УДК 004.8.032.26

Кочурко П.А., Гуменюк А.С.

Нейросетевая система обнаружения атак на базе совокупного классификатора

Введение. Системы обнаружения атак (СОА) являются неотъемлемыми элементами обеспечения информационной безопасности компьютерных сетей. В список решаемых ими задач входят обнаружение аномальной и злоумышленной сетевой активности, а также определение типа данной активности. От того, насколько качественно решены данные задачи, зависит, смогут ли система и персонал произвести необходимые действия по обеспечению сохранности информации и бесперебойному функционированию сети.

Среди требований к системам обнаружения атак можно выделить функционирование в реальном времени, адаптивность и способность к самоорганизации.

Первое подразумевает, что анализироваться должна текущая сетевая активность и обнаруживаться атака должна в момент совершения, в отличие от так называемого оффлайн-анализа журналов регистрации и файлов активности, при котором атаки обнаруживаются значительно позже того, как были совершены. Очевидно, что ценность подобного обнаружения значительно ниже.

Трафик сети в целом и каждого узла по отдельности достаточно разнообразен. Кроме того, сетевые атаки могут видоизменяться и производиться с различными вариациями. С учетом данных факторов система обнаружения атак должна быть способной адаптироваться к тому сетевому окружению, в котором функционирует, и обнаруживать не только известные, но и неизвестные, новые атаки.

Наиболее широко применяемые подходы к построению систем обнаружения атак – сигнатурные и статистические методы – обладают рядом недостатков. Сигнатурные методы, реализовывая технологию обнаружения злоупотреблений (известны атаки, всё остальное – нормальная активность), очень неустойчивы к зашумлению входных данных и модификации атак, а также плохо обнаруживают неизвестные атаки. Статистические методы, чаще всего реализовывая технологию обнаружения аномалий (известна нормальная активность, всё остальное – атаки) имеют хорошую базу для обнаружения неизвестных атак, но не могут сами по себе с достаточным качеством распознавать тип атаки.

Доказано [1, 2], что наилучшего качества обнаружения и распознавания как известных, так и неизвестных атак можно добиться при объединении технологий обнаружения аномалий и злоупотреблений в рамках одной системы. Именно такой подход применен при построении нейросетевой системы обнаружения атак (НСОА) на базе совокупного классификатора. Он состоит из набора частных детекторов, каждый из которых представляет собой рециркуляционную нейронную сеть (РНС). Рециркуляционные нейронные сети могут использоваться как для обнаружения аномалий [3], так и для обнаружения злоупотреблений [4]. А учитывая способность искусственных нейронных сетей к функционированию на зашумленных данных, обобщению, РНС являются хорошим механизмом для построения СОА, отвечающей описанным выше требованиям.

Для тестирования предложенной НСОА проведен ряд экспериментов. Предложенные алгоритмы обосновываются результатами экспериментов на базе данных 199 KDD Cup [3–5]. Она представляет собой информацию о TCP-соединениях реальной локальной вычислительной сети Air Force's Research Laboratory из Рима, штат Нью-Йорк, на основе которых были смоделированы две недели сетевого трафика, включавшего неизвестные и известные атаки. Каждое соединение описывается 41 параметром – основными параметрами (длительность, протоколы, и т.д.), параметрами данных (количество логинов, системных обращений, и т.д.) и статистическим (количество подключений к данному сервису за последнее временное окно, и т.д.). Все соединения в базе данных подразделяются на пять классов: нормальные соединения; DOS-атаки (отказ в обслуживании); probe-атаки (сканирование портов и др.); U2R-атаки (неавторизованное получение привилегий root на данной системе); R2L-атаки (неавторизованный доступ с удалённой системы). Всего – 22 типа атак и нормальные соединения.

Разработанный макет НСОА протестирован в реальном сетевом окружении, в котором наряду с нормальной сетевой активностью производились атаки классов DoS (synflood, udpflood) и Probe (tcpscan). Результаты тестирования показали, что предложенная архитектура НСОА способна обнаруживать и распознавать как известные, так и новые атаки с достаточно высоким качеством.

Статья организована следующим образом. В разделах 2–3 описывается архитектура НСОА и алгоритмы ее обучения, настройки и функционирования. В разделах 4–5 описано тестирование макета НСОА в реальном времени, представлены результаты, сделаны выводы и определены дальнейшие направления развития.

1. Частные нейродетекторы и совокупный классификатор. Обнаружение аномальной деятельности характеризуется поиском сетевой активности, отличающейся от нормального поведения субъектов системы. Вследствие этого необходимо знание характеристик нормального поведения – нормальных сетевых соединений. Нейросетевой подход к обнаружению аномалий должен реализовывать автоматическое получение этих характеристик исходя из обычной сетевой активности субъекта.

Рециркуляционные нейронные сети отличаются от других ИНС тем, что информация, подающаяся на вход, в том же виде восстанавливается на выходе. В процессе обучения весовые коэффициенты РНС настраиваются таким образом, чтобы минимизировать среднеквадратичную ошибку для всех тренировочных входных векторов. Итогом такого обучения станет то, что в процессе функционирования РНС подаваемые на вход вектора будут восстанавливаться на выходе тем более точно, чем больше они схожи с векторами из тренировочного набора. Далеко отстающие вектора, в свою очередь, будут восстанавливаться недостаточно корректно. Как видим, данная ситуация идеально подходит для применения РНС в качестве детекторов аномалий: если обучение производить на нормальной сетевой активности, то РНС автоматически инкапсулирует в себе информацию о профиле нормального поведения субъекта.

