**УДК 004.77**

# МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

**Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М.**

*ФГБУН «Институт программных систем им. А.К. Айламазяна» Российской академии наук, Исследовательский центр мультипроцессорных систем (152021, Ярославская обл., Переславский р-н, с. Веськово, ул. Петра I, д. 4а), e-mail: vmh48@mail.ru*

**Предложено методологическое обеспечение информационной защиты вычислительных систем, включающее последовательность разработки программно-инструментальных средств обнаружения и распознавания сетевых атак, логическую структуру интеллектуальной системы и концепцию многоуровневого анализа информативных признаков. Представленная методология обеспечит воспроизводимость полученных результатов другими исследователями, позволит создавать разнообразные образцы перспективных программно-инструментальных средств обнаружения и распознавания сетевых атак для обеспечения информационной защиты компьютерных систем. Подготовлен ряд рекомендаций по совершенствованию программно-инструментальных средств интеллектуального обнаружения и распознавания сетевых атак, нацеленных на системы облачных вычислений. Рассмотрены тенденции развития соответствующих технологических и программных средств, дана оценка мирового технического уровня в области сбора и представления информации о сетевых потоках, методов выявления аномальных отклонений в поведении сетей передачи данных.**

Ключевые слова: методологическое обеспечение, защита, логическая структура, рекомендации, тенденции.

# METHODOLOGICAL SUPPORT FOR NETWORK ATTACKS INTELLIGENT PROTECTION SYSTEMS

**Kondratyev A.A., Talalaev A.A., Tishchenko I.P., Fralenko V.P., Khachumov V.M.**

*Ailamazyan Program Systems Institute of the Russian Academy of Sciences, Research Center for Multiprocessor Systems (152021, Yaroslavl region, Pereslavl area, Peter I st., 4a), e-mail: vmh48@mail.ru*

**Proposed the methodological support for computer systems information protection, including network attacks detection and identifying software-instrumental tools development sequence, intellectual system logical structure and informative features multilevel analysis concept. The presented methodology will provide the reproducibility of the results obtained by other researchers, will allow to create a variety of samples of promising software-tools detect and identify network attacks to provide computer systems information security. A group of recommendations has arisen to improve the software-instrumental tools for aimed at cloud computing systems network attacks intelligent detection and identification. Considered the appropriate technology and software development trends, the world's technological level estimation of data networks abnormal deviations identifying methods and network flows collection and reporting is given.**

Keywords: methodological support, protection, logical structure, recommendations, trends.

## Введение

В современных условиях задачи проектирования и исследования информационных процессов и вычислительных систем решаются с учетом стандартизации и унификации, развития и применения соответствующих знаний и умений, позволяющих сокращать совокупные затраты на разработку, производство и эксплуатацию [11; 12; 15; 16; 20]. Решение этих проблем важно для всех отраслей народного хозяйства, но в первую очередь для оборонно-космической отрасли, где вопросы формирования методологических основ информационной защиты вычислительных систем и сетей чрезвычайно актуальны.

В настоящей статье приводятся основные результаты работы коллектива исследователей над созданием новых технологий защиты компьютерных сетей от постороннего

вмешательства. При этом большое внимание уделено вопросам методологии создания подобных систем на основе современных средств искусственного интеллекта. Проведенные экспериментальные исследования и сравнение полученных результатов с результатами патентного поиска показывают, что разработанные средства занимают достойное место в ряду имеющихся научно-технических решений. Выполнена систематизация процессов проектирования интеллектуальной защиты вычислительных систем и сетей (ВСиС) от сетевых атак в виде конкретной методологии.

**Понятие методологического обеспечения информационной защиты**

Методология обеспечения информационной защиты ВСиС рассматривает приложение теории, знаний и практики для эффективного построения алгоритмических и программных средств информационной защиты вычислительных систем, удовлетворяющих требованиям пользователей [11; 15; 20]. В рамках этой дисциплины изучается спектр процессов, ведущих к созданию систем обнаружения и распознавания сетевых атак: от разработки требований (через проектирование, разработку и методики испытания) до модернизации программных систем.

Методология – это учение об организации деятельности, которое включает совокупность приемов, методов, способов и принципов научно-технической деятельности, применяемой для получения результата и знаний [12; 16]. Можно выделить две основные крупные части методологии защиты ВСиС.

1. Процесс разработки алгоритмического и программного обеспечения системы информационной защиты. Эта научно-исследовательская часть работы посвящена процессу разработки систем обнаружения и распознавания сетевых атак. Рассматриваются различные модели и подходы процесса разработки, изучаются основные фазы этого процесса: формирование требований, проектирование и испытание.
2. Управление проектом – деятельность, направленная на опытно-конструкторскую реализацию проекта с максимально возможной эффективностью при заданных ограничениях по времени, денежным средствам, а также качеству конечных результатов проекта. Разработка программного обеспечения требует знакомства с методами и инструментами управления проектами. Без четкого управления (т.е. методологии) разработка систем обнаружения и распознавания сетевых атак приводит к непроизводительным затратам времени и средств.

На сегодняшний день представляется возможным изложить процесс разработки методологии защиты ВСиС в виде упорядочения ее в целостную систему с четко определенными характеристиками. Цикл деятельности по разработке системы защиты определяется тремя фазами:

– фаза проектирования, результатом которой являются итоги теоретических исследований и построенная модель (математическая, алгоритмическая) создаваемой системы, ее архитектура, принципы решения задач, методы и план практический реализации;

– технологическая фаза, результатом которой является программная и/или программно-аппаратная реализация алгоритмов и их предварительная отладка;

– рефлексивная фаза, результатом которой является проведение экспериментальных исследований, оценка реализованной системы и определение необходимости ее дальнейшей коррекции.

Рассмотрим основные вопросы методологии информационной защиты вычислительных систем программно-инструментальными средствами обнаружения и распознавания сетевых атак.

