаційних ресурсів. Це стосується і даних, що обробляються та передаються мережевими каналами. 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 впроваджених заходів інформаційної безпеки спрямовані на захист від зовнішніх загроз, попередження несанкціонованого доступу до ресурсів ІС та захисту від витоку конфіденційної інформації. Такі системи використовують різні методи захисту, зокрема і фільтрацію інформації з аналізом контенту для виявлення небажаного розголошення конфіденційної інформації за рахунок публікації файлів, відправки листів, передачі файлів по мережі тощо. Однак, як показують результати досліджень різних центрів, що працюють у галузі інформаційної безпеки, значна кількість інцидентів, пов'язаних з порушенням інформаційної безпеки, викликана внутрішніми загрозами інформаційній безпеці. Джерелом таких загроз є програмно-апаратні засоби ІС та її легальні користувачі.

Проблема захисту інформаційних ресурсів особливо важлива з точки зору захисту персональних даних (ПД). Такий захист передбачає мінімізацію збитків, які виникають при реалізації загроз безпеці ПД. Наслідками реалізації таких загроз може бути завдання фізичної, матеріальної чи фінансової шкоди суб'єкту, до якого вони відносяться. Тому питанням захисту ПД приділяється значна увага у багатьох країнах світу. Перш за все, це стосується питань розробки систем захисту, які включають адміністративно-правові, організаційно-технічні та економічні методи забезпечення захисту таких даних. У цих питаннях важливе місце займають організаційно-технічні методи, які повинні включати програмні, апаратні або апаратно-програмні засоби, що виконують функції захисту інформації. Вони повинні будуватися з урахуванням концепцій захисту ПД, відповідно до структури даних, моделей загроз, методів обробки, аналізу та управління даними, структури баз даних тощо. Іншими словами, проблема захисту ПД передбачає виконання комплексу організаційних і технічних заходів, що формують структуру системи захисту інформації, і які реалізуються у рамках даної системи.

Аналіз останніх досліджень та публікацій

Загрози в 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 ІС, зокрема і питання неконтрольованого поширення даних, на поточний час є актуальними [1, 2]. Це викликано стабільно зростаючою кількістю зафіксованих випадків витоку конфіденційної інформації у всіх країнах світу. При цьому, за різними джерелами, від 70 до 90% даних, що втрачаються, складають ПД, третина з яких втрачається мережевим шляхом. Приблизно однакові частки втрати ПД спостерігаються як за рахунок протиправних, навмисних дій співробітників компаній, так і через їх необережність.

Серед загроз в інформаційній безпеці виділяють дві групи загроз: внутрішні та зовнішні [3]. До зовнішніх загроз відносять загрози, які виникають та якими керують за межами ІС, відносно ресурсів яких вони спрямовані. Внутрішні загрози виникають безпосередньо в межах ІС. Вони можуть надходити від технічного обладнання, недосконалих програмних засобів та персоналу. Практично на усіх підприємствах використовуються програмні і/або апаратні засоби захисту, які призначені для протидії зовнішнім загрозам і досить ефективно їм протистоять. Що стосується засобів захисту від внутрішніх загроз, то тільки незначна частина компаній їх використовує, хоча необхідність у цих засобах об'єктивно існує. В першу чергу це стосується систем попередження несанкціонованого витоку інформації. Слід відмітити, що не спостерігається широке використання подібних систем на об'єктах інформаційної діяльності, хоча певна позитивна динаміка росту їх впровадження існує. Це пов'язано, в першу чергу, з високою вартістю запропонованих на ринку систем захисту від витоку конфіденційної інформації та затратами на їх впровадження.

