ПРЕДНАМЕРЕННОЕ ФОРМИРОВАНИЕ ИНФОРМАЦИОННОГО ПОТОКА СЛОЖНОЙ СТРУКТУРЫ ЗА СЧЕТ ВНЕДРЕНИЯ В СИСТЕМУ СВЯЗИ ДОПОЛНИТЕЛЬНОГО ИМИТАЦИОННОГО ТРАФИКА

***Макаренко Сергей Иванович**, кандидат технических наук*

В работе предложено деструктивное информационно–техническое воздействие на систему связи направленное на повышение времени обработки информационных потоков в узлах маршрутизации. Воздействие реализуется за счет преднамеренного формирования сложной структуры передаваемого по системе связи информационного потока. Формировать сложную структуру информационного потока предлагается за счет внедрения в систему связи дополнительного имитационного трафика с параметрами, рассчитываемыми в соответствии с предложенной в статье методикой. Представленное в статье формализованное описание предлагаемого воздействия может быть использовано в составе модели противника/нарушителя при решении задач обеспечения безопасности и устойчивости систем связи.

***Ключевые слова**: сетевой трафик, управление трафиком, информационно–техническое воздействие, компьютерная атака.*

PREMEDITATED FORMATION OF THE TRAFFIC OF DIFFICULT STRUCTURE DUE TO IMPLEMENTATION IN THE COMMUNICATION SYSTEM OF ADDITIONAL IMITATIVE TRAFFIC

***Sergey Makarenko**, Ph.D.*

A cyber–attack directed on increase of processing time of information flows in routing nodes of communication system is offered in the article. A cyber–attack is implemented by application premeditated formation of the information flow of complex structure circulating in a network. The information flow of complex structure is offered to be received by means of application of additional imitative traffic. Parameters of additional imitative traffic are calculated by a technique offered in the article. The formalized description of offered influence can be used in form of model of the opponent/violator for providing safety and stability of communication systems.

***Keywords**: network traffic, traffic management, cyber–attack.*

Введение

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

К исследованиям, проведенным раннее, и рассматривающим влияние деструктивных воздействий на системы и сети связи по обработке пакетных информационных потоков стоит отнести следующие: работу Шабалина Е.А. по управлению информационными потоками сетей радиосвязи в условиях радиоэлектронного противоборства [2]; работу Чакрян В.Р. по моделированию телетрафика и каналов передачи данных в условиях помех [3]; работу Семеновой О.В. по исследова-

нию систем массового обслуживания с катастрофическими сбоями [4]; работу Вавилова В.А. [5] по анализу систем множественного доступа функционирующих в случайной среде. Однако в этих исследованиях деструктивное воздействие рассматривается как фактор среды функционирования. В данной работе предлагается рассмотреть активное деструктивное воздействие направленное не на дестабилизацию среды передачи или процесса обработки информационных потоков, а на формирование заданной структуры информационных потоков. Предполагается, что такое формирование информационных потоков 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 информационных потоков ниже значений определяемых требованиями к системе связи.

В основу методики предлагаемой в данной работе положены подходы по моделированию трафика со сложной структурой предложенные Алиевым Т.И. [6] и Рыжиковым Ю.И. [7], результаты исследований Бахаревой Н.Ф и Ушакова Ю.А. [8, 9] по обработке информационных потоков со сложной структурой в узлах маршрутизации, а так же работы Коллерова А.С. [9] и Линца Г.И. [11, 12] в которых решаются задачи по направленному формированию структуры сетевого трафика с заданными свойствами.

В работах [8, 9] указывается на существенное повышение времени обработки информационных потоков со сложной структурой в узлах маршрутизации и коммутации пакетов. При этом под потоком сложной структуры понимается поток, у которого коэффициент вариации интервалов времени между поступлениями отдельных пакетов больше единицы (c_τ>1). Как отмечается в этих работах, проведение исследований на аналитических моделях и реальном телекоммуникационном оборудовании показало, что в отдельных случаях увеличение сложности информационного потока по показателю коэффициента вариации с c_τ=1 до c_τ=1,5 увеличивает время обработки в узлах 1,5-2 раза, а при увеличении до c_τ=2 время обработки увеличивается в 5-6 раз!

Рассмотрим реализацию активного деструктивного ИТВ, реализуемого за счет перехвата пакетов, формирования из перехваченных пакетов дополнительного трафика, который внедряется обратно в систему связи с целью формирования сложной структуры передаваемого по ней информационного потока.

