Уфа : УГАТУ, 2010 Вестник УГАТУ Т. 14, № 5 (40). С. 188–194



УДК 004.65

**Н. А. Тишина, И. Г. Дворовой, Н. А. Соловьев**

# ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ ВЕЙВЛЕТ-АНАЛИЗА СЕТЕВОГО ТРАФИКА

В статье предложено решение задачи автоматизации обнаружения вторжений в условиях неопределенности информационных процессов на основе управления межсетевым экранированием в реальном масштабе времени. *Информационная система персональных данных*; *автоматизация*; *мониторинг безопасности*; *обнаружение вторжений*; *вейвлет-анализ*; *сетевой трафик*

## ВВЕДЕНИЕ

Время разговоров о необходимости защиты персональных данных (ПДн), применимости норм ФЗ № 152 «О персональных данных» к организациям и предприятиям, их информационным системам и конкретным приложениям закончилось. Правительством РФ и государственными регулирующими органами определен порядок классификации информационных систем персональных данных (ИСПДн), сформированы конкретные технические требования к соответствующим классам систем [1].

В состав технических требований по защите ПДн при их обработке в ИСПДн входит обнаружение вторжений на основе непрерывного мониторинга информационных процессов (ИП) ИСПДн с автоматическим блокированием каналов передачи ПДн в случае возникновения угрозы безопасности и уведомлением администратора.

## 1. СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Вопросы аксиоматики, терминологии, методологии и связи теории обнаружения вторжений с другими научными дисциплинами находятся в стадии становления. Поэтому под вторжением в работе понимается комплекс угроз безопасности – компьютерные атаки, несанкционированные рассылки, неправомерное изменение конфигурации, мошенничество или саботаж внутренних нарушителей и т. д.

Системы обнаружения вторжений (СОВ или IDS – Intrusion Detection Systems) представляют собой программные или аппаратно-программные средства, автоматизирующие процесс контроля событий, протекающих в компьютерной системе или сети, и самостоятельно анализирующие эти события в поисках признаков проблем безопасности [2].

Ядром СОВ являются реализованные в ней методы обнаружения вторжений, которые можно разделить на два основных вида:

- обнаружение аномалий предполагает использование какой-либо модели для составления «нормального» профиля поведения защищаемой системы и мониторинг отклонения текущего поведения от этого нормального профиля;
- сигнатурный метод позволяет обнаружить атаку, если известны характеризующие ее параметры и их пороговые значения.

Сигнатурный метод характеризуется высокой достоверностью, т. е. низким числом ложных срабатываний, и сравнительно невысокими требованиями к потребляемым ресурсам, но позволяет определять только уже известные атаки.

Метод обнаружения аномалий позволяет обнаруживать известные и неизвестные ранее несанкционированные воздействия, но СОВ, использующие данный метод, как правило, обладают низкой достоверностью принимаемых решений. Это связано с параметрической неопределенностью ИП: нестационарность процессов во времени и пространстве признаков, появление новых и совершенствование существующих несанкционированных воздействий.

Перспективный метод обнаружения вторжений должен обладать:

- возможностью обнаружения известных и неизвестных типов вторжений;
- высокой достоверностью принятия решений, т. е. низким числом ложных срабатываний;
- возможностью работы в реальном масштабе времени;
- автоматическим выбором пороговых значений параметров и их изменением в соответствии с текущим состоянием системы;
- приемлемыми требованиями к потребляемым ресурсам.

Контактная информация: povt@unpk.osu.ru

Очевидно, такой метод будет обладать возможностями сигнатурного метода и обнаружения аномалий, что свидетельствует об актуальности проведения исследований в области автоматизации мониторинга безопасности в условиях параметрической неопределенности ИП ИСПДн.

