БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Постановление Правительства Российской Федерации от 25 августа 2008 г. N 641 "Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS" // Собрание законодательства Российской Федерации. – М.: "Юридическая литература администрации президента Российской Федерации", 2008. – №35. – С. 4037.

2. *Пакулова Е.А.* Аспекты безопасности в системе мониторинга транспортных средств // Материалы I Всероссийская молодежная конференция по проблемам информационной безопасности ПЕРСПЕКТИВА-2009. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 24 – 28.

Пакулова Екатерина Анатольевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: pakulova_e@mail.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; аспирант.

Pakulova Ekaterina Anatolyevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: pakulova_e@mail.ru.
Block "I", 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; post-graduate student.

УДК 681.324

Е.С. Абрамов

ПОСТРОЕНИЕ АДАПТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается методика построения системы защиты информации, позволяющая с помощью методов теории иммунных систем, нечёткой логики, искусственных нейронных сетей, нечеткого многокритериального выбора решений и численных методов оптимизации создать и поддерживать в актуальном состоянии систему защиты информации, в которой обеспечивается поддержание уровня защищенности, адекватного текущим угрозам. Кроме того, решается задача оценки эффективности получившейся новой структуры СЗИ без изменения режима функционирования текущей конфигурации средств защиты.

Иммунные системы; нечёткая логика; искусственные нейронные сети; нечеткий многокритериальный выбор; имитационное моделирование.

E.S. Abramov

DEVELOPMENT OF ADAPTIVE SYSTEM OF INFORMATION SECURITY

There is method of constructing a system of information protection, which allows using the methods of the theory of immune systems, fuzzy logic, artificial neural net-

works, fuzzy multi-criteria selection of solutions and numerical optimization methods to create and maintain up to date system of information protection, which ensures the maintenance of security level that is adequate to the current threats. In addition, describing the solve the problem of assessing the effectiveness of the resulting new structure of the GIS without changing the modus operandi of the current configuration of remedies.

Immune system; fuzzy logic; artificial neural networks; fuzzy multi-criteria selection; simulation modeling.

Постоянно изменяющийся набор угроз безопасности выдвигает свойство адаптивности системы информационной безопасности (СИБ) в разряд первоочередных качеств, необходимых СИБ.

Адаптивность позволяет при ограниченных затратах на организацию СИБ обеспечить заданный уровень безопасности защищаемой АСУ за счет динамической реакции на изменение поля угроз.

Для организации СИБ необходимо от концепции заблаговременного обеспечения защиты информации перейти к концепции системного и регулярного управления уровнем текущей защищенности информации. Система защиты информации, построенная по этому принципу, носит название адаптивной или проактивной системы.

В АСУ существует набор средств и механизмов защиты информации. Однако эти средства разрознены, часто слабо взаимодействуют между собой и зачастую не составляют единую систему. Эффективная СИБ должна решать ряд специфических вопросов, связанных с защитой информации в распределённых системах: распределение ключей, аутентификация терминалов, разграничение доступа, обеспечение целостности данных и т.д. При этом необходимо учитывать, что АСУ должна быть способна к наращиванию и перестройке внутренней структуры.

Поэтому целесообразно разрабатывать систему защиты информации в соответствии с требованиями, предусматривающими использование процессов адаптации, наследования, развития и отбора. Эти процессы реализуются в иммунных системах, функционирующих исходя из принципов подобия механизмов защиты информации в биологических и технических системах. Знание о нормальном поведении системы в данном подходе извлекается из ранее собранных данных. На их основе СИБ должна выявлять любые неприемлемые (новые) изменения, а не искать их среди заранее известного множества событий.

На рис. 1 представлена структура системы защиты информации, реализующей указанные выше принципы.

Обнаружение аномалий при помощи иммунной системы

Нормальное поведение системы часто характеризуется дискретными временными рядами наблюдений. В этом случае проблему обнаружения аномалий можно сформулировать как задачу нахождения недопустимых отклонений в характеристиках системы.

