На правах рукописи

ТИШИНА Наталья Александровна

СИСТЕМА ВЫЯВЛЕНИЯ И БЛОКИРОВАНИЯ АНОМАЛИЙ ТРАФИКА КОРПОРАТИВНЫХ СЕТЕЙ НА ОСНОВЕ ВЕЙВЛЕТ-ПАКЕТОВ

Специальность: 05.13.19
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа - 2012

Работа выполнена в ФГБОУ ВПО
«Оренбургский государственный университет»

Научный руководитель: доктор технических наук, профессор
СОЛОВЬЕВ Николай Алексеевич,
Оренбургский государственный университет, кафедра программного обеспечения вычислительной техники и автоматизированных систем

Официальные оппоненты: доктор технических наук, доцент
МАШКИНА Ирина Владимировна,
Уфимский государственный авиационный технический университет, кафедра вычислительной техники и защиты информации

кандидат технических наук, доцент
БОРОВСКИЙ Александр Сергеевич,
Оренбургский государственный университет, кафедра управления и информатики в технических системах

Ведущая организация: ФГБОУ ВПО «Оренбургский государственный институт менеджмента»

Защита состоится «27» апреля 2012 г. в 10^{00} часов на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете по адресу: 450000, Уфа-центр, ул. К.Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «12» марта 2012 г.

Ученый секретарь
диссертационного совета

доктор техн. наук, профессор С.С.Валеев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В условиях финансовой неустойчивости рынка ведущие корпорации России избавляются от непрофильных видов деятельности, включая поддержку и сопровождение информационно-телекоммуникационных систем, технической основой которых является корпоративная компьютерная сеть (ККС). Задача обеспечения информационной безопасности (ИБ) ККС становится одной из центральных для корпоративных предприятий, имеющих территориально-распределенную структуру и вынужденных использовать сети общего пользования.

Проблемам обеспечения ИБ ККС посвящены работы таких известных российских ученых как Бородакий Ю.В., Васильев В.И., Гаценко О.Ю., Герасименко В.А., Гузаиров М.Б., Зегжда П.Д., Ковалев В.В., Машкина И.В., Остапенко А.Г., Расторгуев С.П. и зарубежных исследователей Андерсона Д., Деннига Д., Лендвера К., МакЛина Д., Сандху Р. и других. В Оренбургском государственном университете эти вопросы исследовались в работах Соловьева Н.А., Саюшкина А.А., Цыганкова А.С., Юркевской Л.А..

Обобщая результаты исследований, можно сделать вывод, что в настоящее время сложилась методологическая база выявления угроз нарушения ИБ ККС, разработаны методы, модели и средства, позволяющие решать широкий спектр задач защиты информации. Вместе с тем, существующие средства обнаружения вторжений, являющиеся первым рубежом систем защиты, надежно работают лишь в условиях стационарности и однородности информационных процессов (ИП). В связи с ростом числа фактов нарушения конфиденциальности, целостности или доступности информации в ККС, использующих сети общего пользования, возникает необходимость разработки принципиально иных подходов к обнаружению вторжений, позволяющих повысить достоверность принимаемых решений. Это определяет *актуальность* проведения исследований в области выявления угроз ИБ ККС в условиях параметрической неопределенности ИП.

Объектом исследования являются методы, модели и средства мониторинга ИБ компьютерных сетей; **предметом –** методы, модели и средства выявления и предотвращения вторжений в инфраструктуру корпоративных сетей; г**раницы исследований –** выявление и блокирование аномалий трафика ККС.

Основной задачей исследований становится разрешение противоречия между существенно возросшей неопределенностью информационных процессов в сетях общего пользования и отсутствием методов достоверного обнаружения аномалий трафика корпоративных сетей в реальном режиме времени.

Эти обстоятельства определяют **цель исследования:** *повышение оперативности и достоверности выявления и блокирования аномалий трафика ККС в ус-*

ловиях параметрической неопределенности ИП.

Для достижения сформулированной цели в диссертации поставлены и решены следующие задачи:

– анализ современных технологий обнаружения и предотвращения вторжений в инфраструктуру корпоративных сетей и особенностей информационных процессов корпоративных сетей, использующих вычислительные сети общего доступа;

– разработка метода выявления и блокирования аномалий трафика корпоративных сетей в условиях параметрической неопределенности информационных процессов;

– разработка методики обоснования порога аномального состояния сетевого трафика и алгоритмов её программной реализации;

– разработка прототипа системы выявления и блокирования аномалий трафика корпоративных сетей на основе управляемого межсетевого экрана и оценка его эффективности.

Научной основой для решения поставленных задач являются: теория системных исследований; теоретические основы информатики; методы и средства защиты информации; методы кратномасштабного анализа (КМА), теории распознавания и статистических решений.

Результаты, выносимые на защиту

1. Результаты анализа современных технологий обнаружения и предотвращения вторжений и особенностей современных корпоративных компьютерных сетей, использующих вычислительные сети общего доступа, свидетельствуют о низкой достоверности и оперативности выявления угроз ИБ ККС средствами обнаружения и предотвращения вторжений в условиях параметрической неопределённости ИП – нестационарности во времени, неоднородности в пространстве субъектов сети и неизвестных типах информационных воздействий.

2. Метод выявления и блокирования аномалий трафика ККС в условиях параметрической неопределенности ИП на основе интеграции вейвлет – пакетной модели сетевого трафика с авторегрессионной моделью прогнозирования его случайной составляющей.

3. Методика и алгоритмы обоснования порога аномального состояния сетевого трафика по критерию Неймана - Пирсона в форме условной минимизации целевой функции с использованием теоремы Куна-Таккера.

4. Прототип системы выявления и блокирования аномалий трафика ККС на основе двухуровневого контура управления базой правил межсетевого экрана и результаты оценки его эффективности.

Научная новизна

1. Научная новизна метода выявления и блокирования аномалий трафика ККС заключается в развитии КМА и его новом применении для моделирования сетевого трафика в условиях параметрической неопределенности ИП на основе интеграции вейвлет – пакетной модели сетевого трафика и прогнозирующей авторегрессией случайной составляющей. Метод отличается, во-первых, тем, что используемая вейвлет-пакетная модель обеспечивает адекватное описание сетевого трафика за счет дополнительной декомпозиции высокочастотных составляющих на аномалии и шумы, что позволяет повысить достоверность принимаемых решений. Во-вторых, использование в вейвлет-пакетной модели прогнозирования случайной составляющей трафика на основе авторегрессии позволяет обеспечить обнаружение аномалий в реальном режиме времени.

