Введение

Создание перспективных систем защиты информации (СЗИ) в последнее время отождествляют с использованием интеллектуальных средств, таких как: экспертные системы (ЭС), системы нечеткой логики (НЛ), нейронные сети (НС), генетические алгоритмы (ГА), реализующих в СЗИ эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности (ИБ) в виде доступной для анализа системы нечетких правил If-Then.

Лабораторные работы преследуют цель ознакомления с процессом проектирования адаптивных СЗИ на основе ЭС, НЛ, нейронных и нейро-нечетких (ННС) сетей, а также с многоцелевой программной средой «Neuro-Fuzzy», позволяющей сформировать базу знаний эксперта ИБ в виде системы продукционных правил, отразить базу знаний в структуре ННС, обучить ННС в соответствии с выбранным алгоритмом обучения нейронных сетей (например, по методу обратного распространения ошибок или генетических алгоритмов), проанализировать результаты обучения и откорректировать исходную базу знаний. Программная среда «Neuro-Fuzzy» разработана при участии студентов каф. БИТ Доскача В. О., Инюшина И. М. и Леонтьева Р. В.

1. Теоретическая часть

В научно-технической литературе значительное внимание уделено применению интеллектуальных средств в организации систем защиты информации (СЗИ) компьютерных сетей (КС) [1],[2]. Исследуется возможность использования, как отдельных интеллектуальных средств [3],[4], так и их комбинаций [5],[6] для обеспечения безопасности КС в условиях высокой динамики угроз [7].

---

[1] *Ryan J., Lin M., Miikkulainen R.* Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAIWorkshop (Providence, Rhode Island), pp. 72-79. Menlo Park, CA: AAAI. 1997.

[2] *Гриднев В.А., Харитонов А.Ю*. Активный аудит субъектов доступа по их информационному профилю в вычислительных сетях // SCM'2005: Сб. докл. Междунар. конф. Т.1. - СПб: СПбГЭТУ «ЛЭТИ», 2005. С. 229 – 234.

[3] *Пантелеев С. В*. Решение задач идентификации динамических объектов с использование нейронных сетей // SCM'2003: Сб. докл. VI Междунар. Конф. – СПб.: СПГЭТУ, 2003. т. 1. С. 334 - 336.

[4] *Бочков М. В., Крупский С. А., Саенко И. Б*. Применение генетических алгоритмов оптимизации в задачах информационного противодействия сетевым атакам // Сб. докл. Всерос. научн. конф. Управление и информационные технологии. Т. 2. СПб.: ЛЭТИ, 2003. – С.13 - 16.

[5] *Gallant S.I*. Neural Network learning and Expert Systems. MIT Press, Cambridge, MA, 1993.

[6] *Бочков М. В*. Реализация методов обнаружения программных атак и противодействия программному подавлению в компьютерных сетях на основе нейронных сетей и генетических алгоритмов оптимизации // SCM'2003: Сб. докл. VI Междунар. конф – СПб.: СПГЭТУ, 2003. т. 1. С. 376 - 378.

[7] *Нестерук Г. Ф., Осовецкий Л. Г., Харченко А. Ф*. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов. (Иммунология систем информационных технологий). – СПб.: Изд-во СПбГУЭФ, 2003.

Известные интеллектуальные средства, применяемые в КС, основаны на принципе подобия реализуемых функций аналогичным функциям биологических систем [8]. К часто используемым в КС интеллектуальным средствам относят базы знаний в составе экспертных систем [9], системы на основе байесовского метода [10], нечеткие логические системы [11],[12] а также нейронные сети [13],[14] эволюционные методы (ЭМ) [15] и гибридные интеллектуальные системы [16], [17],[18].

1.1. Интеллектуальные средства для решения задач классификации в СЗИ

Классификация и кластеризация являются основными задачами, решаемыми интеллектуальными средствами обеспечения ИБ компьютерной сети в условиях динамики внешнего окружения, т. к. необходим постоянный мониторинг уязвимостей КС и поля угроз [19],[20]. Известные средства обеспечения ИБ, такие как: детекторы уязвимостей, детекторы вторжений, антивирусное ПО, межсетевые экраны в обязательном порядке решают задачу классификации входных событий, в простейшем случае, отнесения входных векторов к классу опасных или безопасных, а также задачу кластеризации в случае необходимости расширения классификационных групп входных событий [21].

---

[8] *Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г.* О применении нейро-нечетких сетей в адаптивных системах информационной защиты // Нейроинформатика-2005: Матер. VII всерос. научно-техн. конф. – М.: МИФИ (ТУ), 2005. Ч.1. С. 163 - 171.

[9] *Waterman D.A*. A Guide to Expert Systems. - MA: Addison-Wesley, Reading. 1986.

[10] *Прокопчина С. В*. Байесовские интеллектуальные технологии для аудита и управления сложными объектами в условиях значительной неопределенности // SCM'2002: Сб. докл. VI Междунар. конф. - СПб, 2002. т.1, С. 27 - 31.

[11] *Zadeh L.A., Kacprzyk, J*. Fuzzy Logic for the Management of Uncertainty. – NY: John Wiley. 1992.

[12] *Li H., Gupta M*. Fuzzy Logic and Intelligent Systems. – Boston: Kluwer Academic Publishers. 1995.

[13] *Fu L.M*. Neural Networks in Computer Intelligence. - McGraw-Hill Book, Inc. 1994.

[14] *Круглов В. В., Борисов В. В*. Искусственные нейронные сети. Теория и практика.- 2-е изд. – М.: Горячая линия - Телеком, 2002.

[15] *Davis L*. Handbook on Genetic Algorithms. – NY: Van Nostrand Reinhold. 1991.

[16] *Negnevitsky M*. Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.

[17] *Fuller R*. Neural Fuzzy Systems. - Abo: Abo Akademi University, 1995.

[18] *Рутковская Д., Пилиньский М., Рутковский Л*. Нейронные сети, генетические алгоритмы и нечеткие системы. - М.: Горячая линия –Телеком, 2004.

[19] *Степашкин М. В., Котенко И. В*. Классификация атак на Web-сервер // VIII Санкт-Петерб. междунар. конф. "Региональная информатика-2002": Материалы конференции. Ч. 1. СПб., 2002.

[20] *Нестерук Г. Ф., Молдовян А. А., Костин А. А., Нестерук Ф. Г., Воскресенский С. И*. Организация иерархической защиты информации на основе интеллектуальных средств нейро-нечеткой классификации // Вопросы защиты информации. 2005, № 3. С.16 – 26.

[21] *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.

Задачи классификации в ЭС

Правила как метод представления знаний

Каждое правило состоит из двух частей: часть ЕСЛИ (IF), называемая посылкой или условием, и часть ТО (THEN), называемая заключением.

IF < **посылка**> **THEN** <**заключение**>

Правила могут содержать одну или несколько посылок.

Конъюнктивные правила (conjunction) - правила «И» или «AND» требуют *одновременного* выполнения всех посылок.

IF < посылка 1> AND < посылка 2> …AND < посылка *n*>

THEN < заключение >

Дизъюнктивные правила (disjunction) - правила «ИЛИ» или «OR» требуют выполнения хотя бы одной из посылок.

IF < посылка 1> OR < посылка 2>…OR < посылка *n*>

THEN < заключение >

Часть «THEN» может содержать несколько заключений:

IF < посылка >

THEN < заключение 1> < заключение 2>…< заключение *m*>

Посылка содержит две части: лингвистический объект и его значение (характеристика). Заключение содержит оператор, объединяющий объект и значение его характеристики.

На рис 1 представлена модель системы логического вывода, основанная на процессе рассуждения, аналогичному человеческому[22]. Знания, представленные в виде системы правил логического вывода, хранятся в долговременной памяти. Оперативная информация в виде фактов размещается в оперативной памяти. В процессе рассуждения (reasoning) происходит подстановка фактов в качестве посылок в части «IF» правил. Если правило выполнено, то формируется заключение (conclusion).

Основанная на системе правил экспертная система состоит из базы знаний (knowledge base), базы данных (database), механизма логического вывода (inference engine), средств объяснения результатов (explanation facilities) и удобного пользовательского интерфейса (user interface).