Однією з основних причин актуальності внутрішніх загроз інформаційній безпеці є несанкціонований виток інформації за межі захищених ІС, обсяг якої має сталу тенденцію до зростання. Мінімізувати такі загрози можна шляхом впровадження систем протидії внутрішнім загрозам інформаційній безпеці. Відомі чотири класи таких систем [4]. До них відносяться системи моніторингу та аудиту, системи аутентифікації, засоби шифрування та системи виявлення і попередження витоку інформації. Існують також інші програмно-апаратні засоби захисту інформації від внутрішніх загроз інформаційній безпеці, які не можна безпосередньо віднести до наведених вище класів. 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 від внутрішніх загроз. На сьогоднішній день лише системи виявлення та попередження витоку інформації (DLP-системи) є єдиним рішенням, яке дозволяє запобігти витоку інформації за межі

захищеного простору ІС в реальному масштабі часу. Вони будуються на основі фільтрації даних або зовнішніх атрибутів, які супроводжують процес переміщення даних.

Ключовою функцією DLP-систем є автоматичне виявлення в інформаційних потоках даних обмеженого поширення. Розроблені та впроваджені на сьогоднішній день системи попередження витоку конфіденційної інформації, наприклад, InfoWatch Traffic Monitor, RSA DLP Suite, Symantec Data Loss Prevention, Контур информационной безопастности та ряд інших успішно протидіють несанкціонованому поширенню конфіденційної інформації, у тому числі і мережевими каналами. Ефективність їх роботи, в першу чергу, залежить від якості виявлення заданої до пошуку інформації в загальному потоці даних. Тому саме методи та способи аналізу інформації є ключовими у роботі подібних систем. Реалізовані технології та алгоритми фільтрації даних визначають ефективність роботи таких систем, а також їх вартість та витрати на впровадження. Очевидно, чим ширший функціонал системи, чим вища ефективність виявлення конфіденційної інформації, тим вищими будуть її вартість та витрати на впровадження. При цьому розширення спектру даних, передбачених до аналізу, знижує ефективність фільтрації та потребує впровадження більш ефективних методів проведення аналізу даних.

Процесом управління ПД може бути передбачено залучення до їх обробки як внутрішніх так і зовнішніх операторів, у тому числі і з процедурою обміну даними між ними мережевими каналами. Досить часто ПД обробляються різними ІСОПД, що передбачає обмін даними між системами, віднесеними до різних контурів інформаційної безпеки. Тому мережевими каналами ПД можуть передаватися, як санкціоновано, у межах виконання процедури їх обробки, так і не санкціоновано, внаслідок умисних або ненавмисних дій користувачів ІС і зловмисників, які тим чи іншим шляхом отримали доступ до ресурсів ІС. Це вимагає у процесі проведення контролю за переміщенням ПД не лише виявляти їх у мережевому каналі, але і розрізняти дозволені та недозволені надсилання таких даних. Однак алгоритмами обробки даних відомих систем виявлення та попередження витоку конфіденційної інформації за межі захищених ІС не передбачено виділення дозволених та недозволених надсилань даних, які підлягають захисту. Тому наявні основні засоби забезпечення безпеки ПД, запропоновані алгоритми та системи виявлення конфіденційної інформації у мережевому потоці не можуть бути без застереження використані для попередження несанкціонованого витоку ПД за межі захищених ІС, зокрема і мережевим шляхом [5].

Враховуючи, що переважну частку даних, що втрачаються, складають ПД, а у досить широкого кола суб'єктів інформаційної діяльності до складу конфіденційної інформації входять переважно ПД, впровадження саме систем попередження витоку ПД може зацікавити операторів за умови зниження їх вартості та спрощення процедури впровадження в порівнянні з існуючими аналогами. Розробка подібних систем повинна базуватися на особливостях управління ПД, потребує удосконалення існуючих технологій фільтрації, впровадження нових методів виявлення даних у інформаційному потоці, концептуально змінюючи підходи до їх розпізнавання.

Задачі дослідження

У роботі буде розглянуто структуру системи захисту персональних даних, що обробляються в корпоративних інформаційних системах. Буде розглянутий принцип роботи такої системи. Буде показано, що до структури системи повинні входити модуль перехоплення даних, що надходять до мережевого каналу, модулі проведення контекстного та контентного аналізу, а також модуль управління персональними даними, виявленими при спробі несанкціонованого надсилання їх поза межі захищеної інформаційної системи. Будуть запропоновані підходи до принципів побудови таких модулів. Буде показано, що виявлені випадки несанкціонованих надсилань персональних даних мережевими каналами потребують впровадження спеціальних систем обробки таких даних з метою розробки рекомендацій щодо покращення рівня інформаційної безпеки систем обробки інформації.