Численная характеристика, которая позволяет судить о том, насколько данный входной вектор «похож» или «не похож» на вектор из тренировочного набора – ошибка реконструкции вектора:

$$E^k = \sum_{j=1}^{N(X)} (\bar{X}_j^k - X_j^k)^2 , \qquad (1)$$

где $N(X)$ – количество параметров во входном векторе X (ранг первого и последнего слоёв РНС). При этом, чем меньше ошибка реконструкции (1), тем больше входной вектор похож на нормальный. Если $E^k > T$, где T – некий заданный для данной РНС порог, то соединение признаётся аномалией, или атакой, иначе – нормальным соединением.

Данную методику определения принадлежности входного вектора к одному из двух классов можно применить и прямо противоположным образом. Если при обучении детектора аномалий использовались нормальные векторы, которые восстанавливались в себя, и на основании этого делался вывод об их принадлежности к классу «нормальных», то, обучая детектор на соединениях-атаках, которые

***Кочурко П.А.**, ст. преподаватель кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

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

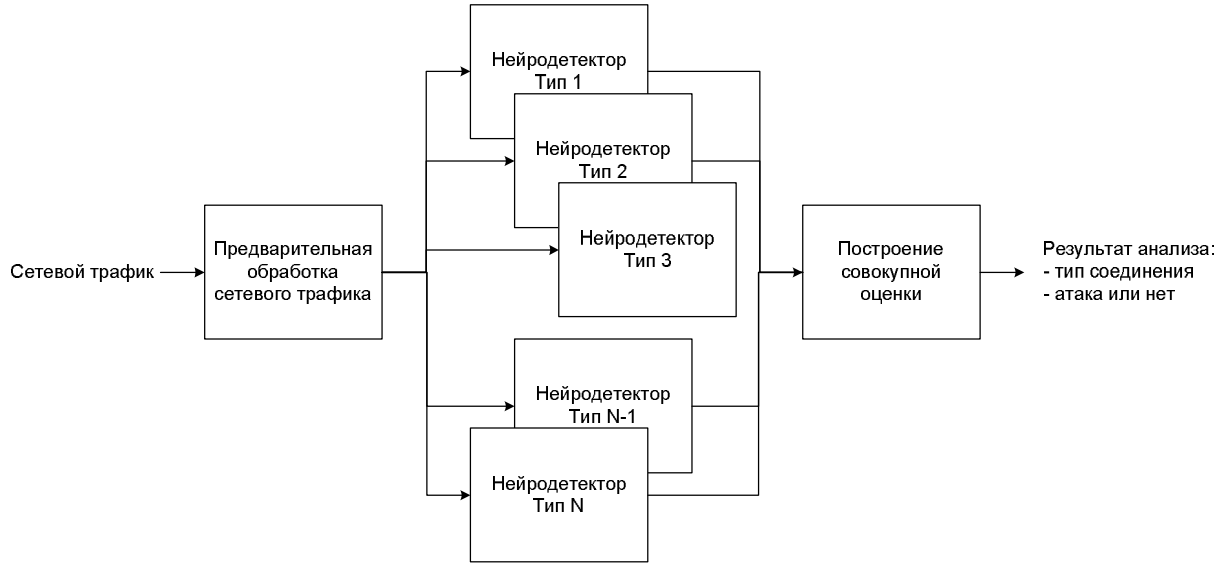

Рис. 1. Структура совокупного классификатора

должны восстановиться в себя, можно делать вывод об их принадлежности к классу «атаки». Таким образом, если в процессе функционирования данного детектора ошибка реконструкции (1) превышает определённый порог, то данное соединение можно отнести к классу «не-атак», то есть нормальных соединений. Так как обучение ведётся на векторах-атаках, то данный подход реализует именно технологию обнаружения злоупотреблений, и оправданно его употребление совместно с подходом, реализующим технологию обнаружения аномалий.

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A), или ко второму (класс $\bar{A}$), которому соответствуют далеко отстающие вектора:

$$\begin{cases} X^k \in A, & \text{если } E^k \le T, \\ X^k \in \bar{A}, & \text{если } E^k > T. \end{cases} \qquad (2)$$

Например, база данных KDD включает соединения нормальные, а также атаки двадцати двух типов, которые радикально отличаются друг от друга. Поэтому в данном случае было бы целесообразно обучить детекторы для каждого из типов отдельно, не объединяя все типы атак в единое целое (см. рис. 1).

Таким образом, выходной информацией каждого частного нейродетектора является ошибка реконструкции (1) и порог T, показывающие, насколько вероятна принадлежность входного образа именно к данному типу. Для получения оценки достаточно отмасштабировать ошибку реконструкции по порогу:

$$\begin{cases} X^k \in A_i, & \text{если } \delta_i^k \le 1, \\ X^k \in \bar{A}_i, & \text{если } \delta_i^k > 1, \end{cases} \qquad (3)$$

где $\delta_i^k = \dfrac{E_i^k}{T_i}$ – относительная ошибка реконструкции. При этом, чем меньше δ_i^k, тем более вероятна принадлежность входного образа X^k к классу A_i.

