УДК 004.056.53

Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть

© Т.И. Булдакова, А.Ш. Джалолов

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрена задача обнаружения вторжений в корпоративную сеть. Выделены основные компоненты системы обнаружения вторжений и описаны их функции. Выполнен анализ различных подходов к выявлению нарушений информационной безопасности. С этой целью дана характеристика основных методов обнаружения вторжений, выделены их достоинства и недостатки. Показано, что для повышения эффективности выявления ситуаций, связанных с возможным вторжением, необходимо использовать современные технологии интеллектуального анализа данных. Поэтому были исследованы особенности технологий Data Mining для применения в системах обнаружения вторжений, по результатам их сравнительного анализа предложены гибридные средства для выявления атак. Показано, что наиболее перспективным для рассматриваемой задачи является использование нейро-нечетких методов. Предложена архитектура нейро-нечеткой системы для обнаружения вторжений в сеть.

Ключевые слова: *информационная безопасность, вторжения, корпоративная сеть, интеллектуальный анализ данных, нейро-нечеткая система.*

Введение. Системы защиты корпоративной сети должны обеспечивать не только пассивное блокирование несанкционированного доступа извне к ее внутренним ресурсам, но и осуществлять обнаружение успешных атак, анализировать причины возникновения угроз информационной безопасности (ИБ) и, по мере возможности, устранять их в автоматическом режиме. Для повышения эффективности выявления ситуаций, связанных с возможным вторжением, предлагается использовать современные технологии интеллектуального анализа данных – технологии Data Mining.

Основные компоненты системы обнаружения вторжений. Процесс обнаружения вторжений является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Другими словами, обнаружение вторжений – это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы. Главная задача систем обнаружения вторжений (СОВ) заключается в автоматизации функций по обеспечению ИБ корпоративной сети и обеспечении «прозрачности» функций ИБ для неспециалистов в области защиты информации. Поэтому СОВ – это системы, собирающие информацию из различных точек корпоративной сети (защищаемой компьютерной системы) и анализирующие эту информацию для выявления не только попыток, но и реальных нарушений защиты (вторжений) [1–3].

Пусть имеем множество ситуаций нарушения ИБ $X = \{X_1, \ldots, X_l\}$, каждое i-е событие описывается вектором признаков $X_i = (x_{1_i}, x_{2_i}, \ldots, x_{n_i})$, где l – количество угроз ИБ; n – количество признаков. По результатам анализа этих признаков происходит идентификация подозрительной деятельности, и СОВ выполняет определенные защитные действия из множества возможных вариантов $Y = \{y_1, \ldots, y_m\}$, где m – количество защитных мер.

Для реализации функций по защите от вторжений современная СОВ должна содержать следующие основные элементы (рис. 1):

подсистему сбора информации;

подсистему анализа;

модуль управления;

модуль реагирования.

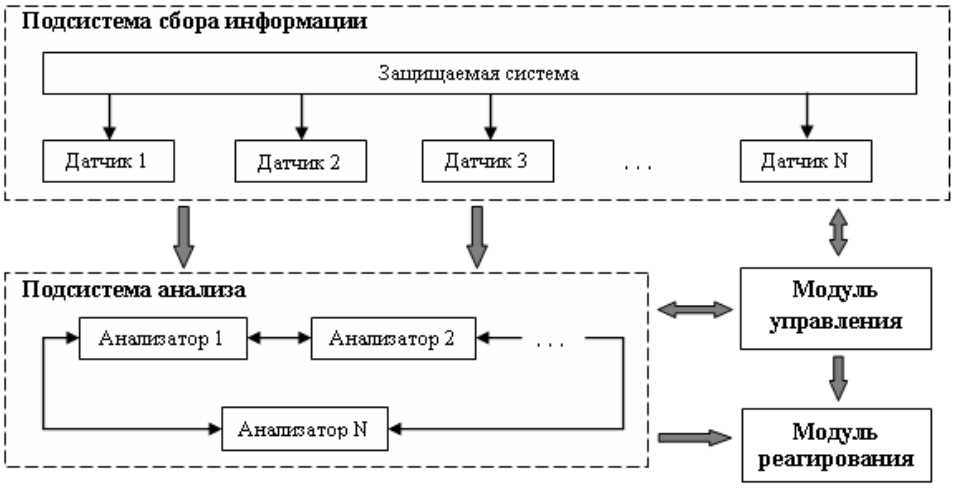


Рис. 1. Общая структура системы обнаружения вторжений

Подсистема сбора информации аккумулирует данные о работе защищаемой системы. Для сбора информации используются автономные модули-датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы.

