УДК 004.67
DOI: 10.15587/2312-8372.2015.41329

Німченко Т. В.

АНАЛІЗ ЗАГРОЗ ПЕРСОНАЛЬНИМ ДАНИМ ТА ЗАСОБІВ ЇХ ЗАХИСТУ

Проведено аналіз загроз персональним даним та засобів протидії їм. Розглянуто завдання, які необхідно реалізувати для захисту персональних даних. 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.

Ключові слова: *захист інформації, персональні данні, загрози, інформаційна безпека, системи, засоби, інформація.*

1. Вступ

Сучасні інформаційні технології набувають глобального характеру. Їх розвиток та розвиток засобів комунікацій, забезпечують все більш широкі можливості доступу до інформаційних ресурсів та переміщення великих масивів даних на необмежені відстані. При цьому забезпечений доступ широкого кола користувачів, розташування яких може бути практично довільним, до ресурсів, що знаходяться будь-де у межах глобальної інформаційної мережі. В умовах інтенсивного розвитку ринку інформаційних продуктів та послуг інформація стала повноцінним товаром, який має свої споживчі властивості та вартісні характеристики. Тому інформація, як продукт що має попит, потребує збереження та надійного захисту.

Широке впровадження інформаційних технологій робить закономірною та актуальною проблему захисту інформації. Про її актуальність говорять оператори інформаційних систем та представники бізнесу, про її актуальність говориться у всіх, без винятку, аналітичних звітах з питань безпеки бізнесу та інформаційної безпеки. Дослідження показують, що лише половина фахівців з інформаційної безпеки вважають свою компанію чи установу такою, що готова протистояти сучасним інформаційним загрозам, зокрема і таким, що можуть призвести до неконтрольованого поширення інформації за межі інформаційних систем, у яких вона обробляється.

2. Аналіз літературних даних і постановка проблеми

До проблеми неконтрольованого поширення особливо чутлива така категорія інформації, як персональні дані (ПД) [1–10]. На поточний час є актуальними питання внутрішньої безпеки інформаційних систем (ІС), зокрема і питання неконтрольованого поширення даних [4, 5]. 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. Серед загроз в інформаційній безпеці виділяють дві групи загроз: внутрішні та зовнішні [6]. 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. Що стосується засобів захисту від внутрішніх загроз, то тільки незначна частина компаній їх використовує, хоча необхідність у цих засобах об'єктивно існує [8]. Однією з основних причин актуальності внутрішніх загроз інформаційній безпеці є несанкціонований витік інформації за межі захищених ІС, обсяг якої має сталу тенденцію до зростання. Мінімізувати такі загрози можна шляхом впровадження систем протидії внутрішнім загрозам інформаційній безпеці [4].

Як показують результати аналізу, опинившись за межами захищеної інформаційної системи, персональні дані стають доступними практично необмеженому колу користувачів і можуть бути знищені чи спотворені, а також можуть бути використані з метою нанесення шкоди особі, якої стосуються, як моральної, так і матеріальної [11]. Тому питанням захисту від неконтрольованого поширення персональних даних приділяється особлива увага зі сторони міжнародного співтовариства та урядів багатьох держав світу.

Дослідження питаннь захисту персональних даних є актуальними для операторів інформаційних систем та фахівців з інформаційної безпеки [9, 10].

3. Об'єкт, ціль та задачі дослідження публікації

Об'єктом дослідження виступають існуючі загрози в інформаційній безпеці під час захисту персональних даних та системи захисту інформації, які запобігають її витоку під час передачі мережевими каналами.

Ціллю публікації є дослідження та аналіз загроз інформаційній безпеці під час передачі персональних даних мережевими каналами, а також заходів протидії цим загрозам.

Задачами дослідження є розгляд існуючих систем захисту інформації, проведення їх порівняння та можливостей застосування.

