МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ
АЗЕРБАЙДЖАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ

ДИССЕРТАЦИОННАЯ РАБОТА

Тема:	**“Построение интеллектуальных интегрированных систем информационной безопасности в открытых корпоративных сетях”**
Студент:	**Асланов К.Дж.**
Факультет:	**“Информатика”**
Спец.:	**«Экономические информационные системы»**
Группа:	
Руководитель:	**Байрамов Х.**

Баку – 2018

СОДЕРЖАНИЕ

Введение

Поступательное развитие информационно-коммуникационных технологий осуществляется в направлении создания корпоративных информационных систем с элементами обучения, в которых присутствуют природоподобные процессы возникновения, адаптации и развития. Развитие структур природоподобных систем привело к разработке теории искусственных нейронных сетей, нечёткой логики и математического аппарата теории нечётких множеств, т.е. методов информационной технологии Soft Computing, которые легли в основу создания автономных интеллектуальных систем.

Для аналитической поддержки интеллектуальных процессов в системах информационной безопасности с каждым годом все больше применяются и совершенствуются методы нечётких вычислений, которые, основываясь на эвристических знаниях специалистов по информационной безопасности, хорошо показали себя в условиях неполной истинности и неопределённости релевантной информации. При этом, задачи оптимизации типа «финансовые затраты / степень защищённости» в корпоративных сетях открытого типа все чаще решаются посредством эволюционного программирования, включающего всевозможные алгоритмы обучения, в том числе и генетически. В дополнение к этому применяемы здесь нейросетевые технологии обеспечивают создание адаптивных механизмов информационной защиты.

Эволюционное программирование опирается на алгоритмы, которые обеспечивают итерацию процесса популяции живых организмов. Популяция на начальной стадии создаётся в результате некоторого опыта, накопленного в прошлом. В процессе эволюции формируется новая популяция посредством селекции наилучших индивидуумов путём многокритериальной оценки. При этом каждый выбранный индивидуум представляет собой потенциальное решение задачи, в частности, информационной безопасности.

В контекстной области нашего исследования выбор в определённом смысле подходящих решений осуществляется на основе применения слабо

структурированных (качественных) критериев оценки. По результатам выбора некоторого списка популяций, как допустимых решений, становится возможным получить оптимальный индивидуум, наиболее полно отвечающий критерию оценки. Претерпевая преобразования популяции в целом, каждый индивидуум повышают свою выживаемость и этот принцип, собственно, и лёг в основу эволюционного программирования, который стал путеводной звездой при решении следующих задач данной диссертации:

- проектирование модели адаптивной информационной защиты корпоративных сетей открытого типа на основе природоподобных гибридных средств защиты информации.
- исследование комплексной системы оценок информационной защищённости корпоративных сетей открытого типа.
- исследование методики проектирования многоуровневой иерархической системы защиты информации на основе экспертных оценок.

При изложении основных вопросов диссертации применялись хорошо известные методы теории информационной безопасности в корпоративных сетях, теории искусственных нейронных сетей, элементы нечёткой логики и математического аппарата теории нечётких множеств. В контексте проводимых исследований особое место было уделено нейросетевому моделированию и применению нейронных сетей, нейро-нечётких (гибридных) систем защиты информации.

Глава I. МЕТОДЫ И СРЕДСТВА МОДЕЛИРОВАНИЯ СЛАБО СТРУКТУРИРОВАННЫХ ПРОЦЕССОВ И ЯВЛЕНИЙ

1.1. Нечёткая логика и нечёткое моделирование, как новый подход к информатизации слабо структурированных объектов

Умение анализировать и прогнозировать социально значимые процессы и явления в условиях неопределённости, одним из факторов которой является слабо структурированность доступной информации, становятся определяющими в проблематике описания информационных угроз, где возможность преодоления существующей неопределённости всё чаще рассматривают в применении новых методов и моделей. Сегодня одним из наиболее перспективных направлений научных исследований в области анализа, моделирования и прогнозирования слабо структурированных процессов и явлений являются нечёткая логика и математический аппарат теории нечётких множеств.

Используемое на протяжении последних десятилетий классическое системное моделирование, как единственно доступный механизм в исследованиях проблемы информационной безопасности, не смогло дать адекватного существующим угрозам результата.

Механизм нечёткого логического вывода, позволяющий объективно отражать причинно-следственные связи между слабо структурированными и/или вовсе неструктурированными характеристиками, более адекватен процессу выявления информационных угроз на самой ранней стадии, «пластично» учитывает особенности потенциальных атак.

Именно это позволяет нам утверждать, что посредством нечеткого моделирования можно добиться результатов, которые по сравнению с методами системного моделирования будут более содержательными и полезными в создании средств информационной безопасности в открытых корпоративных

телекоммуникационных сетях связи, т.к. нечёткая математика позволяет на ряду с обычными числами вовлечь в вычислительный процесс неметризуемые показатели, которыми насыщено все информационное пространство.

Одним из главных преимуществ нечёткого моделирования является его способность к быстрой адаптации на предмет решения новых классов информационных угроз. На основе базовых лингвистических правил создаётся так называемая «грубая» нечёткая модель, которая в условиях эксплуатации системы информационной защиты и программной симуляции (например, в нотации пакета прикладных программ MATLAB) может быть скорректирована и представлена второй моделью. Далее, в процессе эксплуатации пользователь этой модели может обнаружить новые закономерности и взаимосвязи и, тем самым, трансформировать её в более адекватную причинно-следственную связь. Процесс адаптации нечёткой модели является итерационным и длится ровно столько, сколько необходимо шагов для идентификации новых параметров, обеспечивавших адекватное сходство с реальными векторами признаков информационных угроз.

Сам процесс нечёткого моделирования подразумевает:

- развёртывание модели;
- редуцирование модели;
- свёртывание модели;
- конкретизация модели (это фактически вход в методику, то есть использование полученных результатов на практике предотвращения информационных угроз);
- обобщение модели (это уже развитие методики, то есть осознание, осмысление, систематизация полученных результатов внутримодельного исследования на благо и совершенствование самой адаптивной системы информационной защиты).

При этом, характерными особенностями нечёткого моделирования являются:

- нечёткое моделирование позволяет получать более адекватные результаты по сравнению с результатами, которые основываются на использовании методов системного моделирования;
- система нечёткого логического вывода (*Fuzzy Inferences System*), как основа реализации нечёткого моделирования, более естественно описывает характер человеческого мышления и особенно ход рассуждений специалиста по информационной безопасности, чем традиционные формально-логические системы;
- модель, как некоторое представление о системе, отражающая наиболее существенные закономерности её структуры и процесса функционирования, возможно потребует изменения формы представления: вместо традиционных форм (словесная, графическая, табличная), потребуется технологическая документалистика (технологическая карта, информационная карта предотвращения угроз и т.д.);
- общее свойство любой модели – её подобие (адекватность) реальному объекту или системе-оригиналу. Продуктивность построенной модели прежде всего связана с возможностью её применения для получения новой информации о свойствах, закономерностях поведения и функционирования системы-прототипа.
- сам процесс построения моделей и их применения для получения информации о системе-прототипе и составляет суть основного содержания процесса нечёткого моделирования.
- особый класс – управляющие переменные, которые значимы для принятия управленческих решений и смысл которых – оказывать на систему целенаправленное воздействие, оптимально обеспечивающее достижение цели.

В тоже время информационная технология, применяемая в корпоративных сетях, предоставляют пользователю новые инструментальные средства, с помощью которых можно:

- формировать конкретные значения входных параметров модели;
- после одной итерации, получить конкретизацию значений выходных параметров (например, содержательная модель оценки уровней информационных угроз);
- получить оценку точности и верификацию результатов и проверить согласованность значений отдельных параметров модели;
- содержательно интерпретировать полученные результаты в форме управляющих воздействий;
- оценить потенциальную возможность реализации полученных результатов внутри модельного исследования.

Таким образом, исследовательские аспекты модельных представлений в сфере информационной безопасности связаны с:

- неясностью и нечёткими границами потенциальных угроз и информационных атак;
- неоднозначностью семантики отдельных признаков информационных угроз, используемых в процессе отражения информационных атак;
- неполнотой модельных представлений о потенциальных информационных угрозах, при решении проблем, связанных с информационной безопасностью в открытых корпоративных компьютерных сетях;
- невозможностью учёта всех релевантных особенностей решаемых проблем информационной безопасности, как в теории, так и на практике информационной защиты;
- противоречивостью отдельных компонентов векторов признаков информационных угроз;
- неопределённостью наступления некоторых нежелательных событий, относящихся к вероятной возможности информационного коллапса в открытых корпоративных сетях.

1.2. Нечётко-множественное описание в анализе информационных потоков

Понятие нечёткого множества, давшее название одноименной теории Fuzzy Logic, профессор информатики Калифорнийского Университета (Беркли, США) Л.А. Заде (L.A. Zadeh) ввёл в 1965 году [24, 25]. В отличие от стандартной логики Аристотеля, предусматривающей два бинарных состояния (1/0, Да/Нет, Истина/Ложь, On/Off и т.д.), нечёткая логика, как известно, позволяет определять промежуточные значения между стандартными оценками. Примерами таких оценок являются: «БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ», «МЕНЕЕ ВЫСОКИЙ УРОВЕНЬ», «СКОРЕЕ НЕТ, ЧЕМ ДА», «НАВЕРНОЕ ДА», «РЕЗКО ВПРАВО», «РЕЗКО ВЛЕВО» в отличие от стандартных: «ВЫСОКИЙ УРОВЕНЬ» или «НИЗКИЙ УРОВЕНЬ», «ВПРАВО» или «ВЛЕВО», «ДА» или «НЕТ». С помощью разработанного математического аппарата нечётких множеств стало возможным математически формулировать подобные оценки и впоследствии обработать их на компьютере. В результате удалось существенно приблизить механизм компьютерной обработки и анализа данных к человеческому мышлению.

При зарождении теории нечётких множеств первоначальным замыслом являлось построение функционального соответствия между термами (значениями) лингвистических переменных (таких, например, как «ВЫСОКИЙ», «ТЕПЛЫЙ», «ПРИВЛЕКАТЕЛЬНЫЙ» и т.д.) и специальными функциями, выражающими степень принадлежности значений измеряемых параметров (в данном случае, длины, температуры, внешность и т.д.). В качестве примера таких описаний выберем следующую задачу.

Пусть имеется некоторое множество сообщений, поступивших в режиме *on-line* в бухгалтерию от респондентов (например, руководителей региональных филиалов компании или дочерних организаций), фиксирующих текущие финансовые показатели. Предположим, что профильные специалисты

компании мысленно ранжируют величину этих показателей как «СООТВЕТСТВУЮЩАЯ НОРМЕ», «ВЫСОКАЯ», «ОЧЕНЬ ВЫСОКАЯ», «НЕДОСТАТОЧНАЯ», «НИЗКАЯ» и т.п. При этом возникает вопрос: как определить, например, понятие (терм) «СООТВЕТСТВУЮЩАЯ НОРМЕ» в обычной (булевой) логике? Для этого необходимо задать нормативный интервал, для которого можно считать, что финансовый показатель является «СООТВЕТСТВУЮЩИМ НОРМЕ». Допустим, по 9-ти балльной системе это отрезок [5.5; 6.5]. Тогда, согласно стандартной логике, все сообщения респондентов о финансовых показателях в своих филиалах, попадающие в данный интервал, можно считать «СООТВЕТСТВУЮЩИМИ НОРМЕ», а остальные, как «НЕСООТВЕТСТВУЮЩИМИ НОРМЕ».

Тем не менее, может возникнуть вполне резонный вопрос: «А что же показания респондента 6.5001 или 5.4999 можно считать уже недостаточными для определения финансового показателя, как соответствующий норме?» Это и есть главный недостаток чёткой (бинарной) логики. При этом нечёткая логика позволяет ослабить такое строгое разделение в градациях.

Обычно профильный специалист компании, обрабатывающий респондентские данные, действует формально и строго по инструкции: если финансовый показатель составляет 6.5001, или скажем, 5.4999, тогда уровень контрагента по данному показателю является ВЫСОКИМ, или, соответственно, НЕДОСТАТОЧНЫМ, а это уже являются характеристиками из принципиально других уровней и порядков оценки финансовых показателей.

Для показаний финансовых показателей, попавших в отрезок [5.5; 6.5], профильный специалист компании с огромной долей уверенности может утверждать, что финансовое состояние контрагента соответствует норме. Поэтому данному высказыванию будет соответствовать значение 1. Если же финансовый показатель имеет значение 6.5001 или 5.4999, то ему будет ставиться в соответствие значение 0. Другими словами, чем ближе значение финансового показателя к интервалу [5.5, 6.5], тем более уверенно профильный

специалист компании может утверждать, что данный контрагент является успевающим, то есть оценка его уверенности (или достоверности высказывания) будет близка к 1. При удалении от указанного интервала «СООТВЕТСТВУЮЩАЯ НОРМЕ» как в сторону его увеличения, так и в сторону уменьшения значений финансовых показателей, значение достоверности высказывания будет постепенно снижаться до нуля.

Таким образом, данный математический аппарат позволяет сформулировать и математически описать какое-либо качественное понятие – значение лингвистической переменной (терм) посредством так называемой функции принадлежности и далее использовать её как точный механизм, не заботясь более о его «нечёткой» природе.

Графическое описание понятия «СООТВЕТСТВУЮЩАЯ НОРМЕ» (функции принадлежности нечёткого множества «СООТВЕТСТВУЮЩАЯ НОРМЕ») представлено на рис. 1.1.

Рис. 1.1. Трапецеидальная функция принадлежности нечёткого множества «СООТВЕТСТВУЮЩАЯ НОРМЕ»

В качестве функции принадлежности здесь выбрана трапецеидальная функция. Участок трапеции BC (верхнее основание) соответствует интервалу от 5.5 до 6.5. Высказыванию «СООТВЕТСТВУЮЩАЯ НОРМЕ» для этого участка будет соответствовать достоверность равная единице. Участки AB и CD иллюстрируют тот факт, что, если показания респондента попадают в

интервалы от 5.0 до 5.5 и от 6.5 до 7.5, то достоверность высказывания в том, что финансовое состояние контрагента соответствует норме, соответственно, снижается или увеличивается. Формальное описание данной функции выглядит следующим образом:

$$\mu(x) = \begin{cases} 0, & 0 \le x < 5; \\ \frac{10}{7}(x-1), & 5 \le x < 5.5; \\ 1, & 5.5 \le x \le 6.5; \\ \frac{10}{13}(4-x), & 6.5 < x \le 7.5; \\ 0, & 7.5 < x \le 9. \end{cases}$$

Прорывным достижением в развитии математической теории нечётких множеств явилось введение в обращение так называемых нечётких чисел – нечётких подмножеств специализированного вида, соответствующих высказываниям типа «значение переменной примерно равно 9». В качестве примера приведём треугольное нечёткое число с тремя выраженными точками: «МИНИМАЛЬНО ВОЗМОЖНОЕ», «НАИБОЛЕЕ ОЖИДАЕМОЕ» и «МАКСИМАЛЬНО ВОЗМОЖНОЕ» значения рассматриваемого фактора.

Нечёткие треугольные числа – это самый часто используемый на практике тип нечётких чисел, причём чаще всего их используют в качестве прогнозных значений параметра, например, ожидаемое годовое значение среднего балла успеваемости в школе. Предположим, что наиболее вероятным значением среднего балла будет 12%, минимально возможным – 7%, а максимально возможным – 18%. Тогда все эти значения могут быть представлены в виде нечёткого числа $\tilde{A}$ с так называемым опорным вектором (7; 12; 18).

В последующем введение набора операций над нечёткими числами, которые сводятся к алгебраическим операциям с обычными числами при задании определённого интервала достоверности (уровня принадлежности),

получившие в последующем название – Мягкие Вычисления (Soft Computing), предопределило следующий исторический шаг в развитии нечёткой логики. Фундаментальные исследования в этой области были предприняты Д. Дюбуа (D. Dubois) и Х. Прадом (H. Prade). Параллельно с разработкой теоретических основ нечёткой логики, Л. Заде прорабатывал различные возможности ее практического применения. В 1973 году эти усилия увенчались успехом: ему удалось показать, что нечёткая логика может быть положена в основу нового поколения интеллектуальных систем управления. Именно поэтому эту дату логично считать началом второго этапа в развитии нечёткой логики.

За первые тридцать лет своего развития нечёткая логика значительно обогатилась, претерпев ряд существенных изменений и дополнений. В частности, усилиями Б. Коско (B. Kosko) была исследована взаимосвязь нечёткой логики и теории нейронных сетей и доказана основополагающая аппроксимационная теорема (Fuzzy Approximation Theorem), подтвердившая полноту нечёткой логики.

В работах М. Земанковой (M. Zemankova) и А. Кандела (A. Kandel) были заложены основы теории нечётких систем управления базами данных, способных оперировать доступными неточными данными, обрабатывать нечётко заданные запросы, а также наряду с количественными использовать неметризуемые качественные параметры. Ими была разработана нечёткая алгебра, позволяющая при вычислениях комбинировать точные (crisp) и приблизительные значения переменных. И наконец, самое широкое распространение получили изобретённые Б. Коско так называемые нечёткие когнитивные модели (Fuzzy Cognitive Maps), на которых базируется большинство современных систем динамического моделирования в области финансов, политики и бизнеса.

Развитая Б. Коско и другими видными учёными нечёткая логика Л. Заде, впервые имплементированная американскими фирмами в коммерческие системы управления сложными технологическими процессами, за свой более

чем полувековой период существования успела родиться три раза. Эта область знаний является одним из немногих научных направлений, которая была создана в США, развита в Японии и только после этого была вновь признана американцами, которые к тому времени уже безнадёжно утратили стратегическую инициативу.

1.3. Нечётко-множественное моделирование в условиях неопределённости

Проблемами управления слабо структурированными системами в разное время занимались многие исследователи. Наибольший вклад здесь внесли Н. Винер, Л. Заде, Р. Беллман, Р. Циммерман, Я.З. Ципкин, А.А. Красовский, Г.С. Поспелов, Д.А. Поспелов, А.Н. Аверкин, А.Н. Мелихов и многие другие.

Слабо структурированность систем порождается неопределённостью, в условиях которой, собственно, и осуществляется наблюдение за ее поведением. Сам термин «неопределённость» трактуется довольно неоднозначно. Это и понятно, т.к. неопределённость зависит от предметной области исследования и характера той задачи, которую стараются решить. В своей основополагающей работе «Risk, Uncertainty and Profit» Ф. Найт (F. Knight) установил различие между понятиями *риск* и *неопределённость*. Согласно его исследованиям, суть неопределённости радикально отличается от близкого, казалось бы, по смыслу понятия риска. Им было установлено, что имеют место два вида неопределённости: *измеряемая неопределённость*, являющаяся, по сути, риском, и *не измеряемая неопределённость*. Другими словами, риск он определил, как неопределённость, основанную на строго обоснованной (количественной) вероятности.