Результати дослідження

Системи виявлення та попередження витоку конфіденційної інформації базуються на проведенні фільтрації даних методами контекстного або контентного аналізу. Відомі переваги кожного з методів, які полягають у простоті та ефективності методу контекстного аналізу та більш точному контентному аналізі даних. Можна припустити, що поєднання методів контекстної та контентної фільтрації даних може бути основою для створення ефективної системи виявлення та попередження несанкціонованого витоку ПД мережевими каналами. Очевидно, що загальний принцип роботи таких систем досить простий (рис. 1). З метою попередження несанкціонованого поширення даних мережевими каналами достатньо отримати дані, що надходять до каналу передачі інформації, виявити серед них персональні та провести їх аналіз. За результатами аналізу необхідно встановити, чи виявлене надсилання таких даних є дозволеним, передбаченим процесом їх обробки, чи є недозволеним. Подальше управління даними буде залежати від результатів аналізу. Якщо встановлено, що виявлене надсилання ПД виконується у межах встановленого порядку їх обробки, то ПД надсилаються за призначенням. У випадку виявлення спроби несанкціонованого надсилання ПД обробка даних проводиться за відповідними, наперед визначеними алгоритмами захисту інформації.

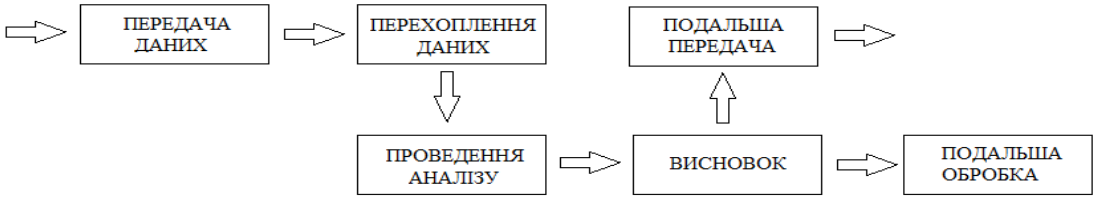

Рис. 1. Загальний принцип роботи системи виявлення та попередження витоку ПД мережевими каналами

Чинними нормативними документами встановлені особливі вимоги до процесів управління ПД при їх обробці у автоматизованих системах. Зокрема, такими документами передбачено встановлення переліку робочих місць, у тому числі і комп'ютеризованих, за якими буде проводитись обробка ПД та визначення кола співробітників, які будуть їх обробляти [6]. Встановлений порядок управління ПД не передбачає їх збереження та проведення обробки таких даних поза межами визначених у встановленому порядку об'єктів ІС. Також не передбачено залучення до їх обробки операторів, допуск яких не оформлено в установленому порядку. Тому в кожній установі, де проводиться обробка ПД, визначені об'єкти ІС, на яких проводиться обробка таких даних. Також визначено коло операторів, які такими даними можуть обмінюватись, у тому числі і таких, що обробляють ПД поза межами корпоративної ІС.

Нормативно встановлені особливості обробки ПД дають можливість змінити підходи до виявлення несанкціонованого поширення даних. Абсолютно очевидно, що ПД можуть надійти до мережевого каналу виключно з робочих місць, за якими проводиться обробка таких даних. При цьому, санкціонованими надсиланнями ПД поза межі ІС будуть лише такі, що відбуваються між операторами, участь яких передбачена в їх обробці встановленим порядком управління такими даними. Виходячи з цього швидкодіючими та ефективними методами контекстного аналізу можна виявити повідомлення, у складі яких можуть бути ПД, надсилання яких поза межі захищеного простору порушить встановлені правила їх обробки. Це будуть повідомлення, що надсилаються операторами, які проводять обробку ПД кореспондентам, участь яких в обробці таких даних не передбачена. До складу таких повідомлень можуть бути включені ПД, помилково або навмисно. Такі повідомлення потребують проведення подальшого аналізу змісту на наявність у їх складі ПД. Всі інші повідомлення можуть бути направлені за призначенням. У їх складі не буде ПД, або такі дані будуть надсилатися в порядку, встановленому правилами їх обробки.

