УДК 681.324

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

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

АНАЛІЗ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В РЕЖИМІ ГРАНИЧНОЇ ЗАВАНТАЖЕНОСТІ КАНАЛУ ЗВ'ЯЗКУ

Проведено аналіз показників ефективності функціонування інформаційно-телекомунікаційної системи при граничному завантаженні її каналу зв'язку. Обрано показник, дані моніторингу якого пропонується застосовувати для пошуку можливостей виявлення повільних атак типу «відмова в обслуговуванні».

Ключові слова: *інформаційно-телекомунікаційна система, інформаційна безпека, завантаженість каналу зв'язку.*

Вступ

Постановка проблеми. Стрімкий розвиток інформаційних технологій та їх широке застосування в усіх сферах людської діяльності дали поштовх для виникнення нового виду злочинності – інформаційної. Поява нових шляхів несанкціонованого доступу до конфіденційної інформації та порушення працездатності інформаційно-телекомунікаційних систем йде паралельно з розвитком інформаційних технологій.

Аналіз літератури [1 – 8] показав, що на теперішній час існує велика кількість загроз інформаційній безпеці, суттєва кількість яких направлена на порушення працездатності інформаційно-телекомунікаційних систем шляхом переповнення каналів зв'язку цих систем. Звідси виникає необхідність аналізу показників ефективності функціонування інформаційно-телекомунікаційних систем з метою виявлення зовнішніх інформаційно-кібернетичних впливів.

Основна частина

Будь-яка інформаційно-телекомунікаційна система спеціального призначення створена для виконання своїх специфічних функцій. Виходячи з цього, можна виділити такі режими роботи ІТС, як робота в умовах низького завантаження, нормальна

робота та робота в умовах граничного завантаження. З точки зору інформаційної безпеки цікавим є режим роботи системи при граничному завантаженні. Детальний аналіз показників ефективності функціонування інформаційно-телекомунікаційної системи при роботі в даному режимі є необхідним для виявлення розповсюджених типів DoS-атак, що є суттєвою загрозою інформаційній безпеці будь-якої інформаційно-телекомунікаційної системи.

Розглянемо основні показники ефективності функціонування ІТС. У загальному випадку показник ефективності функціонування інформаційно-телекомунікаційної системи являє собою кількісну (рідше якісну) характеристику з урахуванням: вихідних часових, точнісних та надійнісних показників трудової діяльності людини-оператора (користувачів, управлінського та обслуговуючого персоналу системи); параметрів і характеристик машини (апаратних, програмних та інформаційних засобів системи); параметрів і характеристик, що визначають умови функціонування ІТС.

Показники ефективності інформаційно-телекомунікаційної системи визначаються процесами її функціонування і розділяються на три групи:

показники цільової ефективності функціонування ІТС або ефективності використання мережі за цільовим призначенням;

показники технічної ефективності ІТС;

показники економічної ефективності функціонування ІТС.

З точки зору інформаційної безпеки цікавими є показники технічної ефективності інформаційно-телекомунікаційної-системи. Показники цієї групи використовуються для оцінки ІТС як складної апаратно-програмно-інформаційної кібернетичної людино-машинної системи при роботі її в різних режимах і умовах. Оцінка може здійснюватися як всієї системи, так і окремих її підсистем, ланок і вузлів. Такими показниками є:

сумарна затримка в ІТС, тобто час доставки повідомлення від відправника до одержувача. Ця затримка залежить від довжини маршруту, швидкості передачі електричних сигналів, що несуть інформацію, пропускної здатності каналу зв'язку, часу на прийом, обробку та передачу інформації в кожному проміжному вузлі;

швидкість передачі пакетів, тобто кількість пакетів, переданих через ІТС за одиницю часу;

фактична пропускна здатність ІТС, тобто середній потік даних, фактично переданих через систему. На відміну від фізичної пропускної здатності каналу або лінії зв'язку, яка визначається можливостями і властивостями середовища передачі, фактична пропускна здатність визначається також багатьма іншими факторами, а саме: використовуваними методами доступу в середу передачі, завантаженням каналу, затримкою інформації, що передається, в проміжних вузлах зв'язку і т.д.

інтегральна пропускна здатність ланки мережі на відрізку часу. Вона представляє собою відношення кількості запитів, що були обслужені, до загальної кількості отриманих запитів і показує, як в середньому ланка мережі справляється з обслуговуванням вхідного потоку запитів від моменту початку відліку до деякого довільного моменту часу (наприклад, за зміну, добу, місяць).

динамічна пропускна здатність ланки мережі, що представляє собою відношення кількості запитів, які були обслужені за певний короткий проміжок часу, до загальної кількості запитів, отриманих в цьому же інтервалі часу. Динамічна пропускна здатність дозволяє судити про те, як ланка мережі справляється з обслуговуванням вхідного потоку запитів на будь-якому заданому (найбільш характерному) відрізку часу. Вона дає можливість відслідковувати роботу ланки системи в динаміці і виробляти рекомендації щодо забезпечення стабільності її функціонування;

середній час реакції ланки мережі на запит користувача. Він складається з часу очікування обслуговування запиту і часу власне обслуговування. Цей показник дуже важливий для оцінки ефективності системи при роботі в інтерактивному режимі;

максимально можливе число активних абонентів, тобто абонентів, що звертаються із запитами на обслуговування в даний момент часу;

коефіцієнт затримки обслуговування абонентів. Це відношення середнього часу реакції на запит абонента при максимальній кількості активних абонентів до цього ж часу при мінімальній їх кількості;

завантаженість каналу зв’язку в довільний момент часу,тобто відношення швидкості передачі пакетів в цей момент часу до фізичної пропускної здатності каналу.

