УДК 004.056.52

В.Е. Сухов

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И НЕЙРОСЕТЕВЫХ ДЕТЕКТОРОВ

Предложена система обнаружения аномалий, использующая аппарат искусственных иммунных систем и нейронных сетей. Описываются структура, алгоритмы функционирования и программная реализация системы обнаружения аномалий.

Ключевые слова: *искусственные иммунные системы, искусственные нейронные сети, обнаружение аномалий, обнаружение вторжений, сетевые технологии, анализ сетевого трафика.*

Введение. Интенсивное развитие вычислительной техники и программного обеспечения обостряет проблему компьютерной безопасности, повышает требования к контролю за состоянием системы, требует качественных методов поиска сбоев и аномалий в ее работе [1]. Информационные системы (ИС) все больше усложняются, и становится все труднее обнаруживать и анализировать аномалии в их функционировании. Серьезной проблемой, с которой сталкиваются разработчики современных систем обнаружения аномалий в функционировании ИС, является то, что современные схемы организации атак и других противозаконных действий характеризуются большой сложностью и запутанностью. В процессе распознавания этих схем необходимо обнаруживать сложные комбинации сетевых транзакций и сопутствующих им фактов [2], что делает контроль за состоянием вычислительной сети очень трудоемким или вообще невозможным без применения специализированных автоматизированных средств.

Сейчас систем обнаружения аномалий как самостоятельных продуктов практически не существует, но распространены системы обнаружения вторжений [3], основанные на анализе сигнатур, которые обнаруживают аномалии, связанные с атаками и вторжениями. Однако сигнатурный метод обладает следующими недостатками:

а) невозможность обнаруживать новые, не встречавшиеся ранее несанкционированные воздействия;

б) неустойчивость к модификациям уже известных атак;

в) неспособность определять распределенные во времени атаки и аномлии.

Помимо этого, большинство систем, использующих сигнатурный метод, например RealSecure и NetRanger, являются дорогостоящими продуктами. Среди бесплатных систем обнаружения вторжений, наиболее часто применяемых для защиты сетей передачи данных, можно выделить только систему Snort, но и для этой системы актуальные базы сигнатур являются платными.

Для построения систем обнаружения аномалий можно использовать различные технологии. В последние годы большое внимание уделяется изучению методов биологического моделирования искусственного интеллекта, таких как искусственные нейронные сети и искусственные иммунные системы, безусловно являющиеся одним из перспективных подходов к решению задач обнаружения аномалий.

Цель работы – разработка системы обнаружения аномалий сетевого трафика, обладающей способностью адаптации к изменениям поведения вычислительной сети и низким числом ложных срабатываний, с использованием методов искусственного интеллекта.

Теоретическая часть. Искусственный нейрон – это информационная модель отдельной нервной клетки мозга. Ограниченное число искусственных нейронов может структурироваться в жесткие необучаемые конфигурации – искусственные нейронные ансамбли. Искусственная нейронная сеть – это более гибкая конфигурация, состоящая из большого числа искусственных нейронов, которые с помощью специальной процедуры обучения могут изменять свои параметры. Искусственная нейронная сеть имеет несколько нейронных слоев. Каждый нейронный слой связан с последующим некой активацион-

ной функцией, множеством коэффициентов и смещений. Каждый нейрон принимает на вход множество значений (координат), вычисляет свой выход по активационной функции и передает получившееся значение в следующий слой.

В настоящее время существует довольно много нейросетевых структур, применяемых для решения различных прикладных задач, однако из проанализированных нейронных сетей наиболее целесообразными для применения в средствах обнаружения аномалий являются многослойный персептрон и самоорганизующаяся карта признаков.

Многослойный персептрон целесообразно использовать в средствах защиты информации, которые базируются на анализе множества дискретных параметров. Эти параметры должны подвергаться предварительной нормализации, ставящей в соответствие содержимому параметра числовой идентификатор.

При использовании многослойного персептрона существует ряд ограничений:

а) не до конца исследованы возможности в области обобщения и вывода новых знаний;

б) невозможность переобучения в процессе практической эксплуатации.

На практике они могут негативно отразиться на возможности диагностирования новых видов атак или неизвестных уязвимостей. Для преодоления указанных ограничений необходимо разработать методику формирования качественной первоначальной обучающей выборки. Также одним из решений является комбинированное применения персептрона с другими видами нейронных сетей.