Подсистема анализа (обнаружения) осуществляет поиск атак и вторжений в защищаемую систему. Она структурно состоит из одного или более модулей анализа – анализаторов. Каждый анализатор выполняет поиск атак или вторжений определенного типа. Входными данными для анализатора является информация из подсистемы сбора информации или от другого анализатора. Результат работы подсистемы представляется в виде индикации о состоянии защищаемой системы и другой необходимой информации.

Модуль управления позволяет управлять компонентами СОВ, а также следить за состоянием защищаемой системы.

Модуль реагирования предназначен для выполнения предопределенных действий в случае установления факта атаки.

Характеристика основных методов обнаружения вторжений. Одним из самых сложных компонентов СОВ является подсистема анализа (выявления нарушений безопасности), от свойств которой фактически зависит безопасность защищаемой корпоративной сети. Эффективность этой подсистемы в значительной степени определяется возможностями используемого метода анализа данных о состоянии защищаемой системы [4, 5]. Поэтому были исследованы наиболее распространенные методы выявления нарушений ИБ (табл. 1).

Таблица 1

Достоинства и недостатки основных методов выявления нарушений ИБ

Метод	Достоинства	Недостатки
Анализ журналов регистрации	простота реализации	ухудшение скорости работы для журналов большого объема; необходима помощь специалистов; нет унифицированного формата хранения журналов; анализ не в реальном времени; на каждый анализируемый узел необходим свой агент
Статистические методы	использование уже разработанного и зарекомендовавшего себя аппарата математической статистики	не чувствительны к порядку следования событий; трудность задания пороговых значений характеристик событий; «статистические» системы могут быть «обучены» нарушителями
Анализ «на лету»	один агент СОВ может просматривать целый сегмент сети; определение атак в реальном масштабе времени; невозможность злоумышленнику скрыть следы своей деятельности	повышенные требования к аппаратному обеспечению (особенно в высокоскоростных сетях); неэффективность работы в коммутируемых сетях и сетях с канальным шифрованием
Профили «нормального поведения»	обнаружение малейших отклонений от «нормального» поведения	большая сложность построения профиля
Использование сигнатур	простота реализации; определение конкретной атаки с высокой точностью и малой долей ложных срабатываний	неспособность выявления новых атак и вторжений; необходимость оперативного обновления баз данных сигнатур; пропуски модификаций известных атак

В последнее время в СОВ стали использовать также технологии интеллектуального анализа данных (Data Mining), позволяющие решать слабоструктурированные и плохо формализуемые задачи, к которым относятся и задачи выявления нарушений ИБ.

Основными целями интеллектуального анализа данных являются поиск функциональных и логических закономерностей в накопленной информации, построение моделей и правил, которые объясняют найденные аномалии и/или прогнозируют развитие некоторых процессов, а также обнаружение скрытых знаний в виде корреляций, тенденций и взаимосвязей, которые аналитик не в состоянии выявить и обобщить самостоятельно. Технологии Data Mining, в отличие от традиционных методов обработки данных, позволяют более эффективно выполнять оценку состояния наблюдаемых процессов, выявлять и ранжировать причины значимых изменений, прогнозировать развитие процессов и вырабатывать рекомендации по подготовке возможных вариантов решений с прогнозом их последствий [6].

Применение технологий Data Mining в СОВ способствует учету профессионального опыта специалистов в области ИБ, принятию решений в условиях неопределенности, адаптации их при появлении новых угроз или их модификаций [7, 8]. С этой целью наиболее часто применяют экспертные системы, нечеткую логику, искусственные нейронные сети.

Особенности технологий Data Mining для обнаружения атак. В экспертной системе знания специалистов-экспертов формализуются в виде набора правил, позволяющих принимать решения в сложных ситуациях. Структурированием знаний экспертов в виде базы знаний занимается аналитик (инженер по знаниям). Основанная на правилах экспертная система состоит из базы знаний, механизма логического вывода, блока объяснения результатов и пользовательского интерфейса. Общая структура экспертной системы (ЭС) приведена на рис. 2.

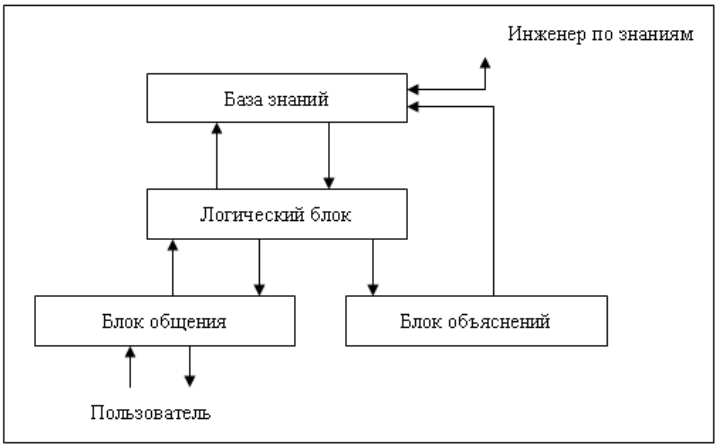


Рис. 2. Структурная схема экспертной системы

Решение задач реализуется с помощью логических выводов на основании знаний, хранящихся в базе знаний. Знания в ЭС организованы в виде системы правил вида:

IF (условие) *THEN* (следствие).

Система логического вывода осуществляет сравнение данных о реальном событии и об эталонной ситуации, хранимой в базе знаний и описывающей наличие вторжений, и в случае совпадения этих данных выполняются заданные действия. Результаты работы ЭС доступны пользователю через диалоговый интерфейс, который позволяет ознакомиться также с ходом логических «рассуждений» системы, которые привели к получению данного результата.

Использование ЭС представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности [4]. Важным достоинством такого подхода является практически полное отсутствие ложных тревог.

База данных (БД) экспертной системы должна содержать сценарии большинства известных на сегодняшний день атак. Для того чтобы оставаться актуальными, экспертные системы требуют постоянного обновления БД, так как даже небольшое изменение уже известной атаки может стать серьезным препятствием для функционирования системы обнаружения атак.

Другим подходом является использование нечеткой логики, которая позволяет применить концепцию неопределенности в логических выводах. Нечеткая логика позволяет описывать правила в незавершенном, «размытом» режиме на основе знаний и весов событий, позволяющих предположить вероятность атаки. В результате можно работать не с конкретными значениями параметров, а с их качественными описаниями.

Степень принадлежности элемента $x \in X$ к нечеткому множеству A описывается его функцией принадлежности $\mu_A(x)$: $X \to [0, 1]$. При этом можно выделить три случая:

1) $\mu_A(x) = 1$ означает полную принадлежность элемента x к нечеткому множеству A, т.е. $x \in A$;

2) $\mu_A(x) = 0$ означает отсутствие принадлежности элемента x к нечеткому множеству A, т.е. $x \notin A$;

3) $0 < \mu_A(x) < 1$ означает частичную принадлежность элемента x к нечеткому множеству A.

Если полное множество X состоит из конечного числа элементов, т. е. $X = \{x_1, x_2, \ldots, x_n\}$, то нечеткое множество A можно представить в следующем виде:

$$A = \frac{\mu_A(x_1)}{x_1} + \frac{\mu_A(x_2)}{x_2} + \ldots + \frac{\mu_A(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu_A(x_i)}{x_i}.$$

Приведенная запись имеет символьный характер. Знак «+» означает не сложение, а скорее объединение. Запись $\frac{\mu_A(x_i)}{x_i}, i = 1, \ldots, n,$ означает, что $\mu_A(x_i)$ относится к элементу x_i, а не означает деление. Фактически запись $\frac{\mu_A(x_i)}{x_i}, i = 1, \ldots, n,$ означает пару $\{x_i, \mu_A(x_i)\}$, $i = 1, \ldots, n$.

Для формализации неточных утверждений типа «x почти равно y» или «x значительно больше, чем y» применяют нечеткие отношения. Нечетким отношением R между двумя непустыми множествами (четкими) X и Y называется нечеткое подмножество прямого декартова произведения $X \times Y$, определяемое следующим образом:

$$R \subseteq X \times Y = \sum_{X \times Y} \frac{\mu_R(x, y)}{x, y}.$$

Если знания представлены с помощью нечетких множеств и нечетких отношений, то для реализации логических выводов в нечеткой среде необходимо применять совокупность правил. Поэтому системы нечеткой логики имеют следующие основные особенности:

– правила принятия решений являются условными высказываниями типа «*IF* …, *THEN* …», которые реализуются с помощью механизма логического вывода;

– вместо одного четкого обобщенного правила нечеткая логика оперирует со множеством частных правил для каждого локального набора данных, для каждой регулируемой величины, для каждой цели управления;

– правила типа «*IF* …, *THEN* …» позволяют решать задачи выбора решения итерационно, в режиме диалога с пользователем, что способствует повышению эффективности этого процесса.

Процесс обработки нечетких правил вывода в системе состоит из четырех этапов:

1) вычисление степени истинности левых частей правил (между «*IF*» и «*THEN*») – определение степени принадлежности входных значений нечетким подмножествам, указанным в левой части правил вывода;

2) модификация нечетких подмножеств, указанных в правой части правил вывода (после «*THEN*»), в соответствии со значениями истинности, полученными на первом этапе;

3) объединение (суперпозиция) модифицированных подмножеств;

4) скаляризация результата суперпозиции – переход от нечетких подмножеств к скалярным значениям.

К основным преимуществам нечеткой логики относятся [9]:

– возможность оперирования нечеткими входными данными;

– возможность нечеткой формализации критериев оценки и сравнения;

– возможность проведения качественных оценок как входных данных, так и выходных результатов;

– возможность проведения быстрого моделирования сложных динамических систем и их сравнительный анализ с заданной степенью точности.

Недостатком нечетких систем является то, что с увеличением входных переменных сложность вычислений увеличивается экспоненциально, в результате увеличивается база правил, что приводит к трудному ее восприятию.

Если структура области решения заранее неизвестна, а известны только отдельные точки области решения, то целесообразно для интеллектуальной обработки информации применить нейронные сети, элементарной составляющей которых является искусственный нейрон. В функциональном отношении его можно представить либо как специализированный процессорный элемент, либо как нелинейный динамический информационный элемент с памятью. Каждый такой элемент (или узел) связан с большим числом других элементов. Особенность этих связей состоит в том, что на вход элемента поступает несколько сигналов $U_{in}(i)$, $i = 1, ..., N$, а на его выходе формируется только один U_{out} (рис. 3).

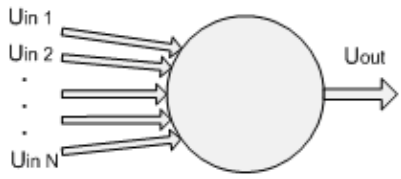


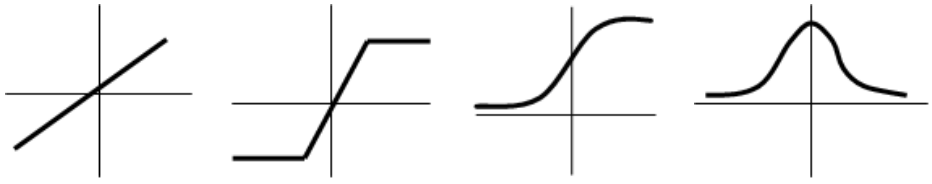
Рис. 3. Схематическое изображение нейропроцессора с N входами и одним выходом

Сигнал U_{out} передается нескольким другим нейронам и так далее. Входные сигналы могут иметь синаптические веса w_i, $i = 1, ..., N$. Математически такой нейропроцессор описывается уравнением

$$U_{out} = f\left[\sum_{i=1}^{N} w_i U_{in}(i) - Q\right],$$

где f – некоторая функция активации, определенная для каждого типа нейрона; Q – порог.

Функция активации определяет зависимость выходного сигнала нейрона от входных сигналов. Эта зависимость может быть выражена с помощью известных функций, например, линейной, кусочно-линейной, сигмоидальной или гауссовой функции (рис. 4).



а *б* *в* *г*

Рис. 4. Различные виды функций активации:

а – линейная функция, *б* – кусочно-линейная функция, *в* – сигмоидальная функция, *г* – функция Гаусса

На практике чаще всего применяют сигмоидальные функции активации. Стандартная сигмоидальная функция определяется как

$$y(x) = \frac{1}{1 + e^{-\beta x}},$$

где β – параметр наклона, который всегда положителен.

Сигмоидальная функция обладает свойством усиливать слабые сигналы и предотвращает насыщение от больших сигналов, так как они соответствуют тем областям аргументов, где сигмоид имеет пологий наклон.

Нейроподобный функциональный элемент (нейропроцессор) является основным процессорным элементом искусственной нейронной сети (ИНС). Фактически ИНС представляет собой адаптивную систему, жизненный цикл которой состоит из двух независимых фаз – фазы обучения сети и фазы работы сети. Обучение считается законченным, когда сеть правильно выполняет преобразование на тестовых примерах и дальнейшее обучение не вызывает значительного изменения настраиваемых весовых коэффициентов. Далее сеть выполняет преобразование ранее неизвестных ей данных на основе сформированной ею в процессе обучения нелинейной модели процесса [9]. Применение нейронных сетей в СОВ позволяет максимально использовать имеющуюся информацию при ограниченном количестве экспериментальных данных.

Если ИНС представляет собой отдельную систему обнаружения атак, то она обрабатывает трафик и анализирует информацию на наличие в нем злоупотреблений. Любые случаи, которые идентифицируются с указанием на атаку, перенаправляются администратору ИБ или используются модулем автоматического реагирования на атаки.

Важным преимуществом ИНС при обнаружении злоупотреблений является их способность «изучать» характеристики умышленных атак и идентифицировать элементы, которые не похожи на те, что

наблюдались в сети прежде. Недостатком нейронных сетей, не позволяющим исследовать процесс формирования классификационных заключений об атаках, является не вполне «прозрачное» представление знаний в информационном поле ИНС и неочевидность процесса формирования результатов их работы.

Сравнительный анализ подходов к интеллектуальному анализу данных показывает, что в каждом из них имеются как сильные, так и слабые стороны. Это отражено в табл. 2, где баллами обозначено: 1 – плохо, 2 – удовлетворительно, 3 – хорошо.

Таблица 2

Сравнительная характеристика интеллектуальных методов анализа вторжений

Характеристики	Экспертные системы	Нечеткие системы	Нейронные сети
Представление знаний	2	3	1
Нечеткие выводы	1	3	3
Адаптируемость	1	1	3
Способность обучения	1	1	3
Описание результата	3	3	1
Простота обслуживания	1	2	3

Из таблицы видно, что целесообразно использовать гибридные средства, в которых сочетаются достоинства отдельных интеллектуальных методов. Сравнение экспертных систем, нечетких систем и нейронных сетей позволяет сделать вывод, что в подсистеме анализа вторжений предпочтительнее сочетать ИНС либо с экспертными системами, либо с подходом нечеткой логики. Поэтому можно выделить следующие варианты применения ИНС в системах обнаружения атак:

1) дополнение нейронной сетью существующих экспертных систем для снижения числа ложных срабатываний, присущих ЭС;

2) нейро-нечеткие методы для обнаружения вторжений.

