На правах рукописи

Пелешенко Виктор Сергеевич

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ИНФОРМАЦИОННОГО ОБМЕНА В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ДЛЯ РЕАЛИЗАЦИИ СРЕДСТВ И МЕТОДА СЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность 05 13 19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Таганрог – 2007

Работа выполнена в Северо-Кавказском государственном техническом университете на кафедре "Защита информации"

НАУЧНЫЙ РУКОВОДИТЕЛЬ
Кандидат технических наук, доцент
Чипига Александр Федорович

ОФИЦИАЛЬНЫЕ ОППОНЕНТЫ
Доктор технических наук, профессор
Бабенко Людмила Климентьевна (Технологический институт Южного федерального университета в г Таганроге)

Кандидат технических наук, доцент
Рядков Сергей Алексеевич (Ставропольский военный институт связи ракетных войск в г Ставрополе)

ВЕДУЩАЯ ОРГАНИЗАЦИЯ
ФГУП НТЦ "Атлас", г Краснодар

Защита диссертации состоится «23» августа 2007 г в 14 20 на заседании диссертационного совета ДМ 212 208 25 при Южном федеральном университете, по адресу
347928, Ростовская область, г. Таганрог, пер Некрасовский, 44, ауд 412

Отзывы на автореферат просьба направлять по адресу 347928, Ростовская область, г Таганрог, пер Некрасовский, 44, Ученому секретарю диссертационного совета ДМ 212 208 25 Галуеву Г А

С диссертацией можно ознакомиться в зональной научной библиотеке Южного федерального университета, по адресу
344007, Ростовская область, г Ростов, ул Пушкинская, 148

Автореферат разослан «25» июля 2007 г

Ученый секретарь
диссертационного совета,
доктор технических наук,
профессор Галуев Г А

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационной работы обусловлена тем, что в настоящее время средства и методы обнаружения сетевых атак базируются, в основном, на аналитических методиках, позволяющих обнаруживать известные атаки Методология обнаружения сетевых атак, как система всех методов, которые применяются в области сетевой защиты информации, представляет собой достаточно разнородные описания как средств и методик, так и системы их применения в теории и на практике

Существенный вклад в развитие методологии обнаружения сетевых атак относительно применения нейросетей внесли такие ученые как Корнеев В В , Райх В В , Синица И Н , Финогенов Д В , Васютин С В , Лебедев С В , участвующие в работе проекта «Исследование методов обнаружения аномальной активности в распределенных компьютерных системах и разработка системы обнаружения компьютерных атак, сочетающей сигнатурный и интеллектуальный анализ данных» (ГРАНТ РФФИ 04-07-90010) Значительный вклад в работы по построению систем обнаружения атак, использующих нейросети, внесли Абрамов Е С «Разработка и исследование методов построения систем обнаружения атак», Дружинин Е Л , Самохин А М , Чернышев Ю А , работающие над созданием Системы Аудита Вычислительных Сетей, решающей вопросы управления, обеспечения качества функционирования и безопасности вычислительных ресурсов, James Cannady, осуществляющий работы по применению нейросетевых технологий в диагностике аномальной сетевой активности

Анализ публикации в открытой печати показал разрозненное использование методов обнаружения и предотвращения сетевых атак, не дающее желаемой эффективности применения средств и способов их выявления

Объектом диссертационных исследований являются статистические и сигнатурные методы, применяющиеся в средствах сетевого и хостового обнаружения и предотвращения сетевых атак

Предметом диссертационных исследований является разработка методики совместного обнаружения и предотвращения сетевых атак, базирующейся на математической модели информационного обмена между узлами в локальной вычислительной сети за счет применения известных и разработанных методик обнаружения враждебных воздействий

Целью диссертационной работы является повышение эффективности обнаружения вторжений в компьютерную сеть за счет разработки и реализации математической модели информационного обмена между узлами в локальной вычислительной сети и методики обнаружения сетевых атак

Научная задача состоит в разработке средств и методов защиты локальной вычислительной сети для повышения вероятности обнаружения сетевых атак

Для решения поставленной общей научной задачи проведена ее декомпозиция на ряд следующих **частных задач**

1 Разработка математической модели, на основе которой возможно рассмотрение обнаружения сетевых атак в формализованном представлении

2 Разработка способа обнаружения атак, совместно использующего статистический и сигнатурный методы обнаружения вторжений

3 Разработка устройства и программной системы для обнаружения известных и неизвестных ранее сетевых атак

4 Разработка методики обнаружения сетевых атак, повышающей процент обнаружения враждебных воздействий

5 Проведение сравнительного анализа выявления вторжений в компьютерную сеть с помощью разработанных средств обнаружения сетевых атак по отношению к известным

Методы исследования При решении поставленных в диссертационной работе задач использованы методы теории вероятностей и математической статистики, теории нейронных сетей, теории математического моделирования, теории информации, теории вычислительных систем и сетей

Научная значимость работы заключается в развитии теории информационной безопасности в области разработки и применения методик и моделей обнаружения существующих, в том числе неизвестных ранее сетевых атак

Научная новизна работы заключается в разработке новых средств и метода обнаружения сетевых атак, базирующихся на разработанной математической модели информационного обмена в локальной вычислительной сети и применении нейронных сетей прямого распространения, Кохонена, классификаторах Карпентера-Гроссберга и сигнатурного анализатора, сочетании сигнатурных и статистических методов, что в результате позволяет выявлять известные и неизвестные сетевые атаки и повысить процент обнаружения атак, не повышая процент ложных срабатываний

Практическая значимость

1 Разработанная математическая модель информационного обмена в локальной вычислительной сети может использоваться в науке и технике при разработке методик, способов, программных и аппаратных средств обнаружения и предотвращения сетевых атак Эта модель также может применяться при разработке и использовании систем сетевой защиты информации

2 Предложенный способ обнаружения сетевых атак сигнатурными и статистическими методами может применяться при разработке и усовершенствовании систем защиты информации

3 Предложенная методика тестирования и определения надежности программного средства обнаружения атак может применяться сотрудниками подразделений по защите информации для определения качества используемых или разрабатываемых средств сетевой защиты

Основные научные результаты, выносимые на защиту

1 Математическая модель информационного обмена между узлами в локальной вычислительной сети, позволяющая однозначно определить формализовано представленные параметры и характеристики сетевых пакетов, необходимые для обнаружения сетевых атак

2 Способ обнаружения вторжений, позволяющий определять как известные, так и неизвестные сетевые атаки, основанный на выявлении сетевых атак сигнатурными и статистическими методами

3 Устройство и программное средство обнаружения вторжений, позволяющие применять разработанный способ и математическую модель информационного обмена между узлами в локальной вычислительной сети для выявления сетевых атак

4 Методика обнаружения сетевых атак, использующая разработанные устроиство и программное средство, повышающая эффективность обнаружения вторжений в локальную вычислительную сеть