Аппарат самоорганизующихся сетей Кохонена представляет большой интерес в рамках решения проблемы поиска аномалий.

Для обучения сети используется метод «Winner Takes All» (WTA) [4], в соответствии с которым группа конкурирующих между собой нейронов получает одни и те же входные векторы. В зависимости от фактических значений весовых коэффициентов суммарные выходы отдельных нейронов могут различаться. По результатам сравнения этих значений победителем признается нейрон, значение выхода которого оказалось наибольшим. Нейрон-победитель вырабатывает на своем выходе состояние 1, а остальные переходят в состояние 0.

Вектор весов нейрона-победителя модифицируется в соответствии со следующей формулой:

$$\mathbf{w} = \mathbf{w} + c\mathbf{x},$$

где c – некоторый положительный параметр обучения, $\mathbf{x}$ – входной вектор, $\mathbf{w}$ – вектор весов нейрона-победителя.

Самоорганизующиеся сети позволяют обнаруживать вторжения по принципу «непохожести» состояния системы на те состояния, на основании которых сеть обучалась. Благодаря этой возможности сеть способна обнаруживать как известные, так и неизвестные атаки.

Результаты анализа применения искусственных нейронных сетей в задачах обнаружения аномалий показали возможность использования их в реальных вычислительных сетях. Однако необходимо учитывать проблему соотношения большого числа анализируемых параметров и скорости работы нейронной сети: чем больше количество параметров, тем ниже скорость работы, в свою очередь уменьшение количества параметров снижает точность выявления аномалий нейронной сетью. Для каждой конкретной вычислительной сети необходимо находить оптимальное соотношение.

Исследования иммунной системы человека показали аналогию между иммунными системами и системами выявления аномалий. Свойства распределенности и самоорганизации (адаптации к изменяющимся условиям), присущие иммунным системам, удовлетворяют основным требованиям к системам выявления аномалий.

При построении иммунных систем пространства объектов разделяются на две части: «свои» и «чужие». «Свои» – это все события, которые носят легитимный характер, а «чужие» – события, вызванные злоумышленниками. Система обнаружения аномалий должна различать эти два класса событий [5].

Для того чтобы система могла точно определить, где «свой» и где «чужой», в ее составе необходимо использовать детекторы, которые реагируют только на «чужие» элементы. Для создания таких детекторов разрабатывается специальный алгоритм обнаружения, называемый алгоритмом «отрицательного отбора» [6]. Случайно сгенерированный детектор тестируют, проверяя на «правильном» наборе данных. Если детектор срабатывает, его удаляют и генерируют новый. Таким образом, создается набор детекторов, которые срабатывают на «чужие» и не обнаруживают легитимные события.

Моделирование иммунной системы включает разработку алгоритмов динамического создания и обновления детекторов аномалий, а также выявления отклонений посредством сопоставления их с текущими данными.

Практическая часть. Функционирование системы обнаружения аномалий базируется на принципах работы искусственной иммунной системы. Система обнаружения аномалий логиче-

ски разделяется на несколько модулей: модуль сбора трафика и формирования статистики, модуль обучения, модуль обнаружения аномалий и модуль оповещения. Структура системы обнаружения аномалий приведена на рисунке 1.

Модуль сбора трафика и формирования статистики перехватывает весь трафик, проходящий через узел сети, на котором установлена система обнаружения аномалий, выделяет в нем определенные признаки, подсчитывает по этим признакам статистику за определенный период и представляет собранную статистику в виде вектора, включающего 20 координат: количество входящих/исходящих/внутрисетевых IP, TCP, UDP пакетов; количество опросов неразрешенных портов UDP; количество завершенных запросов по протоколу UDP; количество незавершенных запросов по протоколу UDP; количество незавершенных запросов по протоколу UDP, тайм-аут ответа на которые истек; количество опросов

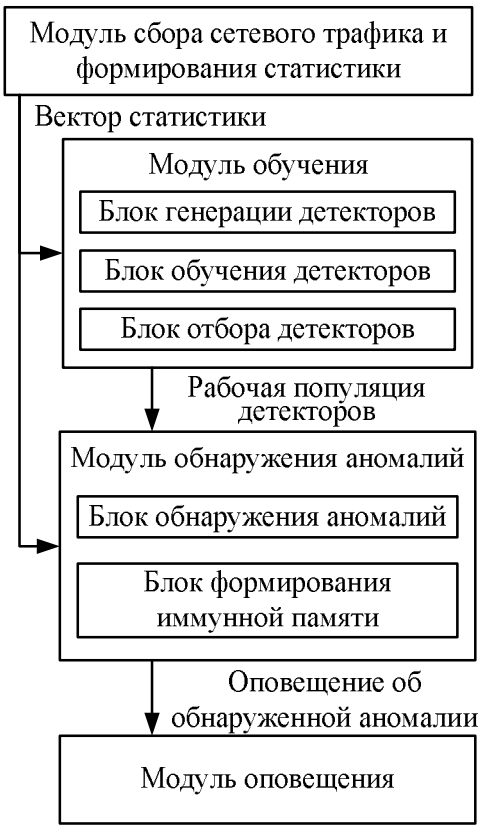

Рисунок 1 – Структура системы

портов TCP; количество опросов разрешенных портов TCP; количество соединений TCP, находящихся в состоянии установления, т.е. SYN SEND; количество соединений TCP, находящихся в открытом состоянии, т.е. ESTABLISHED; количество соединений TCP, находящихся в состоянии закрытия, т.е. FIN SEND в единицу времени; отношение количества опросов разрешенных портов протокола TCP к количеству опросов всех портов этого протокола; отношение количества открываемых соединений TCP к общему количеству соединений [7]. Данные параметры сетевого трафика используются в дальнейшем для обнаружения аномалий.

Модуль обучения использует алгоритм отрицательного отбора [8] для формирования рабочей популяции детекторов, настроенной на анализируемую вычислительную сеть, то есть популяции, имеющей такой набор детекторов, которые с высокой точностью определяли бы аномальный для сети трафик и характеризовались бы низкой частотой ложных срабатываний. Модуль обучения можно условно разделить на следующие блоки: блок генерации детекторов; блок обучения детекторов; блок отбора детекторов.

Для обучения нейросетевого детектора, который представляет собой нейронную сеть Кохонена, используется обучение без учителя. Для обучения сети применяются механизмы конкуренции [9]. При подаче на вход сети вектора побеждает тот нейрон, вектор весов которого наиболее схож с входным вектором. Для нейрона-победителя выполняется соотношение:

$$d(\mathbf{x}, \mathbf{w}^*) = \min_{1<i<n} d(\mathbf{x}, \mathbf{w}_\mathbf{i}),$$

где n – количество нейронов, $\boldsymbol{w}^*$ – вектор весов нейрона-победителя, $d(\mathbf{x},\mathbf{w_i})$ – расстояние между векторами $\mathbf{x}$ и $\mathbf{w_i}$. В качестве меры расстояния используется евклидова мера:

$$d(\mathbf{x}, \mathbf{w}_\mathbf{i}) = \| \mathbf{x} - \mathbf{w}_\mathbf{i} \| = \sqrt{\sum_{j=1}^{n} (x_j - w_{ij})^2}.$$

Вокруг нейрона-победителя образуется окружение или радиус обучения. Радиус обучения определяет, сколько нейронов, кроме нейрона-победителя, участвуют в обучении (т.е. изменяют свои веса) на данной итерации. Радиус обучения принимает наибольшее значение на первой итерации и постепенно уменьшается с увеличением числа итераций таким образом, что в конце обучения корректирует свои веса только нейрон-победитель.

Веса нейрона-победителя и всех нейронов, лежащих в пределах его окружения, подвергаются обучению по правилу Кохонена:

$$\mathbf{w}_\mathbf{i}^{(k+1)} = \mathbf{w}_\mathbf{i}^{(k)} + \eta_i^{(k)} [\mathbf{x} - \mathbf{w}_\mathbf{i}^{(k)}],$$

где $i = \overline{1,n}$, $\mathbf{x}$ – входной вектор, k – номер цикла обучения, $\eta_i^{(k)}$ – коэффициент скорости обучения i-го нейрона из радиуса обучения в k-м цикле обучения.

Коэффициент скорости обучения $\eta_i^{(k)}$ i-го нейрона в k-м цикле обучения разбивается на две части: функцию соседства $G_i(d_i,k)$ и функции скорости обучения $\varepsilon(k)$:

$$\eta_i^{(k)} = G_i(d_i, k)\varepsilon(k).$$

Функция соседства позволяет добиться того, что веса нейронов, находящихся за пределами радиуса обучения, не изменяются. В качестве функции соседства применяется Гауссова функция

$$G_i(d_i, k) = e^{-\frac{d_i}{2\sigma(k)}}.$$

Здесь d_i – расстояние между векторами весов i-го нейрона и нейрона-победителя. При этом $\sigma(k)$ является убывающей функцией от номера цикла обучения. Будем использовать функцию, монотонно убывающую от номера цикла обучения:

$$\sigma(k) = \frac{1}{k}.$$

Определим функцию скорости обучения $\varepsilon(k)$. Данная функция также представляет собой функцию, убывающую от номера цикла обучения. Будем использовать функцию вида

$$\varepsilon(k) = e^{-k}.$$

Применение функции $\eta_i^{(k)}$ позволяет добиться того, что все векторы из обучающей выборки вносят примерно равный вклад в результат обучения.

Обучение состоит из двух основных этапов: на первом этапе обучение производится с достаточно большими значениями скорости и радиуса обучения, что позволяет расположить векторы весов нейронов в соответствии с распределением примеров в выборке. На втором этапе необходимо произвести точную настройку весов при значениях параметров скорости обучения намного меньше начальных. Обучение длится до того момента, пока погрешность квантования при входных векторах не станет достаточно малой величиной (**w*** – вектор весов нейрона-победителя):

$$E = \frac{1}{p}\sum_{i=1}^{p} \| \mathbf{x_i} - \mathbf{w^*} \|^2.$$

При обучении сети Кохонена существует проблема так называемых «мертвых» нейронов. Одной из особенностей любого конкурирующего слоя является то, что некоторые нейроны оказываются незадействованными, так как нейроны, у которых начальные векторы весов значительно удалены от векторов входа, никогда не выигрывают конкуренции независимо от длительности обучения. В результате оказывается, что такие векторы весов не используются при обучении и соответствующие нейроны никогда не становятся победителями. Такие нейроны называют «мертвыми» нейронами, поскольку они не выполняют никакой полезной функции. Вследствие этого входные векторы будут интерпретироваться меньшим числом нейронов, а погрешность квантования – увеличиваться. Поэтому необходимо настроить сеть так, чтоб мог победить каждый из нейронов сети. Для этого алгоритм обучения модифицируется таким образом, чтобы нейрон-победитель терял активность. Одним из приемов учета активности нейронов является подсчет потенциала p_i каждого нейрона в процессе обучения. Первоначально нейронам присваивается потенциал

$$p_i(0) = \frac{1}{n},$$

где n – число нейронов (кластеров). Значение потенциала изменяется каждый раз после подачи входного вектора **x**. В k-м цикле обучения для нейрона-победителя потенциал определяется по правилу:

$$p^*(k) = p^*(k-1) - p_{\min},$$

где $p^*(k)$ – потенциал нейрона-победителя в k-м цикле обучения, $p_{\min}$ – минимальный потенциал, допускающий участие в конкурентной борьбе, задается в пределах от 0 до 1.

Для всех остальных нейронов потенциал определяется по правилу:

$$p_i(k) = p_i(k-1) + \frac{1}{n},$$

где n – число нейронов, i – номер нейрона.

Если значение потенциала $p_i(k)$ опускается ниже уровня $p_{\min}$, то нейрон не рассматривается (он «отдыхает»). Победитель ищется среди оставшихся нейронов, для которых $p_i \geq p_{\min}$. Выбор конкретного значения $p_{\min}$ позволяет установить порог готовности нейрона к конкурентной борьбе. При $p_{\min}$=0 нейроны не исключаются из борьбы, что приводит к появлению «мертвых» нейронов. При $p_{\min}$=1 нейроны побеждают по очереди, так как в каждом цикле обучения только один из них готов к борьбе. Практические исследования показывают, что хороший результат получается при $p_{\min}\approx$0,75.

В сети Кохонена входные значения необходимо нормировать. Для этого используют формулу:

$$x_{ni} = \frac{x_i}{\sqrt{\sum_{j=1}^{n} x_j^2}},$$

где x_{ni} – нормированный компонент входного вектора, n – количество нейронов.

Модуль обнаружения аномалий анализирует статистику, предоставленную модулем сбора

трафика и формирования статистики, путем подачи этой статистики на вход каждого детектора из рабочей популяции. Аномалия обнаружена, если хотя бы один из детекторов признает статистику отличной от нормальной. В модуле обнаружения аномалий можно выделить два функциональных блока: блок обнаружения и блок формирования иммунной памяти (клонирования и мутации детекторов).

В качестве детекторов в модуле обнаружения аномалий используется нейронная сеть на основе многослойного персептрона, который состоит из 20 нейронов распределительного слоя, 10 нейронов скрытого слоя и 2 нейронов выходного слоя. На вход детектора в режиме обнаружения аномалий подаются векторы статистической информации о сетевом трафике. Первый слой нейронных элементов является распределительным. Он распределяет входные сигналы на нейронные элементы второго (скрытого) слоя. Количество нейронных элементов распределительного слоя равняется размерности вектора статистики. Второй слой состоит из нейронов Кохонена, которые используют конкурентный принцип обучения и функционирования в соответствии с алгоритмом WTA. Нейронный слой Кохонена осуществляет кластеризацию входного пространства образов, в результате чего образуются кластеры, каждому из которых соответствует свой нейронный элемент. Третий слой состоит из двух линейных нейронных элементов, которые используют линейную функцию активации. Данный слой осуществляет процедуру окончательного решения о принадлежности сканируемого вектора к нормальной или к аномальной активности.

Модуль оповещения при обнаружении аномалии модулем обнаружения выдает предупреждающее сообщение.

Алгоритм работы системы обнаружения аномалий в режиме обучения заключается в том, что система в течение определенного времени функционирует в сети, обучаясь на типичном (нормальном) для данной сети трафике. Алгоритм функционирования системы в этом режиме представлен на рисунке 2. При первом использовании системы обнаружения аномалий создается начальная популяция, состоящая из множества случайным образом сгенерированных нейросетевых детекторов. Данное множество детекторов должно охватывать всю допустимую область своих значений. Затем начинается захват трафика и формирование на его основе статистических характеристик.

Вектор показателей статистики подается по очереди на вход каждого из нейросетевых детекторов. Те детекторы, которые обнаружили в данном векторе аномальную активность (а ее по определению быть не должно), удаляются из популяции. Данный алгоритм реализует механизм «отрицательного отбора» искусственной иммунной системы.

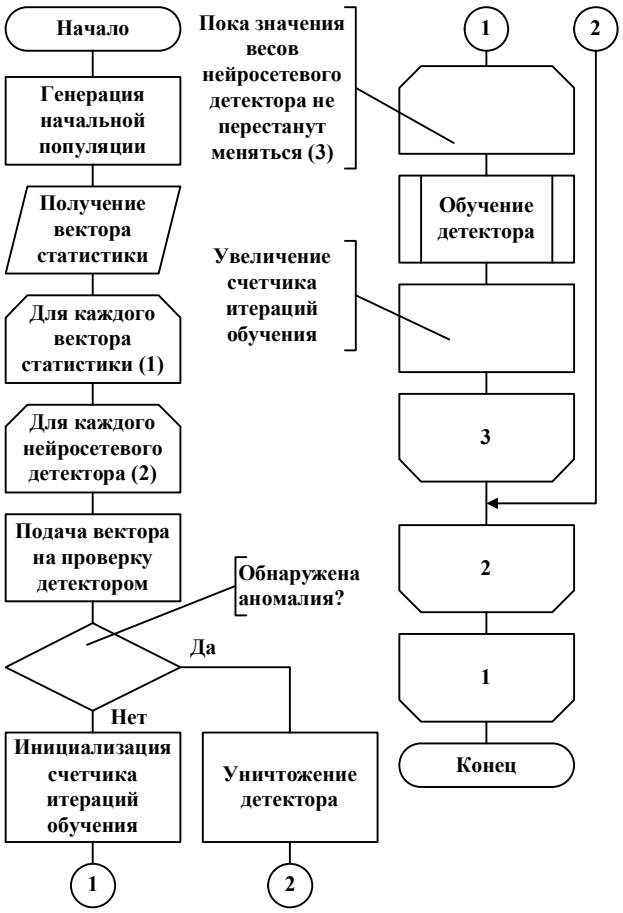

Рисунок 2 – Алгоритм работы системы в режиме обучения

Если аномальная активность детектором не обнаружена, происходит обучение этого детектора. Таким образом, из детекторов формируется рабочая популяция, обученная и правильно функционирующая на нормальном трафике.

В случае функционирования системы в режиме обнаружения аномалий алгоритм работы будет отличаться [10]. Данный алгоритм показан на рисунке 3. Система в этом случае работает с уже сформированной на этапе обучения рабочей популяцией детекторов.

Статистические векторы, сформированные на основе захваченного трафика, поступают на входы нейросетевых детекторов. При классификации детектором статистики как нормальной увеличивается время жизни этого детектора, показывающее его полезность. Время жизни определяет период существования детектора в системе, в течение которого детектор может не обнаруживать аномалии, но при этом останется в ра-

бочей популяции. Большое значение времени жизни означает, что за долгий период функционирования данный детектор не обнаружил ни одной аномалии. При достижении определенного порогового значения детектор удаляется. В качестве порогового используется значение времени жизни, равное 1000 циклам обработки вектора статистики. Если же детектор обнаружил аномалию, то его время жизни сбрасывается и запускается механизм клонирования этого детектора, заключающийся в создании 5 копий данного детектора. Для каждой созданной копии выполняется мутация. Мутация основана на случайном изменении весов нейросетевого детектора на малую величину. Это делается для того, чтобы сходные с обнаруженной детектором аномалии также были выявлены, так как высока вероятность их возникновения. Механизмы клонирования и мутации формируют «иммунную память» системы, таким образом, появлявшиеся в данной сети аномалии и родственные им будут распознаны и в следующий раз.

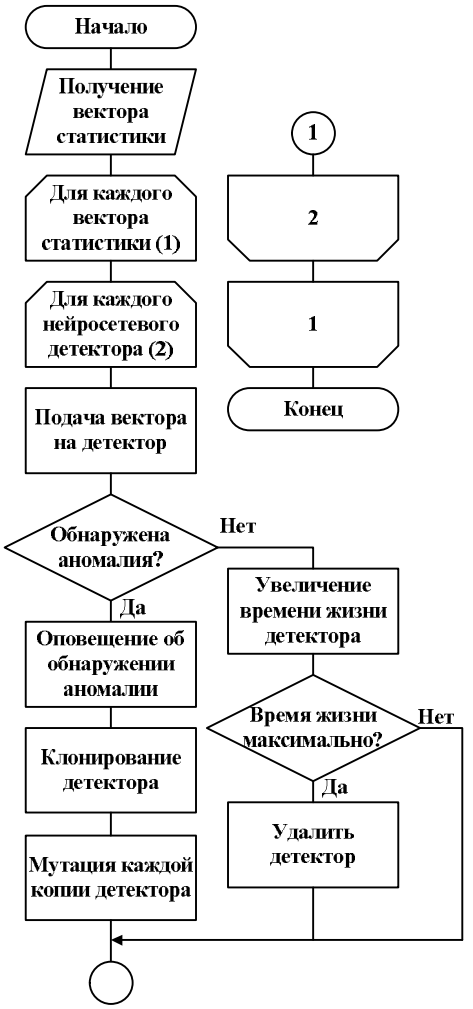

Рисунок 3 – Алгоритм работы системы в режиме обнаружения аномалий

Экспериментальные исследования. Для проведения экспериментального исследования разработанная система обнаружения аномалий была установлена на стенде под управлением операционной системы Windows Server 2008. Стенд имеет следующие аппаратные характеристики: процессор с тактовой частотой 1 ГГц; объем оперативной памяти 2 Гб; объем свободного дискового пространства 30 Гб; сетевая карта.

Разработанная система обнаружения аномалий в течение недели проходила обучение в нормально функционирующей локальной вычислительной сети. За этот период была настроена популяция нейросетевых детекторов. После завершения этапа обучения рабочая популяция нейросетевых детекторов функционировала в режиме обнаружения аномалий. В этот период в локальной вычислительной сети проводились следующие атаки:

а) TCP SYN сканирование по списку наиболее используемых портов, с определением запущенных на этих портах служб и их версий, а также определением операционной системы сканируемого узла;

б) обнаружение активных узлов по методам ICMP echo request иTCP ACK на порт 80;

в) обнаружение активных узлов по методам ICMP echo request и TCP ACK на порты 21, 23, 80, 3389 (никаких действий после обнаружения не производилось);

г) идентификации операционной системы методом отправки NULL-пакетов (без установленных флагов);

д) имитация сетевого аудита паролей;

е) имитация атаки ARP-spoofing;

ж) имитация атаки Port Stealing.

Для имитации атак использовалось программное обеспечение сканер сетевой безопасности OpenVas.

Тестирование системы обнаружения аномалий с помощью имитации атак проводилось циклом из пяти повторений.

Кроме того, в течение одного дня проводилось тестирование системы на нормально работающей сети.

Получены следующие результаты экспериментальных исследований:

а) при проведении атак типа TCP SYN сканирование, обнаружение активных узлов, идентификация операционной системы и Port Stealing система обнаружения аномалий успешно выявила пять из пяти циклов запуска атак;

б) при проведении атаки типа сетевой аудит паролей система обнаружения аномалий выявила три из пяти циклов проведения атаки;

в) при проведении атаки типа ARP-spoofing

система обнаружения аномалий выявила четыре из пяти циклов проведения атаки.

За 24 часа тестирования в режиме нормального функционирования (при отсутствии атак и аномалий) зафиксировано 2 ложных срабатывания.

Заключение. Результаты экспериментальных исследований позволяют сделать вывод о том, что система обнаружения аномалий с достаточно высокой точностью способна распознавать разнообразные сетевые атаки, имея при этом небольшую долю ложных срабатываний. Таким образом, предложенная идея использования нейросетевых детекторов в иммунном алгоритме для выявления аномалий сетевого трафика является эффективной и может быть успешно использована для выявления нештатных ситуаций и возможных нарушений функционирования вычислительной сети. Кроме того, выбранные параметры сетевой статистики не требуют для своего формирования значительных вычислительных затрат и позволяют результативно выявлять аномалии трафика вычислительной сети.

Библиографический список

1. *Панченко А.А., Аникиенко М.В., Пржегорлинский В.Н.* Анализ подходов к построению системы защиты информации на базе модели процесса обработки данных // Вестник Рязанского государственного радиотехнического университета. 2005. № 16. С. 120-123.

2. *Гончаров В.А.*, *Пржегорлинский В.Н.* Исследование возможностей противодействия сетевым информационным атакам со стороны защищенных ОС и систем обнаружения информационных атак // Вестник Рязанского государственного радиотехнического университета. 2007. № 20. С. 10-14.

3. *Гончаров В.А.*, *Пржегорлинский В.Н.* Метод обнаружения сетевых атак, основанный на кластерном анализе взаимодействия узлов вычислительной сети // Вестник Рязанского государственного радиотехнического университета. 2011. № 36. С. 3-10.

4. *Осовский С.* Нейронные сети для обработки информации. – М.: Финансы и статистика, 2002. – 344 с.

5. *Демидова Л.А., Титов С.Б.* Исследование влияния основных параметров алгоритма функционирования искусственной иммунной сети на качество кластеризации объектов // Вестник Рязанского государственного радиотехнического университета. 2012. № 40. С. 54-60.

6. *Дасгупта Д.* Искусственные иммунные системы и их применение. – М.: ФИЗМАТЛИТ, 2006. – 344 с.

7. *Райх В.В., Синица И.Н., Шарашкин С.М.* Макет системы выявления атак на основе обнаружения аномалий сетевого трафика. http://old.lvk.cs.msu.su /files/mco2005/raih.pdf.

8. *Васютин С.В., Завьялов С.С.* Нейросетевой метод анализа последовательности системных вызовов с целью обнаружения компьютерных атак и классификации режимов работы приложений. http://old.lvk.cs.msu.su/files/mco2005/vasytin.pdf.

9. *Cannady J.* Artificial Neural Networks for Misuse Detection. http://csrc.nist.gov/nissc/1998/proceedings/paperF13.pdf.

10. *Балахонцев А.Ю., Сидорик Д.В., Сидоревич А.Н., Якутович М.В*. Нейросетевая система для обнаружения атак в локальных вычислительных сетях. http://elib.bsu.by/bitstream/123456789/7368/1/34.pdf.