

8. Matsui, K. Digital signature on a facsimile document by recursive MH coding / K. Matsui, K. Tanaka and Y. Nakamura // Symposium On Cryptography and Information Security, 1989.

9. Osborne, C. A Digital Watermark / C. Osborne, R. van Schyndel, A. Tirkel // IEEE Intern. Conf. on Image Processing. – 1994. – P. 86–90.

10. Ramkumar, M. Data Hiding in Multimedia. PhD Thesis / M. Ramkumar. – New Jersey Institute of Technology, 1999.

11. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York / B. Schneier. – John Wiley and Sons, 1996.

12. Simmons, G. The History of Subliminal Channels / G. Simmons // IEEE Journal on Selected Areas of Communications. – 1998. – Vol. 16. – № 4. – P. 452–461.

13. Simmons, G. The prisoner's problem and the subliminal channel / G. Simmons // Proc. Workshop on Communications Security (Crypto'83). – 1984. – P. 51–67.

14. Voloshynovskiy, S. Attack Modelling: Towards a Second Generation Watermark Benchmark / [S. Voloshynovskiy et al.] // Preprint. University of Geneva, 2001.

УДК 621.395

В. Л. Тамп, Н. В. Тамп

Череповецкое высшее военное инженерное училище радиоэлектроники,

А. А. Кузьмин

Череповецкий государственный университет

ИМИТАЦИОННАЯ МОДЕЛЬ ПОТОКОВ ЗАПРОСОВ НА ПЕРЕДАЧУ КАДРОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

В статье приводится описание и алгоритм имитационной модели, позволяющей формировать потоки запросов на передачу кадров в информационно-вычислительную сеть (ИВС). Предложенная модель позволяет проводить исследования ИВС для различных ситуаций, возникающих в процессе сетевых атак. Показано, что ее использование позволяет осуществлять имитацию как стандартных, так и аномальных ситуаций, возникающих в ИВС. Модель предназначена для исследования возможных путей повышения информационной безопасности вычислительных сетей.

Интенсивность, экспоненциальный закон, поток запросов, ИВС, информационная безопасность.

The article provides the algorithm and simulation model that allows to generate streams of requests for the frame transfer to the IT system. The suggested model allows the study information and computing networks, for different situations that arise during network attacks. It is shown that its use can simulate both standard and abnormal situations arising in IT system. The model is intended to explore possible ways to improve the information security of computer networks.

Intensity, exponential law, the flow of requests, information networks, information security.

Введение.

Мониторинг информационно-вычислительных сетей показывает, что участились сетевые атаки типа «отказ в обслуживании» (*Denial of service – DoS*) различных модификаций. Существующие алгоритмы, реализованные в современных анализаторах протоколов, не обеспечивают оперативное обнаружение ряда модификаций DoS-атак. В связи с этим возникает необходимость поиска новых подходов для своевременного обнаружения атак на центральный сетевой сервер.

Известно, что разные сетевые атаки вызывают различия аномального поведения ИВС [1]. Исследование этих различий, на наш взгляд, способствует улучшению распознавания типа атаки алгоритмами анализаторов протоколов, т. е. повышают информационную безопасность сети.

Для исследования ситуаций, возникающих при сетевой атаке, предлагается имитационная модель, предназначенная формировать потоки запросов на передачу кадров в ИВС.

Известно, что алгоритмы имитационного моделирования сетевого трафика могут использовать следующие подходы [1], [4]:

– классические модели потоков, применяемые в теории массового обслуживания (экспоненциальный и пуассоновский законы распределения);

– модулированные случайные процессы (гауссов закон распределения);

– потоки с учетом статистического самоподобия сетевого трафика (фрактальные модели);

– последовательности по образцу реального трафика.

Имитационную модель сетевого трафика предлагается строить, используя параметры реального трафика.

Проводились исследования реального потока кадров, для чего фиксировались моменты времени приема каждого кадра. Объем выборки составлял 2000 значений. Гистограмма распределения длительностей между моментами начала передачи соседних кадров показана на рис. 1. Видно (а также доказывается аналитически), что полученная гистограмма аппроксимируется экспоненциальным законом распределения.