5 Результаты сравнительного анализа выявления вторжений в компьютерную сеть с помощью разработанных и известных средств обнаружения сетевых атак

Использование результатов. Разработанные модель, способ, методика, средства и результаты исследований используются в процессе разработки системы сетевой защиты финансового управления администрации Шпаковского муниципального района Ставропольского края и в учебный процесс кафедры защиты информации СевКавГТУ при изучении дисциплины «Теоретические основы компьютерной безопасности»

Достоверность и обоснованность полученных в диссертационной работе результатов обеспечивается строгостью математических выкладок, схожими результатами проводимых экспериментов в данной области, разработкой действующей программы, на которую получено свидетельство о регистрации программы для ЭВМ № 2007610367, разработанным устройством, на которое подана заявка на изобретение №2006137745/20(041073) Справедливость выводов относительно эффективности подтверждается строгостью методики оценки и практическими опытами

Апробация

Основные положения и результаты диссертационной работы докладывались и обсуждались на Международной конференции «Инфокоммуникационные технологии в науке, производстве и образовании» (Инфоком -2), Ставрополь, 2006, Международной научно-практической конференции «Информационные системы, технологии и модели управления производством», Ставрополь, 2005, Научно-технической конференции «Вузовская наука – Северо-Кавказскому региону», Ставрополь, 2005, Научно-практической конференции «Совершенствование методов управления социально-экономическими процессами и их правовое регулирование», Ставрополь, 2005, Научно-технической конференции «Вузовская наука – Северо-Кавказскому региону», Ставрополь, 2005, Международной научно-практической конференции «Информационная безопасность» Таганрог, 2006

Публикации

По теме диссертации опубликовано 5 научных статей и 5 тезисов докладов, 1 статья опубликована в журнале «Известия ТРТУ», входящем в перечень, рекомендованный ВАК РФ для публикации результатов докторских диссертационных работ

Объем и структура работы

Диссертация состоит из введения, четырех глав, заключения, списка литературы, включающего 80 наименований, приложений Основной текст диссертации изложен на 134 страницах, включая 31 рисунок и 14 таблиц

Основное содержание работы

Во введении обоснована актуальность исследований в области обнаружения и предотвращения сетевых атак, основанных на аппарате нейронных сетей и сигнатурного анализа, сформулированы цель работы, решаемые в ней задачи, определена практическая ценность и научная новизна выносимых на защиту результатов

В первой главе проводится обзор моделей обнаружения и предотвращения сетевых атак и показано, что модели делятся на два типа

1 Хостовая (host-based) модель обнаружения сетевых атак подразумевает анализ данных, получаемых и передаваемых в сеть, и анализ различных журналов регистрации, имеющихся на конкретном узле (хосте), путём применения соответствующих методик и алгоритмов В хостовой модели при обнаружении атак используются хостовые СОА К ним относят системы обнаружения атак (СОА) клиент-серверной архитектуры и архитектуры клиент-клиент

К достоинствам хостовых СОА относят то, что такие подсистемы более устойчивы к разрушению всей СОА в целом и их работа не зависит от сети передачи данных, т к , в отличие от архитектуры клиент-сервер, в таких системах все данные об атаках, сигнатурах и настройках хранятся на каждом элементе СОА Также к достоинствам архитектуры относится то, что такая СОА, а точнее ее сенсоры, не загружает вычислительную мощность узлов, т к нагрузка основной работы ложится на сервер СОА

2 Сетевая (network-based) модель обнаружения сетевых атак подразумевает анализ сетевого трафика непосредственно в сети, т е анализируются данные, взятые из технических каналов связи с использованием среды передачи данных и каналообразующего оборудования вычислительной сети, путём применения соответствующих методик и алгоритмов сетевого анализа данных Рассмотрены внутрисегментные и межсегментные СОА К достоинствам такой системы относится то, что в случае направленности атаки на узлы ЛВС она обнаруживается до ее осуществления, и узлы ЛВС не задействованы в обнаружении атак и при обнаружении атаки деструктивное действие, направленное на узлы ЛВС, блокируется на начальном этапе реализации сетевой атаки

Сигнатурный анализ и контроль профилей при обнаружении компьютерных атак включает в себя анализ заданных заранее последовательностей, как самих анализируемых данных, так и последовательностей действий Современные методики обнаружения сетевых

атак достаточно разнородны и не сведены к единому критерию, по которому возможно оценить эффективность их применения

В настоящее время разрабатываемые средства защиты используют возможные комбинации сигнатурных и статистических методов, сетевых и хостовых моделей, но в известных средствах одновременно перечисленные методики и модели не используются

Внутрисетевые средства защиты используют как сетевую, так и хостовую модели обнаружения атак, а средства сетевой защиты между ЛВС пропускают через себя весь трафик, проходящий между сегментами распределенной вычислительной сети

Под защищаемой информационной системой (ИС) понимается система, в которой используются персональные компьютеры (ПК), технические каналы связи, подразумевающие среду передачи данных и каналообразующего оборудования локальной вычислительной сети (ЛВС)

С точки зрения защищенности ИС рассматривают графовую модель системы защиты с полным перекрытием В зависимости от вида средств, методов и алгоритмов управления можно выделить ИС с централизованным и распределенным управлением При этом могут выполняться как жесткие, так и гибкие алгоритмы управления ИС, учитывающие многочисленные факторы Если сеть может быть соединена с другими, то она называется открытой, если не может или не должна, то – закрытой

Учитывая разнородность существующих методик обнаружения сетевых атак, для эффективного обнаружения необходимо также применять достоинства известных и апробированных теоретически и практически методов и моделей

Соответственно для эффективного обнаружения сетевых атак необходима методика, включающая в себя достоинства известных методик с применением сетевого и хостового сбора данных, сигнатурные и статистические методы выявления сетевых атак

Подводятся итоги и формулируются основные задачи на исследование

Во второй главе разработана и исследована математическая модель информационного обмена в локальной вычислительной сети и способ обнаружения сетевых атак

При анализе сетевых пакетов учитываются параметры и характеристики, которые дают полную картину о передаваемых пакетах с точки зрения стандартов протоколов и применяемых нейросетей

Анализ существующих методов функционирования модулей различных датчиков и примеры эксплуатации коммерческих и академических СОА показывают, что наибольшим потенциалом обладают те системы обнаружения атак, которые одновременно используют как хостовые, так и сетевые датчики