Постановка задачи

Имеется пакетная система связи, состоящая из источника и получателя пакетов между которыми ведется передача информационного потока $\lambda_{осн}$, структура которого соответствует пуассоновскому потоку с коэффициентом вариации интервалов времени между поступлениями отдельных пакетов $c_\tau=\sigma_\tau/m_\tau\approx1$. К данной системе связи подключен специализированный комплекс деструктивного воздействия, состоящий из системы перехвата (СП) и системы формирования трафика (СФТ). Задача комплекса деструктивного воздействия сформировать структуру трафика с коэффициентом вариации c_τ>1 за счет внедрения в систему связи дополнительного потока $\lambda_{доп}$ (рис. 1).

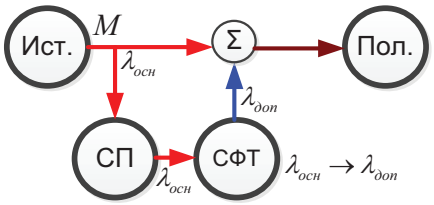


Рис. 1. *Система связи с подключенным к ней специализированным комплексом деструктивного воздействия*

Для формализации задачи введем следующие обозначения:

τ - интервал времени между поступлениями отдельных пакетов в потоке;

p_1 – вероятность поступления пакетов 1-го источника простейшего потока;

p_2 – вероятность поступления пакетов 2-го источника простейшего потока;

T_1 – математическое ожидание значений интервалов времени между поступлениями отдельных пакетов 1-го источника простейшего потока;

T_2 – математическое ожидание значений интервалов времени между поступлениями отдельных пакетов 2-го источника простейшего потока;

$\lambda_1=1/T_1$ – интенсивность поступления пакетов 1-го источника простейшего потока;

$\lambda_2=1/T_2$ – интенсивность поступления пакетов 2-го источника простейшего потока;

m_τ – математическое ожидание значений интервалов времени между поступлениями отдельных пакетов в смешанном потоке;

$\lambda_\Sigma\approx1/m_\tau$ – интенсивность поступления пакетов в смешанном потоке;

σ_τ – среднее квадратичное отклонение значений интервалов времени между поступлениями отдельных пакетов в смешанном потоке;

$c_\tau=\sigma_\tau/m_\tau$ – коэффициент вариации значений интервалов времени между поступлениями отдельных пакетов в смешанном потоке;

$\lambda_{осн}$ – интенсивность отправления пакетов отправителем в основном потоке, передаваемом системой связи;

$\lambda_{доп}$ – интенсивность отправления пакетов СФТ в дополнительном потоке внедряемом в систему связи;

$p_{осн}$ – вероятность приема Получателем пакетов основного потока;

$p_{доп}$ – вероятность приема Получателем пакетов дополнительного потока от СФТ;

Для решения задачи определения параметров деструктивного воздействия сначала рассмотрим модель, используемую для аппроксимации гиперэкспоненциального потока системой экспоненциальных источников, на основе которой в дальнейшем будет сформирована методика направленного формирования сложной структуры информационных потоков.

Модель гиперэкспоненциального потока

В основу модели положены работы [6, 7, 13] в которых указывается на возможность аппроксимации информационных потоков с $c_\tau>1$ гиперэкспоненциальным распределением второго порядка образованным двумя экспоненциальными источниками.

Рассмотрим модель представляющую собой систему из двух источников простейших потоков $И_1$ и $И_2$ (рис. 2). Параметрами этой модели являются: p_1 – вероятность поступления пакетов потока от $И_1$ с математическим ожиданием интервалов между пакетами T_1 (соответственно интенсивностью $\lambda_1=1/T_1$); $p_2=1-p_1$ – вероятность поступления пакетов потока от $И_2$ с математическим ожиданием интервалов между пакетами T_2 (соответственно интенсивностью, $\lambda_2=1/T_2$).

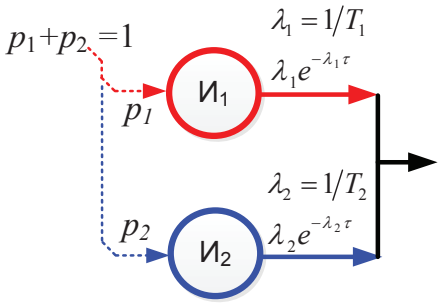


***Рис. 2.** Двухфазное представление гиперэкспоненциального распределения H_2*

Математическое ожидание интервалов между поступлениями отдельных пакетов в условиях одновременного поступления двух потоков будет равно

$$m_\tau = p_1T_1 + p_2T_2. \quad (1)$$

Дисперсия данного процесса будет равна

$$\sigma_\tau^2 = m_\tau(\tau^2) - m_\tau^2 = 2(p_1T_1^2 + p_2T_2^2) - m_\tau^2. \quad (2)$$

