УДК 621.396

Ф.Г. НЕСТЕРУК, А.Ю. ТАТАРИНОВ, Г.Ф. НЕСТЕРУК

ИССЛЕДОВАНИЕ АДАПТИВНЫХ КЛАССИФИКАТОРОВ В СОСТАВЕ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Санкт-Петербургский институт информатики и информатизации РАН (СПИИРАН),
г. Санкт-Петербург, ул. 14-я линия В.О., 39,
Российская Федерация, тел.: +7(812) 328 51 85,
http://www.spiiras.nw.ru/, e-mail: 08p@mail.ru

Анотація. Розглянуто питання організації інкрементний класифікаторів у складі перспективних систем захисту, які здатні адаптуватися до динаміки комп'ютерних атак. Показано, що в адаптивних засобах класифікації для систем захисту доцільно використовувати інкрементні класифікатори сімейства ARTMAP. Класифікатори ARTMAP дозволяють розпізнавати комп'ютерну атаку в режимі реального часу і значного зменшити кількість категорій розпізнавання без істотної втрати точності класифікації.

Аннотация. Рассмотрены вопросы организации инкрементных классификаторов в составе перспективных систем защиты, которые способны адаптироваться к динамике компьютерных атак. Показано, что в адаптивных средствах классификации для систем защиты целесообразно использовать инкрементные классификаторы семейства ARTMAP. Классификаторы ARTMAP позволяют распознавать компьютерную атаку в режиме реального времени и значительного уменьшить число категорий распознавания без существенной потери точности классификации.

Abstract. Discussed the organization of incremental classifiers in the advanced security systems that are able to adapt to the dynamics of computer attacks. It is shown that the adaptive means of classification for security systems appropriate to use an incremental classifier family ARTMAP. ARTMAP classifiers can recognize cyber attacks in real time and significantly reduce the number of categories of recognition without significant loss of classification accuracy.

Ключевые слова: защита информации, адаптация к угрозам, интеллектуальные средства защиты.

ВСТУПЛЕНИЕ

Работа посвящена решению актуальной для компьютерных систем задачи, связанной с обеспечением оперативной реакции системы защиты информации (СЗИ) на угрозы в условиях высокой динамики компьютерных атак. Одно из решений проблемы – применение адаптивных средств классификации (АСК) при разработке перспективных СЗИ [1, 2].

Цель работы – обсуждение подхода к организации интеллектуальной защиты информации на базе АСК с инкрементным обучением. На этапе структурной пластичности помимо увеличения числа кластеров в процессе обучения НС периодически выполняется процедура сокращения их числа за счет удаления малозначащих категорий, и категорий, сформированных посредством пролиферации. Инкрементное обучение позволяет реализовать адаптацию средств классификации в режиме реального времени [3], что принципиально для защиты информационных ресуров компьютерных систем.

В основе АСК лежит биологический принцип двойной пластичности: изменения в структуре системы происходят реже, чем изменения функциональных параметров [4]. Анализ архитектур нейронных сетей (НС) [5] показал перспективность применения в СЗИ сетей теории адаптивного резонанса (ART). Так сети Fuzzy ARTMAP и Cascade ARTMAP [6, 7] позволяет реализовать важные для АСК качества: *стабильность* (сохранение накопленных знаний) и *пластичность* (коррекция знаний в процессе обучения); возможность *отображения априорного опыта* экспертов безопасности в структуре кластеров для формирования исходной базы знаний (БЗ), которая корректируется в процессе эксплуатации посредством инкрементного обучения НС [6]. Кроме того, в Cascade ARTMAP может быть реализована процедура оптимизации БЗ за счет удаления несущественных для классификации кластеров [8].

Рассмотрим функциональные возможности НС семейства ART, принципиально важные для организации адаптивных средств защиты информации, работающих в режиме реального времени.

АНАЛИЗ АСК НА БАЗЕ СЕТЕЙ ARTMAP

Fuzzy ARTMAP (FAM) часто реализуют в виде упрощенной модели (рис. 1) [7], полученной комбинацией самообучаемой сети ART с полем преобразования. FAM состоит из двух уровней узлов (нейронов) с полными связями: M узлов входного слоя F_1, и N узлов соревновательного слоя F_2. Набор вещественных весов $W = \{w_{ij} \in [0,1] : i = 1,2,...,M;\ j = 1,2,...,N\}$ связывает слой F_1 со слоем F_2 прямыми связями. Каждый j-й узел слоя F_2 представляет *категорию распознавания*, которая соответствует вектору-прототипу $w_j = (w_{1j}, w_{2j},..., w_{Mj})$. Слой F_2, связанный через обученные ассоциативные связи с 1, …, L узлами выходного слоя, отображает поле преобразования F^{ab}, где L – число классов в выходном пространстве результатов. Бинарные веса $W^{ab} = \{w_{ij}^{ab} \in \{0,1\} : i = 1,2,...,N;\ j = 1,2,...,L\}$ соединяет слой F_2 с выходным слоем НС. Вектор $w_j^{ab} = (w_{j1}^{ab}, w_{j2}^{ab},..., w_{jL}^{ab})$ связывает j-й узел слоя F_2 с L узлами выходного слоя.

