УДК 004.056: 004.032.26

ИНТЕЛЛЕКТУАЛЬНЫЕ СРЕДСТВА ДЛЯ РЕШЕНИЯ ЗАДАЧ КЛАССИФИКАЦИИ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ.

Степанушко И.В., Трегубенко И.Б.
Черкасский государственный технологический университет, кафедра информатики и информационной безопасности,
E-mail: irttri@rambler.ru, igor.stepanushko@gmail.com

Аннотация

Степанушко И.В., Трегубенко И.Б. Интеллектуальные средства для решения задач классификации в системах защиты информации. *В статье рассматривается сочетание нейронных сетей с системами нечеткой логики, 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 нейронных сетей. Это позволяет отобразить алгоритмы нечеткого логического вывода в структуре нейро-нечеткого классификатора. Адаптивность нейро-нечетких классификаторов позволяет решать задачи идентификации угроз.*

Постановка задачи. Создание перспективных систем защиты информации в последнее время отождествляют с использованием интеллектуальных средств, таких как: экспертные системы, системы нечеткой логики, нейронные сети, генетические алгоритмы, реализующих в системах защиты информации эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности в виде доступной для анализа системы нечетких правил «если-то».

Анализ предыдущих исследований. В научно-технической литературе значительное внимание уделено применению интеллектуальных средств в организации систем защиты информации компьютерных сетей [1,2]. Исследуется возможность использования, как отдельных интеллектуальных средств [3,4], так и их комбинаций для обеспечения безопасности компьютерных систем в условиях высокой динамики угроз. Известные интеллектуальные средства, применяемые в компьютерных сетях, основаны на принципе подобия реализуемых функций аналогичным функциям биологических систем [5]. К часто используемым в КС интеллектуальным средствам относят базы знаний в составе экспертных систем, системы на основе байесовского метода, нечеткие логические системы, а также нейронные сети, эволюционные методы и гибридные интеллектуальные системы.

Формирование цели. Классификация и кластеризация являются основными задачами, решаемыми интеллектуальными средствами обеспечения информационной безопасности компьютерной сети в условиях динамики внешнего окружения, т. к. необходим постоянный мониторинг уязвимостей компьютерной сети и поля угроз.

Изложение основного материала. Известные средства обеспечения информационной безопасности, такие как: детекторы уязвимостей, детекторы вторжений, антивирусное программное обеспечение, 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 [6].

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 нейронной сети. Для устранения отмеченного недостатка целесообразно сочетание нейронных сетей 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 нейронных сетей.

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

Нейронные сети 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. Кроме того, ориентированная на достоверные данные экспертная система не обладает гибкостью и элементами самоорганизации. Нейро-экспертная система (рис.1) имеет организацию, аналогичную структуре экспертной системы. Однако база знаний нейро-экспертной системы организована в форме адаптивного распределенного информационного поля нейронной сети.

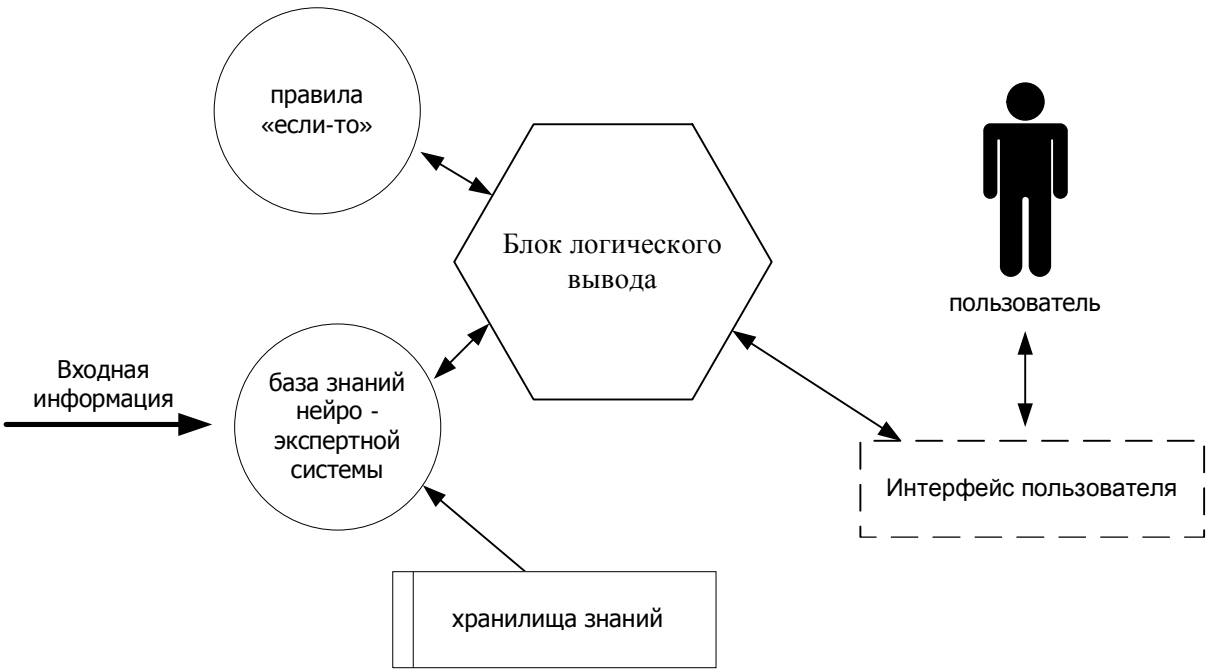

Рисунок 1. Нейро-экспертная система.

Использование нейросетевой базы знаний позволяет устранить основные недостатки основанных на правилах экспертных систем: 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 «если-то» процесса формирования заключения даже в случае неполного выполнения условий в части «если» правила. Активация нейросетевой базы знаний аналогична извлечению знаний, соответствующих правилу «если-то», из информационного поля нейронной сети. Блок логического вывода оперирует нечеткими рассуждениями исходя из потока данных в нейро-экспертной системе.

Выводы. Объединение возможностей нейронных сетей и систем нечеткой логики является перспективным подходом к организации интеллектуальных средств защиты информации. Системы нечеткой логики компенсируют основные «непрозрачности» нейронной сети 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.

Нейронные сети дают возможность отобразить алгоритмы нечеткого логического вывода в структуре нейро-нечеткого классификатора, фиксируя в информационном поле нейронной сети 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.

Список литературы.

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. 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.

6. 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.