8. Аваков, С.М. Новые методы и высокопроизводительные алгоритмы детектирования дефектов для модульной платформы автоматического контроля оригиналов топологии СБИС / С.М. Аваков // Инженерный вестник. – 2006. – № 1 (21) / 5. – С. 88-97.
9. Automatic PCI Inspection Algorithms: A Survey / M. Moganti [et al.] // Computer Vision and Image Understanding. – 1996. – № 63. – P. 287-313.
10. Malki, S. Neural Vision Sensors for Surface Defect Detection / S. Malki, L. Spaanenburg, N. Ray // IEEE International Joint Conference on Neural Networks, Budapest, Hungary, 25-29 July, 2004. – 2004. – Vol. 4. – P. 3155-3160 [Electronic resource]. – 2004. – Mode of access: www.it.lth.se/users/lambert/imaging/ijcnn04-malki.pdf. – Date of access: 12.03.2008.
11. Tal, Efrat. Printed Circuit Board Inspection / Efrat Tal, Inbal Yefet [Electronic resource]. – 2002. – Mode of access: http://visl.technion.ac.il/projects/2002w23/. – Date of access: 12.05.2007.
12. Zuwairie, Ibrahim. Wavelet-Based Printed Circuit Board Inspection System / Ibrahim Zuwairie, Abd. Rahman Al-Attas Syed // International Journal of Signal Processing (IJSP). – 2004. – Vol. 1. – P. 65-71.
13. Szolgay, P. Analogic algorithms for optical detection of breaks and short circuits on the layouts of printed circuit boards using CNN / P. Szolgay, K. Tömördi // International Journal of Circuit Theory and Applications. – 1999. – Vol. 27. – P. 103-116.
14. Лохов, А. Средства проектирования СБИС компании Mentor Graphics. Общий обзор / А. Лохов // Электроника: Наука, Технология, Бизнес [Электронный ресурс]. – 2003. – № 7. – Режим доступа http://www.electronics.ru/issue/2003/7.
15. Awakaw, S. A prospective modular platform of the mask pattern automatic inspection using die-to-database mask method / S. Awakaw, A. Korneliuk, A. Tsitko // Proc. SPIE, Photomask and Next-Generation Lithography Mask Technology XII, Yokohama, Japan, 13-15 April, 2005. – Vol. 5853. – Bellingham, Washington: SPIE, 2005. – P. 965-976.
16. Садыхов, Р.Х. Обработка изображений и идентификация объектов в системах технического зрения / Р.Х. Садыхов, А.А. Дудкин // Искусственный интеллект. – 2006. – № 3. – С. 634-643.

Материал поступил в редакцию 20.09.08

DOUDKIN A.A. Integrated circuit layout inspection based on computer vision systems

Optical inspection methods of integrated circuit layout and their implementation in layout image processing systems are represented in the paper.

УДК 004.8.032.26

Войцехович Л.Ю., Головко В.А., Кочурко П.А., Войцехович Г.Ю.

СИСТЕМА ОБНАРУЖЕНИЯ АТАК КАК ОСНОВНОЙ ЭЛЕМЕНТ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ

Введение. Высочайший уровень угроз информационной безопасности [1] из внешней среды сделал брандмауэр и *Систему Обнаружения Вторжений (Intrusion Detection System - IDS)* необходимой составляющей защищенной информационной системы. В защите нуждаются не только организации и их корпоративные сети, но и пользователи домашних компьютеров, которые не желают, чтобы их личные данные стали достоянием общественности. В современном мире развивающихся стремительными темпами компьютерных технологий и телекоммуникаций злоумышленникам стало гораздо легче достичь поставленных целей, благодаря невнимательности и неосведомленности своих жертв о существующих методах защиты.

Что такое система обнаружения вторжений (или атак) и каково ее место в общей системе защиты? Чтобы внести ясность в этот вопрос, значительная часть материала статьи посвящена именно обзору системы обнаружения вторжений как таковой. В завершающих разделах кратко обсуждается разрабатываемый нами модуль сетевой защиты. В целом статья носит больше обзорный характер, и цель ее – обосновать необходимость проведения исследований в этой области и предложить новый подход к построению систем IDS.

Простейшим средством сетевой защиты может служить брандмауэр (межсетевой экран, firewall) - реализованное программно или аппаратно средство фильтрации сетевого трафика между двумя сетями или компьютером и сетью (персональный брандмауэр). При этом используются сетевые адреса отправителя и получателя запроса или конкретные службы, а анализа передаваемого трафика не происходит. Очевидно, что, ограничившись только брандмауэром, невозможно защитить систему от опытного злоумышленника, поскольку, к примеру, он может на вполне легальном основании обратиться к намеренно или случайно открытой для доступа службе и провести атаку.

Для анализа передаваемых в сети данных необходимо более сложное и интеллектуальное средство – Система Обнаружения Вторжений. Система обнаружения вторжений – программное и/или аппаратное средство для выявления фактов несанкционированной деятельности (вторжения или сетевой атаки) в компьютерной сети или отдельном узле. Такие системы в последнее время получают все большее распространение, поскольку правильно сконфигурированная IDS является серьезным препятствием на пути злоумышленника, и его шансы на успех операции снижаются до минимума.

IDS также хорошо дополняет другие средства защиты. Так, например, после обнаружения IP-адресов, с которых была произведена атака, IDS может передать и пополнить ими черный список брандмауэра.

Еще одним преимуществом IDS является то, что ей безразлично, кто именно совершает противопоказанные действия – незарегистрированный пользователь или системный администратор. И в том, и в другом случае реакция будет одна и та же.

Кроме того, сетевая IDS может контролировать не только внешний входящий и исходящий трафик, но и локальный. Существует печальная статистика, согласно которой около 80% вторжений выполняется в пределах корпоративной сети, т.е. сотрудниками самой же организации. Понятно, что получить необходимую информацию о такого рода вторжении может IDS, настроенная на работу в подсети (сегменте локальной сети).

Реакция IDS при обнаружении нарушения безопасности может быть различной. Выделяют два типа систем: пассивные и активные. Пассивная система при обнаружении угрозы заносит соответствующую запись в журнал регистрации событий или предупреждает администратора, например, посылкой сообщения по специальному каналу. В отличие от пассивных систем, активные IDS предпринимают (самостоятельно или по команде) действия для предотвращения угрозы: дается указание межсетевому экрану блокировать со-

Войцехович Леонид Юрьевич, *аспирант кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Головко Владимир Адамович, *д.т.н., профессор, заведующий кафедрой интеллектуальных информационных технологий Брестского государственного технического университета.*

Кочурко Павел Анатольевич*, ст. преподаватель кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Войцехович Геннадий Юрьевич*, студент факультета электронных информационных систем Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, Беларусь, г. Брест, ул. Московская, 267.

единение, запускается специальная программа или действия злоумышленника нейтрализуются средствами самой IDS. Такие системы, способные предпринимать активные действия против злоумышленника, еще называют *Системами Предотвращения Вторжений (Intrusion Prevention System - IPS)*. В настоящее время все больше происходит уклон в сторону разработки именно IPS.