Нейросетевая экспертная система во многом организована аналогично ЭС. Однако база знаний нейро-экспертной системы организована в виде нейронной сети, знания в которой представлены в форме нечеткого адаптивного распределенного информационного поля. Так как ЭС получает от ИНС данные только о событиях, которые рассматриваются в качестве подозрительных, чувствительность системы возрастает. Если обученная ИНС получила возможность идентифицировать новые атаки, то экспертную систему также следует обно-

вить. В противном случае новые атаки будут игнорироваться ЭС, прежние правила которой не описывают данную угрозу.

Использование нейросетевой базы знаний позволяет устранить один из основных недостатков экспертных систем, основанных на правилах, – невозможность оперирования с не вполне достоверной информацией.

Более перспективным подходом для обнаружения атак является объединение возможностей нейронных сетей и нечеткой логики, поскольку нечеткие ИНС объединяют достоинства ИНС и нечеткой логики, опирающейся на опыт экспертов в области ИБ. Именно нечеткая логика наилучшим образом дополняет нейронные сети, компенсируя две основные «непрозрачности» ИНС: в представлении знаний и объяснений результатов работы интеллектуальной системы. Нечеткие ИНС позволяют решать не только отдельно взятые задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, но и автоматически формировать новые правила при изменении угроз.

Нейро-нечеткая система для обнаружения вторжений в сеть. Применение нечетких нейронных сетей в СОВ обеспечивает: функциональную устойчивость; возможность классификации угроз; описание соответствия «угрозы – механизмы защиты» в виде системы нечетких предикатных правил; адаптивность нейро-нечетких систем защиты информации (системы нечетких правил).

Пусть существует неизвестная целевая зависимость – отображение $y^* : X \to Y$, значения которой известны только на объектах обучающей выборки $X^r = \left[\left(x_1, y_1 \right), \ldots, \left(x_r, y_r \right) \right]$ размерностью r. Применение нейро-нечеткой системы позволяет аппроксимировать неизвестное отображение в виде алгоритма $a : X \to Y$, способного идентифицировать событие ИБ по вектору его признаков и определить защитные действия. Для этого используется множество нечетких правил $R = \left\{ R_1, \ldots, R_k \right\}$ вида:

$$
\begin{aligned}
&R_1 : \text{если } x_1 \in A_1^1 \text{ и } \ldots x_n \in A_1^n, \text{ то } Y \text{ есть } y_1, \\
&R_2 : \text{если } x_1 \in A_1^1 \text{ и } \ldots x_n \in A_2^n, \text{ то } Y \text{ есть } y_2, \\
&\ldots \\
&R_k : \text{если } x_1 \in A_{k_1}^1 \text{ и } \ldots x_n \in A_{k_n}^n, \text{ то } Y \text{ есть } y_m,
\end{aligned}
$$

где A_i^j – соответствующие нечеткие множества, $k = k_1, \ldots, k_n$.

Структурная модель СОВ, включающая нейро-нечеткую систему для идентификации события ИБ, показана на рис. 5.

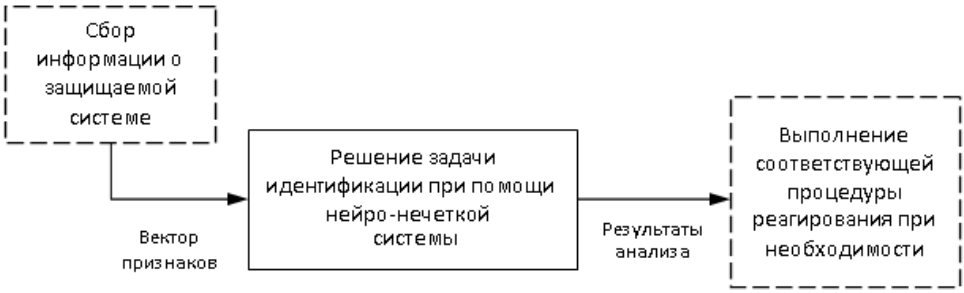


Рис. 5. Структурная модель системы обнаружения вторжений

Нейро-нечеткая система представляет собой ИНС (рис. 6), которая является адаптивным функциональным эквивалентом нечеткой модели вывода [7]. Знания квалифицированных специалистов в области ИБ, представленные в форме нечетких переменных и нечетких правил, отражаются в структуре нейро-нечеткой сети.

