components of an information security management system (ISMS) is improved. The set of components named "Directions" is given a variable length. This provides the flexibility to the processes of analysis, prognostication and informative-analytical support for the decisions concerning information security. For the first time the information security management system data model is developed, that provides concerted processing and storage of operational tasks, knowledge and information security risks under the incompleteness of information. The data is structured according to the improved model of logical and functional relations between the components of an ISMS. For the first time the method of informative-analytical support for information security management is developed, which provides the system approach principles application in information security management. The method is based on the improved model of relations between the components of an ISMS, the developed information security management data model and the developed technique of current information security state estimation. An example of the developed method application in Ukraine's banking system is presented. Recommendations for the scientific and practical use of the developed models and method are provided.
**Keywords:** system approach to information security, model of relations between the components of an ISMS, data model for information security management, information security management method, information security management system, ISMS.

**Домарєв Дмитро Валерійович**, аспірант, Національний авіаційний університет.
E-mail: dimavsesvit@yahoo.com.
**Домарев Дмитрий Валериевич**, аспирант, Национальный авиационный університет.
**Domarev Dmitry**, postgraduate student of the National aviation university.

**УДК 004.056.57**

# СТАТИСТИЧЕСКИЕ СВОЙСТВА ТРАФИКА НА ОСНОВЕ BDS-ТЕСТОВ ДЛЯ РЕАЛИЗАЦИИ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

***Алексей Смирнов, Юрий Дрейс, Дмитрий Даниленко***

*В работе предлагается использовать математический аппарат статистического анализа на основе BDS-тестов для исследования свойств сетевого трафика различных служб и информационных сервисов при определении значимости расхождения или совпадения их характеристик. Полученные результаты экспериментальных исследований статистических свойств сетевого трафика с использованием корреляционного анализа временных рядов подтверждают теоретические предположения о том, что для различных видов трафика (HTTP, FTP, Skype трафик и потоковое вещание) результат BDS-теста дает различные значения, которые могут быть приняты в качестве эталонных при использовании и усовершенствовании механизмов мониторинга сетевой активности, в том числе и для реализации системы обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях.*
***Ключевые слова:*** *телекоммуникационные системы и сети, система обнаружения и предотвращения вторжений, BDS-статистика, статистические свойства трафика.*

**Введение.** Современное развитие телекоммуникационных систем и сетей и применяемых компьютерных технологий привело к появлению качественно новых услуг и сервисов в информационной сфере, внедрению передовых технологий обработки и передачи данных и их доступности широкой пользовательской аудитории [1]. В тоже время интенсивное развитие современных компьютерных технологий привело к появлению новых угроз безопасности информации, возникновению новых форм и способов несанкционированного доступа к вычислительным ресурсам телекоммуникационных систем и сетей [1-4]. В частности, наибольшую уязвимость представляют применяемые методы сетевого управления, технологии доступа к предоставляемым сервисам и услугам, процессы мониторинга состояния телекоммуникационных систем и сетей. Под воздействием вредоносного программного обеспечения отдельные коммуникационные и вычислительные компоненты могут быть переведены в несанкционированные режимы функционирования, приводящие к сбоям, различным нарушениям установленного порядка их использования, уничтожению, искажению, блокированию, несанкционированной утечки обрабатываемой и передаваемой информации, а также к нарушению работы методов и алгоритмов маршрутизации между узлами телекоммуникационной системы [2-4]. Следовательно, разработка и иссле-

дование методов мониторинга сетевой активности, технологий обнаружения вредоносного программного обеспечения и предотвращения его воздействия на защищаемые инфокоммуникационные ресурсы является актуальной научно-прикладной проблемой, ее решение непосредственно связано с обеспечением безопасности современных телекоммуникационных систем и сетей и применяемых компьютерных технологий.

**Целью работы** является реализация системы обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях с использованием математического аппарата статистического анализа на основе BDS-тестов при исследовании свойств сетевого трафика различных служб и информационных сервисов при определении значимости расхождения или совпадения их характеристик, а также совершенствования механизмов мониторинга сетевой активности.

**Анализ последних публикаций.** Для обеспечения безопасности в современных телекоммуникационных системах и сетях применяются различные организационно-технические мероприятия, наиболее эффективные из которых состоят в построении т.н. систем обнаружения (Intrusion Detection System – IDS) и предотвращения (Intrusion Prevention System – IPS) вторжений [2-11]. В основе функционирования IDS и IPS лежит сбор, анализ и обработка информации о событиях, связанных с безопасностью защищаемой телекоммуникационной системы, накопление полученных данных и, на основе результатов проведенного анализа (мониторинга) сетевой активности отдельных служб и сервисов, принятие решения ее состоянии защищаемой системы с выявлением и возможным противодействием несанкционированному использованию инфокоммуникационных ресурсов [2-6].

*Под системой обнаружения вторжений* (СОВ) понимают программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления [2-4]. СОВ обеспечивают дополнительный уровень защиты компьютерных систем за счет обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки на наиболее уязвимые сервисы, атаки, направленные на повышение привилегий, неавторизованный доступ к важным ресурсам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей) [2].

*Под системой предотвращения вторжений* (СПВ) понимают программную или аппаратную систему сетевой и компьютерной безопасности, обнаруживающую вторжения или нарушения безопасности, а также реализующую автоматическую защиту от выявленных нарушений [2-4].

Системы IPS следует рассматривать как расширение систем IDS. В тоже время СПВ отличаются необходимостью отслеживания сетевой активности в реальном времени с быстрым реагированием посредством реализации соответствующих действия по предотвращению выявленных атак. Возможные меры предотвращения атак состоят в блокировке потоков трафика в телекоммуникационной сети, сбросе соединений, выдачи сигналов оператору и т.д. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ (номерами очереди) и ACK (номерами подтверждения) [2].