Коэффициент вариации интервалов между пакетами c_τ будет определяться из выражения

$$c_\tau^2 = \left(\frac{\sigma_\tau}{m_\tau}\right)^2 = \frac{2\left(p_1T_1^2 + p_2T_2^2\right)}{m_\tau^2} - 1, \quad (3)$$

откуда

$$2p_1T_1^2 + 2p_2T_2^2 = \left(c_\tau^2 + 1\right)m_\tau^2. \quad (5)$$

Из выражения (1) выразим T_2

$$T_2 = (m_\tau^2 - p_1T_1)/p_2 \quad (6)$$

и подставим его в выражение (6). Упрощая и приводя подобные получим:

$$\left(2p_1p_2 + 2p_1^2\right)T_1^2 + \left(-4m_\tau p_1\right)T_1 + m_\tau^2\left(2 - p_2\left(c_\tau^2 + 1\right)\right) = 0. \quad (7)$$

Решая квадратное уравнение (7) относительно T_1 получим

$$T_1 = m_\tau\left(1 \pm \frac{1}{2p_1}\sqrt{2p_1p_2\left(c_\tau^2 - 1\right)}\right).$$

Из корней T_1 выберем корень со знаком «+», чтобы гарантировать, что $T_1>0$

$$T_1 = m_\tau\left(1 + \frac{1}{2p_1}\sqrt{2p_1p_2\left(c_\tau^2 - 1\right)}\right). \quad (8)$$

Подставим его в (6), упрощая, получим T_2

$$T_2 = m_\tau\left(1 - \frac{1}{2p_2}\sqrt{2p_1p_2\left(c_\tau^2 - 1\right)}\right). \quad (9)$$

С учетом того, что аппроксимируемый гиперэкспоненциальный поток имеет $c_\tau \geq 1$ то на выражение под квадратным корнем в (8) и (9) дополнительных ограничений не накладывается.

Найдем ограничения на область определения p_1 и p_2 в соответствии с диапазоном изменений и физического смысла показателей c_τ, p_1 и p_2 в выражении (9):

$$\frac{1}{2p_2}\sqrt{2p_1p_2\left(c_\tau^2 - 1\right)} \leq 1,$$

заменяя $p_1=1-p_2$ и избавляясь от радикала

$$\frac{p_1}{2\left(1 - p_1\right)}\left(c_\tau^2 - 1\right) \leq 1,$$

откуда получим ограничения на p_1 и p_2 от c_τ

$$p_1 \leq \frac{2}{c_\tau^2 + 1}, \quad p_2 \geq \frac{c_\tau^2 - 1}{c_\tau^2 + 1}. \quad (10)$$

Для того, чтобы неравенства (10) привести к четкому виду был введен коэффициент $0 \leq k \leq 1$, значение которого влияет на качество формирования трафика:

$$\begin{cases} p_1 = 2k/\left(c_\tau^2+1\right), 0 \le k \le 1 \\ p_2 = 1 - p_1 \end{cases} . \quad (11)$$

Дополнительное исследование на основе имитационной модели [14] показало, что аппроксимация с параметрами (8), (9), (11) соответствует реальному потоку с заданным коэффициентом вариации c_τ.

Проведенный анализ значений математических ожиданий времени между поступлениями отдельных пакетов T_1, T_2 (рис. 3а), соответствующих им интенсивностей λ_1, λ_2 (рис. 3б), а также их вероятностей p_1, p_2 (рис. 3в) для различных целевых значений c_τ=1…3 показали, что ограничения на параметры (8), (9), (11) для формирования гиперэкспоненциального потока с $c_\tau \ge 1$ соответствует условиям

$$\begin{cases} T_1 > T_2 \\ \lambda_1 < \lambda_2 \\ p_1 < p_2, \text{при } c_\tau \ge \sqrt{4k-1} \end{cases} . \quad (12)$$