Такий підхід до виявлення несанкціонованого надсилання ПД суттєво спростить систему захисту. Строго формалізований та вичерпний перелік даних, що підлягають захисту, дозволить застосувати прості та ефективні методи аналізу та спростити процедуру впровадження системи за рахунок автоматизації створення шаблонів контекстного пошуку та словників контентного аналізу. Відповідно до визначеної процедури обробки даних, на рис. 2 наведено структуру системи виявлення та попередження витоку ПД (СПВПД). До складу такої системи входять модулі перехоплення мережевого трафіку, контекстного аналізу та контентної фільтрації. Також до складу системи входить модуль обробки виявлених несанкціонованих надсилань ПД мережевими каналами.

Згідно наведеної структури (рис. 2), дані, що надходять до мережевого каналу з локальної інформаційної мережі, через модуль перехоплення мережевого трафіку передаються до модуля контекстного аналізу. У цьому модулі з потоку інформації виділяються дані, які у своєму складі можуть мати ПД та надсилання яких мережевими каналами порушить встановлені правила їх обробки.

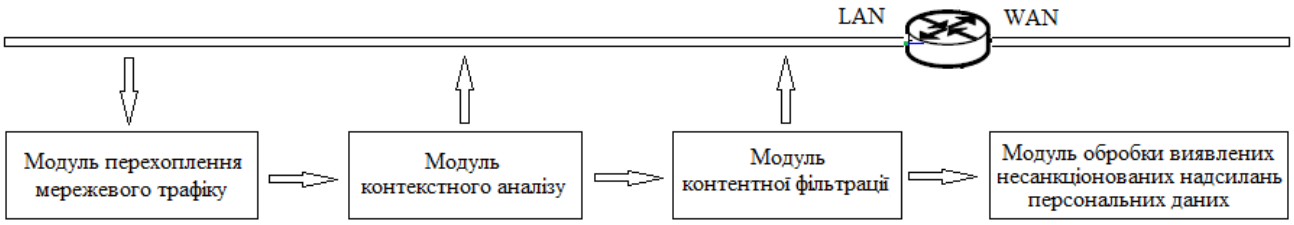

Рис. 2. Структура системи виявлення та попередження витоку персональних даних

В основу роботи модуля контекстного аналізу покладено особливі вимоги до управління ПД. Такі вимоги надають можливість з потоку даних, що надходять до мережевого каналу, виключати масиви даних, які однозначно у своєму складі не будуть мати персональних, а також виявляти повідомлення, у складі яких ПД санкціоновано, у відповідності до встановленого порядку їх обробки, надсилаються поза межі захищеної ІС. Очевидно, що дані, які надходять до мережевого каналу від об'єктів ІС на яких не проводиться обробка ПД, не можуть мати у своєму складі такі дані. У такому випадку немає потреби у проведенні подальшого їх аналізу і вони можуть бути направлені за призначенням. Критерієм, за яким доцільно проводити такий аналіз є об'єкт ІС, з якого дані направлені до мережевого каналу, а атрибутом об'єкту – його мережеві ідентифікатори. Аналіз доцільно проводити

методами контекстної фільтрації, аналізуючи атрибути транспортного пакету, у складі якого дані надходять до мережевого каналу.