**Основная часть.** Одним из эффективных подходов при выявлении зависимостей в информационном трафике является BDS-статистика, построенная на основе BDS-тестов (BDS-методов). BDS-тесты представляют собой эффективные методы выявления зависимостей во временных рядах. Их цель состоит в проверке нулевой гипотезы $H_0$ о независимости и тождественном распределении значений временного ряда $\vec{\xi} = (\xi_1, \xi_2, ..., \xi_N)$, используя для этого критерий значимости. Согласно этому критерию для принятия гипотезы $H_0$ необходимо выбрать критическую область $G_\alpha$, удовлетворяющую условию $P(g \in G) = \alpha,$ где $g(\xi_1, \xi_2, ..., \xi_N)$ – статистика наблюдения, а $\alpha$ – устанавливаемый уровень значимости [7-11].

BDS-тест основан на статистической величине $w(\vec{\xi})$ (BDS-статистике) [7-11]:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)},$$

где $C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m$ – (числитель BDS-статистики) определяется корреляционными интегралами $C_{m,N}(\varepsilon)$, $C_{1,N}(\varepsilon)$ для размерности $m$; $\varepsilon$ – радиус гиперсферы; $\sigma_{m,N}(\varepsilon)$ – среднеквадратическое отклонение разницы $N$ – число элементов временного ряда.

В ряде работ [7-11] были предложены «упрощенные» алгоритмы оценки BDS-статистики. В них для вычисления $C_{m,N}(\varepsilon)$ $(m>1)$ необходимо выполнить «вложение» временного ряда в $m$-мерное псевдофазовое пространство, элементами которого, на основании теоремы Такенса [7-11], являются точки $\xi_i^m=(\xi_i,\xi_{i+1},...,\xi_{i+m})$ с координатами $\{\xi_{i+k}\}_{k=1}^m$ заданными $m$ последовательными значениями исходного временного ряда. Корреляционный интеграл определяет частоту попадания произвольной пары точек фазового пространства в гиперсферы радиуса $\varepsilon$:

$$C_{m,N}(\varepsilon)=\frac{2}{(N-m+1)(N-m)}\sum_{s=m}^{N}\sum_{t=s+1}^{N}\prod_{j=0}^{m-1}I_\varepsilon(\xi_{s-j}^m,\xi_{t-j}^m),$$

$$I_\varepsilon(\xi_i^m,\xi_j^m)=\begin{cases}1, & \left\|\xi_i^m-\xi_j^m\right\|\le\varepsilon\\ 0, & \left\|\xi_i^m-\xi_j^m\right\|>\varepsilon\end{cases},\qquad \{\xi_i\}_{i=1}^N,$$

$$0\le i\le N \text{ и } 0\le j\le N,$$

где $I_\varepsilon(\xi_i^m,\xi_j^m)$ – функция Хевисайда для всех пар значений $i$ и $j$.

Значение корреляционного интеграла стремится к определенному пределу по мере уменьшения $\varepsilon$. Анализ работ [7-11] показал, что существует диапазон значений $\varepsilon$, который позволяет провести вычисления с заданным коэффициентом точности. Этот диапазон зависит от числа элементов временного ряда $N$. Если $\varepsilon$ является слишком маленьким, не будет достаточного количества точек для захвата статистической структуры; если $\varepsilon$ является слишком большим, точек будет слишком много.

В работах [7-11] $\varepsilon$ рекомендовано выбирать таким, что $\varepsilon=0.5\sigma\div2\sigma$, где $\sigma$ – среднеквадратическое отклонение процесса $\{\xi_i\}_{i=1}^N$. В соответствии с теорией статистики, зависимость корреляционного интеграла от $\varepsilon$ имеет вид:

$$C_{m,N}(\varepsilon)\sim\varepsilon^{D_c},$$

где $D_c$ – корреляционная размерность временного ряда.

Для $m=1$ имеем:

$$C_{1,N}(\varepsilon)=\frac{2}{N(N-1)}\sum_{s=1}^{N}\sum_{t=s+1}^{N}I_\varepsilon(\xi_s,\xi_t).$$

Поведенные исследования показали, что при $N\to\infty$, корреляционный интеграл $C_{m,N}(\varepsilon)\Rightarrow C_{1,N}(\varepsilon)^m$, а величина

$$\left(C_{m,N}(\varepsilon)-\left(C_{1,N}(\varepsilon)\right)^m\right)\cdot\sqrt{N-m+1}$$

является случайной асимптотически нормально распределенной величиной с нулевым средним и среднеквадратическим отклонением $\sigma_{m,N}(\varepsilon)$, которое определяется как:

$$\sigma_{m,N}(\varepsilon)=2\sqrt{k^m+2\sum_{j=1}^{m-1}k^{m-j}\cdot(C_{1,N}(\varepsilon))^{2j}+(m-1)^2\cdot(C_{1,N}(\varepsilon))^{2m}-m^2k(C_{1,N}(\varepsilon))^{2m-2}},$$

где

$$k=\frac{1}{(N-1)(N-2)N}\left\{\sum_{t=1}^{N}\left[\sum_{s=1}^{N}I_\varepsilon(\xi_t,\xi_s)\right]^2-3\sum_{s=1}^{N}\sum_{t=s+1}^{N}I_\varepsilon(\xi_t,\xi_s)+2N\right\}.$$

BDS-статистика $w(\vec{\xi})$ является нормально распределенной случайной величиной при условии, что оценка $\hat{\sigma}_{m,N}(\varepsilon)$ близка к ее теоретическому значению $\sigma_{m,N}(\varepsilon)$.