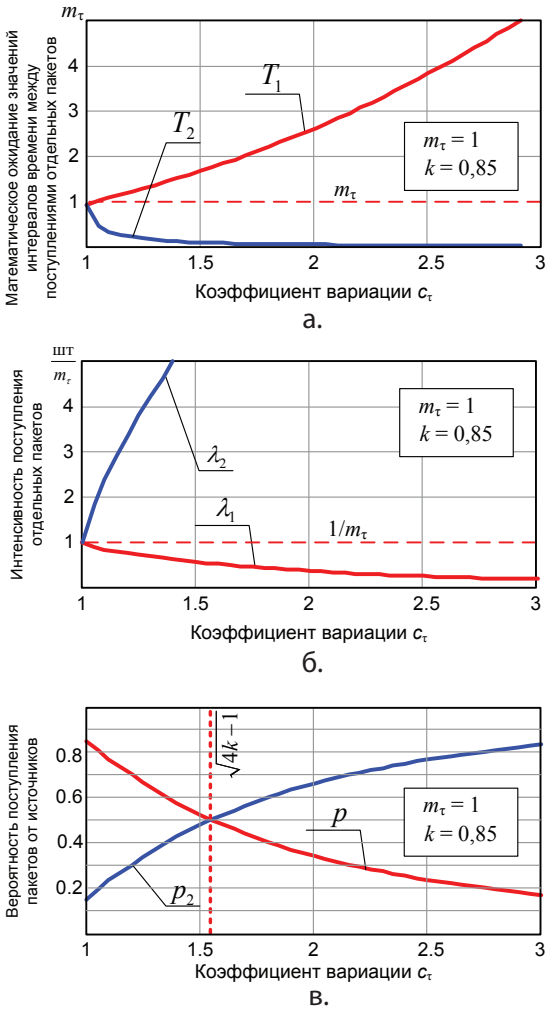


Рис. 3. *Значения T_1, T_2 (а), соответствующих им λ_1, λ_2 (б), а также их вероятностей p_1, p_2 (в) для формирования потока с заданным c_τ*

Таким образом, поток λ_2 (с математическим ожиданием T_2) моделирует основную нагрузку объединенного гиперэкспоненциального потока λ_Σ, а поток λ_1 (с математическим ожиданием T_1) – увеличенную дисперсионную характеристику гиперэкспоненциального потока λ_Σ.

Распределение значений T_1, T_2 и p_1, p_2 для аппроксимации потока с c_τ=1,5; 2; 2,5; 3 приведено на рис. 4. Распределение времени τ для потоков λ_1, λ_2 и λ_Σ без учета вероятностей p_1 и p_2 при c_τ=2 приведено на рис. 5.

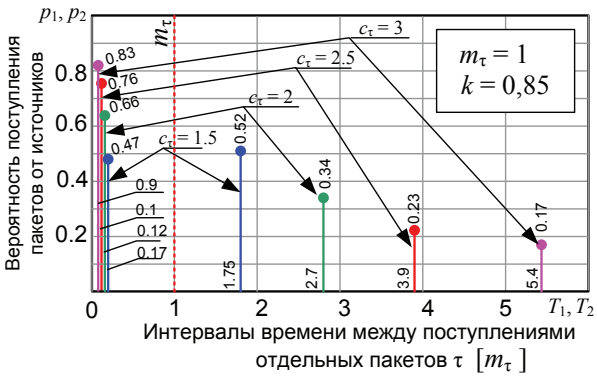


Рис. 4. *Распределение значений T_1, T_2 и p_1, p_2 для аппроксимации потока с различным c_τ*

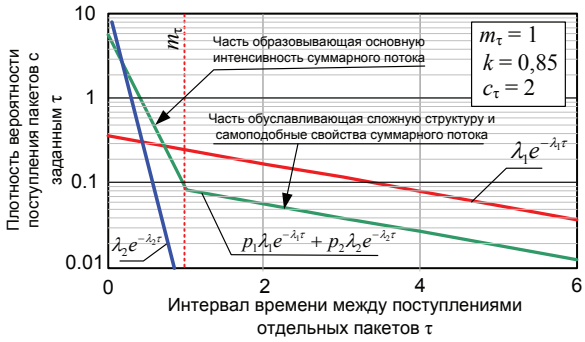


Рис. 5. *Распределение времени τ для потоков λ_1, λ_2 и λ_Σ при c_τ=2*

Методика формирования выходного потока сложной структуры с заданным коэффициентом вариации

Анализ условий (12) позволяет сделать следующий вывод.

В случае если по системе связи передается основной простейший поток $\lambda_{осн} = \lambda_2$ ($p_{осн} = p_2 = 1$) то существует возможность формирования из этого потока $\lambda_{осн}$ выходного потока сложной структуры с заданным коэффициентом вариации ($c_\tau > 1$), за счет внедрения дополнительного потока $\lambda_{доп}$ от СФТ с параметрами $\lambda_{доп} = \lambda_1(c_\tau)$ и $p_{доп} = p_1(c_\tau)$.

