УДК 004.75

Д.т.н., професор Молчанов О.А., магістрант Котенко А.І.

Національний технічний університету України
«Київський політехнічний інститут»

МЕТОД ОРГАНІЗАЦІЇ СИСТЕМИ ОПЕРАТИВНОГО МОНІТОРИНГУ ТРАФІКУ

Вступ

Вирішення питань захисту даних в сучасних інформаційних системах є успішне тільки при умові використання комплексного підходу до побудови системи забезпечення безпеки інформації. Комплексна система захисту інформації (КСЗІ) – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації з обмеженим доступом від розголошення, витоку та несанкціонованого доступу.

В Україні створення КСЗІ в інформаційно-телекомунікаційних системах здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". Нормативи визначають необхідність комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу автоматизованої системи.

Одним із компонентів системи для забезпечення безпеки інформації в корпоративних мережах є системи моніторингу трафіку на предмет забороненого контенту. Основні задачі таких систем – упорядкування доступу до ресурсів мережі Інтернет, запобігання виходу конфіденційної інформації за межі компанії, здійснення моніторингу активності користувачів, забезпечення захисту від вірусів та іншого шкідливого мобільного коду.

Наразі використовують системи, що ґрунтуються на моніторингу мережевих пакетів. Системи мають клас «1.Д» відповідно до НД ТЗІ 2.5-005-99). Такі системи, як правило, встановлюють на маршрутизаторах, що відділяють локальну мережу від глобальної. Системи такого типу захищають від зовнішніх загроз та виконують моніторинг обміну інформацією між локальною та глобальною мережами. Процеси моніторингу в системах такого типу проходять на маршрутизаторі. Позитивною стороною таких систем є можливість комплексного захисту

мережі в цілому. Негативна сторона – неможливість моніторингу та аналізу трафіку всередині мережі.

Іншим типом програмного забезпечення, що використовується для захисту окремого комп'ютера та мережі, в якій він знаходиться є антивірусні системи (клас «1.ЦД» відповідно до НД ТЗІ 2.5-005-99). Програмне забезпечення цього типу, як правило, встановлюється на комп'ютері користувача. Позитивна сторона такої системи – це можливість зосередження процесів моніторингу і процесів генерації трафіку на кожному комп'ютері мережі. Негативна сторона проявляється в неможливості централізованої обробки та аналізу стану мережі, а також у відсутності централізованого механізму керування такими системами.

Таким чином, структура систем, що використовуються для організації моніторингу трафіку не може забезпечити можливість централізованого управління та моніторингу мережі компанії.

Постановка задачі

В межах комплексної системи захисту інформації необхідно запропонувати метод організації підсистеми оперативного моніторингу трафіку – спосіб реалізації системи. Моніторинг здійснюється на предмет забороненого контенту. Система повинна задовольняти вимогам централізації, масштабування та мати можливість інтеграції з іншими підсистемами в межах єдиної комплексної системи захисту інформації за допомогою відкритих протоколів.

Об'єктом дослідження є методи моніторингу мереж на предмет забороненого контенту, що передається по каналах зв'язку компанії.

Предмет дослідження – бізнес-процеси моніторингу http-трафіку, що передається як всередину мережі, так і за її межі.

Клієнт-серверний метод

На сьогодні ринок програмного забезпечення із захисту інформації не має комплексних систем, що ґрунтуються на моніторингу мережевого трафіку на стороні клієнта у контексті корпоративної мережі. Методи такого моніторингу також недостатньо досліджені.

Як відомо, для визначення методу необхідно запропонувати спосіб розв'язку головної проблеми – проблеми моніторингу трафіку. Розглянемо один із способів організації системи моніторингу. Він полягає у введенні в систему двох складових компонентів – серверної та клієнтської.

При такому способі організації на серверну складову покладені задачі по збереженню бази сигнатур загроз, списки блокованих IP-адрес для кожного користувача та оперативні звіти про роботу програм на клієнтських комп'ютерах.

Моніторинг мережі виконується на прикладному рівні мережевої моделі OSI (Open Systems Interconnection). Це зумовлено використанням програмної складової КСЗІ для обміну даними між програмами, що працюють на стороні клієнта, та сервером. Обмін даними виконується з використанням відкритих стандартизованих протоколів та технологій.