2. Новизна методики и алгоритмов обоснования порога аномального состояния сетевого трафика заключается в использовании критерия Неймана – Пирсона в форме условной минимизации целевой функции оценки нормированного порога аномальности на основе метода нелинейной оптимизации с использованием теоремы Куна-Таккера, обеспечивающего минимум среднего риска принятия решений при условии ограничения на вероятность ложной тревоги.

3. Новизна системы выявления и блокирования аномалий трафика ККС заключается в реализации двухуровневого контура управления базой правил межсетевого экрана, адаптивного к аномалиям сетевого трафика.

Практическая значимость обусловлена тем, что разработана программная система выявления и блокирования аномалий трафика ККС на основе двухуровневого контура управления базой правил межсетевого экрана, являющаяся развитием системного программного обеспечения вычислительных сетей, и обеспечивающая повышение достоверности и оперативности выявления угроз нарушения ИБ ККС.

Результаты диссертации в виде методического, программного и информационного обеспечения внедрены в ООО «ТБинформ» (г. Оренбург) и используются в учебном процессе ФГБОУ «Оренбургский государственный университет».

Апробация, публикации. Научные и практические результаты работы обсуждались и получили одобрение на конференциях в период 2007-2011 гг: «Современные информационные технологии в науке, образовании и практике», (Оренбург, 2007г., 2008 г., 2009 г., 2010г.); «Инновации в науке, бизнесе и образовании», (Оренбург, 2008 г.); «Опыт использования и проблемы внедрения инноваций в науке, промышленности, энергетике и строительстве» (Оренбург, 2009); «Компьютерная интеграция производства и ИПИ-технологии» (Оренбург, 2011); «Теоретические вопросы разработки, внедрения и эксплуатации программных средств» (Орск, 2011); «IT-Security Conference for the Next Generation» (Москва-Мюнхен, 2011).

Основные результаты исследований опубликованы в 14 печатных работах, три из которых – в изданиях, определенных ВАК России для опубликования научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук, в одном свидетельстве о государственной регистрации программ.

Работа состоит из введения, четырех разделов, заключения, изложенных на 129 страницах и 8 приложений, содержит 67 рисунков и 41 таблицы. Список использованных источников включает 172 наименования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность исследования, определены объект и предмет исследования, сформулированы цель и научная задача.

В первом разделе проведен системный анализ современного состояния теории и практики в области построения систем предотвращения вторжений (Intrusion Prevention System, IPS) и особенностей ИП современных корпоративных сетей.

Отказ корпоративных предприятий, имеющих территориально-распределенную структуру, от непрофильных видов деятельности, включая поддержку и сопровождение ККС, потребовал использования сетей общего пользования между локальными сегментами. Исследования показали, что отличительной особенностью такой инфраструктуры становится существенной параметрическая неопределенность ИП, что предопределяет высокий уровень ложных тревог и снижение оперативности принимаемых решений.

Основным методом обнаружения вторжений остается анализ сигнатур. Однако сигнатурный метод неустойчив к модификациям вторжений и не обладает адаптацией к появлению новых несанкционированных воздействий. Реализация поведенческого анализа сети – обнаружение аномалий (Network Behavior Anomaly Detection, NBAD), свободного от указанных недостатков, затруднена сложностью адекватного описания модели ИП сети в условиях параметрической неопределенности, возникающей за счет случайных составляющих: нестационарностью и неоднородностью ИП, шумов, помех, новых или модифицированных вторжений, атак и т.д.. Отсюда, основным противоречием между состоянием теории и требованиями практики NBAD становится противоречие между существенно возросшей параметрической неопределенностью ИП и недостаточным уровнем адекватности моделей, используемых в системах обнаружения аномалий (СОА) ККС. В рамках IPS признано целесообразным развитие СОА на методах, обеспечивающих снижение количества ложных тревог в сочетании с работой в режиме реального времени.

Для преодоления выявленных противоречий предлагается разработать СОА на основе средств разграничения доступа, которая, применительно к меж-

сетевому экрану (МСЭ), приводит к двухуровневому контуру управления базой правил, представленному на рисунке 1.

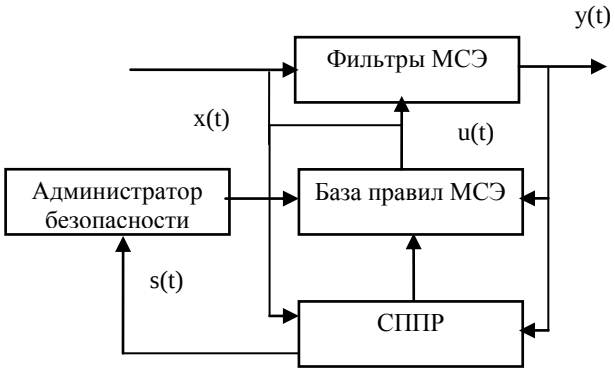

Рисунок 1 – Двухуровневый контур управления базой правил МСЭ

Основной контур строится на основе регулятора, функции которого выполняет база правил МСЭ, формируемая администратором безопасности. Дополнительный контур – средство поддержки принятия решений (СППР), по сути, являющийся контуром адаптации, настраивает вектор $u(t)$ регулятора в основном контуре для достижения цели управления при текущих значениях входных $x(t)$ и выходных $y(t)$ параметров объекта управления – сетевого трафика.

Анализ угроз безопасности ККС позволил определить параметры объекта управления, характеризующие сетевые аномалии. Под аномалией понимается любое отклонение от модели (профиля) нормального состояния трафика сети. Экспериментальные исследования позволили определить параметры объекта управления, имеющие потенциал для выявления аномального состояния трафика: количество потоков, пакетов, байт трафика сети; среднее количество пакетов или байт в потоке.

Во **втором разделе** получил развитие методический аппарат кратномасштабного анализа для выявления аномалий трафика ККС.

На рисунке 2 предложена технология обнаружения и блокирования аномалий трафика ККС.

