УДК 681.324

І.В. Рубан, Є.С. Лошаков

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

СИСТЕМА ПРОТИДІЇ ПОВІЛЬНІЙ DoS-АТАЦІ

Запропонована система протидії повільним DoS-атакам, 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 швидкого розвитку набувають інформаційні технології,які все більше починають проникати 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. Разом з тим, розвиваються засоби несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем, які 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 викликає стійку відмову в обслуговуванні легітимним користувачам, що обумовлюється особливостям функціонування протоколу TCP. Звідси витікає необхідність негайного її блокування після виявлення факту наявності даної атаки та джерел шкідливого трафіку.

Для цього пропонується застосовувати таку структуру інформаційно-телекомунікаційної системи, яка показана на рис. 1.

Рис. 1. Структура ІТКС, що забезпечує блокування повільної DoS-атаки

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.

Комутатор з'єднує робочі станції, що входять у склад інформаційно-телекомунікаційної системи та сервер з маршрутизатором та програмним шлюзом, що з'єднують систему з зовнішньою мережею.

Маршрутизатор є крайньою точкою інформаційно-телекомунікаційної системи та з'єднує останню з її зовнішніми користувачами.

Програмний шлюз застосовується при формуванні альтернативного шляху передачі інформації та маскування під сервер для переадресації на нього шкідливого трафіку з метою ізоляції від нього серверу та основного каналу зв'язку.

Ззовні інформаційно-телекомунікаційної системи знаходяться її легітимні користувачі та джерела шкідливого трафіку, що генерується з метою здійснення зловмисником повільної DoS-атаки. При чому генерування такого трафіку може здійснюватися як одною ЕОМ так і цілою мережею (botnet). Розглянемо графову модель роботи механізму блокування шкідливого трафіка, що представлена на рис. 2.

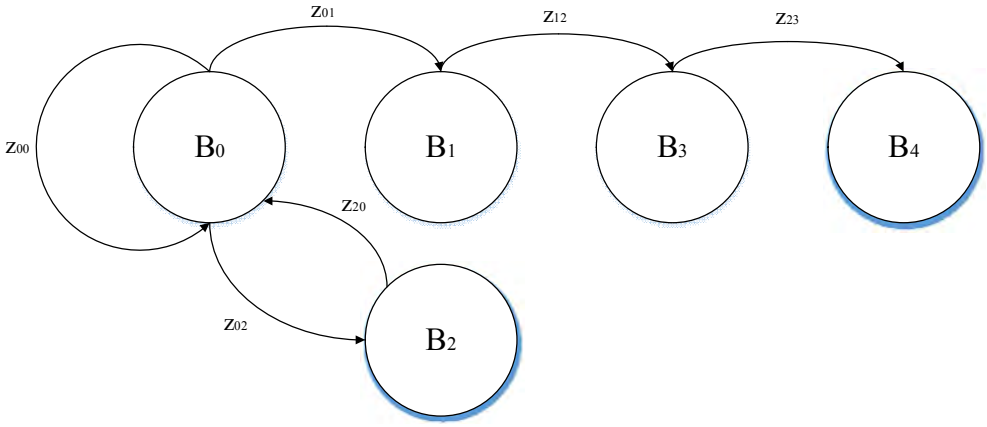

Рис. 2 Графова модель роботи механізму блокування шкідливого трафіка

Стан B_0 – в базі даних містяться джерела шкідливого трафіку.

Стан B_1 – зчитування з БД джерел шкідливого трафіку.

Стан B_2 – відключення порта комутатора, з якого надходить шкідливий трафік.

Стан B_3 – відправлення пакетів по запитах атакуючих на програмний шлюз.

Стан B_4 – підміна у вихідних пакетах вихідної адреси сервера на адресу програмного шлюзу.

Перехід z_{00}– в базі даних відсутні джерела шкідливого трафіку.

Перехід z_{01}– джерелами шкідливого трафіку є ЕОМ з зовнішньої мережі.

Перехід z_{02} – джерелом шкідливого трафіку є ЕОМ з внутрішньої мережі інформаційно-телекомунікаційної системи.

Перехід z_{20} – повернення до зчитування з бази даних джерел шкідливого трафіку.

Перехід z_{13}– почати відправлення пакетів по запитах атакуючих на програмний шлюз.

Перехід z_{34} – почати підміну у вихідних пакетах вихідної адреси сервера на адресу програмного шлюзу.

Алгоритм блокування джерел шкідливого трафіку представлений на рис. 3.

Таким чином, після виявлення джерел шкідливого трафіку здійснюється запуск механізму їх блокування.

З початку перевіряється наявність відповідних записів у базі даних. Після цього з'ясовується походження шкідливого трафіку.

Якщо джерелом є ЕОМ з внутрішньої мережі, проводиться відключення відповідного порта комутатора. Якщо джерело – ЕОМ з зовнішньої мережі, то проводиться зчитування з бази даних вихідних програмних портів, з яких приходить шкідливий трафік. Далі пакети-відповіді, що адресовані атакуючим, відправляються на програмний шлюз. На ньому проводиться підміна вихідної IP-адреси серверу на адресу програмного шлюзу. Це забезпечує маскування серверу і подальше адресування шкідливого трафіку на програмний шлюз, в той час, як легітимні користувачі системи продовжують обслуговуватися, обмінюючись даними з сервером через маршрутизатор.