4. Загрози інформаційній безпеці

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 (рис. 1). Такий висновок зробили експерти за результатами спільного дослідження «Информационная безопасность бизнеса, 2012» [1], яке у 2012 році було проведено у 22 країнах світу відомою у галузі інформаційної безпеки російською компанією «Лабораторія Касперського» спільно з компанією B2B International (Великобританія), що спеціалізується на проведені досліджень для бізнесу з широкого кола питань.

Рис. 1. Основні загрози бізнесу. За матеріалами дослідження «Информационная безопасность бизнеса, 2012» [1]

При цьому у звіті йдеться про те, що немає підстав говорити про зменшення рівня загроз інформаційній безпеці у найближчий час. Навпаки, експерти очікують зростання інтенсивності загроз, підвищення рівня їх технічного супроводження та виникнення нових.

Такий стан справ не може не викликати зацікавленості експертів у галузі інформаційної безпеки. Провідні світові компанії та установи у галузі інформаційної безпеки та безпеки держави протягом останніх років періодично проводили дослідження захищеності інформаційних систем, у тому числі і з точки зору несанкціонованого витоку інформації. Серед них, наприклад, спільні дослідження ФБР та Інституту комп'ютерної безпеки CSI (США) «Computer Crime and Security Survey», дослідження компанії Ernst&Young «Global Information Security Survey, дослідження російських компаній InfoWatch та Лабораторії Касперського [1, 2], періодичні дослідження компанії Perimetrix «Персональные данные в Росии» [3] та ряд інших досліджень. Наведені дослідження проводились шляхом анкетування експертів у галузі інформаційної безпеки та управління бізнесом і аналізу анкет опитування. У якості експертів залучалися співробітники різних за величиною та обсягом послуг компаній у різних галузях господарства з різних країн світу, робота яких пов'язана з питаннями інформаційної безпеки, IT-технологіями та управлінням установами та організаціями.

З точки зору неконтрольованого витоку даних за периметр інформаційних систем, заслуговує на увагу дослідження «Глобальное исследование утечек корпоративной информации и конфедициальных данных» [4], які періодично проводились протягом останніх років компанією InfoWatch. Методика таких досліджень відрізняється від методик попередньо наведених досліджень тим, що аналізувалися не точки зору експертів з тих чи інших питань інформаційної безпеки, а зафіксовані та оприлюднені у загальнодоступних засобах інформації (ЗМІ, Internet тощо) випадки неконтрольованого витоку інформації за периметр інформаційних систем. У даному дослідженні аналізувались інциденти з інформаційної безпеки, які пов'язані виключно з витоком даних. До нього не ввійшли та не аналізувалися дані про інциденти, які пов'язані з зовнішніми загрозами інформаційній безпеці (віруси, зовнішні комп'ютерні атаки, DDoS, фітинг тощо). Іншими словами, дослідження стосується виключно проблеми витоку інформації за межі захищених інформаційних систем установ та організацій з тих чи інших причин.

При цьому результати досліджень, проведених за різними методиками, не суперечать один одному і, в основному, співпадають. Це дає право скористатися ними для виявлення тенденцій розвитку загроз інформаційній безпеці, їх характеру та інтенсивності виникнення, а також оцінити результати, отримані від впровадження тих чи інших методів та систем протидії загрозам.

Як відомо, сучасні технології обробки інформації, і персональних даних у тому числі, передбачають використання інформаційних систем (ІС) [5, 6]. Такі системи представляють собою взаємопов'язану сукупність засобів, методів та персоналу, що забезпечують збір, збереження, обробку, передачу та відтворення інформації з метою досягнення поставленої мети. Інформація є центральним компонентом ІС. При цьому об'єктами захисту стають інформаційна система, у якій обробляється інформація з використанням певних інформаційних технологій, інформаційні технології і, власне, сама інформація.

Серед загроз інформаційній безпеці виділяють дві групи загроз: внутрішні та зовнішні [7]. 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.