Задача обнаружения хаотического сигнала рассматривается как непараметрическая проверка одной из двух гипотез: $H_0$ – наблюдаемые данные (информационный трафик) $\vec{\xi}=(\xi_1,\xi_2,...,\xi_N)$ независимы и одинаково распределены, т.е. плотность (функция) распределения факторизуется $F_N(\xi_1,\xi_2,...,\xi_N)=\prod_{i=1}^N F(\xi_i)$; $H_1$ – полученные в результате эксперимента данные (информационный трафик) имеют определенную зависимость (процесс структурирован).

Согласно гипотезе $H_0$ статистика $w(\vec{\xi})$ асимптотически распределена как $N(0,1)$, если число наблюдений асимптотически стремится к бесконечности. В ряде работ [7-11] обосновывается гипотеза о необходимости проведения экспериментального исследования объемом более 500 наблюдений. Такое количество экспериментов позволит утверждать о достоверности полученных результатов. Исследования показали, что критерием достоверности гипотезы $H_0$ (об отсутствии в информационном трафике каких либо зависимостей) является неравенство:

$|w_{m,N}(\varepsilon)| \le 1{,}96$. Для значения статистики $w_{m,N}(\varepsilon)$ приведенное значение соответствует уровню значимости $\alpha = 0{,}05$ (вероятности ошибки первого рода), и когда приведенное неравенство истинно гипотеза $H_0$ (I.I.D.) принимается с вероятностью $P_{H_0} \approx 0{,}95$.

В случае, когда верна альтернативная гипотеза $H_1$, распределение статистики критерия $w(\vec{\xi})$ изменится. Поэтому при проверке статистических гипотез недостаточно ориентироваться на значение уровня значимости $\alpha$. Следует определить мощность критерия $1-\beta$ или вероятность ошибки второго рода $\beta$ при принятии альтернативной гипотезы $H_1$, что подразумевает, зависимость (возможно нелинейную) временного ряда, если были взяты первые разности натуральных логарифмов. *Мощность критерия* – то вероятность принятия альтернативной гипотезы $H_1$ при применении критерия $w(\vec{\xi})$ при условии, что она верна, т.е. его способность обнаружить имеющееся отклонение от нулевой гипотезы. Очевидно, что при фиксированной ошибке 1-го рода (ее мы задаем сами, и она не зависит от свойств критерия) критерий будет тем лучше, чем больше его мощность (т.е. чем меньше ошибка 2-го рода). Для расчета мощности критерия $1-\beta$ ($\beta = p\left(w(\vec{\xi}) \in G_\alpha \mid H_1\right)$), $G_\alpha$ – критическая область при заданном уровне значимости $\alpha$) необходимо знать условную плотность распределения $p\left(w(\vec{\xi}) \mid H_1\right)$. Мощность критерия (теста) определяется эмпирическим путем.

Для проведения эксперимента и повышения достоверности результатов необходимо выбрать такую размерность вложения *m*, благодаря которой воссоздание фазового пространства не будет ни «слишком редким», ни «слишком переполненным». В ряде работ [7-11] при проведении экспериментов рекомендуется использовать $m = 6$.

Таким образом, проведенный анализ различных подходов в статистическом тестировании показал, что BDS-тест позволяет обнаружить различные типы отклонений от независимости и идентичного распределения, и может служить общим образцовым тестом классификации процессов (временных рядов) $\vec{\xi}$, особенно в присутствии нелинейной динамики.

Основной отличительной особенностью BDS тестирования можно считать его непараметрический характер. Это выражается в том, что в качестве статистик BDS-тест использует нелинейные функции $w(\vec{\xi})$ от наблюдений, распределение которых не зависит от вида распределения наблюдаемых величин $\vec{\xi}$. В этом случае мы получаем возможность получить некоторую информацию о многомерной функции (плотности) распределения $F_N(\xi_1,\xi_2,...,\xi_N)$ анализируя одномерную эмпирическую функцию распределения $p(w)$ статистики $w$.

Расчет BDS-теста можно проводить различными, способами, известно множество реализаций, в данной методике предлагается использовать реализацию от авторов BDS-теста (by W.A. Brock, W.D. Dechert and J.A. Sheinkman). Также были предложены быстрые алгоритмы расчета BDS статистики [7-11]. Пример расчета приведен на рис. 1.

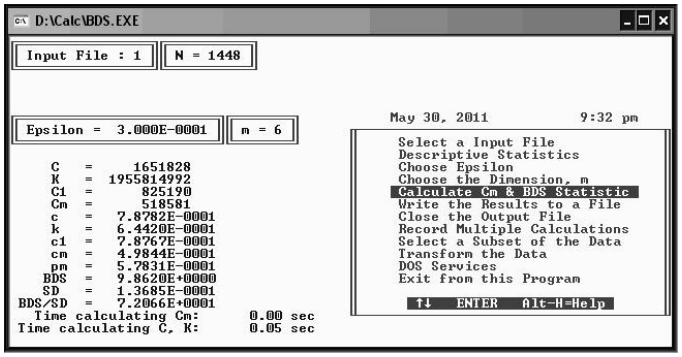


Рис. 1. Пример работы программы расчета BDS-теста

Ниже приведены результаты экспериментальных исследований статистических свойств сетевого трафика на основе корреляционного анализа временных рядов (посредством BDS тестирования). Результаты содержат данные, которые соответствуют наиболее популярным сетевым протоколам и службам.

Размер выборки при проведении исследований статистических свойств на основе корреляционного анализа временных рядов составляет $N = 1000$, расчеты проводились с различными параметрами (результаты приведены в соответствующей таблице).