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. Була запропонована система протидії повільним DoS-атакам, яка представляє собою програмно-апаратний комплекс, що впроваджений в інформаційно-телекомунікаційну систему. Дана система реалізує механізми: аналізу вхідного трафіка, виявлення джерел шкідливого трафіку та його блокування.

Так як джерелом шкідливого трафіку може бути не тільки зовнішній користувач, але й ЕОМ з внутрішньої мережі інформаційно-телекомунікаційної системи, тому передбачено два механізми блокування: внутрішнього джерела та зовнішнього.

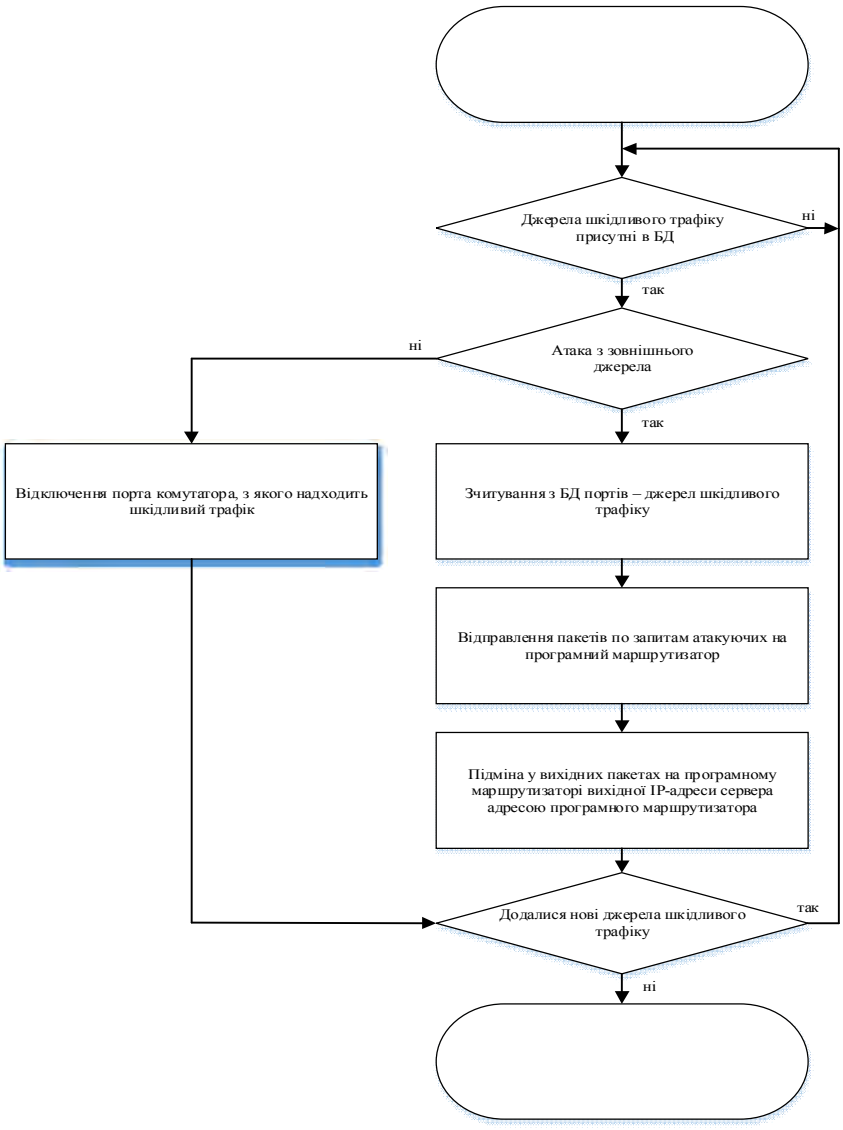

Рис. 3. Алгоритм блокування шкідливого трафіку

Список літератури

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

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

3. Атака из Internet / И.Д. Медведовский, Б.В. Семьянов, Д.Г. Леонов, А.В. Лукацкий. – М.: СОЛОН-Р, 2002. – 368 с.

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

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

6. Столингс В. Основы защиты сетей. Приложения и стандарты / Вильям Столлингс. – М.: Вильямс, 2002.– 432 с.

7. Эриксон Д. Хакинг: искусство эксплойта / Джон Эриксон. 2-е изд. – М.: Символ Плюс, 2009. – 510 с.

Надійшла до редколегії 25.02.2015

Рецензент: д-р техн. наук, проф. К.С. Смеляков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

СИСТЕМА ПРОТИВОДЕЙСТВИЯ МЕДЛЕННОЙ DoS-АТАКЕ

И.В. Рубан, Е.С. Лошаков

Предложена система противодействия медленным DoS-атакам, которая представляет собой программно-аппаратный комплекс, внедряемый в информационно-телекоммуникационную систему.

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

THE SYSTEM OF COUNTERACTION TO SLOW-RATE DoS-ATTACK

I.V. Ruban, Y.S. Loshakov

The system of counteraction to slow-rate DoS-attack which is the program-device complex implemented to information-telecommunication system has been offered.

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