**Цели, задачи и состав нормативно-методологического обеспечения разрабатываемой системы защиты**

Разрабатываемая система должна работать надежно, для чего необходимо обобщать, формализовывать и использовать научный задел, накопленный в отрасли. Концентрированным выражением накопленного опыта являются стандарты. В состав нормативно-методологического обеспечения систем защиты входят стандарты и руководящие документы, методики, шаблоны проектных и программных документов [5; 16]. Нормативное обеспечение в части проектирования системы определяет классификацию программного обеспечения; требования к составу и связям информационных систем, порядку их формирования и развития; общие правила ведения работ; требования к сопровождению и эксплуатации. Целесообразно подробно рассматривать архитектуру интеллектуальной системы защиты; подлежащие регламентации этапы и процессы создания системы защиты; компоненты, относящиеся к общей архитектуре, протоколы связи модулей, интерфейсы; процессы создания, интеграции, сопровождения и дальнейшего развития.

На сегодняшний день существует множество разнообразных методологий процесса разработки программного обеспечения. Применительно к разработке системы защиты предлагаемая методология соответствует общепринятым схемам проектирования «сверху вниз» и «снизу вверх» и включает следующие этапы:

1) изучение состояния вопроса по открытым научно-техническим источникам и патентам, постановка задач;

2) анализ возможных архитектурных решений и предварительное сравнение их моделей (архитектура на основе системы защиты Snort и альтернативная архитектура);

3) выбор, изучение и проверка качества распознавания базы знаний с прецедентами сетевых атак по выделенным признакам (база KDD-99, генераторы типовых атак);

4) доработка базы знаний за счет расширения признакового пространства, усиливающего возможности распознавания (увеличение с 48 до 55 признаков);

5) выбор системы интеллектуальных инструментальных средств для анализа сетевого трафика (метрики, алгоритмы) и методов обучения для обнаружения и распознавания (распознающие автоматы, нейронные сети, метод опорных векторов, статистический анализ (методы ADD DEL));

6) выбор двухуровневой модульной архитектуры обнаружения и защиты (первый уровень – сигнатурный анализ на основе распознающих автоматов, второй уровень – распознавание типа атаки);

7) уточнение состава признаков для двух уровней защиты путем исследования информационной значимости, ранжирования и отбора;

8) программная реализация основных алгоритмов (модулей) инструментальных средств и решение задач анализа трафика в реальном времени;

9) уточнение и доработка комплекса модулей для обеспечения требуемого качества;

10) разработка программы и методик испытаний системы;

11) проведение внутренних испытаний, проверка качества на основе экспериментальных исследований (оценка точности и полноты распознавания) и возврат при необходимости к пункту (4);

12) организация документирования программного обеспечения.

По завершении проектирования система обнаружения и распознавания сетевых атак подвергается приемочным испытаниям, в процессе которых выясняется действительное соответствие выполненной работы техническим требованиям.

**Логическая структура системы защиты**

Основной задачей построения экспериментального образца интеллектуальной программной системы (ЭО ИПС) является обнаружение сетевых атак на системы облачных вычислений, а именно мониторинг трафика сети по протоколам HTTP, SNMP, TCP/IP; выделение информативных признаков на основе трафика и состояния защищаемой системы; принятие решения о наличии атаки или вторжения на основе полученных информативных признаков с использованием методов искусственного интеллекта; предотвращение развития вторжения с использованием управления межсетевым экраном; контроль безопасности собственной работы, в том числе парольное ограничение доступа; обеспечение централизованного управления при помощи графического интерфейса; визуализация обнаруженных атак и вторжений посредством графического интерфейса.

На начальном этапе в соответствии с методологией было предложено использовать открытую систему IDS Snort, на базе которой в дальнейшем была построена и прошла

тестирование первая версия экспериментальной системы защиты от сетевых атак [4; 18]. Система, архитектура которой представлена на рис. 1, предназначалась для защиты от атак типа DDoS и Probe (сканирование портов с помощью программы nmap).

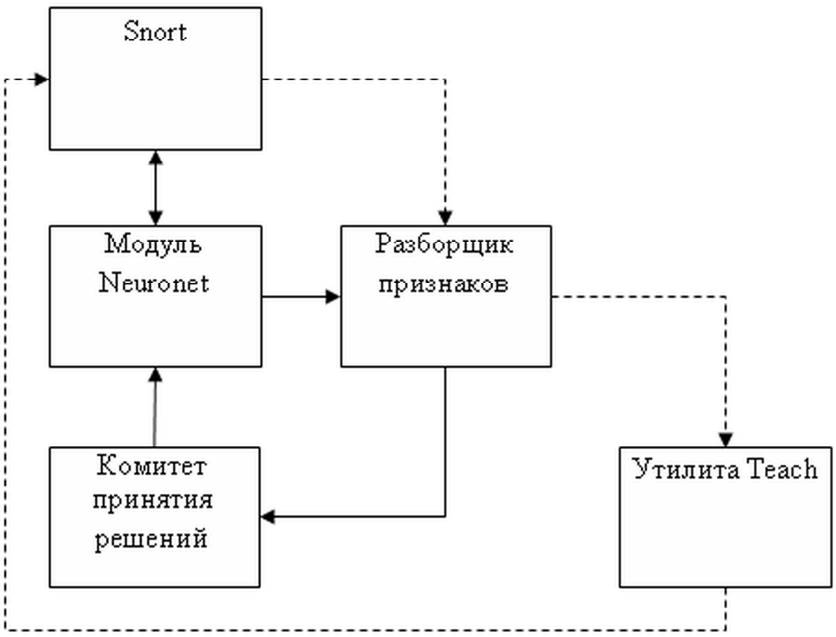


Рис. 1. Общая структура программного комплекса на базе IDS Snort

Преимущество IDS Snort в ее модульности: возможно подключение сразу нескольких независимых модулей обеспечения сетевой защиты. Каждый из них может работать по своему алгоритму. Защита обеспечивается комитетом принятия решений, интегрированным в отдельный программный модуль Neuronet: искусственная нейронная сеть прямого распространения, обучаемая по методу обратного распространения ошибки; классификатор сетевых пакетов на основе расстояния Евклида-Махаланобиса; классификатор на основе метода опорных векторов; статистический профилировщик. Перечисленные классификаторы обучаются с помощью утилиты Teach на основе извлеченных разборщиком признаков.