Совокупный классификатор, реализуя технологию обнаружения злоупотреблений, может строиться путём обучения частных нейродетекторов на базах образов различного типа с последующей настройкой порогов. Однако в таком режиме теряются преимущества обнаружения аномалий.

Учитывая возможность наращивания архитектуры новыми детекторами, более естественным вариантом является следующий режим работы (см. рис. 2) совокупного классификатора: первый детектор обучается на нормальной сетевой активности, а все соединения, признанные аномалиями, формируют обучающую выборку для нового детектора. Аномалиями признаются все соединения, которые ни один частный нейродетектор не признал «своим», то есть для которых все относительные ошибки реконструкции больше 1. Новые нейродетекторы обучаются по мере набора достаточного количества образов в обучающей базе.

Для улучшения качества распознавания типов соединений по добавлении нового детектора производится настройка порогов. Для этого используются генетический алгоритм, функцией соответствия которого является процент правильной классификации образов обучающих выборок, а также алгоритм тонкой настройки порогов [6].

2. Структура НСОА. Представленный подход к обнаружению сетевых атак базируется на анализе сетевого трафика. Система может анализировать как трафик узла сети, так и сегмента сети, в зависимости от расположения (см. рис. 3).

Каждый из изображенных на рисунке вариантов размещения НСОА имеет свои плюсы и минусы. Так, НСОА на шлюзе защищает всю сеть в целом от внешних угроз, но никак не сможет обнаружить атаку с одного внутреннего узла на другой. НСОА на выделенном сервере может анализировать весь трафик сети, для чего необходимо наличие коммутирующего оборудования с т.н. зеркалирующими портами, которые отсылают копию всех пакетов на сервер анализа. Защищая как всю сеть, так и узлы по отдельности, такая система очень требовательна к ресурсам, в том числе коммутирующего оборудования – нагрузка на сеть значительно повышается. Реализация НСОА на каждом отдельном узле сети позволяет защитить данный узел от угроз из внешней и внутренней сетей, но несколько повышает загрузку системы.

Интеллектуальная система, построенная согласно представленному подходу, может успешно функционировать в любом из вариантов, так как нюансы размещения НСОА скрываются от всей системы уже на этапе предварительной обработки данных.

На рис. 4 представлена структура нейросетевой системы обнаружения атак. Целесообразно разделение функций между несколькими программными модулями: это позволяет повысить эффективность их разработки и поддержки. Система состоит из следующих модулей: модуль предварительной обработки данных, модуль обучения и настройки частных нейродетекторов, модуль частного детектора, модуль настройки совокупного классификатора, модуль распознавания атаки, модуль генерации детекторов.

Макет системы реализован для операционной системы GNU/Linux с использованием программного обеспечения с открытым исходным кодом BroIDS, mawk, bash, tee, gcc, распространяемого по лицензии GNU Public License.