На рис. 2 представлен фазовый потрет для полученных экспериментальных данных HTTP трафика. HTTP – это протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и

посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

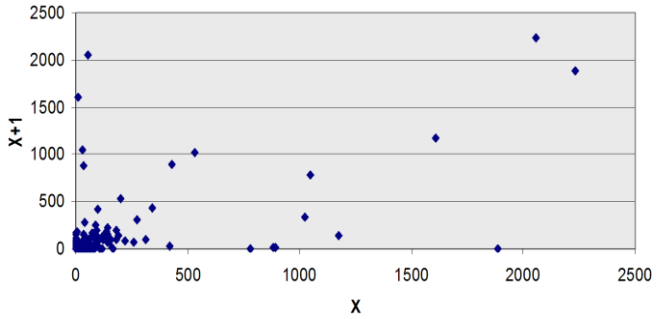


Рис. 2 . Фазовый портрет сетевого трафика при передаче данных с использованием протоколов HTTP

Анализ приведенных данных показывает, что на фазовом портрете сетевого трафика при передаче данных с использованием протоколов HTTP наблюдается наличие некоторой зависимости, состоящей в группировании большинства точек в определенной области (см. рис. 2). В табл. 1 представлены значения BDS-теста с различными наборами параметров.

Таблица 1

Значения BDS-теста для экспериментальных данных HTTP, FTP, Skype трафика и потокового вещания с различными параметрами $m$ и $\varepsilon$

| *Вид сервиса* | $m$ | $\varepsilon = 0.5\sigma$ | $\varepsilon = \sigma$ |
|---|---|---|---|
| HTTP | 4 | 13,52 | 12,69 |
| | 5 | 13,97 | 11,554 |
| | 6 | 13,87 | 10,65 |
| | 7 | 13,58 | 9,92 |
| FTP | 4 | 19,5 | 17,69 |
| | 5 | 17,81 | 16,13 |
| | 6 | 16,49 | 14,91 |
| | 7 | 15,437 | 13,95 |
| Skype | 4 | 16,49 | 180,11 |
| | 5 | 15,05 | 163,77 |
| | 6 | 13,95 | 150,94 |
| | 7 | 13 | 140,58 |
| Потоковое видео | 4 | 32,5 | 18,2 |
| | 5 | 32,254 | 19,28 |
| | 6 | 38,45 | 20,39 |
| | 7 | 41,42 | 28,49 |

Таким образом, как следует из полученных экспериментальных данных, для рассматриваемого вида HTTP трафика характерным значением BDS-теста является:

– для радиуса $\varepsilon = 0.5\sigma$ при $m = 4..7$ значения лежат в диапазоне от $\approx 15$ до $\approx 14$;

– для радиуса $\varepsilon = \sigma$ наблюдается больший разброс значений от 9.92 до 12.69.

Эти значения могут быть использованы в качестве тестовых (эталонных) величин, при детектировании вида трафика и соответствующей сетевой службы.

На рис. 3 представлен фазовый потрет для полученных экспериментальных данных FTP трафика. FTP – протокол, предназначенный для передачи файлов в компьютерных сетях. Он позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами. Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Исходящий порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для скачивания оставшейся части файла, что бывает очень удобно при передаче больших файлов.

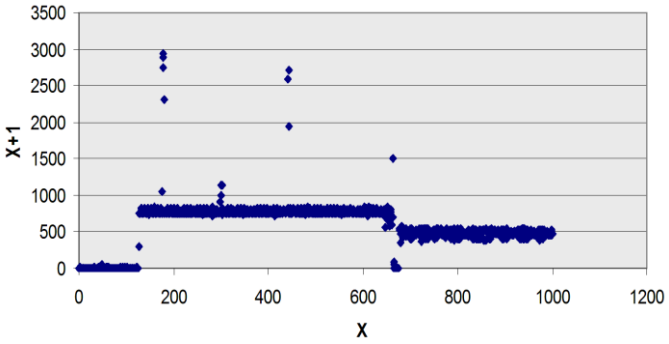


Рис. 3. Фазовый портрет сетевого трафика при передаче данных с использованием протоколов FTP

На приведенном фрагменте экспериментальных данных сетевого трафика с использованием протоколов FTP хорошо видно переход от малого количества пакетов (передача команд протокола, получение списка директорий и др.) и начало активного скачивания файлов на определенном уровне скорости. Т.к. использовался сервер с ограничением скорости загрузки, которая составляла значительно меньше пропускной возможности сети, иногда наблюдаются «всплески», которые быстро убывают до порогового значения ограничения скорости.

На фазовом портрете (см. рис. 3) наблюдается группировка точек, что свидетельствуют о наличии зависимостей в исходных данных. В табл. 1 представлены значения BDS-теста с различными наборами параметров.

Данные из табл. 1 могут быть использованы в качестве эталонных значений для FTP трафика в системе обнаружения вторжений телекоммуникационных систем и сетей.

На рис. 4 представлен фазовый потрет для полученных экспериментальных данных Skype трафика. Skype – бесплатное программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь через Интернет между компьютерами (VoIP), а также платные услуги для звонков на мобильные и стационарные телефоны. Приложение Skype позволяет также совершать конференц-звонки, видеозвонки, а также обеспечивает передачу текстовых сообщений (чат) и передачу файлов. Есть возможность вместо изображения с веб-камеры передавать изображение с экрана монитора.

