УДК 681.324

І.В. Рубан, Є.С. Лошаков

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

ТЕХНОЛОГІЯ ПОБУДОВИ АГЕНТ-ОРІЄНТОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ПОВІЛЬНОЇ DoS-АТАКИ

Запропонована агент-орієнтована система виявлення повільних DoS-атак, яка представляє собою програмно-апаратний комплекс, що запроваджується в інформаційно-телекомунікаційну систему.

Ключові слова: *повільна DoS-атака, інформаційна безпека, комп'ютерна злочинність.*

Вступ

Постановка проблеми. В кінці XX століття все більшого розвитку набувають інформаційні технології. Вони проникають в усі сфери людської діяльності. З одного боку, це призводить до значного підвищення ефективності праці в наслідок впровадження систем автоматизації та засобів обробки і передачі інформації. А з іншого – стає причиною виникнення такого виду злочинності, як інформаційна. Паралельно з розвитком інформаційних технологій розвиваються різноманітні засоби несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем. Вони становлять істотну загрозу інформаційній безпеці інформаційно-телекомунікаційних систем як великих корпорацій, так і державних установ, про що свідчить значна кількість успішно проведених кібернетичних атак по всьому світі.

Аналіз літератури [1 – 8] показав, що існує велика кількість загроз інформаційній безпеці. Постійно з'являються нові види кібернетичних атак. Одними з найбільш розповсюджених видів атак є атаки типу «відмова в обслуговуванні» (DoS-атаки). На теперішній час відома значна кількість способів реалізації даної атаки. Існують засоби виявлення та протидії усім відомим реалізаціям DoS-атаки, крім повільної DoS-атаки, що реалізується завдяки особливостям функціонування протоколу TCP.

Основна частина

Повільна DoS-атака реалізується завдяки особливостям функціонування протоколу TCP. Вона направлена на сервери, що надають відповідні послуги користувачам інформаційно-телекомунікаційної системи. Даний вид атаки може реалізовуватися двома шляхами:

- інсайдерська атака, що реалізується наступним чином. Зловмисник через обслуговуючий персонал інформаційно-телекомунікаційної системи впроваджує програмне забезпечення, що реалізує повільну DoS-атаку, яка запускається у попередньо заданий час або за командою ззовні, та генерує характерні для неї піки трафіку у задані моменти часу.
- атака з зовнішньої мережі, реалізується шляхом генерування одним або багатьма (botnet) комп'ютерами, що знаходяться ззовні до інформаційно-телекомунікаційної системи, яка атакується, відповідних піків трафіку.

Для виявлення та подальшого блокування повільних DoS-атак пропонується застосовувати аналізатор вхідного трафіку, що розміщується в інформаційно-телекомунікаційній мережі.

Аналізатор трафіку представляє собою електронно-обчислювальну машину зі спеціальним програмним забезпеченням. Він аналізує трафік, що поступає на сервер, на предмет наявності шкідливого трафіку, який відправлений зловмисником для реалізації повільної DoS-атаки. Якщо такий трафік виявлений, то він виконує пошук джерел шкідливого трафіку з метою їх подальшого блокування. Аналізатор трафіку функціонує таким чином. Увесь вхідний трафік записується до бази даних. Під записом до бази даних розуміється занесення у відповідну таблицю бази даних вихідних програмних портів (sourceports) вхідних сегментів, а також їх порядкових номерів, що відображають хронологію їх отримання, та часу прибуття. У разі виявлення повільної DoS-атака запускається механізм виявлення джерел шкідливого трафіку. Причому запис вхідних сегментів не припиняється. Графова модель роботи механізму аналізу вхідного трафіка представлена на рис. 1.