Для большинства методов, используемых в задачах обнаружения аномалий (контрольные карты, методы моделирования, использование экспертных систем с базами знаний, распознавание образов и кластеризацию, скрытые марковские модели, нейронные сети) требуется наличие априорной информации о различных условиях возникновения аномалий [3] или точная теоретическая модель защищаемой системы (см. рис. 1).

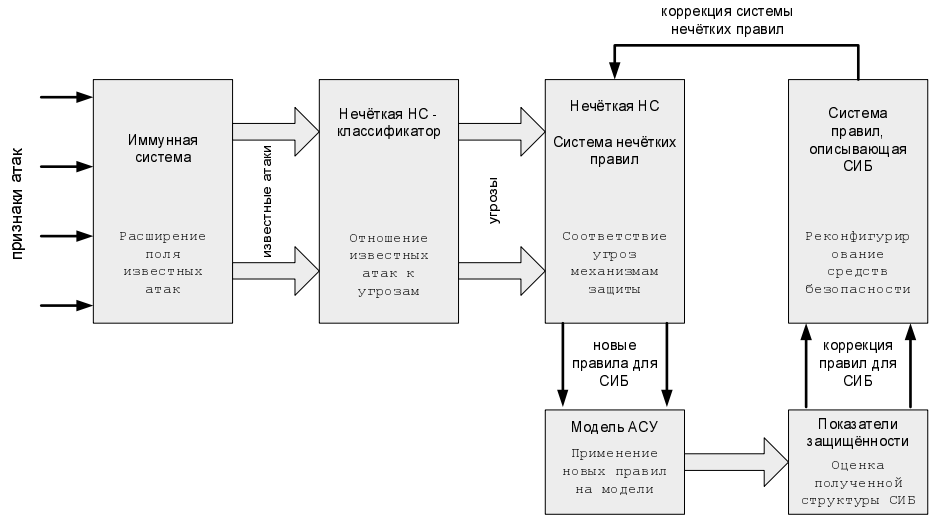

Рис. 1. Структура системы защиты информации

Алгоритм отрицательного отбора

Для решения задачи поиска аномалий предлагается использовать алгоритм отрицательного отбора.

Алгоритм отрицательного отбора состоит в следующем:

1. Определяется «*свой*» как нормальный паттерн активности или устойчивого поведения контролируемой системы или процесса. База данных, описывающих нормальную динамику процессов, представляется как множество из S строк равной длины l, составленных из букв конечного алфавита.

2. Создается набор «*детекторов*» R, ни один из которых не совпадает с какой-либо из строк множества S. Используется правило частичного соответствия, согласно которому две строки совпадают тогда и только тогда, когда они идентичны в r смежных позициях, где величина r выбирается в зависимости от решаемой задачи [4].

3. Данные контролируются путем непрерывного сопоставления детекторов с новыми поступлениями в S. Обнаружение совпадения с детектором рассматривается как изменение (или отклонение) в поведении контролируемой системы.

Кандидаты в набор детекторов генерируются случайно, а затем проверяются на совпадение с собственными строками, и кандидат отвергается, если обнаруживается совпадение. Этот процесс повторяется до тех пор, пока не будет сгенерировано требуемое количество детекторов.

Работа алгоритма делится на два этапа. На первом этапе для данного набора своих строк S и порога соответствия r алгоритм определяет общее число строк, не совпадающих со строками набора S (то есть пересчитываются все неповторяющиеся строки (допустимые *детекторы*)). На втором этапе из допустимых детекторов случайным образом формируется множество строк детектора, контролирующего паттерны поступающих данных.

Обнаружение аномалий

В данном случае задача обнаружения аномалий сведена к задаче обнаружения изменений в строке (совпадения с детектором), при этом подразумевается, что это

изменение (или совпадение) соответствует изменению паттерна нормальной активности.