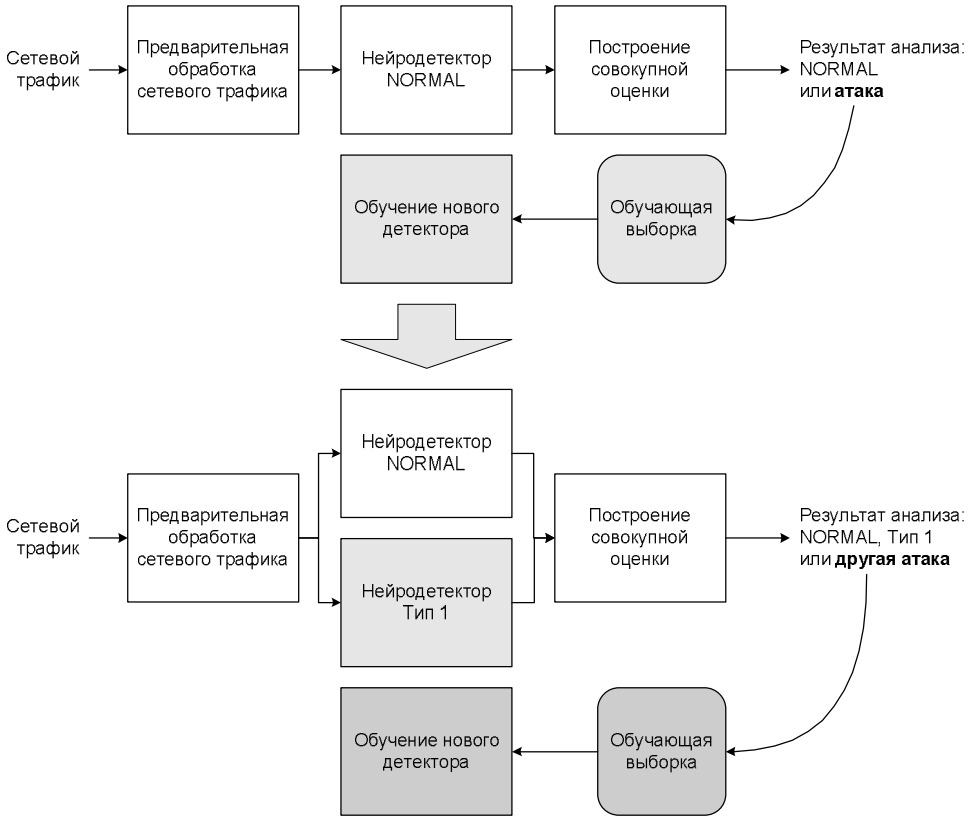

Рис. 2. Режим работы совокупного классификатора с генерацией нового детектора

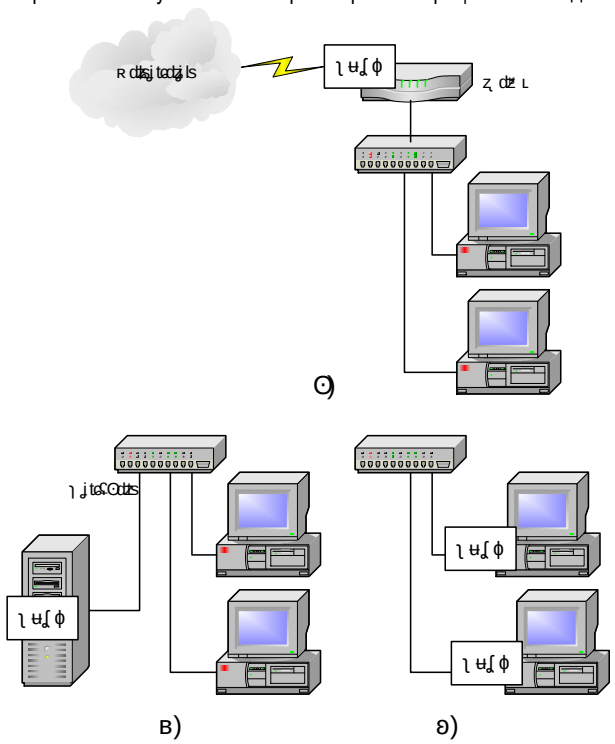

Рис. 3. Варианты расположения НСОА уровня сети и уровня узла
а) на шлюзе между внутренней и внешней сетью; б) на выделенном сервере локальной сети; в) на узле сети

Модуль предварительной обработки данных. Независимо от того, поступает на сетевой интерфейс компьютера только трафик, адресованный данному узлу, зеркалируется трафик всего сегмента сети или трафик проходит как через шлюз, НСОА получает записи о всех сетевых соединениях, сформированные с помощью Bro IDS [7]. Bro представляет собой тонко настраиваемую систему обнаружения атак с открытым исходным кодом, которая выполняет модифицированный скрипт получения записей о соединениях, включающих следующие поля: временной штамп; длительность соединения в секундах; IP-адрес источника соединения; IP-адрес пункта назначения соединения; наименование используемой службы; номер порта на источнике; номер порта на пункте назначения; количество переданных байт; флаг результата соединения.

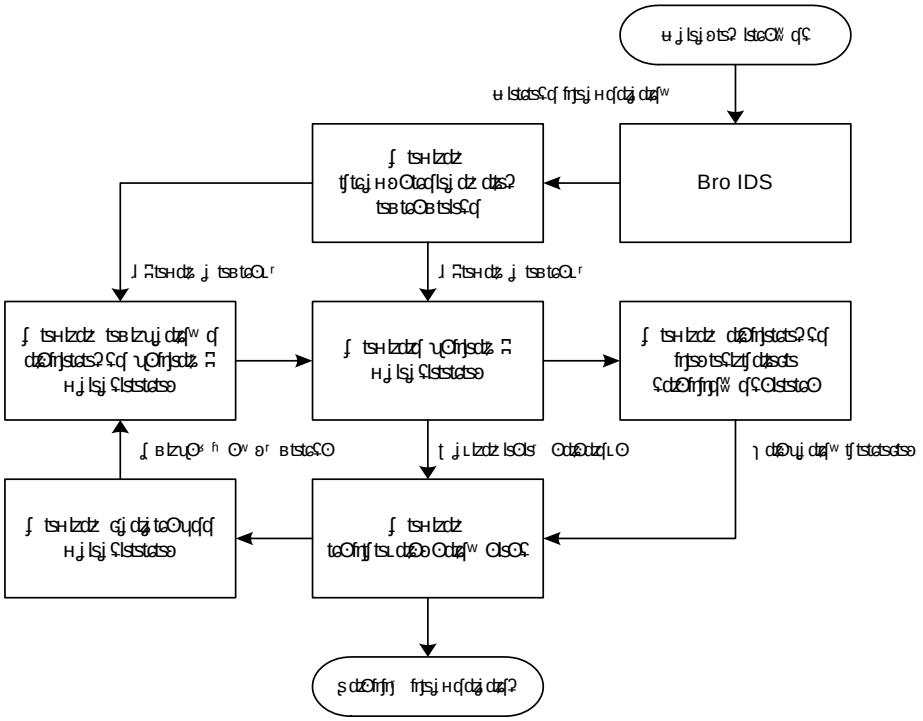

Рис. 4. Структура нейросетевой системы обнаружения и распознавания атак

Таблица 1. Исходные данные для анализа

№	Параметры, подаваемые на вход РНС
–	временной штамп (не будет подаваться на вход РНС, а использоваться для идентификации соединения)
1	длительность соединения в секундах
2	используемый протокол
3	используемая служба прикладного уровня
4	количество отправленных байт
5	количество полученных байт
6	флаг TCP-соединения
7	количество соединений к текущему хосту за последние 2 секунды
8	количество соединений к текущей службе за последние 2 секунды
9	процент соединений к данной службе среди всех обращений
10	процент соединений к другим службам
11	количество соединений к удаленному хосту в течение последних 2 секунд
12	количество соединений к удаленной службе в течение последних 2 секунд
13	процент соединений к данной удаленной службе
14	процент соединений к другим удаленным службам
15	процент соединений соединений к данному хосту при текущем номере порта источника
16	процент соединений к данной службе от разных хостов

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.