Перечень характеристик и параметров расширен и дополнен следующим образом

– протоколы Ethernet – PUP, XNS, IP, ARP, RARP, IPX, NOVL, SNTP, XIMTA, LOOP,

– MAC – адреса отправителя,

– MAC – адреса получателя,

– порты отправителя,

– порты получателя,

– протоколы IP – IP, ICMP, IGMP, TCP, UDP, ISO-IP,

– TCP флаги – FIN, SYN, RST, PSH, ACK, URG, ECH, CWR,

– типы ICMP пакета – ECHO-REPLY, DEST-UNREA, SRC_Q, REDIR, ECHO, TTLX, BADPAR, TIME, TIME REPLY, INFO, INFO-REPLY

Показаны множества входных данных для анализа и значения ошибок первого (ложные тервоги) и второго рода (пропуски атак)

Сетевой трафик ЛВС представлен на рисунке 1 в виде сообщений между узлами, где k –количество узлов в сети, S_{k1} - сообщение от U_k к U_1

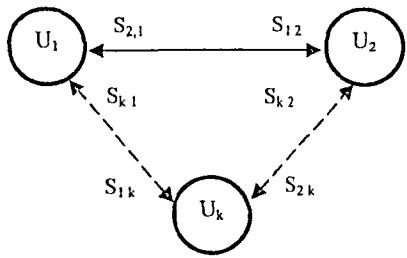


Рисунок 1 – Представление узлов и сообщений

Математическая модель информационного обмена в ЛВС описывается следующим образом

1) при отправке первого сообщения S_{21}^{1} от второго источника сообщений к первому, будет получено первое сообщение S_{12}^{1} от первого источника ко второму и т д, при последнем сеансе связи между первым и вторым источниками последнее сообщение от второго источника к первому будет $S_{21}^{n_{U_{21}}}$, а последним сообщением от первого источника ко второму будет $S_{12}^{n_{U_{12}}}$, где $n_{U_{k1}}$ номер сообщения от источника U_k к источнику U_1,

2) вероятность передачи второго сообщения после первого, и т д, n-го сообщения после n-1 -го - обозначается $P_{k1}^{n_{U_{k1}}}$

Информационный обмен между узлами в сети представляется в следующем виде

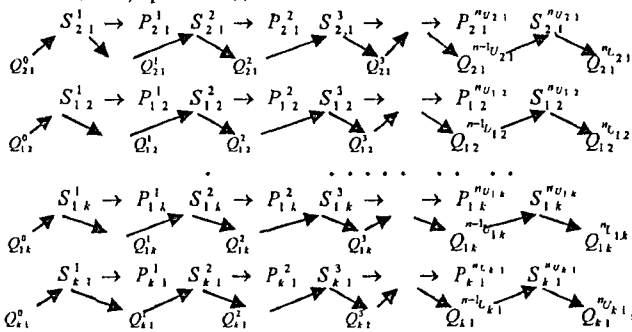
$$\begin{aligned} S_{1k} &= \{S_{1k}^{1}, S_{1k}^{2}, \ , S_{1k}^{n_{U_{1k}}}\} \\ S_{12} &= \{S_{12}^{1}, S_{12}^{2}, \ , S_{12}^{n_{U_{12}}}\} \\ &\\ S_{1k} &= \{S_{1k}^{1}, S_{1k}^{2}, \ , S_{1k}^{n_{U_{1k}}}\} \\ S_{k1} &= \{S_{k1}^{1}, S_{k1}^{2}, \ , S_{k1}^{n_{U_{k1}}}\} \end{aligned} \qquad (1)$$

Тогда вероятность передачи второго сообщения после первого, n-го сообщения после n-1 -го и т д, при штатном режиме работы ИС можно обозначить как P с индексами $n_{U_{21}}$ - n-е сообщение от 2-го источника к 1-му и соответственно $n_{U_{12}}$ - n-е сообщение от 1-го источника ко 2-му источнику сообщений

$$\begin{aligned} &S_{21}^{1} \to P_{21}^{1} \ \ S_{21}^{2} \to P_{21}^{2} \ \ S_{21}^{3} \to \ \ \to P_{21}^{n_{U_{21}}} \ \ S_{21}^{n_{U_{21}}} \\ &S_{12}^{1} \to P_{12}^{1} \ \ S_{12}^{2} \to P_{12}^{2} \ \ S_{12}^{3} \to \ \ \to P_{12}^{n_{U_{12}}} \ \ S_{12}^{n_{U_{12}}} \\ &S_{1k}^{1} \to P_{1k}^{1} \ \ S_{1k}^{2} \to P_{1k}^{2} \ \ S_{1k}^{3} \to \ \ \to P_{1k}^{n_{U_{1k}}} \ \ S_{1k}^{n_{U_{1k}}} \\ &S_{k1}^{1} \to P_{k1}^{1} \ \ S_{k1}^{2} \to P_{k1}^{2} \ \ S_{k1}^{3} \to \ \ \to P_{k1}^{n_{U_{k1}}} \ \ S_{k1}^{n_{U_{k1}}}, \end{aligned} \qquad (2)$$

где $P_{k1}^{n_{U_{k1}}}$ - вероятность приема сообщения $S_{k1}^{n_{U_{k1}}}$ с порядковым номером $n_{U_{k1}}$ после приема сообщения $S_{k1}^{n-1_{U_{k1}}}$ от k-го узла к первому

Модель информационного обмена в ЛВС, учитывающая состояния *узлов после* очередных сообщений, примет вид



(3)

где Q^0 - нулевые состояния узлов до начала работы, $Q^0 = 1$

В таблице 1 представлена классификация сообщений

Таблица 1 - Классификация сообщений

Принадлежность сообщений	Пояснение
допустимые или ожидаемые	при «чистом» трафике
не допустимые или сомнительные	при появлении пакетов с опасными или сомнительными данными
запрещенные или не ожидаемые	при передаче опасных запрещенных пакетов

В соответствии с классификацией сообщений справедливы неравенства

$$\begin{cases} 0 \le P < P_{\min}, \text{если сообщения не ожидаемые,} \\ P_{\min} \le P \le P_{\max}, \text{если сообщения сомнительные,} \\ P_{\max} < P \le 1, \text{если сообщения ожидаемые,} \end{cases} \quad (4)$$

где $P_{\min}$ и $P_{\max}$ - предельные допустимые вероятности, при которых вероятность приема сообщения от одного узла к другому может быть соответственно ожидаемой или нет

Состояния Q рассчитываются по формуле

$$Q = \begin{cases} 1, \textit{если } P_{\max} \le P(S) \le 1, \\ 0, \textit{если } 0 \le P(S) < P_{\max} \end{cases} \quad (5)$$

При всех $Q = 1$ все пакеты, ожидаемые и не представляют угрозы, а в случае присутствия хотя бы одного $Q = 0$ атака обнаружена Присутствие или отсутствие атаки просчитывается по формулам (6) и (7)

$$\prod_{i=1,n} Q_{21}^{t_{U_{21}}} = 1 \qquad \prod_{i=1,n} Q_{21}^{t_{U_{21}}} = 0$$

$$\prod_{i=1,n} Q_{12}^{t_{U_{12}}} = 1 \qquad \prod_{i=1,n} Q_{12}^{t_{U_{12}}} = 0$$