Як показують проведені дослідження [5], протидії загрозам інформаційній безпеці приділяється певна увага з боку операторів ІС. Практично всі оператори впровадили до складу ІС засоби протидії як внутрішнім, так і зовнішнім загрозам. Так склалося, що протидії зовнішнім загрозам приділялося більше уваги, ніж протидії внутрішнім загрозам. Периметр інформаційної системи захищався у більшій мірі, ніж мінімізовувались внутрішні загрози. Тому на сьогоднішній день засоби протидії зовнішнім загрозам впроваджені більш широко, ніж засоби протидії внутрішнім загрозам.

Шляхом впровадження заходів протидії загрозам інформаційній безпеці оператори ІС досягли певного рівня захисту їх окремих компонентів та ІС у цілому від зовнішніх загроз інформаційній безпеці. Такі інформаційні системи називають захищеними [6] і, з певним рівнем ймовірності, можна стверджувати, що інформація, яка опрацьовується такими системами, у їх межах, захищена від зовнішніх загроз.

При цьому гострим залишається питання протидії внутрішнім загрозам інформаційній безпеці, актуальність якого зростає. Так, якщо за результатами до-

слідження «Information security breaches survey 2006», проведеного міжнародною компанією Price Waterhouse Coopers у 2006 році, вважали актуальними питання протидії внутрішнім загрозам інформаційній безпеці 32 % експертів у галузі інформаційної безпеки та безпеки бізнесу, то у 2011 році експерти з ФБР та Інституту комп'ютерної безпеки CSI (США), за результатами дослідження «Computer Crime and Security Survey 2010/2011», проведеного з тією ж аудиторією експертів, визнали проблему протидії внутрішнім загрозам інформаційній безпеці як пріоритетну.

Однією з основних причин актуальності внутрішніх загроз інформаційній безпеці є несанкціонований виток інформації за межі захищених ІС, обсяг якого має сталу тенденцію до зростання. Мінімізувати такі загрози можна шляхом впровадження систем протидії внутрішнім загрозам інформаційній безпеці. Відомі чотири класи таких систем [9]. Серед них системи моніторингу та аудиту, системи аутентифікації, засоби шифрування та системи виявлення і попередження витоку інформації.

Системи моніторингу та аудиту дозволяють реєструвати дії користувачів та процесів у ІС, у тому числі дії та процеси, що пов'язані з пересиланням даних за межі ІС мережевими каналами. Такі системи є важливим засобом при розслідуванні зафіксованих випадків несанкціонованого витоку інформації за периметр захищених ІС та проведенні їх аналізу. Недоліком таких систем є відсутність можливості попередження несанкціонованого витоку інформації. У роботі систем моніторингу та аудиту не передбачені алгоритми проведення аналізу зафіксованих подій. Це означає, що вони не можуть визначити, чи зафіксована подія допустима з точки зору інформаційної безпеки, чи ні. Закономірно, що у таких системах непередбачені будь-які алгоритми блокування передачі даних мережевими каналами.

Системи аутентифікації користувачів ІС застосовуються для захисту від несанкціонованого доступу до даних. У їх основі лежить процес аутентифікації користувача (може бути дво- або триетапний). За його результатами користувачеві може бути або наданий доступ до запрошених ресурсів, або ні, чим попереджається можливий несанкціонований виток інформації за межі ІС. Такі засоби не можуть захистити інформацію від користувача, який за нормами політики безпеки ІС має доступ до даних, але при цьому планує використати їх в цілях, що суперечать нормам чинного законодавства чи політиці безпеки компанії (від інсайдера).

Засоби шифрування носіїв змінюють дані таким чином, що ними неможливо скористатися без спеціальних програм (ключів). Цей клас програм захистить дані від витоку при втраті мобільної системи збереження або обробки інформації та при перехопленні даних зловмисником поза межами захищеної ІС. Ефективність такого засобу захисту нівелюється, якщо разом з даними до зловмисника попадуть ключі шифрування.