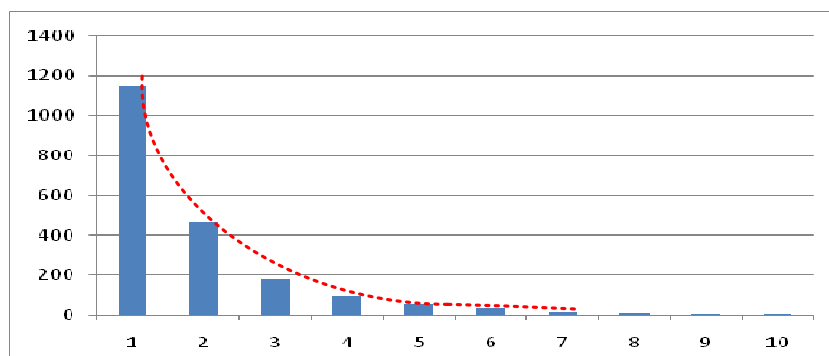


Рис. 1. Гистограмма распределения временных интервалов между моментами передачи соседних кадров

Таким образом, при построении имитационной модели формирования моментов запросов на передачу кадров в сети можно использовать классический подход, использующий экспоненциальный закон их распределения. При постоянном параметре интенсивности λ формируемый поток является стационарным и ординарным.

Многообразие различных ситуаций, возникающих при атаках, определяет необходимость работы модели в различных режимах, отображающих возникающие воздействия на сеть. Предложено проводить исследование сетевого трафика без учета полей форматов протокольных блоков данных (ПБД), основываясь только на последовательности моментов запросов на передачу сообщений в сети.

В настоящее время существует ряд алгоритмов моделирования сетевого трафика, которые, как правило, имитируют работу отдельных пользователей для конкретных стеков протоколов с учетом соответствующих форматов ПБД [3], [4]. Предложенный алгоритм имитационного моделирования позволяет формировать последовательности моментов запросов на передачу кадров в ИВС независимо от используемых протоколов. В нем представляется возможность выбора ряда характеристик модели сетевого трафика при DoS-атаках, например:

- включение (отключение) корреспондентов сети;
- увеличение (уменьшение) интенсивности формируемых потоков запросов;
- изменения интенсивности по заданному закону и т. д.

В связи с тем, что основная цель исследования динамических характеристик заключается в выявлении аномальных ситуаций, происходящих в сети при DOS-атаках, то предложено формировать суммарный поток запросов на основе использования участков локальной стационарности с разными параметрами интенсивности. На рис. 2 представлен алгоритм формирования потоков запросов на передачу кадров в ИВС, реализованный в имитационной модели. Алгоритм реализован в виде программы в среде Delphi 7. Особенность разработанного алгоритма заключается в том, что он:

- позволяет формировать необходимое количество потоков запросов корреспондентов;
- допускает объединение всех потоков запросов корреспондентов в суммарный поток по методу суперпозиции;

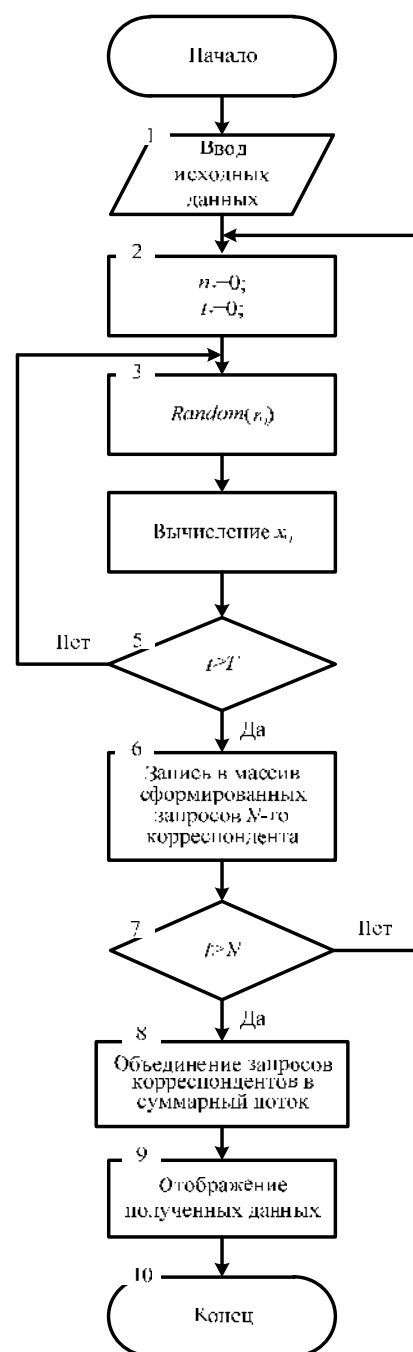


Рис. 2. Алгоритм работы имитационной модели

- обеспечивает изменение интенсивности потока в процессе формирования запросов;
- позволяет выбирать закон изменения интенсивности запросов для заданного корреспондента;
- разрешает задавать время генерации потока запросов корреспондентов.

В роли исходных данных для моделирования выступают:

- количество формируемых корреспондентами потоков, объединенных в общий поток запросов;
- время включения и выключения корреспондентов;
- интенсивность λ_i с заданным значением и законом ее изменения $f_i(\lambda)$ для каждого i -го корреспондента;
- интервал участка локальной стационарности Δt_j ;
- время генерации потока запросов T .

Процесс моделирования потока запросов происходит в несколько этапов:

1. На первом этапе происходит генерация случайного числа, значения которого располагаются в интервале $[0,1)$.

Для формирования потока запросов необходимо генерировать данные, которые будут выступать в виде последовательности случайных чисел. Так как сетевой трафик состоит из потока отдельных дискретных информационных элементов (кадры), то математически он описывается при помощи точечного процесса, состоящего из последовательности величин $T_0, T_1, \dots, T_n, \dots$ ($T_0=0$), которые являются моментами поступления информационных элементов, т. е. моментами запросов на передачу кадров.

При имитационном моделировании учитывалось, что моменты запросов на передачу кадров в исследуемом канале ИВС являются случайным процессом и подчиняются экспоненциальному закону распределения с плотностью распределения λ [4]

$$f(x) = \lambda e^{-\lambda x}, x \geq 0, \lambda > 0.$$

Таким образом, результатом моделирования являются сформированные случайные потоки запросов на передачу пакетов различных абонентов сети с заданной интенсивностью.

2. На втором этапе вычисляются моменты запросов на передачу кадра у всех корреспондентов.

В ходе моделирования использовалась формула вычисления случайных чисел с экспоненциальным распределением вида

$$x_n = -\frac{1}{\lambda} \ln r_n,$$

где λ – задаваемая интенсивность потока, r_n – случайное число, равномерно распределенное в интервале $[0, 1)$. Результат расчета моментов запросов одного корреспондента, рассчитанный с помощью модели, приведен на рис. 3.

3. На третьем этапе происходит объединение всех значений сформированных запросов в общий поток. Результатом является суммарный поток запросов, сформированный по методу суперпозиции из запросов всех корреспондентов сети на передачу пакетов. На рис. 4 показан пример расчета суммарного потока запросов с помощью модели.

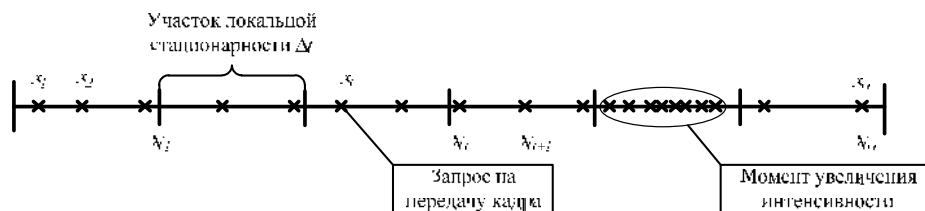


Рис. 3. Пример формирования моментов запросов корреспондента

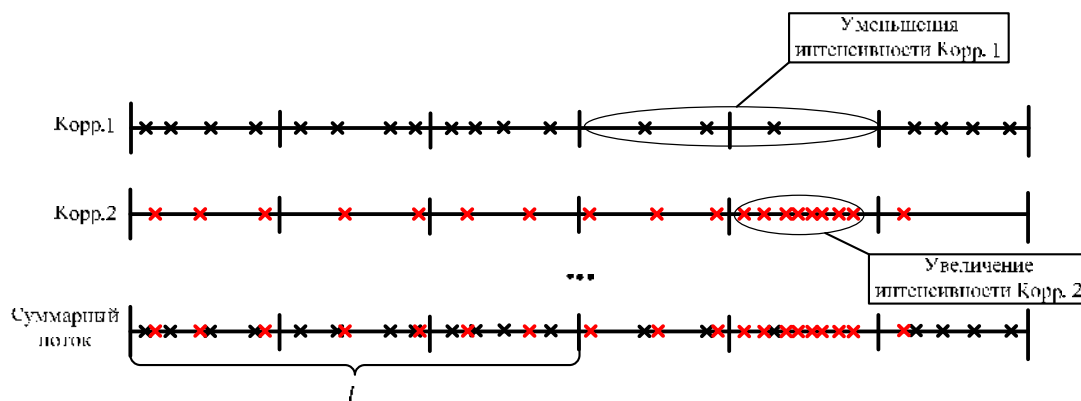


Рис. 4. Суммарный поток запросов, сформированного по методу суперпозиции от запросов корреспондентов сети

В модели с помощью участков локальной стационарности с разными параметрами интенсивности имитируются нестационарные потоки, представляющие собой совокупность сформированных участков.