Процедура обробки ПД може передбачати обмін такими даними між окремими ІСОПД, в тому числі і такими, які розміщені поза межами захищеної корпоративної інформаційної мережі. Наприклад, щомісячна звітність господарюючих суб'єктів до Пенсійного фонду про нарахування заробітної плати своїм співробітникам. Такі надсилання ПД є дозволеними та повинні бути забезпечені ресурсами ІС, в тому числі і підтримуватись ресурсами СПВПД. Виявлення таких надсилань також проводиться у модулі контекстного аналізу. Критерієм їх ідентифікації є кореспонденти, між якими відбувається обмін даними. Дозволеними будуть надсилання ПД, що відбуваються між кореспондентами, для яких процедура обміну такими даними передбачена регламентом їх обробки. Такі повідомлення повинні бути направлені за призначенням. Подальшому аналізу підлягають лише повідомлення, що надходять до мережевого каналу від об'єктів ІС, на яких проводиться обробка ПД та які направлені кореспондентам, надсилання ПД яким не передбачено процедурою обробки таких даних. Їх надсилання може порушити встановлені правила обробки ПД. Така ситуація вимагає проведення аналізу змісту повідомлень.

Для подальшої обробки такі повідомлення направляються до модуля контентної фільтрації (рис. 2). Це пов'язано з тим, що методи контекстного аналізу не є ефективними у разі їх застосування для обробки інформації, яка знаходиться у контейнері. Таку перевірку доцільно проводити методами контентного аналізу. Наприклад, за ключовими словами. При цьому, повідомлення, у яких не виявлено ПД, направляються за призначенням. Повідомлення, у складі яких виявлено несанкціоноване надсилання ПД поза межі захищеної інформаційної системи, потребують подальшої обробки за спеціальними алгоритмами захисту інформації. Така обробка проводиться у модулі обробки виявлених несанкціонованих надсилань ПД (рис. 2).

Для отримання даних, які передаються мережевим каналом, передбачено використання одного з відомих варіантів перехоплення мережевого трафіку: перенаправлення мережевого потоку за допомогою програмного фільтру, встановленого на шлюзі мережі; шляхом організації дзеркального вихідного потоку даних або з використанням окремого серверу перехоплення, включеного на виході ІС. Застосування того чи іншого способу перехоплення визначається задачами, які покладені на систему інформаційної безпеки, обраним порядком управління даними та структурою ІС. Так, при обробці даних дзеркального мережевого потоку виключається вплив системи безпеки на характеристики транспортних каналів передачі даних. Однак, при цьому виключена можливість блокування виявлених несанкціонованих надсилань ПД. Отримання даних на шлюзовому обладнанні мережі може негативно впливати на пропускну спроможність мережі. Але, такий варіант перехоплення даних може розглядатися при багатопроменевому включенні корпоративної ІС до інших мереж. При цьому може бути забезпечений, як режим моніторингу, так і режим блокування передачі даних, що надходять з порушеннями встановленого порядку управління до мережевого каналу. Варіант перехоплення даних за допомогою окремого серверу має властивості наведених варіантів. Однак, такий варіант потребує встановлення додаткового серверного обладнання. Структура модуля контекстного аналізу наведена на рис. 3.

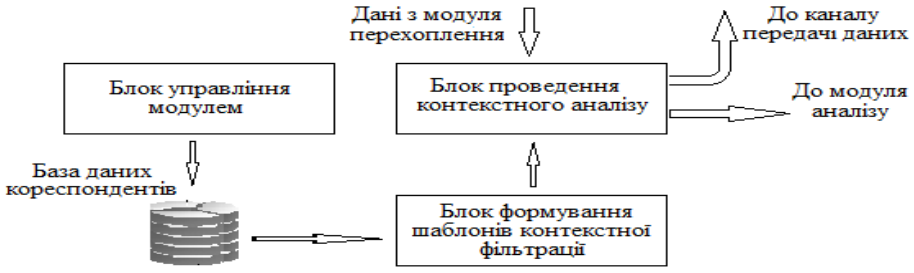

Рис. 3. Модуль контекстного аналізу

Аналіз даних проводиться блоком фільтрації, до якого вони надходять з модуля перехоплення. Процес фільтрації проводиться у два етапи. На першому етапі виділяються повідомлення, які надійшли від об'єктів ІС, де проводиться обробка ПД. На другому етапі з них виключаються повідомлення, які направляються кореспондентам поза межі ІС, яким надсилання ПД передбачено встановленим регламентом їх обробки. За результатами проведення контекстного аналізу дані розподіляються на два потоки. До одного потоку направляються дані, які у своєму складі не мають персональних, та дані, у складі яких є ПД, які направлені до мережевого потоку у відповідності до встановленого порядку їх обробки. Такі дані направляються до мережевого каналу з метою передачі їх за призначенням. До другого потоку направляються дані, які у своєму складі можуть мати ПД, надсилання яких поза межі захищеного інформаційного простору може порушити встановлені правила їх обробки. Ці дані потребують проведення подальшого аналізу.