Причем формирующий поток $\lambda_{доп}$ маскируется под пакеты основного потока $\lambda_{осн}$ ошибочно размноженные в узлах маршрутизации, за счет следующих особенностей:

- поток $\lambda_{доп}$ состоит из перехваченных пакетов основного потока ,

- поток $\lambda_{доп}$ имеет значительно более низкую интенсивность, чем основной поток $\lambda_{осн}$ ($\lambda_{осн} > \lambda_{доп}$),

- поток $\lambda_{доп}$ внедряется в основной поток $\lambda_{осн}$ с относительно невысокой вероятностью p_2 ($p_{осн} > p_{доп}$ при $c_\tau > 1{,}5$).

Данные особенности внедрения дополнительного формирующего потока $\lambda_{доп}$ позволяют говорить о бескомпроматности воздействия по формированию основного потока.

Модель деструктивного воздействия, представляет собой систему из двух источников $И_{осн}$ и $И_{доп}$. Источник $И_{осн}$ генерирует основной поток пакетов в системе связи с параметрами $\lambda_{осн}$, $p_{осн}$, а источник $И_{доп}$ - дополнительный поток оказывающий дестабилизирующее воздействие с параметрами $\lambda_{доп}$, $p_{доп}$ (рис. 6).

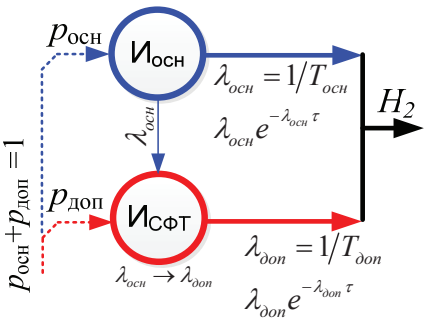


Рис. 6. *Модель деструктивного воздействия за счет формирования объединенного потока сложной структуры*

В модели деструктивного воздействия начальными параметрами являются наблюдаемая статистическое среднее интервалов между пакетами $T_{осн}$ ($T_{осн}=T_2$) и соответствующая ей интенсивность $\lambda_{осн}=1/T_{осн}$ ($\lambda_{осн}=\lambda_2$) от источника $И_{осн}$, а также требуемый коэффициент вариации $c_\tau > 1$ и соответствующий ему параметр k, как результат деструктивного воздействия источника $И_{доп}$.

Определим параметры источника $И_{доп}$.

Из системы (11) найдем вероятность с которой $И_{доп}$ должен внедрять трафик $\lambda_{доп}$ для достижения заданного c_τ

$$p_{доп} = 2k \Big/ \left(1 + c_\tau^2\right), \; 0 \le k \le 1 \quad . \tag{13}$$

Определим математическое ожидание значений интервалов времени между поступлениями отдельных пакетов в смешанном потоке m_τ из выражения (9) учитывая (13) и что $p_{доп}=p_1=1-p_{осн}=1-p_2$:

$$m_\tau = \frac{2T_{осн}\left(p_{доп}-1\right)}{2\left(p_{доп}-1\right)+\sqrt{-2p_{доп}\left(p_{доп}-1\right)\left(c_\tau^2-1\right)}} = \frac{T_{осн}\beta}{\beta-\sqrt{\beta k\left(c_\tau^2-1\right)}} \quad , \tag{14}$$

где $\beta = c_\tau^2 - 2k + 1$. (15)

Из выражения (8) подставляя m_τ получим значение $T_{доп}=T_1$

$$T_{доп} = \frac{T_{осн}\left(p_{доп}-1\right)}{p_{доп}} \times \times \frac{2p_{доп}+\sqrt{-2p_{доп}\left(p_{доп}-1\right)\left(c_\tau^2-1\right)}}{2\left(p_{доп}-1\right)+\sqrt{-2p_{доп}\left(p_{доп}-1\right)\left(c_\tau^2-1\right)}} \tag{16}$$

Выражая $T_{доп}$ через параметры k и c_τ с учетом выражения (13) и (15) получим:

$$T_{доп} = \frac{T_{осн}\beta\left(2k+\sqrt{\beta k\left(c_\tau^2-1\right)}\right)}{2k\left(\beta-\sqrt{\beta k\left(c_\tau^2-1\right)}\right)} \quad , \tag{17}$$