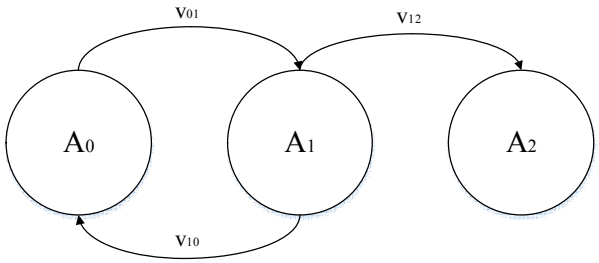

Рис. 1. Графова модель роботи механізму аналізу вхідного трафіка

Стан A_0 – запис в базу даних вхідних сегментів, відправлення пакетів та отримання підтверджень від адресата про їх надходження (ACK). Тобто це стан нормального функціонування серверу.

Стан A_1 – запис в базу даних вхідних сегментів, повторне відправлення пакетів, про надходження яких не прибуло підтвердження від адресата.

Стан A_2 – запис в базу даних вхідних сегментів, вивід повідомлення про наявність повільної DoS-атаки, запуск процесу виявлення джерел шкідливого трафіку.

Перехід v_{01}– неотримання впродовж 1 секунди підтвердження від адресата про надходження відправлених пакетів та наявність піку трафіка. Перехід v_{10} – отримання впродовж 1 секунди підтвердження від адресата про надходження відправлених пакетів. Перехід v_{12} – неотримання впродовж 2 секунди підтвердження від адресата про надходження повторно відправлених пакетів та наявність піку трафіка.

Графова модель роботи механізму виявлення джерел шкідливого трафіка представлена на рис. 2.

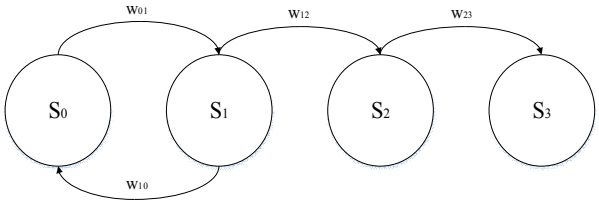

Рис. 2. Графова модель роботи механізму виявлення джерел шкідливого трафіка

Стан S_0 – виділення в базі даних вхідних сегментів, що прибули в інтервалі часу (t_0; t_0 +1) та інтервалі часу (t_0; t_0 +3).

Стан S_1 – сортування виділених сегментів по вихідному програмному порту.

Стан S_2 – визначення програмного порта, з якого прибула найбільша кількість сегментів.

Стан S_3– запуск процесу блокування шкідливого трафіку.

Перехід w_{01}– знайдені сегменти, що прибули і в інтервалі часу (t_0; t_0 +1), і в інтервалі часу (t_0; t_0 +3). Перехід w_{10} – сегменти, що прибули і в інтервалі часу (t_0; t_0 +1), і в інтервалі часу (t_0; t_0 +3) не знайдені. Перехід w_{12} – сортування сегментів по вихідному програмному порту завершено, перехід до визначення порта, з якого прибула найбільша кількість сегментів. Перехід w_{23}– порт, з якого прибула найбільша кількість сегментів, визначений, перехід до блокування шкідливого трафіка.

Алгоритми аналізу вхідного трафіка та виявлення джерел шкідливого трафіка, що реалізуються аналізатором, представлені на рис. 3 та 4 відповідно.

Таким чином, трафік, що надходить на сервер, записується у базу даних, що зберігається безпосередньо на аналізаторі трафіку. Час відправлення вихідних пакетів, які сервер надсилає користувачам також фіксується аналізатором. У разі неотримання підтвердження про надходження хоча б одного відправленого пакета протягом 1 секунди після відправки та наявності піку трафіку у цей час, пакет, що не підтверджений, відправляється повторно. Після повторної відправки пакета сервер очікує підтвердження про його отримання протягом 2 секунд. Якщо пакет-підтвердження не надходить та в цей же час присутній пік трафіку у каналі зв'язку, робиться висновок про наявність повільної DoS-атаки та запускається процес виявлення джерел шкідливого трафіку. Під піком трафіку розуміється короткотермінове стовідсоткове завантаження каналу зв'язку, що створюється в чітко визначені моменти часу, обумовлені повільною часовою шкалою роботи протоколу TCP.

