УДК 623.624

Оператор преобразования трафика для преднамеренного повышения структурной сложности информационных потоков

Макаренко С. И., Коровин В. М., Ушанев К. В.

Постановка задачи. *Развитие теории информационной безопасности и информационного противоборства требует формирования новых информационно-технических воздействий (ИТВ). Эти новые воздействия могут использоваться для тестирования устойчивости и безопасности телекоммуникационных систем, а также для разработки способов их защиты. Наиболее распространенным типом ИТВ на телекоммуникационные системы являются удаленные сетевые атаки. Проведенный анализ способов обнаружения удаленных сетевых атак показал, что в подавляющем большинстве случаев такое обнаружение основано на анализе интенсивности трафика в сети. Новые ИТВ, обладающие свойством бескомпроматности и скрытности, должны обеспечивать неизменность интенсивности трафика при проведении удаленной атаки. К таким ИТВ можно отнести атаки, ориентированные на усложнение структуры трафика. Они основаны на известных фактах снижения своевременности функционирования маршрутизаторов, при обработке в них трафика сложной структуры в десятки раз. Вместе с тем, известные ИТВ, ориентированные на усложнение структуры трафика, требуют внедрения дополнительных пакетов в потоки трафика, что не позволяет им обеспечить высокий уровень бескомпроматности и скрытности от систем обнаружения вторжений, использующих способы анализа интенсивности трафика.* ***Целью работы является*** *разработка научно-методического аппарата (НМА) для обоснования ИТВ, основанных на полном перехвате трафика с последующим преобразованием его структуры в направлении ее усложнения. Такой НМА позволит обеспечить неизменность интенсивности потока трафика, обеспечить формирование структуры трафика с гораздо более высоким уровнем сложности, и, соответственно, более высокий уровень снижения своевременности его обработки в узлах сети.* ***Используемые методы.*** *В основу научно-методического аппарата для обоснования ИТВ, использующего усложнение структуры трафика, положен метод функционального преобразования трафика, ранее обоснованный в работах Г.И. Линца и представителей его научной школы.* ***Результаты и их новизна.*** *В работе обоснован оператор преобразования трафика из простейшего потока в поток со сложной структурой, имеющий распределение Парето. Проведено исследование этого оператора. Выявлено, что преобразование трафика из простого в сложный состоит из двух процессов. Первый процесс – «сжатие» интервалов между пакетами и формирование «пачек» трафика. Второй процесс – «разрежения» интервалов между пакетами и формирование «длинных пауз» между «пачками» пакетов. Исследование процессов преобразования выявило, что процесс «разрежения» интервалов между пакетами в области больших значений интервалов входного трафика, возникает с небольшой вероятностью и негативно отражается на задержках пакетов трафика. В связи с этим, процессом «разрежения» пакетов трафика при обосновании ИТВ можно пренебречь. Исследование процесса «сжатия» пакетов трафика выявило, что при прямом использовании оператора преобразования возникают отрицательные задержки пакетов. Проведено исследование этих задержек, сформированы предложения по исключению отрицательных задержек.* ***Практическая значимость.*** *Полученный оператор преобразования трафика из простейшего потока в поток со сложной структурой составит основу НМА для обоснования новых ИТВ. Такие ИТВ будут обладать свойством бескомпроматности и скрытности по отношению к существующим способам обнаружения сетевых атак, основанных на анализе интенсивности трафика в сети. Эти новые ИТВ могут использоваться для тестирования устойчивости и безопасности телекоммуникационных систем, а также для разработки способов их защиты.*

Ключевые слова: *информационная безопасность, информационное противоборство, сетевые атаки, обнаружение вторжений, способы обнаружения сетевых атак, информационно-техническое воздействие, преобразование трафика, сложный трафик, трафик сложной структуры.*

Актуальность

В настоящее время актуальным направлением исследований является разработка моделей и методов оценки функционирования систем связи в условиях воздействия на них различного рода деструктивных факторов [1]. В настоящее время широко известны работы по оценке функционирования систем и сетей связи при воздействии на них радиоэлектронных помех. Однако, как показано в работах [2, 3], в связи с активным развитием теоретических основ информационной безопасности и информационного противоборства, становится актуальным поиск новых видов информационно-технических воздействий (ИТВ) с целью последующего их использования как для развития моделей противника, на основе которых будут обосновываться способы защиты, так и для развития отечественной методологии информационного противоборства.

Как показано в работе [4], одним из перспективных и высокоэффективных ИТВ является создание сетевых удаленных атак, направленных на отдельные объекты сети. Вместе с тем, использование таких атак приводит к существенному изменению интенсивности общего трафика в сети, что делает возможным успешное обнаружение такого типа ИТВ и успешное их блокирование системами обнаружения вторжений (IDS – Intrusion Detection System).

В работе [5] на основе анализа источников [6-7] проведена классификация аномалий трафика при проведении ИТВ типа «удаленная сетевая атака». Эта классификация приведена на рис. 1, а выявленные соответствия аномалий обобщенны в таблице 1.

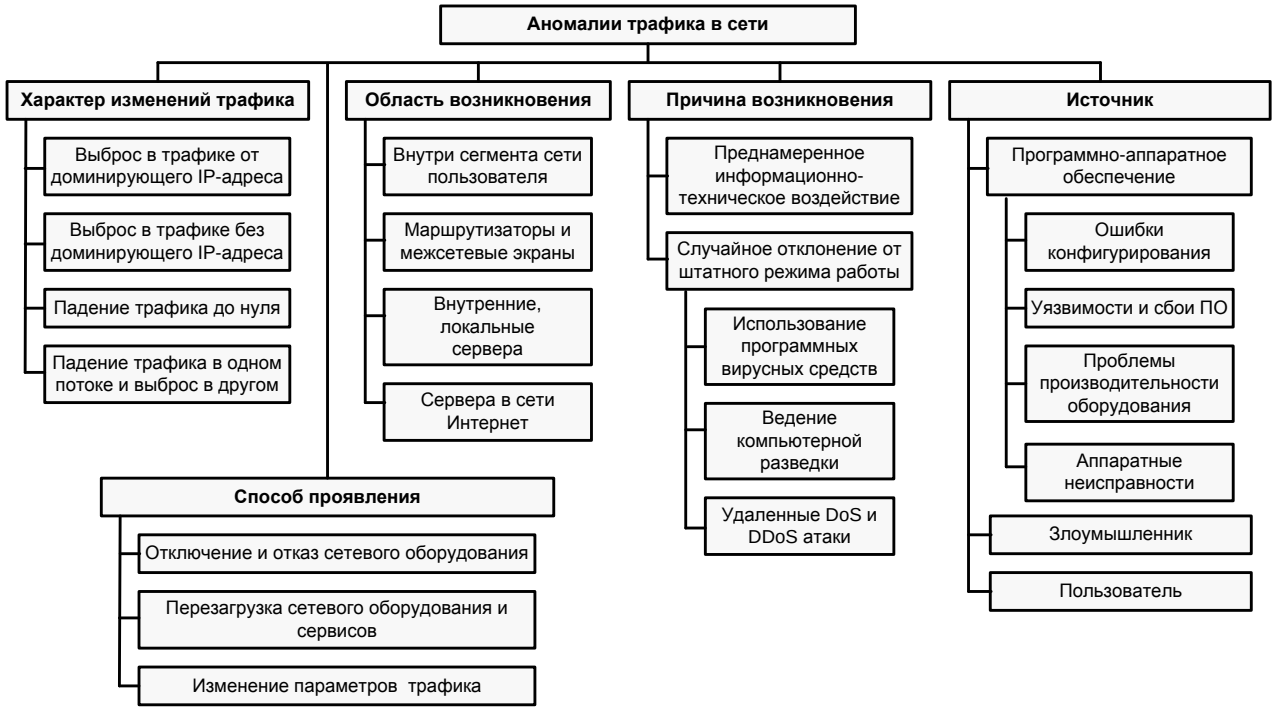


Рис. 1. Классификация аномалий трафика при проведении ИТВ типа «удаленная сетевая атака» [5]

Таблица 1. Классификация аномалий трафика при проведении ИТВ типа «удаленная сетевая атака» [5]

Тип и причина аномалии	Описание	Характеристики изменений трафика
Альфа-аномалия	Необычно высокий уровень трафика типа «точка-точка».	Лавинообразный рост (выброс) интенсивности трафика как по количеству потоков, так и по интенсивности передачи пакетов в них по одному доминирующему направлению «источник-назначение». Небольшая продолжительность (до 10 минут).
DoS, DDoS-атака	Распределённая атака типа «отказ в обслуживании» на один сетевой узел.	Лавинообразный рост интенсивности трафика, как по количеству потоков, так и по интенсивности передачи пакетов в них, от множества источников к одному адресу назначения.
Перегрузка	Необычно высокий спрос на один сетевой ресурс или сервис.	Скачек интенсивности трафика к одному доминирующему IP-адресу и/или доминирующему порту. Обычно кратковременная аномалия.
Сканирование сети/портов	Сканирование сети по определённым открытым портам или сканирование одного узла по всем портам с целью поиска уязвимостей.	Скачкообразное изменение интенсивности трафика внутри потоков и по их количеству от одного доминирующего IP-адреса.
Деятельность червей	Вредоносная программа, которая самостоятельно распространяется по сети и использует уязвимости ОС.	Лавинообразный рост трафика без доминирующего адреса назначения, но всегда с одним или несколькими доминирующими портами назначения.
«Точка-мультиточка»	Распространение контента от одного сервера многим пользователям.	Рост интенсивности трафика от доминирующего источника к нескольким узлам назначения.
Отключения	Сетевые неполадки, которые вызывают падение в трафике между одной парой «источник-назначение».	Падение интенсивности трафика обычно до нуля. Может быть долговременным и включать все потоки «источник-назначение» от (или к) одного маршрутизатора.
Переключения потока	Необычное переключение потоков трафика с одного входящего маршрутизатора на другой.	Падение интенсивности в одном потоке трафика и ее мгновенный рост в другом. Может затрагивать несколько потоков трафика.

Анализ приведенных в таблице данных позволяет сделать вывод, что интенсивность трафика существенным образом зависит от типа ИТВ, что делает возможным не только идентификацию факта атаки, но и распознавание конкретного ее типа.

В настоящее время идентификация и распознавание ИТВ на основе анализа трафика является сложившимся актуальным направлением исследований. Для выявления фактов ИТВ на основе анализа интенсивности сетевого трафика используются следующий научно-методический аппарат (НМА):

- трендовый анализ (например, работы И.М. Ажмухамедова и А. Н. Марьенкова [9, 10]);
- традиционные статистические подходы, основанные, прежде всего, на корреляционном анализе (например, работы О.И. Шелухина, А.А. Талалаева, И.П. Тищенко, В.П. Фраленко, В.М. Хачумова [11, 12]);
- методы на основе вейвлет-анализа (например, работы О.И. Шелухина, А.С. Филиновой, А.В. Гармашева [13-15]);
- подходы на основе классификаторов с использованием теории нечетких множеств (например, работа И. М. Ажмухамедова, А. Н. Марьенкова [16]);
- методы фрактального анализа (например, работы М.А. Басараба, И.С. Строганова [17], О.И. Шелухина, А.А. Антонян [18], M. Mazurek, D. Pawel [19], P. Tarrio, A.M. Bernardos, J.R. Casar [20]);
- методы теории конечных автоматов, которые создаются на основе генетических алгоритмов (например, работа В.П. Фраленко [21]);
- анализ трафика на основе нейронных сетей (например, работы О.И. Шелухина, А.И. Чернышева [22], А.А. Талалаева, И.П. Тищенко, В.П. Фраленко, В.М. Хачумова, Ю.Г. Емельяновой [23, 24, 30], А.К. Большева, В.В. Яновского [25], J.Z. Lei, A. Ghorbani G. Wang, J. Hao, J. Ma, L. Huang [26-28], J. Cannady [29]), в том числе на основе нейро-нечетких систем (например, работы A.N. Toosi, M. Kahani, R. Monsefi [30], Z.A. Orang [31], A. Zainal, M.A. Maarof, S. M. Shamsuddin [32]);
- анализ трафика на основе бионических подходов, которые в свою очередь базируются на технологиях искусственных иммунных систем (например, работы S.A. Hofmeyr и S. Forrest [33, 34]);
- гибридные подходы, объединяющие несколько вариантов и способов анализа трафика (например, работы И.П. Тищенко, В.П. Фраленко, В.М. Хачумова [35], А.А. Браницкого, И.В. Котенко [36], Y.P. Zhou [37], S.T. Powers, J. He [38]).