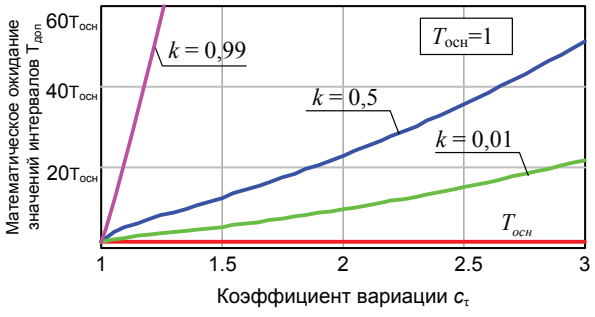
откуда интенсивность $\lambda_{доп}$

$$\lambda_{доп} = \frac{2k\left(\beta-\sqrt{\beta k\left(c_\tau^2-1\right)}\right)}{T_{осн}\beta\left(2k+\sqrt{\beta k\left(c_\tau^2-1\right)}\right)} \quad . \tag{18}$$

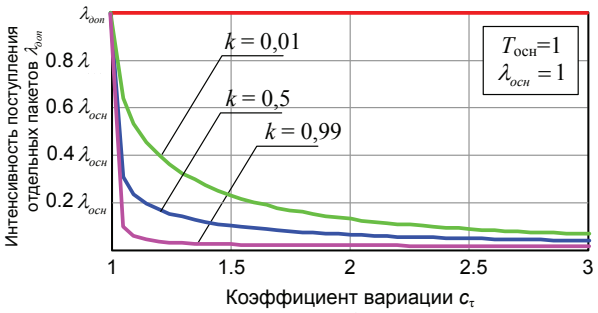
Значения $p_{доп}$ и $\lambda_{доп}=1/T_{доп}$ определяют параметры источника $И_{доп}$ формирующего деструктивные воздействия.

При внедрении в систему связи источника $И_{доп}$ с параметрами $p_{доп}$ и $\lambda_{доп}$ в канале связи будет передаваться результирующий гиперэкспоненциальный поток H_2 образованный двумя экспоненциальными фазами формирующими потоки с математическими ожиданиями времени между пакетами $T_{осн}$ и $T_{доп}$, а также плотностями распределения времен между заявками $\lambda_{осн} e^{-\lambda_{осн} t}$ и $\lambda_{доп} e^{-\lambda_{доп} t}$.

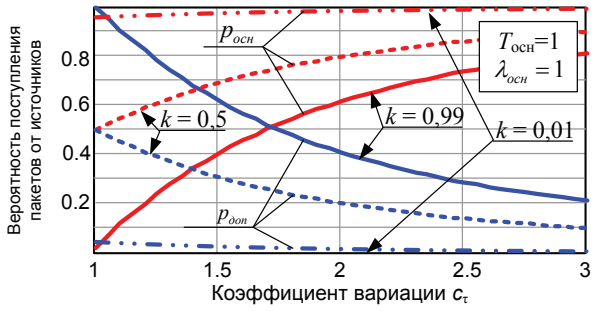
Проведенное исследование аналитических зависимостей определяющих поведение модели от входных параметров $T_{осн}$ и целевого c_τ при ограничениях: $T_{осн}=1$; $k=0{,}01$, 0,5 0,99; $c_\tau=1..3$ представлено на рис. 7, 8.



а.



б.



в.

Рис. 7. *Значения $T_{доп}$ (а), соответствующего им $\lambda_{доп}$, (б), а также вероятностей $p_{доп}$, $p_{осн}$ (в) для формирования потока с заданным c_τ при $T_{осн}=1/\lambda_{осн}=1$*

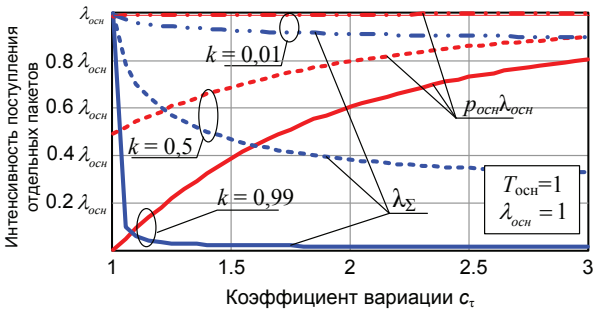


Рис. 8. *Значения интенсивности дополнительного трафика $p_{доп}\lambda_{доп}$ и суммарной интенсивности объединенного потока λ_Σ при формировании потока с заданным c_τ*

Выводы

Анализ графических зависимостей приведенных на рис. 7 показывает, что существует принципиальная возможность за счет внедрения в систему связи дополнительного потока с интенсивностью $\lambda_{доп}$ в восемь и более раз меньшей интенсивности чем основного потока $\lambda_{осн}$ повысить структурную сложность передаваемого информационного потока. Наилучшую бескомпроматность воздействия обеспечивает поток $\lambda_{доп}$ полученный при условии k=0,01, так как в этом случае заданный коэффициент вариации достигается при минимальной вероятности внедрения $p_{доп}$ (рис. 7в) и минимальном снижении интенсивности основного потока $\lambda_{осн}$, и суммарной интенсивности объединенного потока λ_Σ (рис. 8).