Любые изменения, которые превосходят допустимые вариации паттернов данных, должны быть полностью представлены в новой форме записи. Для этого значения сначала нормируются по отношению к определенному фиксированному разбросу, что позволяет определить интервал, к которому они относятся, и затем принадлежность интервалу кодируется в бинарной форме. Однако если величина оказывается за пределами интервала (*MIN*, *MAX*), то она должна кодироваться всеми нулями или всеми единицами, в зависимости от границы интервала, за которую она вышла. Тогда, если каждый набор данных кодируется m двоичными числами (величина m выбирается в зависимости от требуемой точности), то между максимальным значением *MAX* и минимальным *MIN* имеется 2^m-2 различающихся интервалов. Соответственно, размер интервала d равен (*MAX* - *MIN*)/2^m-2). Следовательно, для величины x $MIN \le x \le MAX$, где $MAX = MIN + (2^m-2)*d$, и она может быть отнесена к определенному интервалу (с абсолютной ошибкой по амплитуде d) и закодирована двоичным числом по номеру этого интервала. Например, если амплитуда x такова, что $MIN + n_a d \le x \le MIN + (n_a+1)*d$, тогда она кодируется двоичной строкой, соответствующей номеру интервала n_a (где n_a может меняться в пределах от 1 до 2^m-2) [5].

Данные из скользящего временного окна переводятся в двоичный код, согласно описанной выше схеме. Каждое окно является последовательностью порций данных. Затем из последовательных по времени «картинок» окна создается история процесса, и выделяются его закономерности, рассматриваемые как нормальная динамика наблюдаемого процесса. Необходимое для базы данных количество «картинок» зависит от того, насколько сильно и продолжительно влияют на динамику процесса вариации его характеристик. Как только временные ряды данных начинают воспроизводить сходные паттерны, можно считать, что количество выделенных строк достаточно для определения нормальной динамики процесса. Этот набор строк является *своим (S)*. Затем при помощи алгоритма отрицательного отбора генерируются строки, не имеющие сходства со строками из S, и из них формируется *детектор*. Основные этапы работы алгоритма обнаружения аномалий можно описать следующим образом:

1. Собираются данные в количестве, достаточном для характеристики нормальной динамики процесса.

2. На собранных данных оценивается диапазон изменчивости (*MAX*, *MIN* значения) данных, и в зависимости от требуемой точности выбирается параметр кодирования m.

3. Результаты измерений переводятся в двоичную форму при помощи описанной схемы кодирования.

4. Выбирается размер окна, позволяющий определять паттерны данных.

5. Окно передвигается вдоль временного ряда данных, выделенные паттерны кодируются и хранятся как определение *своего*. В дальнейшем они используются в алгоритме отрицательного отбора.

6. Генерируется набор детекторов, отличающихся от строк *своего*. Для выбора детекторов используется алгоритм частичного сравнения, значение параметра r подбирается в зависимости от задачи [4].

7. Набор детекторов, сгенерированный по одному набору нормальных данных, может с некоторой вероятностью обнаруживать изменения (аномалии) в паттернах других наборов данных [5].

8. При мониторинге процесса используются те же параметры подготовки данных, что и при кодировании начальных паттернов нормальных данных. Активация детектора в результате совпадения с текущим паттерном свидетельствует о появлении измененного паттерна.

На рис. 2 показана схема работы системы обнаружения аномалий, реализующей принципы иммунитета.