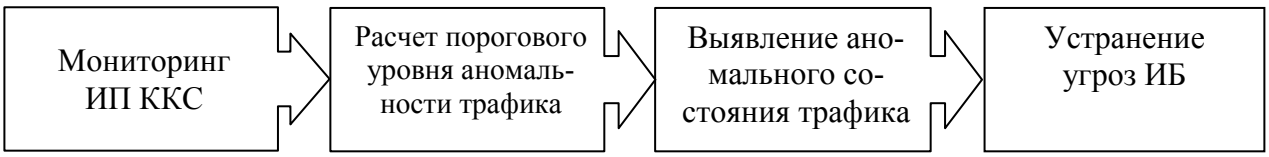

Рисунок 2 – Технология выявления и блокирования аномалий

Под мониторингом ИП ККС понимается анализ характеристик сетевого трафика. При этом трафик сети рассматривается в виде совокупности одномерных числовых рядов $f(t_i)$, заданных в дискретные моменты времени $t_i = i\Delta$, где $i = 0,1,\ldots, N-1$, Δ – интервал между отдельными наблюдениями, N – количество наблюдений.

Модель $f(t_i)$ представляется рядом с разложением по системе функций:

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

где $q_т(t_i)$ – тренд, средние значения по большим интервалам усреднения (медленно меняющаяся во времени функция, описывающая изменения загрузок ККС за интервалы времени большие, чем суточная периодичность);

$q_ц(t_i)$ – циклические компоненты с определенным периодом повторения, как правило, достаточно гладкие по форме (периодическая составляющая, описывающая изменения среднесуточных загрузок ККС);

$\varepsilon_a(t_i)$ – локальные особенности разного порядка, вплоть до резких изменений в определенные редкие моменты – аномалии;

$\varepsilon_ф(t_i)$ – флуктуации, случайные значения более высокого порядка (шумы) вокруг всех вышеперечисленных составляющих функции.

Каждый ряд обрабатывается независимо от остальных. Такое описание трафика позволяет учитывать несколько его характеристик в параллельном режиме.

Параметрическая неопределенность ИП ККС затрудняет адекватное описание трафика по модели (1).

В работах профессора Соловьева Н.А. доказана возможность адекватного описания составляющих модели (1) методами КМА, который предполагает представление функций в различных масштабах, т.е. при различных разрешениях. Преимущество такого подхода очевидно – характерные детали, которые могут оставаться незамеченными при одном разрешении, могут быть обнаружены на другом. Применительно к объекту исследования модель (1) после КМА примет вид:

$$f(t_i) = \sum_{k=-\infty}^{\infty} c_{m,k}\varphi_{m,k}(t_i) + \sum_{m=m'}^{\infty}\sum_{k=-\infty}^{\infty} d_{m,k}\psi_{m,k}(t_i), \quad m,k \in I, \qquad (2)$$

где $\varphi_{m,k}(t)$ – базисная масштабирующая функция;

$\psi_{m,k}(t)$ – базисная вейвлет-функция;

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

m, k – параметры масштаба и сдвига в пространстве целых чисел I.

Первая сумма $q_т(t_i) + q_ц(t_i) = \sum_{k=-\infty}^{\infty} c_{m,k}\varphi_{m,k}(t_i)$ содержит усредненные (с весовыми функциями $c_{m,k}$) значения $f(t_i)$ по диадным интервалам $[k\cdot 2^{-m}, (k+1)\cdot 2^{-m}]$, характеризует тренд и циклические составляющие трафика (суточные и недельные), а вторая $\varepsilon_a(t_i) + \varepsilon_ф(t_i) = \sum_{m=m'}^{\infty}\sum_{k=-\infty}^{\infty} d_{m,k}\psi_{m,k}(t_i)$ – локальные особенности сетевого трафика на фоне случайной шумовой составляющей (флуктуаций).

Исследования показали, что для мониторинга сетевого трафика в качестве базисных функций целесообразно использовать систему вейвлетов Койфмана: койфлеты – 2, представленную на рисунке 3.

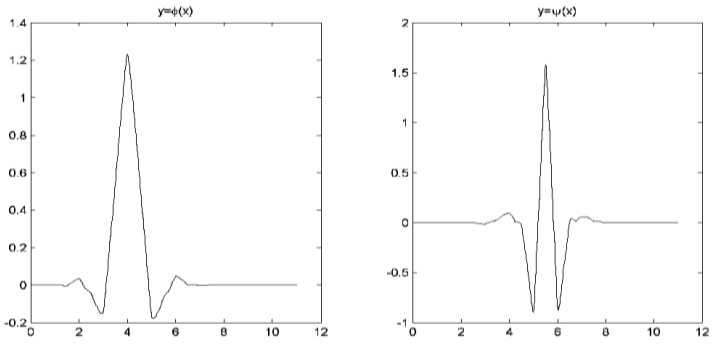

Рисунок 3 – Система вейвлетов: койфлеты – 2

Койфлеты имеют почти симметричную форму, обеспечивают большее количество близких к нулю коэффициентов разложения, обладают высокой крутизной среза полосы пропускания, и, соответственно, обеспечивают лучшее качество разложения и реконструкции сигналов.

В ранее проведенных исследованиях для локальных сетей принималось допущение о том, что флуктуации носят центрированный характер, т.е. $M[\varepsilon_\phi(t_i)] = 0$. Однако использование в ККС для передачи данных сетей общего пользования привело к существенному росту шумовой составляющей $\varepsilon_\phi(t_i)$ ИП и указанное допущение стало неприемлемым.

Автором выдвинута и доказана гипотеза о возможности повышения адекватности модели (2) за счет использования вейвлет-пакетного преобразования (ВПП) сетевого трафика, суть которого не что иное, как развитие КМА с повторной фильтрацией деталей. Применительно к предмету исследования повторная фильтрация деталей позволяет выделить аномальную составляющую и оценить флуктуации.