Необходимо отметить, что большинство исследователей приходят к выводу о сложности и слабой формализуемости задачи достоверной идентификации ИТВ. В связи с этим, во все большем числе работ для идентификации ИТВ на основе анализа интенсивности трафика используются методы теорий интеллектуальных систем. Обзор использования интеллектуальных методов для решения задач идентификации ИТВ представлен в работе П.А. Корнева, А.Н. Пылькина и А.Ю. Свиридова [39]. При этом в работах Ю.Г. Емельяновой, А.А. Талалаева, И.П. Тищенко, В.П. Фраленко, В.М. Хачумова А.А. Кондратьева [21, 24, 35, 40-42]

представлен НМА и структура комплекса обнаружения вторжений на основе таких методов теорий интеллектуальных систем, как нейросетевой анализ и использование генетических алгоритмов.

В связи с тем, что вышерассмотренные подходы к идентификации ИТВ основаны на анализе интенсивности сетевого трафика, то бескомпроматное и эффективное ИТВ не должно вести к изменению этой интенсивности. Вариантом такого ИТВ является сетевая атака, ориентированная на изменение структуры трафика, при том же уровне интенсивности.

В работах [43, 44] указывается на существенное снижение своевременности обслуживания трафика со сложной структурой в узлах маршрутизации и коммутации пакетов.

При этом под трафиком сложной структуры понимается поток, у которого коэффициент вариации интервалов времени между поступлениями отдельных пакетов больше единицы (c_τ>1), где:

$$c_\tau = \sigma(\tau)/m(\tau),$$

c_τ – коэффициент вариации значений интервалов времени между поступлениями отдельных пакетов трафика; $m(\tau)$ – математическое ожидание (МОЖ) значений интервалов τ времени между поступлениями отдельных пакетов трафика; $\sigma(\tau)$ – среднее квадратичное отклонение (СКО) значений интервалов τ времени между поступлениями отдельных пакетов трафика.

Под своевременностью обслуживания трафика в узле сети будем понимать время от момента прихода начала пакета в узел, до момента покидания пакетом узла. Это время определяется задержкой при ожидании пакета в буфере узла и временем его обработки в коммутационном устройстве. При этом время обработки в коммутационном устройстве определяется объемом пакета и, как правило, для этого времени принимается допущение об экспоненциальном законе его распределения.

Результаты сравнительного анализа своевременности обслуживания в узле по показателю времени обслуживания трафика на основе моделей систем массового обслуживания *M*/*M*/1 и *Pa*/*M*/1, представленные в работах [43, 44], где *Pa* – модель сложного трафика в виде потока с Парето распределением, показали следующее.

1. Область, в которой происходит существенное снижение своевременности обслуживания трафика со сложной структурой, определяется параметром формы α в Парето распределении (меньшие значения α соответствуют более высокому уровню сложности трафика) и уровнем загрузки узла сети ρ. Эта область аппроксимируется выражением $\alpha(\rho) \le 0{,}956 + 1{,}114\rho$ при $\alpha \in [1{,}2;\ 2]$ и загрузке $\rho \in [0{,}1;\ 0{,}9]$ – см. рис. 2.

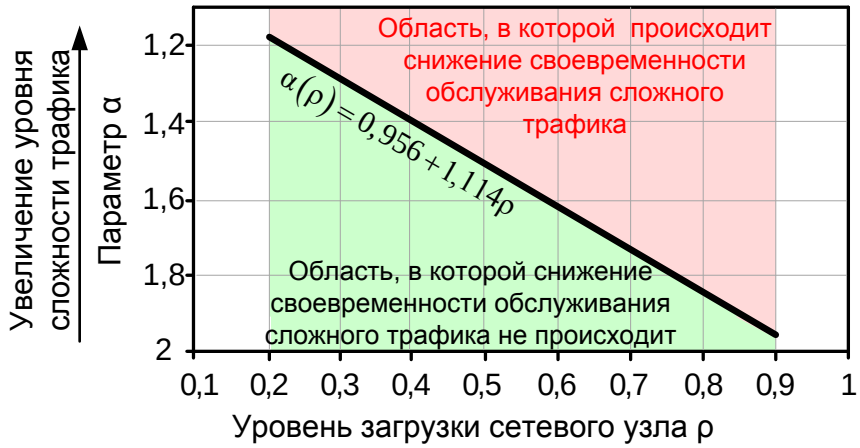


Рис. 2. Область {α, ρ}, в которой происходит существенное снижение своевременности обслуживания трафика со сложной структурой [43]

2. Своевременность обслуживания сложного трафика, представленного потоком с Парето-распределением моментов поступления заявок, со значениями параметра формы 1,3≤α≤2 по показателю «время задержки пакета в узле» в диапазоне загрузки узла 0,6≤ρ≤0,9, может быть аппроксимирована следующей функцией (рис. 3):

$$T_{\text{зад par}}(\alpha,\rho)=A_{\text{p}}(\alpha)\cdot\exp\left[\left(5,52\cdot10^{3}\exp(-4,652\alpha)+10,74\right)\rho\right]+$$
$$+\left(3,451\cdot10^{5}\exp(-8,301\alpha)+1,88\right), \quad (1)$$

где

$$A_{\text{p}}(\alpha)=\begin{cases}\dfrac{4,435\cdot10^{-4}}{1+2,225\cdot10^{6}e^{-6,889\alpha}}, \text{ при } 1,668<\alpha\le 2;\\ \dfrac{1,384\cdot10^{-4}}{1+1,01\cdot10^{19}e^{-28,471\alpha}}, \text{ при } 1,3\le\alpha\le 1,668.\end{cases}.$$

При этом в выражении (1) за единицу принято время обслуживания в системах массового обслуживания *M*/*M*/1 и *Pa*/*M*/1.

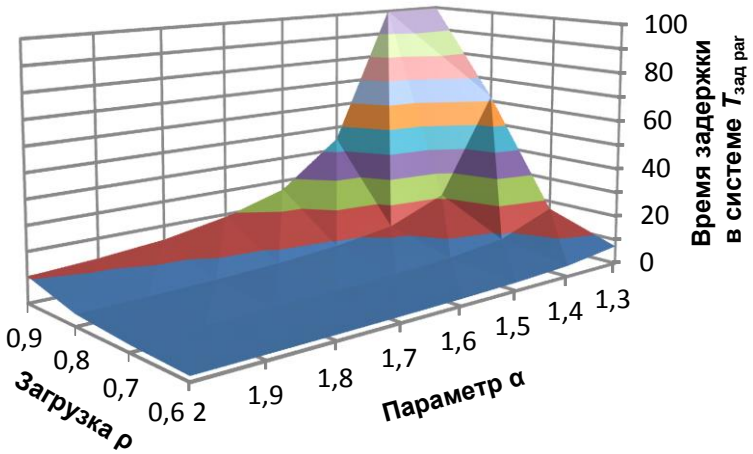


Рис. 3. Своевременность обслуживания сложного трафика по показателю «время задержки пакета в узле» [44]

3. Сравнительный анализ времени задержки в системах массового обслуживания *M*/*M*/1 и *Pa*/*M*/1 показал, что своевременность обслуживания сложного трафика, представленного потоком с Парето-распределением моментов поступления заявок в разы ниже, чем простого, представленного простейшим потоком с экспоненциальным распределением (рис. 4).

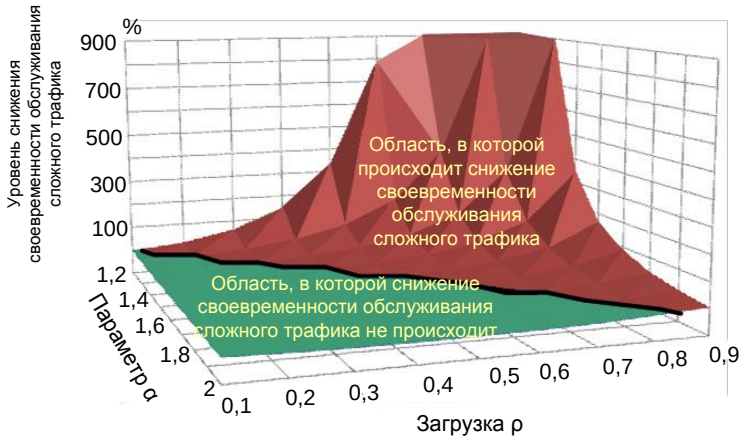


Рис. 4. Уровень снижения своевременности обслуживания трафика со сложной структурой по отношению к трафику с экспоненциальным распределением [43]

Эти выводы вполне согласуются с исследованиями других авторов, в которых регистрируется факты снижения своевременности обработки сложного трафика. К примерам таких исследований можно привести работы известных специалистов – Ю.И. Рыжикова [45, 46], П.А. Будко [47], Л.А. Фомина [48, 58, 59], В.Н. Тарасова, Н.Ф. Бахаревой [49, 50], О.И. Шелухина [51], А.Н. Назарова, К.И. Сычева [52], Е.А. Новикова [62-65].

Таким образом ИТВ, основанное на формировании потоков трафика сложной структуры, может быть использовано для преднамеренного создания условий, направленных на повышение времени обработки информационных потоков в узлах маршрутизации, и как следствие, снижения своевременности обслуживания потоков трафика ниже значений, определяемых требованиями к системе связи.

В работе [53] предложен вариант ИТВ, основанный на формировании структуры информационных потоков трафика с высоким уровнем сложности, за счет внедрения дополнительных имитационных потоков. Однако у этого ИТВ есть ряд недостатков. Во-первых, ИТВ, основанное на внедрении дополнительных пакетов, будет приводить к росту интенсивности трафика, что приведет к идентификации такого ИТВ на основе вышеприведенных способов обнаружения сетевых аномалий. Во-вторых, как показывают исследования этого ИТВ, проведенные в работе [53], доля внедряемого трафика не может быть более 12%, иначе происходит «разваливание потока» – внедряемые пакеты начинают замещать собой «нормальные пакеты». При этом достигаются относительно невысокие значения уровня сложности трафика $c_\tau \rightarrow 2{,}5$.

Для устранения этих недостатков предлагается ИТВ, основанное на полном перехвате трафика с последующим преобразованием его структуры в сторону ее усложнения. Это позволит, с одной стороны, обеспечить неизменность интенсивности потока трафика, а значит, сделает такое ИТВ бескомпоматным относительно способов идентификации сетевых атак на основе анализа интенсивности трафика. С другой стороны – обеспечит формирование структуры трафика с гораздо более высоким уровнем сложности, а соответственно и более высокий уровень снижения своевременности его обработки в узлах сети. Схема системы, осуществляющей такое ИТВ, представлена на рис. 5.

Рис. 5. Схема системы, осуществляющей ИТВ
на основе преобразования структуры трафика

Постановка задачи

Цель работы – разработка ИТВ типа «удаленная сетевая атака», основанного на перехвате трафика и преобразовании его структуры в направлении усложнения. Задача работы – разработка новых элементов НМА теории информационного противоборства для обоснования параметров такого ИТВ. Эта задача может быть декомпозирована на ряд частных задач:

1) обосновать оператор преобразования трафика;
2) исследовать оператор преобразования трафика;
3) предложить рекомендации по рациональному практическому применению оператора преобразования трафика.

Как показано в обзоре [54], для представления сложного трафика можно использовать различные модели – ON-OFF модели; потоки с распределениями Парето, Вейбула, Гамма, потоки Кокса, и другие подходы. В рамках решаемой задачи предлагается использовать поток, в котором время между приходом заявок имеет Парето-распределение. Выбор Парето-распределения в качестве модели сложного трафика обусловлено следующими соображениями.

Во-первых, как показано в работе [43], сложный трафик с коэффициентом вариации c_τ>1 может быть представлен моделью потока с Парето-распределением

$$G(\tau) = 1 - \left(\frac{k}{\tau}\right)^{\alpha}, k > 0, \alpha > 0, \tau > k,$$

где τ – интервал времени между поступлением очередных заявок в потоке с распределением Парето; k – коэффициент масштаба; α – параметр формы распределения Парето.