Так как знания в экспертной системе организованы в виде системы правил вида: **IF** <**условие> THEN** <**следствие>**, то система логического вывода осуществляет сравнение данных из информационной базы с полем **условие** базы

[22] *Newell, A. and Simon, H.A*. (1972). *Human Problem Solving.* Prentice Hall, Englewood Cliffs, NJ.

знаний и в случае четкого совпадения активизируется заданные полем **следствие** действия.

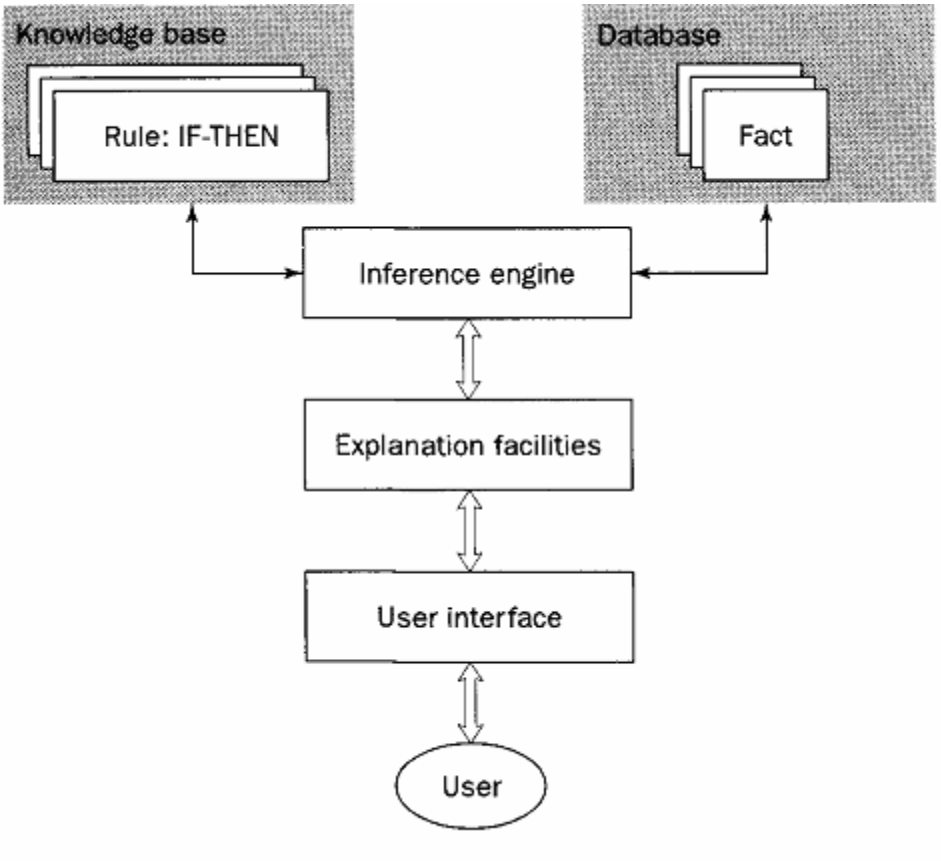

Рис.1

Результаты работы экспертной системы доступны пользователю через диалоговый интерфейс, который позволяет ознакомиться также с ходом логических «рассуждений» системы, повлекших получение данного результата.

Как специализированная система, ЭС предназначена для решения классификационных задач в узкой предметной области исходя из базы знаний, сформированной путем опроса квалифицированных специалистов и представленной системой классификационных правил If-Then. В СЗИ компьютерных сетей используется модель Деннинга [23], основанная на базах знаний экспертной системы, которая содержит систему классификационных правил, соответствующих профилям легальных пользователей КС, сценариям атак на компьютерную сеть [24, 25].

К недостаткам ЭС как средствам решения задач классификации относят:

---

[23] *Denning D. E.* An intrusion detection model // IEEE Trans. on Software Engineering, 1987, SE-13. P. 222–232.

[24] *Porras P. A., Ilgun K.,* and *Kemmerer R. A*. State transition analysis: A rule-based intrusion detection approach. // IEEE Trans. on Software Engineering, 1995. SE-21. P. 181–199.

[25] *Garvey T. D. Lunt T. F*. Model-based intrusion detection // Proc. of the 14th National Computer Security Conference. 1991.

- *Непрозрачность связей* между правилами в базе знаний. Отдельные правила If-Then относительно просты и логически прозрачны, а наглядность их логической взаимосвязи в пределах базы знаний м. б. достаточно низкой. То есть непросто определить противоречивые правила в базе знаний и их роль в решении классификационной задачи.

- *Неэффективная стратегия поиска*. Экспертные системы с большой базой знаний могут оказаться недостаточно производительными для решения оперативных задач обеспечения безопасности компьютерных сетей в реальном масштабе времени.

- *Отсутствие возможности адаптации*. ЭС не обладают способностью к обучению, не могут автоматически изменять базу знаний: корректировать существующие правила или добавлять новые правила If-Then.

Вероятностные методы решения задачи классификации.

Методы недостоверного управления и вероятностных рассуждений применяются в ЭС не только для формирования классификационных заключений в соответствии с правилами If-Then, но и для оценки достоверности проведенной классификации в виде значений фактора уверенности или условной вероятности возникновения события [26].

Возможность оценки достоверности предсказания является существенным достоинством метода вероятностных рассуждений Байеса, т. к. базируется на строгом математическом аппарате теории вероятностей. Примерами практического применения вероятностных рассуждений при решении задач классификации являются ЭС для геологоразведки и управления сложными системами [27],[28].

Факторы уверенности в ЭС

Факторы уверенности – это значение дополнительной экспертной оценки для каждого из правил базы знаний ЭС, которые представляются в виде

IF < **факт** > **THEN** < **гипотеза** > {***cf***},

где *cf* определяет степень доверия к гипотезе *H* (hypothesis) в случае наступления факта *E* (evidence).

---

[26] *Negneyitsky M*. Artificial intelligence : a guide to intelligent systems. Addison-Wesley, 2002 – 394 p.

[27] *Duda R., Gaschnig J. Hart P*. Model design in the PROSPECTOR consultant system for mineral exploration. Expert Systems in the Microelectronic Age / D. Michie, ed. - Edinburgh, Scotland: Edinburgh University Press, 1979. P. 153-167.

[28] *Прокопчина С. В*. Байесовские интеллектуальные технологии для аудита и управления сложными объектами в условиях значительной неопределенности // SCM'2002: Сб. докл. VI Междунар. конф. - СПб, 2002. т.1, С. 27 - 31.

Теория факторов уверенности основана на двух функциях: мере доверия *MB*(*H,E*) и мере недоверия *MD* (*H, E*). Эти функции указывают, соответственно, степень увеличения доверия к гипотезе *H*, если факт *E* произошел, и степень увеличения недоверия к гипотезе *H*, если факт *E* имел место[29].

Мера доверия и недоверия могут быть определена в терминах априорной и условной вероятностей следующим образом:

$$MB(H,E) = \begin{cases} 1 & \text{if } p(H) = 1 \\ \dfrac{max\,[p(H|E), p(H)] - p(H)}{max\,[1,0] - p(H)} & \text{otherwise} \end{cases}$$

$$MD(H,E) = \begin{cases} 1 & \text{if } p(H) = 0 \\ \dfrac{min\,[p(H|E), p(H)] - p(H)}{min\,[1,0] - p(H)} & \text{otherwise} \end{cases}$$

где: $p(H)$ – априорная вероятность, что гипотеза *H* является истинной;

$p(H|E)$ – условная вероятность, что гипотеза Н является истинной при наступлении факта *E*.

Значения *MB*(*H,E*) и *MD* (*H, E*) располагаются между 0 и 1. Мера доверия и недоверия к гипотезе *H* зависит от вида факта *E*. Некоторые факты могут увеличивать меру доверия, а некоторые - увеличивать меру недоверия. Фактор уверенности, certainty factor, рассчитывается, исходя из значений этих мер

$$cf = \frac{MB(H,E) - MD(H,E)}{1 - min\,[MB(H,E), MD(H,E)]}$$

и может изменяться от -1 до +1, определяя степень доверия к гипотезе *H*.