Если HCOA функционирует на уровне узла, то в списке будут встречаться только соединения данного компьютера; если на уровне сети — то соединения различных узлов. Bro единообразно формирует строки соединений, которые передаются по конвейеру на модуль предварительной обработки.

Далее полученные строки соединений последовательно обрабатываются несколькими скриптами на языке awk, которые формируют записи, аналогичные записям базы KDD, после производят кодирование категориальных параметров и нормализацию входных данных. Итогом работы становятся строки чисел, соответствующих параметрам, перечисленным в таблице 1.

Модуль обучения и настройки частных нейросетевых детекторов. Каждый частный детектор представляет собой нелинейную рециркуляционную нейронную сеть с одним скрытым слоем. Алгоритм обучения и функционирования РНС реализован на языке С с использованием компилятора gcc. Благодаря этому программа обладает быстродействием, достаточным для оценки функционирования макета системы в условиях реального времени.

После обучения РНС, производимого по методу послойного обучения, выбирается начальное значение порога для частного детектора. Порог устанавливается равным величине, при которой 5% образов обучающей выборки дают ошибку реконструкции выше порога. После такой настройки порога нейродетектор способен в реальном времени определять принадлежность к своему классу с точностью до 95%.

Время и качество обучения напрямую зависит от количества образов в обучающей выборке. При 500 соединениях время обучения около 10 секунд, при этом, например, среднеквадратичная ошибка на выборке synflood достигла значения 0.001, а на нормальных соединениях — 0.0035. В таблице 2 показаны результаты настройки порогов для детекторов трёх классов при подаче на вход детектора образов из обучающей выборки.

Таблица 2. Результаты настройки порогов нейродетекторов

Наименование класса A_i	DR_i, %	Порог T_i
normal	94,6	0,819415
tcpscan	94,8	0,835775
synflood	94,8	0,785963

Модуль частных нейросетевых детекторов. Обученные модулем обучения и настройки нейросетевые детекторы производят восстановление входного образа на выходном слое РНС, вычисляют относительную ошибку реконструкции и делают вывод о принадлежности входного образа к своему классу. Чем меньше ошибка реконструкции, тем более вероятна принадлежность к данному классу.

Результатом работы частного нейродетектора являются строки, содержащие временную метку для идентификации конкретного соединения; наименование класса, за который отвечает данный детектор; абсолютную ошибку реконструкции входного образа; относительная ошибка реконструкции входного образа, которая и будет использоваться для принятия решения о принадлежности образа к данному классу. Если относительная ошибка реконструкции больше 1, то образ сохраняется для возможного дальнейшего участия в обучении нового детектора.

В таблице 3 отражены результаты анализа частными нейродетекторами соединений трёх классов. На каждый детектор подавались соединения двух других классов, при этом успешным в таком случае считается принятие детекторами решения о непринадлежности данных соединений к их классам.

Таблица 3. Качество обнаружения аномалий частными детекторами

Реальный \ Предсказанный	normal	tcpscan	synflood
normal		100,00%	31,00%
tcpscan	98,20%		84,00%
synflood	99,40%	94,40%	

В начале своего функционирования НСОА может располагать только одним источником данных: нормальным сетевым трафиком. То есть — соединениями класса normal. Обучив на этом трафике нейродетектор класса normal, система начинает обнаруживать аномалии при попытках сетевых атак. Так, при атаке класса tcpscan система все соединения правильно определяет как аномалию (см. таблицу 3) и сохраняет для обработки модулем генерации детекторов. Если же производится атака synflood, то только третья часть соединений будет правильно распознана, как аномалия, чего впрочем хватит для сбора данных для обучения нового детектора.

Как видно из таблицы 3, при подаче образов класса synflood на детектор класса normal результат обнаружения аномалии достаточно низок — всего 31%. При этом детектор класса synflood обнаруживает аномалии в соединениях класса normal с точностью 99,4%. Объединив эти детекторы в одну систему в соответствии с разделом 3.4, можно получить значительный прирост качества распознавания классов.

Тем не менее, можно сделать вывод, что качество обнаружения аномалий, а значит — и результат распознавания неизвестных атак частным детектором normal достаточно высок.

Модуль генерации детекторов. Данный модуль анализирует результат функционирования всех частных нейросетевых детекторов. В случае, если ни один из них не определил принадлежность входного образа к своему классу, то он сохраняется в буфере. При накоплении системой заданного количества аномальных образов в течение атаки, либо при истечении заданного периода времени после получения последнего аномального образа модуль генерации детекторов формирует из созраненных в буфере образов обучающую выборку, которую передает модулю обучения и настройки нейродетекторов.