В результате последующей итерации на основе полученных результатов техническое решение было пересмотрено по ряду соображений, среди которых назовем разобщенность программных модулей: отдельные модули ничего не знают друг о друге, из-за чего не обеспечивается совместное принятие решений. Из других недостатков варианта, базирующегося на IDS Snort, назовем: отсутствие графического интерфейса администратора; отсутствие возможности работы с распределенными системами; отсутствие трекинга (отслеживания) ICMP-пакетов.

На рис. 2 представлен новый вариант экспериментального образца интеллектуальной программной системы (ЭО ИПС).

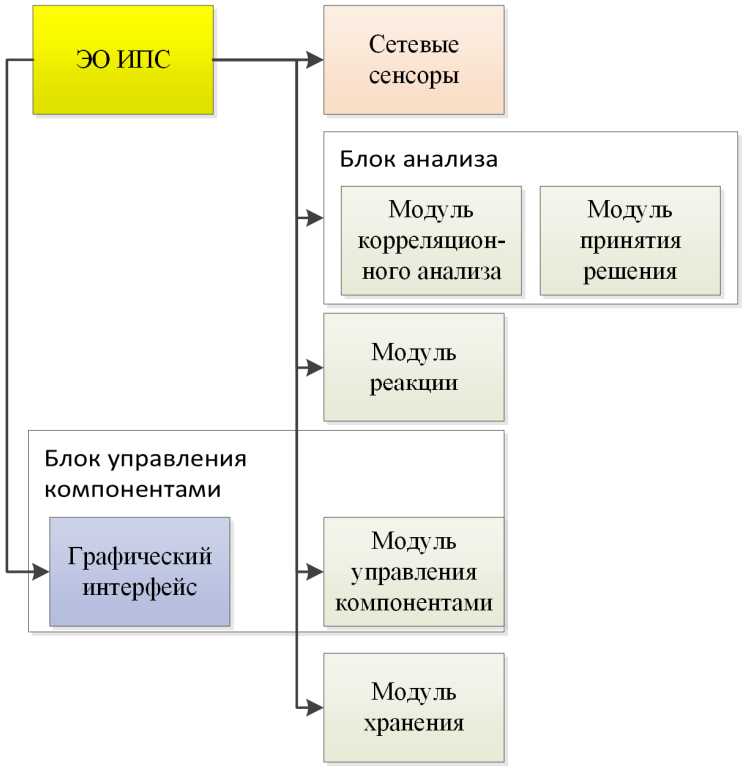


Рис. 2. Архитектура программно-инструментальных средств

Работа системы осуществляется по следующей схеме.

1. Сетевые сенсоры производят захват пакетов из сети, получая при этом некоторые признаки. Далее эти признаки передаются в модуль управления компонентами.
2. Модуль управления компонентами производит контроль всех модулей системы. При поступлении новых признаков сетевых пакетов от сетевых сенсоров данные передаются модулю анализа. Также при необходимости осуществляется запись признаков сетевых пакетов в БД.
3. Модуль корреляционного анализа производит анализ сетевых признаков на значимость, а также анализирует результаты, полученные модулями принятия решения на разных узлах распределенной системы облачных вычислений.
4. Модуль принятия решения определяет принадлежность пакета к обычному сетевому трафику либо к вредоносному трафику.
5. В случае определения факта атаки модуль реакции осуществляет действия сдерживающего характера.
6. Модуль хранения данных осуществляет как хранение настроек системы, так и хранение поступающих признаков сетевых атак.

Описанное взаимодействие модулей затрагивает только работу одного узла вычислительной системы. В действительности экземпляры ЭО ИПС должны располагаться в системе так, чтобы учитывать распределенность облачных вычислений [7].

В новом варианте программного комплекса (ПК) используется та же библиотека LibPcap, что и в IDS Snort. Обеспечивается защита как распределенных, так и централизованных информационных систем комитетом из следующих классификаторов: искусственная нейронная сеть прямого распространения, обучаемая по алгоритму Левенберга-Марквардта; метод опорных векторов; автоматный классификатор сетевых пакетов.

В отличие от варианта с использованием IDS Snort, поддерживается трекинг ICMP-пакетов. Дополнительно в новом варианте ПК применяется алгоритм ранжирования признаков по информативности, обеспечивающий повышение скоростных показателей обработки сетевого трафика. Разработан кросс-платформенный интерфейс администратора, позволяющий осуществлять управление всеми компонентами защиты, в том числе и синхронизацию баз данных. Программный комплекс обеспечивает защиту от атак типа DDoS, Probe (сканирование портов с помощью программы nmap и сбор информации об SNMP-устройствах в сети) и HTTP-эксплойтов. Недостатком текущих реализаций программных комплексов является плохая проработанность механизмов управления комитетом классификаторов, то есть отсутствие свободы выбора набора классификаторов.

В системах защиты, связанных с облачными вычислениями, можно выделить два основных направления:

– технологии защиты, использующие в своей основе архитектуру облачных вычислений и/или предоставляющие сервисы, функционирующие на основе облака;

– технологии, предназначенные для защиты облачных систем (платформ или сервисов).

Данные направления достаточно тесно связаны между собой, поскольку различия между атаками на облако и атаками на обычные системы незначительны и реальные системы могут сочетать в себе оба подхода. В настоящей работе особое внимание было уделено вопросам совершенствования систем защиты от DDoS-атак, приводящим к наиболее значимым потерям.

К основным теоретическим результатам исследования отнесены:

1) обобщение результатов автоматного подхода к описанию и моделированию сетевых атак на основе теории распознающих автоматов, теории взаимодействующих автоматов В.М. Глушкова, теории сетей Петри и автоматного подхода к описанию сетевых атак на облачные вычисления;

2) разработка на этой основе нового класса алгоритмов обнаружения сетевых атак с генетически конфигурируемыми конечными автоматами, которые характеризуются приемлемым временем, затрачиваемым на конфигурирование автоматов (на выборке из полумиллиона записей сетевой активности – порядка 10 часов или 1000 эпох обучения), отсутствием необходимости в экспертных знаниях, высокой скоростью обнаружения

сетевых атак, возможностью дообучения на выборках;

3) создание таблично-алгоритмического подхода к описанию и обнаружению сетевых атак и метода построения комитета классификаторов, учитывающих комплекс интеллектуальных методов, включая алгебраический подход к распознаванию Ю.И. Журавлева, метод опорных векторов, искусственные нейронные сети прямого распространения, обучаемые по методу Левенберга-Марквардта, метрику Евклида-Махаланобиса, корреляционный анализатор;

4) создание методики обнаружения и предотвращения сетевых атак на системы облачных вычислений, определяющей в том числе и выбор направления дальнейших исследований на основе двухуровневой системы; первый уровень, построенный на основе автоматной модели, служит для обнаружения и предупреждения атаки, реализуя сигнатурный подход к распознаванию, а второй проводит точное распознавание типа атаки на основе одновременного анализа всего множества выделяемых признаков.