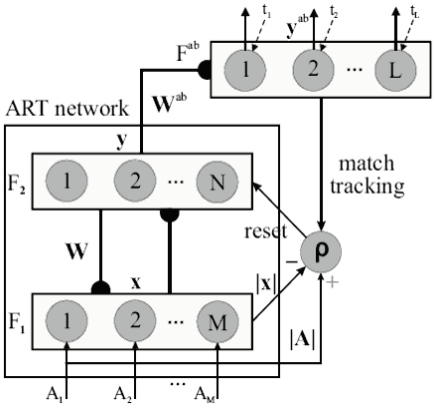


Рис. 1. Архитектура сети Fuzzy ARTMAP

В режиме адаптации FAM использует метод обучения с учителем над нормализованными векторами входного набора обучающей выборки $a = (a_1, a_2,..., a_m)$, $0 \le a_i \le 1$, согласно выходному вектору (output labels) $t = (t_1, t_2,..., t_L)$, где $t_k = 1$, если k – целевая метка класса для вектора $\boldsymbol{a}$, и $t_k = 0$ иначе.

$M = 2m$ представляет размерность вектора $\boldsymbol{A} = (\boldsymbol{a}, \boldsymbol{1}–\boldsymbol{a})$, сформированного из вектора $\boldsymbol{a}$ путем добавления комплементарного фрагмента **1-*a***, где **1** обозначает m-мерный вектор, все координаты которого равны 1.

Геометрическая интерпретация Fuzzy ARTMAP [9]. Шаблон (прототип), соответствующий активному узлу называется *активным шаблоном* (помечен литерой *a*), а шаблон нейтрального узла – *нейтральным шаблоном*, который представляется вектором, все координаты которого равны 1. Нисходящие веса от узла в области F_2^a рассматриваются как *шаблон*. Если имеется активный шаблон w_j^a, соответствующий входным образцам $I^1 = (x(1), x^c(1))$, $I^2 = (x(2), x^c(2))$, …, $I^P = (x(P), x^c(P))$, то согласно правилу обучения FAM w_j^a может быть записан как:

$w_j^a = \wedge_{i=1}^P I^i = (\wedge_{i=1}^P x(i), \wedge_{i=1}^P x^c(i)) = (\wedge_{i=1}^P x(i), \{\vee_{i=1}^P x(i)\}^c)$. Или $w_j^a = (u_j^a, \{v_j^a\}^c)$, где $u_j^a = \wedge_{i=1}^P x(i)$ и $v_j^a = \vee_{i=1}^P x(i)$. Вектор веса w_j^a в терминах M-мерных векторов u_j^a и v_j^a м.б. представлен двумя точками в M-мерном пространстве (рис. 2 для $M = 2$) [9].

Геометрическое представление весов может быть расширено на пространство входных образцов. Входной образец $I = (x, x^c)$ можно геометрически интерпретировать прямоугольником с конечными точками (end-points) x и x, т.е. вектор I может быть представлен прямоугольником размера 0 или отдельной точкой x в M-мерном пространстве.

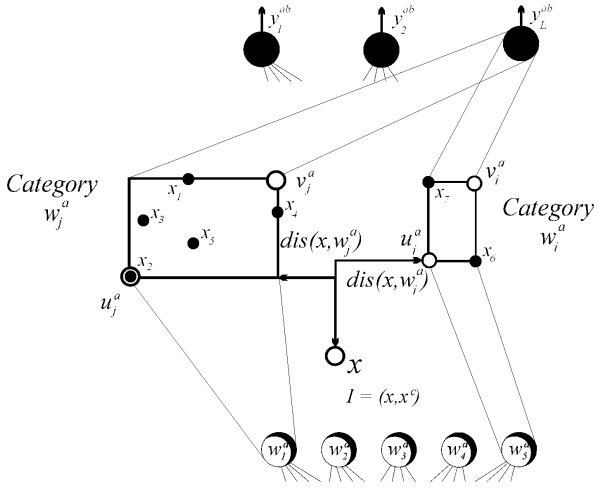
Размер прямоугольника R_j^a с конечными точками u_j^a и v_j^a принят равным норме вектора $L_1 = v_j^a - u_j^a$, где норма вектора – это сумма абсолютных величин ее компонентов. Итак, можно представлять $w_j^a = (u_j^a, \{v_j^a\}^c)$ как прямоугольник R_j^a с конечными точками u_j^a и v_j^a в M-мерном

пространстве, а $I = (x, x^c)$ как точку x в M-мерное пространстве.