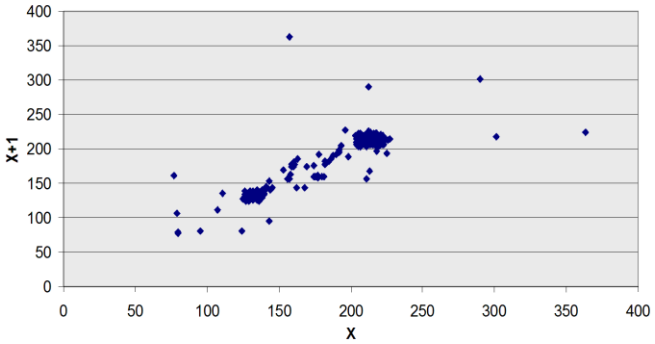


Рис. 4. Фазовый портрет сетевого трафика при передаче данных с использованием приложения Skype

На фазовом портрете для Skype трафика наблюдается 2 области вокруг которых формируется большинство точек, что свидетельствует о наличии зависимостей в исходной последовательности. В табл. 1 представлены значения BDS-теста для Skype трафика с различными наборами параметров.

Полученные результаты исследований Skype трафика, приведенные в табл. 1, могут быть использованы в качестве эталонных значений в системах обнаружения вторжений телекоммуникационных систем и сетей.

На рис. 5 представлен фазовый потрет для полученных экспериментальных данных трафика потокового видео. Потоковое видео – это мультимедиа данные, которое непрерывно получаются пользователем от провайдера потокового вещания. В настоящее время данный сервис очень распространен и по объему трафика составляет около половины передаваемого в сети Интернет трафика.

На соответствующем фрагменте сетевого трафика наблюдается множество всплесков и спадов, характерных для потокового видео. На фазовом портрете (рис. 5) можно выделить 2 области. Первая с распределением близким к случайному. Однако в другой явно выраженной области точки группируются с достаточно большой кучностью, что свидетельствует о наличии зависимостей в исходной последовательностей. В табл. 1 представлены значения BDS-теста с различными наборами параметров для экспериментальных данных потокового видео.

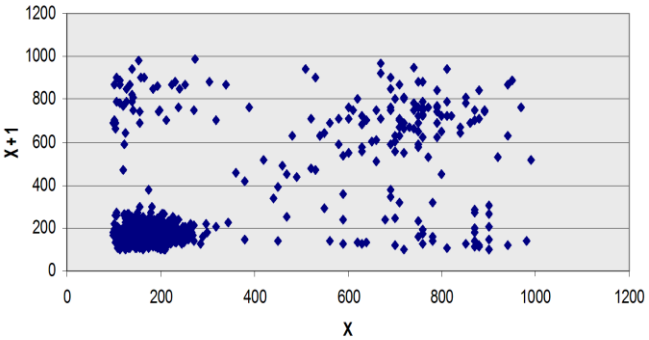


Рис. 5. Фазовый портрет сетевого трафика при передаче данных потокового вещания

Анализ данных табл. 1 показывает, что значения BDS-теста для потокового видео лежат в достаточно большом диапазоне, однако могут быть использованы в качестве эталонных.

Таким образом, полученные результаты экспериментальных исследований статистических свойств сетевого трафика с использованием корреляционного анализа временных рядов показывают, что конкретные значения BDS-теста могут быть «метризированы», для различных служб и сервисов телекоммуникационных систем и сетей.

Проведенные расчеты подтверждают теоретические предположения о том, что для различных видов трафика результат BDS-теста дает различные значения, которые могут быть приняты в качестве эталонных. Так, в табл. 2 приведены усредненные значения, соответствующие различным видам трафика для различных значений $\varepsilon$, что позволяет идентифицировать сетевые сервисы и службы. Например, для значений $\varepsilon = 0.5\sigma$ и $\varepsilon = \sigma$ можно выделить усредненные значения BDS-тестов для каждого вида трафика и по этому признаку возможна организация процесса детектирования сетевой активности отдельной службы или сервиса телекоммуникационной сети.

Следует отметить, что в реальной телекоммуникационной сети популярные сервисы и службы могут использоваться одновременно, что приведет к изменению значений BDS-теста. Однако реализация несанкционированного сетевого вторжения приведет к изменению статистических свойств сетевого трафика и соответствующих значений BDS-статистики.

Таблица 2

Усредненные значения BDS-тестов для различных сервисов и служб телекоммуникационной сети

| Усредненные значения BDS-тестов | | |
|---|---|---|
| Вид сервиса | ε=0.5σ | ε=σ |
| HTTP | 13,7 | 11,2 |
| Skype | 14,6 | 171,9 |
| Мультисервисный трафик | 11,5 | 13,5 |
| FTP | 17,3 | 15,7 |
| Потоковое видео | 36,2 | 21,6 |
| Вредоносное программное обеспечение | 40,7 | 28,5 |

Кроме того, даже в смешанном режиме, как правило, какая-то определенная служба преобладает, что позволяет ее выделить. А следы трафика, генерируемые вредоносным программным обеспечением, вирусами и пр., модифицируют значение теста до уровня, достаточного для формирования решения о подозрительном трафике, т.е. детектированию возможных следов вирусного трафика в общем потоке.

Для оценки статистических свойств информационного трафика в условиях внешних воздействий и структурной идентификации состояния с помощью BDS-тестирования произведено имитационное моделирование фрагмента ТКС в условиях воздействия на систему DoS-атаки. Сбор статистических данных осуществлялось эмпирическим путем с помощью программы «Wireshark».

Результаты идентификации состояния трафика, поступающего в КИУС критического применения, приведены на рис. 6.