Для забезпечення коректного проведення контекстної фільтрації даних важливим є питання формування та підтримання актуальності шаблонів контекстного аналізу. Ступінь відповідності таких

шаблонів встановленому порядку обробки ПД буде визначати якість проведення контекстної фільтрації. Для забезпечення можливості управління процесом фільтрації даних, формування та своєчасного корегування шаблонів контекстного пошуку до структури модуля контекстного аналізу включено блок формування шаблонів контекстної фільтрації (рис. 3). Такі шаблони формуються на основі даних бази операторів, що проводять обробку ПД, і є еталоном для проведення контекстного аналізу. Блок управління модулем забезпечує проведення процесів корегування інформації у базі даних операторів та формування шаблонів контекстного аналізу.

Для проведення контентного аналізу та виявлення ПД у складі документів, які направляються мережевими каналами поза межі захищеної ІС, необхідно забезпечити відновлення змісту такого повідомлення та сформувати словники контентного аналізу. У відповідності до цього на рис. 4 наведено структуру модуля контентної фільтрації.

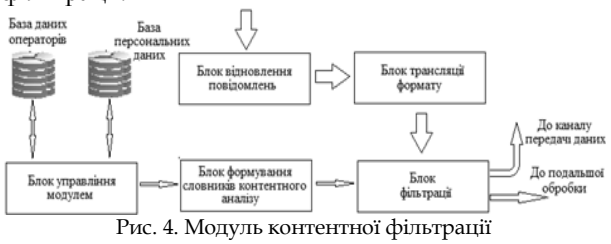

Рис. 4. Модуль контентної фільтрації

Блок відновлення повідомлень формує вихідні форми документів, що направляються зовнішнім кореспондентам з масиву даних, які надходять з модуля контекстного аналізу. Такі документи можуть мати різні форми, могли бути створені у різних форматах та з застосуванням різних типів кодуваня. У блоці трансляції формату (рис.4) виділяється та приводиться до прийнятого формату і типу кодування змістовна складова документу. Формат та тип кодування даних визначаються форматом та типом кодування, які прийняті у блоці фільтрації. Словники контентного аналізу формуються блоком формування словників контентного аналізу на основі даних, занесених до баз даних операторів та ПД. Блок управління модулем (рис.4) забезпечує формування та внесення відповідних коректив до словників контентної фільтрації при інсталяції системи, а також при зміні порядку обробки ПД або їх складу.

Процес фільтрації проводиться у два етапи. На першому етапі виділяються дозволені надсилання ПД поза межі ІС за атрибутами кореспондентів, які можуть бути включені до змістовної частини повідомлення. На другому етапі проводиться виявлення ПД у складі документів, що направлялись кореспондентам, отримання ПД якими не передбачено процедурою їх обробки. У випадку, якщо у складі документу не виявлено ПД, або надсилання таких даних проводиться у межах встановлених правил їх обробки, документ надсилається за призначенням. У випадку, якщо встановлено, що ПД надсилаються з порушенням встановлених правил управління даними, подальша їх обробка проводиться за спеціальними алгоритмами, які повинні бути передбачені у системі захисту інформації.