Практическая значимость метода факторов уверенности для решения задачи классификации подтверждена разработкой ряда экспертных систем и, прежде всего, ЭС для целей медицинской диагностики [28]. Последний подход к классификации более приемлем с точки зрения вычислительной эффективности, т. к. не требует наличия больших объемов статистических данных и сложных расчетов условных вероятностей при большой размерности пространства входных посылок.

Численная оценка классификационных заключений особенно важна в условиях неполноты и низкой достоверности входных признаков, используемых в качестве посылок большинством существующих систем классификации вторжений в компьютерные сети.

---

[29] *Negnevitsky M.* Artificial intelligence : a guide to intelligent systems. Addison-Wesley, 2002 – 394 p.

Задачи нечеткой классификации

Нечеткая классификация является развитием подхода экспертных систем. Основное отличие и достоинство нечеткой классификации – это возможность формулирования достоверных классификационных заключений исходя из неполных и не вполне достоверных входных посылок.

При сохранении математического аппарата, разработанного для систем четкой логики, в нечетких логических системах решена задача преобразования численной и качественной информации в степень принадлежности значений конкретным нечетким множествам (НМ) [30]. НМ описываются посредством функций принадлежности, ставящих в соответствие множеству значений из области определения непрерывной переменной множество значений истинности из интервала [0, 1].

Основные этапы нечеткого логического вывода связаны с процессом формирования классификационных заключений [31]:

1) этап *введения нечеткости* связан с преобразованием посредством входных функций принадлежности каждого из четких входных значений x_i , i = 1, …, , n – число входных значений в истинность соответствующей посылки μ_{xi}, $i = 1,...,n$ для каждого из классификационных правил;

2) этап *логического вывода* соответствует формированию заключения (нечеткого подмножества) по каждому правилу $\mu_{Ri}, i = 1,...,m$, m – количество классификационных правил, исходя из истинности посылок μ_{xi}, $i = 1,...,n$;

3) этап *композиции* нечетких подмножеств позволяет формировать нечеткие подмножества классификационных заключений μ_{Ci}, $i = 1,...,p$, p – число выходов классификатора по правилам μ_{Ri}, $i = 1,...,m$ посредством выходных функций принадлежности;

4) этап *объединения* нечетких подмножеств μ_{Ci}, $i = 1,...,p$ и приведение к четкости приводит к формированию выходного четкого значения y.

По аналогии с ЭС нечеткие логические системы основаны на базе знаний квалифицированных специалистов ИБ в виде системы правил If-Then. Однако существенно расширяют область применения ЭС за счет возможности решения задачи классификации исходя из не вполне достоверных данных и качественной информации.

Системы НЛ обладают возможностями к адаптации, т. к. могут обучаться путем изменения параметров функций принадлежности под реальные значения входных данных и желаемые классификационные заключения. Стоит отметить,

---

[30] *Zadeh L.A., Kacprzyk, J.* Fuzzy Logic for the Management of Uncertainty. – NY: John Wiley. 1992.
[31] *Fuller R.* Neural Fuzzy Systems. - Abo: Abo Akademi University, 1995.

что обучение функций принадлежности нечеткой ЭС с большой базой знаний является трудоемким процессом, требующим значительных затрат времени.

Применение НС в задачах классификации и кластеризации

Наиболее обучаемым интеллектуальным средством для решения задач классификации являются нейронные сети [32]. Доказано, что НС является универсальным аппроксиматором, т. е. любая функция представима в виде многослойной нейронной сети из формальных нейронов (ФН) с нелинейной функцией активации [33].

Формально подтверждена верхняя граница сложности НС, реализующей произвольную непрерывную функцию от нескольких аргументов. Нейронной сетью с одним скрытым слоем и прямыми полными связями можно представить любую непрерывную функцию, для чего достаточно в случае n-мерного входного вектора $2n+1$ ФН скрытого слоя с заранее оговоренными ограниченными функциями активации [34].

Известны многочисленные случаи использования нейросетевых средств для обеспечения безопасности компьютерных сетей, причем большинство случаев связано с решением задач классификации кластеризации. Следует обратить внимание, что из всех рассмотренных ранее интеллектуальных средств НС обдают свойством самоорганизации [35], что позволяет использовать их для решения задачи кластеризации [36].

Возможность самоорганизации рассматривается как одно из наиболее важных качеств нейросетевых СЗИ, которое позволяет адаптироваться к изменению входной информации. Обучающим фактором выступают присутствующие в данных скрытые закономерности и избыточность входной информации. Самоорганизация НС реализуется за счет механизма кластеризации: подобные входные данные группируются нейронной сетью в соответствии с взаимной корреляцией и представляются конкретным ФН-прототипом.

Механизмы классификации и кластеризации входных данных в СЗИ позволяют не только относить классифицируемый объект (вектор входных данных) к одному из известных классов, но и реализовать эволюционные процессы самоорганизации, адаптации, развития в интеллектуальных средствах обеспечения

---

[32] *Negnevitsky M*. Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.
[33] Нейроинформатика. / *А. Н. Горбань, В. Л. Дунин-Барковский, А. Н. Кирдин* и др. - Новосибирск: Наука. Сиб. отд., 1998.
[34] *Hecht-Nielsen R*. Kolmogorov's Mapping Neural Network Existence Theorem // IEEE First Annual Int. Conf. on Neural Networks, San Diego, 1987, V. 3, P. 11-13.
[35] *Джейн А. К., Мао Ж., Моиуддин К М*. Введение в искусственные нейронные сети // Открытые системы. 1997. № 4. С.16-24.
[36] *Уоссермен Ф*. Нейрокомпьютерная техника: Теория и практика. - М.: Мир, 1992.

ИБ компьютерных сетей. Причем лучшие функциональные характеристики получаются при сочетании различных интеллектуальных средств в гибридной системе защиты информации.

1.2. Гибридные средства классификации в СЗИ

В гибридных средствах классификации на основе нейронных сетей сочетаются достоинства объединяемых интеллектуальных подходов. Недостатком нейронных сетей, не позволяющим анализировать процесс формирования классификационных заключений, считается не вполне «прозрачное» с точки зрения администратора безопасности представление знаний в информационном поле НС. Для устранения отмеченного недостатка целесообразно сочетание НС с системами нечеткой логики либо экспертными системами. Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет явным образом отразить в структуре нейронных сетей систему нечетких правил вывода, которые автоматически корректируются в процессе обучения НС.

Нейро-экспертные системы в задачах классификации

Нейронные сети и экспертные системы различаются по способам представления и обработки информации.

НС ориентированы на распределенную параллельную обработку данных, процесс решения задачи логически «не прозрачен», а накопленные в процессе обучения знания распределены по информационному полю НС, что затрудняет объяснение их конкретного местоположения и делает трудновыполнимым отражение в информационное поле НС априорного опыта квалифицированных специалистов информационной безопасности. Опыт в экспертных системах представляется в «прозрачной» для пользователя систем правил IF-THEN, а процесс логического вывода сходен с характером человеческих рассуждений.

НС обладают свойством адаптивности, причем сам процесс обучения достаточно прост и формализуем. В то же время задача приобретения знаний экспертными системами в значительной мере трудоемка, т. к. основана на создании непротиворечивой системы правил логического вывода, основанной на личном опыте отдельных экспертов [37]. Кроме того, ориентированная на достоверные данные ЭС не обладает гибкостью и элементами самоорганизации.

Нейро-экспертная система (рис. 2) имеет организацию, аналогичную структуре ЭС. Однако база знаний нейро-экспертной системы (neural knowledge base)

---

[37] *Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В*. Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2001.

организована в форме адаптивного распределенного информационного поля НС.