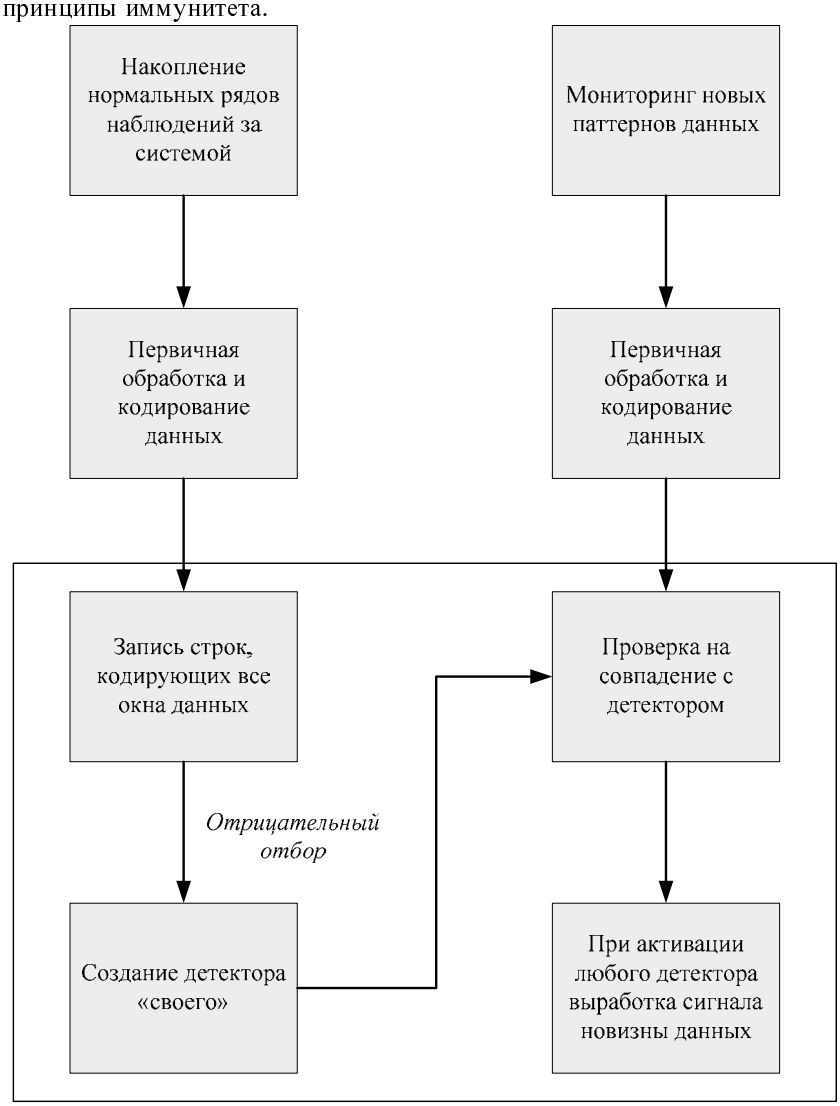

Рис. 2. Схема работы подсистемы обнаружения аномалий, реализующей принципы иммунитета

Нейронечёткие сети и правила

Нейронные сети и информационные системы с нечеткой логикой имеют свои специфические особенности: с одной стороны, возможность обучения, а с другой, процесс решения задач системами с нечеткой логикой достаточно прозрачен для объяснения получаемых выводов [6]. Объединение двух названных подходов *в нечетких НС* позволяет сочетать достоинства нейросетевых вычислительных средств

и нечетких логических систем, опирающихся на априорный опыт в виде заданной системы нечетких предикатных правил [7].

Для целей классификации реализуют нейронечеткие сети (Fuzzy Neural Network, FNN) типа 3, которые применяют для построения систем, основанных на системе нечетких правил вывода [6].

Рассмотрим подход к организации нейронечеткого классификатора, использующего механизм нечеткого логического вывода при решении задачи классификации нечетких входных векторов (Inputs) нейронной сетью с нечеткими связями.

Механизм нечеткого логического вывода основан на базе знаний, формируемой экспертами в виде системы нечетких предикатных правил, например:

$$Ï_1 : åñëè \quad \tilde{x}_1 \quad åñòü \quad A_{11} è \ldots \quad \tilde{x}_n \quad åñòü \quad A_{1n}, \quad òî \quad \tilde{y} = B_1,$$

$$Ï_2 : åñëè \quad \tilde{x}_1 \quad åñòü \quad A_{21} è \ldots \quad \tilde{x}_n \quad åñòü \quad A_{2n}, \quad òî \quad \tilde{y} = B_2,$$

...

$$Ï_k : åñëè \quad \tilde{x}_1 \quad åñòü \quad A_{k1} è \ldots \quad \tilde{x}_n \quad åñòü \quad A_{kn}, \quad òî \quad \tilde{y} = B_k,$$

где $\tilde{x}$ и $\tilde{y}$ – нечеткие входная переменная и переменная вывода, а A_i и B_i – соответствующие функции принадлежности.

