

УДК 681.324

І.В. Рубан, Є.С. Лошаков, Д.В. Прибильнов

Харківський університет Повітряних Сил ім. Івана Кожедуба, Харків

## ОБҐРУНТУВАННЯ ВИБОРУ ІНТЕРВАЛУ СПОСТЕРЕЖЕННЯ ПРИ ОЧІКУВАННІ ПОВІЛЬНОЇ DOS-АТАКИ

*Проведено аналіз можливості реалізації повільної DoS-атаки. Обґрунтовано інтервал спостереження при очікуванні атаки даного типу та можливість її виявлення.*

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

### Вступ

**Постановка проблеми.** Кінець ХХ століття ознаменувався стрімким зростанням темпу розвитку інформаційних технологій та їх широким застосуванням у всіх сферах людської діяльності. З одного боку, це дало змогу суттєво збільшити продуктивність праці, а, з іншого, поклало початок такому виду злочинності, як інформаційна. З кожним роком з'являлися нові шляхи несанкціонованого доступу до конфіденційної інформації та порушення працездатності інформаційно-телекомунікаційних систем.

**Аналіз літератури** [1 – 8] показав, що існує велика кількість загроз інформаційній безпеці. Від більшості з них на даний час існують ефективні методи захисту. Однак методу, що дає змогу ефективно протидіяти повільній DoS-атаці, не існує.

### Основна частина

Можливість реалізації повільної DoS-атаки обумовлюється особливостями роботи протоколу TCP, а

саме механізму тайм-ауту та повторної передачі пакету. Цей механізм працює наступним чином: після відправлення пакету очікується пакет-відповідь протягом інтервалу часу RTO (Retransmission TimeOut). Якщо пакет-відповідь не приходить у продовж цього інтервалу часу, виконується повторна передача пакету, а RTO збільшується таким чином:

$$t_{n+1} = t_n + 2t_n, \quad t_1 = 1, \quad n = \overline{1, k}. \quad (1)$$

Цю особливість використовує зловмисник для реалізації атаки. Він відправляє імпульс трафіку в кінці інтервалу RTO. Внаслідок цього, канал зв'язку переповнюється в момент, коли надходять пакети-відповіді, в зв'язку з цим вони не отримуються. Далі він повторює свої дії. Таким чином, виникає стійка непрацездатність системи. Графічне представлення повільної DoS-атаки, отримане при її експериментальному дослідженні, представлено на рис. 1.

Як видно з рис. 1, піки трафіку доходять до 100% завантаженості каналу зв'язку і з'являються з інтервалами 1, 3, 9, 27 та 81 секунда, що відповідає виразу (1).