Вищевказані показники ефективності функціонування ІТС можуть бути використані при виявленні інформаційно-телекомунікаційних впливів на дану систему.

Так, для виявлення повільної атаки типу «відмова в обслуговуванні» (DoS-атака), що реалізуються шляхом переповнення каналу зв’язку системи в певні моменти часу,пропонується проводити моніторинг його завантаженості з метою подальшого порівняння отриманих даних з раніше зібраними статистичними в режимі граничної завантаженості.

Для отримання статистичних даних необхідно обрати інтервал часу, впродовж якого буде збиратися інформація про завантаженість каналу зв’язку, а також період дискретизації, який визначає моменти часу, в які знімаються значення завантаженості каналу зв’язку. І далі переходити до обробки цієї інформації з метою обчислення ймовірнісних харак-

теристик, а саме математичного очікування завантаження каналу зв'язку M(C) та дисперсії D(C), а також визначення максимальної завантаженості каналу зв'язку C_{max}.

Маючи множину значень завантаженості каналу зв'язку $c_i \in C$, $i = \overline{1,k}$ обчислимо математичне очікування:

$$M(C) = \sum_{i=1}^{k} c_i p_i . \quad (1)$$

Ймовірності кожного і-го значення завантаженості каналу зв'язку знаходяться наступним чином:

$$p_i = \frac{k}{n}, \quad (2)$$

де k – кількість з'явлень і-го значення завантаженості каналу зв'язку;

n – загальна кількість значень завантаженості каналу зв'язку.

Знайдемо дисперсію завантаженості каналу зв'язку:

$$D(C) = \sum_{i=1}^{k} (c_i - M(C))^2 p_i . \quad (3)$$

Визначимо максимальне значення завантаженості каналу зв'язку:

$$C_{max} = \max c_i . \quad (4)$$

Отримавши математичне очікування, дисперсію та максимальне значення завантаженості каналу зв'язку інформаційно-телекомунікаційної системи спеціального призначення при роботі в режимі граничної завантаженості, можна перейти до обґрунтування інтервалу спостереження при очікуванні повільної DoS-атаки, що є актуальною задачею, так як дозволить виробити метод виявлення даного типу атак.

Висновки

Таким чином, з розвитком інформаційних технологій з'являються нові шляхи несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем. Одними з найпоширеніших типів загроз є атаки, що спрямовані на відмову в обслуговуванні легітимним користувачам. Це досягається переповненням каналу зв'язку інформаційно-телекомунікаційної системи як на всьому інтервалі часу, так і в певні моменти (повільна DoS-атака). Було проведено аналіз показників ефективності функціонування ІТС з метою виділення таких, що можуть бути застосовані для виявлення повільних DoS-атак. Обрано показник завантаженості каналу зв'язку як такий, що може використовуватися для виявлення даного типу атак. Разом з цим, для пошуку можливостей виявлення повільних DoS-атак необхідно мати певні статистичні дані роботи системи в режимі граничної завантаженості.

Такими даними є математичне очікування, дисперсія та максимальне значення завантаженості каналу зв'язку інформаційно-телекомунікаційної системи.

Список літератури

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

2. Крис Касперски. Компьютерные вирусы изнутри и снаружи / Касперски Крис. – 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. Жуков Ю. Основы веб-хакинга. Нападение и защита / Юрий Жуков. – СПб.: Питер, 2006. – 208 с.

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

6. Норткат С. Обнаружение нарушений безопасности в сетях / Стивен Норткат, Джуди Новак. – М.: Вильямс, 2003. – 448 с.

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

8. Шремер Н.Ш. Теория вероятностей и математическая статистика / Н.Ш. Шремер. – М.: Юнити, 2004. – 576 с.

Надійшла до редколегії 24.07.2014

Рецензент: д-р техн. наук, с.н.с. О.О. Можаєв, Національний технічний університет «ХПІ», Харків.

АНАЛИЗ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ В РЕЖИМЕ ПРЕДЕЛЬНОЙ ЗАГРУЗКИ КАНАЛА СВЯЗИ

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

Проведен анализ показателей эффективности функционирования информационно-телекоммуникационной системы при предельной загрузке ее канала связи. Выбран показатель, данные мониторинга которого предлагается применять для поиска возможностей выявления медленных атак типа «отказ в обслуживании».

Ключевые слова: *информационно-телекоммуникационная система, информационная безопасность, загрузка канала связи.*

ANALYSIS OF THE FUNCTIONING'S PERFORMANCE INDICATORSOF THE TELECOMMUNICATION SYSTEM WITH THE LIMIT LOADING LINK MODE

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

Analysis of the functioning's performance indicators of telecommunication system with the limit loading link mode has carried out. Indicator which was of fered to apply for searching opportunities of detection slow-rate denial of service attacks has chosen.

Keywords: *telecommunication system, information security, link loading.*