Системи виявлення та попередження витоку інформації (Data Leakage Prevention, DLP-системи) проводять сканування можливих каналів витоку даних в реальному масштабі часу, а також можуть контролювати дії користувачів і процеси обробки та передачі інформації у межах ІС. При цьому такі системи здатні розпізнавати інформацію за певними категоріями. Вони можуть бути комплексними або локальними.

Комплексні DLP-системи контролюють декілька каналів витоку інформації. Наприклад, копіювання на мобільні носії, системи друку, мережеві канали передачі інформації тощо.

Локальні системи контролюють лише один з можливих каналів витоку інформації, найчастіше мережевий. У таких системах можуть бути впроваджені проактивні технології, завдяки яким з'являється можливість не лише виявляти випадки несанкціонованого переміщення інформації за периметр захищених ІС, але і блокувати їх. Додатковою функцією DLP-систем може бути шифрування даних в процесі запису на носії чи у файли.

Існують також інші програмно-апаратні засоби захисту інформації від внутрішніх загроз інформаційній безпеці, які не можна безпосередньо віднести до наведених вище категорій. 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 витоків інформації (DLP-системи) є єдиним рішенням, що дозволяє запобігти витокам інформації за межі захищеного простору ІС в реальному масштабі часу на основі фільтрації даних або зовнішніх атрибутів, які супроводжують процес переміщення даних.

Зазвичай ядро подібних DLP систем складають технології категоризації контенту, які базуються на контейнерному або контекстному аналізі вихідного потоку. Переваги контейнерного аналізу полягають у простоті його реалізації, до недоліків відносять організаційні труднощі при впровадженні та обмежені можливості контролю вихідного трафіку. При контекстному аналізі в основному використовують лінгвістичні або статичні методи аналізу файлів. Кожен з наведених методів має свої переваги та недоліки. Переваги лінгвістичних технологій полягають у тому, що вони працюють безпосередньо зі змістом документів, можуть самоудосконалюватись, їх швидкодія напряму залежить від обсягу потоку інформації, до недоліків відносять залежність від мови повідомлення, низьку ефективність при аналізі структурованої інформації, медійних та графічних файлів. Статистичні методи сприймають файл як послідовність символів, тому ефективно працюють з текстовими документами на різних мовах, а також з медійними та графічними файлами. До недоліків статистичних методів відносять можливий високий відсоток хибних спрацювань та трудомісткий процес налагодження системи.

Існує дві архітектури DLP систем: шлюзова або хостова. Переваги шлюзових систем полягають у простоті реалізації. До недоліків відносять обмежену область застосування та проблемність аналізу деяких видів трафіку, наприклад сімейства SSL. До переваг хостових систем відносять більш широке коло можливостей контролю за витоком даних, зокрема, і немережевими каналами.

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 [10]. Очевидно, що загальний принцип роботи таких систем досить простий (рис. 2).

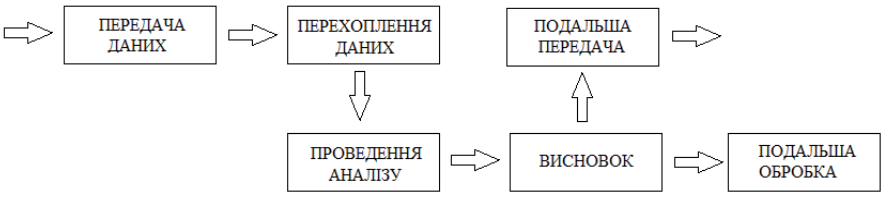

Рис. 2. Загальний принцип роботи системи виявлення та попередження витоку ПД мережевими каналами

Основне призначення систем виявлення та попередження витоку інформації — забезпечити захист від випадкового чи умисного розповсюдження інформації з обмеженим поширенням легальними, такими що мають визначені права доступу користувачами ІС за її межі. З цією метою DLP-системи проводять моніторинг інформації, яка надходить до каналу передачі даних за межі ІС. З метою попередження витоку інформації з обмеженим поширенням через мобільні засоби обробки та засоби тимчасового зберігання інформації (паперові носії та інші немережеві канали витоку) системою може проводитись моніторинг переміщення даних на рівні кінцевих пристроїв та робочих станцій ІС. Також такі системи можуть проводити сканування файлів та баз даних, які обробляються ІС з метою виявлення місць зберігання заданої для контролю інформації. Отримані дані перевіряються на відповідність встановленим правилам безпеки і, у відповідності від результатів порівнянь, проводиться виконання тих чи інших алгоритмів мінімізації загроз інформаційній безпеці.