1. История IDS. В 1985 году в связи с новым витком развития компьютерных технологий резко возрос интерес к проблемам защиты информации. Однако широкое использование IDS в коммерческих целях началось лишь с 1996 года.

В основе зарождения систем IDS, в том виде, в каком они представлены в настоящее время, была работа Дороти Деннинг, опубликованная в 1986 году [2]. В этой работе рассматривались статистические методы для построения системы обнаружения вторжений IDES.

В дальнейшем было предложено использовать в системах обнаружения вторжений методы на основе правил, искусственные нейронные сети, нечеткую логику, искусственные иммунные системы и другие подходы.

В настоящее время разработки в области обнаружения вторжений ведутся как в коммерческих целях отдельными организациями, занимающимися продвижением сетевого оборудования и/или средств защиты информационных ресурсов, так и в научно-исследовательских центрах или университетах, где первоочередная цель – предложить новые алгоритмы и методы, усовершенствовать существующие подходы.

Примерами крупнейших коммерческих компаний, занимающихся разработками IDS, являются Symantec, NAI, Cisco и CheckPoint. Среди программных продуктов компании Symantec, ориентированных на защиту корпоративных сетей любой степени сложности, можно назвать Symantec Intruder Alert и Symantec NetProwler [3]. Еще одним коммерческим продуктом является система RealSecure от Internet Security Systems (ISS) [4].

Примером бесплатно распространяемой системы обнаружения вторжений служит Snort [5]. Благодаря открытости исходного кода и бесплатности можно утверждать, что данная система является самой популярной IDS в мире (фактически классической).

Среди экспериментальных систем можно выделить EMERALD и NetStat. EMERALD [6] является разработкой компании SRI. Эта компания проводила исследования, связанные с обнаружением аномалий (отклонения от нормального поведения). NetStat [7] создавалась в Калифорнийском университете с целью обнаружения вторжений в реальном времени посредством анализа состояний систем и переходов в них.

2. Классификация IDS

Сетевая Система Обнаружения Вторжений (Network-based Intrusion Detection System, NIDS) ведет наблюдение и анализ событий, происходящих в компьютерной сети, и отслеживает циркулирующие сетевые пакеты. Такие системы обеспечивают защиту сразу нескольких узлов. Сетевая IDS способна обнаруживать атаки класса DoS, нарушения контроля доступа, атаки сканирования сети/портов и т.п. Например, резкое необоснованное увеличение потока данных в сети может свидетельствовать о какой-либо разновидности атаки DoS.

Выделяют также *Системы Обнаружения Вторжений уровня узла (Host-based Intrusion Detection System, HIDS)*, такие системы работают на отдельном узле и анализируют события, которые происходят в системе. Для IDS уровня узла источником информации служит, например, состояние оперативной памяти компьютера, файловая система, журналы регистрации, данные системных log-файлов.

Существует два основных метода в области обнаружения вторжений: обнаружение злоупотреблений и обнаружение аномалий. Обнаружение злоупотреблений предполагает наличие сигнатур атак. Основным недостатком таких систем является их неспособность обнаруживать новые или неизвестные атаки, т.е. записи о которых в системе отсутствуют. Обнаружение аномалий связано с построением профиля нормального поведения системы. При этом атакой считается любое отклонение от этого профиля. Главным преимуществом таких систем является принципиальная возможность определения ранее не встречавшихся атак. Большинство коммерческих IDS ориентированы именно на обнаружение злоупотреблений.

Кроме того, часть рынка принадлежит системам IDS, основанным на анализе протоколов, которые в свою очередь можно отнести в отдельную категорию. Такие IDS выполняют поиск несоответствия сетевых пакетов принятым стандартам. Существуют также так называемые “Honey Pots” – системы. Такие IDS развертываются в сети и действуют как приманки для атакующего. Во время выполнения атаки эти системы собирают дополнительные данные о методах, применяемых нападающим, его целях и др.

3. Требования к IDS. Поскольку система IDS должна работать в любых условиях, в том числе на самых загруженных участках, причем желательно, что бы конечный пользователь даже не подозревал о ее существовании, она должна удовлетворять ряду требований:

1) независимость от перегрузок – одно из основных условий, накладываемых на IDS, является сохранение работоспособности в самых жестких условиях. Одними из самых распространенных атак являются атаки загрузки сетевого трафика большим количеством бессмысленных пакетов. Поэтому выбор системы должен выполняться с расчетом на максимальные нагрузки;
2) работа в реальном времени – система должна моментально реагировать на атаку злоумышленника, а в некоторых случаях даже предупреждать подобные действия, ориентируясь по каким-либо тревожным событиям в сети;
3) устойчивость к атакам на саму IDS – любая более-менее хорошо спланированная атака обязательно предполагает действия, направленные на подавление системы безопасности;
4) масштабируемость – подразумевается возможность добавления в систему IDS средств обнаружения новых атак, а также расширения IDS при разрастании корпоративной сети.

4. Структура IDS. Типичная структура IDS включает в себя следующие компоненты:

1) сетевые сенсоры (датчики) – средство для сбора данных о сетевой активности. Сенсоры бывают двух типов: аппаратные, которые представляют из себя отдельное устройство со специфическим оптимизированным для захвата трафика ПО, и программные, которые устанавливаются на отдельные хосты в сети под управлением ОС;
2) модуль анализа полученных данных на предмет выявления подозрительных действий и вторжений;
3) база данных (хранилища данных), в которых накапливается информация о функционировании системы обнаружения вторжений, в том числе сигнатуры обнаруженных атак;
4) средства управления – позволяют администратору взаимодействовать со всеми подсистемами IDS: настраивать работу отдельных узлов, просматривать журналы событий и отчеты, пополнять систему новыми алгоритмами обнаружения вторжений и т.п.
5) отдельно функциональность системы IDS может быть дополнена модулем реагирования, который позволит предпринять ответные меры на действия нарушителя.

Все вышеперечисленные компоненты системы IDS могут быть реализованы в рамках одного компьютера или программного комплекса. Но, как правило, в большой корпоративной сети имеет смысл строить систему обнаружения вторжений по архитектуре клиент-сервер. Так, например, удобно выделить отдельный сервер базы данных для централизованного хранения всей информации, собранной сетевыми сенсорами в разных точках сети. Кроме того, сервер базы данных и консоль администратора безопасности желательно располагать в наиболее защищенных участках.

5. Место IDS в компьютерной сети. Важным вопросом при развертывании системы обнаружения вторжений в сети является вопрос размещения отдельных модулей IDS. Если неправильно их разместить, то какой-то сегмент сети может оказаться незащищенным, в то время как в другом – могут возникать дополнительные перегрузки каналов передачи данных. Поэтому вопросу размещения IDS необходимо уделять особое внимание, от этого зависит, стоит ли вообще IDS затраченных на нее средств.