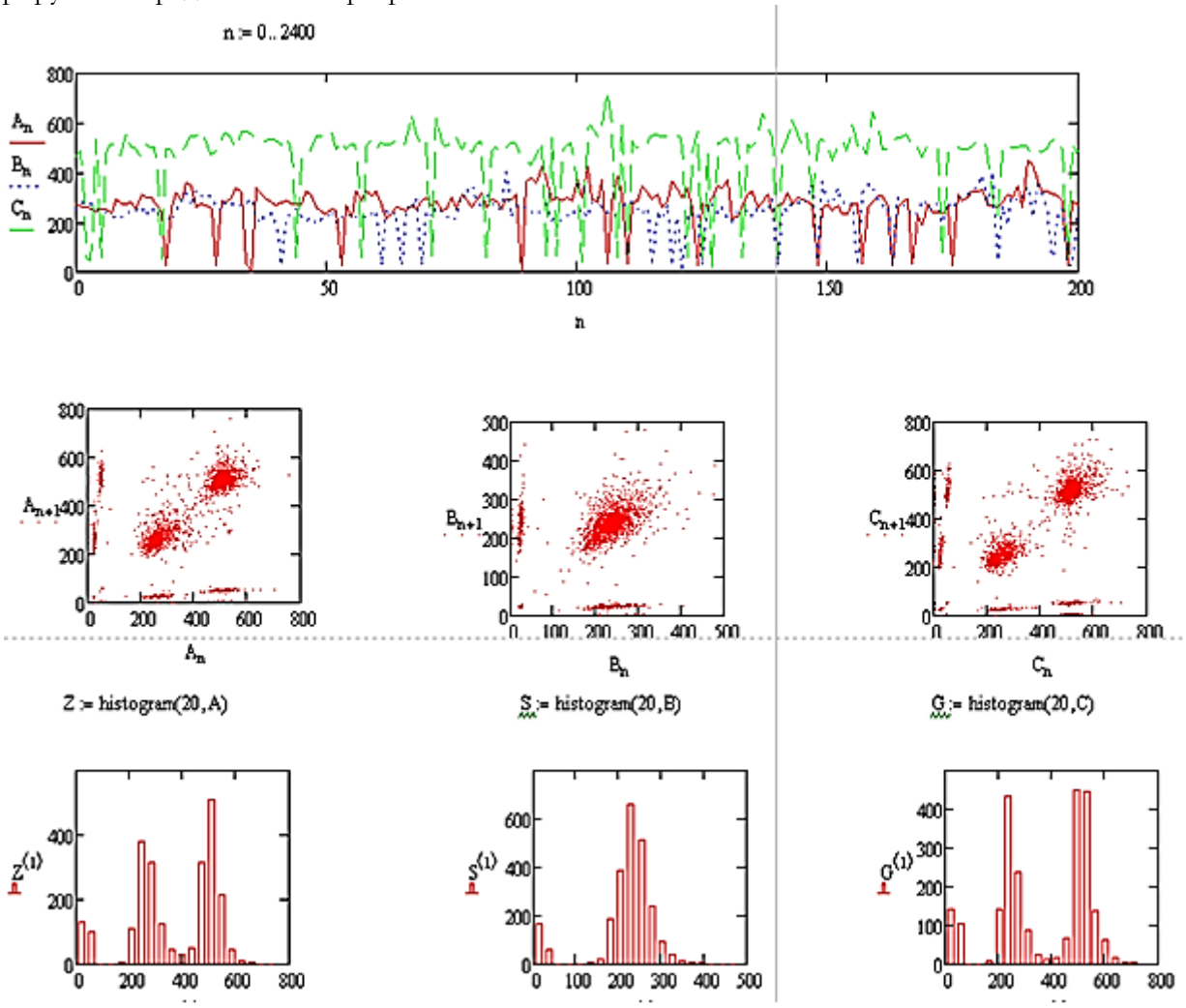


Рис.6. Скриншот результатов BDS-теста КИУС критического применения в условиях DoS-атаки

На данном рисунке представлены графики интенсивности входного потока информации во временной области и их фазовые портреты. Фазовые портреты, иллюстрирующие статистические данные КИУС критического применения подверженной DoS-атаке и отразившей попытку данного вида атаки, представлены на рис. 6. Как видно из графиков даже визуально статистические данные интенсивности входного потока информации аномального и нормального трафиков существенно отличаются (появление второго уровня показателей интенсивности информационного трафика, связанного с увеличением интенсивности входного потока).

На практике именно это увеличение чаще всего приводит к деструктивным изменениям исследуемых систем.

В табл. 3 приведенные значения BDS-статистики для разного информационного трафика в условиях нормального функционирования и во время действия DoS-атаки.

Как видно из табл. 3. в условиях, когда злоумышленные внешние воздействия достигли своей цели результаты BDS-тестирования снижаются практически в 37 раз и достигают уровня, когда система принимают решение о полном отсутствии статистических зависимостей во входной последовательности информационного трафика.

Проведенные исследования показали, что данный факт целесообразно использовать в системах обнаружения злоумышленных вторжений для защиты информации и обеспечения гарантированного уровня безопасности.

Таблица 3

Значение BDS-статистики для различного вида трафиков при N=500

| | m=6 | | m=5 | | m=4 | |
|---|---|---|---|---|---|---|
| | ε=0.5 | ε=0.25 | ε=0.5 | ε=0.25 | ε=0.5 | ε=0.25 |
| IP-телефония | 17.512 | 26.893 | 16.431 | 22.455 | 15.709 | 18.691 |
| Торрент услуги | 45.876 | 67.028 | 40.727 | 49.076 | 35.145 | 41.392 |
| Потоковое видео | 52.329 | 117.954 | 38.824 | 83.730 | 30.032 | 54.371 |
| DoS-атака | 1.391 | 4.298 | 1.692 | 4.939 | 1.847 | 5.231 |

Таким образом, полученные экспериментальные данные подтверждают теоретическое предположение о возможности использования значений BDS-теста для детектирования следов вредоносного программного обеспечения в сетевом трафике.