Таким образом, комплекс деструктивного воздействия, реализованный на основе предложенной в работе методики будет обладать свойством бескомпроматности воздействия. Это свойство достигается, во-первых за счет маскировки дополнительного потока $\lambda_{доп}$ под пакеты основного потока $\lambda_{осн}$ ошибочно размноженные в узлах маршрутизации, во-вторых за счет того, что целевой эффект функционального подавления системы связи достигается, не за счет прямого деструктивного воздействия на средства связи, а за счет использования особенности узлов маршрутизации и коммутации по снижению своей производительности (по показателю своевременности обработки пакетов) в условиях обработки информационных потоков сложной структуры.

Анализ наиболее распространенных протоколов защиты информации: шифрование в ATM; TSL или SSL поверх IP, выполненный на основе работ [15, 16], показал что предлагаемое воздействие может быть реализовано для всех вышеприведенных протоколов, так как шифрование сообщений и аутентификация сеансов связи в них производится до сегментации сообщений на пакеты сетевого (канального) уровня. Применение подобного воздействия в отношении системы связи на основе протокола IPSec будет затрудненно, ввиду наличия в нем туннельного режима и встроенных средств защиты от повторной передачи пакетов внутри сеансов связи.

Полученные в работе результаты по формализированному описанию предлагаемого деструктивного информационно-технического воздействия могут быть использованы в составе модели противника/нарушителя при решении задач обеспечения безопасности и устойчивости систем связи, а также для совершенствования научно-методического аппарата ведения информационного противоборства.

Работа выполнена при государственной поддержке РФФИ инициативного научного проекта №13-07-97518 и поддержке исследований Департаментом приоритетных направлений науки и технологий Минобрнауки РФ – грантом Президента РФ № МК-755.2012.10.

Литература

1. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1(2). 2014. С. 13-21.
2. Шабалин Е.А. Управление информационными потоками сетей радиосвязи в условиях радиоэлектронного противодействия. Автореф. дис. на соиск. уч. ст. канд. техн. наук по спец. 05.13.01. Н. Новгород: НГТУ им. Р.Е. Алексеева, 2008. 18 с.
3. Чакрян Е.А. Многомерные стохастические и имитационные модели телетрафика и каналов передачи данных в условиях помех. Автореф. дис. на соиск. уч. ст. канд. техн. наук по спец. 05.13.18. Ростов-на-Дону: РГУПС, 2009. 18 с.
4. Семенова О.В. Управляемые системы массового обслуживания с катастрофическими сбоями. Дис. на соиск. уч. ст. канд. ф.-мат. наук по спец. 01.01.05. Минск: БГУ, 2004. 116 с.
5. Вавилов В.А. Исследование математических моделей сетей множественного доступа функционирующих в случайной среде. Дис. на соиск. уч. ст. канд. ф.-мат. наук по спец. 05.13.18. Томск: ТГУ, 2006. 158 с.
6. Алиев Т. И. Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363 с.
7. Рыжиков Ю.И. Алгоритмический подход к задачам массового обслуживания. Монография. СПб.: ВКА им. А.Ф.Можайского, 2013. 496 с.
8. Бахарева Н.Ф. Аппроксимативные методы и модели массового обслуживания для исследования компьютерных сетей. Дис. на соиск. уч. ст. док. техн. наук по спец. 05.13.15. Самара: ПГУТИ, 2011. 360 с.
9. Ушаков Ю.А. Формирование оценок производительности корпоративных компьютерных сетей на основе аппроксимативного подхода. Дис. на соиск. уч. ст. канд. тех. наук по спец. 05.13.13. Оренбург: ОГУ, 2009. 144 с.
10. Колеров А.С. Методика формирования значений параметров сетевого трафика, характеризующих канал передачи, в задаче тестирования сетевых систем обнаружения атак // Вопросы защиты информации. 2004. № 4. С. 24-29.
11. Белоусов В.И., Линец Г.И., Михеев Ю.А., Фомин Л.А. Применение сингулярных последовательностей для моделирования трафика в сетях связи // Инфокоммуникационные технологии. 2009. Т. 7. № 1. С. 33-37.
12. Фомин Л.А., Жук А.П., Линец Г.И., Калашников С.В. Способ формирования самоподобных импульсных последовательностей и устройство для его осуществления. Патент RU 2322756 C1.
13. Макаренко С. И. Анализ математических моделей информационных потоков общего вида и степени их соответствия трафику сетей интегрального обслуживания // Вестник ВГТУ. 2012. Т. 8. № 8. С. 28-35.
14. Ушанев К.В. Имитационная модель формирования трафика сложной структуры // Информационные технологии моделирования и управления. 2014. № 3(87). С. 261-272.
15. Макаренко С. И., Бородинов Р.В. Анализ технологий обеспечения качества обслуживания в мультисервисных АТМ сетях // Информационные технологии моделирования и управления. 2012. №1 (73). С. 65-79.
16. RFC 5246. The Transport Layer Security (TSL) Protocol. 2008. URL: book.itep.ru/depository/rfcs/5200/rfc5246.txt (дата обращения 01.06.2014).