5.1. Как подключить сенсоры IDS? Простейший вариант размещения IDS предполагает установку сенсоров системы на входе в сегмент *на разрыв* (рис. 1). Таким образом, весь трафик, поступающий в сегмент, проходит через него, как в случае с брандмауэром. Некоторые сенсоры могут одновременно совмещать функции IDS и брандмауэра.

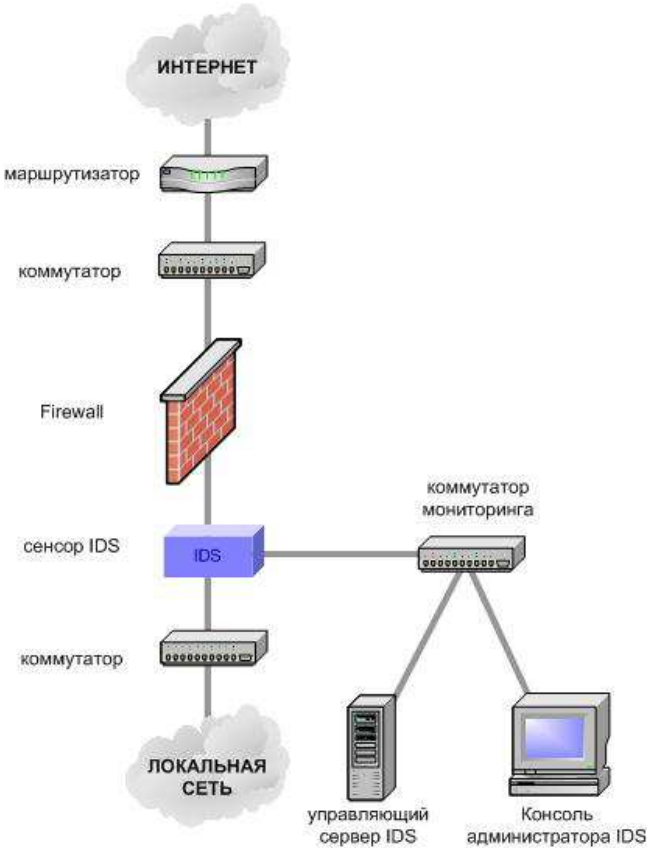

Рис. 1. *Пример использования сенсора, подключенного на разрыв*

Такой подход имеет свои достоинства и свои недостатки. К положительным сторонам можно отнести то, что весь без исключения трафик проходит через IDS, так что при необходимости он может быть легко заблокирован. К отрицательным: высокие требования к производительности системы IDS, поскольку необходимо обрабатывать большой объем трафика; при выходе системы из строя (в том числе от действий злоумышленника), нарушается работоспособность всего сегмента.

Второй вариант размещения IDS подразумевает *параллельное* включение сенсора (т.н. пассивный режим работы сенсора). В этом случае реальный трафик проходит мимо сенсора, а на сам сенсор поступает лишь копия той информации, которая передается в сети.

Существуют различные способы включения пассивного сенсора:

зеркалирование портов коммутатора – большинство современных компьютерных сетей являются сетями коммутации. Более дорогие модели коммутаторов обладают возможностью отразить проходящий через них трафик на отдельный порт (т.н. spanning port). Однако такое решение, несмотря на его простоту, обладает определенными недостатками, например, когда загрузка сети велика, то часть трафика может быть утеряна из-за недостаточной производительности коммутатора;

- ответвление сети (network tap) – это прямое соединение сенсора с физической средой передачи данных, например, с оптическим кабелем. Такое решение обеспечивает сенсор копией всего трафика, циркулирующего в сети, но связано с дополнительными трудностями по выполнению самих ответвлений;
- диспетчер IDS (IDS Load Balancer) – это специальное устройство буферизации сетевого трафика и перераспределения его между системами мониторинга и даже сенсорами IDS. Диспетчер IDS получает копию трафика от одного или нескольких портов коммутаторов, с возможностью зеркалирования, или сетевых ответвлений, и, далее, по заданной администратором схеме распределяет его между конечным оборудованием.

Рис. 2 демонстрирует примеры подключения пассивного сенсора через диспетчер IDS, ответвление и специальный порт коммутатора с функцией зеркалирования.

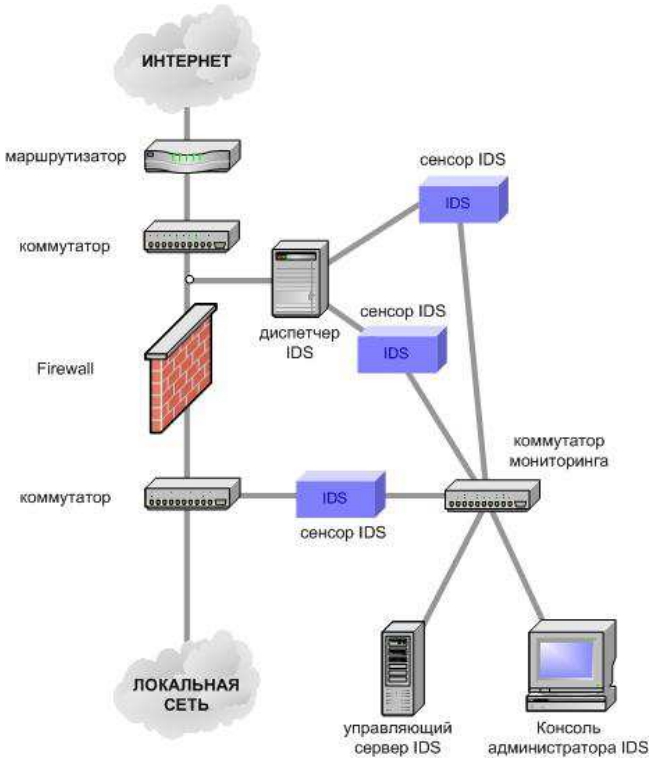

Рис. 2. *Пример использования пассивного сенсора IDS*

Очевидно, что для предотвращения вторжений подключение сенсора IDS в разрыв является предпочтительным, поскольку параллельное соединение обеспечивает минимальные возможности по воздействию на ситуацию в сети.

5.2. Где разместить сенсоры IDS? Для работы системы обнаружения вторжений первоочередным вопросом является размещение сенсора, который будет непосредственно взаимодействовать с сетевым трафиком для выявления в нем атак. Для защиты корпоративной компьютерной сети сенсоры обычно размещают рядом с брандмауэром [8]. При этом возникает вопрос: перед или после брандмауэра следует устанавливать сенсор? Как правило, сенсоры IDS устанавливаются перед брандмауэром (рис. 3).