(6) (7)

$$\prod_{i=1,n} Q_{1k}^{t_{U_{1k}}} = 1 \qquad \prod_{i=1,n} Q_{1k}^{t_{U_{1k}}} = 0$$

$$\prod_{i=1,n} Q_{k1}^{t_{U_{k1}}} = 1 \qquad \prod_{i=1,n} Q_{k1}^{t_{U_{k1}}} = 0$$

При разработке модели обнаружения сетевых атак сигнатурными и статистическими методами предложена следующая формализация

1 Сетевой трафик представляется как совокупность сообщений S с помощью функции отображения $G\ (T,M) \to S$, где T и M - статистические и сигнатурные параметры сообщения,

2 Вероятность P приема сообщений

Матрица таких переходных вероятностей имеет вид

$$P = \begin{pmatrix} P_{2\,1}^{1} & P_{2\,1}^{2} & P_{2\,1}^{3} & \cdots & P_{2\,1}^{n_{2\,1}} \\ P_{1\,2}^{1} & P_{1\,2}^{2} & P_{1\,2}^{3} & \cdots & P_{2\,1}^{n_{1\,2}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ P_{1\,k}^{1} & P_{1\,k}^{2} & P_{1\,k}^{3} & \cdots & P_{1\,k}^{n_{1\,k}} \\ P_{k\,1}^{1} & P_{k\,1}^{2} & P_{k\,1}^{3} & \cdots & P_{k\,1}^{n_{k\,1}} \end{pmatrix} \qquad (8)$$

3 Состояния узлов ИС Q, обозначаемые как Q^0 - нулевые состояния узлов и $Q_{k\,1}^{n_{k\,1}}$ - состояния узлов после принятия сообщений с соответствующими индексами

Матрица состояний имеет вид

$$Q = \begin{pmatrix} Q_{2\,1}^{0} & Q_{2\,1}^{1} & Q_{2\,1}^{2} & \cdots & Q_{2\,1}^{n_{2\,1}} \\ Q_{1\,2}^{0} & Q_{1\,2}^{1} & Q_{1\,2}^{2} & \cdots & Q_{2\,1}^{n_{1\,2}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ Q_{1\,k}^{0} & Q_{1\,k}^{1} & Q_{1\,k}^{2} & \cdots & Q_{1\,k}^{n_{1\,k}} \\ Q_{k\,1}^{0} & Q_{k\,1}^{1} & Q_{k\,1}^{2} & \cdots & Q_{k\,1}^{n_{k\,1}} \end{pmatrix} \qquad (9)$$

4 Статистические показатели $T = \{T_1, T_2, \ldots, T_h\}$, выбор которых осуществляется в зависимости от протокола сетевого взаимодействия, где h - количество статистических показателей. К таким показателям при рассмотрении сетевого трафика в сетях стека протоколов TCP/IP относятся, например

- количество входящих IP-пакетов в единицу времени,
- количество исходящих IP-пакетов в единицу времени,
- количество входящих TCP-пакетов в единицу времени,
- количество исходящих TCP-пакетов в единицу времени
- количество входящих UDP-пакетов в единицу времени,
- количество исходящих UDP-пакетов в единицу времени,
- время получения пакетов,
- время отправления пакетов,
- продолжительность сессии связи в сети,
- входящие в (8) вероятности P,
- входящие в (9) состояния Q

5 Сигнатуры обозначаются как совокупность $M = \{M_1, M_2, \ldots, M_g\}$, выбор которых осуществляется в зависимости от протоколов верхних уровней, где g - количество сигнатур атак

M_1 рассматривается как следующие характеристики и параметры

- поле «адрес отправителя»,
- поле «адрес получателя»,
- поле «тип»,
- поле «данные»,
- поле «CRC»,
- непосредственно сами данные пакетов,

M_2 рассматривается следующим образом

– поле «адрес отправителя»,
– поле «адрес получателя»,
– непосредственно сами данные пакетов и т д

При такой формализации можно определить следующие матрицы совокупностей сигнатур и статистических показателей

	M_1	M_2		M_g
M_1	×	1		0
M_2	×	×		0
			×	0
M_g	×	×	×	×

	M_1	M_2		M_g
M_1	×	1		1
M_2	×	×		1
			×	0
M_g	×	×	×	×

	M_1	M_2		M_g
M_1	×	1		1
M_2	×	×		1
			×	1
M_g	×	×	×	×

(10)

	T_1	T_2		T_h
T_1	×	1		0
T_2	×	×		0
			×	0
T_h	×	×	×	×

	T_1	T_2		T_h
T_1	×	1		1
T_2	×	×		1
			×	0
T_h	×	×	×	×

	T_1	T_2		T_h
T_1	×	1		1
T_2	×	×		1
			×	1
T_h	×	×	×	×

(11)

Элементы матриц совокупностей сигнатур вычисляются по правилу

$$\begin{cases} M_{i,j} = 1, \text{ если } M \in \{M_1 \wedge M_2, M_1 \wedge M_3, M_1 \wedge M_g, \quad M_1 \wedge M_2 \wedge \quad \wedge M_g\} \\ M_{i,j} = 0, \text{ если } M \notin \{M_1 \wedge M_2, M_1 \wedge M_3, M_1 \wedge M_g, \quad , M_1 \wedge M_2 \wedge \quad \wedge M_g\}. \end{cases} \quad (12)$$

Элементы матриц статистических показателей вычисляются по правилу

$$\begin{cases} T_{i,j} = 1, \text{ если } \quad T \in \{T_1 \wedge T_2, T_1 \wedge T_3, T_1 \wedge T_h, \quad , T_1 \wedge T_2 \wedge \quad \wedge T_h\} \\ T_{i,j} = 0, \text{ если } \quad T \notin \{T_1 \wedge T_2, T_1 \wedge T_3, T_1 \wedge T_h, \quad , T_1 \wedge T_2 \wedge \quad \wedge T_h\} \end{cases} \quad (13)$$

При расчете вероятностей P предложено использовать известные нейросети, способные обучаться представленным выборкам двух видов – выборка с "опасным трафиком" и с "безопасным" В виду того, что применение нейросетей прямого распространения, сети Кохонена и сети адаптивно-резонансной теории для обнаружения сетевых атак доказано, предложен способ обнаружения сетевых атак, основанный на нейросетевых и сигнатурном анализаторах

Для обнаружения и предотвращения сетевых атак предлагается использовать известные и рассмотренные параметры и характеристики сетевого трафика и предложенные события фактов сетевых атак Такое использование в рамках методологии обнаружения и предотвращения сетевых атак базируется на следующем

– предложенном матричном представлении совокупностей статистических показателей и сигнатур,