Після того, як був запущений процес виявлення джерел шкідливого трафіку, в базі даних в таблиці вхідних сегментів шукаються сегменти, які прибули і в інтервалі часу (t_0; t_0 +1), і в інтервалі часу (t_0; t_0 +3). Якщо такі сегменти присутні, то проводиться їх сортування за вихідним програмним портом. Після цього для кожного вихідного порта обраховується кількість сегментів, які були з нього відправлені на сервер та прибули у вищевказані інтервали часу. Програмний порт, з якого прибула найбільша кількість сегментів у задані інтервали часу, вважається джерелом шкідливого трафіку і передається механізму блокування.

Таким чином, була отримана агент-орієнтована система виявлення повільних DoS-атаки, яка реалізується у вигляді програмно-апаратного комплексу, впровадженого в інформаційно-телекомунікаційну систему.

Висновки

Таким чином, з розвитком інформаційних технологій з'являються нові шляхи несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем. Одним з таких шляхів є повільна DoS-атака, яку неможливо виявити існуючими на даний момент засобами. Була запропонована технологія побудови агент орієнтованої системи виявлення повільних DoS-атак, яка представляє собою програмно-апаратний комплекс, що впроваджений в інформаційно-телекомунікаційну систему. Дана система реалізує два механізми: аналізу вхідного трафіка та виявлення джерел шкідливого трафіку. Перший механізм записує вхідні пакети до бази даних та аналізує завантаженість каналу зв'язку на предмет наявності характерних для повільної DoS-атаки піків трафіку, а також отримання підтверджень від адресатів про доставку відправлених пакетів. Другий механізм виявляє джерела шкідливого трафіку, аналізуючи вхідні сегменти, що прибули в інтервали часу, в які очікується надходження цього трафіку. Після того, як джерела шкідливого трафіку будуть виявлені, запускається механізм їх блокування.

Список літератури

1. Касперски К. Техника сетевых атак / К. Касперски. – М.: СОЛОН-Р, 2001. – 304 с.

2. Касперски К. Компьютерные вирусы изнутри и снаружи / К. Касперски. – СПб.: Питер, 2006. –526 с.

3. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в интернет / С.А. Петренко, В.А. Курбатов. – М.: ДМК Пресс, 2011. – 396 с.

4. Жуков Ю. Основы веб-хакинга. Нападение и защита / Ю. Жуков. – СПб.: Питер, 2006. – 208 с.

5. Столингс В. Основы защиты сетей. Приложения и стандарты / В.Столинг . – М.: Вильямс, 2002. – 432 с.

6. Эриксон Дж. Хакинг: искусство эксплойта. 2-е издание / Дж. Эриксон. – М.: Символ Плюс, 2009. – 510 с.

Надійшла до редколегії 17.02.2015

Рецензент: д-р фіз.-мат. наук, проф. С.В. Смеляков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