Рис. 3. *Размещение сенсора IDS на границе локальной сети*

Такая конфигурация IDS отслеживает все атаки, поступающие из Internet, что позволит своевременно оповестить администратора сети о попытках проникновения и принять ответные меры. Однако в таком случае могут возникать проблемы с большим числом ложных

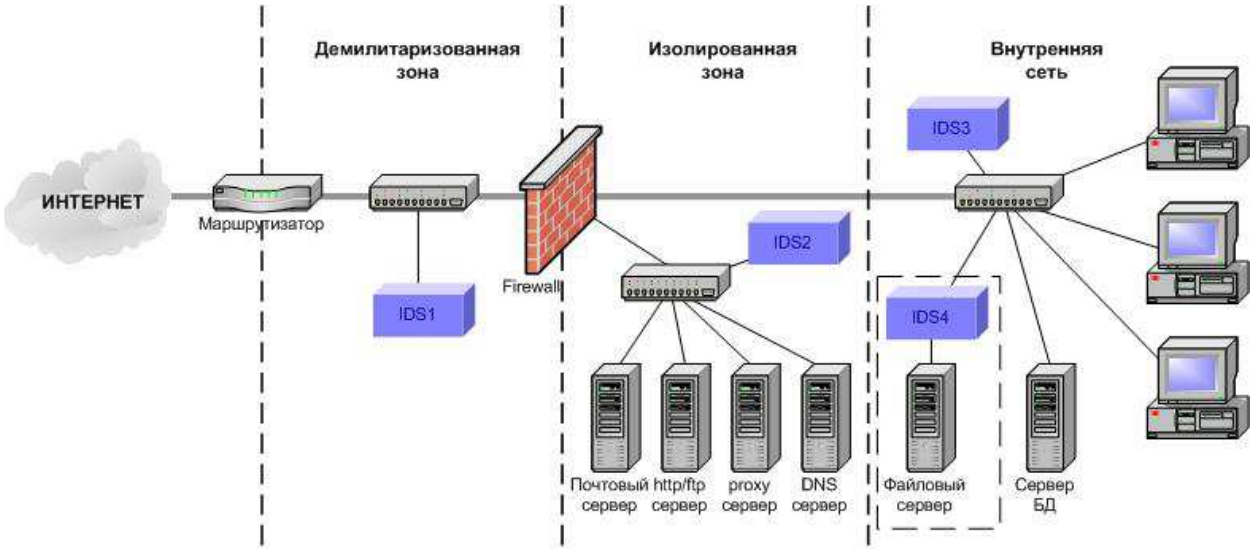

Рис. 4. *Возможное размещение сенсоров IDS*

срабатываний и большей уязвимостью самой IDS со стороны злоумышленников.

Второй вариант размещения сенсора – за брандмауэром. В этом случае IDS гораздо проще правильно сконфигурировать. Вполне очевидно, что правильно настроенный брандмауэр способен устранять большинство несложных сетевых атак. Кроме того, появляется возможность контролировать сам брандмауэр, т.е. видеть, какие атаки он пропускает, и выполнять его настройку.

Однако если позволяют средства, то лучше всего разместить два сенсора: один внешний, а другой внутренний. Преимущества очевидны.

Сенсоры размещают и в других местах локальной сети, для повышения уровня безопасности отдельных ее участков. Так, дополнительные сенсоры системы обнаружения атак уровня сети могут располагаться около ключевых узлов корпоративной сети (серверные, отдельные машины, обеспечивающие работоспособность сети предприятия); в подсетях, представляющих повышенный интерес для злоумышленника (бухгалтерские отделы, научные лаборатории и т.п.); в подсетях, которые уже подвергались нападениям или в которых уже были выявлены подозрительные действия; в сегментах сети, где располагаются хосты, к которым имеют доступ временные пользователи и т.п.

Возможный вариант развертывания сенсоров IDS в корпоративной сети представлен на рис. 4.

В приведенной схеме IDS1 размещена перед брандмауэром, контролируя всю активность на внешних рубежах защищаемой сети. Следующим слабым звеном являются узлы, обеспечивающие представление собственных интернет-ресурсов. Такие узлы обычно располагаются в демилитаризованной и в изолированной зоне корпоративной сети. *Демилитаризованная зона* - участок сети, который находится между шлюзом сети Internet и шлюзом или брандмауэром локальной сети. Под *изолированной зоной* в данном случае понимается тот участок сети, к которому подключены общедоступные ресурсы организации. И та и другая зоны адресуются из глобального Интернета, поэтому являются наиболее уязвимыми. Открытые ресурсы имеет смысл располагать именно в изолированной зоне (почтовый сервер, web-сервер), поскольку, как уже отмечалось выше, межсетевой экран способен защитить систему от большинства не столь серьезных угроз. Однако являясь объектом особого внимания со стороны злоумышленников эти сервера подвержены повышенному риску взлома и сами могут стать инструментом для выполнения более хитроумных схем атак. Поэтому подобные ресурсы нуждаются в дополнительной защите - IDS2. Остальные сегменты локальной сети (ровно как и отдельные хосты) в зависимости от конкретных обстоятельств так же могут быть защищены системами обнаружения вторжений (IDS3 и IDS4). Таким образом, при обнаружении противоправных действий, исходящих из-за пределов локальной сети или от собственных серверов (что представляет еще большую опасность), IDS может предпринять ответные меры: переконфигурировать списки доступа межсетевого экрана, в случае DoS-атаки разорвать соединения посылкой пакетов RST и т.д.

Вообще, следует отметить, что размещение IDS на сетевом периметре (с обеих сторон межсетевого экрана, близко к dial-up серверу и на соединении с сетью партнеров) является наиболее эффективным, поскольку эти узлы работают на достаточно низких скоростях. При установке IDS около критичных серверов для прослушивания трафика сразу возникают проблемы с производительностью IDS, поскольку сервера работают на высоких скоростях. Также при размещении IDS в локальной сети возникают проблемы с высокоскоростными сегментами, и при большой загрузке часть трафика может быть пропущена.

6. Проблемы IDS и необходимость в научном подходе к их разрешению. Необходимость в дальнейшем развитии и исследовании систем обнаружения атак объясняется тем, что современные подходы к обнаружению сетевых атак не дают стопроцентной гарантии безопасности, в то время как действия злоумышленников приобретают все более изощренные формы, а ущерб, наносимый компьютерным системам, только возрастает.

Современное состояние дел в области систем обнаружения вторжений характеризуется рядом проблем. В первую очередь остро стоит проблема ложных срабатываний или ошибка первого рода, когда легитимная деятельность принимается за злоумышленную. Во-вторых, требуются более производительные системы, которые способны работать в гигабитных сетях. В-третьих, такие системы должны быть достаточно отказоустойчивыми, так как в современных условиях организациям зачастую требуются непрерывная работа телекоммуникационных сетей. Четвертая проблема заключается, как уже отмечалось выше, в обнаружении модифицированных атак и неизвестных ранее угроз.

Поэтому экспериментирование с новыми подходами и разработка более совершенных алгоритмов противодействия явным и неявным угрозам безопасности компьютерных сетей остаются первоочередной задачей в области обнаружения вторжений.