**Оценка полноты и эффективности полученных результатов**

Выполненный комплекс исследований позволил достаточно качественно и полно решить основные задачи по защите от сетевых атак, что подтверждает таблица 1.

Таблица 1. Оценка полноты и эффективности полученных результатов

| № этапа | Техническое решение | Эффективность решения |
|---|---|---|
| 1 | Концепция построения системы обнаружения и распознавания сетевых атак для обеспечения информационной защиты вычислительных систем (в том числе кластерных установок). Программно-инструментальные средства обнаружения и распознавания сетевых атак | Построена и испытана архитектура с применением известного перехватчика и анализатора Snort и методов машинного обучения на основе выявления аномального поведения сети. Решения отличаются наличием интеллектуальных инструментов, обеспечивающих информационную безопасность компьютерных систем на основе знаний о структуре и характеристиках трафика |
| 2 | Альтернативное системе Snort программно-инструментальное средство обнаружения и распознавания сетевых атак. Математическое обеспечение для программных модулей и экспериментальный стенд для тестирования модулей системы в кластерных установках | Высокие эксплуатационные возможности интеллектуальной технологии и программных средств на их основе обеспечиваются:<br>1) уникальной модульной архитектурой;<br>2) двухуровневым механизмом обнаружения и распознавания сетевых атак;<br>3) статистическим и нейросетевым распознаванием сетевых атак, применением специальной метрики;<br>4) алгоритмами оценки и выделения информативных признаков сетевых атак по прецедентной информации |
| 3 | Методологическое обеспечение информационной защиты вычислительных систем программно-инструментальными средствами обнаружения и распознавания сетевых атак. Общая методика построения и тестирования экспериментального образца. Предложения по совершенствованию программно-инструментальных | Расширенные функциональные возможности подтверждены<br>1) эффективностью работы комитета модулей анализа на тестовых задачах;<br>2) комплексом мер по тестированию и отладке системы;<br>3) экспериментами по мониторингу и выявлению атак с определением реальных возможностей разработанных программных средств;<br>4) улучшением качества обнаружения и |

| № этапа | Техническое решение | Эффективность решения |
|---|---|---|
| | средств | распознавания атак по точности и полноте в целом на 12% по отношению к сигнатурным методам |

Можно отметить, что все рассмотренные методы обладают как достоинствами, так и недостатками. Несмотря на их некоторую алгоритмическую сложность, система способна распознавать как уже известные, так и новые виды атак. Это достигается за счет наличия двух этапов распознавания, на первом из которых определяется факт наличия или отсутствия атаки с использованием конечного автомата, обладающего высокой скоростью работы. Использование комитета классификаторов на втором этапе позволяет повысить точность выявления как известных, так и неизвестных видов сетевых атак.

По мнению некоторых экспертов, недостаточная проработка вопроса об организации защиты систем облачных вычислений является одним из основных факторов, тормозящих их внедрение [1-3; 19]. Наиболее известные технологии и платформы, связанные с концепцией облачных вычислений, описаны в работах [8; 9; 14; 27; 29; 30; 32].

Организация защиты облачных систем является комплексной задачей и должна включать в себя множество частных решений: контроль сетевого трафика, средства аутентификации и авторизации пользователей, предотвращение работы вредоносного программного обеспечения, защита данных пользователя и др. Следует отметить, что:

– ни одна из существующих систем защиты облачных вычислений не поддерживает указанные функции в полном объеме;

– разрабатываемая экспериментальная система близка по своим функциям к технологии TrippingPoint, однако не использует аппаратных решений, что может снизить затраты на внедрение подобных средств;

– системы защиты облачных сред должны поддерживать полный спектр функций, что может быть выполнено на этапе проведения опытно-конструкторских работ.

Рассмотрим вопрос о специфике систем информационной безопасности облачных систем по отношению к обычным вычислительным системам. Справедливо, что требования к уровню информационной безопасности при работе в облачной среде должны быть значительно выше, поскольку при работе с системами облачных вычислений появляются дополнительные риски, связанные с:

– территориальным расположением центра обработки данных (ЦОД) и имеющимся там уровнем мер безопасности, который не может контролироваться конечным пользователем;

– использованием дополнительного набора программных продуктов, обеспечивающих функционирование пользовательского программного обеспечения в облачной среде;

– использованием широких каналов связи с ЦОД;

– одновременной работой с множеством пользователей (в случае публичного облака).

Однако в случае использования облачной платформы часть ответственности за обеспечение безопасности (большая или меньшая, в зависимости от типа организации облачной среды) перекладывается на «провайдера услуг», притом что методики проведения атак и защиты от них, в целом, остаются неизменными. Таким образом, нельзя провести четкую грань между системами защиты облачных вычислений и системами защиты, предназначенными для защиты «обычных» систем.

**Международный опыт и имеющийся теоретический задел в области построения систем информационной защиты**

В соответствии с методологией должен быть учтен международный опыт и имеющийся теоретический задел в области построения систем информационной защиты. Среди зарубежных исследований следует выделить ряд патентов в области интеллектуальных методов выявления сетевых атак и предлагаемых решений.

*Экспертные системы*

В патенте [US Patent: 7574740] описывается система обнаружения вторжений, основанная на анализе каждого произошедшего в сети события с помощью экспертной системы (ЭС), использующей нечеткую логику. ЭС автоматически анализирует события и генерирует рейтинг опасности, который показывает, является ли событие или серия событий сетевой угрозой. ЭС может быть обучена на базе знаний для обнаружения новых атак без вмешательства человека. Рейтинг опасности определяется на основе множества факторов. Среди них: информация о типе события, сигнатура атаки, продолжительность атаки, история действий атакующего и др. Описана система обнаружения атак на компьютерную сеть и дана оценка уязвимости компонентов сети. Система обнаружения включает в себя сканирующий модуль, один или несколько сенсоров и консоль для работы внутри сети. Сенсор системы обнаружения атак может следить за сетевым окружением для поиска событий, связанных с сетевыми атаками. В ответ на обнаружение такого события сенсор может генерировать запрос на сканирование. Этот запрос инициирует сканирование целевого компьютера для определения уязвимости цели к атаке. Система обнаружения атак, основанная на анализе уязвимости, может оценивать серьезность данной атаки и инициировать сигнал тревоги, приоритет которой зависит от серьезности атаки.

*Искусственные нейронные сети*

В патенте [WO/2002/048959] описывается модуль обнаружения аномальных отклонений, основанный на иерархически упорядоченных нейронных сетях. Обнаружение происходит при помощи наблюдения за поведением определенных частей компьютерной сети. Выходные значения одного слоя нейронных сетей служат входами нейронных сетей

следующего уровня. Результирующее значение единственной нейронной сети последнего слоя представляет собой реакцию модуля на поведение компьютерной сети. Данный метод способствует уменьшению количества ложных атак, которые возможны при функционировании подобного анализатора.

Метод улучшения безопасности передачи информации в компьютерных сетях [Патент US Patent: 7,124,438] включает в себя средство сбора данных используемых соединений и средства обработки и анализа получаемой информации на предмет выявления аномальных отклонений. Для анализа получаемой информации используются нейронные сети, которые обучаются на собранных данных.

Метод [Патент US Patent: 7,181,768] может использовать данные о функционировании отдельно взятого компьютера, входящего в сеть, т.е. данные о работе программного обеспечения. Он основан на выявлении аномального поведения приложений. Программное обеспечение, подвергшееся атаке, начинает вести себя нетипично, в его поведении возникают аномальные отклонения. Для опознавания аномального поведения используется нейронная сеть, которая обучается как на примерах типичного поведения, так и на примерах нетипичного поведения.

Метод [Патент WO/2001/031421] обнаружения сетевых вторжений основывается на выделении некоторого множества характерных для обрабатываемой компьютерной сети черт и последующем анализе наблюдаемых отклонений выбранных характерных черт при помощи нейронных сетей.

Для выявления злоупотреблений в работе [31] сравнивается текущая деятельность с ожидаемыми действиями злоумышленника. Нейронная сеть в эксперименте обучалась более 23 часов, однако затем успешно распознала 98 и 97 процентов записей обучающей и тестовой выборок соответственно. Подтверждено, что нейронные сети потенциально способны классифицировать паттерны сетевой активности.

В работе [33] проводится исследование применимости нейронных сетей для обнаружения вторжений. Цель данной работы в определении нейронных сетей, способных как к бинарной классификации сетевых пакетов на классы «норма» / «атака», так и разделению нескольких классов. Тестировались многослойный персептрон, обобщенные сети прямого распространения, сеть на основе радиальных базисных функций, самоорганизующиеся карты признаков и рециркуляционная нейросеть. Тестирование на базе KDD-99 показало превосходство обобщенных сетей прямого распространения и радиальных базисных функций в многоклассовом случае. В случае с классами «норма» / «атака» хорошо себя показала рециркуляционная нейросеть.

*Корреляционный анализ*

При корреляционном анализе информации о различных сетевых потоках возникает задача организации процесса распределенного сбора данных. В патенте [US Patent: 6,606,316] авторы предлагают следующий подход к реализации этого процесса: управляющая программа на основании заданного описания передает сетевым агентам, установленным на различных узлах компьютерной сети, инструкции по способу сбора сетевых данных и вычисления необходимых статистических показателей.

Одним из возможных способов уменьшения количества ложных тревог, выдаваемых автоматическими средствами выявления аномальных отклонений, является проведение корреляционного анализа данных, поступающих от различных источников. В патенте [US Patent: 7,234,166] авторы предлагают объединять взаимосвязанные события в последовательности. Основная идея предлагаемого метода заключается в том, что появление определенных последовательностей событий позволяет выявлять аномальные отклонения в сетевых потоках данных с большей степенью уверенности, нежели появление отдельных событий, составляющих эти последовательности.

В патенте [WO/2007/058952] авторы предлагают проводить корреляционный анализ данных с учетом конфигурации компьютерной сети. В качестве параметров конфигурации, которые могут быть использованы для улучшения качества работы системы обнаружения аномальных отклонений, авторы предлагают использовать информацию об IP- и MAC-адресах, версиях установленного программного обеспечения. Использование такого рода информации позволяет уменьшить как вероятность пропуска аномального трафика, так и количество ложных тревог, выдаваемых системой. Помимо того, предложенный метод позволяет оценить вероятность успешного проведения атаки.

*Сигнатурный анализ*

Подход, предложенный в патенте [US Patent: 7,237,264], основан на нескольких решениях. Во-первых, при анализе сетевых потоков данных предлагается учитывать системные значения переменных, связанные с используемыми протоколами передачи данных, что позволяет более качественно отслеживать появление аномального сетевого трафика. Во-вторых, сигнатурный анализ сетевых пакетов предлагается производить с учетом контекста. Например, одна и та же строка, встреченная в заголовке http-пакета и в электронном письме, может иметь различное значение для системы выявления аномальных отклонений. В-третьих, один и тот же сетевой трафик может быть как нормальным, так и аномальным в зависимости от установленного на компьютерах программного обеспечения. Помимо того, для выявления аномальных отклонений сетевых потоков предлагается учитывать реакцию узла-адресата на приходящие сетевые пакеты.

*Продукции*

Пример системы, основанной на правилах, содержится в патенте [US Patent: 7,587,759]. Патент описывает защиту от вторжений с использованием базы продукционных правил, сопоставляемых с активными сетевыми приложениями. Эти правила составляют подмножество сигнатур известных атак и существующих эвристических правил, которое гибко меняется, как и характер сетевых взаимодействий. Метод включает определение списка активных сетевых приложений, динамическую систему правил обнаружения вторжений, механизмы оценки сетевого трафика и его блокировки. Обеспечивается включение или выключение защиты при изменении характера сетевых обменов приложений. Предотвращение вторжений основано на правилах, соответствующих активным сетевым приложениям, выполняющимся на компьютере.

*Метод динамических порогов*

В патенте [WO/2007/019349] рассматривается задача автоматической адаптации системы обнаружения аномальных отклонений в условиях динамически изменяющейся сетевой среды. В качестве возможного решения предлагается использовать динамически изменяющиеся пороговые значения в реализуемых методах обнаружения аномальных отклонений.

В патенте [US Patent: 7,185,368] авторы предлагают разделять множество сетевых пакетов в соответствии с сетевыми потоками данных, к которым они относятся. Для каждого сетевого потока насчитывается статистика, на основании которой можно судить о наличии аномальных отклонений. В качестве развития этой идеи предлагается для каждого узла компьютерной сети вычислять суммарную подозрительность ассоциированных с ним сетевых потоков. При превышении некоторого порогового значения сетевая активность данного узла считается аномальной.

*Деревья решений и метод опорных векторов*

В работе [25] показаны два гибридных подхода к моделированию систем обнаружения вторжений (на основе деревьев решений и метода опорных векторов), объединенных в комитет классификаторов для максимизации точности и снижения вычислительной сложности алгоритма. Полученные результаты показывают, что предложенные гибридные системы обеспечивают создание более точных систем обнаружения вторжений. В работе [26] авторами предложен новый алгоритм с использованием деревьев решений, отличающий как атаку от нормального состояния сети, так и определяющий отдельные классы атак. Экспериментальные результаты, полученные на базе KDD-99, показывают, что предложенный алгоритм, регулирующий весовые коэффициенты на основе вероятностного подхода и разбиения обучающей выборки на подмножества до однозначной классификации, распознает до 98% процентов сетевых атак.

*Комбинированные методы*

В работе [Патент Patent US: 7721336] описаны системы и методы динамического обнаружения и предотвращения мошенничества и электронных вторжений в сеть с помощью встроенного набора интеллектуальных технологий. Предлагается система, включающая большое количество методов искусственного интеллекта для обеспечения высокого качества распознавания атак и устойчивости к ним. Базовое решение может состоять из трех компонент: распознавания и предотвращения электронного мошенничества, обучения и запросов. Программа получает на вход данные о совершаемой операции и транзакции и на основе полученных данных о сетевой активности пользователей делает вывод о том, является ли пользователь нарушителем. Модель состоит из множества подмоделей, вносящих вклад в общее решение, в том числе: многоагентные модели, нейронные сети, нечеткую логику, генетические алгоритмы и несколько других механизмов. Компонентная модель обучения состоит из интерфейса и программы подготовки каждой подмодели. В патенте подробно описаны механизмы подготовки моделей и данных для них. В изобретении содержатся методы, которые успешно обнаруживают и предотвращают акты электронного мошенничества и сетевые атаки. Они могут быть использованы в компьютерных сетях и системах облачных вычислений. Для обеспечения распределенной защиты современных сетей передачи данных в работе [21] применяется модель иммунной системы с деревом решений. Авторы отошли от парадигмы централизованной защиты и представили идею автономных систем защиты. В предложенной модели комбинируются подходы, основанные на знаниях и на анализе поведения. В работе [22] производится анализ уязвимостей иммунных систем обнаружения вторжений с использованием генетического эволюционного агента. Используется три типа анализаторов уязвимостей (генетический и два вида оптимизации), различающихся своими возможностями поиска атак. Параллельный генетический алгоритм обнаружения вторжений в компьютерные сети предложен в [23]. Одна из сложностей понимания нормального и аномального поведения в компьютерных сетях в том, что границы между ними не могут быть четко определены. Во многих системах, основанных на аномалиях, возникают сложности из-за генерации ложных тревог. Эта проблема решается авторами работы с помощью нечеткой логики с правилами, строящимися генетическим алгоритмом. Экспериментальные результаты показывают, что предложенный алгоритм позволяет получить набор нечетких правил, подходящий для построения надежной системы обнаружения вторжений.

Среди выполненных в России исследований выделяются в основном работы, использующие нейросетевые методы и решения выявления сетевых атак. В работе [13] для решения задачи обнаружения и предотвращения сетевых атак предлагается использовать

специальную бинарную нейронную сеть, которая обладает двумя важными свойствами: 1) она применима к решению задач, у которых входная информация имеет сложную многосвязную и даже фрактальную структуру; 2) метод обучения является прямой вычислительной процедурой и не сводится к поиску глобального экстремума какой-либо сложной нелинейной функции, что не накладывает никаких принципиальных ограничений на размерность задачи. К сожалению, в работе отсутствуют экспериментальные данные, что затрудняет сравнительный анализ. В работе [10] рассматривается аналогичный подход с той разницей, что была использована ИНС лишь одним выходным нейроном. В рассматриваемой модели выходное значение «0» указывает на отсутствие, а «1» – на наличие атаки. Результаты моделирования свидетельствуют о перспективности рассматриваемого подхода, но для функционирования сети в качестве эффективной системы обнаружения атак необходимо решить ряд важных задач. В частности, реальная система должна извлекать исходные данные из сетевого потока. В работе [17] рассматривается абстрактная математическая модель DDoS-атаки (Distributed denial-of-service) типа SYN Flood и предлагается способ ее обнаружения на ранней стадии с использованием математического аппарата нечетких нейронных сетей. Для решения задачи анализа был использован аппарат нечеткой логики и нейронных сетей. Для формализации знаний экспертов о DDoS-атаке было создано пять лингвистических переменных, каждая из которых характеризует одну из компонент вектора параметров. Программа с обученным классификатором показала хорошие возможности по обнаружению SYN Flood-атаки.

Из сравнительного анализа с другими методами можно сделать вывод, что:

– нейронные сети превосходят алгоритмы, основанные на генетическом обучении, последние обучаются значительно дольше и их сходимость не гарантируется, что осложняет внесение в базу знаний новых классов сетевых атак;

– по своим качествам к нейронным сетям близки алгоритмы на основе метода опорных векторов, однако и они не свободны от недостатков, так как на результаты их работы напрямую влияет выбор функции ядра и другие настройки, кроме того, метод слишком чувствителен к зашумленности анализируемых данных;

– быстрота процесса обучения, простая и понятная классификационная модель, способность к формализации знаний – преимущества деревьев решений; в то же время существует проблема повторений некоторых частей дерева, возможны проблемы с интерпретацией полученных правил.

**Предложения по повышению эффективности интеллектуальных средств**

Для выявления аномальной сетевой активности предложено два уровня классификации. На первом уровне находится классификатор на основе генетически обучаемого конечного

автомата, разделяющего сетевые записи на два класса: «норму» и «подозрение на атаку». На втором уровне: сетевые записи, отнесенные ко второму классу, далее обрабатываются комитетом классификаторов на основе метода опорных векторов [24] и нейронной сети прямого распространения, обучаемой по методу Левенберга-Марквардта [28].

При построении классификаторов применяются методы интеллектуального анализа данных [6]. Каждый классификатор обучается распознавать не только «норму», но и классы атак. В качестве преимуществ относительно других методов и подходов можно выделить выявление неизвестных ранее и модифицированных видов атак; отсутствие необходимости в ведении базы сигнатур; дообучение классификаторов в режиме реального времени; низкий процент ложных срабатываний за счет комитета классификаторов. В таблице 2 приведено сравнение рассмотренных выше методов с предлагаемым решением.

Таблица 2. Сравнение интеллектуальных методов выявления сетевых атак

| Характеристика / Метод | Возможность выявления известных атак | Возможность выявления новых атак | Расширяемость | Простота настройки |
|---|---|---|---|---|
| Экспертные системы | ± | ± | ± | – |
| Искусственные нейронные сети | + | ± | + | – |
| Корреляционный анализ | ± | ± | + | + |
| Сигнатурный анализ | + | – | + | + |
| Продукции | + | ± | + | – |
| Метод динамических порогов | ± | – | ± | + |
| Деревья решений и метод опорных векторов | + | ± | + | + |
| Предложенный метод | + | + | + | ± |

В целях совершенствования инструментальных средств защиты дополнительно предлагается расширить представительство различных интеллектуальных методов в комитете классификаторов для повышения точности и полноты обнаружения и распознавания сетевых атак. В частности:

– качественно улучшить разрабатываемое средство мониторинга и защиты можно за счет применения перспективных методов классификации, например метода релевантных векторов (Relevance Vector Machines, RVM); однако этап обучения RVM-классификатора весьма ресурсоемкий (сложность задачи – $O(n^3)$), что требует создания специального аппаратно-зависимого программного кода для ускорителей вычислений (Intel MIC, Nvidia Tesla и др.);

– улучшить характеристики предлагаемого решения за счет активной интеграции в систему защиты методов, применяемых в современных системах извлечения знаний, – для выявления особенностей и зависимостей в образах интернет-поведения доверенных и враждебных сетевых агентов; в качестве примера успешной работы с неструктурированными данными можно привести известную архитектуру UIMA (Unstructured Information Management

Architecture), позволяющую извлекать знания из неструктурированной информации, в том числе из текстов, аудио-, видеоматериалов и изображений (open source);

– выполнить интеграцию средств защиты на низком уровне – на уровне драйверов или даже ядра операционной системы; это решение позволит существенно повысить скорость обработки за счет исключения множества промежуточных интерфейсных слоев.

**Заключение**

В статье представлены основы методологического обеспечения интеллектуальной программной системы защиты от сетевых атак. Наличие методологии обеспечивает воспроизводимость полученных результатов, позволяет создавать опытные образцы перспективных программно-инструментальных средств обнаружения и распознавания сетевых атак для обеспечения информационной защиты компьютерных систем (в том числе кластерных установок), подготавливает почву для перехода на новый уровень исследований в рамках ОКР.

Выполненные экспериментальные исследования в целом соответствуют общемировым стандартам проверки средств обеспечения сетевой безопасности, в том числе сформулированным Агентством передовых оборонных исследовательских проектов (DARPA, США). Экспериментально проверены и протестированы все заявленные программные модули как раздельно, так и в составе ЭО ИПС в целом.

Завершенные экспериментальные исследования по обнаружению и классификации сетевых атак позволили получить следующие основные характеристики:

– высокий уровень обнаружения атак на основе предложенных классификаторов (точность и полнота около 100%);

– возможность гибкой настройки автоматов (за счет генетических алгоритмов) и дообучения нейросетевых классификаторов с учетом новых сетевых атак;

– способность к распознаванию модифицированных сетевых атак и обнаружению закономерностей и аномалий в потоках данных.

Полученные результаты позволяют говорить о достаточно уверенном обнаружении сетевых атак (при проведении распознавания атак по нескольким классам) и достижении качества распознавания «атака» / «норма», близкого к 100% на тестовой выборке, что обеспечивается комитетом классификаторов (нулевое число ошибок первого и второго рода). Достигнутые характеристики показывают превосходство разработанного программного обеспечения над лучшими среди OpenSource-решений средствами сетевой защиты, а именно – IDS Snort и Bro. Построенная интеллектуальная система на основе аппарата нейронных сетей способна к обучению и адаптации к широкому кругу сетевых атак.

***Работа выполнена при финансовой поддержке Программы фундаментальных научных исследований ОНИТ РАН «Архитектурно-программные решения и обеспечение безопасности суперкомпьютерных информационно-вычислительных комплексов новых поколений», направление № 2 – «Обеспечение безопасности суперкомпьютерных информационно-вычислительных комплексов новых поколений», НИР «Обнаружение и предотвращение распределенных сетевых атак на высокопроизводительные системы облачных вычислений на основе отечественных аппаратно-программных комплексов семейства «СКИФ».***