Реалізовані архітектурні рішення систем контролю за витоком інформації за периметр захищеної ІС, що пропонуються розробниками, мають свою власну побудову. Але, виходячи з призначення DLP-системи та задач, що повинні вирішувати такі системи, основними модулями систем виявлення та попередження витоку інформації за межі захищених ІС є:

- сервер (сервери) контролю вихідного трафіку (СКВТ);
- сканери даних (СД);
- сканери кінцевих пристроїв (СКП);
- агентські програми (АП), які встановлюються на робочих станціях ІС;
- сервер управління (СУ);
- сервер баз даних.

Логіка роботи системи виявлення та попередження витоку інформації полягає у наступному. Сервер контролю вихідного трафіку (СКВТ) аналізує поток інформації, що надходить до каналу передачі даних за межі ІС. Аналіз проводиться з метою виявлення у ньому заданих до пошуку даних обмеженого поширення, тих, на які поширюється заборона щодо передачі за межі ІС. У випадку виявлення таких даних, повідомлення про їх виявлення передається на сервер управління.

Сервер контролю вихідного трафіку може обробляти як сам вихідний поток, так і його копію. У системах, які обробляють копії вихідного трафіку, відсутня можливість блокування виявлених випадків витоку обмежених до передачі даних за периметр ІС. При цьому такі системи не зменшують пропускну спроможність каналу передачі даних. У випадку включення СКВТ в канал вихідного трафіку, DLP-система зможе блокувати передачу по мережевому каналу виявлених заборонених до передачі даних. Але, у цьому випадку, можливе зменшення швидкості інформаційного канального обміну аж до його повного блокування при високих обсягах інформації, що передається мережевим каналом.

З метою виявлення в ІС даних обмеженого поширення DLP-системою запускаються сканери даних, які проводять сканування ресурсів ІС. У випадку виявлення таких даних, СД надсилає повідомлення до серверу управління про виявлений ресурс, зокрема, категорію даних, місцезнаходження, контейнер, у якому вони зберігаються тощо. Реалізація сканерів може бути будь-якою — від виконання процесу сканування СД до запуску програм-агентів на серверах баз даних та кінцевих пристроях ІС.

5. Обговорення результатів дослідження засобів захисту персональних даних

Стаття носить оглядовий характер. Проведені дослідження існуючих загроз інформаційній безпеці під час передачі персональних даних мережевими каналами, а також заходів протидії цим загрозам. Приведені існуючі системи протидії внутрішнім загрозам інформаційній безпеці з подальшим аналізом ефективності їх застосування. Представлений загальний принцип роботи системи виявлення та попередження витоку ПД мережевими каналами. Обговорені архітектурні рішення систем контролю за витоком інформації за периметр захищеної ІС, що пропонуються розробниками.

Результати даних досліджень є базовими та можуть бути використані при розробці систем, які базуються на особливостях управління ПД, та потребують удосконалення існуючих технологій фільтрації, впровадження нових методів виявлення даних у інформаційному потоці, концептуально змінюючи підходи до їх розпізнавання.

На основі проведених наукових досліджень, враховуючи представлені переваги та недоліки, в подальшому можливе удосконалення спеціальних систем виявлення та витоку інформації з метою покращення рівня інформаційної безпеки систем обробки інформації.

