УДК 004.056

К.т.н., доцент Маслянко П.П., магістрант Дубик С.І.

**Національний технічний університету України
«Київський політехнічний інститут»**

ДОСЛІДЖЕННЯ МЕТОДІВ ТА РОЗРОБКА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА МЕРЕЖЕНЕЗАЛЕЖНИХ РІВНЯХ МОДЕЛІ OSI

Вступ

Водночас зі зростанням популярності інформаційно-комунікаційних технологій виникають серйозні загрози розголошення персональних даних, критично важливих корпоративних ресурсів, державних таємниць [1, 2].

За даними інформаційного центру InfoWatch, дослідницько-консультативних компаній у сфері інформаційних технологій Gartner, Forrester і Bloor Research [3], внутрішні джерела витоку інформації переважають над зовнішніми (відповідно 56,5% і 43,5%). Так, тільки економіка США у 2006 р. втратила $65 млрд. внаслідок витоку приватних відомостей через внутрішні джерела. При цьому, найпопулярнішими засобами інформаційної безпеки є засоби захисту від зовніших витоків інформації: на долю антивірусів припадає 98,6%, міжмережевих екранів – 73,9%, контролю доступу – 50,8%, антиспамового програмного забезпечення – 30,5%. Серед засобів захисту інформації від внутрішніх витоків найпоширенішими є засоби контролю доступу – 50,8%, але ці системи не вирішують в повній мірі проблему захисту конфіденційної інформації, адже витік конфіденційних даних може бути здійснений і через персонал, що має доступ до захищуваної інформації.

Найпоширенішими каналами витоку інформації є електронна пошта, інтернет, друкувальні пристрої та мобільні накопичувачі, і при цьому вага витоку даних через сімейство TCP/IP протоколів (SMTP, HTTP, FTP, ICQ, тощо) – найбільша.

Серед тих небагатьох компаній, які займаються розробкою засобів запобігання витокам інформації, лідирують Symantec, MacAfee, Trend Micro, Websence та декілька інших. Проведений аналіз відповідних засобів [3] дозволяє зробити висновок, що до проблем, з якими зустрічаються дані продукти, відносяться проблеми продуктивності, хибного спрацьовування і хибного неспрацьовування програмного продукту.

Виходячи з викладеного, можна зазначити, що проблема дослідження методів та розробки засобів захисту інформації на

мереженезалежних рівнях моделі OSI, зокрема засобів запобігання витокам інформації через сімейство TCP/IP протоколів, дуже важлива і актуальна.

Постановка задачі

Головними задачами роботи є:

– дослідити та проаналізувати методи і підходи, що використовуються при розробці засобів захисту інформації на мереженезалежних рівнях моделі OSI, зокрема у системах запобігання витоку інформації;

– формалізувати завдання і вимоги, що висуваються до засобів запобігання витоку інформації;

– запропонувати модифікацію підходу моніторингу даних, що використовується у засобах запобігання витоку інформації.

Підходи до реалізації засобу запобігання витоку інформації на мереженезалежних рівнях моделі OSI

Розглянемо підходи інспектування трафіку, що використовуються у засобах запобігання витоку інформації [3]:

– підхід, що ґрунтується на правилах і регулярних виразах – інспектування трафіку відбувається за специфічними правилами. Метод застосовується безпосередньо до структурованих даних, що ідентифікуються. До переваг методу відносять легкість реалізації і настроювання та висока швидкість обробки даних. Недоліками методу є високий рівень хибного спрацьовування і низький рівень захисту неструктурованих даних;

– підхід, що ґрунтується на створенні відбитку бази даних – використовує точне співпадання даних до так званих «живих» даних бази даних. Даний підхід можна застосовувати лише для структурованих даних. Перевагою методу є дуже низький рівень помилкового спрацьовування. До недоліків підходу відносять можливі проблеми з продуктивністю системи при великому наборі даних і/або використання так званого «живого» під'єднання до бази даних;

– підхід, що ґрунтується на точній відповідності файлів – для моніторингу даних створюється база даних, що містить «відбитки» файлів – хеш-функції, створені на основі даних файлу. Далі, при інспектуванні даних, створюються «відбитки» цих даних і здійснюється пошук на відповідність «відбиткам» файлів у базі даних. Даний метод використовується в основному для неструктурованих бінарних даних. Підхід працює для будь-якого типу файлу і характеризується низьким рівнем хибного спрацьовування. Головним недоліком методу є те, що його легко оминути;