Для реализации системы нечетких предикатных правил нейронечеткий классификатор должен выполнять следующие действия:

– *введение нечеткости* – по функциям принадлежности, заданным на области определения предпосылок, исходя из фактических значений нечетких переменных $\tilde{x}_i$, определять степень истинности каждой предпосылки;

– *логический вывод* – по степени истинности предпосылок формировать заключения по каждому из правил, образующие нечеткое подмножество для каждой переменной вывода по каждому из правил;

– *композиция* – полученные на предыдущем этапе нечеткие подмножества для каждой переменной вывода по всем правилам объединять с целью формирования нечеткого подмножества для всех переменных вывода.

Пусть задано полное пространство предпосылок $X = \{\tilde{x}_1, ..., \tilde{x}_m\}$ и полное пространство заключений $Y = \{\tilde{y}_1, ..., \tilde{y}_n\}$. Между $\tilde{x}_i$ и $\tilde{y}_j$, $i = 1...m$, $j = 1...n$ существуют нечеткие причинные отношения $\tilde{x}_i \to \tilde{y}_j$, которые можно представить в виде матрицы R с элементами r_{ij}, $i = 1..m$, $j = 1..n$, а предпосылки и заключения – как нечеткие множества A и B на пространствах X и Y, отношения которых можно представить в виде: $B = A \bullet R$, где $\bullet$ – операция композиции, например, max-min-композиция.

В нечетких логических выводах знания эксперта $A \to B$ отражает *нечеткое отношение* $R = A \to B$, (нечеткое причинное отношение предпосылки и заключения), где операция $\to$ соответствует нечеткой импликации. Нечеткое отношение R можно рассматривать как нечеткое подмножество прямого произведения $X \times Y$ полного множества предпосылок X и заключений Y, а процесс получения нечетко-

го результата вывода $B`$ по предпосылке $A`$ и знаниям $A \to B$ можно представить в виде композиционного правила: $B` = A` \bullet R = A` \bullet (A \to B)$.

В полном пространстве предпосылок $X = \{\tilde{x}_1, ..., \tilde{x}_m\}$ максимальное число входных нечетких векторов задается всевозможными сочетаниями координат $\tilde{x}_i$, $i = 1...m$. Каждому входному вектору из пространства X можно поставить в соответствие нечеткий формальный нейрон (ФН) нейронечеткого классификатора, выполняющий операцию логического вывода, например, *min*. Отображение множества результатов логического вывода в полное пространство заключений $Y = \{\tilde{y}_1, ..., \tilde{y}_n\}$ можно реализовать посредством операции композиции, и каждому выходному вектору из пространства Y можно поставить в соответствие нечеткий ФН нейронечеткого классификатора, выполняющий операцию, к примеру, *max*.

Нейронечеткий классификатор m-мерных нормализованных векторов $\boldsymbol{X}$ с нечеткими координаторами $(\tilde{x}_1, ..., \tilde{x}_m)$ представляют в виде трехслойной нечеткой нейронной сети (рис. 3), в которой:

– первый слой содержит m, по числу координат входного вектора, нечетких нейронов с комплементарными нечеткими связями, формирующих m пар нечетких высказываний (НВ) вида $\tilde{x}_i$ *есть* S, $\tilde{x}_i$ *есть* L, $i = 1...m$;

– средний слой содержит до 2^m нечетких нейронов с комплементарными нечетким связями, выполняющих операцию логического вывода (например, *min*) над сочетаниями нечетких высказываний первого слоя НС с целью формирования системы нечетких классификационных заключений;

– выходной слой содержит n, по числу координат выходного вектора, нечетких нейронов с комплементарными нечетким связями, выполняющих операцию композиции (например, *max*) над нечеткими классификационными заключениями второго слоя НС для формирования n-мерных векторов $\boldsymbol{Y}$ выходных нечетких заключений $(\tilde{y}_1, ..., \tilde{y}_n)$.