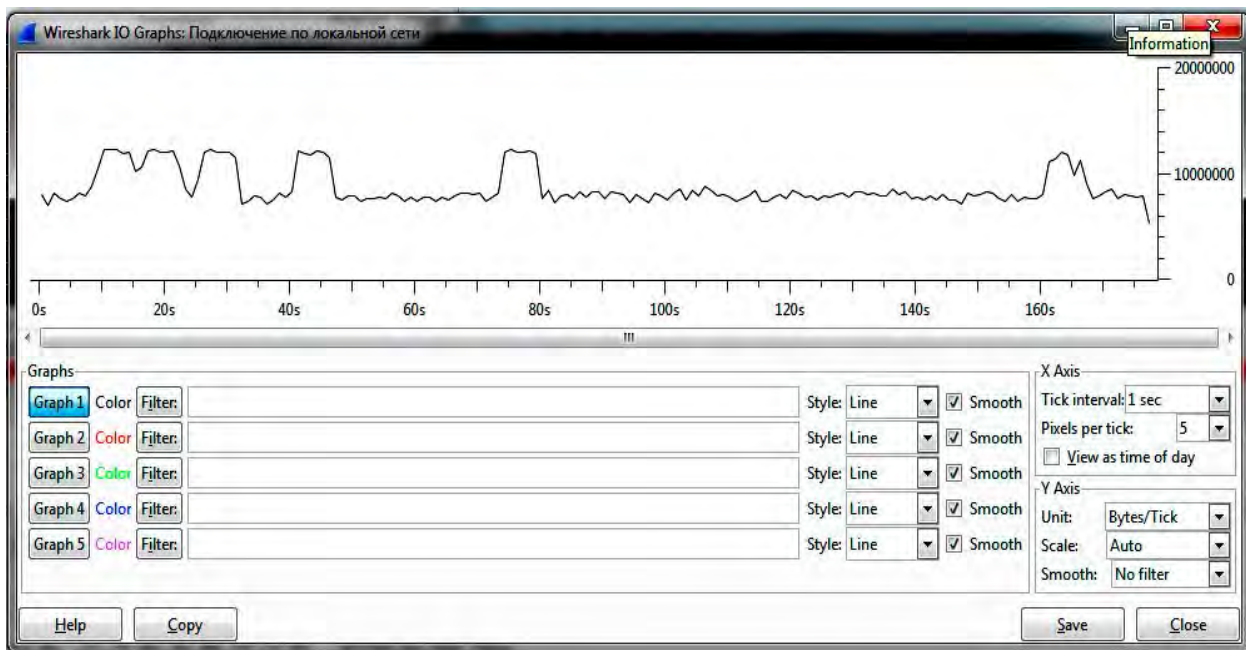


Рис. 1. Графічне представлення повільної DoS-атаки

Фундаментальною можливістю виявлення повільних DoS-атак може бути побудова контрольних характеристик трафіку при штатному режимі з максимальною завантаженістю мережі та подальше виявлення аномалій в структурі трафіку. Під аномалією розуміється подія, що характеризується відхиленням від стандартної структури трафіку, отриманої раніше. Але аномалія ще не говорить про те, що йде атака. Для прийняття рішення про наявність атаки необхідний аналіз отриманої аномалії. При повільних DoS-атаках аномалії будуть мати вигляд короткочасних сплесків трафіку, як показано на рис. 1.

Отримання декількох піків трафіку з вказаними інтервалами однозначно свідчить про те, що йде повільна DoS-атака. Однак інтервал часу, за який проходить один цикл атаки, досить великий. Тому очікувати так довго, щоб зробити висновок про наявність повільної DoS-атаки, нерационально і небезпечно з точки зору нормальної працездатності системи. Звідси витікає необхідність вибору меншого інтервалу часу спостереження.

Розглянемо інтервал завантаження каналу зв'язку від нуля до максимального, отриманого експериментально. Використовуючи нерівність Чебишева, знайдемо ймовірність того, що завантаження каналу в будь-який довільний момент часу потрапить в цей інтервал:

$$P(|X - a| \leq \varepsilon) \geq 1 - \frac{D(X)}{\varepsilon^2}, \quad (2)$$

де  $X$  – випадкова величина,  $a = M(X)$  – математичне сподівання випадкової величини  $X$ ,  $\varepsilon > 0$ .

Стосовно до нашого випадку  $X = C$  – завантаження каналу зв'язку в довільний момент часу,  $a = M(C)$  – математичне сподівання завантаження каналу зв'язку,  $\varepsilon = C_{\max}$  – максимальне завантаження каналу зв'язку. Однак, нам необхідно оцінити  $P(C \leq C_{\max})$  – ймовірність того, що завантаження каналу зв'язку в довільний момент часу не перевищує максимальне. Але для того, щоб використати нерівність Чебишева для оцінки цієї ймовірності необхідно визначити нижню границю інтервалу  $C_0$ , яка повинна бути симетрична максимальному значенню завантаження каналу зв'язку  $C_{\max}$  відносно математичного очікування  $M(C)$ . Тому перейдемо до оцінки ймовірності потрапляння випадкової величини  $C$  до інтервалу  $[C_0; C_{\max}]$ , тобто ймовірності того, що завантаження каналу зв'язку  $C$  в довільний момент часу не перевищить максимальне  $C_{\max}$  та не буде меншим  $C_0$ , для визначення якого використаємо наступний вираз:

$$C_0 = 2M(C) - C_{\max}. \quad (3)$$

Далі для оцінки  $P(C_0 < C \leq C_{\max})$  необхідно перейти до стандартного виду нерівності Чебишева.