Формально, риск определяется как вероятность наступления некоторого события, помноженная на его последствия (если событие совершится). *Истинная неопределённость* (то есть неопределённость в чистом виде) не

может быть представлена подобным образом. Более того, истинная неопределённость чаще всего не может быть описана одним только старанием добыть все больше информации об исследуемом феномене в задаче и ее производных.

Все существующие в настоящее время формальные описания экономики страдают либо *неполнотой*, либо *противоречивостью*, либо и тем и другим. Это объясняется тем, что любой формальный аппарат представления знаний в вычислительной среде априори обладает НЕ-факторами. Содержательную и обоснованную трактовку понятия «НЕ-факторы» в 1982-ом году дал А.С. Нариньяни, который впервые сделал попытку сравнительного рассмотрения комплекса факторов, активно моделируемых в инженерии знаний и некоторых технических приложениях, но недостаточно изученных или вообще игнорируемых в традиционной математике. НЕ-факторами они были названы, поскольку каждый из них получил наименование, лексически и содержательно отрицающее одно из традиционных свойств формальных систем – *точность, полноту, определённость, корректность* и т.п. Другими словами, НЕ-факторы – это попытка на лингвистическом уровне зафиксировать учёт наших «незнаний» при абстрагировании, переходе к формальным системам и интерпретации выводов, полученных на формальном уровне.

Естественно, что феномен неопределённости должен быть учтён и при выработке и описании учебно-методического поведения или, другими словами, при принятии различных учебно-методических решений. В настоящее время для принятия решений в условиях неопределённости современная наука активно применяет аппарат нечётких множеств и его составные части – механизм нечёткого вывода, нечёткую математику и др. Поэтому рабочий формализм

$$\tilde{Y} = F[(\tilde{X}_1, \tilde{X}_2, \ldots, \tilde{X}_n)]$$

для описания процесса принятия решений в условиях неопределённости целесообразно представлять в виде «чёрного ящика» (см. рис. 1.2), входы и выходы которого описываются нечёткими множествами.

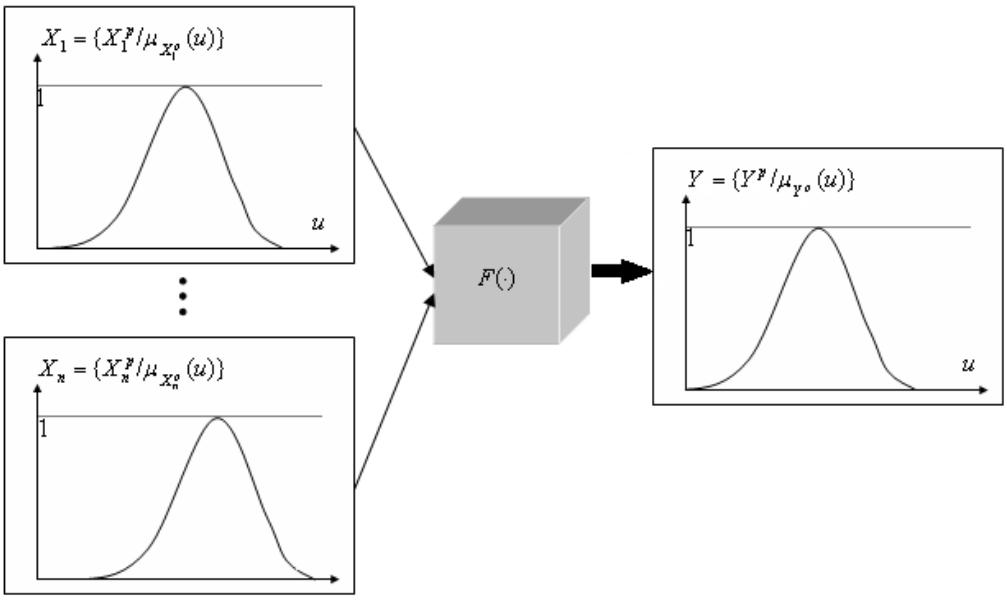

Рис. 1.2. Общая схема многокритериального выбора в условиях неопределённости

Принцип «чёрного ящика», как известно, является основным принципом информационной модели. В противоположность аналитическому методу, при котором моделируется внутренняя структура системы, при подходе «чёрный ящик» моделируется внешнее функционирование системы. С точки зрения пользователя, структура модели системы, «спрятанная в чёрном ящике», имитирует процесс принятия решений на основе данных экспериментов или наблюдений.

Моделирование на основе «чёрного ящика» проигрывает «жёстким» математическим формализмам и экспертным системам по степени «объяснимости» полученных результатов. Тем не менее, отсутствие ограничений на сложность моделей многокритериальных оценок определяет важную практическую значимость информационных моделей. Можно выделить несколько типов «черных ящиков», которые отличаются характером запросов к

ним и на основе которых осуществляется постановка основных задач анализа и моделирования процессов принятия решений. Перечислим некоторые из них. Это:

- моделирование отклика слабо структурированной системы на внешние воздействия;
- классификация внутренних состояний слабо структурированной системы;
- прогноз динамики изменения слабо структурированной системы;
- оптимизация параметров слабо структурированной системы относительно заданной целевой функции;
- оценка полноты описания слабо структурированной системы и сравнительная информационная значимость её параметров.

Глава II. ИНТЕЛЛЕКТУАЛЬНЫЕ СРЕДСТВА МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ БЕЗОПАСНОСТИ

Необходимость интеграции эволюционных особенностей в системах информационной безопасности, таких как развитие биосистемы и адаптируемость, активно обсуждается в ряде научных и научно-технических средств информации [74]. Такие известные IT-вендоры как Microsoft сообщают о внедрении «активных технологий защиты» на основе компилированных ими программ оценки поведения с точки зрения существующих потенциальных угроз [88]. В частности, если имеют место вмешательство компьютерного вируса или хакерские атаки, то предлагаемые ими интеллектуальные средства информационной безопасности регулирует защиту компьютерной сети или блокирует её [85].

2.1. Анализ использования интеллектуальных средств в системах защиты информации

Проблема эволюции систем информационной безопасности все ещё остаётся актуальной. В дополнение к обычным средствам защиты, таким как антивирус, детекторы уязвимостей, сетевые экраны и детекторы для корпоративных сетей, также используется автоматическая защита [37], в том числе:

- *корреляторы событий* – учреждается для анализа журналов средств информационной безопасности, операционных систем и приложений, а также для анализа признаков информационных атак;
- *программы обновления* – устанавливаются для устранения недостатков (прежде всего – ошибок программного обеспечения), идентифицированных как автоматизация процедур коррекции и поиска потенциальных слабых мест системы;

- *средства аутентификации, авторизации и администрирования* – устанавливаются для идентификации информации и аутентичности вмешательства пользователей в информационные ресурсы;
- *системы управления рисками* – предназначены для моделирования и идентификации возможного ущерба в результате нападения на корпоративную сеть.

2.1.1. Интеллектуальные средства и проблемы защиты информации

Большинство публикаций по использованию интеллектуальных систем информационной безопасности в основном посвящены системам, которые способны обнаруживать информационные атаки [11, 26, 34, 54, 55, 59, 60, 61, 98]. В качестве интеллектуальных средств здесь активно и плодотворно рассматриваются такие средства, как искусственные нейронные сети (ANN – *Artifical Neural Networks*), нечёткие логические системы (FIS – *Fuzzy Inferences Systems*) и интеллектуальные экспертные системы (IES – *Intellectual Expert Systems*) [29, 30, 38, 40, 118, 124].

Схемы обнаружения атак делятся на две категории: 1) идентификация злоупотреблений; 2) обнаружение или выявление аномалий. Первая категория включает обнаружение известных недостатков IT-систем, а вторая – выявляет не свойственные пользователям IT-систем формы поведения. Для обнаружения аномалий определены действия, которые отличаются от шаблонов, назначенных пользователям или группам пользователей. Обнаружение аномалий, как правило, связано с базой данных контролируемых действий [99, 108, 120], а обнаружение злоупотреблений происходит в результате сравнения активности пользователя с известными образцами хакерского поведения и описывает сценарии атак, используя методы, полученные из так называемых предикатных правил вида «*IF* <...>, *then* <...>» [97, 111]. Если активность пользователя не совпадает с установленными экспертами предикатными

правилами и/или не соответствует им, то механизм обнаружения идентифицирует потенциальные атаки.

Большинство систем обнаружения непроизвольного, злонамеренного поведения и различного рода аномалий основаны на предложенной Д. Денингом (Denning D.E.) модели [102]. Эта модель поддерживает набор профилей для законных пользователей, выравнивает соответствующий поднабор подсистемы аудита, делает профиль в режиме *off-line* и сообщает обо всех обнаруженных аномалиях.

В целях определения аномального поведения путём сравнения нормального режима работы системы с ситуациями, спровоцированными поведениями пользователей, часто используют статистические методы анализа. Поведение пользователя можно проиллюстрировать в виде модели на основе подхода, предложенного в [105]: прогностическими шаблонами [125] или анализом изменений ситуаций [118]. Чтобы обнаружить факт нанесения информационной атаки, они используют простые методы сравнения.

В системах обнаружения информационных атак можно указать следующие примеры приложения нейронных сетей. С целью исключения ложных подключений к работе обнаружения информационных угроз, которые в основном присущи существующим экспертным системам, активно применяются нейронные сети для фильтрации входящих данных. Поскольку экспертная система получает информацию о событиях, которые рассматриваются как подозрительные, её чувствительность увеличивается. Если нейронная сеть идентифицируют новые угрозы в результате обучения, то экспертную систему следует обновить. В противном случае новые атаки не будут учитываться экспертной системой, так как предыдущие правила не смогут идентифицировать угрозу.

Если нейронную сеть можно будет использовать как автономное средство для защиты от информационных угроз, тогда её можно использовать для анализа сетевого трафика и путём выявления возможных аномалий

идентифицировать несанкционированные вмешательства. Любое такое событие, которое идентифицировано как информационная атака, переправляется администратору сети по безопасности и/или используется системой информационной безопасности, которая автоматически реагирует на новые вызовы. По сравнению с предыдущими подходами нейронные сети имеют преимущество, потому что предусматривают только один уровень анализа, и при этом могут сравнительно быстро адаптироваться к новым условиям. в криптографических системах информационной безопасности Более того, в криптографических системах информационной безопасности нейронные сети могут быть использованы для хранения криптографических ключей в распределённых телекоммуникационных сетях связи [93].

Основным недостатком нейронных сетей является то, что они слишком «пристрастны» к проведению анализа входных данных [103]. Однако использование гибридных нейронных экспертных систем и/или нейро-нечётких систем позволяет структуре СИБ автоматически генерировать систему нечётких правил, которая в автоматическом режиме регулирует обучение нейронной сети [113]. Адаптивная функция гибридных нейро-нечётких систем позволяет им автоматически определять новые угрозы, определять и сравнивать поведения пользователей с существующими системными шаблонами и автоматически генерировать новые правила при изменении угроз и поддерживать бесперебойное функционирование технической составляющей информационной системы безопасности.

2.1.2. Интеллектуальные средства моделирования систем защиты информации

Для обнаружения несанкционированных действий и противодействия им применяется множество различных математических методов и интеллектуальных средств [8]. Так, для обнаружения процессов, связанных с

управлением потоками информации, и несанкционированных помех процессе, выполняемом в ИТ-системах, и для расчёта мощности вычислительных сетей, может применяться математический аппарат скрытых Марковских цепей [92] на предмет принадлежности к одному из признанных классов информационных угроз. В некоторых случаях, например, в [4, 18, 19, 43, 44] изучается применение интеллектуальных многоагентных систем для защиты информации. В частности, в перечисленных работах имеет место краткое изложение реализации инструментов атаки и онтологии прикладной области, структуры агентов СИБ во взаимодействия и координации.

Другая группа исследований [42, 90, 106] посвящена использованию мультиагентных и интеллектуальных технологий для обнаружения атак на web-сервере, проверки степени защиты и обучения ИТ-системам. Здесь рассматриваются подходы к созданию систем моделирования информационных атак на web-сайты. Эти подходы основаны на использовании онтологии сетевых атак, их стратегий использования, а также внедрении программ хранения и атак уязвимостей.

В целях идентификации динамических объектов в терминах математического описания и мониторинга информационных систем в [12, 77] рассматривается специфические особенности применения многослойных нейронных сетей. В работах [7, 9, 20, 72] исследуются логические базисы нейронных сетей и генетического алгоритма с точки зрения подавления программных угроз, направленных на затруднение доступности ресурсов. В данном случае нейронная сеть используется для обнаружения атак в сетевом трафике, для аутентификации форматов данных, для динамического определения участников интерактивного обмена информацией.

Генетические алгоритмы обеспечивают оптимальные решения проблем управления с параметрами маршрутизации и трафика, при условии, что идентификационные данные информационных атак в информационном шуме или нехватка информации являются нечёткими.

Для реализации активного аудита безопасного функционирования IT-систем в [10, 53] рассматриваются возможности применения математического аппарата теории нечёткого множеств. Методы Data Mining (то есть интеллектуальные методы анализа данных) здесь используются для оценки степени защиты от несанкционированных помех и выявления злоупотреблений пользователей и программных атак. Эти методы осуществляют профилактику от несанкционированных вмешательств на основе принципа адаптивной безопасности, то есть в режиме последовательности «анализ – прогнозирование – предупреждение».

Некоторые исследования, отражённые в работах [6, 15, 21, 49, 56, 95], посвящены идентификации и аутентификации пользователей по их биометрическим и фонетической параметрам. В основном в этих исследования для решения указанной проблемы используются математический аппарат нейронных сетей и методы быстрой обработки сигналов.

Таким образом, на основе проведённого анализа становится очевидным, что необходимо разработать единый подход к использованию интеллектуальных средств для организации комплексной адаптации IT-систем на основе комбинировании природоподобных средств [75] вместо решения отдельных вопросов защиты информации по средствам индивидуальных применений экспертных систем, системы нечёткого логического вывода и искусственных нейронных сетей. Проект информационной защиты на основе природоподобных средств защиты должен реализовываться как единый комплексный процесс адаптивной защиты IT-системы путём их интеграции внутри СИБ [76].

Нечёткие нейронные сети считаются наилучшими природоподобными инструментами для решения проблемы информационной безопасности. Применение нечётких нейронных сетей в сфере информационной безопасности проектируются на основе эвристических знаний, знаний экспертов и их опыта в предметной области. Механизм нечёткого логического вывода,

генерированный в виде нечётких импликативных правил, структурно и параметрически оптимизированные посредством нейронной сети, предоставляет широкую возможность использовать эвристические знания в области информационной безопасности [46, 91, 104]. Последующее обучение нейронной сети на предмет идентификации неизвестной угрозы создаёт возможность адаптировать логический процесс анализа угроз путём структурного переформатирования логических правил для синтеза СИБ [64, 104, 114].

Для адаптивных СИБ требуемые характеристики нечёткой нейронной сети являются:

- Защита элементной базы и и функциональная устойчивость;
- Возможность классификации угроз;
- Описание «механизма защиты от угроз» посредством системы нечётких предикатных правил;
- Адаптивность нейро-нечётких средств информационной защиты;
- Транспарентность нейро-нечётких средств информационной защиты и системы нечётких логических правил;
- Параллельность распределённых вычислений.

2.2. Интеллектуальные средства для классификации угроз в системах защиты информации

Проблемы классификации и кластеризации имеют существенные значения при обеспечении информационной безопасности посредством интеллектуальной корпоративной информационной системы безопасности в контексте динамического изменения окружающей среды, поскольку существующие недостатки и каналы уязвимости в корпоративных сетях связи требуют перманентного мониторинга всего спектра возможных угроз [64, 90].

В случае необходимости обнаружения уязвимостей и выявления вмешательств, антивирусное программное обеспечение, экраны сетевой безопасности и известные кластеризаторы информации при необходимости осуществляют классификацию и/или кластеризацию инцидентов. В самом простейшем случае эти инструменты делят входные векторы на опасные или безопасные классы.

2.2.1. Решение проблем классификации информационных угроз с применением экспертных систем

Одним из способов классификации угроз являются экспертные системы (ЭС), которые формируются по средствам знаний, описанных в виде логических правил. Каждое правило состоит из двух частей: левой – IF <…>, называемого предпосылкой или условием, и правой – THEN <…>, называемой последствием или выводом:

IF<предпосылка>, THEN<вывод>.

Правила могут включать одно или несколько предпосылок. Конъюнктивные правила подразумевают выполнения логических операции «И» или «AND» (*conjunction*), и требуют выполнения всех присутствующих в правилах суждений. Например,

IF<предпосылка 1>AND<предпосылка 2>AND … AND<предпосылка *n*>, THEN<вывод *m*>.

Дизъюнктивные правила подразумевают выполнения логических операции «ИЛИ» или «OR» (*disjunction*), и требуют выполнения всех присутствующих в правилах суждений (предпосылок). Например,

IF<предпосылка 1>OR**<предпосылка 2>**OR **…** OR**<предпосылка *n*>, THEN<вывод *m*>.**

Кроме того, правая часть правил «THEN» может также включать несколько выводов. В этом случае логическое правило может быть отражено следующим образом:

IF <предпосылка>, THEN <вывод 1>, <вывод 2>, ..., <вывод *m*>.

Сами суждения состоят из двух частей: лингвистического объекта и принимаемых им слабо структурированных значений (термов). В результате лингвистический объект включает оператор, связывающего его с его термом.

На рис. 2.1 представлена модель системы логического вывода, основанная на процессе мышления человека [67]. Знания, поддерживаемые лингвистическими правилами, хранятся в памяти на долгосрочной основе. Фактическая информация, хранящаяся в виде фактов, содержится в оперативной памяти. В процессе рассуждений (*reasoning*) в разделе правил «IF» рассуждения позиционируются в виде суждений. Если правило выполняется, то сам вывод (*conclusion*) осуществляется.