Зависимость между коэффициентом вариации c_τ и параметром α распределения Парето в диапазоне αϵ[1,2; 2] с погрешностью до 3,27% может быть аппроксимирована выражением [21]

$$c_\tau(\alpha) = 1{,}41 \cdot 10^4 \cdot e^{-5{,}384 \cdot \alpha} + 1{,}52,$$

откуда

$$\alpha = \frac{1}{5{,}384} \ln\left(\frac{c_\tau + 1{,}52}{1{,}41 \cdot 10^4}\right).$$

Во-вторых, как показано в большинстве работ по сложному трафику (например, в работах [47, 52]), самоподобный трафик с коэффициентом Херста H также может быть представлен моделью потока с Парето-распределением. При этом зависимость между коэффициентом Херста в диапазоне Hϵ[0,5; 1] и параметром α имеет вид [47]

$$\alpha = 3 - 2H.$$

В-третьих, корректность и адекватность моделирования сложного трафика потоком с Парето-распределением моментов поступления заявок подтверждается аналогичным подходом, используемым различными исследователями в работах [47, 55, 57].

В качестве модели входного трафика, который подвергается преобразованию, используется простейший поток, который давно и традиционно используется для моделирования информационных потоков в сетях в теории телетрафика, с функцией распределения:

$$F(\tau) = 1 - e^{-\lambda\tau},$$

Для формализации задачи в работе введены следующие обозначения:

τ – интервал времени между поступлением смежных очередных пакетов трафика;

$\tau_{вх}$ – интервал времени между поступлением пакетов входного потока трафика, который будет подвергнут преобразованию;

$\tau_{вых}$ – интервал времени между поступлением пакетов выходного потока трафика, который уже преобразован;

$\Delta\tau = \tau_{вых} - \tau_{вх}$ – задержка пакета при выполнении преобразования;

$\Delta\tau_{min}$ – минимальное значение задержки пакета трафика при выполнении преобразования;

$\Delta\tau_{max}$ – максимальное значение задержки пакета трафика при выполнении преобразования;

$f(\Delta\tau)$ – плотность распределения задержки пакетов трафика при выполнении преобразования;

λ – параметр экспоненциального распределения;

α – параметр формы распределения Парето;

k – коэффициент масштаба распределения Парето;

H – коэффициент Херста, определяющий уровень самоподобия трафика;

ρ – загрузка сетевого узла;

m – математическое ожидание;

σ – среднее квадратическое отклонение;

c_τ – коэффициент вариации трафика, его дисперсионная характеристика, определяющая структурную сложность трафика.

Обоснование оператора преобразования трафика

Для обоснования оператора преобразования трафика был использован метод функционального преобразования трафика, впервые предложенный в работе Г.И. Линца, Л.А. Фомина, С.А. Скоробогатова [58]. В ней метод функционального преобразования трафика предлагался в качестве направления снижения структурной сложности входного трафика. Дальнейшее развитие метод функционального преобразования получил в работах Г.И. Линца и его коллег [57, 59, 60], где на основе этого метода решается задача обеспечения инвариантности мультисервисной сети к структуре входного трафика.

Вместе с тем, анализ исследований Г.И. Линца и его коллег [57-60] показал, что полученные в них результаты носят общетеоретический характер, а разработанный НМА функционального преобразования трафика трудно применим на практике. В частности этим НМА не учитываются требования по качеству обслуживания (QoS – Quality of Service) трафика (задержка преобразования, требуемый объем буфера преобразователя, вероятность отказа в обслуживании), а также сохранение вероятностно-временных параметров преобразования (равенство математических ожиданий входного и выходного потоков трафика, только положительный сдвиг во времени поступивших пакетов, невозможность преобразования всех пакетов и т.д.).

В работе К.В. Ушанева, С.И. Макаренко [56] решена задача разработки НМА преобразования трафика с учетом требований по QoS и вышеуказанных дополнительных параметров, но применительно к задаче снижения структурной сложности трафика. Вместе с тем, в этой работе, так же как и в работах Г.И. Линца, не рассматривается задача преобразования структуры трафика в направлении его усложнения.

Таким образом, для обоснования оператора преобразования трафика в направлении усложнения его структуры будет использован метод функционального преобразования трафика, рассмотренный в работах Г.И. Линца и его коллег [57-60]. Дальнейшее совершенствование процесса преобразования трафика на основе обоснованного оператора будет вестись с учетом требований по QoS и параметров преобразования, в соответствии с наработками, представленными в работе [56].

В соответствии с поставленной задачей, входной поток трафика моделируется простейшим потоком и имеет экспоненциальное время распределения между поступлениями очередных заявок:

$$F(\tau_{вх}) = 1 - e^{-\lambda\tau_{вх}}. \quad (2)$$

Выходной поток трафика моделируется потоком сложной структуры и имеет Парето-распределение значений времени между поступлениями очередных заявок:

$$G(\tau_{вых}) = 1 - \left(\frac{k}{\tau_{вых}} \right)^{\alpha}, k > 0, \alpha > 0, \tau > k. \quad (3)$$

Сформируем оператор φ, который задает отображение:

$$\varphi : F(\tau_{вх}) \rightarrow G(\tau_{вых}). \quad (4)$$

С учетом свойства инвариантности дифференциалов вероятности можно записать:

$$f(\tau_{вх}) d\tau_{вх} = g(\tau_{вых}) d\tau_{вых}, \quad (5)$$

откуда в общем виде можно получить оператор преобразования:

$$g(\tau_{вых}) = f(\tau_{вх}) \left| \frac{d\tau_{вх}}{d\tau_{вых}} \right|. \quad (6)$$

Проинтегрировав выражение (5), получим

$$\int_0^{\tau} f(\tau_{вх}) d\tau_{вх} = \int_0^{\tau} g(\tau_{вых}) d\tau_{вых}. \quad (7)$$

Последнее выражение определяет равенство функций вероятности входного и выходного процессов:

$$F(\tau_{вх}) = G(\tau_{вых}). \quad (8)$$

Определим оператор преобразования из (8) с учетом того, что функция $G(\tau_{вых})$ определяется выражением (3):

$$F(\tau_{вх}) = 1 - \left(\frac{k}{\tau_{вых}} \right)^{\alpha},$$

откуда получим оператор преобразования произвольного экспоненциального распределения $F(\tau_{вх})$ в поток с Парето-распределением:

$$\tau_{вых} = \left(\frac{k^{\alpha}}{1 - F(\tau_{вх})} \right)^{\frac{1}{\alpha}}. \quad (9)$$

Из последнего выражения определим оператор преобразования потока φ с экспоненциальным распределением в поток с распределением Парето, с учетом того, что функция $F(\tau_{вх})$ определяется выражением (2):

$$\tau_{вых} = \varphi(\tau_{вх}) = \left(\frac{k^{\alpha}}{1 - \left(1 - e^{-\lambda \tau_{вх}}\right)} \right)^{\frac{1}{\alpha}} = k\, e^{\frac{\lambda \tau_{вх}}{\alpha}}. \quad (10)$$

Введем дополнительные условия для преобразования (10), определяемые физикой процесса преобразования трафика:

1) введем ограничения на нормировку параметров. Все параметры и результаты нормируем к параметру входного распределения, приняв его за значение единицы: $m(\tau_{вх})=1/\lambda=1$;
2) введем ограничения на уровень сложности преобразуемого трафика, который, в соответствии с работой [43], определяется по параметру α, причем $1<\alpha\leq 2$ (большему значению параметра α соответствует меньший уровень сложности трафика);

3) введем допущение о равенстве математических ожиданий входного и выходного потоков, что соответствует требованию обеспечения инвариантности средней интенсивности входящего и выходящего потоков:

$$\frac{1}{\lambda}=\frac{\alpha k}{\alpha-1},$$

откуда, с учетом ограничения № 1, получим соотношение между параметрами α и *k* в Парето-распределении для одного и того же λ=1:

$$k=\frac{\alpha-1}{\alpha}. \qquad (11)$$

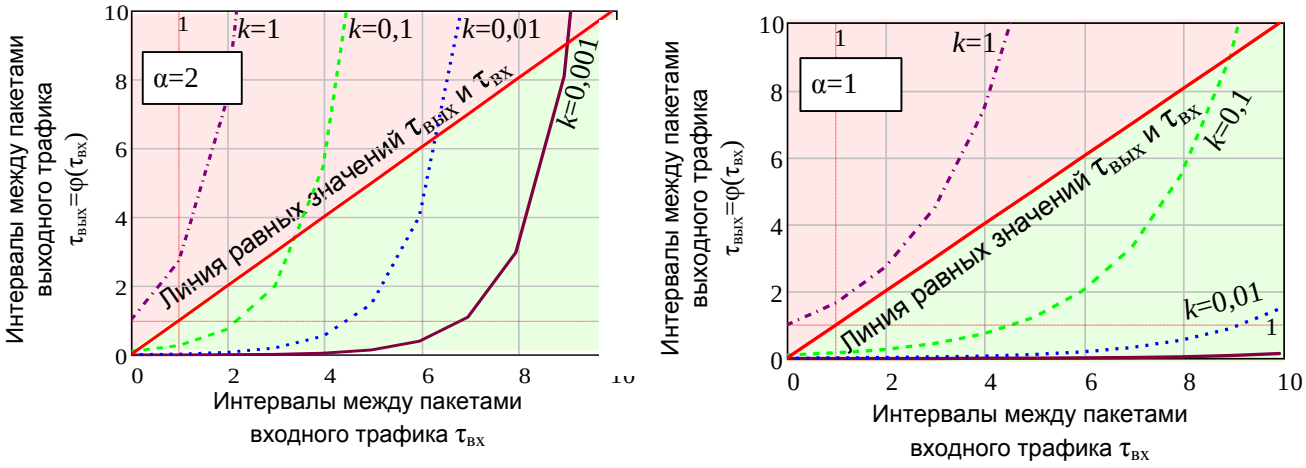
С учетом ограничения № 2 получим, что параметр *k* в условиях нормировки имеет область значений $0<k\leq 1$, при области определения $1<\alpha\leq 2$.

В условиях учета реальных, а не нормированных значений λ, параметр *k* будет определяться по формуле:

$$k=\frac{\alpha-1}{\alpha\cdot\lambda}.$$

Исследование оператора преобразования трафика на предмет выявления в нем типовых процессов

Исследуем оператор преобразования φ, определяемый выражением (10). При этом учтем ограничения на сложность трафика $1<\alpha\leq 2$. Результаты исследования оператора преобразования $\tau_{вых}=\varphi(\tau_{вх})$, для предельных значений сложности трафика α=1 и α=2, для параметра $0<k\leq 1$ представлены на рис. 6.



а. б.

Рис. 6. Результаты исследования оператора преобразования $\tau_{вых}=\varphi(\tau_{вх})$ для предельных значений сложности трафика:
а) низкий уровень сложности трафика α=2;
б) наиболее сложный трафик α=1.

Анализ зависимостей, представленных на рис. 6, позволяет сделать вывод о том, что область определения оператора $\tau_{вых}=\varphi(\tau_{вх})$ можно разделить на две подобласти:

1) область D_1 ($\tau_{вых}\leq\tau_{вх}$), в которой преобразование $\tau_{вых}=\varphi(\tau_{вх})$ направленно на «сжатие» интервалов между пакетами и формирование «пачек» трафика, что соответствует росту вероятности коротких интервалов между приходом пакетов выходного трафика;
2) область D_2 ($\tau_{вых}>\tau_{вх}$), в которой преобразование $\tau_{вых}=\varphi(\tau_{вх})$ направленно на «разрежение» интервалов между пакетами и формирование «длинных пауз» между «пачками», что соответствует формированию более длинного «хвоста» плотности распределения интервалов времени между пакетами выходного трафика.

При анализе процессов преобразования также необходимо учитывать, что параметр k в распределении Парето (3), которому соответствует выходной трафик, принимает не произвольные значения, а определяется выражением (11) при условии $m(\tau_{вх})=1/\lambda=1$. С учетом этого, процессы преобразования трафика на основе оператора $\tau_{вых}=\varphi(\tau_{вх})$ фактически зависят только от параметра сложности трафика α.