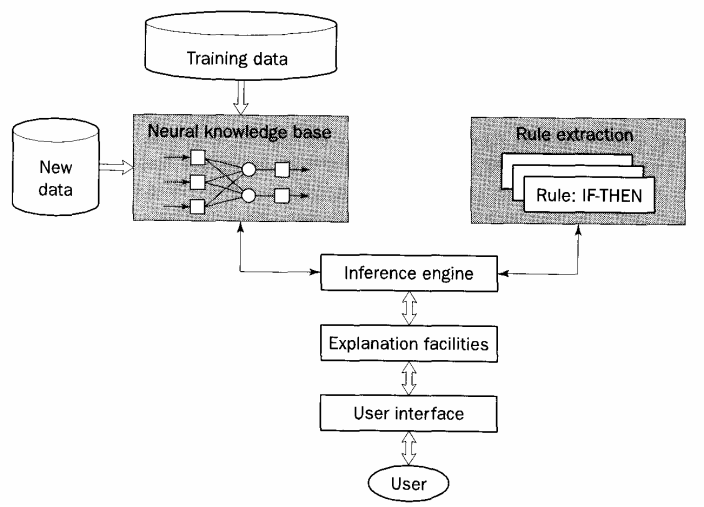

Рис. 2.

Использование нейросетевой базы знаний позволяет устранить основные недостатки основанных на правилах ЭС: невозможность оперирования с не вполне достоверной информацией и трудоемкость адаптации базы знаний. Нейросетевая база знаний корректирует зашумленную или искаженную входную информацию (new data), что эквивалентно активации в правиле If-Then процесса формирования заключения даже в случае неполного выполнения условий в части If правила. Активация нейросетевой базы знаний аналогична извлечению знаний, соответствующих правилу If-Then (rule extraction), из информационного поля НС. Блок логического вывода (inference engine) оперирует нечеткими рассуждениями исходя из потока данных в нейро-экспертной системе.

Нейро-нечеткие методы классификации

Объединение возможностей НС и систем НЛ является перспективным подходом к организации интеллектуальных средств защиты информации. Системы НЛ компенсируют основные «непрозрачности» НС в представлении знаний и объяснении результатов работы интеллектуальной системы. Нечеткая логика позволяет формализовать качественную информацию, полученную от экспертов информационной безопасности, использовать ее в процессе рассуждений в качестве посылок для системы правил, позволяющих анализировать результаты работы системы.

Механизм нечеткого логического вывода используется при описании базы знаний, формируемой экспертами ИБ, в виде системы правил (rules) нейро-нечеткой классификации, например:

$$R_1: \text{если } \tilde{x}1 \text{ есть } S \text{ и } \tilde{x}2 \text{ есть } S, \text{ то } \tilde{y} = L,$$
$$\mathrm{R}_2: \text{если } \tilde{x}1 \text{ есть } S \text{ и } \tilde{x}2 \text{ есть } L, \text{ то } \tilde{y} = S,$$
$$\mathrm{R}_3: \text{если } \tilde{x}1 \text{ есть } L \text{ и } \tilde{x}2 \text{ есть } S, \text{ то } \tilde{y} = S,$$
$$\mathrm{R}_4: \text{если } \tilde{x}1 \text{ есть } L \text{ и } \tilde{x}2 \text{ есть } L, \text{ то } \tilde{y} = L.$$

где $\tilde{x}_i$ и $\tilde{y}_j$ - нечеткие входные и выходная переменные, а L - «большая» (Large) и S - «малая» (Small) - входные и выходные функции принадлежности.

Нейро-нечеткий классификатор - это НС (рис. 3), которая является адаптивным функциональным эквивалентом нечеткой модели вывода. Специализация описания выражается в формировании системы нечетких правил, представляющих процедуру получения заключений на заданном множестве посылок. Специализация нейросетевой реализации классификатора (рис. 3) проявляется в функциональной разнородности слоев формальных нейронов (ФН).

Нейронные сети дают возможность отобразить алгоритмы нечеткого логического вывода в структуре нейро-нечеткого классификатора, фиксируя в информационном поле НС априорную информацию, которая в процессе предэксплуатационного обучения может корректироваться.

Адаптивность нейро-нечетких классификаторов позволяет решать не только задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, но и автоматически формировать новые правила при изменении поля угроз информационной безопасности компьютерной сети.

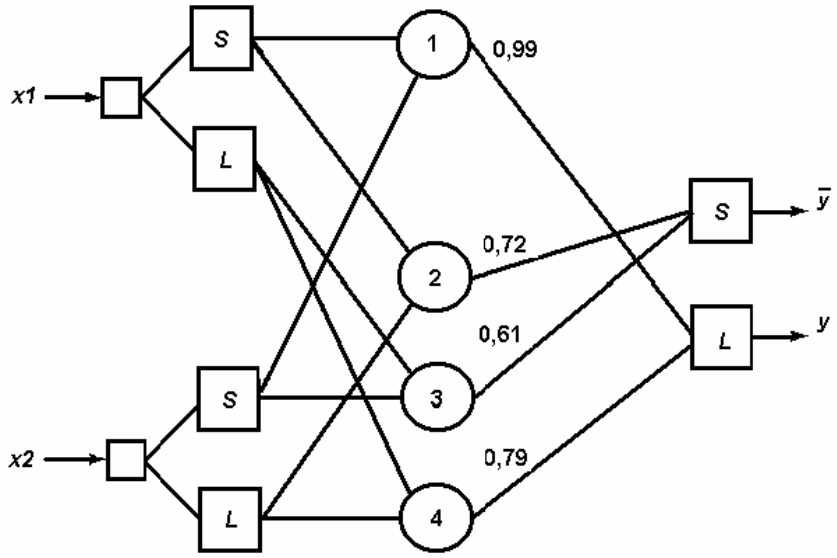

Рис. 3.

Как и в случае нейро-экспертных систем необходима коррекция информационного поля НС путем предэксплуатационного обучения.

Знания квалифицированных специалистов ИБ, представленные в форме нечетких правил логического вывода, могут быть отражены в структуре нейро-нечеткого классификатора. Последующее обучение классификатора позволяет настроить веса связей (т. е. откорректировать достоверность отдельных правил) и устранить противоречивость системы правил в целом.

Основным недостатком нейро-нечетких классификаторов является низкая избыточность информационных полей, что негативно сказывается на функциональной устойчивости средств защиты к дестабилизирующим воздействиям. Известны подходы введения избыточности в информационные поля НС, связанные с комплементарностью представления и дублированием информации [38], а также использованием информации о состоянии СЗИ [39]. Поэтому следует обратить внимание на пути введения избыточности в информационные поля нейро-нечетких классификаторов.

Комплементарность представления информации при решении задачи классификации

Введение избыточности в информационные поля нейро-нечеткого классификатора базируется на механизмах обеспечения защищенности биосистемы [40]:

- представление информации структурированными полями,
- информационная избыточность за счет комплементарного дублирования структурированных информационных полей,
- информационная избыточность, выражающаяся в наличии повторяющихся фрагментов информационного поля.

Избыточность информационного поля обеспечивает возможность для распределенного хранения знаний в структурированных полях нейро-нечеткой сети, а специализация слоев ФН позволяет анализировать результаты обучения информационных полей НС.

В качестве аппарата для формализации преобразований над нечеткими высказываниями можно использовать аналог нормальных форм для в виде дизъюнктивной (ДНФ) и конъюнктивной (КНФ) нормальных форм. То есть правила логического вывода If-Then, описывающие базу знаний экспертов безопасности (процесс формирования классификационных заключений), представляются в виде двух систем правил: конъюнктивной и дизъюнктивной, которые отража-

---

[38] *Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г., Воскресенский С. И., Грибачев В.П.* Информационная избыточность нейро-нечетких средств обеспечения безопасности // Вопросы защиты информации. 2005, № 3. С. 12 – 16.

[39] *Нестерук Г. Ф., Молдовян А. А., Нестерук Ф. Г., Воскресенский С. И., Костин А. А*. Повышение избыточности информационных полей адаптивных классификаторов системы информационной безопасности // Специальная техника. 2006, № 1. С. 60 – 63.

[40] *Лобашев М. Е*. Генетика. – Л.: Изд-во ленинградского университета, 1969.

ются в специализации групп ФН в слое композиции нейро-нечеткого классификатора (рис. 4).