Висновки

Розглянуто завдання, які необхідно реалізувати для захисту персональних даних при формуванні та створенні інформаційних систем обробки персональних даних. Наведено шляхи їх вирішення з метою мінімізації загроз, пов'язаних з несанкціонованим поширенням даних мережевими каналами. Показано, що попередження несанкціонованого витоку персональних даних мережевими каналами потребує впровадження спеціальних систем виявлення та блокування таких надсилань. Створено систему виявлення та попередження витоку персональних даних мережевими каналами. В основу роботи системи покладено особливі вимоги до управління персональними даними. Застосування такого підходу дозволило суттєво спростити структуру системи захисту у порівнянні з існуючими аналогами. Запропонований алгоритм роботи системи забезпечує виявлення персональних даних, які надходять до мережевого каналу та ідентифікацію дозволених і недозволених надсилань таких даних, що особливо актуально з точки зору обробки персональних даних. Включення до складу системи модулів автоматизованого формування шаблонів контекстного пошуку та словників контентного аналізу спростить процедуру впровадження системи та забезпечить високу ефективність виявлення несанкціонованих надсилань персональних даних мережевими каналами.

Література

[1] Коржов В.В. Защита персональных данных: проблемы и пути решения [Текст] / В.В. Коржов // Открытые системы. — 2010. — №10. — С. 11.

[2] Марков А.П. Проблемы и решения по защите персональных данных в информационных системах персональных данных [Текст] / А.П. Марков, Б.И. Сухинин // Компьютерная безопасность. — Улан-Уде: ВСГТУ. — 2009. — №5. — С. 20-27.

[3] Аверченков В.И. Формализация процесса выбора состава средств обеспечения безопасности на объекте защиты/ В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин // Вестник компьютерных и информационных технологий. — 2010. — № 11. — С. 45-50.

[4] Защита персональных данных в информационных системах [Електронний ресурс]. — Режим доступу: http://www.osp.ru/lan/2008/12/5808691/

[5] Сулавко А.Е. Технологии защиты от внутренних угроз информационной безопасности / А.Е. Сулавко // Вестник СибАД., — 2011 №1 (19). — С. 45-51.

[6] Типовий порядок обробки персональних даних у базах персональних даних. Міністерство юстиції України від 30.12.2011 N 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних».

УДК 621.96 (045)

Филоненко С.Ф., Мужик И.М., Нимченко Т.В. Система предупреждения утечки персональных данных сетевыми каналами

Аннотация. *Утечка информации, в частности персональных данных, сетевыми каналами является актуальной проблемой информационной безопасности. По этому, в статье рассмотрены методы минимизации угроз персональным данным. Рассмотрены задачи, которые необходимо реализовать для защиты персональных данных при формировании и создании информационных систем защиты информационных ресурсов. Приведены пути их решения с целью минимизации угроз персональным данным. Показано, что предупреждение несанкционированной утечки персональных данных сетевыми каналами требует внедрения специальных систем обнаружения и блокировки таких посыланий сетевыми каналами. Создана система выявления и предупреждения утечки персональных данных сетевыми каналами. В основу работы системы положены особые требования к управлению персональными данными. Применение такого подхода позволяет выявлять персональные данные в сетевом потоке, проводить идентификацию разрешенных и неразрешенных посыланий таких данных сетевыми каналами и предупреждать их несанкционированное распространение сетевыми каналами.*

Ключевые слова: *персональные данные, сетевые каналы, информация, защита, системы защиты, утечка информации, система предупреждения утечки информации.*

Filonenko S., Muzhik I., Nimchenko T. Personal data leakage prevention system for network channels

Abstract. *One of the actual problems of information security is information leakage, in particular personal data, using network channels. That's why in this paper methods of threats minimizing to personal data have been considered. Tasks that need to be implemented for the personal data security in the formation and establishment of information security systems were considered. Their solutions in order to minimize threats to the personal data were considered. Prevent unauthorized leakage of personal data network channels requires the introduction of special systems of detection and blocking of sending such network channels have been shown. System to identify and prevent the leakage of personal data network channels was created. The basis of the system was based on the specific requirements for the management of personal information. This approach allows to identify the personal data in the network flow, the identification resolved and unresolved parcels such data network channels and prevent their unauthorized distribution network channels.*

Key words: *personal data, network channels, information, security, security systems, information leakage, data leakage prevention system.*

Отримано 2 *вересня 2014 року*, затверджено редколегією 17 *вересня 2014 року*