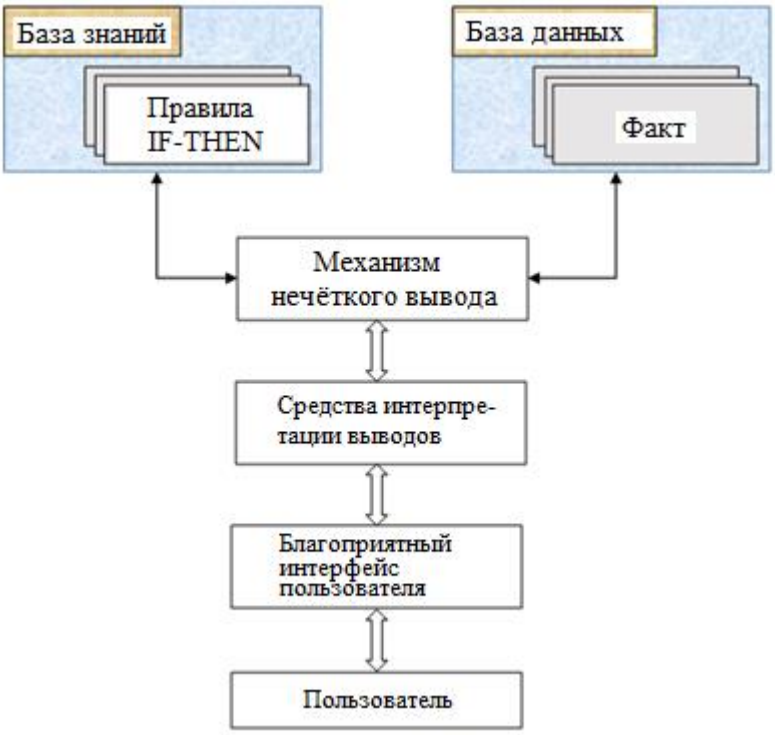

Рис. 2.1: Экспертная система

Основанная на системе предикативных правил Экспертная Система включает в себя следующее элементы:

- База знаний (*Knowledge Base*);
- База данных (*Data Base*);
- Механизм логического вывода (*Inference Engine*);
- Средства интерпретации результатов (*Explanation Facilities*);
- Благоприятный интерфейс пользователя (*User Interface*).

В случае, когда знания в Экспертной Системе сформированы в виде совокупности импликативных правил вида «IF<предпосылка>, THEN<последствие>», тогда система логическая вывода производит сравнение базы данных с базой знаний, и в случае чёткого перекрытия активируются действия, назначенные для поля результатов.

Результаты работы Экспертной Системы становятся известны пользователю посредством диалогового интерфейса. В то же время через этот интерфейс пользователь может ознакомиться с логическими «суждениями», к которым подводит пользователя эта система.

Созданная в результате опроса, проведённого между профессиональными экспертами, Экспертная Система оформляется как специализированная система для решения задач классификации в достаточно узкой предметной области на основе сформулированной базы знаний посредством системы логических правил вида «*If* <…>, *then* <....>». Как упоминалось выше, модель Деннина [102] основана на базе знаний Экспертной Системы в составе СИБ открытой корпоративной телекоммуникационной сети связи. Экспертные Системы подобного типа включают в себя правила классификации сценарий возможных информационных атак и соответствуют информационным профилям юридических пользователей корпоративной сети [105, 118].

В качестве средства решения задач классификации Экспертной Системе присущи следующие недостатки:

- *Скрытость отношений между правилами в базе знаний*. Некоторые правила вида «*If <…>, then <....>*» являются относительно простыми и логически прозрачны, но прозрачность их логического взаимодействия может быть в пределах базы знаний, которая является достаточно низкой. Другими словами, не так просто определить правила, которые противоречивы в базе знаний и их роль в решении проблемы классификации.
- *Неэффективность стратегии поиска*. Экспертная Система, которая обладает обширной базой знаний в плане оперативного решения проблем безопасности в составе СИБ открытой корпоративной телекоммуникационной сети связи может быть недостаточно продуктивной в режиме реального времени.
- *Отсутствие свойств приспособляемости (адаптации)*. Экспертные Системы не обладают способностями к обучению. Они не могут автоматически изменять свою базу знаний: корректировать существующие правила или имплементировать новые правила «*If <…>, then <....>*».

2.2.2. Нечёткая классификация информационных угроз

Нечёткая классификация – это дальнейшее развитие в области информационной безопасности, существенно расширяющее возможности ЭС для классификации информационных угроз. Основное отличие и преимущество нечёткой классификации заключается в том, что она может обеспечить более правдивые результаты, основанные на нечётких или неполных, то есть слабо структурированных неточных суждениях. Нечёткая классификация позволяет решать проблемы преобразования как числовой, так и качественной информации в функциональные возможности, создавая конкретные нечёткие кластеры (или нечёткие множества) посредством нечётких логических систем

[66]. При этом сами нечёткие множества восстанавливаются так называемыми функциями принадлежности, принимающими свои значения из отрезка [0; 1].

Классификация посредством системы нечёткого логического вывода осуществляется в несколько этапов: [104]:

1) Фаззификация входной информации, подразумевающая описание входных характеристик x_i (i=1÷n) посредством нечётких множеств с помощью функций принадлежности μ_{x_i}, отвечающих требованиям установленных правил для классификации информационных угроз;
2) Для левых частей импликативных правил определение единого нечёткого множества с функциями принадлежности μ_{R_i} $(i = 1,2, \dots, m)$, где m – это число правил классификации, как пересечение соответствующих нечётких множеств с функциями принадлежности μ_{x_i}, отражающих входные характеристики, описывающие слабо структурированные признаки классификации информационных угроз;
3) Композиция нечётких импликативных правил путём применения операции импликации между нечёткими множествами-предпосылками μ_{R_i} $(i = 1,2, \dots, m)$ и нечёткими множествами – последствиями μ_{C_i} $(i = 1,2, \dots, p)$, и редуцирование, тем самым, нечёткого вывода относительно принадлежности информационной угрозы тому или иному классу угроз;
4) Дефаззификация нечётких выводов системы μ_{C_i} $(i = 1, 2, \dots, p)$, то есть их точечная оценка посредством, например, центроидного метода.

Подобно Экспертным Системам нечёткие логические системы, состоящие из нечётких логических правил вида «*If* <…>, *then* <....>», основаны на эвристических знаниях профессиональных экспертов в области информационной безопасности. Тем не менее нечёткие системы логического вывода существенно расширяют сферу применения приложений Экспертных Систем с точки зрения обработки слабо структурированных данных,

характеризующие качественную информацию, подлежащею анализу на наличие информационных угроз.

Кроме того, нечёткие логические системы обладают способностью адаптироваться, потому что могут допускать структурную и параметрическую настройку, то есть в зависимости от желаемых выводов классификации изменять структуру правил и оптимизировать параметры функций принадлежности нечётких множеств, описывающих термы лингвистических переменных. При этом следует также отметить, что настройка параметров функций принадлежности нечётких множеств, описывающих термы лингвистических переменных в левых и правых частях импликативных правил вида «*If* <…>, *then* <….>» требует затрат значительного времени обучения.

2.2.3. Применение нейронных сетей в решении задач классификации и кластеризации информационных угроз

С точки зрения классификации информационных угроз нейронные сети, как интеллектуальные средства, являются ещё более продуктивными, т.к. они способны к обучению и адаптации к новым условиям информационной среды [115]. Доказано, что нейронные сети являются универсальными аппроксиматорами для произвольных непрерывных функций, означающее, что любая непрерывная функция может быть описана посредством сети состоящая из формальных (искусственных) нейронов, характеризующиеся своими функциями активации [32].

Формально подтверждён верхний предел возможности нейронных сетей, аппроксимирующих произвольные непрерывные функции, зависящие от нескольких и/или многих аргументов. Любую непрерывную функцию, заданную в табличном виде, можно описать с помощью нейронной сети. В случае, когда входной вектор является *n*-мерным, наличие нелинейных

нейронов в «скрытом» слое нейронной сети в количестве $2n+1$ считается достаточным [33].

Известны многочисленные случаи использования нейронных сетей для защиты корпоративных сетей. Большинство приложений здесь основаны на проблемах классификации и кластеризации. В то же время следует отметить, что среди всех перечисленных интеллектуальных средств информационной защиты только нейронные сети обладают автономной способностью к обучению [96].

Одной из наиболее важных особенностей нейросетевой системы информационной безопасности является самоорганизация, позволяющая адаптироваться под изменения входной информации. Наличие скрытой информации в совокупности входной информации, а также обилие доступной информации в поступающих данных являются благоприятной основой для обучения нейронных сетей. Самоорганизация нейронных сетей обусловлена механизмом кластеризации: одни и те же входы сгруппированы нейронной сетью на основе взаимной корреляции и описываются конкретными функциональными нейронами в качестве прототипов.

Механизмы классификации и кластеризации входных данных в системах информационной безопасности помимо установления того или иного известного классов объектов (вектора входных данных) обладают возможностью самоорганизации, адаптации, развития интеллектуальных средств информационной безопасности в открытых корпоративных сетях, а также для эволюционирования процессов обеспечения информационной безопасности. Тем не менее, наиболее передовые функциональные возможности в системах информационной безопасности достигаются путём сочетания различных адаптивных интеллектуальных средств в общих системах гибридной защиты информации.

2.3. Гибридные средства в решении задач классификации угроз

Гибридные средства классификация, основанные на применении нейронных сетей, сочетают в себе преимущества всех существующих интеллектуальных подходов. Он считается дефектом в сетях нейронов из-за того, что знание информационной платформы нейронных сетей, которое не позволяет анализировать результаты процесса классификации, полностью прозрачно с точки зрения менеджера безопасности. Рекомендуется, чтобы нейронная сеть работала совместно с нечёткой системой логического вывода или Экспертными Системами, чтобы устранить этот недостаток. Использование гибридных нейротрансмиттеров или нейро-нечётких систем позволяет сетям нейронов чётко идентифицировать систему нечётких правил внутри структуры. Эти правила автоматически регулируются во время обучения нейронных сетей.

2.3.1. Нейро-экспертные системы в решении задач классификации угроз

Нейронные сети и экспертные системы отличаются с точки зрения правил представления и обработки информации.

Нейронные сети сосредоточены на распределённой параллельной обработке данных, которая с точки зрения логики решения задач не транспарантная, а знания, накопленные в процессе обучения, распределяются по синоптическим связям. Все это затрудняет объяснение конкретного местоположения этих знаний и отражает опыт специалистов по профессиональной безопасности в информационном пространстве НК. В экспертных системах эвристический опыт отражается, как известно, в форме «*If* <...>, *then* <....>», которая является достаточно транспарантной для пользователя, а процесс логического извлечения знаний похож на человеческое мышление.

Нейронные сети являются адаптивными средствами, и сам процесс обучения может быть довольно простым и формальным. В то же время приобретение знаний экспертными системами требует значительных усилий, поскольку знания основаны на системе правил, основанных на личном опыте отдельных экспертов, которые не конфликтуют друг с другом [22]. Кроме того, данные, связанные с экспертными системами, не являются достаточно гибкими и самоорганизующимися.

Нейро-экспертная система имеет структуру, похожую на структуру Экспертных Систем. Отличие состоит в том, что её база знаний организована как адаптивная распределённая информационная платформа (рис. 2.2).

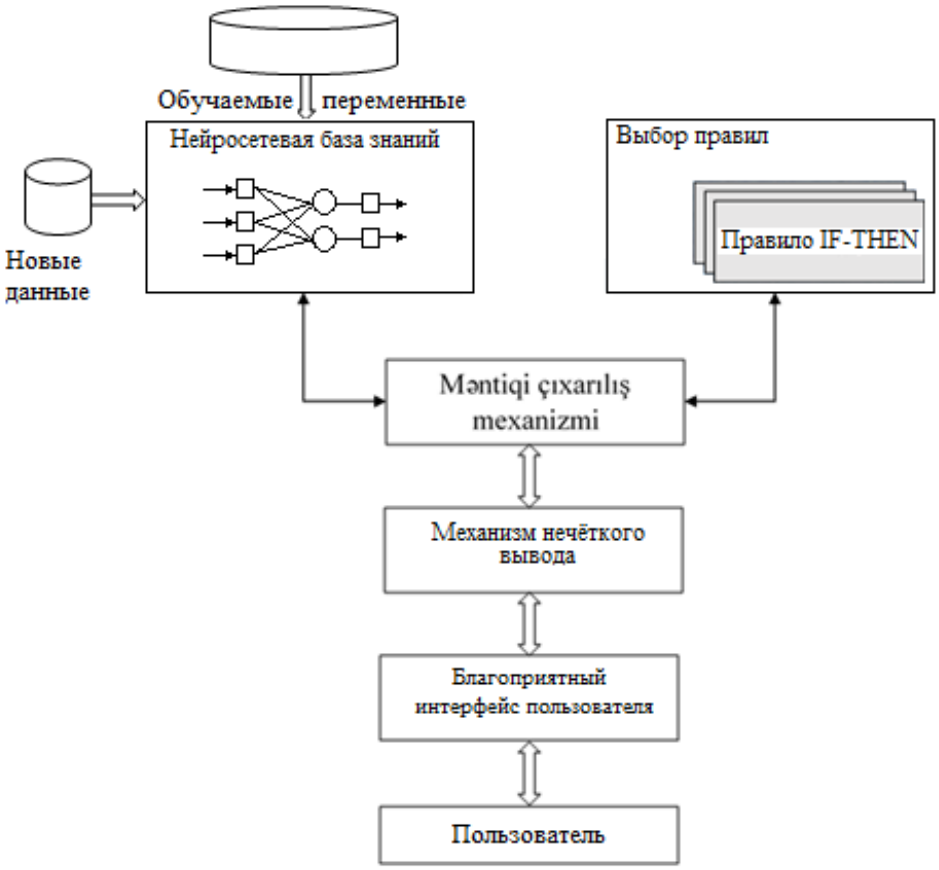

Рис. 2.2: Структура нейро-экспертной системы

Использование нейросетевой базы знаний позволяет устранить основные недостатки, такие как неспособность соблюдать правила на основе

Экспертных Систем и сложность адаптации базы знаний. Нейросетевая база знаний регулирует зашумлённую и искажённую входную информацию: если неполные условия выполняются в разделе «*If <…>*», тогда будет активировано неявное правило «*If <…>, then <....>*». Активация нейросетевой базы знаний связана с удалением знаний из информационной платформы нейронной сети (извлечение правила), «*If <…>, then <....>*» неявно. Механизм логического вывода работает на нечётких суждениях в экспертной среде нейро симуляции.

2.3.2. Нейро-нечёткие системы в решении задач классификации угроз

Одним из перспективных средств в информационной защите открытых корпоративных телекоммуникационных сетей связи являются гибридные системы, реализованные, например, посредством нечёткой системы вывода в логическом базисе нейронной сети.

Как хорошо известно, нейронные сети и нечёткие логические системы являются универсальными методами моделирования причинно-следственных связей. Их совместное применение даёт возможность создавать принципиально новые средства, которые позволяют существенно расширить классы решаемых задач классификации информационных угроз. Несмотря на то, что нечёткие логические системы и нейронные сети формально схожи, между ними все же существуют определённые различия.

Как было сказано выше, нечёткая логическая система, являясь структурированным численно оценивающим механизмом, строится в виде нечётких импликативных правил вида «*If <…>, then <....>*». Для представления композиционного правила вывода взвешивается выход каждого правила в соответствии со степенью принадлежности его входов и по всем выходам правил вычисляется центроид, обеспечивающий генерацию подходящего чёткого выхода.

Чаще всего проектирование нечёткой логической системы проводится методами подбора (*trail-and-error design*). При этом, большинство подходов подразумевает субъективный (экспертный) выбор функций принадлежности и лингвистических правил. Тем не менее функции принадлежности и/или импликативные правила подлежат настройке, что обуславливает структурную и параметрическую оптимизацию нечёткой логической системы.

Проводимые исследования в этом направлении включают:

- модификацию правил, основанную на концепции «*linguistic phase plane*»;
- метод «логического испытания» (“*logic examination*”) для процесса конвертации входных-выходных данных в нечёткие правила управления, основанный на концепции «нечёткой идентификации».

Существенное развитие технологии оптимизации нечётких логических систем нашли своё отражение во многих работах. Однако, до сих пор продолжаются вестись активные исследования в области проектирования нечётких логических систем.

Поддающиеся к обучению нейронные сети, проявили себя как устойчивые к различным шумам средствами, которые способны обобщать свои приобретённые свойства. Они состоят из большого числа взаимосвязанных процессорных элементов (искусственных нейронов), которые отличаются своими свойствами обучения и генерируются на основе обучающих образцов или сценарий. Классификация образов, а в нашем случае – информационных угроз, является одной из основных прикладных функций нейронных сетей, наравне с распознаванием образов, аппроксимацией непрерывных функций, оптимизацией и кластеризацией сигналов.

В виду того, что «скрытые» слои нейронных сетей не являются транспарантными для их пользователей, в настоящее время большинство исследований сконцентрированы вокруг формирования оптимальных структур и размеров сетей. К месту важно отметить, что нейронные сети стали широко

применяться, начиная с середины 80-х годов прошлого века. Именно в это время американский учёный Д. Румелхарт разработал градиентный алгоритм обучения «error backpropagation», который, по существу, позволил нейронным сетям применяться в проектировании нечётких логических систем гибридного типа.

В системах нечёткого логического вывода, реализованных на базе логического базиса нейронных сетей, все входные и выходные нейроны представляют соответственно входные и выходные характеристики, а нейроны «скрытых» слоёв отождествляют функции принадлежности и нечёткие импликативные правила. Это позволяет симулировать способы человеческих суждений в рамках нейросетевой структуры, а также сохранять согласованные правила нечёткого вывода, как и в случае экспертных систем и обычных нечётких систем логического вывода. Более того, предлагаемая архитектура нейро-сетевой модели системы нечёткого вывода в рамках оптимизации целевой функции позволяет достаточно просто формулировать как параметрическое обучение (то есть обучение функций принадлежности), так и структурное обучение (выбор оптимального набора нечётких импликативных правил). Такой подход обеспечивает оригинальное решение задачи многокритериальной оценки информационных угроз или атак.

В контексте приведённых рассуждений обобщённую схему гибридной нейро-нечёткой системы классификации информационных угроз или атак можно представить так, как это показано на рис. 2.3. Данная схема вбирает в себя три основные компоненты: фаззификатор, базовые нечёткие правила и механизм нечёткого вывода, и дефаззификатор.

Фаззификатор осуществляет процедуру описание качественных и/или количественных входных сигналов, как термов лингвистических переменных, в виде нечётких множеств посредством функций принадлежности. Базовые правила включают представляют собой нечёткие импликативные правила вида «*If* <…>, *then* <....>», которые описывают начальные эвристические знания об

уже известных видах информационных угроз. Механизм нечёткого вывода, реализуя композицию импликативных правил, на выходе генерирует нечёткий вывод о характере и классе информационной угрозы. Дефаззификатор обеспечивает представление нечётких выводов о характере и классе информационной угрозы в виде обычных чисел посредством, например, центроидного метода.