На рис. 7 представлены графики, соответствующие процессам «разрежения» и «сжатия» в операторе преобразования, при значениях:

- $\alpha=1{,}2$ (наиболее сложный трафик);
- $\alpha=1{,}6$ (стандартный уровень сложности Интернет трафика);
- $\alpha=2$ (низкий уровень сложности трафика);

при расчетном значении $k=(\alpha-1)/\alpha$ для каждого α.

Также на рис. 7. представлены вероятности для значений $\tau_{вх}=m(\tau_{вх})+\sigma(\tau_{вх})=2$ и $\tau_{вх}=m(\tau_{вх})+2\sigma(\tau_{вх})=3$, которые соответственно равны $P(\tau_{вх}\leq2)=0{,}865$ и $P(\tau_{вх}\leq3)=0{,}95$. Таким образом можно утверждать, что с вероятностью $P=0{,}95$ значения интервалов входного трафика $\tau_{вх}$ не превысят значения 3 при нормировании $m(\tau_{вх})=1/\lambda=1$.

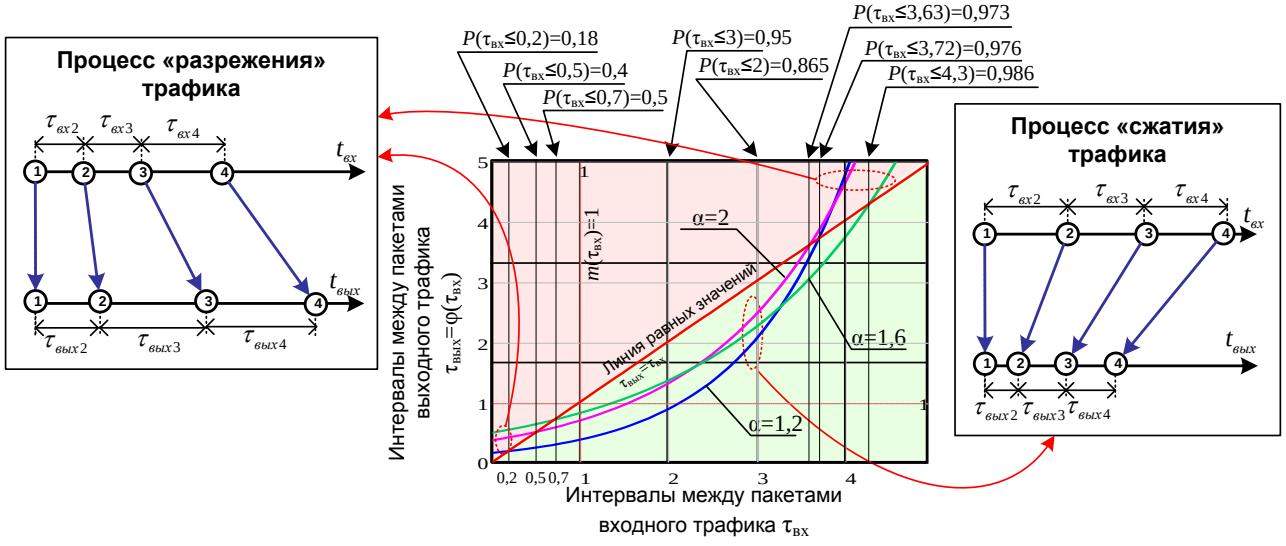


Рис. 7. Процессы преобразования при различных значениях уровня сложности трафика α

Анализ рис. 7 позволяет сделать вывод, что при преобразовании трафика, как правило, с большой вероятностью будет выполняться процесс «сжатия» трафика, чем его «разрежение» (таблица 2).

Таким образом, процесс «сжатия» интервалов выходного трафика по сравнению с интервалами входного трафика является основным процессом преобразования, который проводится с тем большей вероятностью, чем больше требуемая сложность формируемого сложного трафика. Процесс «сжатия» приводит к тому, что отдельные пакеты входного простейшего потока объединяются в «пачки» пакетов.

Вместе с тем, анализ процесса позволяет предположить, что оператор преобразования $\tau_{вых}=\varphi(\tau_{вх})$ не может быть применен в явном виде для прямого «сжатия» трафика, так как может случиться ситуация, когда поступивший пакет должен быть оправлен раньше времени своего поступления (рис. 7). Это требует отдельного, более глубокого исследования процесса «сжатия» при формировании трафика.

Таблица 2. Вероятности процессов «сжатия» и «разрежения» трафика при его преобразовании

Уровень сложности выходного трафика	Вероятность процесса «разрежения» пакетов трафика	Вероятность процесса «сжатия» пакетов трафика
Низкий уровень сложности трафика $\alpha=2$	0,524	0,476
Стандартный уровень сложности Интернет трафика $\alpha=1,6$	0,427	0,573
Наиболее высокий уровень сложности трафика $\alpha=1,2$	0,194	0,806

Кроме того, анализ графиков на рис. 6 позволяет сделать вывод о том, что после некоторого значения $\tau_{вх}$, процесс «сжатия» сменяется процессом «разрежения», при этом увеличивающимся значениям $\tau_{вх}$ соответствуют все более и более возрастающие значения $\tau_{вых}$. При этом вероятность процесса «разрежения» пакетов в области высоких значений $\tau_{вх}$ весьма мала:

- для формирования трафика с низким уровнем сложности с $\alpha=2$ вероятность процесса «разрежения» пакетов – $P(\tau_{вх}>4,3)=0,014$;
- для формирования трафика с нормальным уровнем сложности с $\alpha=1,6$ вероятность процесса «разрежения» пакетов – $P(\tau_{вх}>3,63)=0,027$;
- для формирования трафика с высоким уровнем сложности с $\alpha=1,2$ вероятность процесса «разрежения» пакетов – $P(\tau_{вх}>3,72)=0,024$.

Как видно, вероятность поступления пакетов с интервалами $\tau_{вх}>3$ весьма мала. Вместе с тем, поступление пакетов с интервалом $\tau_{вх}$, находящегося в диапазоне $\tau_{вх}>3,5$, которому соответствует процесс «разрежения» трафика,

приводит к тому, что оператор преобразования $\tau_{вых}=\varphi(\tau_{вх})$ формирует для таких значений $\tau_{вх}$ неоправданно высокие значения $\tau_{вых}$ (достигают значений десятков и сотен условных единиц). В результате, из-за необходимости соблюдать последовательность пакетов в выходном трафике, новые пакеты, поступающие в это время, вынуждены ожидать в системе преобразования. Это приводит к быстрому накоплению очереди пакетов и росту среднего времени задержки пакетов в системе преобразования трафика.

Исследование процесса «сжатия» трафика в операторе преобразования

Для рассмотрения процессов «сжатия» трафика введем параметр задержки пакета как разность между интервалом отправки пакета и интервалом поступления пакета (рис. 8):

$$\Delta\tau=\tau_{вых}-\tau_{вх}.$$

С учетом выражения (10):

$$\Delta\tau(\tau_{вх})=k\,e^{\frac{\lambda\tau_{вх}}{\alpha}}-\tau_{вх}. \quad (12)$$

Таким образом, параметр задержки пакета $\Delta\tau(\tau_{вх})$ в системе преобразования является детерминированной функцией от случайного аргумента $\tau_{вх}$, который, в свою очередь, имеет экспоненциальное распределение. Это позволяет аналитически вывести и исследовать функцию плотности распределения $f(\Delta\tau(\tau_{вх}))$.

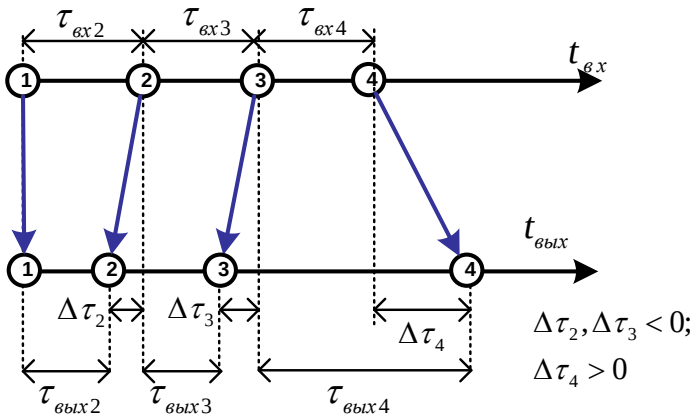


Рис. 8. Задержка $\Delta\tau=\tau_{вых}-\tau_{вх}$ в системе преобразования трафика

Для получения плотности вероятности $f(\Delta\tau(\tau_{вх}))$ для детерминированной функции $\Delta\tau(\tau_{вх})$ от случайного аргумента используем известное выражение [61]:

$$f(\Delta\tau)=f_{\tau_{вх}}\left(\tau_{вх}(\Delta\tau)\right)\left|\frac{d\tau_{вх}(\Delta\tau)}{d\Delta\tau}\right|. \quad (13)$$

Применение этого выражения требует непрерывности и монотонности функции $\Delta\tau(\tau_{вх})$ [61]. Исследуем функцию $\Delta\tau(\tau_{вх})$ на интервалы монотонности, найдя точки ее перегиба.

Первая производная функции $\Delta\tau(\tau_{вх})$ равна:

$$\frac{d}{d\tau_{вх}}\Delta\tau(\tau_{вх})=\frac{\lambda k}{\alpha}e^{\frac{\lambda\tau_{вх}}{\alpha}}-1.$$

Эта производная обращается в ноль при:

$$\tau_{вх}=\frac{\alpha}{\lambda}\ln\left(\frac{\alpha}{\lambda k}\right). \quad (14)$$

Таким образом, функция $\Delta\tau(\tau_{вх})$ имеет два интервала монотонности $\tau_{вх}\in\left[0;\frac{\alpha}{\lambda}\ln\left(\frac{\alpha}{\lambda k}\right)\right]$ и $\tau_{вх}\in\left[\frac{\alpha}{\lambda}\ln\left(\frac{\alpha}{\lambda k}\right);\infty\right)$.

Рассмотрим функцию $\Delta\tau(\tau_{вх})$ на первом из этих интервалов т.к. значения $\tau_{вх}\to 0$ соответствуют наиболее высоким значениям функции плотности вероятности $f(\tau_{вх})$ – см. рис. 9.

В явном виде использование выражения (13) по отношению к $\Delta\tau(\tau_{вх})$ невозможно. Т.к. выражение (12) для $\Delta\tau(\tau_{вх})$ является трансцендентным, что не позволяет выразить функцию $\tau_{вх}(\Delta\tau)$ в явном аналитическом виде. Для преодоления этого затруднения представим экспоненциальную функцию в выражении (12) через разложение в ряд Тейлора, ограничившись двумя членами ряда:

$$\Delta\tau(\tau_{вх})=k\,e^{\frac{\lambda\tau_{вх}}{\alpha}}-\tau_{вх}=k\left(1+\sum_{i=1}^{2}\left[\frac{1}{i!}\left(\frac{\lambda\tau_{вх}}{\alpha}\right)^{i}\right]\right)-\tau_{вх}=$$

$$=\left(\frac{\lambda^2 k}{2\alpha^2}\right)\tau_{вх}^2+\left(\frac{\lambda k}{\alpha}-1\right)\tau_{вх}+k. \quad (15)$$

Выражение (15) позволяет со степенью адекватности, достаточной для инженерных расчетов, представить функцию $\Delta\tau(\tau_{вх})$. На интервале $\tau_{вх}\le 2$ (вероятность $P(\tau_{вх}\le 2)=0{,}865$) погрешность представления выражением (15), точной функции $\Delta\tau(\tau_{вх})$ не превышает 20%. Причем наибольшую точность приближения выражение (15) показывает в области $\tau_{вх}\to 0$, которая соответствует наиболее вероятным значениям $\tau_{вх}$. Кроме того, точка перегиба (14) при любых $\alpha=1..2$ и $k=(\alpha-1)/\alpha$ соответствует условию $\tau_{вх}>2$. Таким образом, интервал $\tau_{вх}\le 2$, на котором выражение (15) задается с достаточным уровнем адекватности, полностью принадлежит первому интервалу монотонности, определенному ранее.