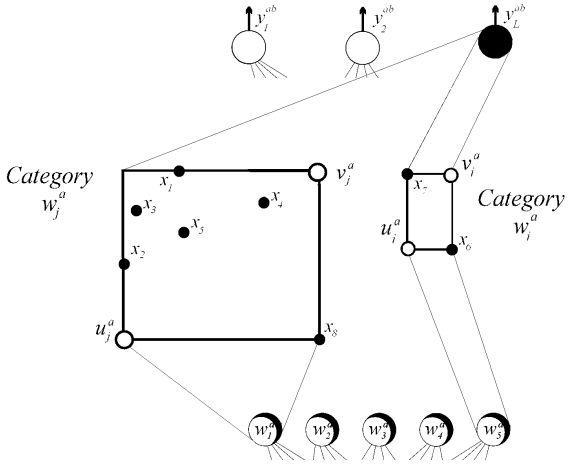
В течение процесса обучения FAM «сжатые» представления входных образцов, принадлежащих к набору обучения, формируются в области F_2^a и могут визуализироваться как прямоугольники, соответствующие активированным узлам в F_2^a. Идея соотнесения прямоугольника с кластером (узлом НС), состоит в том, что в пределах его границ разместились соответствующие этому узлу входные образцы. В FAM представления входных образцов, размещенные в слое F_2^a, ассоциируются (are mapped) в ходе обучения с их правильными выходными образцами (метками).

Каждый нисходящий вектора веса w_j^a, соответствующий узлу j в слое F_2^a, в M-мерном пространстве интерпретируется прямоугольником с конечными точками u_j^a и v_j^a, а входной образец $I = (x, x^c)$ – M-мерным вектором входа x (рис. 2). Расстояние $dis(x, w_j^a)$ между входным образцом x и прямоугольником R_j^a, представляющего категорию w_j^a, который не включает x, – это минимальное расстояние от x до точки, принадлежащей границе прямоугольника R_j^a.

Рис. 2 иллюстрируют процесс коррекции размеров кластера АСК. В ходе обучения классификатора сформированы две категории w_i^a и w_j^a, $i \neq j$. При поступлении нового входного образца $I = (x, x^c)$ определяются его удаленность $dis(x, w_i^a)$ и $dis(x, w_j^a)$ от каждого из кластеров (рис. 2.а). В режиме «быстрого» обучения более близкий j-й кластер увеличивается и включает в себя входной образец (рис. 2.б).



а) – отнесение образца $I=(x,x^c)$ к j-у кластеру



б) – коррекция размеров j – го кластера АСК

Рис. 2. Геометрическая интерпретация процесса коррекции размеров кластера

Cascade ARTMAP как обобщение Fuzzy ARTMAP [10] позволяет отображать правила нечеткого логического вывода (НЛВ) в составе БЗ на топологию НС согласно этапам НЛВ [6, 8].

Отображение правила НЛВ на кластеры Cascade ARTMAP позволяет до начала обучения НС реализовать передачу опыта эксплуатации средств защиты – априорные знания (эволюционное свойство наследования). В процессе адаптации НС на примерах обучающей выборки происходит коррекция БЗ (эволюционное свойство развития). В процессе обучения правила НЛВ могут быть созданы динамически (эволюционное свойство пластичности), что отличает Cascade ARTMAP от нейро-нечетких сетей со статической заданной структурой нейронов в слоях НС [1, 2]. За счет свойства самостабилизации инкрементное обучение в Cascade ARTMAP не приводит к забыванию накопленных знаний (эволюционное свойство стабильности), а также к модификации правил НЛВ в составе БЗ.

Использование процедуры извлечения правил в ARTMAP [8] позволяет текущее состояние Cascade ARTMAP преобразовать в компактный набор правил НЛВ, что обеспечивает «прозрачность» представления знаний в НС, и выполнять сравнение исходного набора правил с правилами, полученными в процессе адаптации НС (рис. 3) [6]. С каждым правилом ассоциируется фактор доверия (важность правила), что позволяет ранжировать и оценивать компоненты знания.