– предложенной модели информационного обмена в ЛВС,

– предложенной формальной методике обнаружения и предотвращения попыток НСД

– практическом применении разработанной методики и совместной модели обнаружения сетевых атак,

– методике практической реализации совместной модели обнаружения и предотвращения вторжений

Обозначение процедур обнаружения СА представлены в таблице 2

Таблица 2 – Обозначение процедур обнаружения СА

Пары процедур	Одновременное применение процедур обнаружения сетевых атак	Обозначение
$g_1 \wedge g_2$	обнаружение СА в реальном и регламентируемом режимах времени	g_{12}
$g_3 \wedge g_4$	хостовое и сетевое обнаружение СА	g_{34}
$g_5 \wedge g_6$	применение сигнатурных и статистических методов	g_{56}
$g_7 \wedge g_8$	сбор информации из хранилищ данных и *непосредственно* из ЛВС	g_{78}

Объединение вида $G = \{g_{12} \wedge g_{34} \wedge g_{56} \wedge g_{78}\}$ показывает обнаружение СА всеми процедурами

Для обнаружения сетевых атак, одновременно используя сигнатурные и статистические методы, необходимы этапы, представленные на рисунке 2

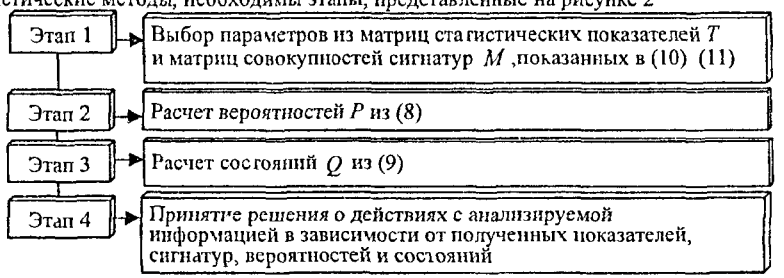


Рисунок 2 – Способ совместного обнаружения СА

В третьей главе реализован способ совместного обнаружения сетевых атак в виде программного средства и функциональных схем устройства Разработанное устройство представлено в виде функциональных блоков и описания связей между блоками

Функциональная схема устройства показана на рисунке 3

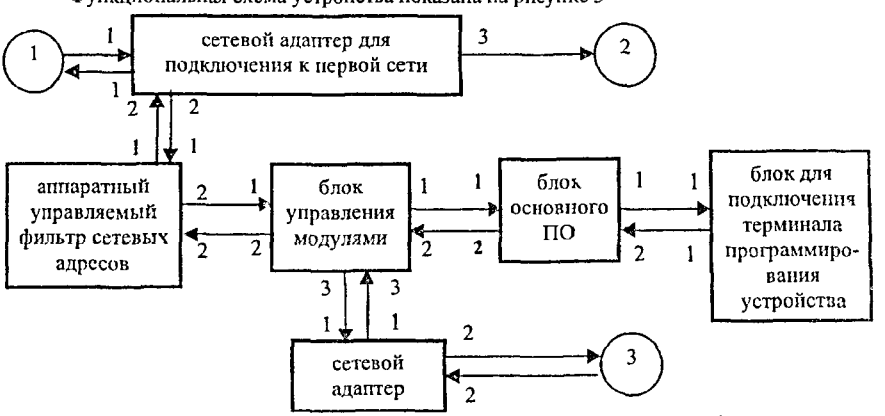


Рисунок 3 – Функциональная схема устройства со связями между блоками

Задачей данного устройства является повышение информационной защищенности компьютерных сетей, обработка и управление сетевым информационным потоком

обеспечение обнаружения и предотвращения как известных сетевых атак, так и ранее не известных сетевых атак и аномалий сетевого трафика

Техническим результатом является то, что совместная работа блоков устройства обеспечивает в случае необходимости изменение данных, передаваемых через устройство от одной информационной системы к другой, посредством предотвращения аппаратным управляемым фильтром сетевых адресов передачи запрещенных пакетов Программные средства основного блока и блока управления обеспечивают управление информацией, передаваемой между сетевым адаптером для подключения одной сети и сетевым адаптером для подключения другой сети

Отличием от аналогов является то, что при обнаружении используется сигнатурный и статистический методы, скорость обработки сетевых пакетов зависит от реализации в устройстве сетевых адаптеров, т к на суть работы устройства в целом аппаратная конфигурация данного блока не влияет

Устройство представляет собой при первом варианте подключения - аппаратно–программный модуль контроля и управления информационным потоком между «потенциально враждебной средой» (ПВС) и «защищаемой информационной системой» (ЗИС)

При втором варианте подключения - аппаратно–программный модуль (АПМ) контроля и управления информационным потоком между локальными подсетями

При третьем варианте подключения - аппаратно–программный модуль контроля и управления информационным потоком между отдельными узлами в сети

Основным назначением устройства служит обеспечение контроля и обработка передаваемых и получаемых информационных потоков таким образом, чтобы после обработки поток не содержал информации, появление которой может обеспечить несанкционированный доступ к информационной системе (ИС), её элементам и обрабатываемой в ней информации При функционировании устройства в сетевой адаптер для подключения к сети поступает необработанный входящий/исходящий трафик первой сети, который содержит пакеты, передаваемые в среде передачи данных, в которой установлено предлагаемое устройство Блок управления осуществляет программное управление сетевым адаптером 1 как обычным сетевым адаптером для приема и передачи данных, где под управлением понимается включение/выключение сетевого адаптера и разрешение на прием/передачу Далее без изменений информация передается как исходящий трафик первой сети и обрабатывается в аппаратном управляемом фильтре сетевых адресов, где проходит обработку пакетным аппаратным фильтром, работа которого заключается в сравнении адресов в передаваемых пакетах с разрешенными адресами и сравнении непосредственно самих передаваемых данных с шаблоном, занесенным изначально Затем информация поступает в основной модуль для окончательного анализа и обработки Работа данного блока является основной частью анализа всех обрабатываемых данных

В основной блок загружается программа, основанная на работе нейросети, отличительной особенностью которой является ее самообучение и изменение реакции на определенную информацию В данном случае это информация о содержащихся в пакетах данных На каждом уровне нейросети принимается решение о пригодности пакетов к определенному классу, вследствие чего дальнейшая передача пакета зависит от вывода нейросети, заключающегося в решении передачи рассмотренного пакета данных на желаемый адрес или изменении информации в пакете путём удаления или внесения дезинформирующих данных Изначально на малообученной нейросети вероятность пропуска запрещённой информации будет высока, но при применении обученной нейросети эта вероятность будет снижена до минимума, что, в свою очередь, повышает уровень защищенности защищаемой ИС

Данный блок, управляя всем устройством, также изменяет конфигурацию аппаратного управляемого фильтра сетевых адресов путем выявления адресов, с которых