Для анализа данных необходимо применять самые современные технологии обработки информации. Необходимо сделать IDS более интеллектуальными, что поможет отслеживать сложные схемы атак. Перспективным направлением в области развития систем IDS по-прежнему остаются системы обнаружения аномалий. Кроме того, программно-аппаратное обеспечение компьютерных сетей должно эволюционировать по пути интеграции в единую систему

безопасности, где каждый узел выполняет четко определенную функцию в вопросе обеспечения защиты.

7. Разработка системы обнаружения вторжений на базе нейронной сети. Наши исследования в области систем обнаружения вторжений в первую очередь направлены на разработку модуля распознавания, как наиболее сложного и наукоемкого элемента в структуре IDS. Здесь мы предлагаем применить подходы, которые часто относят к области Искусственного Интеллекта, а именно: нейронные сети и иммунные системы [9].

Искусственные нейронные сети (ИНС) имеют потенциал для решения большого количества проблем, характерных для других современных подходов к обнаружению сетевых атак:

- обученная нейронная сеть функционирует достаточно быстро, что позволит значительно повысить пропускную способность IDS;
- нейронные сети обладают высокой обобщающей и прогностической способностью и поэтому в состоянии отслеживать модифицированные атаки и даже ранее неизвестные атаки;
- нейронные сети также хорошо зарекомендовали себя при работе с зашумленными образами, что тоже немаловажно для решения вышеобозначенной проблемы;
- нейронные сети позволяют создавать достаточно развитые структуры, которые, обладая большой гибкостью и масштабируемостью могут превратиться в эффективный инструмент в руках разработчика средств защиты компьютерных систем.

В рамках выполняемых нами исследований разрабатывается специальное программное обеспечение для тестирования предлагаемых нейросетевых подходов в условиях реальной компьютерной сети на реальных данных. Рассмотрим имеющиеся наработки в этом направлении более подробно.

Выше были перечислены основные составляющие типичной сетевой системы обнаружения вторжений: сетевые сенсоры, модуль анализа (распознавания), база данных, средства управления. Для проведения лабораторных испытаний предлагается объединить все эти составляющие в одном программном продукте, который будет совмещать в себе функции сниффера (захват трафика), анализатора и средства управления. Установив такую программу на отдельный компьютер, пользователь сможет обнаруживать атаки как на этот компьютер, так и на другие компьютеры, подключенные к данному сегменту сети. Недостатком такой системы является высокая требовательность к ресурсам. Поэтому такое решение пригодно в первую очередь для лабораторных исследований.

7.1. Захват трафика. Первоочередной задачей при построении системы обнаружения атак является захват сетевого трафика. Захват трафика выполняется сетевым адаптером, работающим в режиме promiscuous mode, т.е. прослушивающем все пакеты в сети.

7.1.1 Варианты реализации. Для анализа сетевого трафика разрабатываемыми нейросетевыми методами может понадобиться различное количество параметров TCP-соединений – как основные параметры, так и вычисляемые, и параметры, получаемые из данных. Учитывая, что главное требование к модулю слежения за сетевой активностью – низкая загрузка процессора, ведь этот модуль должен работать в системе постоянно, целесообразно предложить несколько вариантов реализации, которые можно будет использовать в дальнейшем в зависимости от того, какие данные понадобятся для анализа.

В настоящее время наиболее распространены операционные системы двух типов: семейства Microsoft Windows и различные дистрибутивы на ядре Linux.

Учитывая идеологию построения Linux – множество маленьких простых частей вместе решают очень сложные комплексные задачи – пока нет необходимости в разработке отдельного модуля перехвата трафика: для исследовательских целей вполне достаточны свободные программы типа tcpspy, tcpdump и другие, выходная информация которых может направляться непосредственно модулям предварительной обработки данных и нейросетевого анализа. Если же предоставляемых этим семейством программ данных окажется мало, то всегда есть возможность нарастить их функционал, либо написать собственные модули. Стоит отметить, что большинство данных программ базируется на библиотеке pcap, опыт работы с которой получен при разработке модулей для Windows.

Для семейства операционных систем Windows программы с соответствующей функциональностью небесплатны и имеют закрытую архитектуру, вследствие чего не могут быть модифицированы и интегрированы в общую систему анализа сетевой активности. Поэтому целесообразно разработать собственные модули, которые будут реализовывать именно ту функциональность, которая может накладываться на них методами нейросетевого анализа.

В следующих пунктах рассмотрим реализованные варианты модулей слежения.

7.1.2 Перехватчик пакетов на основе Local Network Monitor API

Local Network Monitor API от NT Kernel Resources [10] – это высокопроизводительная система фильтрации стетевых запросов на уровне приложения для Windows NT/2000/XP/2003/Vista, которая позволяет контролировать активность протоколов семейства IP локальной системы в реальном времени. API работает на уровне Transport Driver Interface (TDI) сетевых операций ядра операционной системы и позволяет просматривать и контролировать всю сетевую активность на уровне приложений. При взаимодействии с Windows Packet Filter Kit от того же производителя можно добиться высокой функциональности (сочетание с межсетевым экраном и т.д.).

С помощью данного API реализован модуль слежения за сетевой активностью – пакетов протокола TCP и с возможностью блокирования пакетов, что окажется в дальнейшем полезным для активной защиты. Следствием того, что производится только слежение за пакетами, но не соединениями, является высокая скорость работы и низкое потребление системных ресурсов.

Данное API имеет не бесплатную лицензию для целей разработки, а не обучения, потому дальнейшее его использование должно быть обосновано требованиями методов нейросетевой обработки данных.

7.1.3 Монитор соединений на базе Windows Sockets и IPHelper API

WinSock (сокращение от Windows Sockets) – это интерфейсная прослойка между Windows-приложением и базовой сетью TCP/IP. Интерфейс сокетов впервые появился в Berkeley Unix как API для работы с сетями TCP/IP. Winsock базируется на Berkeley Sockets API и включает большую часть стандартных функций BSD API, а также некоторые расширения, специфические для Windows. Поддержка сетевого взаимодействия через TCP/IP в Windows-программе сводится к вызову функций Winsock API и использованию библиотеки WINSOCK.DLL, реализующей интерфейс Winsock.

Модулем мониторинга создаются потоки перехвата пакетов для каждого установленного сетевого интерфейса в системе, представляющие собой сокеты в неразборчивом режиме (promiscuous mode). Они перехватывают все пакеты, которые следуют через сетевой интерфейс. По получении пакета он расшифровывается, и данные заголовка пакета позволяют начать его обработку и сопоставление с соединением: от IPHLPAPI получается список активных соединений системы (таблица соединений с указанием локального и удаленного адресов и портов, состояния и процесса, который открыл это соединение); в этом списке находится то соединение, к которому относится данный пакет; производится изменение характеристик данного соединения (количество переданных байт, длительность функционирования) во внутренних таблицах программы. Каждую секунду и по каждому принятому сетевому пакету производится новый запрос к IPHLPAPI, что позволяет следить за текущими открытыми соединениями в реальном режиме времени.

Вся получаемая информация отображается в окне программы в удобном для пользователя табличном представлении (рис. 5). Закрытые соединения отображаются серым цветом и по прошествии четырех секунд исчезают из таблицы.

Основное достоинство данного варианта сетевого монитора – использование стандартных средств операционной системы без каких бы то ни было промежуточных систем или API. Благодаря этому достигается высокая производительность.

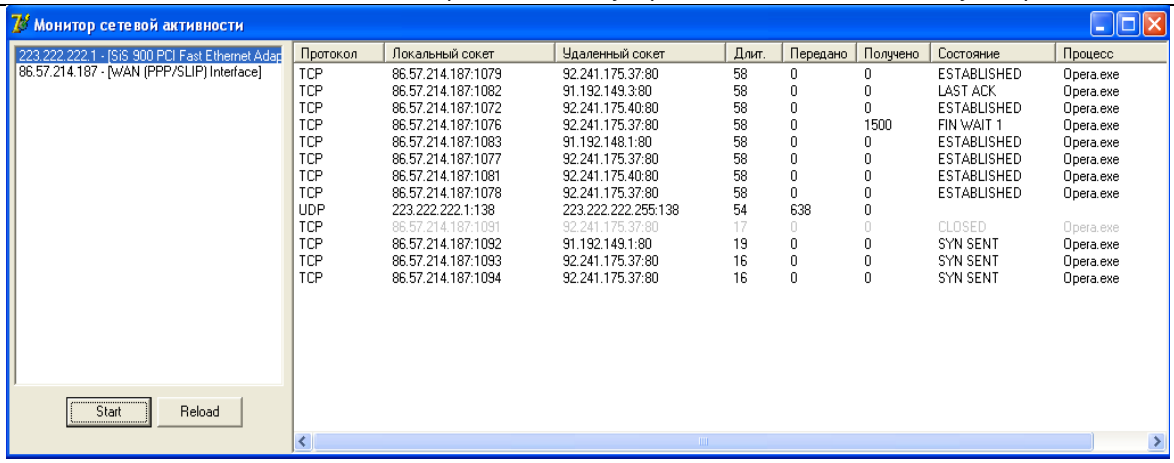

Рис. 5. *Отображение данных*

7.1.4 Монитор соединений на базе WinPCap

Монитор сетевого трафика NetMonitor реализует функции слежения за сетевым трафиком по протоколам TCP, UDP и ICMP и по заголовкам пакетов отслеживает соединения. По завершении соединения данные о нём могут приводиться к формату KDD записи и передаваться для дальнейшего нейросетевого анализа.

Реализация функций перехвата трафика с любого сетевого интерфейса (рис. 6) обеспечивается свободно распространяемым драйвером WinPCap 4.1, которая является портом UNIX-библиотеки pcap для Windows и должна быть заранее установлена на компьютере [11]. WinPCap представляет собой драйвер перехвата пакетов стека протоколов TCP/IP.

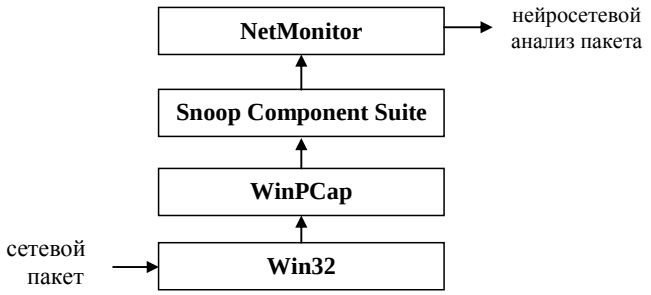

Рис. 6. *Схема работы перехвата сетевых пакетов*

Взаимодействие с WinPCap ведётся не напрямую, а через библиотеку компонентов Snoop Component Suite 2.0 [12]. Библиотека предоставляет невизуальные компоненты для получения информации о перехваченных пакетах протоколов IP, TCP, UDP, ICMP, а также обо всех сетевых интерфейсах, используемых системой и их адресах.

NetMonitor определяет все доступные сетевые интерфейсы (до 10) и для каждого создаёт Snoop компоненты перехвата TCP, UDP и ICMP пакетов, а так же объекты мониторинга. При перехвате пакета на любом из интерфейсов Snoop определяет протокол, к которому тот относится, и соответствующий объект вызывает обработчик события перехвата, коим является метод анализа пакетов объекта мониторинга.

Каждый заголовок пакета анализируется, отслеживаются процессы установления и разрыва TCP-соединения, и данные обо всех соединениях по каждому локальному порту накапливаются. Каждое соединение проходит следующие стадии [13]:

а) LISTEN – ожидание запроса на соединение со стороны чужих портов и программ TCP;
б) SYN-SENT – ожидание парного запроса на установление соединения. С нашей стороны запрос уже сделан;
в) SYN-RECEIVED – ожидание подтверждения после того, как запрос соединения уже принят и отправлен;
г) ESTABLISHED – состояние открытого соединения, принимаемые данные можно представить пользователю. Это нормальное состояние соединения в фазе передачи данных;
д) FIN-WAIT-1 – ожидание запроса от чужой программы TCP, или подтверждения ранее отправленного запроса на закрытие соединения;
е) FIN-WAIT-2 – ожидание запроса на закрытие соединения со стороны чужой программы TCP;
ж) CLOSE-WAIT – ожидание запроса на закрытие соединения со стороны своего клиента;
з) CLOSING – ожидание подтверждения со стороны чужой программы TCP запроса о закрытии соединения;
и) LAST-ACK – ожидание запроса на закрытие соединения, ранее отправленного чужой программе TCP (запрос включал также подтверждение получения чужого запроса на закрытие соединения);
к) TIME-WAIT – ожидание, когда истечет достаточное количество времени и можно быть уверенным, что чужая программа TCP получила подтверждение своего запроса на закрытие соединения;
л) CLOSED – состояние полного отсутствия соединения.

При этом формируется флаг результата соединения [14]:

а) SF – нормальное SYN/FIN завершение;
б) REJ – соединение отклонено: инициирующий SYN вызвал RST в ответе;
в) S0 – состоние 0: инициирующий SYN встречен, но нет ответа;
г) S1 – состояние 1: обмен SYN'ами произведен, и больше ничего;
д) S2 – состояние 2: соединение установлено, инициатор закрыл свою сторону;
е) S3 – состояние 3: соединение установлено, ответчик закрыл свою сторону;
ж) S4 – состояние 4: SYN ACK встречен, но не было инициирующего SYN;
з) RSTOSn – соединение сброшено инициатором, когда оно было в состоянии n;
и) RSTRSn – соединение сброшено ответчиком, когда оно было в состоянии n;
к) SS – встречен SYN для частично закрытого соединения;
л) SH – соединение в состоянии 0 закрыто раньше, чем получен SYN ACK;
м) SHR – соединение в состоянии 4 закрыто раньше, чем встречен оригинальный SYN;
н) OOS1- SYN ACK не совпадает с инициирующим SYN;
о) OOS2 – инициирующий SYN передан заново с другим номером очереди.

В случае с пакетами протоколов UDP и ICMP, которые работают без установления логического соединения условно считаем соединением последовательный набор пакетов переданных между парой сокетов. Если хоть один сокет изменился, то значит соединение закончилось.

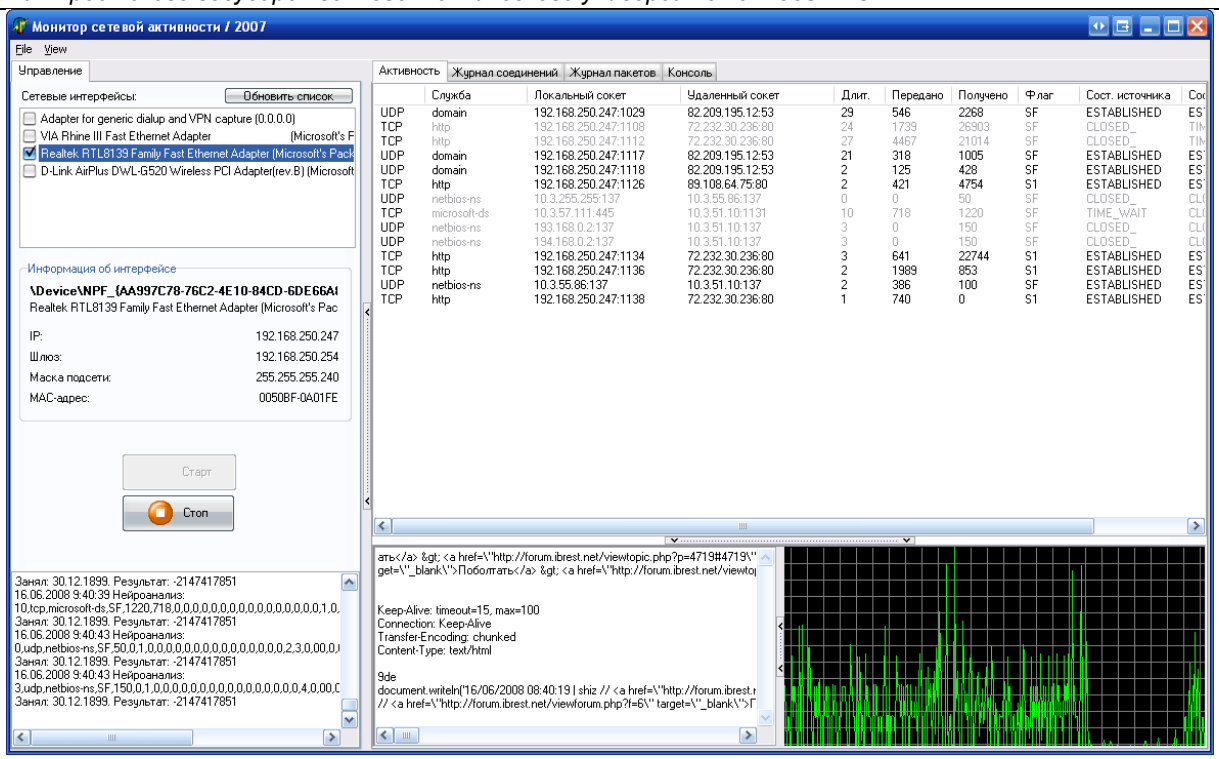

Рис. 7. *Монитор сетевой активности на базе WinPcap*

По завершении соединения формируется строка KDD [15] формата, которая может быть передана на обработку нейросетевому модулю.

Внешний вид программы представлен на рис. 7.

Достоинством данного сетевого монитора является комплексный подход к вычислению характеристик соединения. Недостаток – следствие достоинств – более высокая нагрузка на ресурсы системы вследствие высокого объема вычислительной работы и отслеживания состояний соединений своим алгоритмом.

7.2. Предварительная обработка. Данные, полученные из сети в виде отдельных пакетов, не могут в таком виде передаваться на обработку в блок анализатора. Необходим предварительный этап расчета заранее определенных параметров, отражающих характер сетевых соединений. В нашей работе используются 18 параметров сетевого соединения, хотя ничто не мешает увеличить их число. Все используемые нами параметры можно разбить на две основные категории: основополагающие характеристики TCP-соединения и временные характеристики.

Первую категорию параметров составляют такие параметры, которые можно получить из заголовков сетевых пакетов. К этой категории относятся: длительность соединения, количество переданных байт данных, состояние соединения (отслеживается по флагам SYN, FIN, RST) и т.п.

В свою очередь временные параметры отражают статистику соединений за определенный промежуток времени. Только после того как эти данные рассчитаны, они могут быть переданы далее на обработку в нейросетевой анализатор.

7.3. Анализатор. Следующим важным узлом, требующим отдельного рассмотрения, является анализатор.

Выполним нейросетевую постановку задачи. В этом случае в качестве средства анализа будет использоваться искусственная нейронная сеть. Архитектуры нейронных сетей, применяемые нами в области обнаружения вторжений, рассмотрены в предыдущих работах [16, 17]. В качестве анализатора можно использовать следующую модель классификации (рис. 8):

Этот классификатор состоит из рециркуляционной нейронной сети (RNN) и многослойного персептрона (MLP), которые соединены последовательно. Каждый образ, поступающий на вход модели, представлен 18-размерным вектором. На основании значения на выходе нейронной сети можно заключить, к какому из 5-ти классов сетевой активности относится входной вектор (DoS, U2R, R2L, Probe или Normal).

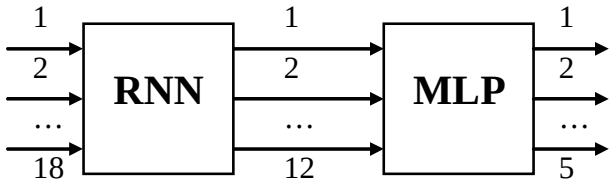

Рис. 8. *Базовая модель классификации*

Задачей RNN является сжатие входного 18-размерного вектора в выходной вектор меньшей размерности, который представляет из себя главные компоненты [18]. Многослойный персептрон осуществляет обработку сжатого пространства входных образов с целью распознавания класса атаки.

7.4. Средства управления и информирования. Средства управления включают в себя два основных модуля: монитор сетевого сегмента и модуль отображения результатов работы анализатора.

Первый модуль (рис. 5, рис. 7), представляющий собой монитор сетевого трафика, отображает информацию о регистрируемых пакетах (IP, TCP, ICMP, UDP и др.), отслеживает соединения в сегменте сети и выводит подробную информацию о каждом из них (такую как длительность, количество переданных данных в рамках соединения, его состояние и т.п.).

Второй модуль (рис. 9) отображает результаты анализа захваченного трафика на предмет поиска нежелательной активности, и в случае чего информирует администратора.

Заключение. Направления дальнейшего развития представленной модели системы IDS могут быть сформулированы только после проведения всесторонних экспериментов на реальных данных компьютерной сети, включающей большое количество станций пользователей и другое сетевое оборудование. Однако некоторые аспекты можно оговорить уже сейчас. Так, необходимо перенести уже имеющуюся версию для систем Windows на системы класса Unix, поскольку под управлением этой операционной системы чаще всего функционируют ключевые узлы компьютерной сети, тем более что возможность

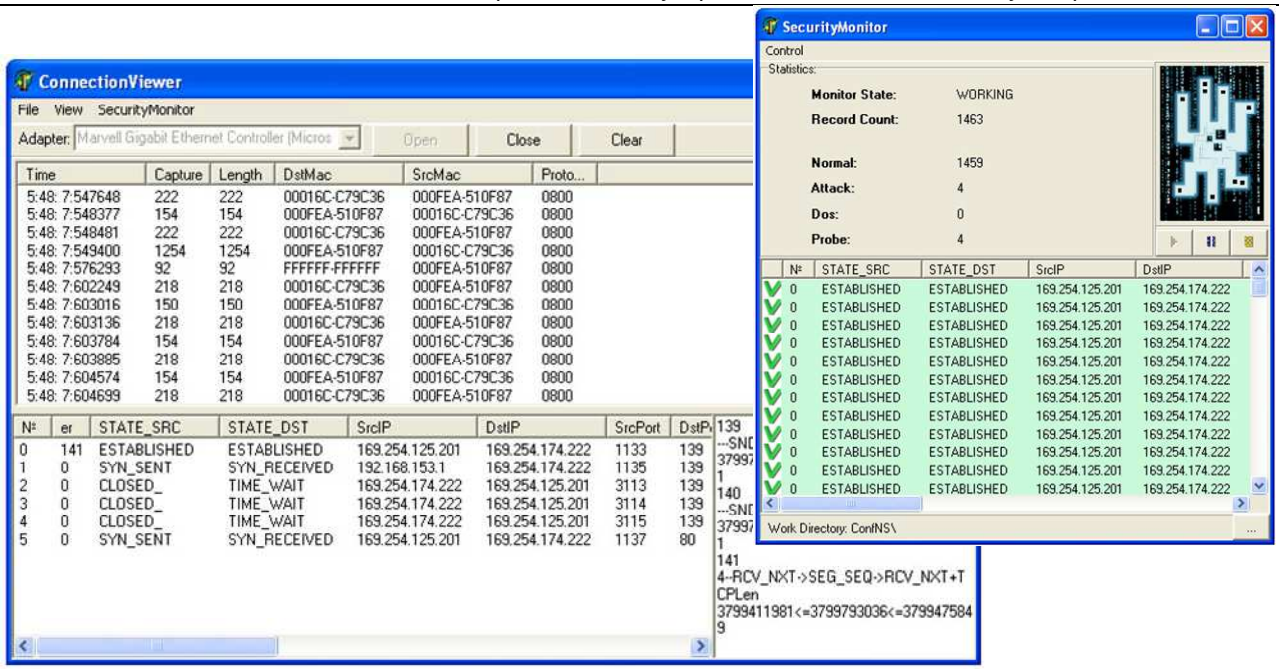

Рис. 9. *Вид диалоговых окон разрабатываемого ПО*

использования Pcap в той и другой среде значительно упрощает эту задачу. Дальнейшее развитие представленного ПО также видится в построении клиент-серверной архитектуры, позволяющей вести контроль состояния сети централизованно, получая информацию от сенсоров, расположенных в разных сегментах сети. Это позволит выполнять анализ функционирования сети как единого целого с учетом корреляции всех событий, происходящих в разных ее участках.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Web Application Security Consortium. [Электрон. ресурс]. - Режим доступа: www.webappsec.org.
2. D. Denning. An Intrusion Detection Model // In Proceedings of IEEE Conference on Security and Privacy - Oakland, USA, 1986. – P. 118-131.
3. Symantec Official Website. [Электрон. ресурс]. - Режим доступа: http://www.symantec.com.
4. ISS Web site. [Электрон. ресурс]. - Режим доступа: http://www.iss.net.
5. Snort Web site. [Электрон. ресурс]. - Режим доступа: http://www.snort.org.
6. P. A. Porras and P. G. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances // Proceedings of National Information Systems Security Conference - Baltimore MD, October 1997.
7. G. Vigna, R. Kemmerer. NetSTAT: a network-based intrusion detection approach // In Proceedings of the 14th Annual Computer Security Applications Conference – Scottsdale, AZ, Dec. 1998. – P. 25-34.
8. Норткат С., Новак Д. Обнаружение нарушений безопасности в сетях. 3-е изд. / Пер. с англ. – М.: Издательский дом “Вильямс”, 2003. – 448 с.
9. Безобразов С. Искусственные иммунные системы для защиты информации: применение LVQ сети // IX Всероссийская научно-техническая конференция «Нейроинформатика - 2007»: Сборник научных трудов. В 3-х частях. Ч. 2. - М.: МИФИ, 2007.
10. NT Kernel Resources. [Электрон. ресурс]. - Режим доступа: http://www.ntkernel.com.
11. WinPCap: the Free Packet Capture Architecture for Windows. [Электрон. ресурс]. - NetGroup, Politecnico di Torino (Italy), 2004. - Режим доступа: http://winpcap.polito.it.
12. K. M. Lee. Snoop Component Suite 2.0. [Электрон. ресурс]. - Режим доступа: http://www.snoopanalyzer.com.
13. RFC793. Протокол управления передачей (Transmission Control Protocol). Проект DARPA Internet. Спецификация протокола. – DARPA, 1981.
14. Z. Zhang. Data Mining Approach for Network Intrusion Detection / Z. Zhang. - Department of Computer Science, California State University, Sacramento, 2002.
15. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. - University of California, Irvine, 1999.
16. Головко В.А., Войцехович Л.Ю. и Шевеленков В.В. Нейросетевые принципы построения нейронных систем обнаружения атак на компьютерные сети // Вестник БрГТУ. Физика, математика, информатика. – 2006. - №5(41). – С. 14-19.
17. V. Golovko and L. Vaitsekhovich. Boosting Algorithms for Ensembles of Neural Network Classifiers in Intrusion Detection Domain // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2008) - Minsk, 2008. - P. 70-74.
18. Головко В.А. Нейронные сети: обучение, организация и применение. Кн. 4: Учеб. пособие для вузов / Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.

Материал поступил в редакцию 20.09.08

VOITSCEKHOVICH L.Y., GOLOVKO V.A., KOCHURKO P.A., VOITSCEKHOVICH G.Y. Intrusion detection system as a basic protection element of computer networks

High level of threads in computer networks has made a firewall and an Intrusion Detection System a necessary part of protected information environment. In the article we discuss classification of intrusion detection systems, their structure, the basic aspects of construction and deployment in a computer network; and also our developments in this area are submitted. The aim of the article is to prove the necessity of carrying out further researches and to offer a new approach for construction of intrusion detection systems.