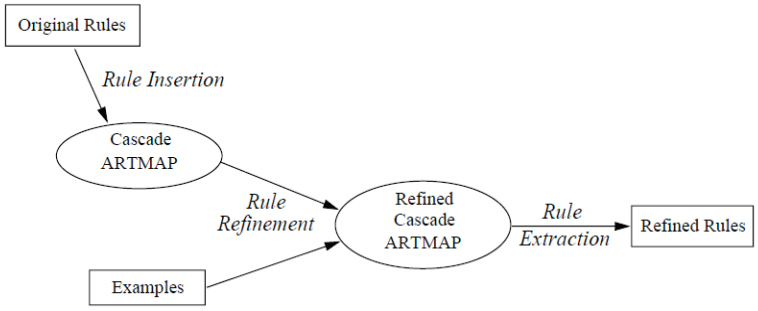


Рис. 3. Cascade ARTMAP, использующая априорные знания

Добавление правила (Rule Insertion). Структура Cascade ARTMAP совместима с представлением знаний в экспертных системах (правила IF-THEN) и правила НЛВ м. б. конвертированы в конкретные категории распознавания. Инициализация Cascade ARTMAP известными правилами НЛВ (фиксация априорных знаний в структуре НС) фрмирует исходную структуру классификатора, что помогает ускорить процесс обучения НС и точность предсказания, т.к. формирует кластеры, которые могут не охватываться векторами обучающей выборки.

Процесс добавления правил НЛВ производится в два этапа: 1) все правила разделяются по именам атрибутов и создается таблица символов, в которой каждый атрибут имеет уникальной вхождение; 2) основываясь на данных из таблицы символов, выполняется преобразование каждого правила в два 2M-размерных вектора ***A*** и ***B***, где M – общее число атрибутов в таблице символов, которые используются как входные векторы для модулей ART_a и ART_b соответственно. Правила НЛВ представляются в формате:

IF $x_1, x_{2,}..., x_M, \bar{x}_1, \bar{x}_{2,}..., \bar{x}_M$ THEN $y_1, y_{2,}..., y_N, \bar{y}_1, \bar{y}_{2,}..., \bar{y}_N$

где $x_1, x_{2,}..., x_M$ и $y_1, y_{2,}..., y_N$ – прямые значения атрибутов, а $\bar{x}_1, \bar{x}_{2,}..., \bar{x}_M$ и $\bar{y}_1, \bar{y}_{2,}..., \bar{y}_N$ – дополнительные значения атрибутов.

АСК оперирует с парой комплементарных векторов ***A*** = (a, a^c) и ***B*** = (b, b^c).

Причем для каждого индекса j = 1, …, M

$$(a_j, a_j^c) = \begin{Bmatrix} (1,0),\ if\ c_j = x_i,\ i \in \{1,...,M\} \\ (0,1),\ if\ c_j = \bar{x}_i,\ i \in \{1,...,M\} \\ (0,0),\ else \end{Bmatrix}, \qquad (b_j, b_j^c) = \begin{Bmatrix} (1,0),\ if\ c_j = y_i,\ i \in \{1,...,N\} \\ (0,1),\ if\ c_j = \bar{y}_i,\ i \in \{1,...,N\} \\ (0,0),\ else \end{Bmatrix},$$

где c_j – это j-й атрибут в таблице символов.

Обучение и уточнение правил (Learning and Rule Refinement). Обучение в Cascade ARTMAP более сложное чем в Fuzzy ARTMAP из-за дополнительной обработки правил, включенных в процесс предсказания. Используют алгоритм перебора с возвратом (backtracking), который идентифицирует те правила слоя F_2^a , которые ответственны за прогнозирование через трассировку от последнего активированного правила. Т.о. если для заданного J выбрана последняя категория из слоя F_2^a, которая выполнила предсказание, алгоритм идентифицирует предшествующее множество $\psi(J)$, которое

содержит категорию J и все категории из F_2^a, которые привели к выбору категории J. Обратное распространение происходит в направлении $F_2^a \to F_1^a \to F_1^b \to F_2^b \to F^{ab} \to F_2^a$.

Извлечение правил из Cascade ARTMAP**.** Правила представляются в явной форме (рис. 4) [8]. Каждая категория в поле F_2^a соответствует категории распознавания для входных векторов из ART_a. Через поле преобразования F^{ab}, каждая категория связывается с категорией F_2^b из ART_b, которая кодирует предсказание. Векторы обученных весов (один для каждой категории F_2^a) представляют правила, которые связывают зависимые и независимые атрибуты. Набор правил эквивалентен категориям в слое F_2^a.