Нечеткие нейроны первого слоя в соответствии с заданным типом функции принадлежности f формируют комплементарные пары значений истинности для входных нечетких переменных $\tilde{x}_i$, $i = 1...m$ координат входного вектора $\boldsymbol{X}$. Координаты входного вектора нормализованы путем деления на значение ядра нечеткой переменной. При заданном значении координаты вектора $\boldsymbol{X}$ на отрезке области определения каждой паре значений истинности входных нечетких переменных соответствуют значения ординат функций принадлежности S (small) и L (large), которые в сумме дают 1, то есть каждый нечеткий формальный нейрон первого слоя реализует пару «частично противоположных» нечетких высказываний, которые через комплементарную пару нечетких связей подаются на средний слой НС.

Нечеткая связь на выходе ФН представляет собой совокупность взвешенных межнейронных связей, веса которых отражают распределение истинности в нечетком множестве, соответствующем некоторой функции принадлежности [8]. Пара функций принадлежности, например S и L, образуют две нечеткие связи, составляющие одну комплементарную нечеткую связь.

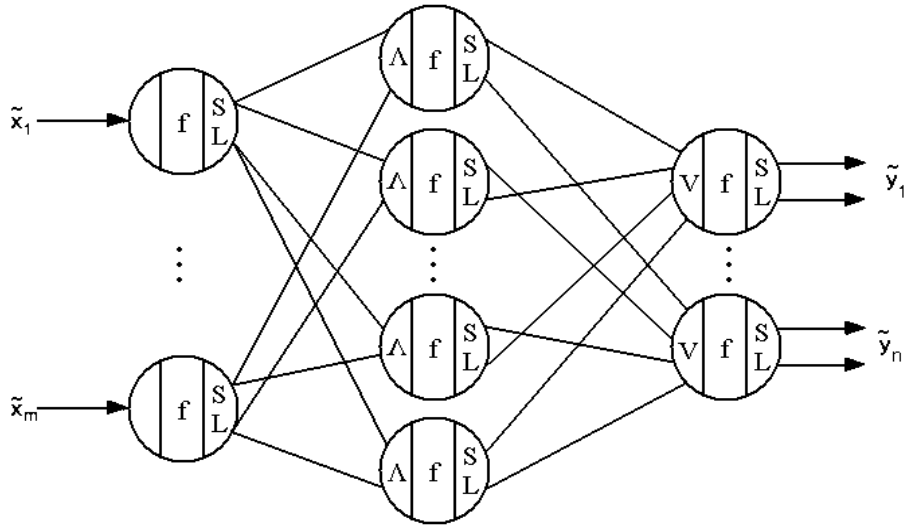

Рис. 3. Нейронечеткий классификатор в виде трехслойной нечеткой нейронной сети

Если средний слой нечеткой НС содержит максимальное число нечетких нейронов «И», то промежуточный вектор нечетких заключений будет содержать все возможные нечеткие классификационные заключения, которые могут следовать из всех возможных векторов входных нечетких посылок.

Выходной слой нечеткой НС образован из нечетких нейронов «ИЛИ» (по числу нечетких заключений $\tilde{y}_j, \quad j=1..n$) и формирует вектор выходных нечетких заключений в соответствии с заданной экспертами системой нечетких предикатных правил.

Последующее обучение нейронечеткого классификатора может производиться с использованием алгоритмов адаптации нейронечетких сетей, в частности с использованием механизма нечеткой межнейронной связи [8]. Обучение нейронечеткого классификатора на наборе векторов обучающей выборки позволит выявить возможную противоречивость исходной системы нечетких предикатных правил и устранить из структуры нейронной сети незначащие связи (неточные заключения из исходной системы нечетких предикатных правил).

Коррекция системы нечётких правил

Коррекция системы нечётких правил расширяет систему нечетких правил логического вывода, которая учитывает не только координаты входного вектора X, но и координаты вектора текущего состояния системы информационной безопасности *Z*.

В процессе работы классификатора производится не только идентификация вектора *Y* по векторам *X* и *Z*, но и формируются предложения *C* по изменению состояния системы [9].