В основу ВПП заложены рекуррентные соотношения вида:

$$c_{m+1,2p,k} = \sum_n h_n c_{m,p,2k+n},\ d_{m+1,2p,k} = \sum_n g_n c_{m,p,2k+n}, \qquad (3)$$

$$c_{m+1,2p+1,k} = \sum_n h_n d_{m,p,2k+n},\ d_{m+1,2p+1,k} = \sum_n g_n d_{m,p,2k+n},\ k = 0..N/2^m. \qquad (4)$$

где m – номер масштабного уровня; p – номер узла в пределах масштабного уровня; k – номер коэффициентов в пределах узла.

Сущность алгоритмов ВПП отражена на рисунках 3 и 4.

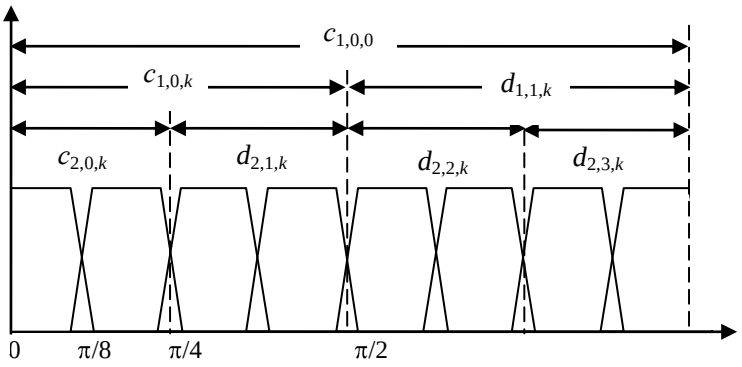

Рисунок 3 – Спектральные характеристики ВПП

На первом этапе преобразования первый цифровой фильтр h_n из числового ряда $f_k = c_{0,0,k}$ выделяет путем децимации аппроксимирующие коэффициенты $c_{m,p,k}$, а фильтр g_n – детализирующие коэффициенты $d_{m,p,k}$. При переходе с масштабного уровня m на уровень $m + 1$ как аппроксимирующие $c_{m,p,k}$, так и детализирующие коэффициенты $d_{m,p,k}$ разделяются вновь на низкочастотные ($c_{m+1,p,k}$) и высокочастотные ($d_{m+1,p,k}$) части спектрального диапазона. Дополнительная декомпозиция высокочастотных составляющих спектра трафика позволяет выделить локальные особенности (аномалии) и оценить флуктуации.

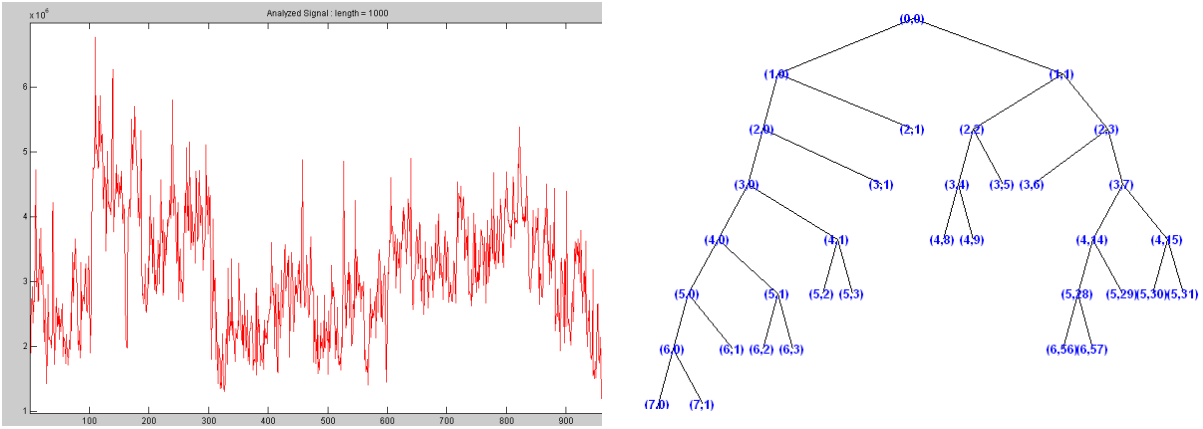

Рисунок 4 – Сетевой трафик и его ВВП

Из множества возможных базисов вейвлет-разложения – от «минимального» (алгоритм Малла) до полного ВПП на всех уровнях детализации экспериментально с учетом временных ограничений выбираются те, на которых аномальное состояние трафика проявляется наиболее четко. В качестве критерия выбора оптимального базиса ВПП предложено использовать критерий минимума энтропии, характеризующей уровень усреднения и определяющей количество существенных коэффициентов модели трафика. Дополнительными ограничениями являются ресурсные затраты.

Пусть значения номеров уровней m и номеров узлов p определены по результатам выбора оптимального базиса ВПП. Среди них номера уровней m_{o1}.. m_{ol} и номера узлов p_{o1} ..p_{oz} характеризующих аномалии и номера уровней $m_{\phi 1}$.. $m_{\phi l}$ и узлов $p_{\phi 1}$ ..$p_{\phi z}$, характеризующих шум. Тогда модель сетевого трафика, описывающая аномалии на фоне шумовой составляющей, принимает вид:

$$f_d(t_i) = \varepsilon_a(t_i) + \varepsilon_{\text{ф}}(t_i) = \sum_{m=m_{o1}}^{m_{ol}} \sum_{p=p_{o1}}^{p_{oz}} \sum_{k=0}^{N/2^m} d_{m,p,k} \psi_{m,p,k}(t_i) + \sum_{m=m_{\phi 1}}^{m_{\phi l}} \sum_{p=p_{\phi 1}}^{p_{\phi z}} \sum_{k=0}^{N/2^m} d_{m,p,k} \psi_{m,p,k}(t_i). \qquad (5)$$

Отсюда разность между эталонным $f_{d^э}(t_i)$ состоянием сетевого трафика (эталонный режим без аномалий), рассчитываемым в процессе обучения, и регистрируемым уровнем в процессе мониторинга сети $f_{d^p}(t_i)$ в предположении равенства флуктуаций $\varepsilon_\phi^э(t) = \varepsilon_\phi^p(t)$, определит текущий уровень отклонения от эталонного состояния трафика ККС:

$$\tilde{\varepsilon}_a(\text{t}_\text{i}) = f_{d^э}(t_i) - f_{d^p}(t_i) = \sum_{m=m_{o1}}^{m_{ol}} \sum_{p=p_{o1}}^{p_{oz}} \sum_{k=0}^{N/2^m} d^э{}_{m,p,k} \psi_{m,p,k}(t_i) - \sum_{m=m_{o1}}^{m_{ol}} \sum_{p=p_{o1}}^{p_{oz}} \sum_{k=0}^{N/2^m} d^p{}_{m,p,k} \psi_{m,p,k}(t_i). \qquad (6)$$

Таким образом, использование ВПП позволяет повысить адекватность описания модели сетевого трафика (6) за счет устранения влияния флуктуаций. Однако предложенная модель не обеспечивает управление базой правил МСЭ в режиме реального времени в силу необходимости пересчета нормального состояния трафика сети $f_{d^э}(t)$ на каждом интервале мониторинга сети.