Рис. 2.3: Классификация информационных угроз на основе адаптивной системы нечёткого вывода

Ясно, что основной проблемой в проектировании адаптивной системы нечёткого вывода является идентификация подходящих входных-выходных функций принадлежности и нечётких логических правил. Основанная на базовой структуре и концепции, представленных на рис. 2.3, нечёткая система логического вывода в нейросетевом исполнении с коннекционной топологической структурой способна устранить данную проблему. На рис. 2.4 представлена структура такой системы, которая состоит из 5-ти слоёв.

По аналогии с «рефлекторно дугой», нейроны 1-го входного слоя (или рецепторы) олицетворяют входные лингвистические переменные, нейроны 5-го выходного слоя по сути выполняют роль эффекторов. Нейроны 2-го и 4-го

слоёв имитируют всевозможные функции принадлежности, чтобы отражать термы лингвистических переменных в виде подходящих нечётких множеств. Каждый нейрон 3-го слоя генерирует одно единственное нечёткое импликативное правило. Тогда совокупность подобных нейронов в составе 3-го слоя формируют базовый набор нечётких логических правил. Связи между 3-им и 4-ым слоями в совокупности генерируют ассоциативный механизм вывода. Входные связи 3-го слоя определяют предпосылки для левых частей правил вида «*If* <...>, *then* <....>», а входные связи 4-го слоя отождествляют последствия. Другими словами, в совокупности эти нечёткие отношения формируют причинно-следственные связи в рамках механизма нечёткого вывода.

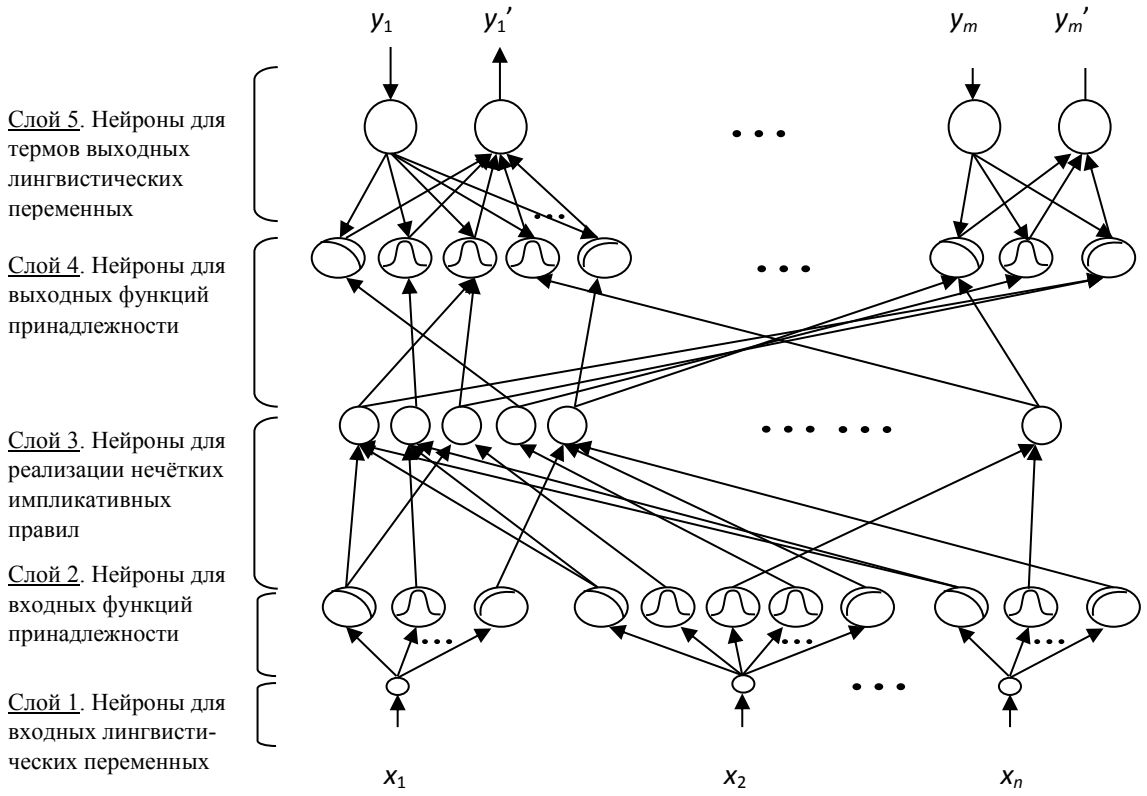

Рис. 2.4: Адаптивная система нечёткого вывода в логическом базисе feedforward пятислойной нейронной сети

Входные сигналы нейронов из разных слоев в общем виде формулируются как:

$$\text{Input} = f(u_1^k, u_2^k, \ldots, u_p^k;\ w_1^k, w_2^k, \ldots, w_p^k), \tag{2.1}$$

где k – это порядковый номер слоя; p – порядковый номер входной связи; u_i^k (i=1÷p) является i-ым сигналом из k-го слоя; w_i^k (i=1÷p) – является весовым коэффициентом i-ой связи из k-го слоя.

В рамках указанных обозначений выходы активированных нейронов формулируются как:

$$\text{Output} = o_i^k = a(f)\ (i=1 \div p), \tag{2.2}$$

где $a(\cdot)$ есть функция активации.

В частности, полагая $f = \sum_{i=1}^{p} w_i^k u_i^k$, то в качестве функции активации часто выбирают сигмоидальную функцию вида:

$$a = \frac{1}{1+e^{-f}}. \tag{2.3}$$

Опишем функции нейронов каждого из пяти слоёв предлагаемой нейронной сети.

Первый слой: Для этого слоя нейроны, как правило, выбираются линейными, то есть такими, чтобы с их помощью можно было передавать входные сигналы на нейроны следующего слоя напрямую по взвешенным единицами связям ($w_i^1 = 1$), а именно:

$$f = u_i^1 \text{ и } a=f. \tag{2.4}$$

Второй слой: Нейроны этого слоя воспроизводят функции принадлежности, например, следующего колоколообразного типа,

описывающего в частности *j*-ый терм *i*-ой входной лингвистической переменной x_i:

$$f = -\frac{(u_i^2 - m_{ij})^2}{\sigma_{ij}^2} \text{ и } a=e^f, \tag{2.5}$$

где m_{ij} и σ_{ij} соответственно являются центрами и плотностями близлежащих элементов, описывающего *j*-ый терм *i*-ой входной лингвистической переменной x_i. В данном случае вес синоптической связи ко 2-му слою (w_{ij}^2) интерпретируется как m_{ij}.

3-ий слой: Синоптические входные связи этого слоя, применяются для имитации предпосылок в причинно-следственных отношениях, отражаемых нечёткими импликативными правилами вида «*If* <...>, *then* <....>». Каждый нейрон воспроизводит нечёткую логическую операцию «И» в виде взятия следующего минимума:

$$f = \min\left(u_1^3, u_2^3, ..., u_p^3\right) \text{ и } a=f. \tag{2.6}$$

Здесь весовые коэффициенты входных в 3-й слой синоптических связей (w_{ij}^3), считаются единичными.

Четвёртый слой: Нейроны этого слоя функционируют в двух режимах, то есть обеспечивают передачу сигналов в обоих направлениях: с низу в верх и с верху в низ. В первом режиме передачи сигналов входные в 4-ый слой синоптические связи имитируют нечёткую логическую операцию «ИЛИ», чтобы интегрировать инициированное правило, реализуеющее последствие в виде:

$$f = \sum_{i=1}^{p} u_i^4 \text{ и } a=\min(1, f). \tag{2.7}$$

Здесь весовые коэффициенты входных синоптических связей также считаются единичными, то есть $w_{ij}^4 = 1$.

Пятый слой: В случае применения гибридного алгоритма обучения в этом слое также предусматривается наличие нейронов двух типов. Нейроны первого типа обеспечивают передачу сигналов с верху в низ для снабжения нейронной сети обучающими данными. Для них имеют место следующие линейные равенства:

$$f=y_i \text{ и } a=f. \tag{2.8}$$

Нейроны второго типа обеспечивают передачу сигналов с низу в верх для осуществления вывода системы. Эти узлы и присоединенные к ним связи имитируют работу дефаззификатора. Если предположить, что m_{ij}^5 и σ_{ij}^5 являются, соответственно, центрами и ширинами выходных функций принадлежности, тогда для симуляции центроидного метода дефаззификации могут быть использованы следующие выражения:

$$f = \sum w_{ij}^5 u_i^5 = \sum (m_{ij}\sigma_{ij}) u_i^5 \text{ и } a = \frac{f}{\sum \sigma_{ij} u_i^5}. \tag{2.9}$$

Здесь весовые коэффициенты входных в 5-ый слой синоптических связей (w_{ij}^5) отражаются как: m_{ij} и σ_{ij}. При *on-line* алгоритме обучения нейроны из этого слоя индуцируют сигналы в режиме снизу в верх, тем самым обеспечивают итоговый консолидированный вывод относительно класса информационной угрозы.

Таким образом сочетание возможностей нейронных сетей с возможностями нечётких систем логического вывода являются одним из перспективных направлений в области организации интеллектуальной защиты информации. Такое сочетание в известном смысле компенсирует (или вовсе устраняет) нетранспарентность нейронных сетей при описании ключевых знаний и интерпретации результатов работы всей интеллектуальной системы.

Нечёткая логика позволяет формально интерпретировать информацию о качестве, предоставляемую специалистами в области информационной безопасности, и создаёт суждения для системы правил, которые позволяют им анализировать производительность системы.

Механизм нечёткого логического вывода используется в форме ключевых правил нейро-нечёткой классификации для отражения базы знаний, которые на начальном этапе формализуются специалистами по информационной безопасности, например, в следующем виде:

R_1: “Если $\tilde{x}_1 = S$ и $\tilde{x}_2 = S$, тогда $\tilde{y} = L$”;

R_2: “Если $\tilde{x}_1 = L$ и $\tilde{x}_2 = S$, тогда $\tilde{y} = S$”;

R_3: “Если $\tilde{x}_1 = S$ и $\tilde{x}_2 = L$, тогда $\tilde{y} = S$”;

R_4: “Если $\tilde{x}_1 = L$ и $\tilde{x}_2 = L$, тогда $\tilde{y} = L$”.

В данном случае $\tilde{x}_i$ и $\tilde{y}_j$ являются соответственно входными лингвистическими переменными; L и S – нечёткие множества, описывающие термы этих переменных, например, типа: LARGE – БОЛЬШОЕ) və (SMALL – МАЛОЕ).

Нейро-нечёткий классификатор – это адаптивный функциональный эквивалент нечёткой модели эксперта, реализованный на базе нейронной сети (см. рис. 2.5). Спецификация его образа основана на формировании системы нечётких правил, которая описывает процедуру получения результатов во множестве суждений. Специфика нейро-нечёткой реализации классификатора проявляется в функциональном несоответствии формальных (искусственных) нейронов.

Нейронные сети в рамках структуры нейро-нечёткого классификатора предоставляют возможность отражать нечёткий логический вывод путем организации априорной информации на своей информационной платформе.

Априорная информация же может быть скорректирована во время процесса обучения, который, как правило, проводится до эксплуатации.

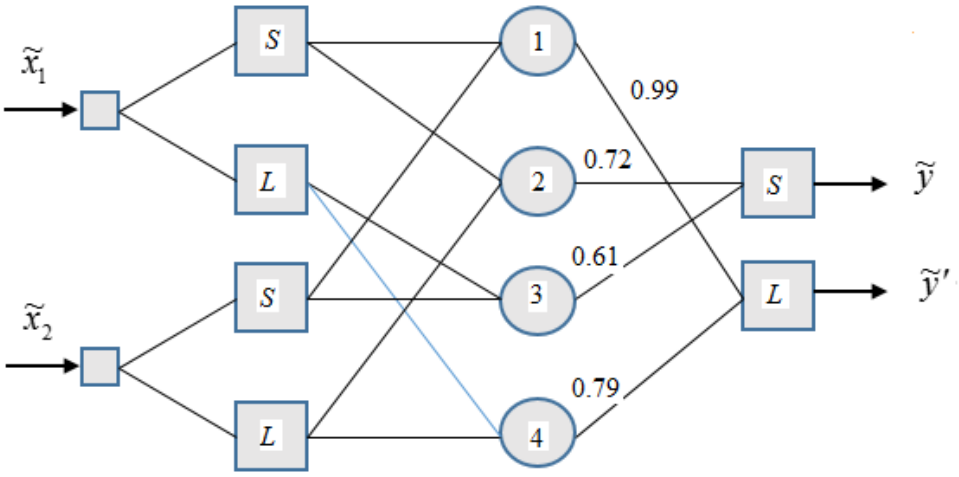

Рис. 2.5. Пример нейро-нечёткого классификатора

Нейро-нечёткие классификаторы могут быть адаптированы для обеспечения автоматического создания новых правил в случае изменений в информационной безопасности корпоративных сетей наряду с идентификацией угроз, которые решаются путём комбинирования поведения пользователя с шаблонами внутри системы.

Как и в случае с системами нейро-экспертизы, информационная платформа Нейронных сетей должна быть отрегулирована до начала эксплуатации.

Знания профильных специалистов в области информационной безопасности, описанные в виде нечётких правил, могут быть отражены в структуре нейро-нечёткого классификатора. В результате последующего обучения нейро-нечёткого классификатора осуществляется настройка весовых коэффициентов синоптических связей (то есть уточняется правдивость отдельных правил, а противоречия в правилах устраняются в целом).

Основным недостатком нейро-нечетких классификаторов заключается в том, что информационная площадка здесь является мало вмесатительной. Это

отрицательно сказывается на функциональной устойчивости защиты от деструктивных эффектов.

2.3.3. Интерпретация представлений информации при решении задачи классификации информационных угроз и атак

Введение избыточности в информационные поля нейро-нечёткого классификатора основывается на средствах обеспечения защищённости природоподобных систем. В частности, на:

- отображении релевантной информации структурированными полями,
- избыточности информации за счёт дублирования структурированных информационных полей,
- избыточности информации, обусловленной наличием повторяющихся фрагментов информационного поля.

Избыточность информационного поля предоставляет возможность для того, чтобы имеющиеся в активе знания можно было хранить в распределённом формате в структурированных информационных полях гибридной нейро-нечёткой сети, а специализация слоёв функций настройки позволяет анализировать результаты обучения информационных полей нейронных сетей.

В качестве аппарата для формализации преобразований над нечеткими высказываниями, как правило, используются аналоги нормальных форм, то есть в виде дизъюнкции и конъюнкции. Иначе говоря, нечёткие импликативные правила вида «*If* <...>, *then* <....>», описывающие экспертную базу знаний в области информационной безопасности в процессе формирования заключений относительно классификации информационных угроз, отражаются посредством двух типов систем правил: конъюнктивной и дизъюнктивной, которые, в свою очередь, представляются в специализации групп функций настройки в ключевом скрытом слое композиционирования нейро-нечёткого классификатора (рис. 2.6).

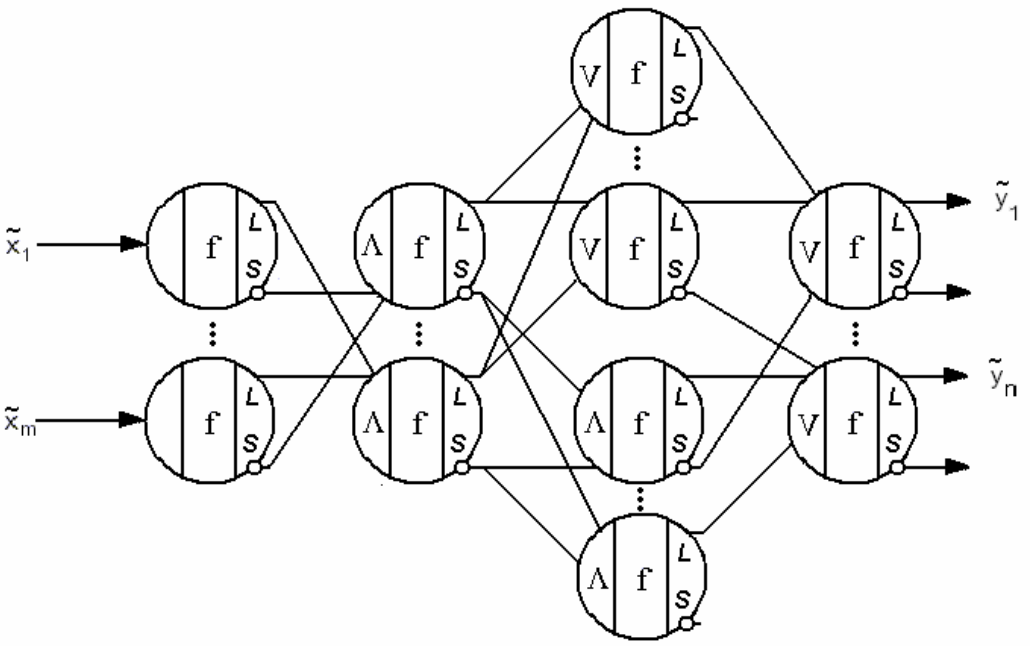

Рис. 2.6. Классическая схема нейро-нечёткого классификатора

В первую группу входят нечёткие искусственные нейроны «*дизъюнкция*», реализующие логическую операцию «max» над минтермами, во вторую группу входят нечёткие искусственные нейроны «*конъюнкция*», реализующие логическую операцию «min» над макстермами. В результате на выходах $L(\tilde{x}_i)$ и $S(\tilde{x}_i)$ первой группы из искусственного нейрона «дизъюнкция» будет реализовано, соответственно, прямое и инверсное представление системы нечётких классификационных правил, а на выходах $L(\tilde{x}_i)$ и $S(\tilde{x}_i)$ второй группы из искусственного нейрона «конъюнкция» – соответственно, инверсное и прямое представление системы нечётких правил классификации.

2.4. Моделирование систем информационной защиты и оценка безопасности корпоративных сетей

Моделирование средств информационной защиты и оценка уровня безопасности корпоративных сетей являются обязательными шагами на пути

автоматизации процесса обнаружения уязвимостей и информационных атак на корпоративные сети с целью их адаптации и эволюционирования и развития корпоративных сетей [25, 73].

2.4.1. Моделирование систем информационной защиты

В средствах массовой информации, отражающих сведения об использовании эффективных методологий, часто отмечается, что использование средств информационной безопасности, в том числе применение имитационных моделей, позволяют существенно снизить издержки, связанные с эксплуатацией открытых корпоративных телекоммуникационных сетей связи [67]. Интеллектуальные методы направлены на создание экономически жизнеспособных оптимальных природоподобных средств информационной безопасности с точки зрения минимизации ущерба, вызванного нарушениями информационной безопасности. Очевидно, что применение относительно дешёвых средств защиты информации (антивирусные программы, организационные ограничения и т.д.) значительно снижает общую потерю. Поэтому небольшие инвестиции в сферу развития средств защиты информации эффективны в сравнительно небольших организациях, которые не подвергаются специальным компьютерным атакам. Для крупных динамически развивающихся компаний, работающих в острой конкурентной среде, увеличение затрат на средства информационной безопасности не всегда приводит к желаемым сокращения ущерба от информационной атаки против открытых корпоративных сетей.