Для иммунного уровня защиты (отношение атак к угрозам) координаты вектора *Z* могут отражать системные характеристики АСУ, к примеру, такие как:

- тип установленного программного обеспечения;
- обновления установленного ПО;

– работающие сервисы;
– поддержка многопользовательского режима;
– использование в АСУ устройств ввода/вывода информации, таких как дисководы, CD/DVD-приводы, USB-порты;
– наличие средств резервного копирования информации;
– беспроводное подключение к ЛВС АСУ.

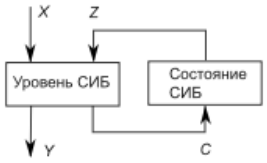

Рис. 4. Коррекция нейронечёткого классификатора

Для рецепторного уровня защиты (уровень соответствия актуальных угроз механизмам защиты АСУ и оценка полученной конфигурации СИБ) координаты вектора *Z* могут отражать структурные характеристики СИБ, к примеру, такие как:
– беспроводное подключение к ЛВС АСУ, множество используемых в СИБ механизмов защиты;
– распределение механизмов защиты по иерархии СИБ;
– активность используемых механизмов защиты;
– показатели (рейтинг) защищенности АСУ.

Оценка эффективности получившейся конфигурации

Оценка эффективности системы защиты информации относится к задачам многокритериального оценивания, поскольку такую сложную систему невозможно полно охарактеризовать с помощью единственного показателя. Поэтому, для оценки эффективности необходимо использовать счетное множество показателей: $W=\{Wi:i=1,n\}$, где n – количество показателей, а в качестве показателей могут выступать показатели эффективности вероятностно-временного характера функционирования системы защиты информации.

Существуют два основных подхода к многокритериальной оценке эффективности сложных систем [2]. Первый связан со сведением множества частных показателей $\{Wi\}$ к единственному интегральному показателю W_0. Второй подход используется при наличии значительного числа частных показателей эффективности системы, имеющих приблизительно одинаковую важность. Критерием оценки эффективности в этом случае может служить достижение одним из показателей экстремального значения с соблюдением ограничений и условий на другие свойства системы при выполнении всех установленных к СЗИ требований [1].

Рассмотрим показатели эффективности, которые могут быть использованы при решении задачи сравнения различных получившихся структур СЗИ. Целью функционирования системы защиты информации является поддержание заданного уровня защищенности. Поэтому показатели эффективности должны характеризовать динамические свойства системы защиты информации и позволять оценивать ее характеристики как адаптивной системы. Такую возможность предоставляют показатели эффективности вероятностно-временного характера, имеющие в общем случае смысл функций распределения. Такими показателями могут быть:
– вероятность преодоления системы защиты информации P_n за время T_n;

– вероятность доставки единицы информации (например, пакета данных) от абонента к абоненту $P_д$ за время $T_д$;

– аппаратурная сложность S.

Значения $P_п$, $T_п$, $P_д$ и $T_д$ могут быть определены с помощью имитационного моделирования (либо аналитически). Показатель аппаратурной сложности S может быть определен, например, как количество типовых модулей в системе защиты информации. Однако при анализе структур различных типов, различающихся, например, количеством и распределением механизмов защиты, получение аналитического выражения для показателя S практически невозможно. Это связано со значительным различием типов механизмов защиты информации, со множеством способов их практической реализации и, следовательно, с невозможностью сведения их аппаратурной избыточности к общей единице измерения. Поэтому целесообразно в этом случае рассматривать S как качественный показатель, а для его оценки использовать методы теории нечетких множеств. При этом количественные показатели $P_п$, $T_п$, $P_д$ и $T_д$ тоже могут рассматриваться как нечеткие при условии, что для них определены максимальные и минимальные допустимые значения.

Функции принадлежности в соответствии с [2] могут быть определены как: $mP=(P-Pmin)/(Pmax-Pmin)$, $mT=(1/T-1/Tmax)/(1/Tmin-1/Tmax)$. Тогда задача выбора структуры и оптимизации системы защиты логически разбивается на два этапа:

1) выбор структуры системы защиты информации;

2) оптимизация системы защиты информации.