Reference

1. Makarenko S.I., Chucklyaev I.I. The terminological basis of the informational conflict` area // Voprosyi kiberbezopasnosti. N 1(2). 2014. S. 13-21.
2. Shabalin E.A. Upravlenie informatsionnyimi potokami setey radiosvyazi v usloviyah radioelektronnogo protivodeystviya. Abstract of PhD Thesis. N. Novgorod: NGTU im. R.E. Alekseeva, 2008. 18 s.
3. Chakryan E.A. Mnogomernyie stohasticheskie i imitatsionnyie modeli teletrafika i kanalov peredachi dannyih v usloviyah pomeh. Abstract of PhD Thesis. Rostov-na-Donu: RGUPS, 2009. 18 s.
4. Semenova O.V. Upravlyaemyie sistemyi massovogo obsluzhivaniya s katastroficheskimi sboyami. Diss. Ph.D. Minsk: BGU, 2004. 116 s.
5. Vavilov V.A. Issledovanie matematicheskih modeley setey mnozhestvennogo dostupa funktsioniruyuschih v sluchaynoy srede. Diss. Ph.D. Tomsk: TGU, 2006. 158 s.
6. Aliev T. I. Osnovyi modelirovaniya diskretnyih sistem. SPb: SPbGU ITMO, 2009. 363 s.
7. Ryzhikov Yu.I. Algoritmicheskiy podhod k zadacham massovogo obsluzhivaniya. Monografiya. SPb.: VKA im. A.F.Mozhayskogo, 2013. 496 s.
8. Bahareva N.F. Approksimativnyie metodyi i modeli massovogo obsluzhivaniya dlya issledovaniya kompyuternyih setey. Diss. Ph.D. Samara: PGUTI, 2011. 360 s.
9. Ushakov Yu.A. Formirovanie otsenok proizvoditelnosti korporativnyih kompyuternyih setey na osnove approksimativnogo podhoda. Diss. Ph.D. Orenburg: OGU, 2009. 144 s.
10. Kolerov A.S. Metodika formirovaniya znacheniy parametrov setevogo trafika, harakterizuyuschih kanal peredachi, v zadache testirovaniya setevyih sistem obnaruzheniya atak // Voprosyi zaschityi informatsii. 2004. N 4. S. 24-29.
11. Belousov V.I., Linets G.I., Miheev Yu.A., Fomin L.A. Primenenie singulyarnyih posledovatelnostey dlya modelirovaniya trafika v setyah svyazi // Infokommunikatsionnyie tehnologii. 2009. T. 7. N 1. S. 33-37.
12. Fomin L.A., Zhuk A.P., Linets G.I., Kalashnikov S.V. Sposob formirovaniya samopodobnyih impulsnyih posledovatelnostey i ustroystvo dlya ego osuschestvleniya. Patent RU 2322756 C1.
13. Makarenko S.I. Analyzing of mathematical models of general type data streams and degree of their conformity to integral service net traffic // Vestnik VGTU. 2012. T. 8. N 8. S. 28-35.
14. Ushanev K.V. Imitatsionnaya model formirovaniya trafika slozhnoy strukturyi // Informatsionnyie tehnologii modelirovaniya i upravleniya. 2014. N3(87). S. 261-272.
15. Makarenko S.I., Borodinov R.V. Analiz tehnologiy obespecheniya kachestva obsluzhivaniya v multiservisnyih ATM setyah // Informatsionnyie tehnologii modelirovaniya i upravleniya. 2012. N 1(73). S. 65-79.
16. RFC 5246. The Transport Layer Security (TSL) Protocol. 2008. URL: book.itep.ru/depository/rfcs/5200/rfc5246.txt