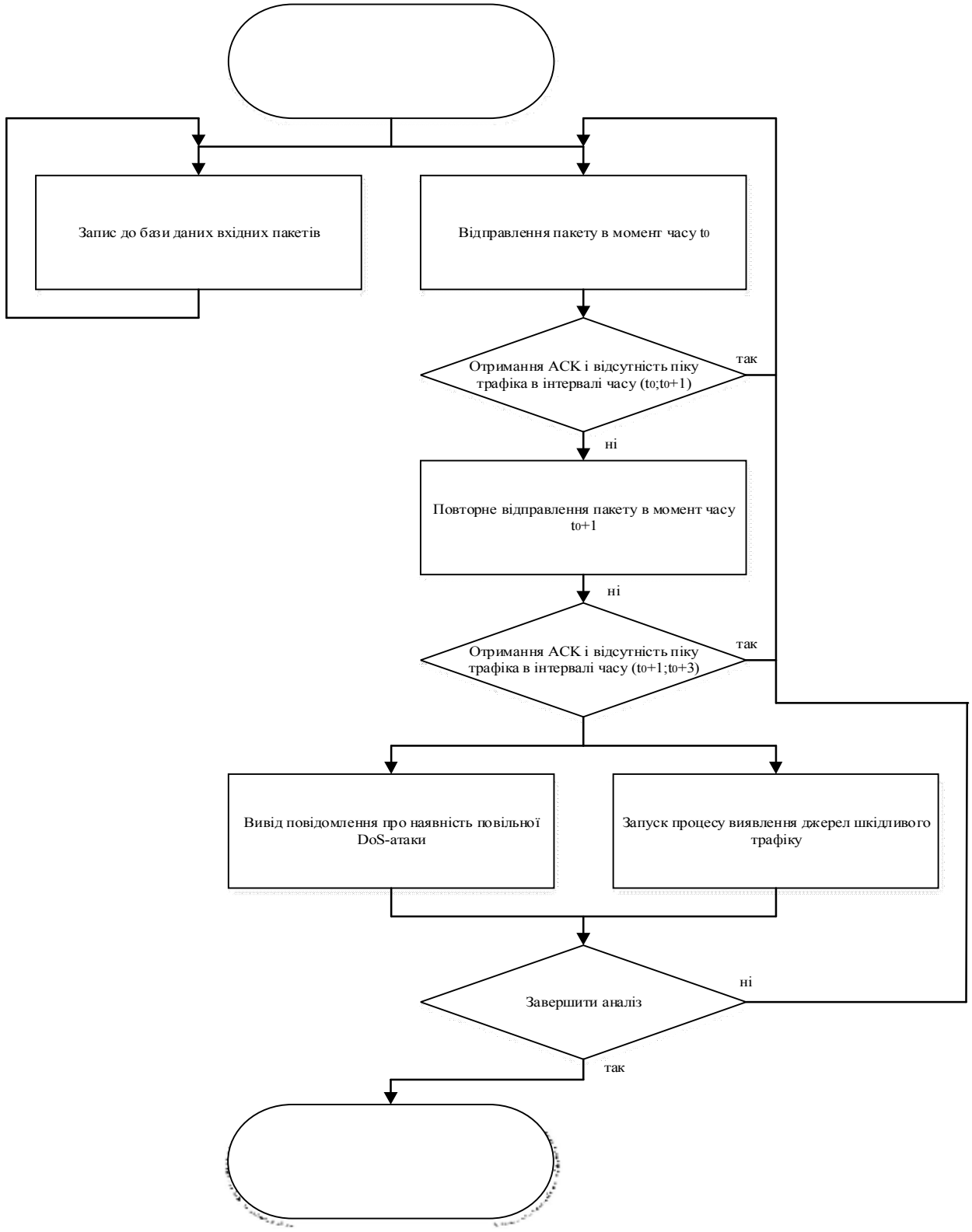

Рис. 3. Алгоритм аналізу вхідного трафіку

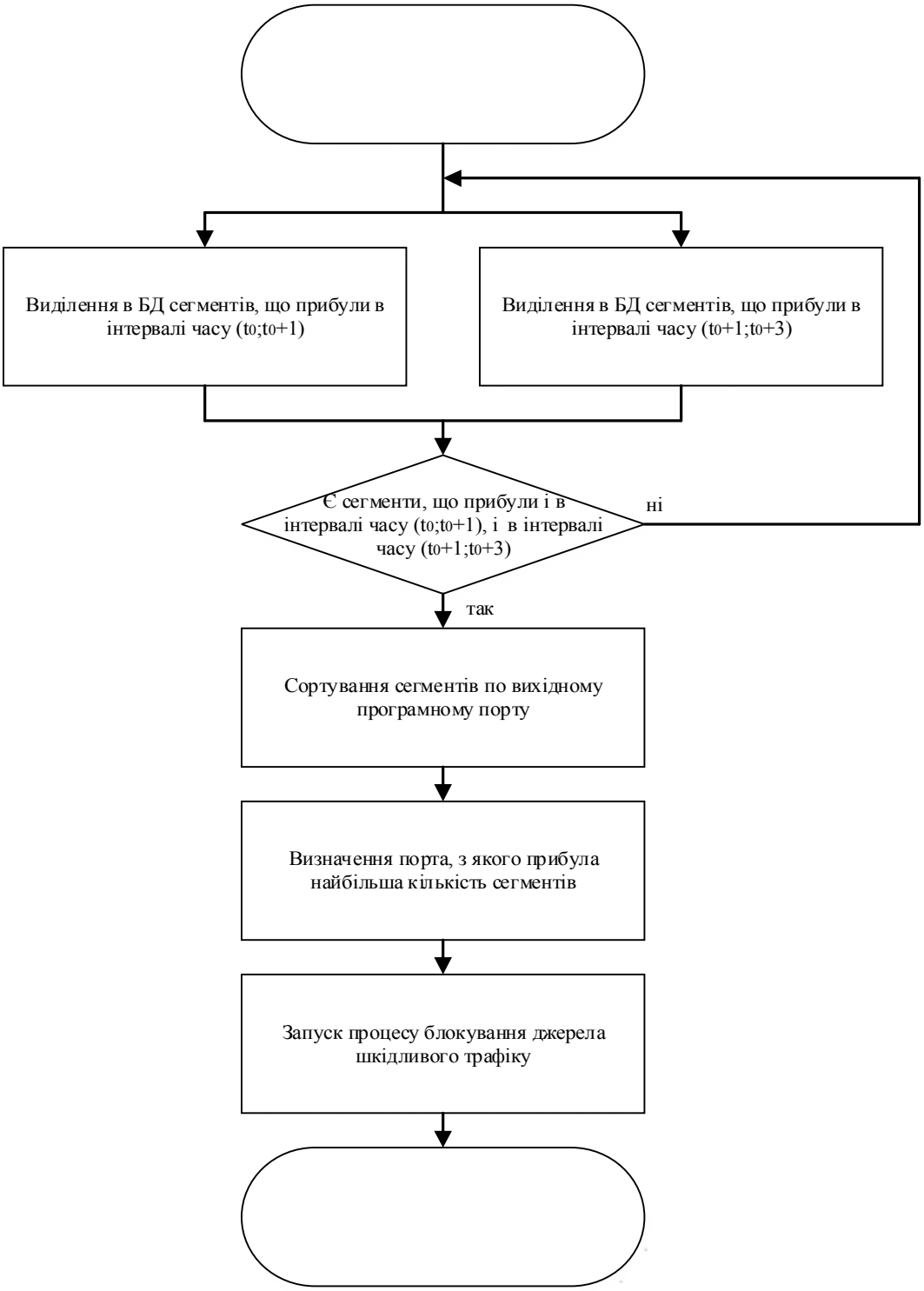

Рис. 4. Алгоритм виявлення джерел шкідливого трафіку

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ АГЕНТ-ОРИЕНТИРОВАННОЙ СИСТЕМЫ ВЫЯВЛЕНИЯ МЕДЛЕННОЙ DoS-АТАКИ

И.В. Рубан, Е.С. Лошаков

Предложена агент-ориентированная система выявления медленных DoS-атак, которая представляет собой программно-аппаратный комплекс, внедренный в информационно-телекоммуникационную систему.

Ключевые слова: *медленная DoS-атака, информационная безопасность, компьютерная преступность.*

THE TECHNOLOGY OF BUILDING AGENT-ORIENTED SYSTEM FOR SLOW-RATE DOS-ATTACK'S DETECTION

I.V. Ruban, Ye.S. Loshakov

The agent-oriented system for slow-rate DoS-attack's detection which is the program-device complex implemented to information-telecommunication system has been offered.

Keywords: *slow-rate DoS-attack, information security, computer crime.*