Для формирования функции $\tau_{вх}(\Delta\tau)$, обратной функции $\Delta\tau(\tau_{вх})$, найдем корни квадратного уравнения (15):

$$\tau_{вх\,1}(\Delta\tau)=\frac{2\alpha^2}{\lambda^2 k}\left(\frac{2\alpha^2-2\alpha\lambda k}{4\alpha^2}+\frac{\sqrt{\alpha^2-2\alpha\lambda k-\lambda^2k^2+2\lambda^2k\,\Delta\tau}}{2\alpha}\right);$$

$$\tau_{вх\,2}(\Delta\tau)=\frac{2\alpha^2}{\lambda^2 k}\left(\frac{2\alpha^2-2\alpha\lambda k}{4\alpha^2}-\frac{\sqrt{\alpha^2-2\alpha\lambda k-\lambda^2k^2+2\lambda^2k\,\Delta\tau}}{2\alpha}\right). \quad (16)$$

Графический вид функций $\tau_{вх\,1}(\Delta\tau)$ и $\tau_{вх\,2}(\Delta\tau)$ представлен на рис. 9. В связи с тем, что диапазону $\tau_{вх}\leq 2$ соответствует функция $\tau_{вх\,2}(\Delta\tau)$, то именно она будет рассматриваться в дальнейшем.

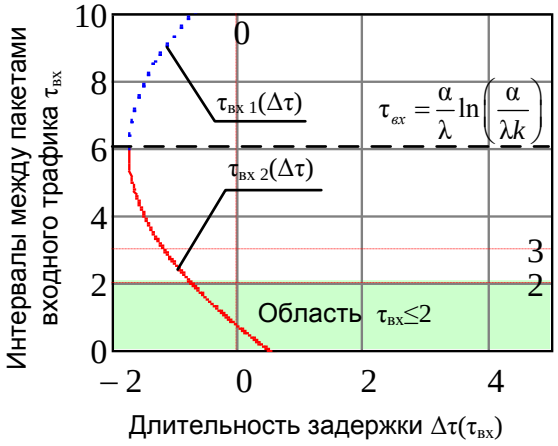


Рис. 9. Графики функций $\tau_{вх\,1}(\Delta\tau)$ и $\tau_{вх\,2}(\Delta\tau)$

Для нахождения дифференциала $d\tau_{вх}/d\Delta\tau$ в выражении (13) продифференцируем функцию $\tau_{вх\,2}(\Delta\tau)$, определяемую выражением (16):

$$\frac{d\tau_{вх}(\Delta\tau)}{d\Delta\tau}=\frac{d\tau_{вх\,2}(\Delta\tau)}{d\Delta\tau}=\frac{-a}{\sqrt{a^2-2a\lambda k-\lambda^2k^2+2\lambda^2k\,\Delta\tau}}. \qquad (17)$$

Окончательно выражение (13) для плотности вероятности $f(\Delta\tau)$ с учетом выражений (16) и (17) будет иметь вид:

$$f(\Delta\tau)=\lambda\cdot\exp\left[-\frac{2a^2}{\lambda\,k}\left(\frac{2a^2-2a\lambda k}{4a^2}-\frac{\sqrt{a^2-2a\lambda k-\lambda^2k^2+2\lambda^2k\,\Delta\tau}}{2a}\right)\right]\times$$

$$\times\left|\frac{-a}{\sqrt{a^2-2a\lambda k-\lambda^2k^2+2\lambda^2k\,\Delta\tau}}\right|. \qquad (18)$$

Исследуем функцию (17).

Из рис. 9 видно, что минимальное значение функция $\Delta\tau(\tau_{вх})$ принимает в точке перегиба: $\tau_{вх}=\frac{\alpha}{\lambda}\ln\left(\frac{\alpha}{\lambda k}\right)$. Таким образом, с учетом выражения (12), можно сделать вывод, что область определения функции $f(\Delta\tau)$ ограничена слева значением:

$$\Delta\tau_{\min}\left(\tau_{вх}=\frac{\alpha}{\lambda}\ln\left(\frac{\alpha}{\lambda k}\right)\right)=-\frac{1}{\lambda}\left(\alpha\ln\left(\frac{\alpha}{\lambda k}\right)-1\right), \qquad (19)$$

которое зависит от параметров распределения Парето α и входного потока λ.

Также из рис. 9 видно, что верхнее значение области определения $f(\Delta\tau)$ определяется из выражения (12) при $\Delta\tau(\tau_{вх}=0)$. Откуда:

$$\Delta\tau_{\max}(\tau_{вх}=0)=k. \qquad (20)$$

Область определения функции плотности вероятности $f(\Delta\tau)$, ограниченная графиками $\Delta\tau_{min}$ и $\Delta\tau_{max}$, определяемых выражениями (19) и (20) соответственно, при допущениях о нормировке $m(\tau_{вх})=1/\lambda=1$ и $k=(\alpha-1)/\alpha$ представлена на рис. 10.

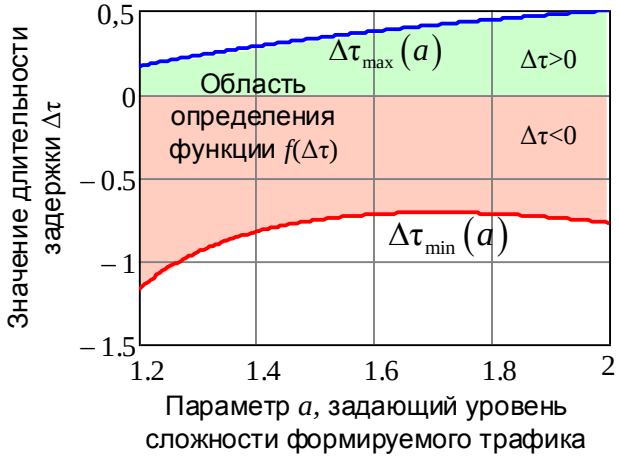


Рис. 10. Область определения функции плотности вероятности $f(\Delta\tau)$, ограниченная графиками $\Delta\tau_{min}$ и $\Delta\tau_{max}$, в зависимости от параметра α

Из рис. 10 видно, что максимального значения $\Delta\tau_{min}\approx -0,7$ достигает при $\alpha\approx 1,7$. При этом для всего диапазона $\alpha=1,2\ldots2$ эта нижняя граница области определения $f(\Delta\tau)$ лежит в диапазоне $\Delta\tau<0$. Более того, видно, что большая часть области определения лежит в диапазоне $\Delta\tau<0$, что не позволяет использовать оператор преобразования $\tau_{вых}=\varphi(\tau_{вх})$ в этой области, т.к. задержки поступающих пакетов не могут быть отрицательными.

Рассмотрим поведение функции плотности вероятности $f(\Delta\tau)$ на области ее определения.

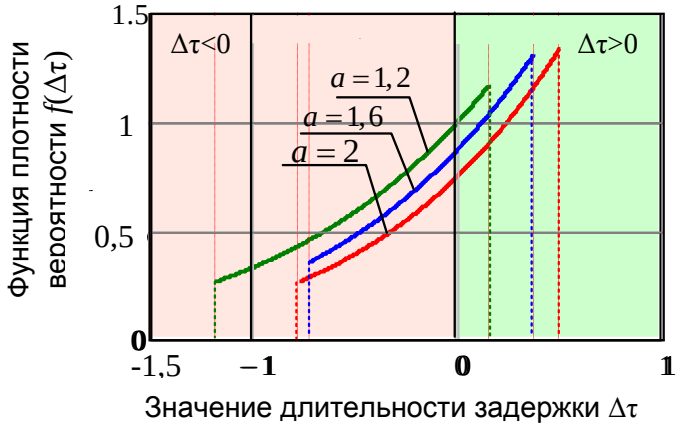


Рис. 11. Графики плотности вероятности $f(\Delta\tau)$ при различных значениях уровня сложности α формируемого трафика

Дело в том, что значения $\Delta\tau_{max}$ в области определения $f(\Delta\tau)$ соответствуют значениям $\tau_{вх}\to 0$, которые при экспоненциальном законе распределения $\tau_{вх}$, являются наиболее вероятными. И при высокой вероятности

группирования величины $\Delta\tau$ в диапазоне $\Delta\tau>0$ можно ограничиться применением оператора преобразования только в этой области.

На рис. 11 представлены графики плотности вероятности $f(\Delta\tau)$ при различных значениях уровня сложности формируемого трафика α=1,2, 1,6, 2, при допущениях о нормировке $m(\tau_{вх})=\lambda=1$ и $k=(\alpha-1)/\alpha$.

В таблице 3 приведены параметры плотностей вероятности $f(\Delta\tau)$ при вышеуказанных значениях α. Отсутствие равенства единице крайнего столбика в таблице 3 объясняется введенными вверху допущениями о сужении области определения и рассмотрении при исследовании только функции $\tau_{вх\,2}(\Delta\tau)$.

Таблица 3. Параметры плотности вероятности $f(\Delta\tau)$ при различных значениях уровня сложности α формируемого трафика

Уровень сложности формируемого трафика	Область определения функции $f(\Delta\tau)$		Вероятность того, что значение $\Delta\tau$ попадет в заданную область		
	$\Delta\tau_{min}$	$\Delta\tau_{max}$	$[\Delta\tau_{min}, 0]$	$[0, \Delta\tau_{max}]$	$[\Delta\tau_{min}, \Delta\tau_{max}]$
Низкий уровень сложности трафика α=2	–0,773	0,5	0,363	0,508	0,871
Стандартный уровень сложности Интернет трафика α=1,6	–0,721	0,375	0,417	0,403	0,82
Высокий уровень сложности трафика α=1,2	–1,169	0,167	0,65	0,178	0,828

Таким образом, оператор преобразования $\tau_{вых}=\varphi(\tau_{вх})$ не может быть применен в чистом виде для прямого «сжатия» трафика, так как при этом с вероятностью $P(\Delta\tau<0)\approx0,5$ возникает ситуация, когда поступивший пакет должен быть отправлен раньше времени своего поступления (рис. 11, табл. 3). В связи с этим, процессы преобразования трафика в направлении его усложнения требуют дальнейших исследований.

Рекомендации по рациональному практическому применению оператора преобразования трафика

Проведенное исследование оператора преобразования трафика позволило сформировать следующие рекомендации по рациональному практическому применению оператора преобразования трафика для разработки соответствующего ИТВ, а также рекомендации по направлениям дальнейших исследований.

1) В операторе преобразования трафика φ предлагается ввести параметр дополнительной задержки всех поступающих входных пакетов. Это необходимо, чтобы компенсировать отрицательные значения задержки пакетов в системе преобразования, которые невозможно реализовать в реальной системе. Значение этой задержки и порядок ее использования в составе оператора преобразования является направлением дальнейшего исследования. Вместе с тем, уже сейчас ясно, что этот параметр должен зависеть от уровня

сложности формируемого сложного трафика α и соответствовать минимальному значению $\tau_{вых}=\varphi(\tau_{вх})$ при $\tau_{вх}=0$. Вместе с тем, при введении такой задержки, необходимо учитывать требования по обеспечению QoS трафика при использовании ИТВ, основанного на преобразовании структуры трафика в направлении ее усложнения.

2) При реализации ИТВ, основанного на преобразовании структуры трафика, необходимо обеспечивать не только требуемый уровень сложности выходного трафика, но и обеспечивать соответствие параметров выходного трафика требованиям QoS, иначе протоколы системы связи примут решения о недостаточном качестве соединения и его разрыве. В связи с этим, дальнейшим направлением исследования является согласование процесса преобразования трафика (по параметрам времени задержки пакетов в системе преобразования и вероятность отказа в обслуживании) с требованиями по QoS для преобразуемого трафика.