## 2. ПОСТАНОВКА ЗАДАЧИ

Под мониторингом ИП ИСПДн понимается анализ сетевого трафика (объем переданной информации в байтах, количество переданных пакетов, загрузка процессора) за определенный интервал времени. Трафик рассматривается как одномерный цифровой массив данных в виде числового ряда $f(t_i)$, заданный в дискретные моменты времени $t_i = i\Delta$, где $i = 0,1,\ldots, N-1$; $\Delta$ – интервал между отдельными наблюдениями; $N$ – количество наблюдений.

Математически $f(t_i)$ представляется в виде ряда с разложением по системе базисных функций:

функции тренда $q_m(t_i)$ – средних значений по большим интервалам усреднения (медленно меняющаяся во времени функция, описывающая изменения среднесуточных загрузок сети за интервалы времени большие, чем суточная периодичность);

циклических компонент с определенным периодом повторения $q_ц(t_i)$, как правило, достаточно гладких по форме (периодическая составляющая, описывающая изменения среднесуточных загрузок);

локальных особенностей (аномалий) разного порядка $\varepsilon_a(t_i)$, вплоть до вторжений – резких изменений в определенные редкие моменты;

флюктуаций значений более высокого порядка (шумов) $\varepsilon_ф(t_i)$ вокруг всех вышеперечисленных составляющих, относительно которых делается предположение, что в случайные моменты времени математическое ожидание $M[\varepsilon_ф(ti)] = 0$.

Отсюда математическая модель сетевого трафика представляется в виде:

$$f(t_i) = q_m(t_i) + q_ц(t_i) + \varepsilon_a(t_i) + \varepsilon_ф(t_i). \qquad (1)$$

Параметрическая неопределенность определяется первыми двумя составляющими ряда, что затрудняет адекватное описание сетевого трафика по модели (1) известными методами статистического или гармонического анализа [2, 3].

Авторами выдвинута гипотеза о возможности адекватного описания составляющих (1) методами теории вейвлет-анализа (ВА) [4].

## 2. ВЕЙВЛЕТ-МОДЕЛЬ СЕТЕВОГО ТРАФИКА

ВА предполагает представление одномерного цифрового массива (сетевого трафика) в различных масштабах, т. е. при различном разрешении. Преимущество такого подхода очевидно – характерные детали, которые могут оставаться незамеченными при одном разрешении, легко могут быть обнаружены на другом.

Вейвлет-модель (1) примет вид:

$$f(t_i) = \sum_{k=-\infty}^{\infty} c_{m,k}\,\varphi_{m,k}(t) + \sum_{m=m'}^{\infty}\sum_{k=-\infty}^{\infty} d_{m,k}\,\psi_{m,k}(t), \qquad (2)$$

$$m,k \in I,$$

где $\varphi_{m,k}(t)$ – масштабирующая функция, с помощью которой выполняется аппроксимация сетевого трафика;

$\psi_{m,k}(t)$ – вейвлет-функция, выделяющая детали сетевого трафика и его локальные особенности;

$c_{m,k}$, $d_{m,k}$ – апроксимирующие и детализирующие коэффициенты;

$m$, $k$ – параметры масштаба и сдвига;

$I$ – множество целых чисел $\{-\infty, \infty\}$.

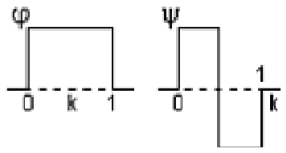
Первая сумма в (2) содержит усредненные (с весовыми функциями $\varphi_{m,k}$) значения $f(t_i)$ по диадным интервалам $[k\cdot 2^{-m}, (k+1)\cdot 2^{-m}]$, характеризует тренд и циклические составляющие трафика:

$$q_m(t_i) + q_ц(t_i) = \sum_{k=-\infty}^{\infty} c_{m,k}\,\varphi_{m,k}(t), \qquad (3)$$

а вторая – значения флюктуаций на данных интервалах, характеризующих активность (аномальность) субъектов сети, с учетом случайной шумовой помехи

$$\varepsilon_a(t_i) + \varepsilon_ф(t_i) = \sum_{m=m'}^{\infty}\sum_{k=-\infty}^{\infty} d_{m,k}\,\psi_{m,k}(t). \qquad (4)$$

Исследования авторов [4, 5] показали, что для мониторинга сетевого трафика целесообразно использовать масштабирующую функцию $\varphi_{m,k}(t)$ и вейвлет Хаара $\psi_{m,k}(t)$, представленные на рис. 1.




*а* *б*

**Рис. 1.** Масштабирующая функция (*а*) и вейвлет Хаара (*б*)

ВА при последовательном увеличении значений $m$ приводит к форме быстрых итерационных вычислений вейвлет-коэффициентов вида:

$$c_{m+1,k} = \sum_n h_n \, c_{m,2k+n}, \qquad (5)$$

$$d_{m+1,k} = \sum_n g_n \, c_{m,2k+n}. \qquad (6)$$

Для массивов цифровых данных сетевого трафика в качестве значений $c_{0,k}$ принимаются исходные значения одномерного числового ряда, т. е. $c_{0,k} = f(k) = f(t_0)$. Отсюда явный вид вейвлета требуется только для расчета коэффициентов $h_n$ и $g_n$, а при собственно быстром вейвлет-преобразовании используются уже полученные значения коэффициентов на соответствующем уровне детализации.

Уравнения (5), (6) обеспечивают реализацию быстрого ВА одномерного числового ряда на основе пирамидального алгоритма вычисления вейвлет-коэффициентов (алгоритм Маллата), приведенного на рис. 2.

Сущность операций алгоритма Маллата заключается в следующем. С учетом спектров коэффициентов $h_n$ и $g_n$, на первом этапе преобразования первый цифровой фильтр $c_{1,k}$ из числового ряда $f_k = c_{0,k}$ выделяет низкие частоты $|\omega| \le \le \omega/2$, а другой фильтр $d_{1,k}$ выделяет верхние частоты $\pi/2 \le |\omega| \le \pi$. Поскольку на выходе фильтра $c_{1,k}$ отсутствует верхняя половина частот, то частота дискретизации выходного множества может быть уменьшена в 2 раза, т. е. выполнена децимация выходного массива, что и производится в (2) сдвигами ($2k + n$) через 2 отсчета по входному массиву. Соответственно, на выходе фильтра $d_{1,k}$ освобождается место в области низких частот, и аналогичное прореживание выходного цифрового массива приводит к транспонированию верхних частот на освободившееся место. Следовательно, каждый из выходных цифрового массивов несет информацию о своей половине частот, при этом выходная информация представлена таким же количеством отсчетов, что и входная.

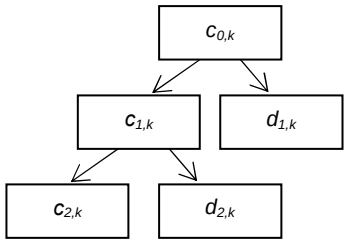



**Рис. 2.** Алгоритм Маллата

Таким образом, выражение (2) показывает возможность аппроксимации любой произвольной функции $f(t_i)$ набором простых локальных функций $\varphi_{m,k}(t)$ и $\psi_{m,k}(t)$, ортогональных на разных уровнях значений $m$ и полностью покрывающих пространство $L^2(R)$ за счет смещений $k$. Переход от $m$ к $m$+1 эквивалентен замене $t$ на $2t$, т. е. перемасштабированию функций $\varphi_{m,k}(t)$ и $\psi_{m,k}(t)$.

Если реализовать модель (2) в режимах обучения и анализа, то в первом случае зафиксируется эталонный ряд $f^э(t_i)$, а во втором на программно управляемом интервале будет регистрироваться текущая загрузка сети $f^р(t_i)$. Разность между $f^э(t_i)$ и $f^р(t_i)$ определит текущий уровень аномальности ИП $f_a(t_i)$:

$$f_a(t_i) = \sum_{k=-\infty}^{\infty} \sum_{m=m'}^{\infty} d^{\,р}{}_{m,k} \, \Psi_{m,k}(t) + \\ + \sum_{m=m'}^{\infty} \sum_{k=-\infty}^{\infty} d^{\,э}{}_{m,k} \, \Psi_{m,k}(t). \qquad (7)$$

Зависимость (7) позволяет устранить тренд и циклическую составляющую и на определенном уровне разрешения оценить активности субъектов ИСПДн.

На рис. 3–5 представлены основные схемы алгоритмов мониторинга ИП, реализованные в программной системе «Анализатор Аномальности» [6].

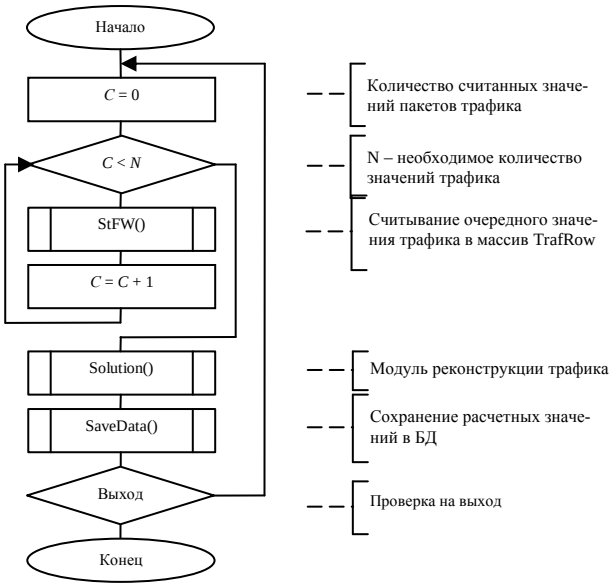



**Рис. 3.** Укрупненный алгоритм мониторинга ИП

Таким образом, ВА позволяет адекватно описать нестационарные во времени и неоднородные в пространстве ИП ИСПДн.

## 3. МЕТОДИКА ОБОСНОВАНИЯ ПОРОГОВОГО УРОВНЯ АНОМАЛЬНОСТИ

В основу обоснования положен метод статистических решений для задачи проверки двухальтернативной гипотезы: $H_0$ и $H_1$ выражают предположения об отсутствии или наличии вторжения на текущем уровне активности $f_a(t_i)$ субъектов ТС.

Для того, чтобы задача обнаружения вторжений обрела математическую содержательность, введены показатели – вероятности ложной тревоги $p_{лт}$ и пропуска вторжения $p_{пв}$, понимая под ложной тревогой принятие решения $\hat{H}_1$ об обнаружении вторжения при условии, что в наблюдаемом $f_a(t_i)$ вторжение отсутствует, а под пропуском вторжения – принятие решения $\hat{H}_0$ о том, что вторжения в $f_a(t_i)$ нет, при условии, что в действительности информационная атака (ИА) имеет место.

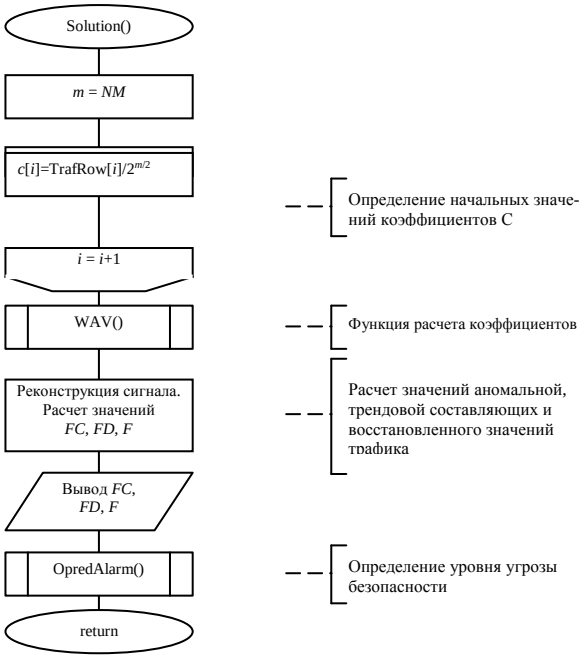



**Рис. 4.** Алгоритм реконструкции трафика Solution()

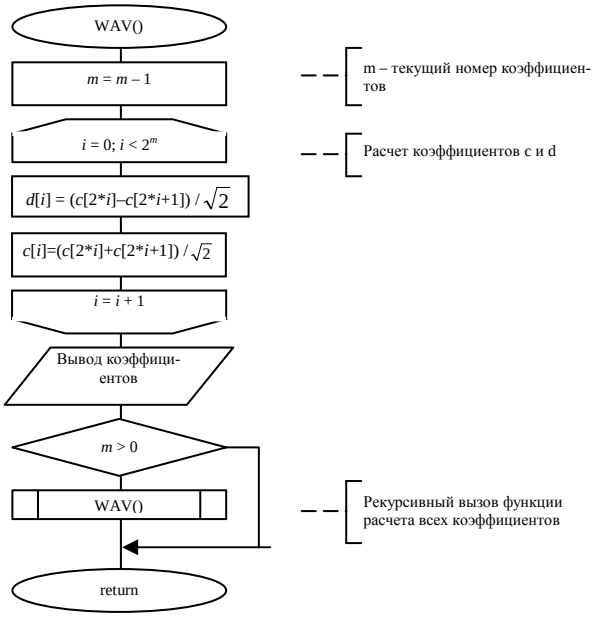



**Рис. 5.** Алгоритм расчета вейвлет-коэффициентов Wav()

В результате экспериментальных исследований ИП системы электронного документооборота DIRECTUM ОАО «Оренбургнефть» [7] доказано, что на интервале 5-10 минут закон распределения носит нормальный характер, что позволило, используя методику определения вероятностей $p_{пв}$ (прямая штриховка), $p_{лт}$ (косая штриховка), представленную на рис. 6, вывести расчетные зависимости для искомых вероятностей:

$$p_{лт} = P(\hat{H}_1 \mid H_0) = \\ = P(z \geq z_{П} \mid H_0) = \int_{z_n}^{\infty} W(z \mid H_0)dz, \quad (8)$$

$$p_{пв} = P(\hat{H}_0 \mid H_1) = \\ = P(z < z_{П} \mid H_1) = \int_{-\infty}^{z_n} W(z \mid H_1)dz, \quad (9)$$

где $z = \int_0^T f_a(t_i)\varepsilon_a(t_i)dt$ – корреляционный интеграл, определяющий степень сходства наблюдаемой реализации $f_a(t_i)$ с ожидаемой аномалией $\varepsilon_a(t_i)$; $z_n$ – пороговый уровень аномальности сетевого трафика; $W(z/H_1) = P(z < z_n / H_i)$ – плотность вероятности $z$ при гипотезе $H_i$, $i$ = = 0,1; $T$ – интервал наблюдения.

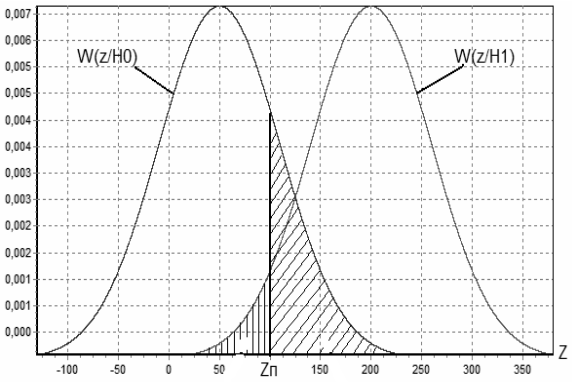



**Рис. 6.** Методика определения вероятностей

Так как $z$ есть линейное преобразование случайного процесса в наблюдаемом $f_a(t_i)$, то $W(z/Hi)$ – одномерные нормальные плотности вероятностей. С учетом математического ожидания $\bar{z}$ и дисперсии $D\{z\}$, расчетные зависимости для искомых вероятностей примут вид

$$p_{лт} = \frac{1}{\sqrt{2\pi}} \times \\ \times \int_{Zn}^{\infty} \frac{1}{\sqrt{D(z)}} \exp(-\frac{z^2}{2D(z)})dz = 1 - \Phi(h); \quad (10)$$

$$p_{пв} = \frac{1}{\sqrt{2\pi}} \times \\ \times \int_{-\infty}^{zn} \frac{1}{\sqrt{D(z)}} \exp(-\frac{(z-\bar{z})^2}{2D(z)})dz = \Phi(h-q); \quad (11)$$

где $\Phi(x) = (1/\sqrt{2\pi}) \int_{-\infty}^{x} \exp(-k^2/2)dk$ – интеграл вероятности при $k = z(\sqrt{D(z)})^{-1}$;

$h = z_n(\sqrt{D(z)})^{-1}$ – нормированный пороговый уровень;

$q = z(\sqrt{2\bar{z}/N_0})^{-1}$ – параметр обнаружения, равный соотношению сигнал/шум.

С помощью соотношений (7), (8) рассчитывается $z_n$ в соответствии с принятым критерием оптимальности. При использовании критерия Неймана – Пирсона требуется минимизировать $p_{пв}$ при фиксированном значении $p_{лт}$, т. е. найти нормированный порог $h$, решив обратную функцию $\Phi^{-1}(*)$ вида $h = \Phi^{-1}(1 - P_{лт})$, и путем подстановки $h$ в (8) определить минимальную величину $p_{пв}$. Полученные оценки $p_{пв}$ и $p_{лт}$ в форме условной минимизации целевой функции $p_{пв} + \mu p_{лт}$, где $\mu$ – неопределенный множитель Лагранжа, рассчитанный на основе метода нелинейного программирования с использованием теоремы Куна-Таккера [7], при заданных условиях реализации ИП обеспечивают оптимальную величину среднего риска при $p_{лт} \leq$ $\leq 0{,}05$. Данная методика реализована в программном продукте, алгоритм работы которой представлен на рис. 7.

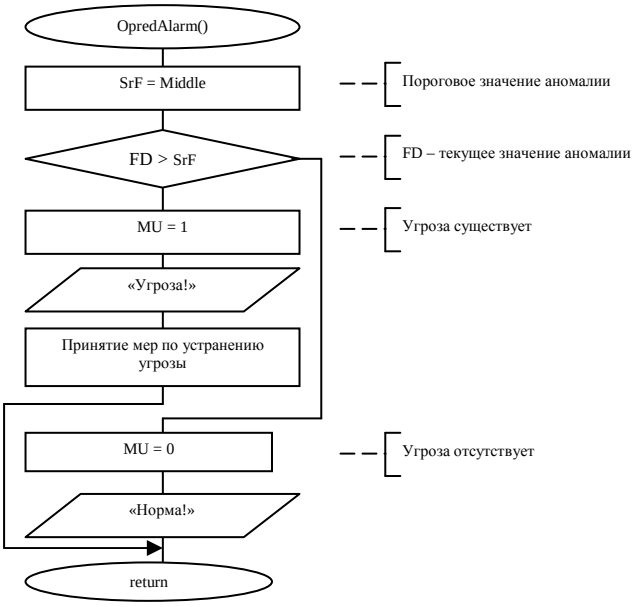



**Рис. 7.** Алгоритм расчета порога аномальности

Таким образом, предложенная методика и алгоритм расчета порога аномальной активности субъектов сети являются развитием методов распознавания теории статистических решений в задаче обнаружения вторжений.

## 4. ПРОТОТИП СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ОЦЕНКА ЕГО ЭФФЕКТИВНОСТИ

В качестве прототипа принята среда брандмауэра Windows NT со средствами обнаружения вторжений IDS Snort и StopAttak. Развитием прототипа является двухуровневый контур управления базой правил брандмауэра, представленный на рис. 8.

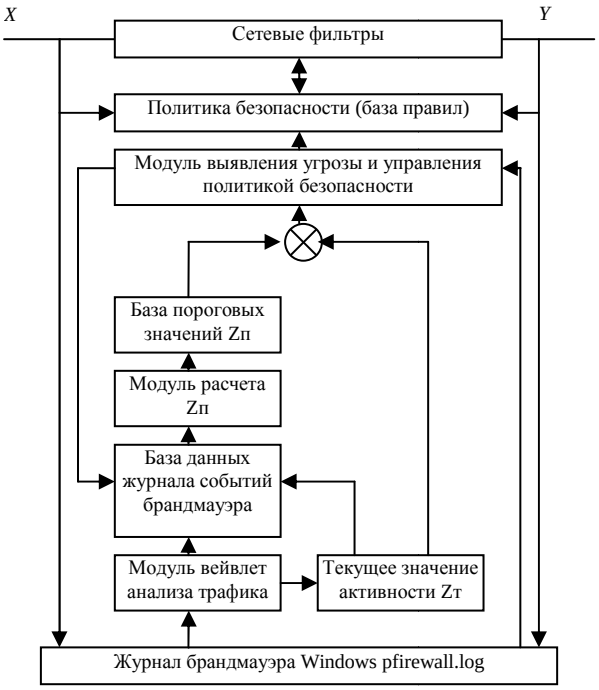



**Рис. 8.** Контур автоматического обнаружения вторжений

Предложенный контур является развитием архитектуры межсетевого экранирования (МСЭ) с поддержкой функции автоматического управления базой правил брандмауэра при обнаружении вторжения или аномальной активности субъектов ИСПДн.

Оценка эффективности прототипа автоматической системы обнаружения вторжений проведена на экспериментальном участке телекоммуникационной сети системы электронного документооборота и управления взаимодействием DIRECTUM ОАО «Оренбургнефть». Результаты эксперимента представлены на рис. 9 и в таблице 1.

Результаты эксперимента свидетельствуют, что с применением новой технологии принятия решений в СОВ следует ожидать обеспечение вероятности обнаружения вторжений при решении задач ПДн на уровне 0,78–0,88 при ограничении на допустимую вероятность ложной тревоги, причем положительный эффект новой технологии принятия решений усиливается по мере увеличения единого информационного поля ИСПДн.

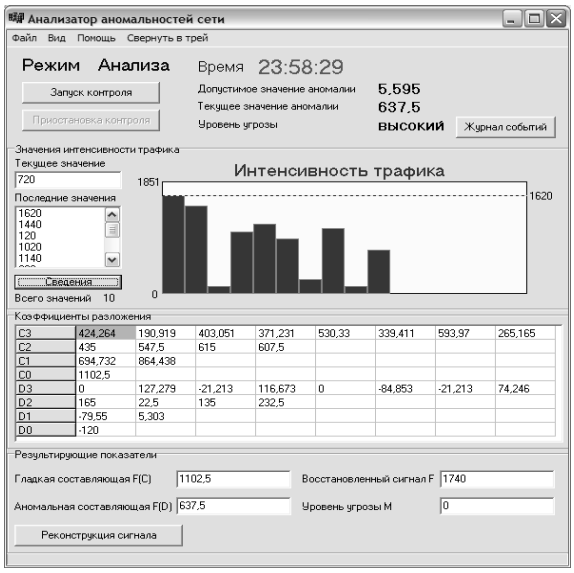



**Рис. 9.** Экранная форма результата эксперимента

**Оперативность и достоверность решений**

| Тип вторжения | IDS | Ср. время обнар, с | Вер. обнар., $(1-p_{па})$ | Оценка точн., $\varepsilon_{рпа}$ |
|---|---|---|---|---|
| Сканер пор- | Snort | 4,11 | 0,86 | 0,04 |
| | StopAttak | 3,86 | 0,84 | 0,0376 |
| | AA | 3,8 | 0,94 | 0,028 |
| DOS - атаки | Snort | 2,08 | 0,72 | 0,0724 |
| | StopAttak | 1,22 | 0,79 | 0,0674 |
| | AA | 0,98 | 0,84 | 0,05 |
| Атаки на сервер spam | Snort | 2,78 | 0,66 | 0,023 |
| | StopAttak | 2,46 | 0,7 | 0,046 |
| | AA | 2,28 | 0,84 | 0,049 |
| | Snort | – | – | – |
| | StopAttak | 3,6 | 0,8 | 0,0430 |
| | AA | 3,15 | 0,86 | 0,0469 |

По сравнению с известными IDS, предложенное решение СОВ обладает более высокими характеристиками: по быстродействию на 10–12%, по вероятности пропуска атаки – на 12–22% при допустимом уровне вероятности ложной тревоги 0,05.

## ВЫВОДЫ

1. Предложено развитие метода ВА для моделирования сетевого трафика, обеспечивающее повышение достоверности принимаемых решений СОВ в условиях параметрической неопределенности ИП.

2. Разработан контур автоматизации администрирования безопасности ИСПДн, являющийся развитием архитектуры МСЭ с поддерж-

кой функции автоматического управления базой правил доступом, обеспечивающий повышение оперативности принимаемых решений СОВ.

3. Предложена методика обоснования порога аномальной активности субъектов ИСПДн, являющаяся развитием методов распознавания теории статистических решений в задаче обнаружения вторжений в условиях параметрической неопределенности ИП.

4. Предложенное решение задачи обеспечения безопасности ИСПДн в условиях параметрической неопределенности ИП – автоматизации мониторинга безопасности на основе ВА позволяет повысить достоверность обнаружения вторжений на 10–12% с вероятностью обнаружения 0,78–0,88 при ложной тревоге не более 0,05.

## СПИСОК ЛИТЕРАТУРЫ

1. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. М: ФСТЭК, 2008. 30 с.

2. **Аграновский А. В., Хади Р. А., Якубец М. Б.** Статистические методы обнаружения аномального поведения в системах обнаружения атак // Информационные технологии. 2005. № 3. С. 34–38.

3. **Петренко С. А., Беляев А. В.** Сравнительный анализ методов обнаружения компьютерных атак // Проблемы информационной безопасности. Компьютерные системы. 2008. № 2. С. 48–53.

4. **Соловьев Н. А., Юркевская Л. А.** Метод идентификации угроз безопасности информационных ресурсов АСУ на основе мультиразрешающего анализа // Вестник Самарского государственного технического университета. 2007. С. 12–16.

5. **Блаттер К.** Вейвлет-анализ. Основы теории. М.: ТЕХСФЕРА, 2006. 272 с.

6. Анализатор Аномальности. Свидетельство о государственной регистрации программы для ЭВМ № 2008610111 / Ю. А. Азиатцев [и др.]. М.: Федеральная служба по интеллектуальной собственности, патентам и товарным знакам, 2008.

7. **Тишина Н. А., Соловьев Н. А.** Статистическое обоснование порогового уровня аномальной активности субъектов сети с использованием теоремы Куна-Таккера // Инновации в науке, бизнесе и образовании: сб. науч. тр. Оренбург: Тип. ОГИМ, 2008. С. 25–47.

## ОБ АВТОРАХ

**Тишина Наталья Александровна,** асп. каф. ПОВТАС. Дипл. матем. (ОГПУ, 2000). Готовит дисс. в обл. защиты информации.

**Дворовой Иван Геннадьевич,** асп. той же каф. Дипл. инж. по инф. сервису (ЮРГУЭС, 2006). Готовит дисс. в обл. администрирования сетей и инф. безопасности.

**Соловьев Николай Алексеевич,** зав. той же каф. Дипл. инж. по радиотехнике (ЯВЗРУ, 1973, КВЗРИУ, 1980). Д-р техн. наук по киберн., системн. анализу и моделир-ю систем и процессов (ВА ВПВО, 2001). Иссл. в обл. автом. упр-я и принятия решений.