В большинстве случаев модель по информационной защите в компаниях является частью общей системы управления рисками и учитывает фактические угрозы, ошибки программного обеспечения, важность, интервал и сроки прерывания работы различных ресурсов, вероятность нападения, тип защиты и возможный ущерб. Риск менеджмент в корпоративных сетях открытого типа

позволяет рассчитать существующие риски, моделировать контрмеры и оценивать остаточные риски [37].

Биологическое сходство в рамках защиты IT-безопасности основывается на многоуровневой иерархии системы защиты информации, механизмах иммунной защиты и накопленном опыте. Популярным IMM, как правило, является реализация низкоуровневой функции системы защиты и иммунной защиты от вирусов. [39], до 70% вирусных атак происходит извне, защищённая точка доступа к корпоративной сети и до 30% внутри. Первые атаки можно назвать внешними угрозами жизни системы, а второй – внутренними угрозами. В любом случае активируется иммунная защита биосистемы. Это обновление предварительно заполняется корпоративной сетью до распространения вируса.

Этот подход противоречит биосистемной аналогии, в частности, с системной иммунной защитой, поскольку большинство антивирусных защитных систем (в отличие от биосистем) расположены в антивирусном центре за пределами корпоративной сети. Поиск антивирусного центра на краю защищённой IT-системы является мошенническим:

- во-первых, необходимо создать настроенный канал для загрузки вирусов и троянских коней под названием обновления антивирусного программного обеспечения;
- во-вторых, необходимо иметь доступ к конфиденциальной информации в случае автоматической передачи подозрительных файлов для существования вирусов.

Более того, время реакции такой иммунной системы измеряется в лучшем случае несколькими часами, что неприемлемо для большинства применений. Именно поэтому сфера применения этого подхода ограничивается восстановлением повреждённой корпоративной сети (как аналог процесса реанимации пациента путём введения биосистемы).

Иммунные функции в биосистемах реализуются по средствам:

- внутренних механизмов, которые обеспечивают быстрый ответ на распределённые угрозы по уровням иерархии средств информационной защиты;
- долгосрочные процессы сбора жизненного опыта (эвристических знаний) с эволюционным характером [39].

Природоподобный аналог IT-систем в эволюционных процессах основан на реализации набора механизмов наследования, развития, адаптации и отбора, которые присущи биосистемам. Однако интеллектуальные средства обнаружения атак и несанкционированных информационных потоков в открытой корпоративной сети ориентированы прежде всего на адаптивный характер будущего проектирования средств информационной безопасности [20, 40, 43]. Тем не менее, средства информационной безопасности на уровне почтовых шлюзов и сетевых экранов часто используются для обнаружения внешних атак, а на уровне сервера эти средства устраняют внутренние угрозы в корпоративной сети открытого типа. Хорошо известные интеллектуальные средства информационной безопасности, как правило, реализует только механизмы для немедленной реакции и устранения угроз с целью стабильного поддержания жизнеспособности корпоративной сети и на практике не принимает во внимание координационную деятельность, которая присуща функционированию нервной системы.

Постепенная адаптация иерархической системы жизнеобеспечения и защиты эволюционных процессов с использованием всего арсенала доступны в природоподобных системах управления и безопасности. Поэтому и IT-системам необходима иерархия уровней защиты, отличных от иммунного уровня системы информационной безопасности. Прежде всего, накопление жизненного опыта биологического организма требует существования более высоких уровней системы информационной безопасности (например, уровней рецепторных средств защиты), который выполняет ассоциативные отношения между следующими уровнями системы информационной безопасности (такими

как атаки и угрозы). Другими словами, требуется иерархический уровень накопления жизненного опыта в IT-системах, особенно в корпоративных и/или локальных сетях с распределёнными и параллельными компьютерными средствами обработки информации. Данный подход должен быть описан в форме структурированных информационных платформ, которые подходят для последовательности на следующем этапе реализации системы.

2.4.2. Методы оценки информационной безопасности в корпоративных сетях открытого типа

Хорошо известно, что методы оценки информационной безопасности в корпоративных сетях связи формируются в результате существования набора механизмов безопасности и средств защиты, а также набора методов работы, эксплуатации и тестирования.

В работе [1] рекомендуется использовать индикатор оценки как оценку информационной безопасности корпоративной сети. Этот показатель учитывает распределение механизмов безопасности на многоуровневой модели системы информационной безопасности и изменение вероятности вредоносного вмешательства многоуровневой модели системы информационной безопасности для защищённого объекта в зависимости от катушки. Можно показать, что статичность – это достоверность защиты корпоративной сети связи, которая не учитывает такие параметры, как частота сбоев и атак, возникающих в результате угроз информационной безопасности, как дефект этого подхода (модели).

В работе [1] уровень информационной защищённости оценивается в зависимости от ущерба, вызванного случайным характером корпоративной сети. Здесь совпадение угроз оценивается как факторы риска, описываемые нечёткими величинами, а указание защиты IT-системы определяется как матрица нечётких отношений между отношениями риска, сформированными методом экспертной оценки, и степенью защиты корпоративных сетей.

Основным недостатком этого метода оценки является то, что нет никаких указаний на то, что показатели защиты были связаны с расположением механизмов защиты в структуре системы информационной безопасности.

В работе [67] рассматривается оценка системы информационной безопасности в зависимости от потерь, возникших в результате анализа инвестиций и угроз информационной безопасности, а также наличия «нематериального» убытка (см. Таблицу 2.1), который «очернил» имя и репутацию бизнес-структуры, приведшее к падению стоимости её акций и, тем самым, к понижению её уровня конкурентоспособности на рынке потребительских товаров и услуг.

Таблица 2.1

Характеристики количественных нематериальных показателей

Размер ущерба	**Характеристики количественных нематериальных показателей**
Слишком незначительный	Ущерб можно проигнорировать
Малый	Ущерб можно легко предотвратить, а затраты, связанные с удалением угроз, малы.
Умеренный	Устранение угроз, вызванных несанкционированным вмешательством, не связано с крупными издержками и не затрагивает критические проблемы, но состояние рынка ухудшается, а некоторые из клиентов могут быть потеряны.
Серъёзный	Важнейшие проблемы имеют решающее значение. Рыночная позиция теряется в течение длительного времени. Устранение угроз, вызванных угрозами, требует больших затрат.
Слишком	В результате этой угрозы невозможно решить

серьёзный	важнейшие проблемы информационной безопасности. Организация прекращает свою деятельность.

В последнем случае «объёмы нематериальных убытков» и «вероятность потери» обуславливают применение семантических индикаторов (см. Таблица 2.2) [67]. Указание возможности «потери потенциала» связано с частотой угрозы в течение определённого периода времени.

Таблица 2.2.

Семантические характеристики наносимых угроз информационной безопасности

Частота наступления информационных угроз	**Оценка вероятности наступления**	**Семантические характеристики наносимых угроз информационной безопасности**
Нулевая степень	Ближе к нулю	Практически угроза информационной безопасности не наступит никогда
Один раз за несколько лет	Слишком малая	Угроза информационной безопасности наступает в редких случаях
Один раз в год	Низкая	Скорее всего угрозы информационной безопасности не будет
Один раз в месяц	Средняя	Скорее всего угроза информационной безопасности наступит
Один раз в неделю	Выше средней	Угрозы информационной безопасности наступят обязательно
Один раз в день	Высокая	Отсутствуют способы положительного решения проблемы

		информационной безопасности

На основании [67], не существуют подходящих методов для поиска оптимального спроса для компаний, работающих динамично в конкурентной среде. Обеспечение информационной безопасности с точки зрения оценочного критерия «ценность / эффективность» для разных вариантов рекомендуется проводить следующие мероприятия:

- Стоимость системы информационной безопасности в открытых корпоративных телекоммуникационных сетях связи не должна превышать определённую сумму (как правило, не более 20% от общей стоимости IT-системы);
- Уровень ущерба не должен превышать установленного уровня, например, «МАЛЕНЬКИЙ».

Оценки, известные до сих пор, отражают статический статус бизнес-объекта, защищённого произвольными инструментами информационной защиты. Они не учитывают возможности адаптации системы информационной безопасности для фактической загрузки механизма защиты для устранения последствий нападения, динамики изменения зоны опасности и изменения зоны опасности, и не обеспечивают необходимых указаний по изменению состава и многоуровневой структуры механизмов безопасности системы информационной безопасности.

Глава III. АДАПТИВНЫЕ МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАНОСТИ

В сложных рукотворных (то есть природоподобных, созданных непосредственно самим человеком) технических системах наметилась тенденция к применению природоподобных элементов биосферы. В области информационных технологий эта тенденция особенно нашла свое отражение в искусственных нейронных сетях, так как их топологическая структура ближе к организации нервной системы биологических систем, к архитектуре современных IT-систем, то есть корпоративных телекоммуникационных сетей связи.

3.1. Иерархия уровней систем информационной безопасности

Как отмечалось в предыдущей главе, иерархическая организация систем информационной безопасности относится к биологическим (природоподобным) системам. Биологическое сходство в структуре защиты IT-систем основано на иерархии системы информационной безопасности, включающей: механизмы сбора опыта в информационных платформах иммунной защиты и нейронных сетях. Известно, что нервная система, как адаптивный инструмент, играет особую решающую роль в эволюции биосистем, обеспечивающий к тому же взаимодействие с окружающей средой. Задуманная Всевышним нервная система человека призвана, по-видимому, чтобы сформулировать элементарные рефлексы, реагирующие на внешние воздействия, такие как явления самоорганизации. Другими словами, отражение ею действительности является продуктом более высоких уровней информационной безопасности биосистемы в результате внешнего раздражения. Рефлексы хранятся в генетической памяти на более низких уровнях защиты информации и передаются следующим поколениям.

Самоорганизующееся поведение обеспечивает целенаправленное поведение биосистемы, необходимость образовательной системы, разрабатывает новую форму памяти в форме адаптивной информационной платформы нейронных сетей.

Переход к качественно новой форме нервной системы обусловлен поведенческими реакциями в биосистемах. Наличие поведенческих реакций подтверждает, что существует сложная связь между внешними воздействиями и реакциями организма. Различные природные носители: происходит распад информации между ДНК и нервными клетками. Поведенческая информация формируется на основе генетически передаваемых поведенческих реакций через ДНК, закреплённую на информационной платформе нервной системы. Однако поведенческие реакции биосистем не ограничиваются теми, которые передаются путём заживления. Им присуще собирание жизненного опыта и переход к будущим поколениям посредством его обучения. Результаты обучения для передачи поколениям основаны на ДНК.

Создание интеллектуальных систем информационной безопасности основано на иерархической организации защиты информации, а именно на:

- биологическое сходство архитектуры IT-систем;
- на известные механизмы информационной безопасности в биосистемах, в том числе:
    1. иерархия уровней защиты в биосфере, нуклеотид – кодон – ген – хромосома – ДНК – ... – организм – ... – биосфера;
    2. хранение генетической информации на нижних уровнях иерархии (кодон – ген – хромосома – ДНК), механизмы мутации хромосом, кодирование и декодирование информации, на основе критерия «свой/чужой» производится разбиение информации;
    3. на верхних уровнях иерархии через сенсорные органы (например, рецепторы) осуществляется связь биосистемы с внешней средой и

осуществляется накопление опыта в нейросетевых структурах нервной системы;

4. изменение генетической информации не связано с изменением формы изображения, а содержание информации не связано с изменением жизненного опыта;
5. обеспеченность биосистем, чтобы они были способны адаптироваться к информационной безопасности, включая принятие жизненного опыта, позволяющего им преуспеть в значимых ситуациях, в частности, признание их собственных и других, выбирая поведение в сложной и постоянно меняющейся среде;

- существование иерархии уровней информационной защиты IT-систем:
  - в адаптивных системах защиты информации вся необходимая информация содержится в форме так называемых информационных полей на двух уровнях иерархии: внизу, в виде площадки, где идентифицируются, собственно, сами угрозы, и на верхнем уровне иерархии, в виде площадки накопленного опыта, в котором уже известным информационным угрозам ставится в соответствие механизмы защиты информации,
  - на нижнем уровне адаптивных систем защиты информации, который называется, как иммунный, осуществляется проверка на предмет соответствия передаваемых сообщений в IT-системе по так называемому критерию «свой/чужой», а также проверяется сама форма (контейнер) представления информации;
  - информация, которая является идентифицирующей, является персональной для каждой системы информационной безопасности и, как правило, связана с формой, а не с контентом;
  - верхний уровень системы информационной безопасности называется рецепторным, который необходим для обеспечения интерактивного взаимодействия с окружающей средой и накопления эвристических

знаний в виде информационной площадки адаптивных систем информационной безопасности;

– передача и унаследование информации в адаптивных системах информационной безопасности – это перенос информационных площадок нейросетевых структур иммунного и рецепторного уровней биосистем, сформированных в процессе жизненного цикла некоторой IT-системы, в последующие поколения (потомкам) для реализации самой системы.

3.2. Методика проектирования адаптивной системы защиты информации

Способы проектирования современных адаптивных систем защиты информации базируются на основных дифференциальных (аппроксимационных) свойствах нейронных сетей и нечетких систем логического вывода, которые самым тесным образом связаны с процессами адаптивностью, обучаемостью, возможностью представления эвристических знаний экспертов по информационной безопасности посредством системы нечетких импликативных правил, трансперентных для детального анализа контекстных причинно-следственных связей между входными и выходными характеристиками.

Способность нейронных сетей к обучению рассматривается как одно из наиболее важных свойств адаптации, что позволяет в самые быстрые сроки настраиваться к возможным изменениям входной информации. При этом, в качестве обучающего фактора выступает избыточность релевантной информации и скрытые в исторических данных той или иной закономерности. В процессе адаптации все это в существенно видоизменяет информационное поле в применяемой нейронной сети, которая, снижая уровень избыточности входной информации, способна сегментировать в исторических данных

существенные признаки. За счёт имплементированных в нейронные сети механизма кластеризации посредством применения соревновательных методов обучения удаётся классифицировать поступающие информации: похожие или в определённом смысле подобные входные векторы исторических данных группируются посредством нейронной сети в виде обособленного кластера и демонстрируются конкретным искусственным нейроном – прототипом. Осуществляя кластеризацию входных данных, нейронная сеть устанавливает соответствующие усреднения по кластеру функциональных параметров искусственных нейронов – прототипов, которые в свою очередь минимизируют ошибку демонстрации сгруппированных в кластер входных данных.

Подход к проектированию системы адаптивной информационной защиты в рамках IT-систем подразумевает:

- решение задачи классификации, включая:
  - угроз по вектору признаков информационных атак;
  - механизмов информационной безопасности по вектору потенциальных угроз: осуществляется соотнесение посылок на нижнем (нечёткого вектора признаков информационных атак) и верхнем (нечёткого вектора угроз) уровнях защиты с классификационными заключениями соответственно на нижних уровнях (выявленными угрозами) и на верхних уровнях (механизмами информационной безопасности, необходимых для оперативного купирования поля известных информационных угроз);
- решение задачи кластеризации угроз по существующим признакам информационных атак и механизмам защиты по установленному вектору угроз, как адаптация процесса классификации при увеличении поля потенциальных угроз: осуществляется группировка входных векторов (на нижних уровнях иерархии системы адаптивной защиты – векторов с компонентами в виде признаков информационных атак, а на верхних уровнях – векторов информационных угроз), и прикрепление

поступающего вектора угроз к одной из установленных групп, либо классификация нового признака информационной угрозы и формирование, тем самым, новой группы угроз, в том числе на нижних уровнях иерархии – группы угроз, а на верхних уровнях – группы соответствующих механизмов защиты, необходимых для оперативного купирования поля известных информационных угроз;

- формирование так называемых матриц экспертных оценок, необходимых для установления степени соответствия на нижних уровнях иерархии системы защиты потенциальных угроз существующим признакам информационной атаки и, на верхних уровнях защиты – механизмов информационной защиты полю выявленных угроз;
- представление в виде систем нечётких логических импликативных правил результатов решения задач информационной безопасности, сформированных в процессе логического вывода классификационных заключений по нечётким предпосылкам, обусловленные: на нижних уровнях иерархии системы защиты потенциальных угроз путём соотношения «признаки информационной атаки – угрозы», а на верхних уровнях – путём соотношения «угрозы – адаптивные механизмы защиты»;
- реализация систем нечётких импликативных правил в виде адаптивных структур, например, в виде нейро-нечётких классификаторов, включая на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа «признаки информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;
- реализация последствий решения задачи распознавания информационных угроз в виде обычных (чётких) классификаторов посредством самонастраевоемой нейронной сети: на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа «признаки

информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;

- передача и/или наследование адаптивной системой защиты информации опыта (эвристических знаний) в области обеспечения информационной безопасности, приобретённого в процессе эксплуатации подобной IT-системы, в проектируемую систему защиты информации путём перенесения информационных полей чётких и нейро-нечётких классификаторов, включая на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа «признаки информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;
- с целью формирования информационных полей чётких и нейро-нечётких классификаторов производится обучение классификаторов по средствам обучающих множеств – выборок входных векторов: на нижних уровнях информационной защиты – векторов, с компонентами в виде признаков информационных атак, а на верхних уровнях – векторов потенциальных угроз);
- в процессе эксплуатации IT-системы производится адаптация информационных полей чётких и нейро-нечётких классификаторов, включая на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа «признаки информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;
- по результатам адаптации осуществляется настройка адаптируемых матриц экспертных оценок и систем нечётких импликативных (продукционных) правил;
- по результатам выполнения генерация новых нечётких импликативных правил в случае расширения классификации, включая на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа

«признаки информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;

- формирование комплекса количественных оценок степени защищённости IT-системы, исходя из результатов обучения и распределения механизмов защиты по иерархии системы защиты информации;
- с целью выявления наиболее применяемых и/или неприменяемых в корпоративной сети адаптивных механизмов информационной защиты производится детальный анализ топологической структуры связей нейро-нечётких классификаторов, транспарантной системы нечётких импликативных (продукционных) правил и комплекса оценок защищённости;
- производятся спецификации на разработку отсутствующих адаптивных механизмов защиты;
- путём расширения перечня используемых адаптивных механизмов защиты и их размещения в иерархии адаптивной системы защиты информации осуществляется общая настройка топологической структуры системы информационной безопасности.