3) Исследование процессов «разрежения» трафика в области высоких значений $\tau_{вх}$ показало, что вероятность поступления пакетов с такими интервалами весьма мало. Например: $P(\tau_{вх}>2)=0{,}135$ и $P(\tau_{вх}>3)=0{,}05$. Вместе с тем, поступление пакетов с интервалом $\tau_{вх}$, находящемся в диапазоне $\tau_{вх}>3$, которому соответствует процесс «разрежения» трафика, приводит к тому, что оператор преобразования $\tau_{вых}=\varphi(\tau_{вх})$ формирует для таких значений $\tau_{вх}$ неоправданно высокие значения $\tau_{вых}$ (достигают значений десятков и сотен условных единиц). В результате, из-за необходимости соблюдать последовательность пакетов в выходном трафике, новые пакеты, поступающие в это время, вынуждены ожидать в системе преобразования. Это приводит к быстрому накоплению очереди пакетов и росту среднего времени задержки пакетов в системе преобразования трафика, которое не совместимо с требованиями QoS. В связи с этим, предлагается при инженерной реализации системы преобразования трафика не использовать преобразование для входных пакетов, поступающих с интервалами $\tau_{вх}>2$ (при доле преобразованных пакетов 86,5%) или $\tau_{вх}>3$ (при доле преобразованных пакетов 95%).

Выводы

Современные системы IDS для обнаружения ИТВ типа «удаленная сетевая атака» широко используют анализ интенсивности трафика, поступающего от различных узлов сети. Для обеспечения бескомпроматности ИТВ необходимо обеспечить неизменность интенсивности трафика, поступающего от атакующего узла. Таким ИТВ может быть воздействие, ориентированное на усложнение структуры трафика при обеспечении инвариантности его интенсивности. Использование такого ИТВ позволит обеспечить существенное снижение своевременности обработки потоков трафика в узлах сети до 7-9 раз!

Ранее разработанное ИТВ, ориентированное на усложнение структуры трафика [53], использовало внедрение в поток передаваемого трафика дополнительных имитационных пакетов. Однако у этого ИТВ есть ряд недостатков. Во-первых, такое ИТВ, основанное на внедрении дополнительных

пакетов будет приводить к росту интенсивности трафика, что приведет к его выявлению. Во-вторых, при таком ИТВ достигаются относительно невысокие значения уровня сложности трафика.

Для устранения этих недостатков предлагается ИТВ, основанное на полном перехвате трафика с последующим преобразованием его структуры в сторону ее усложнения. Это позволит обеспечить неизменность интенсивности потока трафика, обеспечить формирование структуры трафика с гораздо более высоким уровнем сложности, и, соответственно, более высокий уровень снижения своевременности его обработки в узлах сети.

Для разработки такого ИТВ, основанного на преобразовании структуры трафика, предлагается использовать метод функционального преобразования трафика, впервые предложенный в работе Г.И. Линца, Л.А. Фомина, С.А. Скоробогатова [58].

В работе обоснован оператор преобразования трафика из простейшего потока в поток со сложной структурой, имеющий распределение Парето. Проведено исследование этого оператора. Выявлено, что преобразование трафика из простого в сложный состоит из двух процессов. Это процесс «сжатия» интервалов между пакетами и формирование «пачек» трафика, что соответствует росту вероятности коротких интервалов между пакетами выходного сложного трафика. И процесс «разрежения» интервалов между пакетами и формирование «длинных пауз» между «пачками» пакетов, что соответствует формированию «длинного хвоста» плотности распределения интервалов выходного сложного трафика.

Исследование процессов преобразования выявило, что процесс «разрежения» интервалов между пакетами в области больших значений интервалов входного трафика возникает с небольшой вероятностью и негативно влияет на процесс преобразования. В связи с этим, данным процессом при формировании инженерной системы ИТВ можно пренебречь. Исследование процесса «сжатия» пакетов трафика выявило, что при прямом использовании оператора преобразования возникают отрицательные задержки пакетов в системе ИТВ, что противоречит физическому смыслу процесса. Проведено исследование этих задержек, построена функция плотности вероятности, проведен анализ области ее определения. Сформированы предложения по исключению отрицательных задержек при преобразовании трафика. Кроме того, сформированы направления дальнейших исследований, направленных на доработку процесса преобразования трафика и согласования его с требованиями по QoS, используемыми в сети.

Литература

1. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. № 4. 2013. С. 69-79.

2. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1(2). 2014. С. 13-21.

3. Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178. URL: http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf (дата обращения 17.09.2016).

4. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения 05.12.2016).

5. Микова С. Ю., Оладько В. С., Нестеренко М. А. Подход к классификации аномалий сетевого трафика // Инновационная наука. 2015. № 11. С. 78-80.

6. Багров Е. В. Мониторинг и аудит информационной безопасности на предприятии // Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность. 2011. № 5. С. 54-56.

7. Артамонов В. А. Обнаружение сетевых аномалий через реконструкцию сетевого трафика // Известия Южного федерального университета. Технические науки. 2007. Т. 76. № 1. С. 127-130.

8. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. О.И. Шелухина. – М.: Горячая линия-Телеком, 2013. – 220 с.

9. Ажмухамедов И. М., Марьенков А. Н. Поиск и оценка аномалий сетевого трафика на основе циклического анализа // Инженерный вестник Дона. 2012. Т. 20. № 2. С. 17-26.

10. Ажмухамедов И. М., Марьенков А. Н. Выявление аномалий в вычислительных сетях общего пользования на основе прогнозирования объема сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2012. № 3. С. 35-39.

11. Шелухин О. И., Судариков Р. А. Анализ информативных признаков в задачах обнаружения аномалий трафика статистическими методами // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 3. С. 14-18.

12. Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М. Распределённая система защиты облачных вычислений от сетевых атак // Вестник СибГУТИ. 2013. № 3. С. 46-62.

13. Шелухин О. И., Филинова А. С. Сравнительный анализ алгоритмов обнаружения аномалий трафика методами дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 89-97.

14. Шелухин О. И., Гармашев А .В. Обнаружение аномальных выбросов телекоммуникационного трафика методами дискретного вейвлет-анализа // Электромагнитные волны и электронные системы. 2012. Т. 17. № 2. С. 15-26.

15. Шелухин О. И., Гармашев А. В. Обнаружение DOS и DDOS-атак методом дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2011. № 1. С. 44-46.

16. Ажмухамедов И. М., Марьенков А. Н. Определение аномалий объема сетевого трафика на основе аппарата нечетких множеств // Вестник

Астраханского государственного технического университета. 2011. № 1. С. 48-50.

17. Басараб М. А., Строганов И. С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30-40.

18. Шелухин О. И., Антонян А. А. Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 6. С. 61-64.

19. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol // Przegląd Elektrotechniczny. 2014. Vol. 90. № 1. P. 127-130.

20. Tarrío P., Bernardos A. M., Casar J. R. Weighted least squares techniques for improved received signal strength based localization // Sensors. 2011. Т. 11. № 9. С. 8569-8592.

21. Фраленко В. П. Обнаружение сетевых атак с помощью генетически создаваемых конечных автоматов // Вестник РУДН. Серия Математика. Информатика. Физика. 2012. № 4. С. 96-102.

22. Шелухин О. И., Чернышев А. И. Исследование и моделирование нейросетевых алгоритмов обнаружения аномальных вторжений в компьютерные сети // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 12. С. 102-106.

23. Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М. Эксперименты по нейросетевому мониторингу и распознаванию сетевых атак // Информационное противодействие угрозам терроризма. 2010. № 15. С. 81-86.

24. Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М. Разработка нейросетевого модуля мониторинга аномальной сетевой активности // Нейрокомпьютеры: разработка и применение. 2011. № 7. С. 32-38.

25. Большев А. К., Яновский В. В. Применение нейронных сетей для обнаружения вторжений в компьютерные сети // Вестник Санкт-Петербургского университета. Серия 10. Прикладная математика. Информатика. Процессы управления. 2010. № 1. С. 129-135.

26. Lei J. Z., Ghorbani A. Network Intrusion Detection Using an Improved Competitive Learning Neural Network // Proc. of Second Annual Conf. on Communication Networks and Services Research. 2004. P. 190-197.

27. Wang G., Hao J., Ma J., Huang L. A New Approach to Intrusion Detection Using Artificial Neural Net-works and Fuzzy Clustering // Expert Systems with Applications. 2010. Vol. 37. No. 9. P. 6225-6232.

28. Lei J. Z., Ghorbani A. A. Improved Competitive Learning Neural Networks for Network Intrusion and Fraud Detection // Neurocomputing. 2012. Vol. 75. No. 1. P. 135-145.

29. Cannady J. Artificial Neural Networks for Misuse Detection // Proc. of National Information Systems Security Conf. 1998. P. 368-381.

30. Toosi A. N., Kahani M., Monsefi R. Network Intrusion Detection Based on Neuro-Fuzzy Classification // Proc. of Intern. Conf. on Computing and Informatics. 2006. P. 1-5.

31. Orang Z. A., et al. Using Adaptive Neuro-Fuzzy Inference System in Alert Management of Intrusion Detection Systems // Intern. Journal of Computer Network and Information Security. 2012. Vol. 4. No. 1. P. 32-38.

32. Zainal A., Maarof M. A., Shamsuddin S. M. Ensemble Classifiers for Network Intrusion Detection System // Information Assurance and Security. 2009. Vol. 4. P. 217-225.

33. Hofmeyr S. A., Forrest S. Architecture for an Artificial Immune System // Journal of Evolutionary Computation. 2000. Vol. 8. No. 4. P. 443-473.

34. Hofmeyr S. A. An Immunological Model of Distributed Detection and its Application to Computer Security: PhD dissertation. – Department of Computer Sciences, University of New Mexico. 1999. – 113 p.

35. Тищенко И. П., Фраленко В. П., Хачумов В. М. Программно-инструментальные средства обнаружения и распознавания сетевых атак // Прикладная физика и математика. 2013. № 4. С. 70-85.

36. Браницкий А. А., Котенко И. В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов // Информационно-управляющие системы. 2015. № 4. С. 69-77.

37. Zhou Y. P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection // Asia-Pacific Conf. on Information Processing. 2009. Vol. 1. P. 21-24.

38. Powers S. T., He J. A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection // Information Sciences. 2008. Vol. 178. No. 15. P. 3024-3042.

39. Корнев П. А., Пылькин А. Н., Свиридов А. Ю. Применение инструментария искусственного интеллекта в системах обнаружения вторжений в вычислительные сети // Современные проблемы науки и образования. 2014. № 6. С. 1715.

40. Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. 2011. № 3 (7). С. 3-15.

41. Кондратьев А. А., Тищенко И. П., Фраленко В. П. Разработка распределенной системы защиты облачных вычислений // Программные системы: теория и приложения. 2011. № 4 (8). С. 61-70.

42. Емельянова Ю. Г., Фраленко В. П. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения. 2011. № 4 (8). С. 17-31.

43. Ушанев К. В. Имитационные модели системы массового обслуживания типа $Pa/M/1$, $H_2/M/1$ и исследование на их основе качества обслуживания трафика со сложной структурой // Системы управления, связи и безопасности. 2015. № 4. С. 217-251.

44. Ушанев К. В., Макаренко С. И. Показатели своевременности обслуживания трафика в системе массового обслуживания *Pa*/*M*/1 на основе аппроксимации результатов имитационного моделирования // Системы управления, связи и безопасности. 2016. № 1. С. 42-65. – URL: http://sccs.intelgr.com/archive/2016-01/03-Ushanev.pdf (дата обращения 01.12.2016).

45. Рыжиков Ю. И. Расчет систем обслуживания с групповым поступлением заявок // Информационно-управляющие системы. 2007. № 2. С. 39-49.

46. Рыжиков Ю. И. Полный расчет системы обслуживания с распределениями Кокса // Информационно-управляющие системы. 2006. № 2. С. 38-46.

47. Будко П. А., Рисман О. В. Многоуровневый синтез информационно-телекоммуникационных систем. Математические модели и методы оптимизации. – СПб.: ВАС, 2011. – 476 с.

48. Малофей О. П., Фомин Л. А., Родионов В. В., Ряднов Д. С. Моделирование самоподобного трафика при построении сетей NGN // Известия Южного федерального университета. Технические науки. 2009. № 11. С. 176-186.

49. Бахарева Н. Ф., Карташевский И. В., Тарасов В.Н. Анализ и расчет непуассоновских моделей трафика в сетях ЭВМ // Инфокоммуникационные технологии. 2009. Т. 7. № 4. С. 61-66.

50. Тарасов В. Н., Бахарева Н. Ф., Горелов Г. А. Математическая модель трафика с тяжелохвостным распределением на основе системы массового обслуживания H_2/M/1 // Инфокоммуникационные технологии. 2014. Т. 12. № 3. С. 36-41.

51. Шелухин О. И., Иванов Ю. А., Пастухов А. С. Исследование влияния самоподобия ON-OFF источников на скорость интернет-трафика // Электротехнические и информационные комплексы и системы. 2008. Т. 4. № 1-2. С. 97-100.

52. Назаров А. Н., Сычев К. И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. – Красноярск: «Поликом», 2010. – 389 с.

53. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. № 3 (4). 2014. С. 7-13.

54. Макаренко С. И. Анализ математических моделей информационных потоков общего вида и степени их соответствия трафику сетей интегрального обслуживания // Вестник Воронежского государственного университета. 2012. Т. 8. № 8. С. 28-35.

55. Задорожный В. Н., Долгушин Д. Ю., Юдин Е. Б. Аналитико-имитационные методы решения актуальных задач системного анализа больших сетей / Под ред. В. Н. Задорожного – Омск: Издательство ОмГТУ, 2013. – 324 с.

56. Ушанев К. В., Макаренко С. И. Преобразование структуры трафика с учетом требований по качеству его обслуживания // Радиотехнические и телекоммуникационные системы. 2015. № 2. С. 74-84.

57. Линец Г. И. Методы структурно-параметрического синтеза, идентификации и управления транспортными телекоммуникационными сетями для достижения максимальной производительности: Автореф. дис. … д-ра техн. наук. Ставрополь: Северо-Кавказский федеральный университет, 2013. – 34 с.

58. Линец Г. И., Фомин Л. А., Скоробогатов С. А. Снижение влияния самоподобности трафика в пакетных сетях // Автоматизация, телемеханизация и связь в нефтяной промышленности. 2008. № 11. С. 38-42.

59. Линец Г. И., Фомин Л. А., Скоробогатов С. А., Криволапов Р. В. Способ снижения влияния самоподобности в сетевых структурах и устройство для его осуществления // Патент на изобретение № 2413284. 27.02.2011.

60. Линец Г. И., Фомин Л. А., Говорова С. В., Меденец В. В. Построение мультисервисных сетей на основе функциональных преобразований трафика // Инфокоммуникационные технологии. 2014. Т. 12. № 4. С. 40-45.

61. Вентцель Е. С. Теория вероятностей. – М.: Высшая школа, 2002. – 575 с.

62. Новиков Е. А., Павлов А. Р., Зиннуров С. Х. Метод оперативного планирования частотно-временного ресурса спутника-ретранслятора при нестационарном входном потоке сообщений // Авиакосмическое приборостроение. 2014. № 5. С. 14-23.

63. Новиков Е. А. Оперативное распределение радиоресурса спутника-ретранслятора при нестационарном входном потоке сообщений с учетом запаздывания в управлении // Информационно-управляющие системы. 2014. № 2 (69). С. 79-86.

64. Новиков Е. А., Косяков Е. Н., Павлов А. Р. Динамическое резервирование радиоресурса в сетях спутниковой связи при передаче самоподобного трафика // Труды Научно-исследовательского института радио. 2014. № 2. С. 49-60.

65. Жуков С. Е., Новиков Е. А., Павлов А. Р. Метод динамического распределения радиоресурса ретранслятора в сетях спутниковой связи с учетом неоднородности трафика и запаздывания при управлении // Труды Научно-исследовательского института радио. 2014. № 1. С. 74-80.

References

1. Mikhailov R. L., Makarenko S. I. Estimating Communication Network Stability under the Conditions of Destabilizing Factors Affecting it. *Radio and telecommunication systems*, 2013, no. 4, pp. 69-79 (in Russian).

2. Makarenko S. I., Chucklyaev I I. The Terminological Basis of the Informational Conflict Area. *Voprosy kiberbezopasnosti*, vol. 2, no. 1, 2014, pp. 13-21 (in Russian).

3. Makarenko S. I., Mikhailov R. L. Information Conflicts – Analysis of Papers and Research Methodology. *Systems of Control, Communication and Security*, 2016,

no. 3, pp. 95-178. Available at: http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf (accessed 17 September 2016) (in Russian).

4. Makarenko S. I. Information Weapon in Technical Area – Terminology, Classification and Examples. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 292-376. Available at: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (accessed 05 December 2016) (in Russian).

5. Mikova S. Iu., Oladko V. S., Nesterenko M. A. Podkhod k klassifikatsii anomalii setevogo trafika [The approach to classification of anomalies in network traffic]. *Innovatsionnaia nauka*, 2015, no. 11, pp. 78-80 (in Russian).

6. Bagrov E. V. Monitoring i audit informatsionnoi bezopasnosti na predpriiatii [Monitoring and auditing of information security in the enterprise]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriia 10: Innovatsionnaia deiatel'nost*, 2011, no. 5, pp. 54-56 (in Russian).

7. Artamonov V. A. Obnaruzhenie setevykh anomalii cherez rekonstruktsiiu setevogo trafika [Detection of network anomalies through the reconstruction of network traffic]. *Izvestiya SFedU. Engineering Sciences*, 2007, no. 1, pp. 127-130 (in Russian).

8. Sheluhin O. I., Sakalema D. Zh., Filinova A. S. *Obnaruzhenie vtorzhenii v komp'iuternye seti (setevye anomalii)* [Intrusion detection in computer networks (network anomalies)]. Moscow, Goriachaia liniia - Telekom Publ., 2013. 220 p. (in Russian).

9. Azhmukhamedov I. M., Marenkov A. N. Poisk i otsenka anomalii setevogo trafika na osnove tsiklicheskogo analiza [Search and evaluation of anomalies in network traffic]. *Engineering journal of Don*, 2012, vol. 20, no. 2, pp. 17-26 (in Russian).

10. Azhmukhamedov I. M., Marenkov A. N. Vyiavlenie anomalii v vychislitel'nykh setiakh obshchego pol'zovaniia na osnove prognozirovaniia ob"ema setevogo trafika [Anomaly detection in computer networks based on the prediction of network traffic]. *Information Security Problems. Computer Systems*, 2012, no. 3, pp. 35-39 (in Russian).

11. Sheluhin O. I., Sudarikov R. A. Analysis of diagnostic criteria for statistical network anomaly detection. *T-Comm*, 2014, vol. 8, no. 3, pp. 14-18 (in Russian).

12. Talalaev A. A., Tishchenko I. P., Fralenko V. P., Khachumov V. M. Distributed security system for cloud protection from network attacks. Vestnik SibGUTI, 2013, no. 3, pp. 46-62 (in Russian).

13. Sheluhin O. I., Filinova A. S. The comparative analysis of detection algorithms detection of traffic anomalies methods of the discrete wavelet-analysis. *T-Comm*, 2014, vol. 8, no. 9, pp. 89-97 (in Russian).

14. Sheluhin O. I., Garmashev A. V. Detection of abnormal spikes in network traffic by methods of discrete wavelet analysis. *Elektromagnitnye volny i elektronnye sistemy*, 2012, vol. 17, no. 2, pp. 15-26 (in Russian).

15. Shelukhin O. I., Garmashev A. V. Obnaruzhenie DOS i DDOS-atak metodom diskretnogo veivlet-analiza [Detection DOS and DDOS attacks using discrete wavelet analysis]. *T-Comm*, 2011, no. 1, pp. 44-46 (in Russian).

16. Azhmukhamedov I. M., Marienkov A. N. Network traffic anomaly detection based on fuzzy sets apparatus. *Vestnik of Astrakhan State Technical University*, 2011, no. 1, pp. 48-50 (in Russian).

17. Basarab M. A., Stroganov I. S. Anomaly detection in information processes based on multifractal analysis. Voprosy kiberbezopasnosti, 2014, vol. 7, no. 4, pp. 30-40 (in Russian).

18. Sheluhin O. I., Antonian A. A. Analysis of changes in the fractal properties of telecommunication traffic caused by abnormal invasions. *T-Comm*, 2014, vol. 8, no. 6, pp. 61-64 (in Russian).

19. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol. *Przegląd Elektrotechniczny*, 2014, vol. 90, no. 1, pp. 127-130.

20. Tarrío P., Bernardos A. M., Casar J. R. Weighted least squares techniques for improved received signal strength based localization. *Sensors*, 2011, vol. 11, no. 9, pp. 8569-8592.

21. Fralenko V. P. Intrusion Detection using Genetically Generated Finite Automata. *Bulletin of the Russian University of Peoples' Friendship. Series Mathematics. Informatics. Physics*, 2012, no. 4, pp. 96-102 (in Russian).

22. Shelukhin O. I., Chernyshev A. I. Research and modeling neural network algorithm for detecting an abnormal intrusion. *T-Comm*, 2014, vol. 8, no. 12, pp. 102-106 (in Russian).

23. Talalaev A. A., Tishchenko I. P., Fralenko V. P., Khachumov V. M. Eksperimenty po neirosetevomu monitoringu i raspoznavaniiu setevykh atak [Experiments on neural network monitoring and detection of network attacks] // *Information counteraction to the terrorism threats*, 2010, no. 15, pp. 81-86 (in Russian).

24. Talalaev A.A., Tishchenko I. P., Fralenko V. P., Khachumov V. M. Working out neural of the module of monitoring of abnormal network activity. *Neyrokompyutery: razrabotka i primenenie*, 2011, no. 7, pp. 32-38 (in Russian).

25. Bolshev A. K., Yanovskiy V. V. Using artificial neural networks in network intrusion detection. *Vestnik of St. Petersburg State University. Series 10. Applied Mathematics. Computer Science. Control Processes*, 2010, no. 1, pp. 129-135 (in Russian).

26. Lei J. Z., Ghorbani A. Network Intrusion Detection Using an Improved Competitive Learning Neural Network. *Proc. of Second Annual Conf. on Communication Networks and Services Research*, 2004, pp. 190-197.

27. Wang G., Hao J., Ma J., Huang L. A New Approach to Intrusion Detection Using Artificial Neural Net-works and Fuzzy Clustering. *Expert Systems with Applications*, 2010, vol. 37, no. 9. pp. 6225-6232.

28. Lei J. Z., Ghorbani A. A. Improved Competitive Learning Neural Networks for Network Intrusion and Fraud Detection. *Neurocomputing*, 2012, vol. 75, no. 1, pp. 135-145.

29. Cannady J. Artificial Neural Networks for Misuse Detection. *Proc. of National Information Systems Security Conf*, 1998, pp. 368-381.

30. Toosi A. N., Kahani M., Monsefi R. Network Intrusion Detection Based on Neuro-Fuzzy Classification. *Proc. of Intern. Conf. on Computing and Informatics*, 2006, pp. 1-5.

31. Orang Z. A., et al. Using Adaptive Neuro-Fuzzy Inference System in Alert Management of Intrusion Detection Systems. *Intern. Journal of Computer Network and Information Security*, 2012, vol. 4. no. 1, pp. 32-38.

32. Zainal A., Maarof M. A., Shamsuddin S. M. Ensemble Classifiers for Network Intrusion Detection System. *Information Assurance and Security*, 2009, vol. 4, pp. 217-225.

33. Hofmeyr S. A., Forrest S. Architecture for an Artificial Immune System. Journal of Evolutionary Computation, 2000, vol. 8, no. 4, pp. 443-473.

34. Hofmeyr S. A. *An Immunological Model of Distributed Detection and its Application to Computer Security: PhD dissertation*. Department of Computer Sciences, University of New Mexico. 1999. 113 p.

35. Tishchenko I. P., Fralenko V. P., Khachumov V. M. Software and tools for network attacks detection and identification. *Applied Physics and Mathematics*, 2013, no. 4, pp. 70-85 (in Russian).

36. Branitskiy A. A., Kotenko I. V. Network Attack Detection Based on Combination of Neural, Immune and Neuro-fuzzy Classifiers. *Informatsionno-upravliaiushchie sistemy*, 2015, no. 4, pp. 69-77 (in Russian).

37. Zhou Y. P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection. *Asia-Pacific Conf. on Information Processing*, 2009, vol. 1, pp. 21-24.

38. Powers S. T., He J. A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection. Information Sciences, 2008, vol. 178, no. 15, pp. 3024-3042.

39. Kornev P. A., Pylkin A. N., Sviridov A. U. Using artificial intelligence in intrusion detection systems. *Modern problems of science and education*, 2014, no. 6, pp. 1715 (in Russian).