Схема функционирования разработанного программного СОА показана на рисунках 4 1-4 2

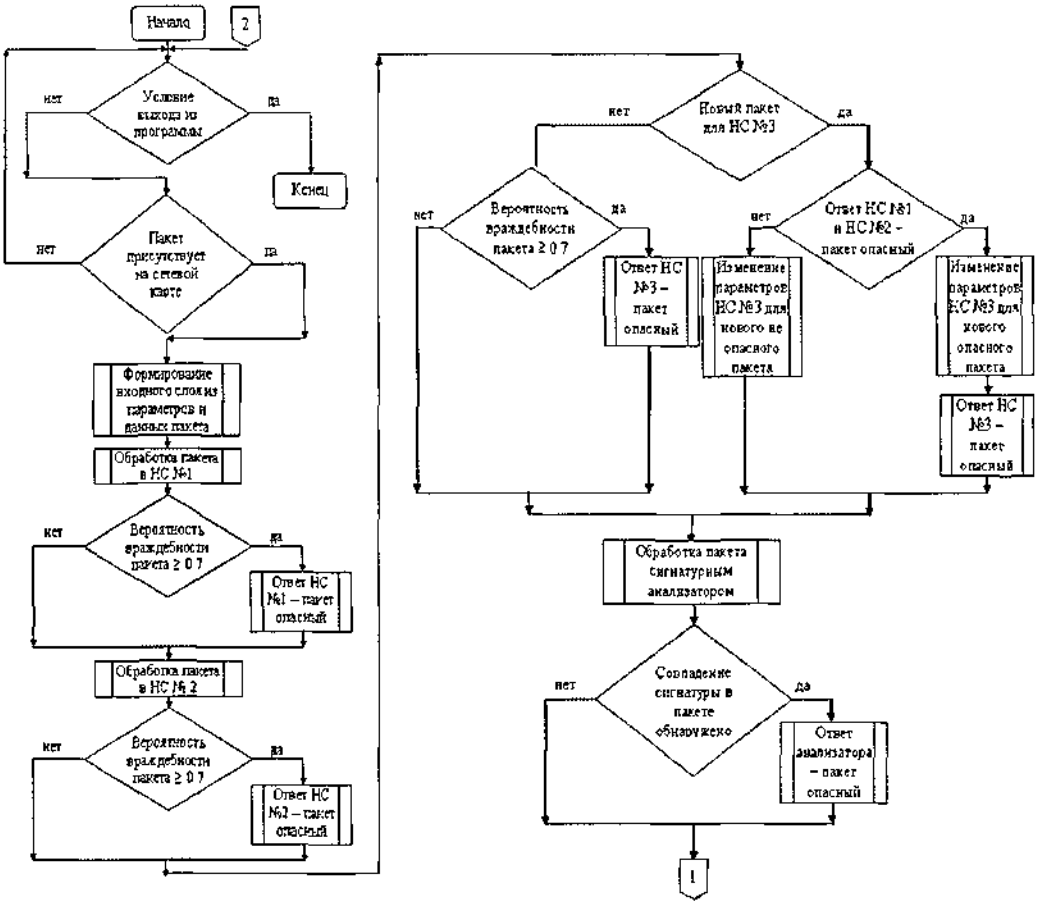


Рисунок 4 1 – Обобщенный алгоритм работы разработанного программного средства обнаружения сетевых атак

передается запрещённая информация, и занесения их в список запрещенных адресов Вследствие этого уменьшается риск приема и передачи опасной информации

После обработки данных в основном блоке принимается решение, после которого обработанный информационный поток предаётся на сетевой адаптер 2, где необходимые пакеты данных передаются как из ИС, так и в ИС

Модуль для подключения терминала программирования устройства предназначен для добавления в основной модуль недостающей или обновлённой информации для работы нейросети Для обучения элементов нейросети и повышения качества работы нейронов, предполагается обмен данными с аналогичным устройством Такая особенность устройства позволяет накапливать системе информацию об уязвимостях, появляющихся в других ИС, что снижает риск осуществления новых атак на защищаемую ИС и даёт возможность пресечения ещё не появившихся в конкретной ИС попыток осуществления НСД

Для обнаружения и предотвращения сетевых атак предложена разработанная программа «Программа обнаружения и предотвращения сетевых атак» (ПОиПСА)

Программа предназначена для выявления в сетевом трафике как известных, так и измененных сигнатур, а также поиска сетевых как известных, так и ранее не известных сетевых атак Программа обучается на специально подготовленном «чистом» сетевом трафике, не содержащем вредоносных данных пакетов и «грязном» трафике, содержащем вредоносные данные пакетов При работе она анализирует полученные сетевые пакеты и в результате работы нескольких анализаторов, использующих нейросеть итогового анализатора, принимающего решение об отсутствии или присутствии сетевых атак, и анализатора, использующего сигнатурный метод поиска и выявления сетевых атак, отображает вывод о присутствии или отсутствии атаки

Схема функционирования разработанного программного СОА показана на рисунках 4 1-4 2

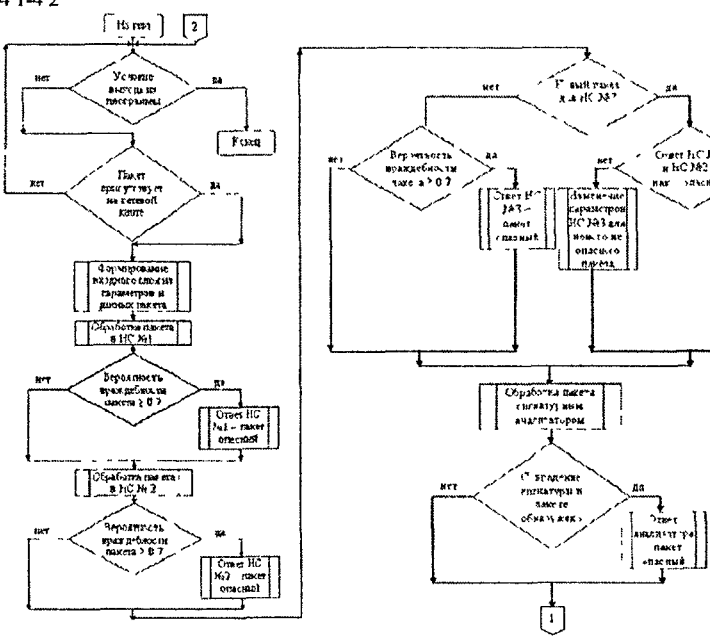


Рисунок 4 1 – Обобщенный алгоритм работы разработанного программного средства обнаружения сетевых атак

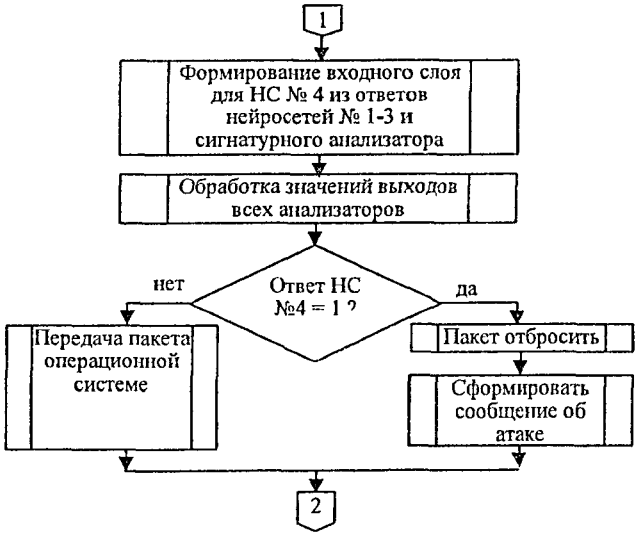


Рисунок 4 2 – Продолжение обобщенного алгоритма работы разработанного программного средства обнаружения сетевых атак

В четвертой главе разработана методика обнаружения сетевых атак и проведено тестирование СОА

Каждой процедуре ОПСА ставится в соответствие процедура обхода Множество соответствий процедур ОПСА и процедур обхода имеет вид

$$G_1' = \{g_1 \to g'_1, g_2 \to g'_2, \quad , g_8 \to g'_8\}, \qquad (14)$$

где каждое соответствие - это обход процедуры обнаружения

g'_1 – обход процедуры обнаружения СА в реальном режиме времени, g'_2 – обход процедуры обнаружения СА в регламентированном режиме времени, g'_3 – обход процедуры хостового сбора данных для анализа, g'_4 – обход процедуры сетевого сбора данных для анализа, g'_5 – обход процедуры применения сигнатурных методов, g'_6 – обход процедуры применения статистических методов, g'_7 – обход процедуры сбора информации для обработки из хранилищ данных, g'_8 – обход процедуры сбора информации для обработки непосредственно из ЛВС

В общем виде тестирование представляется в виде попытки обхода процедур обнаружения сетевых атак, показанных на рисунке 5

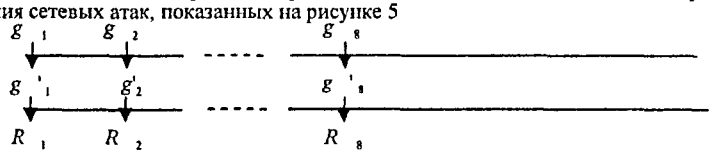


Рисунок 5 – Поэтапная процедура реализации тестирования

На рис 5 результаты тестирования каждой процедуры попытки обхода ОПСА обозначены как R_1, , R_8

В рамках методологии обнаружения сетевых атак, методика включает в себя следующие этапы

Этап 1 Применение математической модели процесса связи узлов в ЛВС трафик рассматривается как сообщения, вероятности и состояния, сообщения классифицируются на опасные и не опасные, вычисляются вероятности принадлежности сообщений в соответствии с их классификацией, вычисляются состояния узлов в ЛВС

Этап 2 Применение способа обнаружения сетевых атак обнаружение атак осуществляется одновременным использованием процедур обнаружения СА, в сетевом трафике осуществляется выявление сигнатур атак и аномалий

Этап 3 Применение устройства и/или программного средства обнаружения сетевых атак программное средство обнаружения СА реализуется с использованием сигнатурного и нейросетевых анализаторов, используется устройство обнаружения СА, в структуру защищаемой ЛВС включаются устройство и/или программное средство обнаружения сетевых атак

Для оценки надежности обнаружения СА СОА был выбран метод Каплана-Майера, преимущество которого состоит в том, что оценки не зависят от разбиения времени наблюдения на интервалы Методы анализа выживаемости в основном применяются к таким задачам, к которым применяют и другие методы, однако их особенность в том, что они применяются к неполным данным Цензурированные (такие наблюдения, при которых интересующая переменная представляет момент наступления события) наблюдения типичны, когда наблюдаемая величина представляет время до наступления некоторого критического события, а продолжительность наблюдения ограничена по времени Также более часто, чем обычная функция распределения, в этих методах используется так называемая функция выживания (для ОПСА – выживание узлов в ЛВС) $S(t)$, представляющая собой вероятность того, что объект (под объектом понимается узел в ЛВС) или система проживет время больше t С помощью значений такой функции определяется насколько своевременно и надежно СОА будет обнаруживать атаки и ИС будет оставаться в неатакованном состоянии

Значения функции выживания рассчитываются по следующей формуле

$$S(t)=\prod[(n-j)/(n-j+1)]^{\delta_{(j)}}, \qquad (15)$$

где $S(t)$ - функции выживания,

n - общее число событий (времен окончания),

j - порядковый номер отдельного события,

$$\delta_{(j)}=\begin{cases}1, \text{ если } j\text{-е событие означает отказ (атака не обнаружена)},\\ 0, \text{ если } j\text{-е событие означает обнаружение атаки}\end{cases}, \qquad (16)$$

При проведении оценки надежности обнаружения СА в соответствии с этапами, приведенными на рисунке 6, были получены значения показателей, представленные на рисунке 7

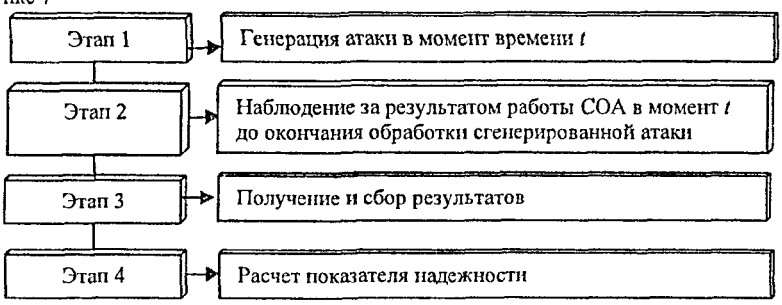


Рисунок 6 – Этапы проведения оценки надежности обнаружения СА

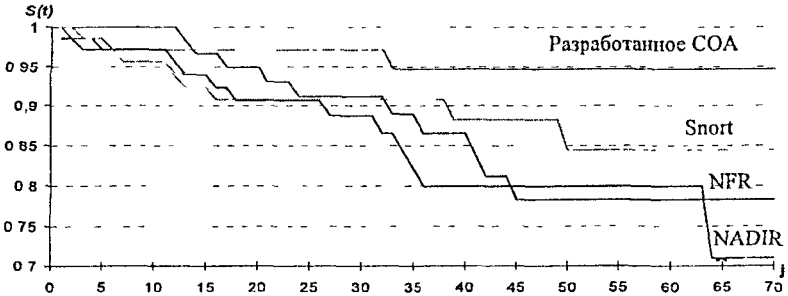


Рисунок 7 – Значения показателей надежности обнаружения СА СОА

Результаты сравнения с аналогами показаны в таблице 3

Таблица 3 – Результаты сравнения работы СОА

Наименование СОА	Общее количество сгенерированных типов атак	Количество модифицированных атак	Процент удачного обнаружения
Разработанное СОА	15	5	97 %
Snort	15	5	84 %
Network Flight Recorder	15	5	75 %
NADIR	15	5	71 %

В таблице 4 показаны интервалы задержек (в секундах) обработки пакетов и принятия решения об атаке

Таблица 4 – Временные задержки в СОА

Размеры пакетов		< 64	64-127	128-255	256-511	512-1023	>1023	Среднее время задержки на каждом шаге (сек)
шаг 1	время (сек)	0,000002	0,000025	0,000048	0,000071	0,000094	0,000117	0,0000595
шаг 2		0,000047	0,000072	0,000097	0,000122	0,000147	0,000172	0,0001095
шаг 3		0,000092	0,000117	0,000142	0,000167	0,000192	0,000217	0,0001545
шаг 4		0,000086	0,000087	0,000088	0,000089	0,00009	0,000091	0,0000885
шаг 5		0,000012	0,000167	0,000322	0,000477	0,000632	0,000787	0,0003995
шаг 6		0,000232	0,000238	0,000244	0,00025	0,000256	0,000262	0,000247
общее время задержки (сек)		0,000471	0,000706	0,000941	0,001176	0,001411	0,001646	0,0010585

В таблице 4 интервалы задержек обозначены как шаг 1 – передача пакета от драйвера сетевой карты драйверу СОА, шаг 2 – время обработки пакета в анализаторе №1, шаг 3 – время обработки пакета в анализаторе №2, шаг 4 – время обработки пакета в анализаторе №3, шаг 5 – время обработки пакета в сигнатурном анализаторе, шаг 6 – время выработки решения о присутствии атаки

Основные результаты диссертационного исследования

1 Разработана математическая модель процесса связи узлов в локальной вычислительной сети, в которой представлены сообщения, передаваемые в ЛВС, вероятности их передачи, состояния узлов, статистические и сигнатурные параметры, позволяющая рассматривать процесс обнаружения сетевых атак использующий такую формализацию

2 Разработан способ обнаружения вторжений, позволяющий обнаруживать как известные, так и не известные ранее сетевые атаки, основанный на обнаружении сетевых атак сигнатурными и статистическими методами, использующими нейросети прямого распространения, сеть Кохонена, сеть теории адаптивного резонанса и сигнатурный анализатор

3 Разработаны устройство обнаружения сетевых атак в виде функциональных схем, на которое подана заявка на изобретение №2006137745/20(041073), и программное средство обнаружения вторжений, на которое получено свидетельство о регистрации в Роспатенте №2007610367, позволяющие выявлять известные и неизвестные ранее сетевые атаки

4 Разработана методика обнаружения сетевых атак, использующая разработанный способ, устройство и программное средство обнаружения сетевых атак для выявления вторжений в локальную вычислительную сеть, повышающая эффективность обнаружения аномалий и злоупотреблений

5 Проведен сравнительный анализ надежности обнаружения сетевых атак по методу Каплана-Майера, позволяющий оценить процент выявления атак на любом количестве временных интервалов наблюдения

По теме диссертационной работы опубликованы следующие работы

1 Чипига А Ф , Пелешенко В С Формализация процедур обнаружения и предотвращения сетевых атак // Известия ТРТУ Таганрог 2006 С 96-101

2 Пелешенко В С Обзор методик обнаружения сетевых атак // Материалы второй международной научно-технической конференции «Инфокоммуникационные технологии в науке, производстве и образовании», часть II – Ставрополь, 2006 С 53-56

3 Чипига А Ф , Пелешенко В С Обзор моделей систем обнаружения атак в ЛВС и выявление их недостатков // Материалы второй международной научно-технической конференции «Инфокоммуникационные технологии в науке, производстве и образовании», часть II – Ставрополь, 2006 С 150-153

4 Пелешенко В С Подход к построению аппаратно-программного комплекса для обнаружения и предотвращения сетевых атак на защищаемые информационные системы // Материалы международной научно практической конференции «Информационные системы, технологии и модели управления производством» – Ставрополь, 2005 С 37-38

5 Пелешенко В С Разработка и применение модели информационного обмена для выявления атак и злоупотреблений // Материалы IX региональной научно-технической конференции «Вузовская наука – Северо-Кавказскому региону» Том первый – Ставрополь, 2005 С 99

6 Чипига А Ф, Пелешенко В С Построение нейросистем выявления и предотвращения атак // Материалы V региональной научно-практической конференции «Совершенствование методов управления социально-экономическими процессами и их правовое регулирование» – Ставрополь, 2005 С 237-241

7 Чипига А Ф , Пелешенко В С Математическая модель процессов связи узлов в сети при обнаружении и предотвращении несанкционированного доступа к информации // Сборник научных трудов Северо-Кавказского государственного технического университета –2006 -№2, Ставрополь С 109-114

8 Пелешенко В С Обзор средств обнаружения атак и устранение их недостатков // Сборник научных трудов Северо-Кавказского государственного технического университета –2006 -№2, Ставрополь С 109-114

9 Чипига А Ф , Пелешенко В С Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа // Вестник Северо-Кавказкого государственного технического университета – №1 (8) – 2000 с 180-182

10 Чипига А Ф , Пелешенко В С Формализация процедур обнаружения и предотвращения сетевых атак // Научно-практический журнал "Информационное противодействие угрозам терроризма" – 2006 – № 8 С 156-163

11 Чипига А Ф , Пелешенко В С

Свидетельство о регистрации программы для ЭВМ // Свидетельство об официальной регистрации программ для ЭВМ "Программа обнаружения и предотвращения сетевых атак", №2007610367 2007

Личный вклад автора в работах, написанных в соавторстве, состоит в следующем [1] – разработка методики формализации процедур обнаружения сетевых атак, [3] – анализ моделей систем обнаружения сетевых атак, [6] – разработка структуры системы выявления сетевых атак, [9] – разработка методики оценки защищенности АС от НСД, [10] – разработка методики формализации процедур обнаружения сетевых атак, [11] – разработка и реализация программного средства обнаружения сетевых атак

Подписано в печать 23 07 07
Формат 60x84 1/16 Усл п л – 0 75 Уч -изд л – 1 5
Бумага офсетная Печать офсетная Заказ 1132 Тираж 100 экз
ГОУ ВПО «Северо-Кавказский государственный технический университет»
355029, г Ставрополь, пр Кулакова, 2

Издательство ГОУ ВПО «Северо-Кавказский государственный технический университет»
Отпечатано в типографии ГОУ ВПО «СевКавГТУ»