Модуль настройки совокупного классификатора. Сразу после появления в системе нового частного нейродетектора модуль настройки совокупного классификатора, используя в качестве входных образов обучающие выборки всех входящих в него детекторов, производит подбор наилучших порогов. Цель — сделать качество распознавания классов максимальным. Для этого используется стандартный генетический алгоритм, реализованный с помощью библиотеки libGA [8]. Количество хромосом устанавливается равным количеству частных нейродетекторов, а в качестве функции соответствия выбирается подсчет процента верно классифицированных образов.

Тонкая настройка классификатора в соответствии с [5] может производиться либо вместо генетической настройки, либо после неё. В процессе тонкой настройки подбираются такие пороги, которые дают максимальное качество распознавания классов на образах обучающих выборок детекторов.

В таблице 4 показано качество распознавания классов соединений совокупными классификаторами до настройки классификатора ($DR_{нач}$), после генетической настройки ($DR_{ген}$), после тонкой настройки ($DR_{тон}$), после генетической и тонкой настроек вместе ($DR_{ген+тон}$).

Таблица 4. Результаты настройки совокупных классификаторов

Состав классификатора	$DR_{нач}$, %	$DR_{ген}$, %	$DR_{тон}$, %	$DR_{ген+тон}$, %
normal+tcpscan	99	99	99	99
normal+synflood	97,3	99,7	99,7	99,7
normal+tcpscan+synflood	95,2	95,4	95,4	95,4

Как видно из таблицы 4, качество распознавания при любом из методов настройки улучшается, причем равнозначно.

Модуль распознавания атак. Модуль распознавания атак накапливает результаты анализа входного образа всеми на данный момент функционирующими частными нейродетекторами. Стоит отметить, что детекторы работают параллельно, потому порядок выдачи ими строк результата по умолчанию неопределён. Поэтому модуль накапливает все результаты в едином массиве, идентифицируя соединения по временным меткам. Как только для одного соединения получены результаты от всех детекторов, сравниваются относительные ошибки и выбирается класс, к которому вероятнее всего относится данное соединение. При этом, если все относительные ошибки больше 1, то делается вывод о том, что, возможно, соединение не принадлежит ни к одному из данных классов. Режим распознавания нового класса может быть отключен, и тогда даже среди относительных ошибок выше 1 будет выбрана наименьшая и сделан вывод о принадлежности к одному из классов.

Выходные данные модуль распознавания атак формирует в виде строк, содержащих вывод о принадлежности соединения к одному из известных классов, либо о неизвестном классе; относительные ошибки реконструкции на каждом из детекторов; в качестве дополнительной информации – первоначальная строка соединения формата BroIDS.

3. Тестирование НСОА. Для тестирования НСОА был выбран узловой вариант реализации системы обнаружения атак (см. рис. 3, в). Как сказано выше, алгоритмы функционирования в различных вариантах ничем друг от друга не отличаются, потому данный вариант можно считать репрезентативным.

В локальной сети (см. рис. 5) из двух рабочих станций на одной установлена НСОА, вторая выполняет роль злоумышленника. Нормальная сетевая активность «жертвы» включает в себя обычный интернет-серфинг по протоколам http, ftp и другим, dns-запросы, общение в IM-чатах, загрузку медиа-контента. На подобной активности обучался частный нейродетектор класса normal.

Сетевые атаки производились с компьютера-«злоумышленника» с помощью специализированных программ, распространяемых в сети Интернет. Производились следующие атаки:

- **tcpscan** – атака класса probe, сканирует порты жертвы по протоколу tcp;

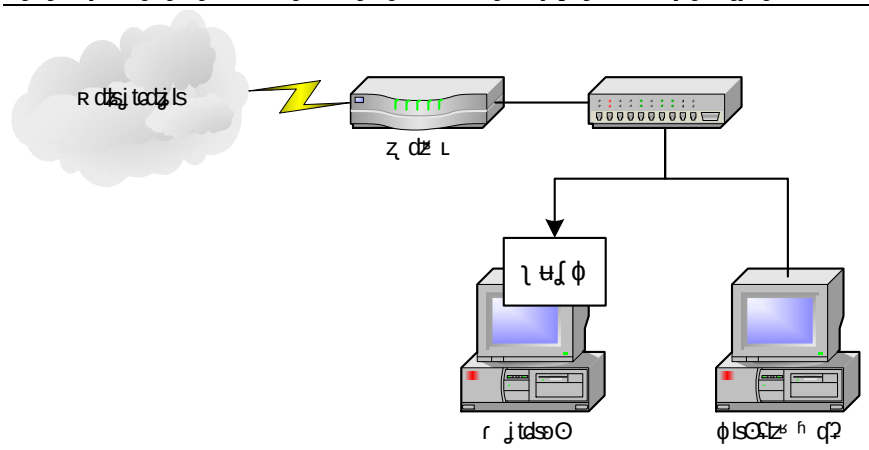

Рис. 5. Экспериментальное сетевое окружение

- **synflood** – атака класса DoS, потоком tcp-пакетов с установленным флагом syn заполняет приемный буфер жертвы;
- **udpflood –** атака класса DoS, затапливает жертву udp-пакетами, жертва вынуждается отвечать icmp-unreach пакетами, что является собой дополнительную нагрузку на неё.

В таблице 5 представлены результаты распознавания соединений, составлявших обучающие выборки (по 500 каждого класса), модулем распознавания атак в режимах без генерации нового класса атак и с генерацией нового класса. В случаях, когда в состав HCOA не входил детектор того класса, который подавался на вход, успешным результатом считалось обнаружение атаки нового класса.

Таблица 5. Тестирование совокупных классификаторов на образах обучающей выборки

Состав классификатора	Режим работы	DR_{normal}, %	$DR_{tcpscan}$, %	$DR_{synflood}$, %
normal+tcpscan	без нового	98,4	99,6	–
	с новым	97,6	95,2	25,4
normal+synflood	без нового	99,4	–	100
	с новым	59,8	94	98
normal+tcpscan+synflood	без нового	98,2	94	94
	с новым	91,4	91,2	94

Как видно из результатов распознавания, метод совокупного классификатора успешно реализует как технологию обнаружения злоупотребления, так и обнаружения аномалий.

В режиме работы без генерации нового класса модуль распознаёт известные классы с высочайшей степенью точности (от 94% до 100%). Однако неизвестные атаки в таком режиме в полном соответствии с принципами обнаружения злоупотреблений не распознаются.

При включении режима генерации нового детектора, то есть добавлении к обнаружению злоупотреблений еще и обнаружения аномалий, несколько ухудшается качество распознавания известных классов. Тем не менее, появляется возможность обнаружения соединений неизвестных классов и формирования обучающей выборки для нового детектора.

Как видим, качество обнаружения неизвестных атак разнится для различных классификаторов, однако даже такого показателя достаточно для формирования обучающей выборки для третьего детектора. После его обучения, настройки и запуска совокупного классификатора с новым детектором в составе, модуль начинает распознавать соединения более качественно за счет применения технологии обнаружения злоупотреблений.

В таблице 6 представлены ошибки первого (FN) и второго рода (FN) при решении задачи обнаружения атаки.

Таблица 6. Качество обнаружения атак HCOA на образах обучающей выборки

	FN, %	FP, %
normal+tcpscan		
Без генерации нового класса		1,60
На известных атаках	0,40	
На неизвестных атаках	87,60	
С генерацией нового класса		2,40
На известных атаках	0,00	
На неизвестных атаках	63,00	
normal+synflood		
Без генерации нового класса		0,60
На известных атаках	0,00	
На неизвестных атаках	90,80	
С генерацией нового класса		40,2
На известных атаках	0,00	
На неизвестных атаках	0,00	
normal+tcpscan+synflood		
Без генерации нового класса		1,80
На известных атаках	0,04	
С генерацией нового класса		**8,60**
На известных атаках	**0,00**	

Как видно из данной таблицы, качество обнаружения известных атак очень велико – одинаково малы ошибки первого и второго рода. Если же необходимо распознавание и неизвестных атак, то необходимо включать режим работы с генерацией нового класса, за что приходится жертвовать увеличением количества ложных срабатываний.

HCOA может функционировать не только в т.н. off-line режиме, то есть анализе ранее сохраненных файлов, как было произведено выше. Основным режимом функционирования является работа в реальном времени с анализом текущего сетевого трафика. Каждое сетевое соединение анализируется сразу после своего завершения. Благодаря тому, что одна атака обычно состоит из множества последовательных соединений [93], она может быть обнаружена уже в процессе своего совершения.

Реализация HCOA включает в себя функцию журналирования трафика. Благодаря этому после работы в режиме реального времени совокупного классификатора из трех нейродетекторов тот же самый трафик в офф-лайн-режиме был проанализирован другими вариантами HCOA из одного и двух нейродетекторов.

В таблицах 7 и 8 представлены результаты распознавания и обнаружения атак HCOA в реальном времени всеми вариантами HCOA. На вход подавался трафик, на котором детекторы не обучались. Кроме того, здесь добавлены соединения атаки udpflood, которых не было ранее. Как и в предыдущем случае, когда в состав HCOA не входил детектор того класса, который подавался на вход, успешным результатом считалось обнаружение атаки нового класса.

Таблица 7. Качество распознавания типов атак в реальном времени

Состав классификатора	Режим работы	DR_{normal}, %	$DR_{tcpscan}$, %	$DR_{synflood}$, %	$DR_{udpflood}$, %
normal	с новым	98,78	99,31	0,00	99,36
normal+tcpscan	без нового	99,02	99,70	–	–
	с новым	98,78	98,67	0,00	99,95
normal+synflood	без нового	99,26	–	85,27	–
	с новым	92,17	98,71	85,27	48,87
normal+tcpscan+synflood	без нового	98,77	98,03	94,88	–
	с новым	91,19	98,03	94,88	48,42

Таблица 8. Качество обнаружения атак в реальном времени

	FN, %	FP, %
normal		
С генерацией нового класса		1,22
На неизвестных атаках	7,68	
normal+tcpscan		
Без генерации нового класса		0,98
На известных атаках	0,20	
На неизвестных атаках	100,00	
С генерацией нового класса		1,22
На известных атаках	0,26	
На неизвестных атаках	10,70	
normal+synflood		
Без генерации нового класса		0,73
На известных атаках	14,72	
На неизвестных атаках	33,32	
С генерацией нового класса		7,82
На известных атаках	14,72	
На неизвестных атаках	0,10	
normal+tcpscan+synflood		
Без генерации нового класса		1,22
На известных атаках	1,09	
На неизвестных атаках	48,44	
С генерацией нового класса		**8,81**
На известных атаках	**1,09**	
На неизвестных атаках	**0,01**	

Как видно из таблиц 7 и 8, совокупный классификатор в реальном времени способен качественно обнаруживать и распознавать сетевые атаки, анализируя соединения, которых не было в обучающей выборке.