4. На заключительном этапе результаты моделирования записываются в файл и отображаются в графическом виде на экране монитора ПЭВМ. Результат моделирования – потоки запросов на передачу кадров корреспондентов сети и их объединение в суммарный поток. Сформированные потоки запросов представляют собой, по сути, временные ряды, состоящие из запросов на передачу от K корреспондентов с возможностью изменения интенсивности потока запросов у каждого корреспондента.

Выводы.

Разработанная модель позволит проводить исследование ИВС для различных ситуаций, возникающих в процессе воздействия модифицированных DoS-атак. С ее помощью появляется возможность формирования сетевого трафика с заданными характеристиками.

Таким образом, имитационная модель формирует последовательности моментов запросов на передачу кадров в магистральном канале СЛС с заданным законом изменения интенсивности, обладающие свойствами ординарности и нестационарности. Использование модели позволит осуществлять имитацию как стандартных, так и аномальных ситуаций, встречающихся в ИВС. Один из вариантов предусматривает формирование эталонных ситуаций, возникающих при сетевой атаке в реальной обстановке, что может быть использовано для повышения информационной безопасности сети.

Литература

1. Брэгг, Р. Безопасность сетей / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М., 2006.
2. Вентцель, Е. С. Исследование операций / Е. С. Вентцель. – М., 1972.
3. Добровольский, Е. В. Моделирование сетевого трафика с использованием контекстных методов / Е. В. Добровольский, О. Л. Нечипорук. – Одесса, 2005.
3. Шелухин, О. И. Моделирование информационных систем / О. И. Шелухин, А. М. Тенякшев, А. В. Осин. – М., 2005.

УДК 536.24

Н. В. Телин

Череповецкий государственный университет

КИНЕТИКА НАКИПЕОБРАЗОВАНИЯ НА ПОВЕРХНОСТИ ТЕПЛООБМЕНА

В статье предложен единый подход к оценке кинетики кристаллизации накипеобразователей на поверхности теплообмена. Разработана методика оценки образования накипи на теплообменных поверхностях тепломеханического оборудования.

Кинетика, кристаллизация, теплоноситель, теплообмен, нагрев, охлаждение, накипеобразование, накипь, тепломеханическое оборудование.

In the article a unified approach of evaluation of crystallization kinetics formation of scale on the heat transfer surface is suggested. Method for estimation of scale formation on heat transfer surfaces of mechanical equipment is developed.

Kinetics, crystallization, heat transfer material, heat transfer, heating, cooling, scaling, scale, thermal and mechanical equipment.

Введение.

При использовании теплоносителей, содержащих растворенные соли и газы, на поверхности теплообмена ответственных элементов тепломеханического оборудования образуются отложения. Непрерывно растущий на поверхности теплообмена слой отложений, имеющий высокие механические свойства и низкий коэффициент теплопроводности, снижает интенсивность теплопередачи и нарушает гидравлический режим тепломеханического оборудования, что является основной причиной повреждения экранированных труб паровых и водогрейных котлов.

Экспериментальное изучение процессов образования отложений на поверхностях теплообмена ответственных элементов тепломеханического оборудования является довольно сложной задачей, поэтому их теоретическое изучение становится наиболее предпочтительным. Однако практическая реализация

предлагаемых на настоящее время расчетных соотношений связана с необходимостью экспериментального определения коэффициента скорости накипеобразования [1]. Кроме того, при разработке математических моделей отсутствует ясность в факторах, определяющих интенсивность процесса образования отложений. В работе [2], например, показано, что определяющим фактором процесса выпадения солей жесткости на поверхности нагрева является предел растворимости солей при соответствующей температуре. Скорость процесса определяется значением местной тепловой нагрузки во второй степени. Другие авторы считают, что масса отложений на поверхности теплообмена может быть пропорциональна плотности теплового потока в первой, второй и, как предполагается, другой, более высокой, степени. В данной работе предпринята попытка выработать