На первом этапе методами теории нечетких многокритериальных задач оптимизации определяется множество Паретооптимальных структур СЗИ. В общем случае множество Парето может быть как пустым, так и содержащим произвольное количество элементов. В работе [2] описаны методы, позволяющие добиться, чтобы множество Парето было не пустым и содержало конечное число элементов. Среди определенного таким образом множества структур системы защиты выбирается в качестве базовой одна. Показатели эффективности на этом этапе – нечеткие.

На втором этапе проводится синтез рациональной системы защиты информации в рамках выбранной на первом этапе структуры. Для этого методами теории численной оптимизации формируется состав протоколов, реализующих определенные на первом этапе службы и механизмы защиты информации, оптимизируется их распределение по уровням АСУ. Показатели эффективности $P_п$, $T_п$, $P_д$ и $T_д$ на этом этапе – четкие.

Функционирование адаптивной системы информационной безопасности

Конкретная постановка задачи оптимизации определяется задаваемым надсистемой уровнем защищенности информации в зависимости от условий функционирования. Можно предложить следующие постановки:

1) минимизировать значения вероятности преодоления механизмов защиты $P_п$ с учетом ограничения на вероятность доставки пакета $P_д$ за заданное время $T_д$;

2) максимизировать $P_д$ при заданных ограничениях на вероятность $P_п$ за время $T_п$;

3) найти $F^*=max\ F(P_п, T_п, P_д, T_д)$, где F – функция, осуществляющая свертку частных показателей эффективности $P_п$, $T_п$.

Синтезированная на втором этапе система защиты информации будет поддерживать заданный уровень защищенности. Когда надсистема определит, что условия функционирования изменились, она выработает новое требуемое значение

уровня защищенности информации, и оптимизация системы защиты информации будет проведена заново.

Заключение

Предлагается методика построения системы защиты информации, позволяющая с помощью методов теории иммунных систем, нечёткой логики, искусственных нейронных сетей, нечеткого многокритериального выбора решений и численных методов оптимизации создать и поддерживать в актуальном состоянии систему защиты информации, в которой обеспечивается поддержание уровня защищенности, адекватного текущим угрозам. Кроме этого, решается задача оценки эффективности получившейся новой структуры СЗИ без изменения режима функционирования текущей конфигурации средств защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Горбунов А.Л., Чуменко В.Н.*, Выбор рациональной структуры средств защиты информации в АСУ. [Электронный ресурс] / Режим доступа: http://kiev-security.org.ua/box/2/26.shtml - свободный. – 03.12.2009.

2. Нечеткие множества в моделях управления и искусственного интеллекта. / Под ред. Д.А.Поспелова. - М.:Наука, 1986.

3. *Kozma R., Kitamura M., Sakuma M., Yokoyama Y.* Anomaly Detection by neural network models and statistical time series analysis // Proc. IEEE International Conference on Neural Networks, Orlando, Florida, June 27–29, 1994.

4. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Serf-nonself discrimination in a computer // Proc. IEEE Symposium on Research in Security and Privacy, Oakland, CA, 16–18 May, 1994. P. 202–212.

5. *Dasgupta D., Forrest S.* Novelty detection in time series data using ideas from immunology // ISCA 5th International Conf. on Intelligent Systems, Reno, Nevada, June 19–21, 1996.

6. *Fuller R.* Neural Fuzzy Systems. – Abo: Abo Akademi University, 1995. 252 p.

7. *Negneyitsky M.* Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.

8. *Нестерук Г.Ф., Куприянов М.С., Елизаров С.И.* К решению задачи нейронечеткой классификации // Сб. докл. VI Междунар. конф. SCM'2003. – СПб.: СПГЭТУ, 2003. Т. 1. – С. 244–246.

9. *Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Воскресенский С.И., Костин А.А.,* Повышение избыточности информационных полей как системы безопасности.

10. *Баутов А.* Эффективность защиты информации. [Электронный ресурс] / Режим доступа: http://www.bre.ru/security/19165.html. - свободный. – Загл. с экрана.

Абрамов Евгений Сергеевич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: abramoves@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Abramov Evgeny Sergeevich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: abramoves@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; associate professor.