40. Yemelyanova Yu. G., Talalaev A. A., Tishchenko I. P., Fralenko V. P. Neyrosetevaya tekhnologiya obnaru-zheniya setevykh atak na informatsionnye resursy [Neural network intrusion detection technology to in-formation resources]. *Programmnye sistemy: teoriya i prilozheniya*, 2011, vol. 7, no. 3, pp. 3-15 (in Russian).

41. Kondratev A. A., Tishchenko I. P., Fralenko V. P. Razrabotka raspredelennoy sistemy zashchity oblachnykh vychisleniy [Development of a distributed cloud computing security]. *Programmnye sistemy: teoriya i prilozheniya*, 2011, vol. 8, no. 4, pp. 61-70 (in Russian).

42. Yemelyanova Yu. G., Fralenko V. P. Analiz problem i perspektivy sozdaniya intellektualnoy sistemy obnaruzheniya i predotvrashcheniya setevykh atak na oblachnye vychisleniya [Analysis of the problems and prospects of creating an intelligent system to detect and prevent network attacks on cloud computing]. *Programmnye sistemy: teoriya i prilozheniya*, 2011, vol. 8, no. 4, pp. 17-31 (in Russian).

43. Ushanev K. V. Simulation Models of Queuing Systems of Type *Pa*/*M*/1, H_2/*M*/1 and Research on the Basis of their Quality of Service Traffic with a Complicated Structure. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 217-251 (in Russian).

44. Ushanev K.V., Makarenko S. I. The Timeliness Indicators of Traffic Service in Queue Systems Pa/M/1 Based on Approximation of Imitating Modeling Results. *Systems of Control, Communication and Security*, 2016, no. 1, pp. 42-65. Available at: http://sccs.intelgr.com/archive/2016-01/03-Ushanev.pdf (accessed 01 December 2016) (in Russian).

45. Ryzhikov Y. I. Raschet sistem obsluzhivanija s gruppovym postupleniem zajavok [Calculation of Systems of Service with Group Receipt of Demands]. *Informatsionno-upravliaiushchie sistemy*, 2007, no. 2, pp. 39-49 (in Russian).

46. Ryzhikov Y. I. Polnyj raschet sistemy obsluzhivanija s raspredelenijami Koksa [Full Calculation of System of Service with Cox's Distributions]. *Informatsionno-upravliaiushchie sistemy*, 2006, no. 2, pp. 38-46 (in Russian).

47. Budko P. A., Risman O. V. *Mnogourovnevyj sintez informacionno-telekommunikacionnyh sistem. matematicheskie modeli i metody optimizacii* [Multilevel Synthesis of Information and Telecommunication Systems. Mathematical Models and Methods of Optimization]. Saint-Petersburg, Military Academy of Communications, 2011. 476 p. (in Russia).

48. Malofej O. P., Fomin L. A., Rodionov V. V., Rjadnov D. S. Modelirovanie samopodobnogo trafika pri postroenii setej NGN [Modeling of a Self-Similar Traffic at Creation of the NGN Networks]. *Izvestiya Southern Federal University. Engineering Sciences*, 2009, no. 11, pp. 176-186 (In Russian).

49. Bakhareva N. F., Kartashevskii I. V., Tarasov V. N. Analiz i raschet nepuassonovskih modelej trafika v setjah EVM [The Analysis and Calculation of Not-Poisson Traffic Models in Computer Networks]. *Infokommunikacionnye Tehnologii*, 2009, vol. 7, no. 4, pp. 61-66 (in Russian).

50. Tarasov V. N., Bakhareva N. F., Gorelov G. A. Matematicheskaja model' trafika s tjazhelohvostnym raspredeleniem na osnove sistemy massovogo obsluzhivanija [The Mathematical Model of Traffic with Heavy Tail Distribution on the Basis of Queuing System Type of H_2/M/1]. *Infokommunikacionnye Tehnologii*, 2014, vol. 12, no. 3, pp. 36-41 (in Russian).

51. Sheluhin O. I., Ivanov Y. A., Pastuhov A. S. Issledovanie vlijanija samopodobija ON-OFF istochnikov na skorost' internet-trafika [Research of Influence of Self-simIlarity of ON-OFF of Sources on Internet Traffic Speed]. *Elektrotehnicheskie i informacionnye kompleksy i sistemy*, 2008, vol. 4. no. 1-2, pp. 97-100 (in Russian).

52. Nazarov A. N., Sychev K. I. *Modeli i metody rascheta pokazatelej kachestva funkcionirovanija uzlovogo oborudovanija i strukturno-setevyh parametrov setej svjazi sledujushhego pokolenija* [The Models and the Methods of Measuring of Quality Indicators of Nodal Equipment Functioning and Network Structural Parameters of Next Generation Networks]. Krosnoyarsk, Polykom Publ., 2010. 389 p. (in Russian).

53. Makarenko S. I. Premeditated formation of the traffic of difficult structure due to implementation in the communication system of additional imitative traffic. *Voprosy kiberbezopasnosti*, 2014, vol. 4, no. 3, pp. 7-13 (in Russian).

54. Makarenko S. I. Analyzing of Mathematical Models of General type Data Streams and Degree of their Conformity to Integral Service Net Traffic. *Proceedings of Voronezh State University*, 2012, vol. 8, no. 8, pp. 28-35 (in Russian).

55. Zadorozhnii V. N., Dolgushin D. U., Udin E. B. *Analitiko-imitatsionnye metody resheniia aktual'nykh zadach sistemnogo analiza bol'shikh setei* [Analytical-Imitating Methods of the Decision of Actual Problems of the System Analysis of the Big Networks]. Omsk, Omsk State Technical University Publ., 2013. 324 p. (in Russian).

56. Ushanev K. V., Makarenko S. I. Traffic structure conversion with requirements for the traffic service quality. *Radio and telecommunication systems*, 2015, no. 2, pp. 74-84 (In Russian).

57. Linec G. I. *Metody strukturno-parametricheskogo sinteza, identifikacii i upravlenija transportnymi telekommunikacionnymi setjamin dlja dostizhenija maksimal'noj proizvoditel'nosti.* Diss. dokt. tehn. nauk [The Methods of Structural Parametric Synthesis, Identification and Control of Transport Telecommunication Networks for Achievement of the Maximum Productivity. Extended Abstract of Dr. habil. Thesis]. Stavropol, Northern-Caucasus State University, 2013. 34 p. (in Russian).

58. Linec G. I., Fomin L. A., Skorobogatov S. A. Snizhenie vlijanija samopodobnosti trafika v paketnyh setjah [Lowering of Influence of Self-Similitude of Traffic on Package Networks]. *Automation, Telemechanization and Communication in Oil Industry*, 2008, no. 11, pp. 38-42 (in Russian).

59. Linec G. I., Fomin L. A., Skorobogatov S. A., Krivolapov R. V. *Sposob snizhenija vlijanija samopodobnosti v setevyh strukturah i ustrojstvo dlja ego osushhestvlenija* [The Way of Lowering Self-Similitude on Network Structures and the Device for Its Realization]. Patent Russia, no. 2413284, 27 February 2011. (in Russian).

60. Linec G. I., Fomin L. A., Govorova S. V., Medenec V. V. *Postroenie mul'tiservisnyh setej na osnove funkcional'nyh preobrazovanij trafika* [Creation of Multiservice Networks on the Basis of the Functional Transformations of Traffic]. *Infokommunikacionnye Tehnologii*, 2014, vol. 12, no. 4, pp. 40-45 (in Russian).

61. Venttsel E. S. *Teoriia veroiatnostei* [Probability theory]. Moscow, Vysshaia Shkola Publ., 2002. 575 p. (in Russian).

62. Novikov E. A., Pavlov A. R., Zinnurov S. H. Method of operative planning of the satellite repeater's time-and-frequency resource under non stationary ingress flow. *Aerospace Instrument Making*, 2014, no. 5, pp. 14-23 (in Russian).

63. Novikov E. A. Operative distribution of satellite repeater radio resource in terms of non-stationary ingress flow with account of time lagged control. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 69, no 2, pp. 79-86 (in Russian).

64. Novikov E. A., Kosyakov E. N., Pavlov A. R. Dynamic reservation of a radio resource in satellite communication networks by transfer of the self-similar traffic. *Trudi NIIR*, 2014, no. 2, pp. 49-60 (in Russian).

65. Zhukov S. E., Novikov E. A., Pavlov A. R. Method of radio resource dynamic distribution in networks of satellite communication taking into account heterogeneity of a traffic and delay at management. *Trudi NIIR*, 2014, no. 1, pp. 74-80 (in Russian).

Статья поступила 09 декабря 2016 г.

Информация об авторах

Макаренко Сергей Иванович – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей и систем связи к преднамеренным деструктивным воздействиям; радиоэлектронная борьба; информационное противоборство. E - mail: mak-serg@yandex.ru

Коровин Виталий Михайлович – кандидат технических наук. Старший преподаватель кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: цифровая стеганография, прием и обработка сложных радиотехнических сигналов; математическое моделирование процессов в системах связи. E - mail: 9112116532@mail.ru

Ушанев Константин Владимирович – кандидат технических наук. Инженер лаборатории кафедры систем и средств радиоэлектронной борьбы космического назначения. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: передача и обработка трафика со сложной и самоподобной структурой. E - mail: stan_007@mail.ru

Адрес: Россия, 197198, г. Санкт-Петербург, ул. Ждановская д. 13.

The Traffic Transformation Operator for Deliberate Increase of the Structural Complexity of the Information Stream

S. I. Makarenko, V. M. Korovin, K. V. Ushanev

Statement of the problem. *Theory of information security and theory of information warfare evolve and require the development of new models of cyber-attacks. These new cyber-attacks can be used to test resilience and security of the telecommunication systems. Analysis of means of identifying cyber-attacks showed that their detection is based on the analysis of intensity of the network traffic. Thus, the new cyber attacks that have a high stealth, it must ensure that the traffic intensity remain the same in during the attack. Such cyber-attacks can be based on the formation of the complexity structure of traffic that is transmitted on the network.* ***The aim of the paper*** *is development of the scientific-methodological apparatus for the research of cyber-attacks which are based on the transformation of the traffic structure to make it more complicated. This scientific-methodological apparatus will keep the same intensity of traffic, but to ensure the formation of traffic patterns with a much higher level of complexity. This traffic processed in the individual network nodes and reduces of timeliness of the network as a whole.* ***Methods used.*** *The scientific-methodological apparatus for the research of cyber attacks is based on the method of functional transformation of traffic.* ***Results and novelty.*** *The traffic transformation operator that proposed in paper from the elementary stream makes a stream with a complex structure. This operator was researched. The research revealed that the traffic transformation consists of two processes. The first process is compression*

of the intervals between packets and formation of the "packs" of traffic. The second process is "rarefaction" of the intervals between the packets and formation of the long pauses between "packs" of packets. Proposals for the use of these two processes to substantiate the parameters of cyber-attacks made in the paper. ***Practical significance.*** *The traffic transformation operator is the basis of scientific-methodological apparatus for the study of a new cyber attacks. Such a cyber attack will be covert in relation to existing means for attack detection which is based on the analysis of the network traffic intensity. These new cyber-attacks can be used to test resilience and security of telecommunication systems, and to develop protection methods.*

Key words: *information security, information warfare, network attack, intrusion detection, methods of detecting network attacks, information technology impact, converting traffic, complex traffic, complex structure.*

Information about Authors

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. A. F. Mozhaisky Military Space Academy. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E–mail: mak-serg@yandex.ru

Vitaly Mikhaylovich Korovin – Ph.D. of Engineering Sciences. Senior Lecturer at the Department of Networks and Communication Systems of Space Systems. A. F. Mozhaisky Military Space Academy. Field of research: digital steganography, reception and processing of complex radio signal; mathematical modeling of processes in communication systems. E - mail: 9112116532@mail.ru

Konstantin Vladimirovich Ushanev – Ph.D. of Engineering Sciences. The Engineer of the Laboratory of the Department of the Space Electronic Warfare Systems. A. F. Mozhaisky Military Space Academy. Field of research: the transmission and servicing of the complicated structure traffic and self-similar structure traffic. E-mail: stan_007@mail.ru

Address: Russia, 197198, Saint-Petersburg, Zhdanovskaya str., 13.