– підхід, що ґрунтується на частковій відповідності файлів – даний підхід в своїй основі використовує «відбитки» даних, як і попередній метод. Але

створюється «відбиток» не всього файлу, а його частин. Таким чином головний недолік попереднього підходу усувається. Метод придатний для захисту неструктурованих даних. Недоліком методу можуть бути хибні спрацьовування;
– статистичний аналіз – використовуються статистичні методи, аналогічні тим, які використовуються у антиспамових програмах. Даний підхід вимагає великого обсягу даних, що інспектуються, і характеризується дуже високими рівнями хибного спрацьовування і хибного неспрацьовування;
– підхід, що ґрунтується на використанні словників – підхід базується на використанні словників, ключових фраз, кількості слів і їх позиції. Застосовується для пошуку витоків конфіденційної інформації для неструктурованих даних. Такий підхід у більшості випадків не може визначатися користувачем системи і характеризується дуже високими рівнями хибного спрацьовування і хибного неспрацьовування.

Розробка засобу запобігання витоку інформації через стек протоколів TCP/IP

Проведений аналіз існуючих підходів дозволяє стверджувати, що не існує універсального методу моніторингу різних типів даних. Розглянемо модифікацію підходу, що ґрунтується на частковій відповідності файлів. Суть даної модифікації полягає у:
– наданні користувачам системи можливості регулювати розмір гранулюючого параметра, за допомогою якого обчислюється розмір частин файлу і створюються «відбитки» даних. Таким чином, чим вищий даний параметр, тим менша й імовірність хибних спрацьовувань (але при дуже великому значенні даного параметра зростає ймовірність хибних неспрацьовувань за рахунок можливого «забруднення» даних);
– використання понять дозволених і захищуваних даних. Дана модифікація дозволяє значно скоротити хибні спрацьовування (у зв’язку з тим, що більшість корпоративних документів мають схожу структуру – однаковий початок і кінець документів);
– «відбитки» даних обчислюються між визначеними позиціями байтів (орієнтовними точками). Орієнтовні точки вираховуються як локальні мінімуми вибраної функції на області байтів, визначеною гранулюючим параметром.

Завдання і вимоги до засобів запобігання витоку інформації через стек протоколів TCP/IP

До вимог, які висуваються до засобів запобігання витоку інформації, відносяться наступні [3]:

– багатоканальність – система має здійснювати моніторинг декількох можливих каналів витоку даних: у мережевому оточенні це як мінімум моніторинг e -mail, Web и IM (instant messengers) ;
– уніфікований менеджмент – система повинна мати уніфіковані засоби управління політикою інформаційної безпеки, аналізом і звітами за всіма каналами моніторингу;
– активний захист – система має не лише виявляти факти порушення політики безпеки, але й при необхідності примушувати до її виконання, наприклад, блокувати підозрілі повідомлення;
– урахування змісту і контексту – окрім виявлення фактів витоку інформації, система має враховувати і контекст (протокол, відправник, адресат, тощо).

Висновки

У роботі розглянуто основні завдання і вимоги до засобів запобігання витоку інформації, докладно проаналізованіо підходи, що застосовуються для моніторінгу даних. На основі проведеного дослідження, з урахуванням недоліків і переваг існуючих методів вирішення поставленої проблеми, запропонований удосконалений підхід, що ґрунтується на частковій відповідності файлів.

Одним з можливих напрямків подальших досліджень у сфері захисту інформації, є спроба стандартизації методів і підходів, що використовуються в засобах запобігання витокам конфіденційних даних крізь внутрішні джерела. Також актуальними проблемами, що потребують поглибленного вивчення, є створення і використання нових або модифікація існуючих методів і підходів до аналізу інформації.

Література

1. *Биячуев Т.А.* / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004. – 161 с.
2. *Платонов В.В.* Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студ. высш. учеб. Заведений / В.В.Платонов. – М.: Издательский центр «Академия», 2006. – 240 с.
3. *Скиба В.Ю., Курбатов В.А.* Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер. – 2008. – 320 с.