## Список литературы

1. Акимов Е. ИКС: Защита в облаках — дело тонкое [Электронный ресурс]. - URL: http://www.iks-media.ru/articles/4214279.html (дата обращения: 07.04.2014).
2. Васильев В. Безопасность облачных сред [Электронный ресурс]. - URL: http://www.pcweek.ru/security/article/detail.php?ID=139185 (дата обращения: 07.04.2014).
3. Вестник российской ИТ-индустрии: Symantec создает новую систему безопасности для облаков [Электронный ресурс]. - URL: http://newsroll.pcmag.ru/go.php?nid=153387 (дата обращения: 07.04.2014).
4. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П., Фраленко В.П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения : электрон. научн. журн. — 2011. — № 3 (7). — С. 3-15 [Электронный ресурс]. - URL: http://psta.psiras.ru/read/psta2011_3_3-15.pdf (дата обращения: 07.04.2014).
5. Емельянова Ю.Г., Фраленко В.П. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения : электрон. научн. журн. — 2011. — № 4 (8). — С. 17-31 [Электронный ресурс]. - URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf (дата обращения: 07.04.2014).
6. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. — Новосибирск : ИМ СО РАН, 1999. — 270 с.
7. Кондратьев А.А., Тищенко И.П., Фраленко В.П. Разработка распределенной системы защиты облачных вычислений // Программные системы: теория и приложения : электрон. научн. журн. — 2011. — № 4 (8). — С. 61-70 [Электронный ресурс]. - URL: http://psta.psiras.ru/read/psta2011_4_61-70.pdf (дата обращения: 07.04.2014).
8. Крупин А. Облачные антивирусы — в теории и на практике. Часть 2 [Электронный ресурс]. - URL: http://www.3dnews.ru/software/cloud-ativiruses-2 (дата обращения: 07.04.2014).
9. Крупин А. «Облачный» антивирус [Электронный ресурс]. - URL: http://www.computerra.ru/terralab/softerra/424961 (дата обращения: 07.04.2014).
10. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак // Доклады ТУСУРа. — 2008. — № 2 (18), часть 1. — С. 37-41.

11. Куликов С.Б. Основы философского анализа науки: методология, смысл и цель. — Томск : Изд-во Том. гос. пед. ун-та, 2005. — 184 с.
12. Кун Т. Логика и методология науки. Структура научных революций. - М. : Прогресс, 1977. — 146 с.
13. Магницкий Ю.Н. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем // Динамика неоднородных систем. — 2008. — С. 200-205.
14. Машевский Ю. Антивирусный прогноз погоды: облачно [Электронный ресурс]. - URL: http://www.comprice.ru/articles/detail.php?ID=438040 (дата обращения: 07.04.2014).
15. Овчинников В.Г. Методология проектирования автоматизированных информационных систем: основы системного подхода. - М. : Компания Спутник, 2005. — 84 с.
16. Позин Б. Стандарты и методологии в жизненном цикле программного обеспечения информационных систем // Директор информационной службы. — 2001. — № 10 [Электронный ресурс]. - URL: http://www.osp.ru/cio/2001/10/171950/ (дата обращения: 07.04.2014).
17. Слеповичев И.И., Ирматов П.В., Комарова М.С., Бежин А.А. Обнаружение DDoS-атак нечеткой нейронной сетью // Известия Саратовского университета. — 2009. — Т. 9, сер. Математика. Механика. Информатика, вып. 3. — С. 84-89.
18. Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. Разработка нейросетевого модуля мониторинга аномальной сетевой активности // Нейрокомпьютеры: разработка и применение. — 2011. — № 7. — С. 32-38.
19. Черняк Л. Безопасность: облако или болото? [Электронный ресурс]. - URL: http://www.osp.ru/os/2010/01/13000673/ (дата обращения: 07.04.2014).
20. Чешев В.В. Техническое знание как объект методологического анализа. — Томск : Изд-во Том. ун-та, 1981. — 186 с.
21. Abadeh M.S., Habibi J., Barzegar Z., Sergi M. A parallel genetic local search algorithm for intrusion detection in computer networks // Engineering Applications of Artificial Intelligence. - 2007. - № 20. - P. 1058-1069.
22. Кеннеди Дж. Нейросетевые технологии в диагностике аномальной сетевой активности / пер. с англ. А.В. Лукацкого // Безопасность информационных систем. — 1997. — № 3. — С. 25-29.
23. Cannady J. Artificial neural networks for misuse detection // In Proceedings of the 1998 National Information Systems Security Conference (NISSC’98). Arlington. 1998. P. 443-456.
24. Corinna C., Vapnik V. Machine Learning. 1995. vol. 20, num. 3. P. 273-297.

25. Dewan Md. F., Nouria H., Emna B., Mohammad Z.R., Chowdhury M.R. Attacks Classification in Adaptive Intrusion Detection using Decision Tree // In Proc. of the International Conference on Computer Science (ICCS 2010). Rio De Janeiro, Brazil. 2010. P. 86–90.
26. Gerry D., Douglas B., Haiyu H., John H. Vulnerability analysis of immunity-based intrusion detection systems using genetic and evolutionary hackers // Applied Soft Computing. 2007. № 7. P. 547-553.
27. Intel Cloud SSO [Электронный ресурс]. - URL: http://www.intelcloudsso.com/ (дата обращения: 07.04.2014).
28. Levenberg K. A Method for the Solution of Certain Problems in Least Squares // Quart. Appl. Math. 1944. vol. 2. P. 164-168.
29. McAfee Cloud Security [Электронный ресурс]. - URL: http://www.mcafee.com/ru/solutions/cloud-security/cloud-security.aspx (дата обращения: 07.04.2014).
30. Networking Network and Cloud Security [Электронный ресурс]. - URL: http://h17007.www1.hp.com/us/en/products/network-security/index.aspx (дата обращения: 07.04.2014).
31. Sandhya P., Ajith A., Crina G., Johnson T. Modeling intrusion detection system using hybrid intelligent systems // Journal of Network and Computer Applications. 2007. № 30. P. 114-132.
32. Semantec $O_3$ [Электронный ресурс]. - URL: http://www.symantec.com/theme.jsp?themeid=O3 (дата обращения: 07.04.2014).
33. Swimmer M. Using the danger model of immune systems for distributed defense in modern data networks // Computer Networks. 2007. № 51. P. 1315-1333.

**Рецензенты:**

Сачков Ю.Л., д.ф.-м.н., руководитель Исследовательского центра процессов управления ФГБУН «Институт программных систем им. А.К. Айламазяна» Российской академии наук, с. Веськово.

Знаменский С.В., д.ф.-м.н., зав. лабораторией Исследовательского центра системного анализа ФГБУН «Институт программных систем им. А.К. Айламазяна» Российской академии наук, с. Веськово.