Предложено прогнозировать величину $f_{d^э}(t)$ на s шагов вперед, используя модель динамической системы, на выходе которой генерируются стохастические процессы в зависимости от вектора детализирующих вейвлет-коэффициентов $\text{D}^э(t) = \{\text{d}^э{}_{m,p,k}\}$, зашумленного некоторым неконтролируемым шумом $\varepsilon_\phi(t)$. Из множества структур моделей данного вида для рассматриваемой совокупности наблюдений выбран класс ARIMAX-моделей линейной разностной динамической системы. Исследования показали, что из известных представителей класса ARIMAX-моделей наиболее приемлемым для обработки характеристик сетевого трафика является ARX-модель.

Выведено математическое описание предсказателя ARX-модели случайной составляющей сетевого трафика $\tilde{f}_{d^э}(t+s)$ с регрессором в форме вейвлет-коэффициентов вида

$$\tilde{f}_{d^э}(t+s) = \sum_{i=1}^{r} a_i f_{\text{d}^э}(t-i) + \sum_{i=1}^{q} b_i D^э(t-i), \qquad (7)$$

где a_i и b_i – параметры модели;

$f_{d^э}(t-i)$ – случайная составляющая вейвлет-пакетной модели (5), определяющая предыдущее значения выхода (образцы);

$D^э(t)=\{d^э_{m,p,k}\}$, $m=m_{o1},...m_{ol}$; $p=p_{o1},...p_{oz}$; $k=0..(N+1)/2^m$ – вектор вейвлет-коэффициентов (регрессор);

r, q – глубина «истории» прогноза.

Тогда прогнозируемый уровень отклонения от нормального состояния трафика $\tilde{\varepsilon}_a(t_i)$ устанавливает зависимость состояния трафика в момент времени t от предыдущих состояний в моменты времени t-1, t-2, …, t-r:

$$\tilde{\varepsilon}_a(t)=\tilde{f}_{d^э}(t)-f_{d^р}(t), \qquad (8)$$

где $\tilde{f}_{d^э}(t)$, $f_{d^р}(t)$ – модельное и текущее значения случайной составляющей сетевого трафика.

Значения параметров $\{a_i,b_i\}$ определяются из условия минимума ошибки прогноза по методу наименьших квадратов, что делает возможным экспериментальное определение величин r и q, равные соответственно 7 и 8.

Таким образом, ARX-модель (7) прогнозирует текущие значения случайной составляющей $f_{d^э}(t)$ трафика сети на величину глубины прогноза s, тем самым, повышая оперативность принятия решения при выявлении сетевых аномалий, не требуя постоянного пересчета эталонных значений.

В основу построения СППР СОА (см. рисунок 1) положены модели (5) и (7), используемые в двух режимах: обучение и анализ. В режиме обучения проводится моделирование эталонного состояния трафика сети. Технология обучения представлена на рисунке 5.

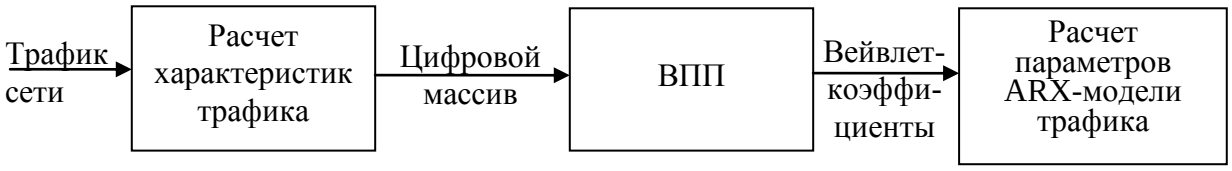

Рисунок 5 – Технология обучения СППР

СППР собирает информацию о трафике, воспринимая его как эталонный режим работы сети. При этом СППР на основе пакетов, прошедших через средство разграничения доступа, фиксирует отсчеты характеристик трафика и запоминает их в базе данных.

Сначала в ходе вейвлет-разложения полученные цифровые массивы отсчётов, представляющие трафик сети, преобразуются в наборы коэффициентов с помощью алгоритма ВПП. Далее на основе полученных коэффициентов с помощью модели (7) прогнозируется эталонный уровень трафика $\tilde{f}_{d^э}(t)$. Входной вектор $D^э(t)$ модели формируется из высокочастотных коэффициентов $d^э_{m,p,k}$. Вектор предыдущих значений выхода $f_{d^э}(t)$ составляется из значений характеристик трафика, восстановленных из высокочастотных компонент. В режиме

анализа по реальным отсчётам трафика, рассчитывается $f_{d^p}(t)$ и текущий уровень отклонения от нормального поведения сетевого трафика по выражению (8).

Предложенная методика оценки уровня отклонения от нормального состояния сетевого трафика реализована в программной системе на основе реализации многопоточности для ускорения вычислений. Основные схемы алгоритмов программной системы представлены на рисунке 6.