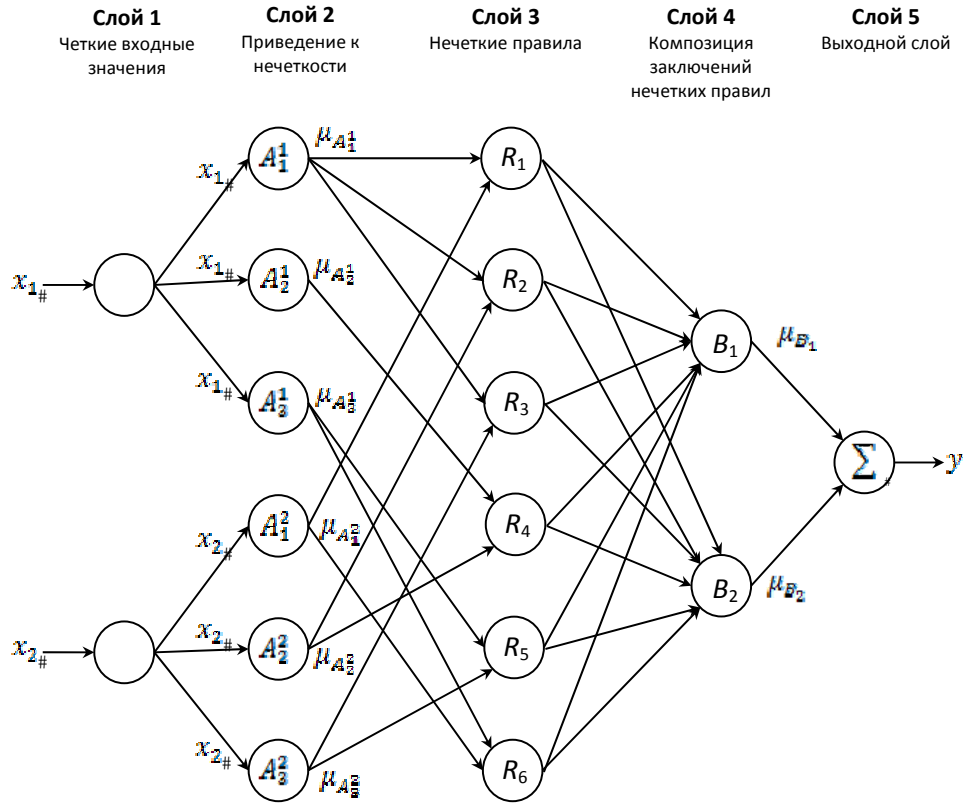


Рис. 6. Нейро-нечеткая сеть

Основные этапы нечеткого логического вывода распределены по слоям ИНС и реализуются, к примеру, для сети с двумя входами x_1, x_2 и одним выходом y следующим образом:

1) введение нечеткости выполняется слоем входных функций принадлежности $\mu_{A_1^1} - \mu_{A_3^1}$, $\mu_{A_1^2} - \mu_{A_3^2}$, осуществляющих преобразование каждого из четких входных значений x_1 и x_2 в степень истинности соответствующей предпосылки для каждого правила;

2) нечеткому логическому выводу соответствует слой нечетких правил $R_1 - R_6$, который по степени истинности предпосылок $\mu_{A_i^1}$, $\mu_{A_i^2}$, $i = 1, 2, 3$ формирует заключения по каждому из правил;

3) композиция заключений нечетких правил $R_1 - R_6$ проводится слоем выходных функций принадлежности μ_{B_1}, μ_{B_2} (output membership functions) с целью формирования нечетких подмножеств B_1, B_2;

4) композиция нечетких подмножеств B_1, B_2 и приведение к четкости выполняется в выходном слое и приводит к формированию выходного четкого значения y.