6. Висновки

Результати проведених досліджень показують, що попередження витоку персональних даних зумовлює необхідність контролю каналів їх передачі. Такий контроль необхідно проводити з використанням технологій та систем, які передбачають моніторинг інформації, що передається мережевими каналами. При цьому технології повинні виявляти персональні дані в інформації, що передається. Аналіз існуючих методів та підходів показує, що побудова оптимальних технологій захисту персональних даних базується на поєднанні існуючих методик контекстного аналізу інформації з урахуванням форматів їх передачі, а також алгоритмів реагування на виявлені спроби передачі персональних даних. При цьому необхідно формування та підтримка спеціальних баз даних, які дозволять проводити аналіз та реалізацію алгоритмів виявлення та реагування несанкціонованої передачі інформації.

Література

1. INFOBEZ-EXPO — международная выставка-конференция [Электронный ресурс]. — 2013. — Режим доступа: \www/ URL: http://infobez-expo.ru/
2. Информационная безопасность бизнеса [Электронный ресурс]. — 2012. — Режим доступа: \www/URL: http://www.kaspersky.ru/other/custom-html/brfwn/Bezopasnost_Screen.pdf
3. Инсайдерские угрозы в России 2009 [Электронный ресурс]. — 2009. — Режим доступа: \www/URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf
4. Коржов, В. В. Защита персональных данных: проблемы и пути решения [Текст] / В. В. Коржов // Открытые системы. — 2010. — № 10. — С. 11.
5. Марков, А. П. Проблемы и решения по защите персональных данных в информационных системах персональных данных [Текст] / А. П. Марков, Б. И. Сухинин // Компьютерная безопасность. — 2009. — № 5. — С. 20–27.
6. Аверченков, В. И. Формализация процесса выбора состава средств обеспечения безопасности на объекте защиты [Текст] / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин // Вестник компьютерных и информационных технологий. — 2010. — № 11. — С. 45–50.
7. Німченко, Т. В. Критерій визначення з переліку даних тих, що відносяться до категорії персональні [Текст] / Т. В. Німченко // Вісник інженерної академії України. — 2015. — № 1. —С. 199–202.
8. Сулавко, А. Е. Технологии защиты от внутренних угроз информационной безопасности [Текст] / А. Е. Сулавко // Вестник СибАД. — 2011. — № 1(19) — С. 45–51.
9. Філоненко, С. Ф. Система попередження витоку персональніх даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко // Ukrainian Scientific Jornal of Information Security. — 2014. — Vol. 20, № 3. — P. 279–285.
10. Німченко, Т. В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами [Текст] / Т. В. Німченко, І. М. Мужик, А. І. Мужик // Вісник інженрної академії України. — 2014. — № 3–4. — С. 199–203.
11. Гуцалюк, М. Інформаційна безпека України: нові загрози та організація протидії [Текст] / М. Гуцалюк // Правова інформатика. — 2004. — № 3. — С. 37–41.

АНАЛИЗ УГРОЗ ПЕРСОНАЛЬНЫМ ДАННЫМ И СРЕДСТВ ИХ ЗАЩИТЫ

Проведен анализ угроз персональным данным и средств противодействия им. Рассмотрены задания, которые необходимо реализовать для защиты персональных данных. Приведены пути их решения с целью минимизации угроз персональным данным. Показано, что предупреждение несанкционированного вытока персональных данных сетевыми каналами требует внедрения специальных систем выявления и блокировки таких посыланий сетевыми каналами.

Ключевые слова: защита информации, персональные данные, угрозы, информационная безопасность, системы, средства, информация.

Німченко Тетяна Василівна, *кандидат технічних наук, доцент, кафедра засобів захисту інформації, Інститут інформаційно-діагностичних систем, Національний авіаційний університет, Київ, Україна,* ***e-mail: fiona54@ukr.net****.*

Нимченко Татьяна Васильевна, *кандидат технических наук, доцент, кафедра средств технической защиты информации, Институт информационно-диагностических систем, Национальный авиационный университет, Киев, Украина.*

Nimchenko Tatiana, *Institute of Information-Diagnostic Systems, National Aviation University, Kyiv, Ukraine,* ***e-mail: fiona54@ukr.net****.*