**Выводы.** Полученные результаты экспериментальных исследований статистических свойств сетевого трафика с использованием корреляционного анализа временных рядов подтверждают теоретические предположения о том, что для различных видов трафика результат BDS-теста дает различные значения, которые могут быть приняты в качестве эталонных, т.е. и по этому признаку возможна организация процесса детектирования сетевой активности отдельной службы или сервиса телекоммуникационной сети.

Полученные результаты корреляционного анализа сетевого трафика на основе BDS-тестирования рекомендуется использовать: во-первых, в качестве составной части аналитической компоненты современных антивирусных систем; во-вторых, возможно использование корреляционного анализа сетевого трафика для организации работы одного из основных элементов системы мониторинга сетевой активности в качестве сенсорной подсистемы (датчики по сбору информации о трафике) и аналитической части (компонент модуля принятия решений).

## ЛИТЕРАТУРА


[1]. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2010. – 944 с.

[2]. NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). – Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg. – 127 pages (February 2007).

[3]. Brian Caswell, Jay Beale, Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. – Syngress Media, U.S. 2006. http://www.lehmanns.de/ shop/sachbuch-ratgeber/21797174-9780080549279 - snort-intrusion-detection-and-prevention-toolkit#drm1

[4]. Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Т.II. Средства защиты в сетях, 2008. – 558 с.

[5]. Ушаков Д.В. Развитие принципов функционирования систем обнаружения сетевых вторжений на основе модели защищенной распределенной системы: Дис. канд. техн. наук: 05.13.19 Москва, 2005. – 175 с.

[6]. Смирнов Н.В. Курс теории вероятностей и математической статистики для технических приложений. Изд. 2. / Н.В. Смирнов, И. В. Дунин-Барковский. – М.: Наука, 1969.-512 с.

[7]. Шеффе Г. Дисперсионный анализ: Пер. с англ. Изд. 2. – М.: Наука, 1980. – 512 с.

[8]. Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе BDS-тестирования / А.А.Кузнецов, С.Г.Семенов, С.Н.Симоненко, Е.В.Мелешко // Науково-технічний журнал "Наука і техніка Повітряних Сил Збройних Сил України". Випуск 2 (4). – Харків: ХУПС. – 2010. – С. 131 - 137.

[9]. The method of processing and identification of telecommunication traffic based on BDS-tests / S. Semenov, A.Smirnov., E.Meleshko // The book of materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)» –Kiev, Ukraine, National Aviation University “NAU-Druk” Publishing House, October 13-14, 2010. – С.166-168.

[10]. B. LeBaron "A Fast Algorithm for the BDS Statistic", Studies in Nonlinear Dynamics and Econometrics. 1997. Vol. 2. No. 2. P. 53-59.

[11]. D. Chappell J. Padmore and C. Ellis. "A note on the distribution of BDS statistics for a real exchange rate series", Oxford Bulletin of Economics and Statistics, 58, 3, 561- 566, 1996.

## REFERENCES


[1]. Olifer V.G., Olifer N.A. (2010) «Computer networks. Principles, technologies, and protocols», *St. Petersburg.: Peter*, 944 p.

[2]. NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 127 pages

[3]. Brian Caswell, Jay Beale, Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. – Syngress Media, U.S. 2006. http://www.lehmanns.de/ shop/sachbuch-ratgeber/21797174-9780080549279 snort-intrusion-detection-and-prevention-toolkit #drm1

[4]. Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. (2008) «Information security in open systems. Textbook for high schools». *M.: T.II. Remedies in networks,* 558 p.

[5]. Ushakov DV (2005) Development of the principles of functioning of network intrusion detection systems based on the model of a distributed system protected: Dis. Candidate. tehn. Sciences: 05.13.19 Moscow, 175 p.

[6]. Smirnov N.V., Dunin-Barkovskii I.V. (1969) «Course on probability theory and mathematical statistics for technical applications» *Moscow: Nauka*, 512 p.

[7]. Scheffe H. (1980) «The analysis of variance», Moscow: Nauka, 512 p.

[8]. Kuznetsov A.A., Semenov S.G., Simonenko S.N., Meleshko E.V. (2010) «Method of structural identification information flows in telecommunication networks based on BDS-test», "Nauka i tehnika Povitryanih Forces Zbroynih forces of Ukraine", Preview Issue 2 (4), Kharkiv: Hoopes, P. 131-137.

[9]. Semenov S., Smirnov A., Meleshko E. (2010) «The method of processing and identification of telecommunication traffic based on BDS-tests», The book of materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)» Kiev, Ukraine, National Aviation University "NAU-Druk" Publishing House, October 13-14, C.166-168.

[10]. B. LeBaron (1997) "A Fast Algorithm for the BDS Statistic", Studies in Nonlinear Dynamics and Econometrics, Vol. 2. No. 2. P. 53-59.

[11]. D. Chappell J. Padmore and C. Ellis. (1996) "A note on the distribution of BDS statistics for a real exchange rate series", Oxford Bulletin of Economics and Statistics, 58, 3, 561- 566.