Віднімемо від кожного члена нерівності математичне очікування  $M(C)$ . Отримаємо:

$$P(C_0 - M(C) < C - M(C) \leq C_{\max} - M(C)). \quad (4)$$

Так як значення  $C_0 - M(C)$  та  $C_{\max} - M(C)$  рівні за абсолютним значенням, маємо:

$$P(|C - M(C)| \leq C_{\max} - M(C)). \quad (5)$$

Нерівність Чебишева приймає вигляд:

$$P(|C - M(C)| \leq C_{\max} - M(C)) \geq 1 - \frac{D(C)}{(C_{\max} - M(C))^2}. \quad (6)$$

Тоді маємо наступний вираз для оцінки ймовірності того, що завантаження каналу зв'язку в довільний момент часу не перевищує максимальне:

$$P(C_0 < C \leq C_{\max}) \geq 1 - D(C) / (C_{\max} - M(C))^2. \quad (7)$$

Проведено експериментальне дослідження роботи інформаційно-телекомунікаційної системи спеціального призначення в режимі граничного завантаження каналу зв'язку. Було визначено максимальне значення завантаженості каналу зв'язку, яке склало 68%, математичне сподівання, яке склало 52,3% та дисперсію, що склала 14,6%.

Використовуючи вираз (7), знайдемо ймовірність того, що завантаженість каналу зв'язку інформаційно-телекомунікаційної системи  $C$  не перевищить  $C_{\max}$ :

$$P(C_0 < C \leq 68) \geq 1 - \frac{14,6}{(68 - 52,3)^2} \geq 0,94. \quad (8)$$

Тоді ймовірність аномалії, в тому числі піку трафіку, характерного для повільної DoS-атаки,  $P_a \leq 0,06$ . А ймовірність отримання двох піків за короткий проміжок часу буде дорівнювати  $P_a^2$  і складає менше 0,0036.

Тому, отримавши два піки трафіку з інтервалом близько 1 секунди, можна зробити висновок, що почалася повільна DoS-атака.

## Висновки

Таким чином, з розвитком інформаційних технологій постійно з'являються нові шляхи несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем. Одним з таких шляхів є повільна DoS-атака, яку дуже важко виявити в наслідок того, що канал зв'язку переповнюється тільки в певні моменти часу. Але це є суттєвою небезпечкою, тому що призводить до стійкої непрацездатності інформаційно-телекомунікаційної мережі. Можливим шляхом виявлення даного типу атак є моніторинг трафіку системи на предмет наявності характерних для повільної DoS-атаки піків трафіку. Як було показано вище, достатньо отримати два таких піки з інтервалом близько 1 секунди, щоб зробити висновок про наявність повільної DoS-атаки.

## Список літератури

1. Касперски Крис. Техника сетевых атак / Крис Касперски. – М.: СОЛОН-Р, 2001. – 304 с.
2. Касперски Крис. Компьютерные вирусы изнутри и снаружи / Крис Касперски. – СПб.: Питер, 2006. – 526 с.
3. Медведовский И.Д. 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. Столлингс Вильям. Основы защиты сетей. Приложения и стандарты / Вильям Столлингс. – М.: Вильямс, 2002. – 432 с.

6. Жуков Юрий. Основы веб-хакинга. Нападение и защита / Юрий Жуков. – СПб.: Питер, 2006. – 208 с.
7. Норткат Стивен. Обнаружение нарушений безопасности в сетях / Стивен Норткат, Джуди Новак. – М.: Вильямс, 2003. – 448 с.
8. Эриксон Джон. Хакинг: искусство эксплойта. 2-е издание / Джон Эриксон. – М.: Символ Плюс, 2009. – 510 с.
9. Шремер Н.Ш. Теория вероятностей и математическая статистика / Н.Ш. Шремер. – М.: Юнити, 2004. – 576 с.

Надійшла до редколегії 28.08.2014

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

## ОБОСНОВАНИЕ ВЫБОРА ИНТЕРВАЛА НАБЛЮДЕНИЯ ПРИ ОЖИДАНИИ МЕДЛЕННОЙ DoS-АТАКИ

И.В. Рубан, Е.С. Лошаков, Д.В. Прибыльнов

*Проведен анализ возможности реализации медленной DoS-атаки. Обоснован интервал наблюдения при ожидании атаки данного типа и возможность ее выявления.*

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

## JUSTIFICATION OF THE CHOICE OF THE OBSERVATION INTERVAL OF WAITING SLOW-RATE DOS-ATTACKS

I.V. Ruban, Y.S. Loshakov, D.V. Pribilnov

*Analysis of the capabilities of realization of slow-rate DoS-attack has carried out. The observation interval of waiting for this type of attack and the possibility of identifying has justified.*

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