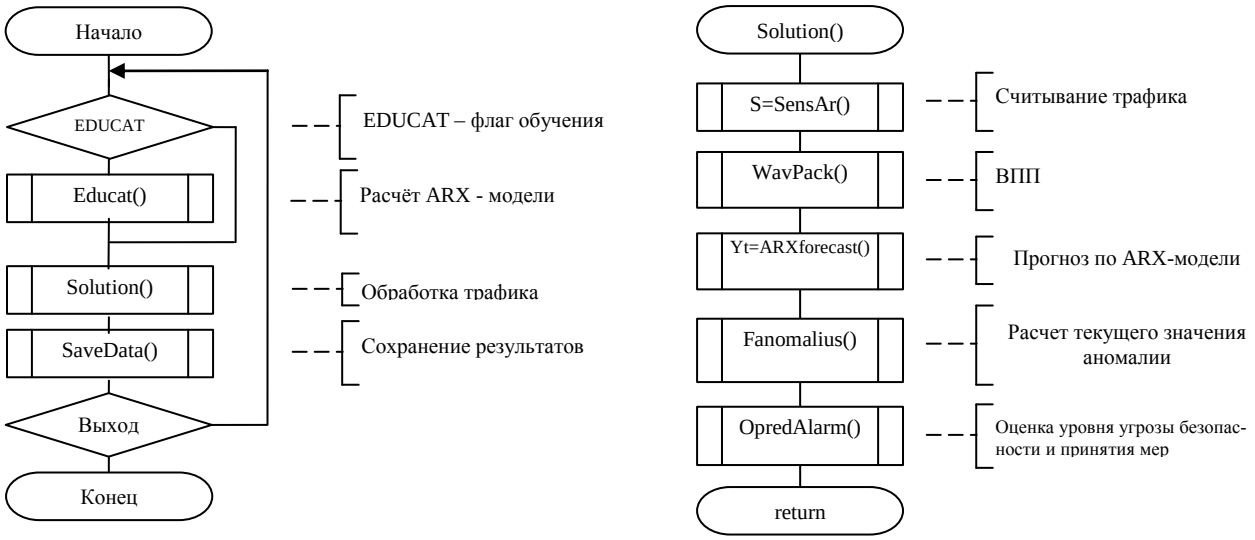

Рисунок 6 – Алгоритмы мониторинга ИП ККС и определения уровня аномальности

Таким образом, метод вейвлет–преобразований с использованием анализа высокочастотных составляющих трафика сети на основе вейвлет-пакетов и авторегрессионной модели позволяет повысить адекватность описания состояния трафика ККС в условиях параметрической неопределенности ИП и обеспечить оперативность принятия решений при выявлении сетевых аномалий близкую к реальному масштабу времени.

Третий раздел посвящен разработке методики обоснования порогового уровня аномального состояния сетевого трафика. В основу обоснования положен метод статистических решений для задачи проверки двухальтернативной гипотезы: H_0 и H_1 выражают предположения об отсутствии или наличии аномалии на текущем уровне сетевого трафика $f_{d^p}(t)$.

Для того чтобы задача обнаружения аномалий обрела математическую содержательность введены показатели – вероятности ложной тревоги $p_{лт}$ и пропуска аномалии $p_{па}$, понимая под ложной тревогой факт решения $\hat{H}_1$ об обнаружении аномалии при условии, что в наблюдаемом $f_{d^p}(t)$ аномалия отсутствует, а под пропуском аномалии – принятие решения $\hat{H}_0$ о том, что аномалии в $f_{d^p}(t)$ нет при условии, что в действительности она имеет место.

С целью обоснования применимости методов проверки статистических гипотез на основе экспериментальных данных по критерию Пирсона доказана нормальность закона распределения случайных погрешностей определения состояния сетевого трафика. Отсюда выведены зависимости для расчета вероятностей $p_{па}$, $p_{лт}$:

$$p_{лт} = \frac{1}{\sqrt{2\pi}} \int_{z_n}^{\infty} \frac{1}{\sqrt{D(z)}} \exp(-\frac{z^2}{2D(z)}) dz = 1 - \Phi(h), \qquad (9)$$

$$p_{па} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z_n} \frac{1}{\sqrt{D(z)}} \exp(-\frac{(z-\bar{z})^2}{2D(z)}) dz = \Phi(h-q), \qquad (10)$$

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

$z = \int_0^T f_a(t_i)\varepsilon_a(t_i)dt$ – 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;

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

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

Пороговый уровень аномальности сетевого трафика z_n рассчитывается в соответствии с принятым критерием оптимальности. В СППР СОА использован критерий Неймана – Пирсона в форме задачи условной оптимизации целевой функции $p_{па}$ +μ (0,05 – $p_{лт}$) в следующей формулировке: минимизировать $p_{па}$ при ограничении на величину $p_{лт}$, т.е. найти нормированный порог h, и путем подстановки h в (10) определить минимальную величину $p_{па}$.

В основу решения задачи условной оптимизации положен метод нелинейного программирования с использованием теоремы Куна-Таккера. Для этого составлена функция Лагранжа с ограничением $0{,}05 - p_{лт} \geq 0$ вида:

$$L(h,\mu) = p_{па} + \mu(0{,}05 - p_{лт}) = \Phi(h-q) + \mu(\Phi(h) - 0{,}95), \qquad (11)$$

где μ – неопределенный множитель Лагранжа.

Расчеты показали, что пороговый уровень аномальности сетевого трафика пропорционален квадратному корню из дисперсии, т.е. $z_n = 1{,}644685\sqrt{D(z)}$, при этом обеспечивается минимум среднего риска принятия неверного решения.

Таким образом, предложенная методика и алгоритм обоснования динамического порога аномального поведения сетевого трафика являются развити-

ем методов распознавания теории статистических решений в задаче обнаружения аномалий трафика ККС.

В четвертом разделе разработан прототип системы выявления и блокирования аномалий и оценена эффективность его применения.

В качестве прототипа принята среда брандмауэра Cisco Secure Private Internet Exchange (PIX) Firewall. Совершенствованием прототипа в условиях параметрической неопределенности ИП является двухуровневый контур управления базой правил брандмауэра, представленный на рисунке 7.

Предложенный контур является развитием архитектуры межсетевого экранирования с поддержкой функции автоматического управления базой правил брандмауэра при обнаружении аномалий трафика ККС.

Разработана программная система СОА клиент-серверной архитектуры, включающая два программных средства: сенсор и программа выявлений аномалий «Анализатор Аномальности - 2». Оценка эффективности прототипа системы выявления и блокирования аномалий проведена на основе имитационного эксперимента реальной ККС дочерней структуры корпорации «ТНК-ВР» – ООО «ТБинформ» в г.Оренбурге (акт от 16.01.2011 г).