В первую группу включают нечеткие ФН «дизъюнкция», реализующих операцию max над минтермами, во вторую группу – нечеткие ФН «конъюнкция», реализующих операцию min над макстермами. В результате на выходах $L(\tilde{x}_i)$ и $S(\tilde{x}_i)$ первой группы из ФН «дизъюнкция» будет реализовано, соответственно, прямое и инверсное представление системы нечетких классификационных правил, а на выходах $L(\tilde{x}_i)$ и $S(\tilde{x}_i)$ второй группы из ФН «конъюнкция» - соответственно, инверсное и прямое представление системы нечетких классификационных правил.

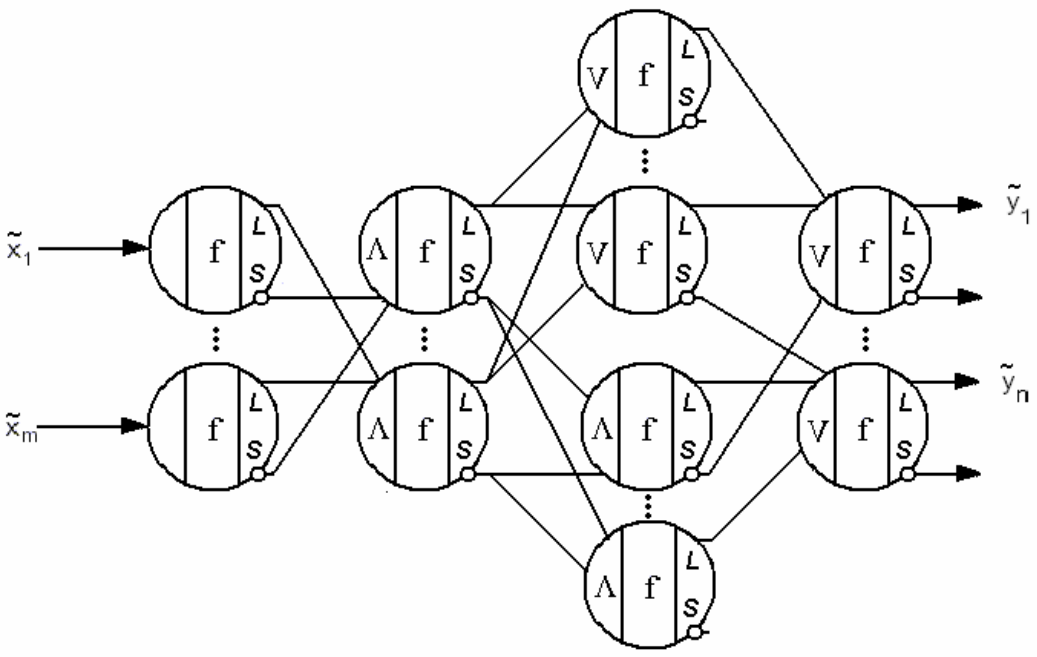

Рис. 4.

Выделение двух групп ФН в слое композиции позволяет объединить на нечетких ФН «дизъюнкция» дополнительного 4-го слоя нейро-нечеткого классификатора одноименные правила реализуемой системы нечетких классификационных правил.

Введение избыточности в информационное поле нейро-нечеткого классификатора позволяет анализировать результаты нейросетевых средств защиты информации.

2. Практическая часть

Многоцелевая программная среда «Neuro-Fuzzy» позволяет ознакомиться с возможностями и провести исследования интеллектуальных средств защиты информации.

2.1. Моделирование адаптивных средств защиты информации

Программные средства моделирования адаптивных средств защиты информации позволяют:

- знания экспертов информационной безопасности отразить в структуре нейронной или нейро-нечеткой сети,
- обучить нейронной или нейро-нечеткую сеть на множестве пар векторов обучающие выборки,
- проанализировать информационное поле нейронной или нейро-нечеткой сети после завершения процесса обучения,
- откорректировать исходную базу знаний экспертов информационной безопасности.

Исходя из базы знаний экспертов информационной безопасности, представленной в виде системы правил нечеткого логического вывода, программные средства автоматически формируют топологию нейро-нечеткого классификатора. То есть база знаний экспертов отражается в структуре нейро-нечеткого классификатора (рис. 5). Узлы В образуют входной слой НС, узлы И – слой логического вывода НС, соответствующий одноименному этапу процедуры нечеткого логического вывода, узлы ИЛИ – слой композиции нейро-нечеткого классификатора.

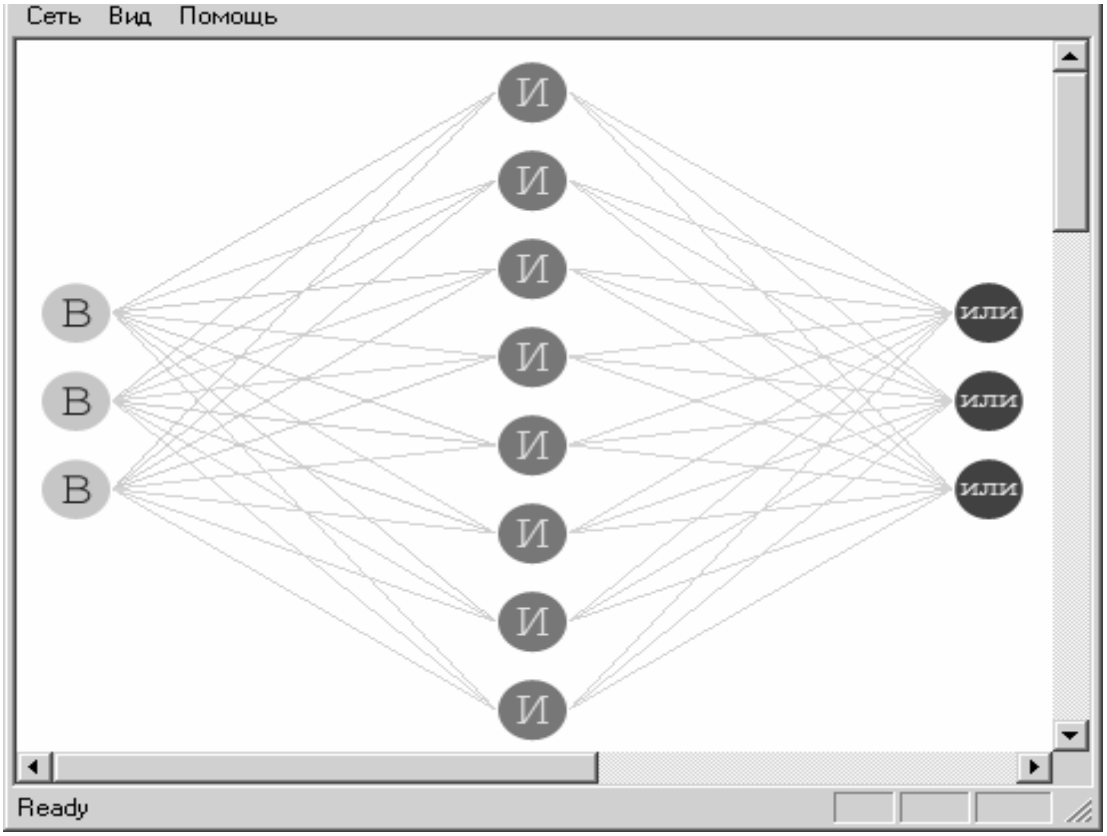

Рис. 5.

Диалоговая среда моделирования адаптивных СЗИ

Диалоговая среда (далее программа) позволяет моделировать работу адаптивных средств защиты, которые в составе модели адаптивной СЗИ используется для решения задач классификации уязвимостей и известных угроз информационной безопасности корпоративной сети.

Программа также позволяет исследовать процессы адаптации структуры адаптивных классификаторов к изменению выявленных уязвимостей и расширению поля угроз.

Диалоговая среда включает три программных модуля: RulesEditor - редактор правил, NeuralNetworkBuilder – программная среда построения нейронных сетей, Forecast – среда исследования процессов адаптации нейронных и нейронечетких сетей.

RulesEditor - редактор правил

Редактор правил позволяет выполнять следующие операции:

- создание нового проекта;
- формирование системы правил;
- редактирование правила;
- смена режима конъюнктивная/дизъюнктивная форма;
- открытие ранее сохраненного проекта;
- быстрое сохранение проекта;
- сохранение проекта под именем;
- закрытие проекта;
- экспортирование результатов.