## СТАТИСТИЧНІ ВЛАСТИВОСТІ ТРАФІКУ НА ОСНОВІ BDS-ТЕСТІВ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯ В ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ


У роботі пропонується використовувати математичний апарат статистичного аналізу на основі BDS - тестів для дослідження властивостей мережевого трафіку різних служб та інформаційних сервісів при визначенні значущості розбіжності чи збігу їх характеристик. Отримані результати експериментальних досліджень статистичних властивостей мережевого трафіку з використанням кореляційного аналізу часових рядів підтверджують теоретичні припущення про те, що для різних видів трафіку (HTTP, FTP, Skype трафік і потокове мовлення ) результат BDS -тесту дає різні значення, які можуть бути прийняті в якості еталонних при використанні та удосконаленні механізмів моніторингу мережевої активності, в тому числі і для реалізації системи виявлення та запобігання вторгнень в телекомунікаційних системах та мережах.



**Ключові слова:** телекомунікаційні системи та мережі, система виявлення і запобігання вторгнень, BDS-статистика, статистичні властивості трафіку.


## STATISTICAL PROPERTIES OF TRAFFIC BASED ON BDS-TESTS FOR REALIZING SYSTEM OF INTRUSION DETECTION AND PREVENTION IN A TELECOMMUNICATIONS NETWORK


The paper presents the mathematical apparatus of statistical analysis based on the BDS- test to investigate the properties of network traffic of various services and information services in determining the significance of differences or match their characteristics. The obtained experimental results of the statistical properties of network traffic using correlation analysis of time series confirm the theoretical assumption that different types of traffic (HTTP, FTP, Skype traffic and streaming ) BDS- test result gives different values that can be taken as reference using and improving mechanisms for monitoring network activity, including the implementation of a system for intrusion detection and prevention in telecommunication systems and networks.



**Index Terms:** telecommunication systems and networks, system intrusion detection and prevention, BDS-statistics, the statistical properties of the traffic.



**Смирнов Алексей Анатольевич**, доктор технических наук, доцент, профессор кафедры программного обеспечения Кировоградского национального технического университета.
E-mail: assa_s@mail.ru

**Смірнов Олексій Анатолійович**, доктор технічних наук, доцент, професор кафедри програмного забезпечення Кіровоградського національного технічного університету.

**Smirnov Alexey**, Doctor of technical sciences, Associate Professor, Professor of Academic Department of software Kirovograd National Technical University.

**Дрейс Юрий Александрович**, кандидат технических наук, доцент кафедры безопасности информационных и коммуникационных систем Житомирского военного института им. С.П. Королева Государственного университета телекоммуникаций.
E-mail: dr_yr_al@mail.ru
**Дрейс Юрій Олександрович**, кандидат технічних наук, доцент кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Державного університету телекомунікацій.

**Dreis Yurii**, PhD in Eng., Associate Professor of Academic Department of Security Information and Communication Systems of the Zhytomyr Military Institute named after S.P. Koroleva of the State University of Telecommunication.

**Даниленко Дмитрий Алексеевич**, аспирант кафедры программного обеспечения Кировоградского национального технического университета.
E-mail: dmitriy.danilenko@kiroe.com.ua
**Даниленко Дмитро Олексійович**, аспірант кафедри програмного забезпечення Кіровоградського національного технічного університету.
**Danilenko Dmitry**, graduate student of Academic Department of software Kirovograd National Technical University.

**УДК 004.056.5(045)**

# РІШЕННЯ ЗВОРОТНОЇ ЗАДАЧІ ЕКОНОМІЧНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Євген Левченко, Руслана Прус***

*При розв'язку зворотної задачі економічного менеджменту задають параметри інформаційної системи і знаходять необхідну кількість ресурсів і їх оптимальний розподіл між об'єктами. Критерієм оптимальності є мінімізація загальних втрат, які включають втрати від витоку інформації і витрати на її захист, або максимізація прибутку від інвестицій в захист і їх рентабельності. Розглянуто систему з двох об'єктів, які відрізняються вразливістю і кількістю інформації. Розв'язок знаходиться в області існування сідлової точки, що забезпечує реальність одержаних результатів, оскільки ні одна з сторін не зацікавлена в зміні своєї стратегії. Виконання обох умов – забезпечення режиму сідлової точки і оптимізація розподілу ресурсів – досягається шляхом управління параметрами інформаційної системи – вразливостями об'єктів і розподілом інформації по об'єктах. Рішення зворотної задачі є першим кроком до синтезу системи. Наступний крок – вибір засобів захисту для кожного об'єкта з врахуванням їх вартості та імовірності нейтралізації можливих загроз.*

***Ключові слова:*** *інформаційна безпека, математична модель, вразливість, оптимізація, сідлова точка.*

**Вступ.** Розвиток інформаційної сфери приводить до зростання обсягів і вартості інформації і, як наслідок, до ускладнення систем захисту та збільшення їх вартості. В цих умовах зростають вимоги до створення систем, в яких досягаються найкращі технічні та економічні показники.

Рішення поставленої задачі утруднене через низку причин. Це складність багаторівневих багаторубіжних систем захисту, невизначеність дій суперника, неможливість точного визначення захисних спроможностей системи, зокрема, такого важливого показника, як її вразливість, а також відсутність статистичної інформації про результати протистояння систем нападу і захисту. Через ці складнощі основна увага при дослідженні захисних систем приділяється їх аналізу, хоча створення оптимальних систем часто несе в собі елементи синтезу.

Аналіз системи захисту може вестись в двох протилежних напрямках:

– пряма задача – по заданим ресурсам захисту визначити частку втраченої інформації;

– зворотна задача – по заданому граничному значенню втрат інформації визначити необхідну кількість ресурсів захисту.

Рішення зворотної задачі складніше, ніж прямої, проте ця задача викликає значний інтерес, оскільки її розв'язок можна вважати першим кроком у синтезі оптимальних систем захисту.

**Мета роботи** – розробка методики розв'язку зворотної задачі, який забезпечує досягнення оптимальних значень показників інформаційної системи.