Результаты тестирования в реальном времени практически полностью повторяют результаты анализа обучающих выборок. Столь же качественно обнаруживаются и распознаются известные атаки, а в режиме с генерацией нового класса – и неизвестные атаки.

Проблемная для распознавания в качестве нового класса атака synflood начинает отлично распознаваться после обучения для нее соответствующего нейродетектора. Впрочем, это приводит к обратному результату для атаки udpflood, вследствие того, что она наполовину состоит из соединений, полностью аналогичных synflood. Однако даже то, что каждое второе соединение распознается как чуть-чуть другая атака, не отражается негативно на качестве обнаружения атаки – это всё равно атака и всё равно атака на отказ в обслуживании.

Как уже говорилось выше, основная часть макета НСОА – частные нейродетекторы – реализованы на языке С, для того чтобы можно было оценить быстродействие системы. Измерение показало, что анализ одним детектором одного соединения занимает в среднем 24 микросекунды, следовательно, совокупный классификатор из трёх нейродетекторов тратит на анализ одного соединения в среднем 72 микросекунды. Таким образом, без учета потерь на ввод-вывод и предварительную обработку данных, пропускная способность совокупного классификатора равняется 13888,9 соединений в секунду, этого достаточно для успешного решения задачи обнаружения и распознавания сетевых атак в реальном времени даже при большинстве DoS-атак. Однако стоит заметить, что данный макет не предназначен для промышленного использования, поскольку ввод-вывод и предварительная обработка для большей наглядности реализованы на интерпретируемом языке awk, а следовательно, слишком сильно замедляют работу системы.

Заключение. Подход к построению систем обнаружения атак, представленный в данной работе, отличается от аналогов высоким уровнем обнаружения и распознавания как известных, так и новых сетевых атак. НСОА, базирующаяся на совокупном классификаторе из частных нейродетекторов, обладает свойствами адаптивности и самоорганизации и способна реализовывать свои основные функции в реальном времени.

Перспективным направлением работ является разработка НСОА, использующей для анализа не данные о каждом конкретном соединении, а интегральные характеристики трафика. Подобный подход позволит использовать НСОА в сетях с высокой загрузкой, например, на магистральных каналах или в точках обмена трафиком.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Giacinto, G. Selection of image classifier / G. Giacinto, F. Roli, G. Fumera // Electron. – 2000. – Vol. 26, №5. - pp. 420-422.
2. Xu, L. Methods for combining multiple classifiers and their applications to handwriting recognition / L. Xu, A. Krzyzak, C. Y. Suen // IEEE Trans. Syst. Man Cybernitics. – 1992. - №22. - pp. 418-435.
3. Кочурко, П.А. Нейросетевой детектор аномалий / П.А. Кочурко // Известия Белорусской инженерной академии. – 2005. – №1(19)/2. – С. 78–81.
4. Кочурко, П.А. Совокупность детекторов на основе рециркуляционных нейронных сетей для распознавания класса сетевых атак / П.А. Кочурко // Вестник Брестского государственного технического университета. – 2005. – №5: Физика, математика, информатика. – С. 61–66.
5. Кочурко, П.А. Совокупный детектор атак на основе нейронных сетей / П.А. Кочурко // Инженерный вестник. – 2006. – №1(21)/1. – С. 90–96.
6. Кочурко, П.А. Настройка порогов нейросетевых детекторов для распознавания классов сетевых атак / П.А. Кочурко // Современные проблемы математки и вычислительной техники: материалы VI Республиканской научной конференции молодых учёных и студентов, Брест, 26-28 ноября 2009 г. / Брест. гос. техн. ун-т. – Брест, 2009.
7. Bro Intrusion Detection System [Electronic resourse] – Lawrence Berkeley National Laboratory, 2010. – Mode of access: http://bro-ids.org. – Date of access: 09.11.2010.
8. Corcoran, A.L. and Wainwright, R.A. LibGA: A User-Friendly Workbench for Order-Based Genetic Algorithm Research / A.L. Corcoran, R.A. Wainwright // The 1993 ACM/SIGAPP Symposium on Applied Computing (SAC 93): proceedings, Indianapolis, Indiana, February 14–16. – Indianapolis, 1993.

Поступила в редакцию 10.11.10

KOCHURKO P.A., GOLOVKO V.A. Construction neuronetwork of system of detection and recognition of attacks

The questions of construction neuronetwork of system for the decision of tasks of detection and recognition of types of attacks are considered on the basis of the cumulative qualifier from private neuronetwork of detectors distinguished ability to self-organizing and detection of unknown attacks. The modular structure of system is described, the algorithms of functioning and ways of realization are resulted. The experimental testing of the constructed breadboard model of system in real time is made.