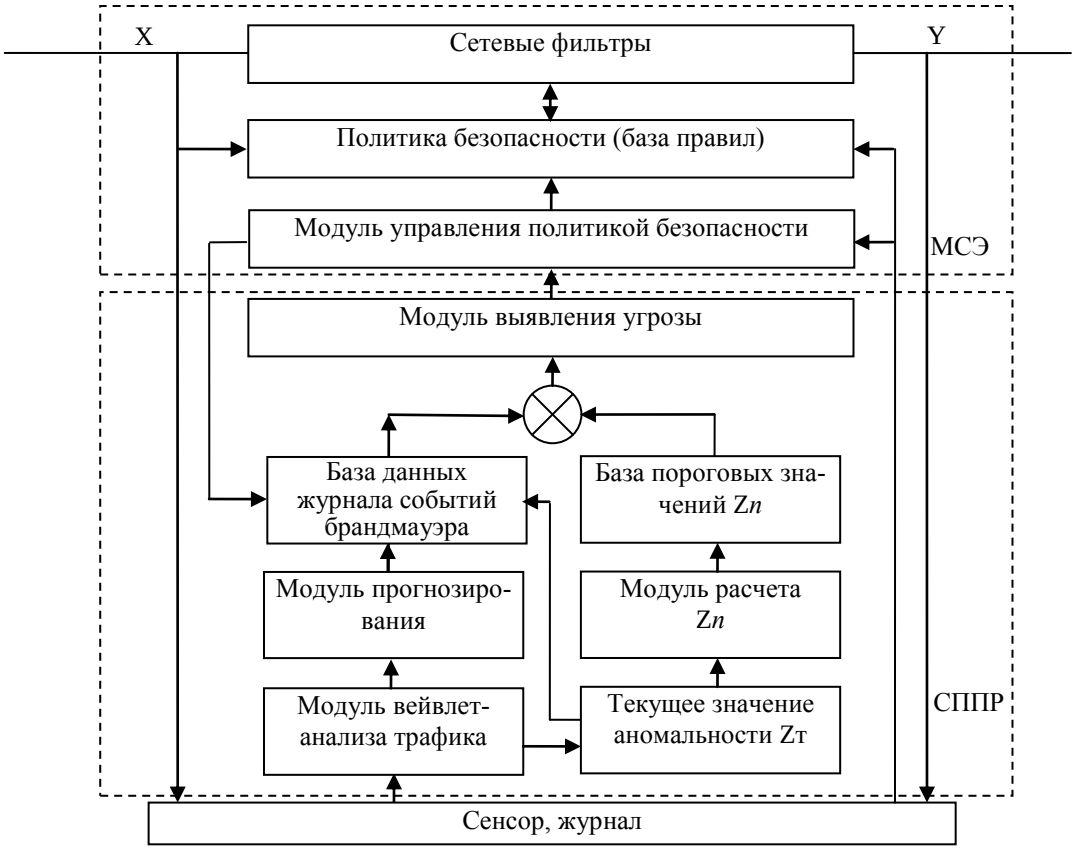

Рисунок 7 – Контур управления системы обнаружения аномалий

Результат работы программной системы в процессе проведения эксперимента представлен в виде экранной формы на рисунке 8.

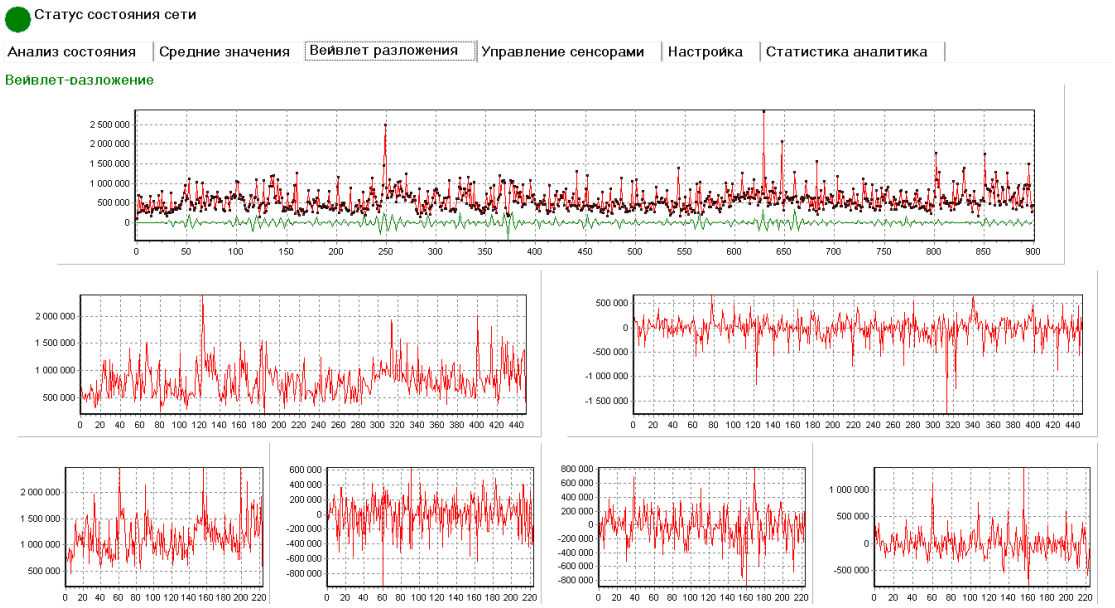

Рисунок 8 – Экранные формы системы обнаружения аномалий

Результаты эксперимента свидетельствуют, что с применением новой технологии принятия решений в СОА следует ожидать обеспечение вероятности обнаружения аномалий в ККС на уровне 0,78 – 0,88 при вероятности ложной тревоги – 0,05. По сравнению с известными IPS Sourcefire 3D® System и StopAttack разработанное средство обладает более высокими характеристиками: по быстродействию на 4 – 8%, по вероятности обнаружения аномалии – на 8 – 10% при допустимом уровне вероятности ложной тревоги 0,05. Этот факт подтверждает достижение цели исследования, целесообразность выбранного направления автоматизации мониторинга ИБ в условиях параметрической неопределенности ИП ККС и обоснования системы выявления и блокирования аномалий трафика ККС.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Результаты анализа современных технологий обнаружения и предотвращения вторжений свидетельствуют о низкой достоверности и оперативности выявления угроз ИБ ККС в условиях параметрической неопределённости ИП – нестационарности во времени, неоднородности в пространстве субъектов сети и неизвестных типах информационных воздействий.