Последовательность выше приведённых мероприятий в рамках рассматриваемого подхода к проектированию адаптивных средств защиты информации может варьироваться. Тем не менее, обязательными здесь являются следующие процедуры:

- построение матриц адаптируемых экспертных оценок и на их основе создание начальных систем нечётких продукционных импликативных правил и классификаторов, включая на нижних уровнях иерархии системы защиты потенциальных угроз классификаторов типа «признаки информационной атаки – угрозы», а на верхних уровнях – классификаторов вида «угрозы – адаптивные механизмы защиты»;
- идентификация обнаруженной информационной угрозы и при необходимости расширение поля ранее выявленных угроз путем

кластеризация угроз с последующей адаптацией информационных полей на основе обучения нейронных сетей на всех уровнях иерархии системы защиты информации;

- в следствии изменения поля угроз процесс кластеризации сопровождается структурной и параметрической настройкой и/или (при необходимости) расширением системы нечётких правил путём генерации новых импликативных правил;
- в результате обучения классификаторов уровней информационной защиты наблюдаемая трансформация поля информационных угроз влечёт за собой структурную и параметрическую модификацию систем нечётких импликативных правил, а также матриц адаптивных экспертных оценок;
- при расширении системы нечётких импликативных правил за счёт генерации новых правил формулируется описание нового (приобретённого) механизма информационной защиты;
- транспарентность системы нечётких импликативных правил позволяет сформировать спецификацию на создание отсутствующего и/или приобретаемого нового механизма информационной защиты;
- на основании комплексного анализа имеющихся в наличии адаптивных оценок защищённости корпоративной телекоммуникационной сети связи с точки зрения экономической целесообразности новый приобретённый механизм информационной защиты включается в состав адаптивных средств защиты информации.

3.3. Модель иерархической системы адаптивной защиты информации

Иерархическая модель адаптивной защиты информации использует природоподобный принцип биосистемной аналогии, в частности, она применяется в рамках иерархии системы активной защиты информационных

процессов и ресурсов в природоподобной или биологической системе. Согласно этому принципу на нижних уровнях иерархии природоподобной системы применяются механизмы иммунной защиты, а на верхних уровнях иерархии применяются механизмы адаптивной памяти и накопления опыта на протяжении функционирования нервной системы [84].

Иерархическая модель адаптивной защиты информации в корпоративных телекоммуникационных сетях связи характеризуется следующими качествами:

- сама система защиты информации является иерархически многоуровневой;
- использует экспертные оценки для привнесения эвристических знаний в виде системы нечётких импликативных правил;
- эволюционный характер адаптивных средств защиты информации обеспечивается, прежде всего, аппроксимационными свойствами и способностями к обучению за счёт структурной и параметрической оптимизации нейро-нечётких сетей, то есть гибридных систем, реализующих систему нечётких импликативных правил в логическом базисе нейронной сети.

На нижнем уровне иерархии системы защиты информации по совокупности установленных признаков, носящих неполный и/или не вполне достоверный характер, решается задача классификации и/или кластеризации информационных атак.

Другими словами, на нижнем уровне системы защиты информации, на основе эвристических знаний экспертов по информационной безопасности, система нечётких импликативных правил реализуется в логическом базисе нейронной сети. Данная система описывает процесс логического вывода относительно заключения на предмет типа информационных атак, используя, при этом, векторы входных признаков в качестве нечётких предпосылок.

На нижних уровнях иерархии системы защиты информации также применяются аппаратно-программные (в том числе и нейросетевые) средства идентификации информационных атак [58]. В данном случае, задача нечёткого распознавания информационных угроз успешно решается с применением гибридных нейро-нечётких систем классификации. При этом, если достоверность классификации по известным информационным угрозам меньше некоторого заранее установленного уровня, то при наличии признаков информационной атаки классификация угроз расширяется за счёт введения новой градации в классификацию и, тем самым, решается задача кластеризации угроз.

В случае, если классифицируется ранее неизвестная угроза, то процесс кластеризации заметно расширяет систему нечётких правил, соответствующих уровню системы информационной защиты. На верхних уровнях иерархии для каждого эшелона многоуровневой системы защиты информации адаптивные средства защиты информации используют результаты классификации нижних уровней иерархии в виде предпосылок системы нечётких импликативных правил с целью генерации нечётких заключений относительно соответствий между обнаруженными угрозами и имеющимися в наличии механизмов информационной защиты. Другими словами, здесь решается задача классификации адаптивных механизмов информационной защиты путём генерации нечёткого вывода относительно вектора нечётких признаков информационных угроз, для нейтрализации которых данные механизмы информационной защиты должны быть полностью задействованы.

Проще говоря, для каждого эшелона многоуровневой системы защиты информации, применяя в качестве предпосылок результаты нечеткой классификации типов информационных атак, посредством системы нечетких импликативных правил описывается соответствие между информационными угрозами и механизмами защиты, исходя из эвристических знаний экспертов по информационной безопасности. После обучения нейронная сеть на данном

уровне иерархии способна будет определить достоверность нейтрализации угрозы, заданной в отдельном правиле набора всевозможных информационных угроз, посредством соответствующего механизма защиты рассматриваемого эшелона многоуровневой системы защиты информации.

После обучения нейронной сети, подразумевающее настройку весовых коэффициентов синоптических связей и порогов нелинейных нейронов из скрытых слоёв, при расширении размерности входного вектора признаков потенциальных информационных угроз степень достоверности процесса классификации по адаптивным механизмам защиты, включая активность механизмов защиты отдельных эшелонов, ниже некоторого установленного уровня, то при выявлении признаков информационной атаки классификация адаптивных механизмов защиты расширяется путём введения новой градации (шкалы) в классификацию, что предопределяет решение задачи кластеризации механизмов защиты в рамках системы информационной защиты.

После адаптации нечёткой системы вывода в логическом базисе нейронной сети к соответствующему эшелону данных анализ нечеткого импликативного правила по вновь введённому механизму защиты информации позволяет пользователю в рамках системы информационной защиты сформировать соответствующую спецификацию на отсутствующий механизм защиты. Для эшелонов иерархической многоуровневой системы информационной защиты необходимо сформировать новые лингвистические переменные, такие как «*частота реализации угрозы*» и «*потенциальный ущерб*», где экспертные оценки имеют первостепенное значение.

Также необходим верхний уровень иерархии системы информационной защиты, на котором производится обобщение достигнутых результатов (предпосылок) в виде активности адаптивных механизмов защиты. Наблюдаемые частоты реализации и ущерба от информационной угрозы помогают сформировать системы нечетких импликативных правил – обоснованных заключений о необходимости расширения контента

активированных механизмов защиты по отдельным эшелонам средств защиты информации. Активация подходящего адаптивного механизма информационной защиты производится, если агрегированные оценки, учитывающие величину нанесённого потенциального ущерба, частота реализации информационных угроз и достоверность нейтрализации угроз данным механизмом защиты, превышают установленные пороговые значения.

3.4. Структура модели иерархической адаптивной системы защиты информации

Проектирование адаптивной системы защиты информации, которая является многоуровневой и, соответственно, иерархической, должно осуществляться в комплексном порядке (см. рис. 3.1).

Ключевым звеном модели адаптивной системы защиты информации в корпоративных телекоммуникационных сетях связи считается методика оценки степени и их защищённости. По средствам адаптивных средств информационной защиты, таких как искусственные многослойные feedforward нейронные сети, нечёткие системы логического вывода в логическом базисе многослойной нейронной сети и обычных систем нечётких импликативных правил, данная модель должна предусматривать координацию взаимных связей между применяемыми в рамках системы информационной защиты классификаторов информационных угроз и соответствующих механизмов защиты, структурированность модели системы информационной безопасности, программных и инструментальных средств оценки показателей защищённости от информационных угроз и, собственно, самого рейтинга корпоративной телекоммуникационной сети связи.

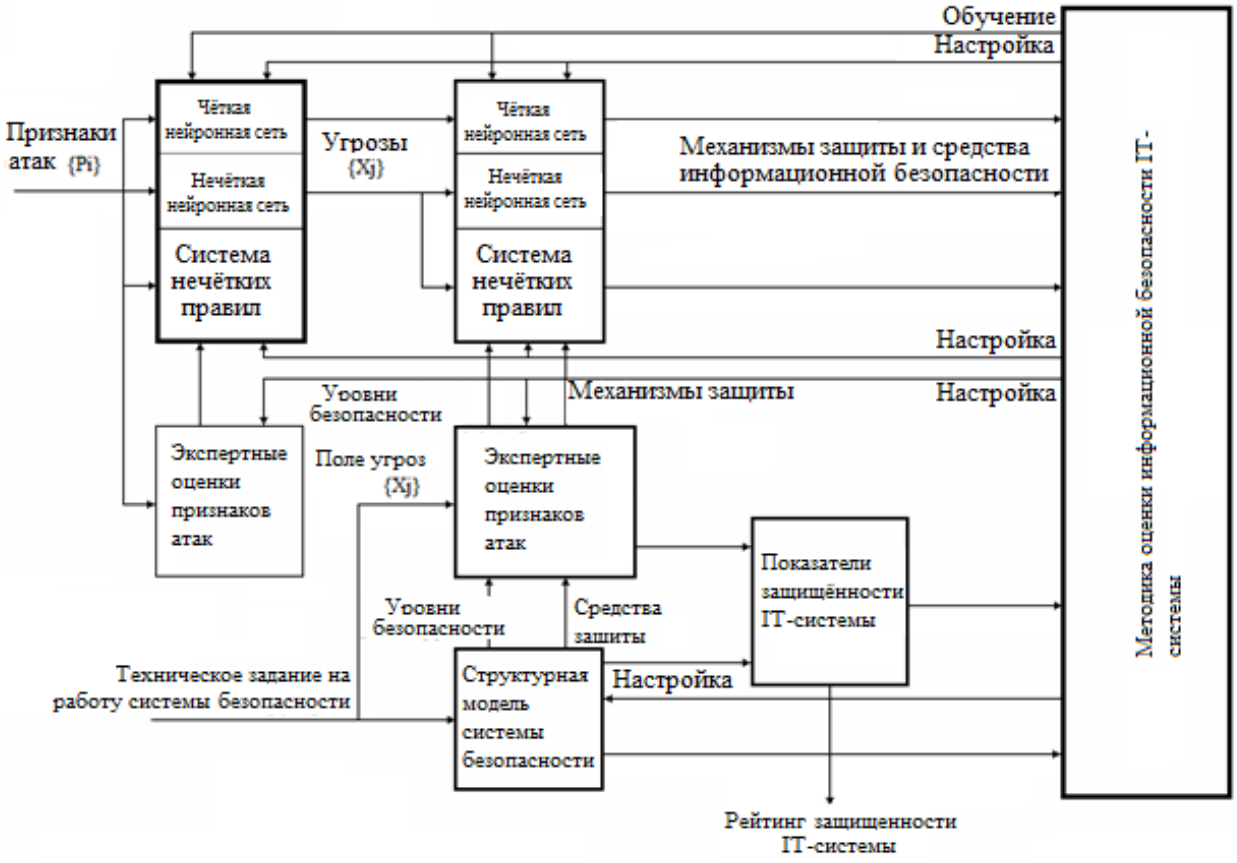

Рис. 3.1: Структура модели системы адаптивной защиты информации

Любое поле информационных угроз является динамичным, поэтому оно диктует первоочередную необходимость наличия свойства адаптивности у механизмов защиты корпоративных сетей открытого типа. Другим не менее важным и характерным свойством проектируемой системы информационной защиты является возможность реализации накопленных эвристических знаний о потенциальных информационных угрозах, которое обеспечивается посредством соответствующей информационно-полевой компоненты многоуровневой иерархии механизмов защиты. Тем не менее, произвольное применение относительно широкого набора всевозможных механизмов защиты в объекте информатизации считается нецелесообразным. Обычно в корпоративных сетях ограничиваются минимально необходимым составом механизмов защиты, то есть таким, чтобы его состав был достаточным для отражения потенциальных угроз, оговоренных в сформулированной

спецификации при проектировании системы информационной безопасности в корпоративных сетях.

Структурная модель иерархической системы информационной безопасности в корпоративных сетях выбирается в соответствии с техническим заданием на её проектирование. Модель должна учитывать многоуровневую иерархию запланированных механизмов защиты, а эвристические знания специалистов по информационной безопасности отображается в виде массивов данных экспертных оценок. На базе таких массивов, собственно, и генерируются системы нечетких импликативных правил для классификации:

- угроз по признакам информационных атак;
- адаптивных механизмов защиты на поле информационных угроз.

Системы нечётких импликативных правил для последующей адаптации и анализа представляются в виде нечётких нейронных сетей, которые настраиваются путём обучения на основе установленного множества входных векторов с компонентами в виде нечётких множеств, описывающих признаки информационной атаки.

Параллельно с этим обучаются нейро-сетевые классификаторы из расчёта того, что число формируемых кластеров должно равняться числу импликативных правил в системе нечёткого вывода.

Обычные гибридные (нейросетевые) классификаторы адаптивных механизмов информационной защиты обучаются аналогичным образом, но уже по заранее установленным векторам известных информационных угроз.

Кроме того, для исходных массивов данных привлечённых экспертных оценок рассчитываются показатели информационной защищённости и суммарного (взвешенного) рейтинга корпоративной сети, которые затем используются в общей методике оценки защищённости корпоративной сети для рабочего анализа и настройки, как массивов данных самих экспертных оценок, так и структурной и параметрической оптимизации нейросетевых классификаторов и систем нечётких импликативных правил.

Аналогично с природоподобными системами априорные данные в адаптивной системе защиты информации хранятся и могут передаваться из поколения в поколение путём тиражирования и последующей модификации корпоративной сети в виде перераспределённых адаптивных информационных полей нейронных сетей:

- поля известных потенциальных угроз «иммунных» уровней защиты;
- поля приобретённых эвристических знаний в рецепторных уровнях информационной защиты.

Процесс адаптации полей известных потенциальных угроз «иммунных» уровней защиты органично связан с решением задач кластеризации и классификации, которые обуславливают расширение информационного поля известных угроз на нижних уровнях иерархии средств защиты информации.

Модификация выявленных в прошлом информационных угроз, как правило, должно отражаться на верхних уровнях иерархии системы защиты информации в соответствующем пространстве эвристических знаний, формализованных и поддерживаемых посредством специальной топологической структуры системы нечётких импликативных правил, реализуемой в логическом базисе многослойной нейронной сети. Процесс адаптации системы нечётких импликативных правил происходит посредством настройки параметров нечёткой нейронной сети на основе какого-нибудь супервизорного алгоритма обучения, который адаптирует систему нечетких импликативных правил путем сопоставления механизмов информационной защиты известным информационным угрозам.

3.5. Механизмы построения модели адаптивной системы информационной защиты

Таким образом, в качестве механизмов реализации интеллектуальных (или адаптивных) особенностей системы информационной защиты необходимо выбирать такие инструменты, которые могли бы обладать способностями хранить знания, приобретённые в процессе обучения, а также возможность нечёткого распределённого информационного поля нейронной сети.

С точки зрения концепции модели адаптивной системы информационной защиты другим важным механизмом является нечёткий логический вывод, который основывается на нечётком представлении входной в нейронную сеть информации и, тем самым, обеспечивает применение эвристические знания специалистов в области информационной безопасности. Материализация данной идеи осуществляется посредством предварительного обучения (или структурной и параметрической оптимизации) системы нечётких импликативных правил, реализованных в логическом базисе нейронной сети.

Способность интеграции системы нечётких импликативных правил в состав иерархической структуры системы защиты информации с возможностью её обучения на информационном пространстве известных угроз позволяет вовремя устранить несовместимость с реальностью начальной системы нечётких импликативных правил, а также предоставляет возможность анализировать сам процесс нечёткого логического вывода с целью конкретизации имеющейся в наличии и/или синтеза новой системы нечётких импликативных правил адаптивной системы защиты информации.

Следующей особенностью при построении модели адаптивной системы защиты информации, является способность нейронных сетей и гибридных нейро-нечётких систем реализовывать классификацию и кластеризацию информационных атак и потенциальных угроз.

3.5.1. Нечёткий вывод в логическом базисе нейронной сети

Нечёткий логический вывод. Нечёткие нейронные сети включают в себя системы с нечёткого вывода, основанные на априорной практике, которая, как правило, реализуется в виде комбинированного применения обычных нейронных сетей и системы нечётких импликативных правил. Механизм нечёткого логического вывода формируется специалистами по безопасности в виде системы импликативных правил, например, в виде:

$$\begin{cases} R_1\text{: “Если } x \text{ есть } A_1, \text{то } y \text{ есть } B_1\text{”;} \\ R_2\text{: “Если } x \text{ есть } A_2, \text{то } y \text{ есть } B_2\text{”;} \\ \dots \\ R_n\text{: “Если } x \text{ есть } A_n, \text{то } y \text{ есть } B_n\text{”,} \end{cases}$$

и формирует в таком виде так называемую базу знаний. В данном случае, *x* является входной лингвистической переменной (например, угроза), *y* является выходной лингвистической переменной (например, механизмы защиты), A_i и B_i (i=1÷n) – нечёткие множества, описывающие термы (значения) соответствующих лингвистических переменных.

Применяемые в правилах импликации (нечёткие отношения) вида $R=A \Rightarrow B$ отражают знания специалиста по информационной безопасности в виде причинно-следственных связей между предпосылками (угрозами) и заключениями относительно выбора механизма защиты. Здесь символ «⇒» обозначает операцию нечёткой импликации. Вообще в нечёткой среде используются различные импликации. Ниже, в таблице 3.1 представлены наиболее распространённые из них.

Таблица 3.1.

Нечёткие операторы импликаций

№№	Название импликации	Нечёткие операторы импликаций
1.	L. Zadeh	$I_m(x,y) = \max(1-x, \min(x,y))$
2.	Lukasiewicz	$I_a(x,y) = \min(1, 1-x+y)$
3.	Minimum (Mamdani)	$I_c(x,y) = \min(x,y)$

4.	Standard Star (Godel)	$I_g(x,y)=\begin{cases}1, x\le y\\ y, x>y\end{cases}$
5.	Kleene – Dienes	$I_b(x,y)=\max(1-x,y)$
5.	Gaines	$I_\Delta(x,y)=\begin{cases}1, x\le y\\ \dfrac{y}{x}, x>y\end{cases}$
7.	Yager	$I_E(x,y)=y^x$

Само отношение R можно рассматривать как нечёткое подмножество прямого декартового произведения $X\times Y$ – полного множества угроз X и механизмов защиты Y, а процесс достижения нечёткого результата вывода по предпосылке и существующим знаниям – в виде композиционного правила:

$$B=A^{\circ}R=A^{\circ}(A\Rightarrow B),$$

где «°» обозначает операцию, например, максиминную композицию вида [47, 63]:

$$\mu_{\tilde{G}}(i)=\max_{w\in W}(\min\mu_{\tilde{A}}(w),\mu_{\tilde{D}}(w,i)).$$

Механизм нечёткого логического вывода подразумевает последовательное выполнение следующих процедур [1]:

1) Фаззификация, то есть введение нечёткости или, проще говоря, по заданным функциям принадлежности нечётких подмножеств области определения входных признаков, описываемых соответствующими термами, назначается степень истинности каждой информационной угрозы для каждого конкретного правила, исходя из фактических значений нечёткого множества;

2) Логический вывод, подразумевающий формирование по степени истинности угроз нечёткого заключения по каждому из правил, образующие нечеткое подмножество универсума для каждого механизма защиты;

3) Композиция правил: полученные на предыдущем шаге нечёткие подмножества универсума для каждого механизма защиты объединяются с целью формирования нечёткого подмножества для универсума всех механизмов защиты (по всем правилам);

4) Дефаззификация, то есть численное описание нечётких выводов, полученных на предыдущем шаге. На этом шаге осуществляется преобразование нечёткого набора выводов по всем правилам в численное значение итоговой защищённости корпоративной сети.

Указанные процедуры нечёткого логического вывода, например, для следующего набора импликативных правил

$$\begin{cases} R_1\text{: “Если } x \text{ есть } A, \text{то } y \text{ есть } D\text{”;} \\ R_2\text{: “Если } y \text{ есть } B, \text{то } y \text{ есть } E\text{”;} \\ R_3\text{: “Если } z \text{ есть } C, \text{то } y \text{ есть } F\text{”,} \end{cases} \tag{3.1}$$

могут быть реализованы в нотации MATLAB\Fuzzy Inference System так, как это показано на рис. 3.2. В данном случае, x, y и z – входные лингвистические переменные соответствующих известных угроз; y – выходная лингвистическая переменная, соответствующая итоговой защищённости корпоративной сети; A, B, C, D, E и F – нечёткие множества, описывающие соответствующие семантические данные признаков информационных угроз.

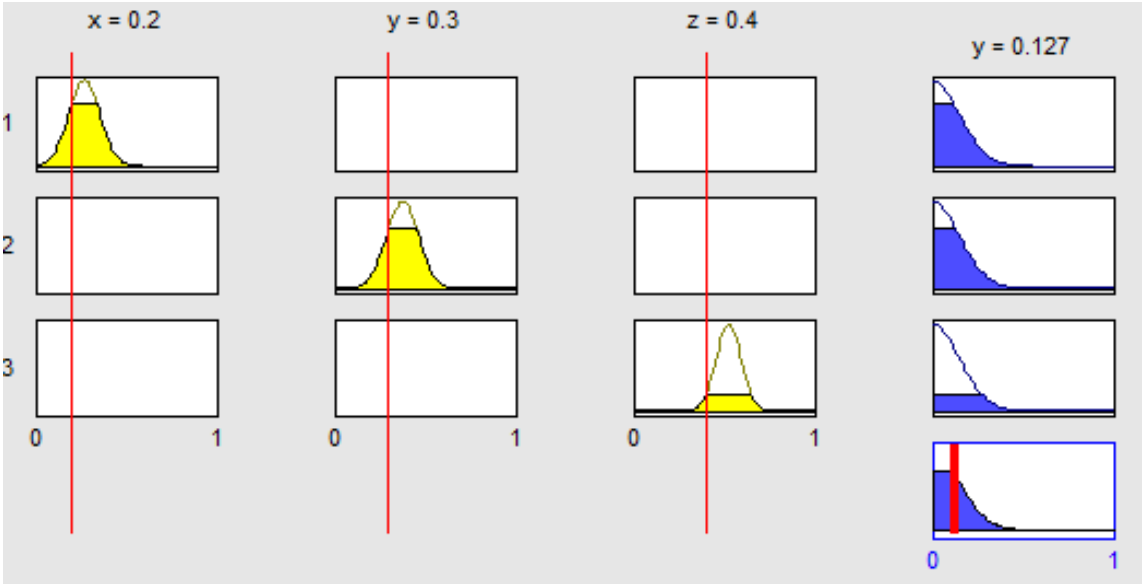

Рис. 3.2: Реализация правил (3.1) в нотации MATLAB\Fuzzy Inference System

Пояснение процедур механизма нечёткого вывода дадим в следующей интерпретации:

Шаг 1: на основании значений непрерывных переменных по семантикам *A, B, C* находятся степени истинности $\alpha(x_0)=A(x_0)$, $\alpha(y_0)=B(y_0)$ и $\alpha(z_0)=C(z_0)$ информационной угрозы для каждого из нечётких импликативных правил.

Шаг 2: посредством логической операции «min» в соответствии со степенями истинности $\alpha(x_0)=A(x_0)$, $\alpha(y_0)=B(y_0)$ и $\alpha(z_0)=C(z_0)$ удаляются верхние части семантик *D, E* и *F*, после чего формируются нечёткие заключения по каждому из правил, образующие нечёткое подмножество универсума для каждого механизма защиты.

Шаг 3: посредством логической операции «max» осуществляется объединение усечённых семантик и формируются комбинированное нечёткое подмножество, описываемого семантикой $\mu_{\Sigma}(y)$ и соответствующего нечёткому логическому выводу для выходной переменной *w* итоговой защищённости корпоративной сети.

Шаг 4: определяется, например, с использованием центроидного метода дефаззификации, численное значение терма выходной лингвистической переменной.

Нечёткая классификация информационных признаков. В рамках механизма классификации, входящего в состав адаптивных средств защиты информации, целесообразно использовать сочетание возможностей нейронных сетей и элементов нечёткой логики. В частности, искусственные нейронные сети и системы нечёткого вывода имеют характерные особенности, например, возможность обучения нейронных сетей и транспорентность процесса решения задач информационной безопасности посредством систем нечёткого логического вывода, интерпретирующих объяснения получаемых нечётких

выводов. Комбинирование этих методов в гибридную нейро-нечёткую систему обеспечивает получение выгоды от совместного применения достоинств нейросетевых структур и нечётких логических систем, опирающихся на эвристические знания экспертов в области информационной безопасности.

Как следует из опыта разработки гибридных нейро-нечётких систем (см таблицу 3.1) [104] в целях классификации информационных угроз применяются гибридные нейро-нечёткие системы 1-го типа, которые решают задачу отнесения нечёткого входного вектора к чёткому классу, а нейро-нечёткие сети остальных типов применяются для построения нечётких систем, основанных на системе нечётких импликативных правил вывода.

По нечётким векторам признаков информационных угроз посредством нейронной сети, веса синоптических связей которой являются нечёткими, рассмотрим метод формирования нейро-нечёткого классификатора, использующего механизм нечёткого логического вывода для классификации соответствующего адаптивного механизма информационной защиты [101].

Таблица 3.1

Нейронные сети, используемые для решения задач классификации

Тип нечёткой нейронной сети	**Веса**	**Вход**	**Желаемый выход**
1	Чёткий	Нечёткий	Чёткий
2	Чёткий	Нечёткий	Нечёткий
3	Нечёткий	Нечёткий	Нечёткий
4	Нечёткий	Чёткий	Нечёткий
5	Чёткий	Чёткий	Нечёткий
6	Нечёткий	Чёткий	Чёткий
7	Нечёткий	Нечёткий	Чёткий

Сам механизм нечёткого логического вывода основан на базе эвристических знаний специалистов по информационной безопасности, которая формируется в виде системы нечётких импликативных правил следующего вида:

$$\begin{cases} R_1\text{: “Если } x_1 \text{ есть } \tilde{A}_{11} \text{ и } x_2 \text{ есть } \tilde{A}_{12} \text{ и … и } x_n \text{ есть } \tilde{A}_{1n}, \text{то } y \text{ есть } \tilde{B}_1\text{”;} \\ R_2\text{: “Если } x_1 \text{ есть } \tilde{A}_{21} \text{ и } x_2 \text{ есть } \tilde{A}_{22} \text{ и … и } x_n \text{ есть } \tilde{A}_{2n}, \text{то } y \text{ есть } \tilde{B}_2\text{”;} \\ \dots \\ R_m\text{: “Если } x_1 \text{ есть } \tilde{A}_{m1} \text{ и } x_2 \text{ есть } \tilde{A}_{m2} \text{ и … и } x_n \text{ есть } \tilde{A}_{mn}, \text{то } y \text{ есть } \tilde{B}_m\text{”,} \end{cases} \quad (3.2$$

где x_i и y_j (i=1÷n; j=1÷m) – нечёткие входные переменные и переменные вывода, соответствующие информационным угрозам и механизмам защиты; $\tilde{B}_j$ – нечёткие множества, описывающие их соответствующие термы.

Теперь предположим, что задано полное пространство угроз (предпосылок) X={x_1, x_2, ..., x_n} и полное пространство механизмов защиты (заключений) Y={y_1, y_2, ..., y_m}. Тогда между x_i и y_j (i=1÷n; j=1÷m) существуют нечёткие причинно-следственные отношения в виде $x_i \Rightarrow y_j$, которые можно представить в виде матрицы R=[r_{ij}] (i=1÷n; j=1÷m), а предпосылки и заключения можно представить в виде нечётких множеств $\tilde{A}$ и $\tilde{B}$ на пространствах X и Y, отношения которых можно представить в виде: $\tilde{B} = \tilde{A} \circ R$, где «°» означает логическую операцию композиции правил, например, максиминная композиция.

Для реализации системы нечётких импликативных правил нейро-нечёткий классификатор в составе адаптивных средств информационной защиты по нечётким векторам признаков угроз обязан выполнять следующие действия:

- Фаззификацию по заданным на области определения входных нечётких множеств функциям принадлежности. В результате фаззификации в соответствии с термом нечёткой переменной устанавливается степень истинности для каждой потенциальной угрозы.

- Логический вывод, предусматривающий по степени истинности потенциальных информационных угроз генерацию нечёткого заключения по каждому из импликативных правил. Данное заключение (conclusion) является нечётким подмножеством универсума по каждой выходной лингвистической переменной, ассоциирующейся с соответствующим механизмом защиты.
- Композиция, которая предусматривает объединение полученных на предыдущем этапе нечётких подмножеств для каждой лингвистической переменной вывода по всем правилам с целью формирования единого нечёткого подмножества универсума для всех переменных вывода.

В полном пространстве информационных угроз, описанных n-мерным вектором признаков $X=\{x_1, x_2, ..., x_n\}$, максимально число входных векторов с нечёткими компонентами задаётся по средствам всевозможных сочетаний координат x_i. Каждому входному вектору из пространства X можно сопоставить нечёткий нейрон гибридного нейро-нечёткого классификатора, выполняющий операцию логического вывода, например, логическую операцию «min». Отображение множества результатов нечёткого логического вывода в полное пространство нечётких выводов реализуется посредством операции композиции правил, согласно которому каждому выходному вектору из пространства Y можно сопоставить нечёткий искусственный нейрон нейро-нечёткого классификатора, выполняющий, например, логическую операцию «max».

Нейро-нечёткий классификатор n-мерных нормализованных векторов угроз X с нечёткими координаторами $(x_1, x_2, ..., x_n)$ может быть представлен в виде трёхслойной нечёткой нейронной сети (см. рис. 3.3), в которой:

- 1-ый слой содержит n угроз – по числу координат входного вектора угроз, нечётких искусственных нейронов с комплементарными нечёткими связями, формирующих n пар нечётких высказываний вида: x_i есть S и x_i есть L ($i=1\div n$).

- скрытый слой содержит до 2^n нечётких нейронов, каждый из которых выполняет операцию логического вывода (например, операцию «min») над сочетаниями нечётких множеств 1-го слоя нейронной сети для формирования системы нечётких заключений по классификации информационных угроз;
- выходной слой содержит m нечётких нейронов – по числу координат выходного вектора. Эти нейроны симулируют нечёткую операцию композиции (например, max) над классификационными выводами 2-го слоя нейронной сети с тем, чтобы сформировать m-мерные векторы Y выходных нечётких выводов (y_1, y_2, ..., y_m).

Нечёткие нейроны из первого слоя формируют комплементарные пары значений истинности для входных нечётких переменных x_i координат входного вектора угроз X. При заданном значении координаты вектора угроз X на отрезке области определения каждому значению чёткой переменной сопоставляется значение ординат функций принадлежности S (small) и L (large), которые в сумме дают 1 (рис. 3.4).

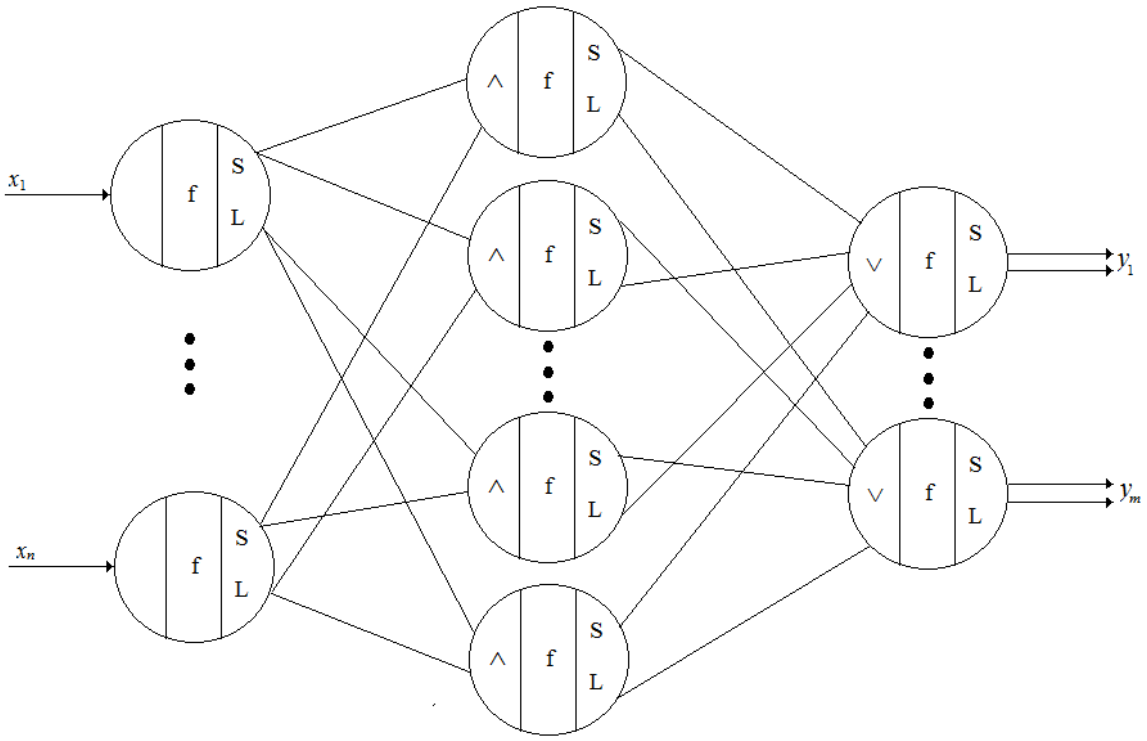

Рис. 3.3: Нейро-нечёткий классификатор

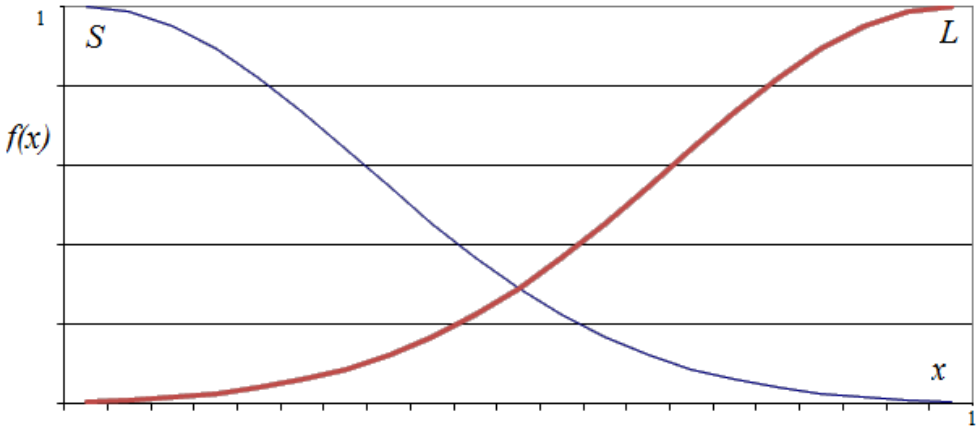

Рис. 3.4: Функции принадлежности комплементарной нечёткой связи

Изображённая на рис. 3.4 пара функций принадлежности *S* и *L* образуют два нечётких отношения, составляющие одну комплементарную нечёткую связь.

Если второй слой нечёткой многослойной нейронной сети содержит максимальное число нечётких нейронов типа логической операции «И», тогда промежуточный вектор нечётких заключений должен включать в себя всевозможные нечёткие заключения относительно классификации признаков угроз, которые могут быть истекать из всех возможных векторов угроз.

Третий слой нечёткой многослойной нейронной сети включает в себя нечёткие нейроны типа логической операции «ИЛИ», по числу равные количеству нечётких заключений типа y_j (j=1÷m), и формирует вектор нечётких выводов в соответствии с системой нечётких импликативных правил, отображающих заранее установленные эвристические знания специалистов по информационной безопасности системой.

Дальнейшая структурно-параметрическая настройка нейро-нечёткого классификатора адаптивного механизма защиты на основе нечётких векторов угроз осуществляется супервизорным алгоритмом обучения нейро-нечётких сетей с применением механизма нечётких отношений. В результате структурно-

параметрической настройки нейро-нечёткого классификатора на основе обучающего множества векторов известных угроз появляется возможность обнаружить возможную логическую противоречивость в системе нечётких импликативных правил и устранить из многослойной структуры нейронной сети несущественные причинно-следственные связи (или необоснованные генерации заключений в системе нечётких правил).

2.5.2. Формирование и формулирование эвристических знаний в адаптивных средствах защиты информации

Формирование и формулирование эвристических знаний в информационных полях гибридных классификаторов из состава иерархических уровней адаптивных средств защиты информации, происходит в процессе структурно-параметрической настройки гибридных нейросетевых моделей защиты информации.

Рассмотрим один из супервизорных алгоритмов обучения гибридных классификаторов, базирующийся на системе нечётких импликативных правил. Предположим, что гибридный классификатор в виде нейро-нечёткой структуры, имеющей N входов – по числу заданных потенциальных угроз, должен реализовать некоторое отображение:

$$y^k = f(x^k) = f(x_1^k, x_2^k, \dots, x_N^k)$$

согласно обучающему множеству $\{(x^1, y^1), (x^2, y^2), \dots, (x^n, y^n)\}$, где $k = 1 \div n$ является размерностью обучающего множества.

Для формализации этого отображения f воспользуемся системой нечеткого логического вывода, которая для всех i=1÷m, где i – обозначает число применяемых адаптивных механизмов защиты, отражается следующей системой импликативных правил:

R_i: “Если x_1 есть v_{i1} и x_2 есть v_{i2} и … и x_n есть v_{in}, то y есть z_i”,

где v_{ij} – семантическая данная (слабо структурированный терм), соответствующая j-й уязвимости для i-го механизма защиты, z_i – вещественное число, характеризующее степень применения i-го механизма защиты в процессе формирования значения итоговой защищённости системы.

Степень истинности i-го правила α_i устанавливается посредством моделирования логической операции «И», скажем, посредством операции арифметического умножения

$$\alpha_i = \prod_{j=1}^{n} v_{ij}(x_j^k).$$

Согласно центроидному методу дефаззификации чёткий (численный) вывод системы определяется как:

$$o^k = \frac{(\sum_{i=1}^{n} \alpha_i z_i)}{(\sum_{i=1}^{n} \alpha_i)},$$

а функции ошибки для k-го предъявленного сценария можно определить, как

$$E_k = 0.5(o^k - y^k).$$

Для параметрической настройки системы исходных импликативных правил в логическом базисе многослойной нейронной сети, подразумевающее оптимизацию параметров функций принадлежности нечётких множеств, описывающих термы из левых частей правил, можно применить градиентный метод обучения «error backpropagation» ровно также, как и при обучении обычных feedforward нейронные сети. Данный алгоритм реализуется на основании следующих итеративных равенств:

$$z_i(t+1) = z_i(t) - \eta \frac{\partial E_k}{\partial z_i} = z_i(t) - \eta(o^k - y^k) \frac{\alpha_i}{\alpha_1 + \alpha_2 + \cdots + \alpha_m},$$

где $\eta \in (0;\ 1)$ является постоянной величиной, устанавливающей скорость обучения, принимаемой заранее самим пользователем. При выборе большего значения η скорость обучения будет скорым, но при этом качество будет хуже. Верно и обратное.

3.6. Методика оценки защищённости корпоративной сети

Основанная на эвристических знаниях по информационной безопасности экспертная оценка достоверности нейтрализации поля известных угроз по средствам имеющихся в наличии адаптивных механизмов защиты формируется на каждом эшелоне многоуровневой системы защиты информации. Нанесённый ущерб от применения угроз в корпоративных сетях необходимо оценивать в относительных слабо структурированных величинах, например, по отношению к максимальной величине, допустимой для данной компании. Размер потенциального ущерба рассчитывается за определённый период времени с учётом наблюдаемой частоты активации информационных угроз.

1. Исходные экспертные оценки достоверности нейтрализации поля известных угроз отражаются в следующей матричной форме. Для каждого эшелона иерархической системы защиты информации оценивается достоверность нейтрализации угроз по средствам адаптивных механизмов защиты с дальнейшим формированием матрицы достоверности «механизмы защиты – угрозы» вида:

$$MT_{m\times p} = \begin{bmatrix} mt_{11} & mt_{12} & \dots & mt_{1p} \\ mt_{21} & mt_{22} & \dots & mt_{2p} \\ \dots & \dots & \dots & \dots \\ mt_{m1} & mt_{m2} & \dots & mt_{mp} \end{bmatrix}$$

и матрицы достоверности «угрозы – эшелоны» вида:

$$TE_{p\times n} = \begin{bmatrix} te_{11} & te_{12} & \dots & te_{1n} \\ te_{21} & te_{22} & \dots & te_{2n} \\ \dots & \dots & \dots & \dots \\ te_{p1} & te_{p2} & \dots & te_{pn} \end{bmatrix}$$

где m – число механизмов защиты; p – число известных угроз.

Для каждого эшелона иерархической системы защиты информации оценивается уровень потенциального ущерба и формируются матрицы «эшелоны – ущерб» вида:

$$EZ_{n\times p} = \begin{bmatrix} ez_{11} & ez_{12} \dots & ez_{1p} \\ ez_{21} & ez_{22} \dots & ez_{2p} \\ \dots & \dots \dots & \dots \\ ez_{n1} & ez_{n2} \dots & ez_{np} \end{bmatrix}$$

и матрицы «ущерб-МЗ» вида:

$$ZM_{p\times m} = \begin{bmatrix} zm_{11} & zm_{12} \dots & zm_{1m} \\ zm_{21} & zm_{22} \dots & zm_{2m} \\ \dots & \dots \dots & \dots \\ zm_{p1} & zm_{p2} \dots & zm_{pm} \end{bmatrix},$$

где m – адаптивных число механизмов защиты, p – число известных угроз, n– число эшелонов иерархической системы защиты информации.

2. Для каждого эшелона иерархической системы защиты информации экспертные оценки в виде системы нечётких импликативных правил отображаются в структуре гибридных систем. В процессе структурной и параметрической настройки нечётких нейронных сетей на основе обучающего множества в составе многоуровневой системы защиты информации, производится автоматическая настройка системы нечетких импликативных правил, а также основных показателей потенциального ущерба и истинности нейтрализации набора угроз соответствующим эшелоном или адаптивным механизмом иерархической системы защиты информации. Точность исходных экспертных оценок проверяется путём сопоставления элементов приведённых матриц, либо путём сопоставления агрегированных оценок защищённости до и после процесса обучения гибридных систем защиты информации.

3. Агрегированные оценки защищённости корпоративной сети определяют путём несложных математических операций над матрицами. В частности, умножение матриц *MT* и *TE* позволяет получить искомую матрицу *ME*, отражающую истинности активации известных адаптивных механизмов

защиты, которые в целях нейтрализации потенциальных угроз распределены по эшелонам иерархической системы защиты информации:

$$ME_{m\times n} = \begin{bmatrix} me_{11} & me_{12} \dots & me_{1n} \\ me_{21} & me_{22} \dots & me_{2n} \\ \dots & \dots & \dots \\ me_{m1} & me_{m2} \dots & me_{mn} \end{bmatrix}.$$

В данном случае m – число механизмов защиты, n – число эшелонов иерархической системы защиты информации.

Умножение матрицы потенциального ущерба *ET* и *TM* даёт матрицу потенциального ущерба типа «эшелоны-МЗ» *EM,* отражающую распределение потенциального ущерба от реализации известных угроз по механизмам защиты и эшелонами иерархической системы защиты информации.

$$EM_{n\times m} = \begin{bmatrix} em_{11} & em_{12} \dots & em_{1m} \\ em_{21} & em_{22} \dots & em_{2m} \\ \dots & \dots & \dots \\ em_{n1} & em_{n2} \dots & em_{nm} \end{bmatrix}.$$

Здесь m – число эшелонов иерархической системы защиты информации, n – число механизмов защиты.

Промежуточные оценки, например, находящаяся на пересечении 1-ой строки и 2-го столбца агрегированных показателей характеризуют активность применения конкретного механизма защиты, либо отдельного эшелона в рамках иерархической системы защиты информации, а также позволяют оценить размер нанесённого потенциального ущерба с точки зрения адаптивных механизмов защиты и эшелонов многоуровневой системы информационной безопасности.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Основными результатами, содержащимися в диссертационной работе, являются следующие:

- Рассмотрена модель адаптивной системы информационной защиты в корпоративных телекоммуникационных сетях открытого типа, характеризующаяся применением многоуровневой иерархии адаптивных нейросетвых структур защиты информации, комплекса агрегированных показателей информационной защищённости, который основан на эвристических знаниях специалистов по информационной безопасности.
- Предложена и исследована методика анализа и применения адаптивной системы защиты информации в корпоративных телекоммуникационных сетях открытого типа, которая характеризуется совместным применением адаптируемых эвристических знаний специалистов по информационной безопасности, инструментов искусственного интеллекта на базе многослойных нейронных сетей с целью минимизации соотношения «финансовые затраты / информационная защищённость» при проектировании адаптивных систем информационной защиты.
- Рассмотрен достаточно обширный комплекс интегральных показателей для оценки защищённости корпоративных телекоммуникационных сетей открытого типа посредством имплементированной автономной систем информационной безопасности, который отличается за счёт учёта истинности активации адаптивных механизмов защиты, частоты активации информационных угроз, размера потенциального ущерба от реализации угроз в корпоративных сетях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ажмухамедов И.М. Концептуальная модель управления комплексной безопасностью системы // Вестник АГТУ. Серия: «Управление, вычислительная техника и информатика» 1/2010 г., с. 62-66
2. Бабенко Л.К., Макаревич О.Б., Федоров В.М., Юрков П.Ю. Голосовая текстонезависимая система аутентификации идентификации пользователя // Нейрокомпьютеры: разработка и применение. 2003, №10-11.
3. Бочков М.В. Реализация методов обнаружения программных атак и противодействия программному подавлению в компьютерных сетях на основе нейронных сетей и генетических алгоритмов оптимизации // Сб. докл. VI Межд. конф. по мягким вычислениям и измерениям SCM’2003. – СПб.: СПГЭТУ, 2003. т.1. С. 376-378.
4. Бочков М.В., Копчак Я.М. Метод идентификации вычислительных сетей при ведении компьютерной разведки // Сб. докл. VI Междунар. конф. SCM’2003 – СПб.: СПГЭТУ, 2003. т.1. С.288-290.
5. Бочков М.В., Крупский С.А., Саенко И.Б. Применение генетических алгоритмов оптимизации в задачах информационного противодействия сетевым атакам. // Управление и информационные технологии. Всерос. науч. конф., Сб. док. т.2. – СПб.: ЛЭТИ, 2003. С.13-16.
6. Бочков М.В., Логинов В.А., Саенко И.Б. Активный аудит действий пользователей в защищённой сети // Защита информации. Конфидент. 2002, №4-5. С.94-98.
7. Вакка Дж. Секреты безопасности в Internet. – Киев: Диалектика, 1997.
8. Веселов В.В., Елманов О.А., Карелов И.Н. Комплекс мониторинга информационных систем на основе нейросетевых технологий // Нейрокомпьютеры: разработка и применение. 2001, №12.
9. Галушкин А.И. Нейрокомпьютеры и их применение. – М.: ИПРЖР, 2000. - Кн. 3.

10. Головань А.В., Шевцова Н.А., Подладчикова Л.Н., Маркин С.Н., Шапошников Д.Г. Детектирование информативных областей лиц с помощью локальных признаков // Нейрокомпьютеры: разработка и применение. 2001, №1.
11. Головин Р.А., Платонов В.В. Data-mining для обнаружения вторжений. Кластерный анализ информации // Информационная безопасность регионов России (ИБРР-2005): Матер. IV Санкт-Петерб. межрегион. конф. – СПб: Политехника-сервис, 2005. С. 94-95.
12. Городецкий В.И., Карсаев О.В., Котенко И.В. Программный прототип многоагентной системы обнаружения вторжений в компьютерные сети // ICAI'2001. Международный конгресс «Искусственный интеллект в XXI веке». Труды конгресса. т.1. М.: Физматлит, 2001.
13. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. М.: СИНТЕГ, 1999.
14. Гузик В.Ф., Галуев Г.А., Десятерик М.Н. Биометрическая нейросетевая система идентификации пользователя по особенностям клавиатурного почерка // Нейрокомпьютеры: разработка и применение. 2001, №7-8.
15. Девянин П.Н. и др. Теоретические основы компьютерной безопасности. – М.: «Радио и Связь» – 2000.
16. Джейн А.К., Мао Ж., Моиуддин К.М. Введение в искусственные нейронные сети // Открытые системы. 1997. №4. С.16-24.
17. Домарев В.В. Безопасность информационных технологий. Системный подход. – Киев, Изд-во «Диасофт», 2004, 992 с.
18. Жижелев А.В., Панфилов А.П., Язов Ю.К., Батищев Р.В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Изв. вузов. Приборостроение. 2003. т. 46, №7. С. 22-29.
19. Зегжда Д.П., Мешков А.В., Семьянов П.В., Шведов Д.В. Как противостоять вирусной атаке. – СПб.: BHV, 1995.

20. Зегжда П.Д., Зегжда Д.П., Семьянов П.В., Корт С.С., Кузьмич В.М., Медведовский И.Д., Ивашко А.М., Баранов А.П. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996.
21. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: Изд-во БХВ-Петербург, 2003.
22. Ивахненко А.Г., Ивахненко Г.А., Савченко Е.А., Гергей Т. Самоорганизация дважды многорядных нейронных сетей для фильтрации помех и оценки неизвестных аргументов // Нейрокомпьютеры: разработка и применение. 2001, №12.
23. Ивахненко А.Г. и др. Нейрокомпьютеры в информационных и экспертных системах // Нейрокомпьютеры: разработка и применение. 2003, №2.
24. Игнатьев М.Б., Фильчаков В.В., Осовецкий Л.Г. Активные методы обеспечения надёжности алгоритмов и программ. – СПб.: Политехника, 1992.
25. Карпычев В.Ю., Минаев В.А. Цена информационной безопасности // Системы безопасности. 2003, №5. С.128-130.
26. Касперски К. Атака на Windows NT. Вкладка «Обзор антивирусных средств от AIDSTEST до информационной иммунной системы» // LAN / Журнал сетевых решений. 2000, декабрь, С. 88-95.
27. Кеммерер Р., Виджна Дж. Обнаружение вторжений: краткая история и обзор // Открытые системы. 2002, №7-8.
28. Коврига С.В. Методические и аналитические основы когнитивного подхода к SWOT-анализу // Проблемы управления, 2005, №5. − с. 58-63.
29. Коржов В. Автоматизация безопасности // Computerworld Россия. 2004, №17 – 18. с. 53.
30. Корнеев В.В., Васютин С.В. Самоорганизующийся иерархический коллектив экспертов // Нейрокомпьютеры: разработка и применение. 2003, № 2.

31. Корноушенко Е.К., Максимов В.И. Управление процессами в слабо формализованных средах при стабилизации графовых моделей среды // Труды ИПУ РАН: Сб. науч. Тр. – М.: ИПУ РАН, 1999. – т.2. – с. 82–94.
32. Котенко И.В, Степашкин М.В. Интеллектуальная система моделирования атак на web-сервер для анализа уязвимостей компьютерных систем // Сб. докл. VI Международной конф. по мягким вычислениям и измерениям SCM’2003. – СПб.: СПГЭТУ, 2003. т. 1. С. 298-301.
33. Котенко И.В. Модели противоборства команд агентов по реализации и защите от распределённых атак «Отказ в обслуживании» // Тр. междунар. научно-технич. конф. IEEE AIS’03 и CAD-2003. – М.: Физматлит, 2003. т.1. С. 422-428.
34. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – 2-е изд., стереотип. – М.: Горячая линия-Телеком, 2002.
35. Кузнецова В.Л., Раков М.А. Самоорганизация в технических системах. – Киев: Наук. думка, 1987.
36. Кулик С.Д. Биометрические системы идентификации личности для автоматизированных фактографических информационно-поисковых систем // Нейрокомпьютеры: разработка и применение. 2003, № 12.
37. Курило А. П., Зефиров С. Л., Голованов В. Б. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
38. Липаев В.В., Филинов Е.Н. Мобильность программ и данных в открытых информационных системах, М.,1997.
39. Лобашев М.Е. Генетика. – Л.: Изд-во ленинградского университета, 1969.
40. Логинов В.А. Методика активного аудита действий субъектов доступа в корпоративных вычислительных сетях на основе аппарата нечётких множеств // Сб. докл. VI Междунар. конф. SCM’2003. – СПб.: СПГЭТУ, 2003. т.1. С. 240-243.
41. Лукацкий А. В. Обнаружение атак. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 608 с.

42. Макаревич О.Б., Федоров В.М., Тумоян Е.П. Применение сетей функций радиального базиса для текстонезависимой идентификации диктора // Нейрокомпьютеры: разработка и применение. 2001, №7-8.
43. Максимов В.И., Корноушенко Е.К. Аналитические основы применения когнитивного подхода при решении слабо структурированных задач // Труды ИПУ РАН. – М.: 1999. – Т. 2. – с. 95-109.
44. Медведовский И.Д., Платонов В.В., Семьянинов П.В. Атака через Интернет. – СПб.: НПО Мир и семья, 1997.
45. Милославская Н.Г., Тимофеев Ю.А., Толстой А.И. Уязвимость и методы защиты в глобальной сети Internet. – М.: МИФИ, 1997.
46. Нейроинформатика // А.Н.Горбань, В.Л. Дунин-Барковский, А.Н. Кирдин и др. – Новосибирск: Наука. Сиб. отд., 1998.
47. Нестерук Г.Ф., Осовецкий Л.Г., Нестерук Ф.Г. Адаптивная модель нейро-сетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2003, №3.
48. Норткат С., Новак Дж. Обнаружение вторжений в сеть: Пер. с англ. – М.: Издательство «ЛОРИ», 2001. – 384с.
49. Норткатт С. Анализ типовых нарушений безопасности в сетях. М.: Издательский дом «Вильямс», 2001.
50. Осипов В.Ю. Концептуальные положения программного подавления вычислительных систем // Защита информации. Конфидент. 2002. №4-5. С. 89-93.
51. Осовецкий Л., Шевченко В. Оценка защищённости сетей и систем // Экспресс электроника. 2002. №2-3. С.20-24.
52. Пантелеев С.В. Решение задач идентификации динамических объектов с использование нейронных сетей // Сб. докл. VI Международной конф. SCM’2003. – СПб.: СПГЭТУ, 2003. т.1. С. 334-336.
53. Петров В.В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия. Диссертация на

соискание учёной степени кандидата технических наук, 05.12.13, Москва, 2004, 199 с.

54. Платов В.В., Петров В.В. Исследование самоподобной структуры телетрафика беспроводной сети // Радиотехнические тетради. М.: ОКБ МЭИ. 2004. №3. С. 58-62.
55. Прангишвили И.В. О методах эффективного управления сложными системами // Тр. 5-ой междунар. конф. “Когнитивный анализ и управление развитием ситуаций” (CASC’2005) / ИПУ РАН. − М.: 2005. – с. 7-15.
56. Решение задач обеспечения информационной безопасности на основе системного анализа и нечёткого когнитивного моделирования. Ажмухамедов И.М. Доступно на http://arxiv.org/ftp/arxiv/papers/1204/1204.3245.pdf (дата обращения: 30.09.2015)
57. Робертс П. Защита на клиенте // Computerworld Россия. 2004, №16. с. 44.
58. Скотт Хокдал Дж. Анализ и диагностика компьютерных сетей: Пер. с англ. – М.: Издательство «ЛОРИ», 2001. – 354с.