Програмне забезпечення, що працює на клієнтських комп'ютерах, виконує фільтрацію контенту, використовуючи інформацію, отриману з сервера. Сформувавши запит, система перевіряє тіло документа, що передається в мережу, і в разі виявлення конфіденційної, або забороненої інформації блокує процедуру відправки запиту. Аналогічний процес проходить і при отриманні відповіді клієнтом. Інформація про роботу фільтрів надсилається клієнтською складовою на сервер, де може бути проаналізована одразу після надходження.

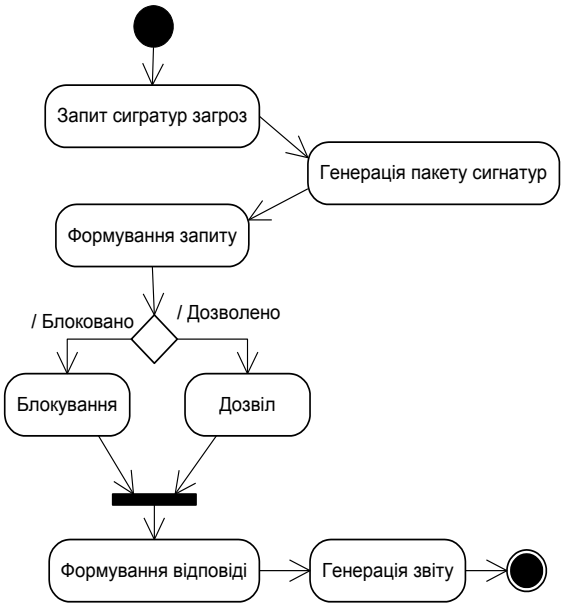

Рисунок. Модель обробки запиту. Діаграма діяльності в нотації UML

Контроль трафіку визначається правилами фільтрації – списки користувачів за групами доступу (white, black, all, default), списки ресурсів (URL, IP-адреси серверів), для яких дозволено і не дозволено доступ, ключові слава і словосполучення, поява яких в тексті запитів і відповідей є забороненою (конфіденційна інформація), списки форматів файлів і типів даних (MIME-типів та інше).

Сигнатури повідомлень, що зберігаються на сервері, можуть бути представлені як списками доступу до окремих комп'ютерів мережі, так і регулярними виразами, що визначають шаблони на класи контенту, що передається мережею.

Таким чином, спосіб організації системи оперативного моніторингу за клієнт-серверним методом полягає у наступному:

- програмне забезпечення розділяється на дві складові – серверну і клієнтську;
- процеси моніторингу і контролю трафіку відбуваються на клієнтському програмному забезпеченні;

- процеси звітності і оперативного контролю зосереджуються на сервері.

Система, розроблена за клієнт-серверним методом, буде мати клас «3.КД» відповідно до державного стандарту автоматизованих систем НД ТЗІ 2.5-005-99. Така система – це розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Використання клієнт-серверної архітектури системи дає можливості масштабування та побудову комплексної системи захисту інформації, що задовольняє поставленим вимогам.

Висновки

Метод реалізації системи оперативного моніторингу Інтернет-трафіку на предмет забороненого контенту дозволяє поєднати можливості по централізації контролю за процесом моніторингу і разом з тим зменшити навантаження на сервери системи. Це стає можливим за допомогою введення клієнтського програмного забезпечення.

Централізація системи моніторингу дозволяє створити систему аналізу загроз, що ґрунтується на оперативних звітах. Така складова дає можливість автоматизувати процес створення сигнатур, зменшивши тим самим час реакції системи на нові загрози.

Наведений принцип організації системи може бути застосований в широкому спектрі інтеграційних систем забезпечення безпеки, де важливими є показники масштабованості та централізації.

Варто також зауважити, що таке поєднання підсистем в єдину комплексну систему захисту інформації дає можливість підвищити клас автоматизованої системи захисту інформації до «3» відповідно до НД ТЗІ 2.5-005-99.

Література

1. *М. Спортак, Ф. Паппас.* Компьютерные сети и сетевые технологии. "ДиаСофт", 2004 год. – 720 с.
2. ДСТСЗІ СБ України, НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
3. ДСТСЗІ СБ України, НД ТЗІ 3.6-001-00. «Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу».
4. *Танненбаум Ендрю.* «Современные операционные системы» 2 изд. – СПб.: Питер, 2002. – 1040 с.