2. Получил развитие метод выявления и блокирования аномалий трафика ККС на основе интеграции вейвлет – пакетной модели сетевого трафика и прогнозирующей авторегрессии её случайной составляющей.

3. Разработана методика обоснования порога аномального поведения трафика ККС по критерию Неймана - Пирсона в форме условной минимизации целевой функции с использованием теоремы Куна-Таккера, обеспечивающая

минимум среднего риска принятия решений при условии ограничения на вероятность ложной тревоги.

4. Разработан прототип системы выявления и блокирования аномалий трафика ККС на основе двухуровневого контура управления базой правил межсетевого экрана, прошедший государственную регистрацию в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам. Экспериментальное исследование эффективности системы свидетельствует, что применение новой технологии обеспечивает вероятность обнаружения аномалий на уровне 0,78 – 0,88 при вероятности ложной тревоги не более 0,05, при этом сравнительные характеристики оперативности разработанной системы выше на 4 – 8% по сравнению с известными аналогами систем обнаружения аномалий.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Тишина, Н.А. Методика принятия решений в системах обнаружения вторжений / Н.А. Соловьев, И.Г. Дворовой, Н.А. Тишина // Информация и безопасность / научно-практический журнал. – Воронеж, 2010. – №1. С.127–130.

2. Тишина, Н.А. Обнаружение вторжений на основе вейвлет-анализа сетевого трафика / Н.А. Тишина, Н.А. Соловьев, И.Г. Дворовой // Вестник УГАТУ / научно-практический журнал. – Уфа, 2010. – Т .14. №5(40). С. 188 –194.

3. Тишина, Н.А. Автоматизация администрирования безопасности электронного документооборота в условиях параметрической неопределенности информационных процессов / Н.А. Соловьев, И.Г. Дворовой, Н.А. Тишина // Информация и безопасность / научно-практический журнал. – Воронеж, 2010. – №1. С.115 – 118.

В других изданиях

4. Тишина, Н.А. Прогнозирование временных рядов как задача нейроматематики // Современные информационные технологии в науке, образовании и практике: Материалы VI всероссийской научно-практической конференция с международным участием / ОГУ. – Оренбург: Оренбургский государственный университет, 2007. С. 125 – 126.

5. Тишина, Н.А. Обоснование порога аномальной активности субъектов телекоммуникационной сети / Н.А. Тишина, Л.А. Юркевская, И.Г. Дворовой. Современные информационные технологии в науке, образовании и практике: Материалы VII всероссийской научно-практической конференция с международным участием / ОГУ. – Оренбург: Оренбургский государственный университет, 2008. С. 64 – 66.

6. Тишина, Н.А. Статистическое обоснование порогового уровня аномальной активности субъектов сети с использованием теоремы Куна-Таккера / Н.А. Тишина, Н.А. Соловьёв // Инновации в науке, бизнесе и образовании. Сборник материалов международной научно-практической конференции /

Оренбург, 2008. С.72 – 80.

7. Тишина, Н.А. Особенности задачи распознавания классов сетевых атак / Н.А. Тишина, Н.А. Соловьев // Современные информационные технологии в науке, образовании и практике: Материалы VIII всероссийской научно-практической конференции (с международным участием) / Оренбург: ИПК ГОУ ОГУ, 2009. С. 80 – 82.

8. Тишина, Н.А. Анализ процесса решения задачи распознавания классов сетевых атак / Н.А. Соловьев, Н.А. Тишина // Опыт использования и проблемы внедрения инноваций в науке, промышленности, энергетике и строительстве: Материалы научно-практической конференции. – Оренбург: ОГИМ, 2009. – С. 216 – 223.

9. Тишина, Н.А. Сканер безопасности сети на основе вейвлет-преобразования / Н.А. Соловьев, Н.А. Тишина, А.А. Липский, И.Г. Дворовой / Свидетельство о государственной регистрации программы для ЭВМ № 2010611858. – М.: Федеральная служба по интеллектуальной собственности, патентам и товарным знакам, 2010.

10. Тишина, Н.А. Моделирование сетевого трафика на основе вейвлет-преобразования и авторегрессионной модели // Современные информационные технологии в науке, образовании и практике: Материалы IX всероссийской научно-практической конференции (с международным участием). – Оренбург: ООО «Комус», 2010. С. 41 – 44.

11. Тишина, Н.А. Развитие теории кратномасштабного анализа для задачи обнаружения вторжений / Н.А. Тишина, Н.А. Соловьев // Теоретические вопросы разработки, внедрения и эксплуатации программных средств: Материалы Всероссийской научно-практической конференции. – Орск: Издательство ОГТИ, 2011. С. 143 – 148.

12. Тишина, Н.А. Система обнаружения аномалий корпоративной вычислительной сети / Н.А. Тишина, С.А. Огарков // Компьютерная интеграция производства и ИПИ-технологии (КИП – 2011): Сборник материалов V всероссийской научно-практической конференции – Оренбург: ИП Осиночкин Я.В., 2011. С. 557 – 561.

13. Тишина, Н.А. Развитие вейвлет-анализа для идентификации аномальной активности субъектов телекоммуникационной сети / Н.А. Соловьев, Н.А. Тишина // Вычислительная техника и новые информационные технологии: межвузовский научный сборник. Выпуск седьмой – Уфа: Уфимский государственный авиационный технический университет, 2011. С. 132 – 138.

14. Тишина, Н.А. Обнаружение аномалий в сети на основе вейвлет-пакетов и ARX- моделей //«IT-Security Conference for the Next Generation». – М.: ЗАО «Лаборатория Касперского», ФВМиК МГУ, 2011. С.27 – 28.

Диссертант Н.А.Тишина

ТИШИНА Наталья Александровна

СИСТЕМА ВЫЯВЛЕНИЯ И БЛОКИРОВАНИЯ АНОМАЛИЙ ТРАФИКА КОРПОРАТИВНЫХ СЕТЕЙ НА ОСНОВЕ ВЕЙВЛЕТ-ПАКЕТОВ

Специальность: 05.13.19
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук