На правах рукописи

ЖУЛЬКОВ Евгений Владимирович

ПОСТРОЕНИЕ МОДУЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ КЛАССОВ СЕТЕВЫХ АТАК

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург - 2007

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования “Санкт-Петербургский государственный политехнический университет”.

Научный руководитель:

Кандидат технических наук, профессор Платонов Владимир Владимирович

Официальные оппоненты:

доктор технических наук, профессор Гаценко Олег Юрьевич

кандидат технических наук, доцент Шишкин Владимир Михайлович

Ведущая организация:

ГОУ “Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича”

Защита состоится « » _____ 2007 г. в ____ часов на заседании диссертационного совета Д 212.229.27 при ГОУ ВПО
“Санкт-Петербургский государственный политехнический университет”
по адресу 195251, Санкт-Петербург, Политехническая 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в фундаментальной библиотеке
ГОУ ВПО “Санкт-Петербургский государственный политехнический университет”.

Автореферат разослан « » _____ 2007 г.

Ученый секретарь диссертационного совета Платонов В.В.

Общая характеристика работы

Как следует из ежегодного отчета Федерального Бюро Расследовании США, освещающего статистику компьютерных преступлений, в этом году сократилось количество атак на компьютеры и компьютерные системы. Несмотря на это, общая сумма ущерба среди интервьюируемых организаций составляет более 66 миллионов долларов США, значительная часть которых пошла на возмещение ущерба от сетевых атак. Эти и другие данные подчеркивают актуальность задачи построения защищённых сетей.

Для защиты сетей существует большое количество программно-аппаратных средств защиты информации, лидирующие позиции среди них занимают межсетевые экраны. Для построения защищённого участка сети недостаточно использования только межсетевых экранов, так как эта технология позволяет избежать неавторизованного доступа до определённых сетевых сервисов, однако авторизованные соединения получают полный доступ. Поэтому для решения этой проблемы и для проверки авторизованного доступа широко используются системы обнаружения вторжений (СОВ). В случае проверки параметров межсетевого взаимодействия – сетевые СОВ.

Для анализа параметров используется ряд методов. В подавляющем числе случаев коммерческие системы используют сигнатурный метод поиска вторжений, заключающийся в поиске заранее известных атак по формальным признакам – параметров заголовков, передаваемым данным. Недостатком данного подхода считается невозможность обнаруживать неизвестные атаки.

В научных и исследовательских проектах изучаются сетевые СОВ, работающие на основе аппарата нейронных сетей (НС). Благодаря обобщающим свойствам НС появляется возможность эффективно обнаруживать ранее неизвестные атаки. Изучение свойств НС в составе СОВ выполнены в работах таких ученых, как В. Корнеев, В. Райх, А. Сплошнов, А. Масалович, А. Ежов и зарубежных ученых Дж. Кеннеди, М. Моради, А. Бивенса, А. Гоша, А. Шварцбарда и других.

Как показал анализ работ, несмотря на положительные результаты, которые были получены авторами, эти работы обладают рядом недостатков, которые ограничивают промышленное применение рассмотренных СОВ. Во-первых, СОВ были в состоянии выявить факт наличия атаки, однако СОВ не могли их клас-

сифицировать, что затрудняло дальнейший анализ и устранение угроз и уязвимостей системы. Во-вторых, авторов интересовала сама возможность применения тех или иных типов НС для поиска сетевых вторжений, они не развивали архитектуру самого решения. Все исследования объединяло то, что параметры межсетевого взаимодействия подавались на вход одной НС. В данной работе такой подход к построению СОВ назван ***монолитным***. Можно указать следующие недостатки монолитного подхода:

1. Все параметры, даже несвязанные между собой, анализируются в рамках одной НС. Это приводить к уменьшению эффективности поиска и к увеличению времени обучения НС.
2. В случае изменения топологии компьютерной сети, невозможно переобучить часть НС, необходимо переобучать всю сеть сразу.
3. В случае изменения политики безопасности затруднено отключение ряда анализируемых параметров.
4. Все параметры сетевого взаимодействия обрабатываются однотипно, тогда как должна существовать возможность варьирования обработки различных параметров.

В диссертационной работе рассмотрен новый подход к построению многоуровневой сетевой СОВ, заключающийся в том, что группы однотипных параметров межсетевого взаимодействия подаются на входы отдельных модулей первого уровня, каждый из которых представляет собой иерархическую структуру нескольких НС различного типа и выполняет обнаружение аномалий по заданной группе параметров. Результаты работы модулей первого уровня подаются на вход решателя второго уровня, принимающего окончательное решение о наличии атаки и её классификации. Данный подход назван в работе ***модульным***, характеризуется наличием двух уровней и имеет следующие особенности:

- на первом уровне происходит предварительная обработка информации, на втором – окончательная, при этом на вход второго уровня подаётся выходная информация первого уровня;
- обработка на уровнях осуществляется при помощи ряда нейронных сетей (модулей), причём на первом уровне их количество и тип может варьироваться и определяться конкретной решаемой задачей. Однотипные параметры подаются на вход отдельной нейронной сети первого уровня;

- для увеличения эффективности анализа каждый из параметров может быть подан на вход одного или нескольких модулей, также между модулей первого уровня целесообразно добавить элементы с обратной связью;
- второй уровень анализа обрабатывает информацию, поступившую от нейронных сетей первого уровня, определяет и классифицирует атаки в данный момент времени.

Использование модульного подхода обеспечивает следующие преимущества перед монолитным подходом:

1. Снимаются ограничения на количество анализируемых параметров.
2. Обеспечивается возможность переобучения отдельных модулей без остановки работы всей системы в целом.
3. Появляется возможность динамического отключения отдельных модулей.
4. Анализ несвязанных параметров производится в рамках разных модулей.
5. Наличие двухуровневой архитектуры позволяет более эффективно классифицировать наблюдаемую атаку.

Актуальность

Разработка новых подходов к обнаружению сетевых атак для построения защищённых информационных систем и совершенствования методов защиты является актуальной.

Цель диссертационной работы

Целью диссертационной работы является разработка модульного подхода к построению СОВ для повышения эффективности обнаружения атак.

Для достижения этой цели в работе решались следующие основные задачи:

1. Анализ подходов к построению СОВ.
2. Разработка подхода к построению СОВ на базе НС.
3. Разработка архитектуры СОВ.
4. Разработка методик обучения и тестирования СОВ.
5. Экспериментальная проверка предложенного подхода и разработанных методик.

Объект и предмет исследования

Объектом исследования данной работы являются сетевые системы обнаружения вторжений, нейронные сети, сетевые атаки и методы обработки данных,

предметом – методы обеспечения безопасности и обработки информации в защищённых информационных системах.

Научная новизна работы

Научная новизна диссертационной работы состоит в следующем:

1. Предложен новый подход к построению модульной СОВ на базе НС, заключающийся в использовании иерархии модулей с обратными связями. Каждый модуль содержит определённый тип НС.
2. Разработана архитектура модульной СОВ на основе предложенного подхода, позволяющая обнаруживать и классифицировать сетевые вторжения.
3. Разработаны методики обучения и тестирования СОВ.
4. Предложены рекомендации по построению модульной СОВ и применению разработанных методик.

Практическая ценность работы

Практическая ценность состоит в том, что её результаты позволяют:

1. Даны рекомендации по повышению эффективности обнаружения сетевых вторжений при использовании СОВ на базе НС.
2. Подготовлена база данных записей сетевого трафика с атаками различных классов для использования в методическом процессе.
3. Реализован прототип модульной СОВ для анализа сетевых атак семейства протоколов TCP/IP.

Внедрение результатов

Практическая ценность и новизна работы подтверждаются актами внедрения в ГОУ Санкт-Петербургский государственный политехнический университет и Санкт-Петербургском Региональном Центре Защиты Информации.

Положения, выносимые на защиту

На защиту выносятся следующие положения:

1. Анализ подходов к построению СОВ на базе НС и требований к ним.
2. Модульный подход к построению СОВ.
3. Методики обучения и тестирования СОВ.
4. Архитектура модульной СОВ и требования к архитектуре, позволяющие повысить эффективность обнаружения.

Апробация и публикация результатов работы

Научные результаты, полученные в диссертационной работе, докладывались на 3 общероссийских научно-технических конференциях, опубликованы в 10 печатных работах.

Структура и объём диссертации

Диссертационная работа состоит из введения, четырех глав, заключения, приложений и списка литературы. Работа изложена на 155 листах (включая 27 рисунков, 37 таблиц и список литературы из 76 наименований)

Содержание работы.

Во введении обоснована актуальность темы диссертации, приводятся постановка задачи, краткая аннотация содержания работы по разделам, дана оценка новизны, достоверности и практической ценности полученных результатов, сформулированы защищаемые положения.

В первой главе рассмотрена предметная область, а именно, даны общие понятия теории информационной безопасности, причины возникновения атак, их типы и методы защиты от сетевых атак. Обоснована необходимость использования сетевых СОВ для защиты участка сети, рассмотрены различные типы СОВ и принципы их работы, дан обзор ряда коммерческих и свободно распространяемых решений.

Рассмотрены основные принципы теории НС, представлены алгоритмы обучения НС типа многослойный персептрон. Проанализированы существующие исследовательские работы использования аппарата НС в сетевых СОВ.

Во второй главе выявлены и проанализированы недостатки СОВ, использующих метод поиска аномалий, и обоснован выбор метода поиска злоупотреблений. Рассмотрены недостатки существующих работ, введено понятие монолитного подхода к построению СОВ на базе НС. В работе предложен модульный подход к построению СОВ.

Существуют два противоположных метода поиска вторжений в систему – поиск аномалий (anomaly detection) и поиск злоупотреблений (misuse detection). Основное различие данных методов заключается в том, что при поиске аномалий СОВ рассчитана на поиск отклонений от нормального режима работы, тогда как поиск злоупотреблений нацелен на обнаружение заранее известных атак и вторжений. Другими словами, при поиске аномалий СОВ знает, как должна ра-

ботать система и любое отклонение от нормального поведения она считает аномальным. При поиске злоупотреблений СОВ знает сигнатуры атак, что позволяет выявлять атаки на этапе их появления. Оба метода имеют свои недостатки:

- основной недостаток поиска аномалий – на практике сложно построить профиль нормальной активности пользователя, так как, во-первых, нет гарантий, что на этапе построения этого профиля, в системе не наблюдались атаки, а во-вторых, стиль работы пользователя за персональным компьютером может изменяться во времени и нет возможности построить один профиль;
- недостаток поиска злоупотреблений заключается в том, что этот подход не позволяет обнаруживать ранее неизвестные атаки. Количество возможных вариаций атак, которые могут быть обнаружены анализатором, зависят от реализации.

Одним из основных достоинств применения НС в обработке информации является их обобщающие свойства. Это позволяет, в частности, обнаруживать ранее неизвестные атаки. В работе доказывается целесообразность применение НС в качестве анализатора при поиске злоупотреблений, так как, во-первых, не используется поиск аномалий, во-вторых, устраняется недостаток поиска злоупотреблений.

Анализ работ по теме исследования показал, что практически все они обладали одним существенным недостатком, ограничивающим практическое применение – анализ параметров проводился в рамках одной НС (монолитный подход). Исключение составляет работа Ф.Куппенса (Frederic Cuppens) и Я.Бузиды (Yacine Bouzida), которые применили два различных аппарата – нейронные сети и деревья решений. Для устранения недостатков монолитного подхода в работе предлагается использовать не одну НС для анализа параметров, а несколько. В диссертационной работе представлен новый подход к построению СОВ – модульный.

Принцип модульного построения СОВ заключён в использовании иерархически расположенных модулей, каждый из которых содержит НС различного типа и подсистему обработки входных данных (рис. 1). Для повышения эффективности анализа также введёна обратная связь между модулями первого уровня.

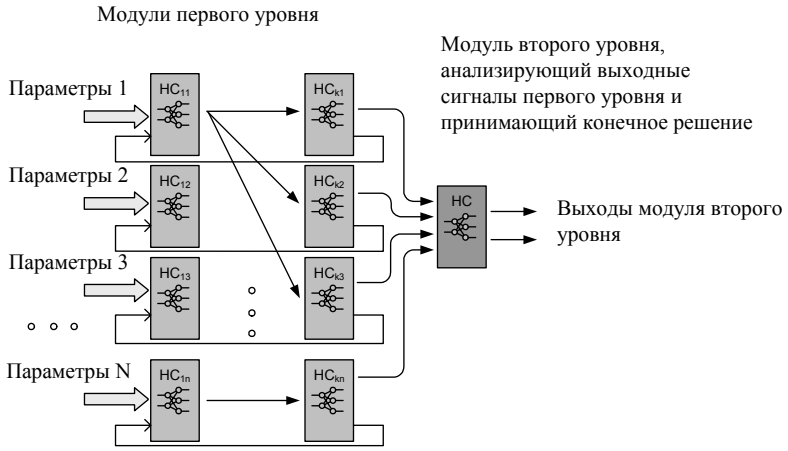

Рис. 1. Модульный подход к обнаружению

Модульная СОВ позволяет более эффективно, по сравнению с монолитным, обнаруживать и классифицировать атаки.

В третьей главе представлена разработанная архитектура СОВ; разработана методика по обучению, тестированию и использованию СОВ. Выделены и описаны сетевые атаки, которые использовались для обучения и тестирования системы; проведена их классификация, и на основе анализа этих атак отобраны группы параметров межсетевого взаимодействия для обработки в СОВ. Разработаны методы обработки и подготовки значений параметров для подачи на вход СОВ; обоснована необходимость реализации генератора сетевого шума и предложена его реализация.

Проведенные исследования показали, что наиболее оптимальной оказалась архитектура, представленная на рис. 2.

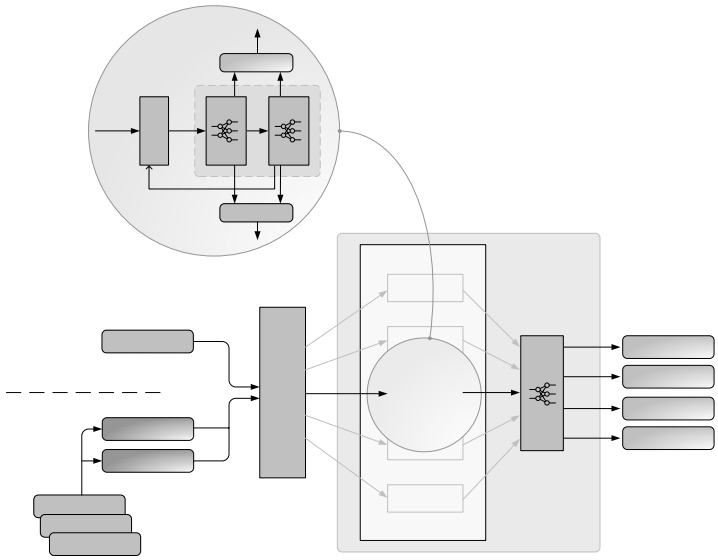

Рис. 2. Архитектура модульной СОВ

В качестве источника данных для обучения НС, входящих в состав модулей, используются подготовленные базы атак и генератор сетевого шума. Обработка данных заключается в усреднении методом “скользящего окна”, нормализации данных, добавлении шума и удалении нулевых векторов. Модули первого уровня представляют иерархически расположенные две НС. Вторая НС подключается в том случае, если наблюдается подозрительный вектор и первая НС не может дать точного ответа – есть аномалия или нет. Вторая НС имеет механизм обратной связи с обработчиком данных, динамически изменяя параметры для более подробного изучения. Введение обратной связи позволяет более эффективно изучать данные и уменьшить количество ложных срабатываний системы. Выходы модулей первого уровня, которые сигнализируют о наличии аномалий по одной из групп параметров, подаются на вход модуля второго уровня, который принимает окончательно решение о наличии атаки и, при возможности, производит дополнительно классификацию атаки.

В качестве исходных данных для обучения используются 3 базы атак - база лаборатории Линкольна министерства обороны США, из которой выбраны 20 атак; база атак канадского центра исследований связи, после анализа выбрано 37 атак; собственная база атак, в которой представлены в основном результаты работы различных сканеров – nmap, nessus, saint. Общее количество различных типов атак – 63, общее количество примеров атак в этих базах, которые используются для обучения – 3685.

Разработанная таксономия атак, опирающаяся на распространённую таксономию Ховарда, включает в себя следующие классы атак:

- атаки, связанные с аутентификацией – подбор паролей, подбор имен пользователей и так далее (3 атаки);
- методы сокрытия атак – использование различных особенностей работы стека TCP/IP для сокрытия атак от СОВ (16 атак);
- сканирование (3 атаки, связанные с результатами работы различных сканеров безопасности);
- отказ в обслуживании (6 атак);
- атаки, использующие уязвимости протокола Telnet (6 атак);
- атаки, использующие уязвимости протоколов TCP/IP (3 атаки);
- атаки, использующие уязвимости протокола FTP (7 атак);

- атаки, использующие уязвимости различных почтовых протоколов – POP3, IMAP, SMTP (3 атаки);
- атаки, использующие уязвимости протокола HTTP (16 атак).

В результате анализа атак этих классов был обоснован выбор 132 параметров межсетевого взаимодействия, которые использовались СОВ для выявления факта наличия атак.

В работе обоснован выбор метода поиска злоупотреблений, который, в свою очередь, потребовал разработки генератора сетевого шума, необходимого для эффективного обучения модулей НС и системы. В качестве основы для построения генератора шума была использована база DARPA, которая помимо атак содержит записи сетевых данных без атак.

Для усреднения параметров межсетевого взаимодействия в работе использован метод “скользящего окна” (рис. 3). В данном методе левая граница временного интервала смещается на величину меньшую, чем размер самого интервала.

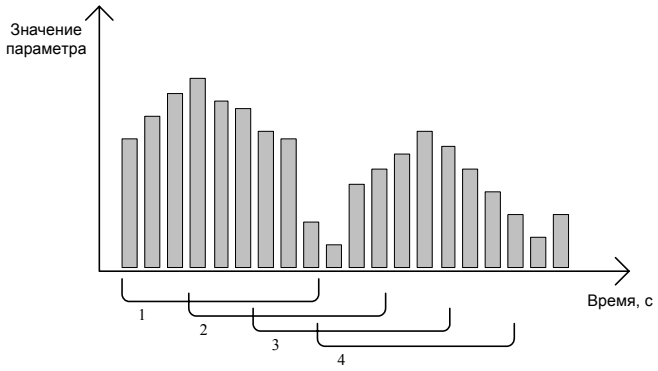

Рис. 3. Метод “скользящего окна”

Оценка математического ожидания для дискретного равномерного распределения (вероятность появления каждого значения $\mathrm{P}(X = x_i) = \frac{1}{n},\ i = 1 \ldots n$) равна среднему арифметическому и находится по формуле $\mathrm{E}X = \frac{1}{n}\sum_{i=1}^{n} x_i$, где x – элементы усредняемого множества X, $X=\{x_1,\ldots,x_n\}$. В том случае, если мы изучаем временной ряд, то n – это количество временных отрезков в усредняемом множестве X.

На практике интерес представляет изучение ряда таких множеств, каждое из которых будет представлять элемент одного вектора для подачи на вход НС.

Пусть V – множество средних значений изучаемого параметра, $V=\{V_1,...,V_N\}$, где N – количество интервалов усреднения.

В случае применения скользящего окна, среднее значение параметра вычисляется по формуле: $V_i = \frac{1}{n_i} \sum_{j=1+k\cdot i}^{n_i+k\cdot i} x_j$, где i - номер очередного окна, n_i - количество временных интервалов в окне, k – временной сдвиг окна, x_j – элемент выборки из временного окна.

Для решения различных задач, связанных с анализом данных при помощи НС, необходимо выбрать тип НС и алгоритмы их работы и обучения, которые будут наиболее эффективно решать поставленную задачу. В ходе выполнения работы были проведены исследования, в рамках которых были рассмотрены 10 различных типов НС, 7 функций активации и 11 алгоритмов обучения. Как показал анализ наиболее эффективными для решения задач обнаружения сетевых атак оказались следующие НС:

- многослойный персептрон с автономным градиентным алгоритмом обучения;
- самообучающаяся сеть Кохонена с использованием слоя Гроссберга.

Для реализации СОВ в работе обоснован выбор многослойного персептрона, для обучения которого используется алгоритм обратного распространения ошибки. Алгоритм включает следующие шаги:

1. На входы НС подается один из возможных векторов в режиме обычного функционирования НС, когда сигналы распространяются от входов к выходам. Рассчитываются значения для каждого слоя по формуле $s_j^{(n)} = \sum_{i=0}^{M} y_i^{(n-1)} \cdot w_{ij}^{(n)}$, где где M – число нейронов в слое $n-1$ с учетом нейрона с постоянным выходным состоянием $+1$, задающего смещение; $y_i^{(n-1)}=x_{ij}^{(n)}$ – *i-ый* вход нейрона j слоя n; $y_j^{(n)} = f(s_j^{(n)})$ –результат функции активации.

2. Вычисляются значения производной функции активации слоя N для выходного слоя по формуле $\delta_l^{(N)} = (y_l^{(N)} - d_l) \cdot \frac{dy_l}{ds_l}$.

Рассчитываются изменения весов слоя N по формуле $\Delta w_{ij}^{(n)} = -\eta \cdot \delta_j^{(n)} \cdot y_i^{(n-1)}$.

3. Рассчитываются по формулам $\delta_j^{(n)} = \left[\sum_k \delta_k^{(n+1)} \cdot w_{jk}^{(n+1)}\right] \cdot \frac{dy_j}{ds_j}$ и $\Delta w_{ij}^{(n)} = -\eta \cdot \delta_j^{(n)} \cdot y_i^{(n-1)}$ соответственно $\delta^{(n)}$ и $\Delta w^{(n)}$ для всех остальных слоев, $n=N-1,...1$.

4. Корректируются веса в НС $w_{ij}^{(n)}(t) = w_{ij}^{(n)}(t-1) + \Delta w_{ij}^{(n)}(t)$.

5. Если ошибка сети превышает заданный порог, переход на шаг 1. В противном случае – конец.

В главе приводится разработанная методика построения и обучения СОВ, которая включает в себя следующие основные этапы:

1. Анализ топологии сети для выявления классов актуальных атак.
2. Выбор параметров межсетевого взаимодействия.
3. Анализ выбранных параметров для формирования групп, которые будут подаваться на вход модулей первого уровня.
4. Построение ряда модулей первого уровня.
5. Построение модуля второго уровня СОВ.
6. Подготовка данных для обучения.
7. Обучение НС, входящих в состав модулей первого и второго уровней.
8. Тестирование СОВ.

Разработана методика тестирования СОВ, определяющая возможность обнаруживать неизвестные атаки и оценивать эффективность работы СОВ при помощи вычисления вероятностей ошибок первого и второго рода.

Четвертая глава посвящена экспериментальной проверке предложенного подхода, для чего разработан прототип модульной СОВ. Дано описание программной реализации и решений, которые были использованы для построения прототипа. Проведён количественный анализ выбранных атак и множеств, которые используются для обучения модулей и тестирования СОВ. Представлены и проанализированы результаты обучения модулей первого и второго уровней. Проанализирована скорость обучения и работы прототипа СОВ.

В результате выполнения работы были получены данные, подтверждающие эффективность использования модульного подхода для анализа восьми различных классов сетевых атак, а также получены численные оценки эффективности обнаружения. Приведено сравнение результатов работы модульной СОВ с результатами однотипных исследований.

Общее время, потраченное на обучение 40 модулей первого уровня, превысило 61 час, при этом средняя скорость обучения модулей составила 16091 векторов в секунду. Обучение модуля второго уровня заняло 28 часов при скорости в 14281 векторов в секунду. Анализ показал, что скорость работы СОВ превышает 58839 векторов в секунду. Замеры производительности выполнялись на персональном компьютере на базе процессора AMD Athlon 1.34 ГЦ с оперативной памятью DDR2 768МБ.

После обучения и тестирования была получена оценка надежности классификации наблюдаемых сетевых параметров (табл. 1), построенная на основании матрицы неточностей (confusion matrix). Матрица надежности классификации позволяет провести оценку ошибок первого и второго родов. Значение первого столбца – классы подаваемых на вход СОВ данных, значение первой строки – возможные выходы СОВ, значение в ячейках – вероятность причисления входного класса к одному из возможных выходных. Общая точность классификации атак рассчитывается по формуле $AC = \frac{\sum_{i=0}^{N} P_{ii}}{\sum_{i=0}^{N}\sum_{j=0}^{N} P_{ij}}$, где P_{ij} – значение ячейки матрицы неточностей, N – количество столбцов и строк в матрице. Общая точность классификации СОВ равна 59%.

Таблица 1. Надежность классификации СОВ.

	Аутент.	Сокр.	Ош. Ftptelnet	Ош. HTTP	Ош. Mail	Ош. TCPIP	Шторм	Нормальное	Сканиров
Аутентифик	**86**	0	0	1	1	9	0	3	1
Сокрытие	0	**59**	1	3	0	37	0	0	0
Ош.Ftptelnet	0	5	**49**	2	1	42	0	0	0
Ош.HTTP	1	6	1	**56**	0	31	0	3	1
Ош.Mail	0	0	0	0	**63**	37	0	0	0
Ош.TCPIP	4	0	0	0	1	**93**	0	0	0
Шторм	0	0	0	0	0	2	**97**	0	0
Нормальное	3	0	0	3	0	33	0	**61**	1
Сканиров.	1	0	0	1	0	6	0	0	**92**

Анализ показал, что невысокое значение точности классификации обусловлено тем, что атаки, связанные с особенностями работы стека TCP/IP (“Ош. TCPIP” в табл. 1) не отличаются от остальных классов, в частности от класса нормальной активности (“Нормальное” в табл. 1). В том случае, если не рассматривать этот класс атак, точность классификации увеличивается.

Ошибки работы СОВ первого и второго родов представлены в табл. 2. Точность обнаружения атак, рассчитываемая по формуле $A = \frac{TN + TP}{TN + TP + FN + FP}$, равна 92%.

Таблица 2. Эффективность обнаружения и ошибки I и II родов.

Обнаружение нормальной работы (TN), %	91
Обнаружение атаки (TP), %	93
Ошибка I рода (FN), %	7
Ошибка II рода (FP), %	9

Оценка эффективности работы после тестирования СОВ на ранее неизвестных данных представлена в табл. 3. Точность обнаружения атак – 84%.

Таблица 3. Эффективность обнаружения и ошибки I и II родов на неизвестных данных.

Обнаружение нормальной работы, %	86
Обнаружение атаки, %	82
Ошибка I рода, %	14
Ошибка II рода, %	18

Из приведённых результатов видно, что модульная СОВ с большой вероятностью обнаруживает атаку на систему (93% известных и 82% неизвестных ранее атак обнаружено). Классификация атак в данной реализации прототипа производится менее эффективно (для класса FTPTelnet – всего в 49%, общая точность классификации – 59%). Это объясняется тем, что класс атак, использующих уязвимости стека TCP/IP, оказался малоразличимым относительно других классов.

В работе приводится сравнение результатов диссертационной работы с результатами, полученными в рамках исследований других ученых, таких как А. Гош, А. Бивенс. Авторы изучали использование СОВ различных типов, в качестве тестовых выборок они использовали те же базы атак. Процент обнаруженных атак и вероятность ошибки второго рода, полученные в этих работах, представлены в таблице 4.

Таблица 4. Сравнение результатов работы.

Работа	**База/СОВ**	**Обнаружено атак, %**	**Ошибка II рода, %**
Диссертационная работа, 2007	DARPA,CRC/НС	93	9
А.Бивенс, Ч.Палагири, 2002	DARPA/НС	76	24
А.Гош, А.Шварцбард, 1999	DARPA/НС	91	19

Полученные результаты позволяют утверждать, что разработанный модульный подход к построению СОВ и методика использования этой системы позволяют более эффективно обнаруживать факт наличия атаки.

В результате диссертационных исследований были выполнены следующие задачи:

1. Проведён анализ подходов к построению СОВ.
2. Разработан подход к построению СОВ на базе НС.
3. Разработана архитектура СОВ.
4. Разработана методика обучения и тестирования СОВ.
5. Проведены эксперименты для проверки предложенного подхода и разработанных методик.

Основные результаты диссертационного исследования изложены в 10 печатных работах, основные работы представлены в списке:

1. Жульков Е.В., Платонов В.В. Прототип системы обнаружения вторжений на основе модульных нейронных сетей. // Материалы XVI общероссийской научно-технической конференции “Методы и Технические Средства Обеспечения Безопасности Информации”. СПб.: - 2007. - С. 89.

2. **Жульков Е.В., Платонов В.В. Применение модульного подхода к построению нейронных сетей для поиска аномалий. // Проблемы информационной безопасности. Компьютерные системы. СПб.: - 2006. - №3. – С. 30-34. (перечень ВАК).**

3. Жульков Е.В. Платонов В.В. Развитие сетевых систем обнаружения вторжений на базе модульных нейронных сетей. // Сборник материалов V общероссийской научной конференции “Математика и Безопасность Информационных Технологий”. М.: МаБИТ-2006 – С. 108.

4. Жульков Е.В., Платонов В.В. Основные пути развития систем обнаружения вторжений на базе модульных нейронных сетей. // Материалы XV общероссийской научно-технической конференции “Методы и Технические Средства Обеспечения Безопасности Информации”. СПб.: - 2006. – С. 99.

5. Жульков Е.В., Платонов В.В. Направления развития модульного построения нейронных сетей для обнаружения вторжений. // Материалы XIV общероссийской научно-технической конференции. СПб.: - 2005. – С. 86.

6. Жульков Е.В. Томилин В.Н. Модульный подход к построению сетевой системы обнаружения вторжений на основе аппарата нейронных сетей. //Материалы XII общероссийской научно-технической конференции. СПб.: - 2004. – С. 89.