Создание нового проекта

При активации программы открывается окно (рис. 6), предназначенное для организации пользовательского интерфейса в процессе формирования базы знаний нейросетевого классификатора.

Для создания нового проекта воспользуйтесь опцией меню **Project->Create.** В открывшемся окне **Init** на закладке **Input names** (по умолчанию) введите названия входов, причем имя каждого входа вводится с новой строки (рис. 7). В том же окне на закладке **Output names** введите названия выходов, начиная имя каждого выхода на новой строке (рис. 8).

Рис. 6.

Автоматически формируется шаблон нового правила, аналогичный показанному на рис. 9. В сформированном шаблоне не следует выполнять никаких операций по редактированию.

Рис. 7

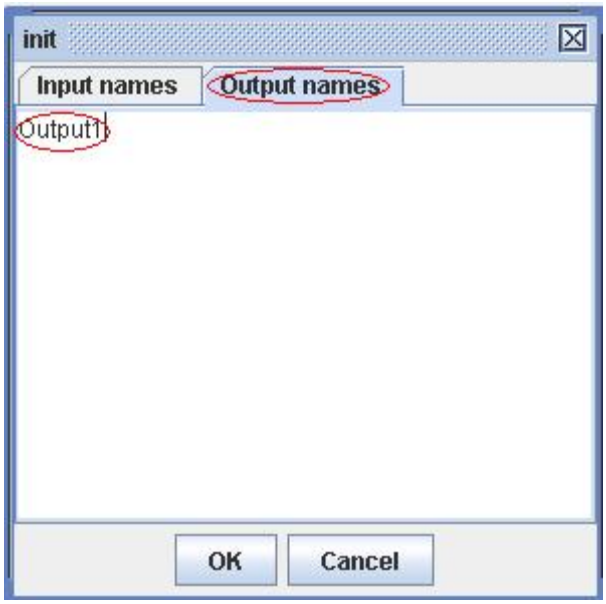

Рис. 8

Рис. 9

Формирование системы правил

Для того чтобы активировать правило, представленное в виде шаблона, следует щелкнуть правой кнопкой мыши на строке с правилом и в выпавшем меню выбрать пункт **Add New Rule** (рис. 10).

Рис. 10

Для формирования необходимого для базы знаний количества правил (рис. 11) следует указанные в предыдущем абзаце действия повторить требуемое число раз.

Если возникла необходимость в удалении одного из правил, то следует щелкнуть правой кнопкой мыши на соответствующей строке системы правил и в выпавшем меню выбрать пункт **Delete Rule** (рис. 12).

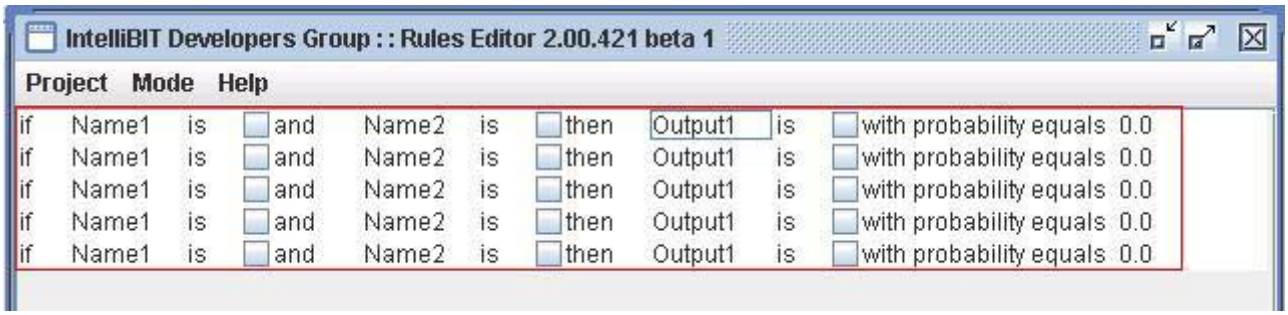

Рис. 11

Рис. 12

Редактирование правила

Для редактирования правила в процессе формирования базы знаний следует задать истинность или ложность условий, образующих часть If правила, а также истинность или ложность заключения (гипотезы) – в части Then правила. С той целью проставляется символ √ - «галочка» в отведенных для этого полях (рис. 13). Проставленная галочка эквивалентна значению входной логической переменной ИСТИНА (TRUE), а отсутствие галочки - значению входной логической переменной ЛОЖЬ (FALSE).

Кроме того, для экспертных систем, использующих метод Байеса или факторов уверенности, следует проставить значение из диапазона от 0 до 1, соответствующее степени доверия к данной гипотезе, в поле, названном «с вероятностью, равной __» (with probability equals__).

Рис. 13

Смена режима КНФ/ДНФ

Для изменения типа правила (конъюнктивное или дизъюнктивное) воспользуйтесь опцией меню **Mode->CNF** или **Mode->DNF** (рис.14). При этом логическая взаимосвязь условий в части If правила будет описываться с помощью логической операции «Дизъюнкция» - OR или логической операции «Конъюнкция» - AND.

Рис. 14

Открытие ранее сохраненного проекта

Открытие проекта, сохраненного в одном из предыдущих сеансов работы с редактором правил, осуществляется с помощью меню **Project->Open** (рис. 15). В открывшемся окне **Open rules project** (рис. 16) следует выбрать конкретный файл проекта с расширением **rpf**.

Рис. 15

Быстрое сохранение проекта или сохранение проекта под именем

Чтобы сохранить базу знаний, сформированную в процессе работы, следует воспользоваться опцией меню **Project->Save** или **Project->Save As** (рис. 17).

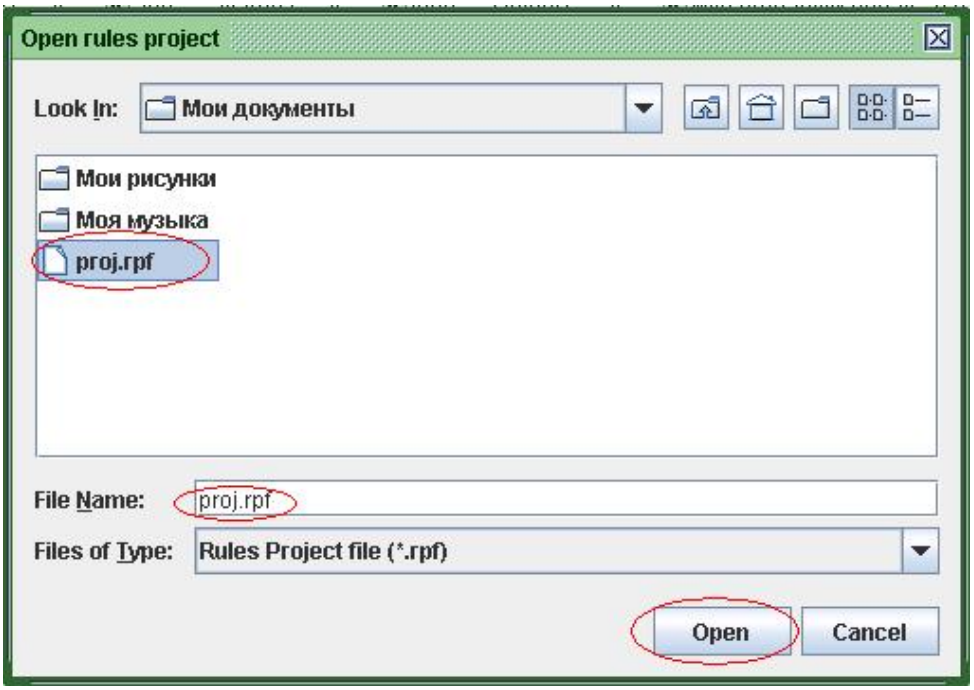

Рис. 16

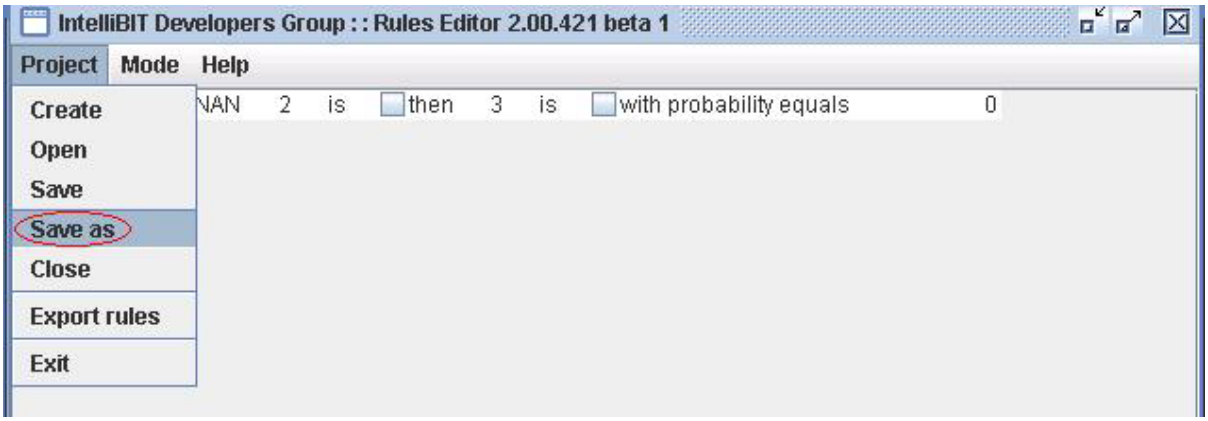

Рис. 17

В появившемся окне следует выбрать папку, задать имя сохраняемому файлу (рис. 18) и нажать кнопку **Save**.

Закрытие проекта

Для того чтобы закрыть проект в процессе работы программы (например, чтобы открыть другой), вам следует воспользоваться пунктом меню **Project->Close** (рис.19).

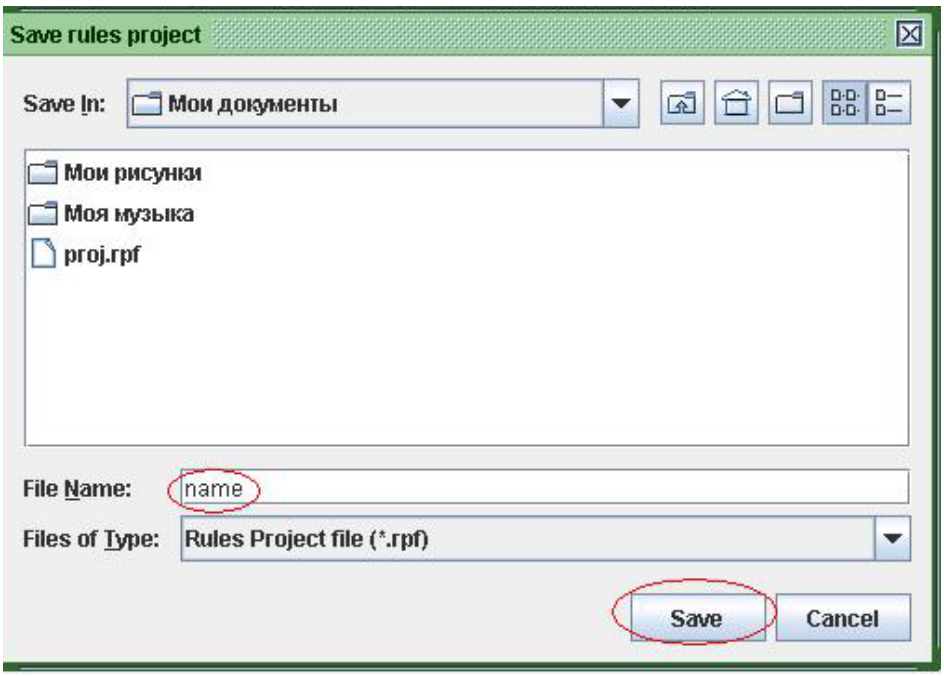

Рис. 18

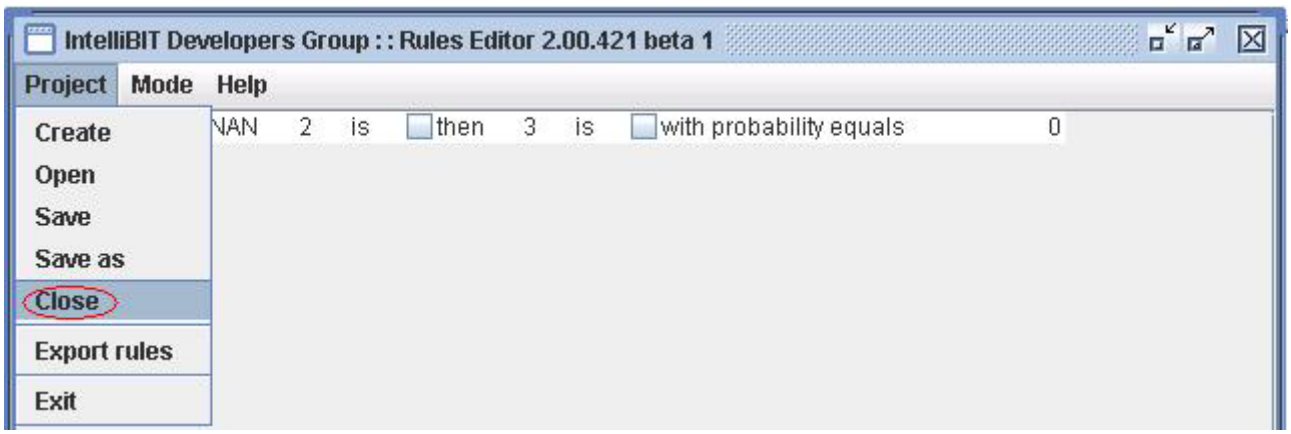

Рис.19

Экспортирование результатов

Для того чтобы экспортировать созданные вами правила в файлы, содержащие структуру нейронной сети и обучающую выборку, вам необходимо воспользоваться опцией меню **Project->Export Rules** (рис.20).

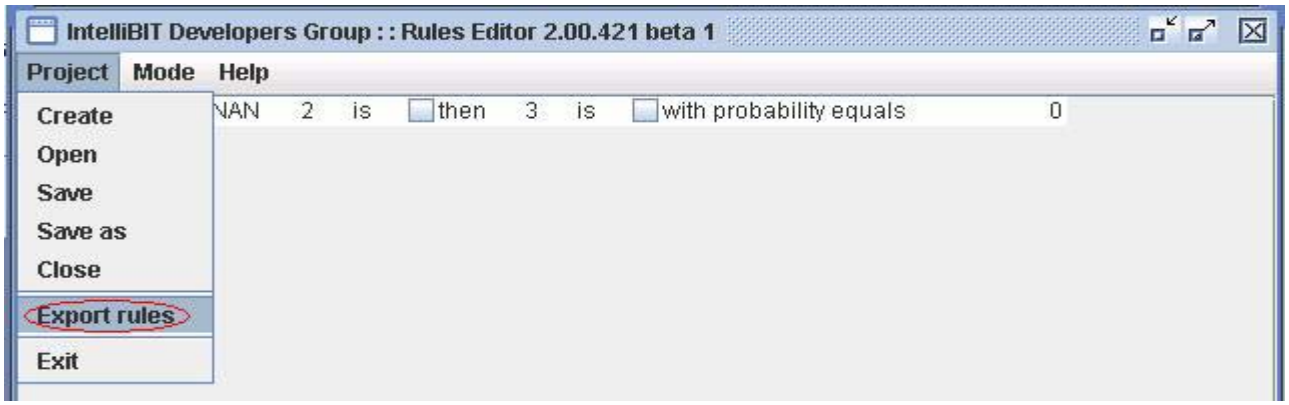

Рис. 20

В открывшемся окне **Export rules** (рис. 21) с помощью кнопок **Browse** необходимо указать пути к файлам, в которых вы хотите сохранить структуру нейронной сети (верхнее поле) и обучающую выборку (нижнее поле).

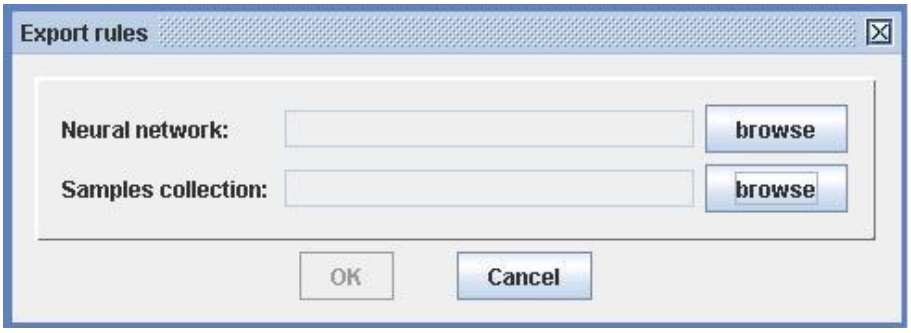

Рис. 21

На рис. 22 и 23 показаны окна сохранения НС и обучающей выборки.

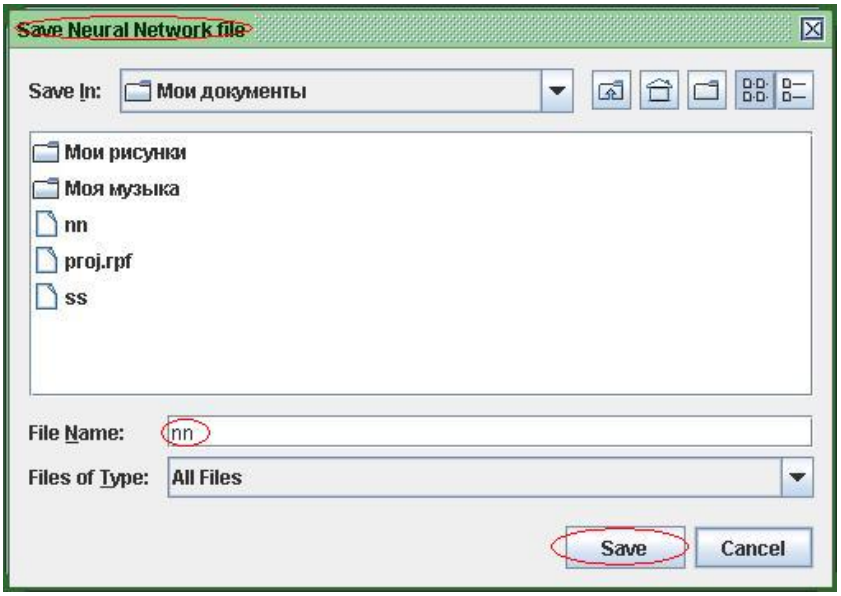

Рис. 22

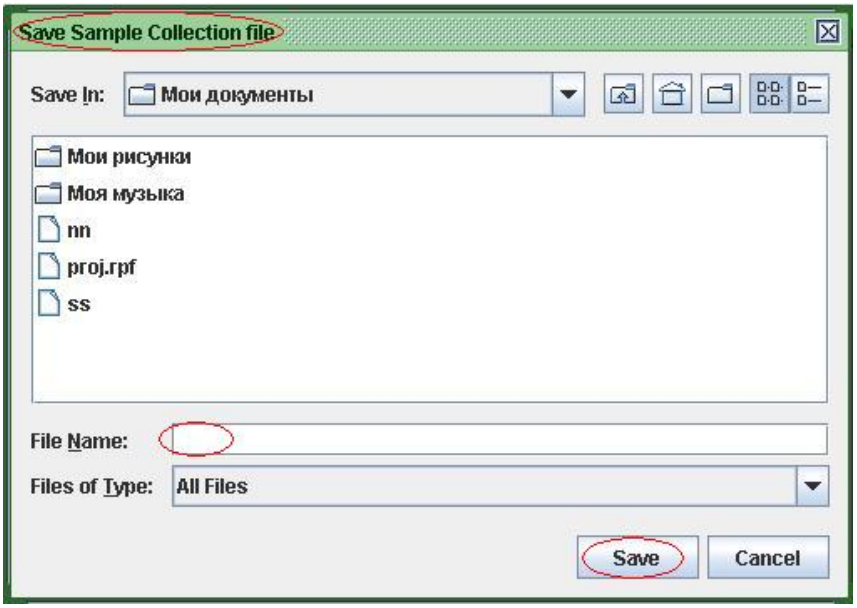

Рис. 23

2.2. Задания на формирование базы знаний для адаптивных средств защиты информации

Задание к лабораторной работе № 1

Исходя из оговоренного в задании поля угроз (табл.1), которые используются в качестве посылок, необходимо сформулировать продукционные правила базы знаний.

Таблица 1

Координаты входного вектора	Посылки для части If продукционных правил – заданный перечень угроз
1	Вирусная атака на ПК
2	Вирусная атака на ЛВС
3	Угрозы целостности информации
4	Угрозы конфиденциальности информации
5	Попытки НСД к информации

В качестве заключений продукционных правил следует использовать заданный перечень используемых механизмов защиты – МЗ (табл. 2)

Таблица 2

Координаты выходного вектора	Заключения для части Then продукционных правил – заданный перечень МЗ
1	Обнаружение вирусной атаки на ПК
2	Обнаружение вирусной атаки на ЛВС
3	Обнаружение искажения программ и данных
4	Криптографическая защита информации на носителях
5	Криптографическая защита информации в сетях передачи данных
6	Парольная защита
7	Управление полномочиями пользователей
8	Учет работы пользователей

То есть необходимо описать системой продукционных правил соответствие каждого из восьми механизмов защиты пяти типам заданных угроз.

1. Создайте новый проект.
2. Сформируйте систему конъюнктивных продукционных правил, например:

   «If (Угроза1) and (Угроза2) and … and (Угроза5)
   Then (Механизм защиты1)»
3. Сохраните базу знаний в виде структуры нейронной сети.
4. Сформируйте систему дизъюнктивных продукционных правил вида:

«If (Угроза1) or (Угроза2) or … or (Угроза5)
Then (Механизм защиты1)»

5. Сохраните базу знаний в виде структуры нейронной сети.
6. В соответствии с теорией факторов уверенности для каждой из баз знаний задайте экспертные оценки в виде двух функций: меры доверия MB(H,E) и меры недоверия MD (H, E). Функции указывают, соответственно, степень увеличения доверия к гипотезе H, если факт E произошел, и степень увеличения недоверия к гипотезе H, если факт E имел место.

Напоминаем, что мера доверия и недоверия следует определить следующим образом:

$$MB(H,E) = \begin{cases} 1 & \text{if } p(H) = 1 \\ \dfrac{max\,[p(H|E), p(H)] - p(H)}{max\,[1,0] - p(H)} & \text{otherwise} \end{cases}$$

$$MD(H,E) = \begin{cases} 1 & \text{if } p(H) = 0 \\ \dfrac{min\,[p(H|E), p(H)] - p(H)}{min\,[1,0] - p(H)} & \text{otherwise} \end{cases}$$

где: $p(H)$ – априорная вероятность, что гипотеза H является истинной;

$p(H|E)$ – условная вероятность, что гипотеза H является истинной при наступлении факта E.

Фактор уверенности - certainty factor рассчитайте, исходя из значений этих мер

$$cf = \frac{MB(H,E) - MD(H,E)}{1 - min\,[MB(H,E), MD(H,E)]}$$

7. Введите рассчитанные значения факторов уверенности в соответствующие строки сформированных конъюнктивных и дизъюнктивных систем продукционных правил. Сохраните каждую из баз знаний в виде структуры нейронной сети для дальнейших исследований.

Сформированные подобным образом базы знаний, отраженные в информационных полях НС, описывают классификационные заключения, устанавливающие соответствие, например, между одним из 8 механизмов защиты и 5 вышеперечисленными угрозами. То есть на входы НС следует подавать 5 значений – признаков того, что данный набор угроз актуален в ИТ-системе и может привести к нарушению целостности, конфиденциальности и доступности информационных ресурсов. На выходах НС должны быть сформированы 8 значений координат вектора, определяющего, в какой степени каждый из механизмов защиты отвечает требованиям по нейтрализации текущего поля угроз.

Содержание