Так как в архитектуре нейро-нечеткой системы используются нечеткие правила, основанные на знании экспертов в области защиты информации, то для обучения целесообразно выбрать метод обучения с учителем, например, метод минимизации среднеквадратичной ошибки [9]. Его преимущества состоят в возможности широкого использования и математической простоте. В качестве функций активации нейронов предпочтительнее выбрать сигмоидальные, а в качестве функций принадлежности можно выбрать, например, *Z*-образные и *S*-образные функции.

Обучение нечеткой ИНС позволяет не только настроить веса связей (т. е. откорректировать достоверность отдельных нечетких правил), но и устранить противоречивость системы нечетких правил в целом. В случае отсутствия априорной информации по данной предметной области, но при достаточном объеме обучающей выборки нейро-нечеткая сеть автоматически преобразует скрытые в данных обучающей выборки закономерности в систему правил нечеткого логического вывода.

Таким образом, применение нейро-нечеткой системы является наилучшим вариантом построения одного из модулей СОВ, который будет проводить анализ данных, полученных от подсистемы сбора информации, и сообщать об обнаружении несанкционированных действий, подтверждая факт наличия вторжения или атаки.

Заключение. Выполнен анализ существующих подходов для решения задачи обнаружения вторжений в корпоративную сеть. Показано, что перспективным направлением при разработке средств обнаружения атак является использование технологий Data Mining. Поскольку системы нечеткой логики компенсируют основные «не-

прозрачности» ИНС в представлении знаний и объяснении результатов работы интеллектуальной системы, то для построения модуля анализа информации в СОВ предложена нейро-нечеткая система. Более того, включение нечеткой логики в состав нейросетевых средств обнаружения атак на корпоративную сеть позволяет учитывать априорный опыт экспертов ИБ, реализовать присущее нейронным сетям нечеткое представление информации, извлекать знания из входных неполных и не вполне достоверных данных.

ЛИТЕРАТУРА

[1] Шаньгин В.Ф. *Информационная безопасность компьютерных систем и сетей*. Москва, ИД «ФОРУМ»: ИНФРА-М, 2008, 416 с.

[2] Мельников В.В. *Защита информации в компьютерных системах*. Москва, Финансы и статистика, 1997, 368 с.

[3] Allen J., Christie A., Fithen W. et al. *State of Practice of intrusion detection technologies*. *Technical Report CMU/SEI-99-TR-028*. Carnegie Mellon Software Engineering Institute, 2000.

[4] Лукацкий А.В. *Обнаружение атак*. 2-е изд. СПб.; БХВ-Петербург, 2003, 596 с.

[5] Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков. *Инженерный журнал: наука и инновации,* 2012, вып. 3. URL: http://engjournal.ru/catalog/it/security/127.html

[6] Булдакова Т.И., Джалолов А.Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах. *Научно-техническая информация*. Серия 1, 2012, № 6, с. 16–22.

[7] Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф., Воскресенский С.И. К моделированию адаптивной системы информационной безопасности. *Перспективные информационные технологии и интеллектуальные системы*, 2004, № 4, с. 25–31.

[8] Negnevitsky M. *Artificial intelligence: a guide to intelligent systems.* 2nd edition. Harlow, England: Addison-Wesley, 2005, 415 p.

[9] Круглов В.В., Дли М.И., Голунов Р.Ю. *Нечеткая логика и искусственные нейронные сети*. Москва, Физматлит, 2001, 224 с.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Булдакова Т.И., Джалолов А.Ш. Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть. *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/987.html

Булдакова Татьяна Ивановна окончила МВТУ им. Н.Э. Баумана в 1980 г. Д-р техн. наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор около 150 опубликованных работ. Область научных интересов: информационно-аналитические системы, интеллектуальные технологии, системный анализ, моделирование. e-mail: buldakova@bmstu.ru

Джалолов Ахмад Шарофиддинович окончил Финансовую академию при Правительстве Российской Федерации в 2010 г. Аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор шести опубликованных работ. Область научных интересов: информатизация органов государственного управления, ситуационные центры, системы поддержки принятия решений.