Роль механизма извлечения правил – выбрать и описать ограниченное множество часто используемых категорий. Для оценки значимости каждой категории F_2^a рассчитывается фактор доверия, который учитывает частоту использования и точность предсказания. Удаление категорий с низким фактором доверия приводит к снижению сложности НС и, следовательно, повышению оперативности СЗИ.

Удаление правил. Каждый входной вектор задействует несколько категорий в F_2^a в отличии от использования только одной категории в Fuzzy ARTMAP. Для того чтобы оценить частоту использования и точность, для каждой категории j в F_2^a вводятся три счетчика: счетчик кодирования c_j – отслеживает число обучающих векторов, закодированных категорией j; счетчик предсказаний p_j – число предсказаний выполненных категорией j на тестовой выборке; и счетчик успешных предсказаний s_j – число успешных предсказаний выполненных категорией j на тестовой выборке.

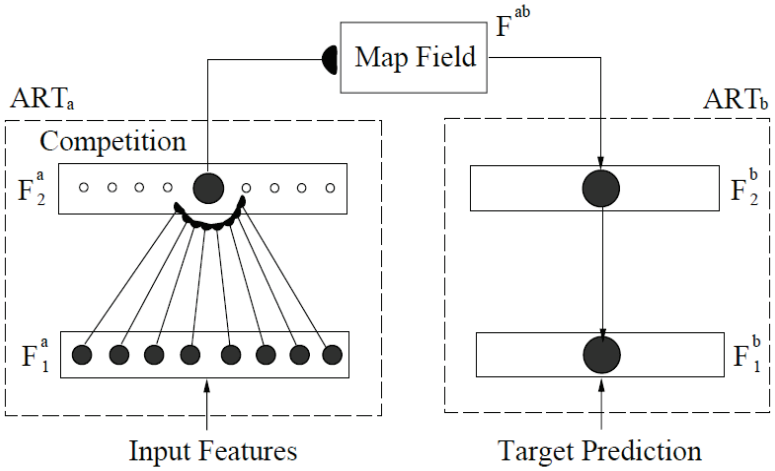


Рис. 4. Представление правил в Cascade ARTMAP

Для каждого входного вектора обучающей выборки c_j=c_j+1, для каждой категории j в предшествующем множестве $\psi(J)$, где J – последняя выбранная категория сделавшая предсказание. Для каждого входного вектора тестовой выборки p_j=p_j+1 для каждой категории F_2^a из предшествующего множества $\psi(J)$, выполнившей предсказание из тестового набора; s_j=s_j+1, для каждой категории F_2^a из предшествующего множества $\psi(J)$, если предсказание из тестового набора выполнено корректно. Используя счетчики кодирования, предсказания и успешного предсказания, рассчитываются значения использования (U_j) и точности (A_j) для каждой категории в F_2^a:

$$U_j = c_j / \max\{c_k : k \in F_2^a\}, \qquad A_j = P_j / \max\{P_k : k \in F_2^a\},$$

где k – каждая из категорий, принадлежащих слою F_2^a, P_j – процент правильно предсказанных категорий j, рассчитанный как $P_j = s_j / p_j$. U_j и A_j используются для расчета фактора доверия по формуле $CF_j = \gamma U_j + (1-\gamma) A_j$, где $\gamma \in [0,1]$ – весовой коэффициент.

После того, как определен фактор доверия распознанные категории могут быть удалены, используя одну из стратегий. *Пороговое удаление* – категории в слое F_2^a с фактором доверия ниже заданного порога τ (по умолчанию 0,5) удаляются из НС. Дополнительно задают число категорий, которые должны остаться в системе. Это скоростной метод. *Локальное удаление* – удаляется одна категория за шаг. Алгоритм удаляет категорию с наименьшим фактором доверия. Если удаление

категории повлекло за собой снижение точности классификации, то ее возвращают. *Гибридная* стратегия сокращает категории, используя пороговое удаление, а затем применяет алгоритм локального удаления.

ИССЛЕДОВАНИЕ СЕТЕЙ ARTMAP В СОСТАВЕ СЗИ

Для исследования возможности применения сети Cascade ARTMAP в составе СЗИ разработана тестовое программное обеспечение для оценки влияния числа кластеров (категорий) на точность и скорость решения задачи нейросетевой классификации компьютерных атак [11].

Оценка качества классификации при применении алгоритма удаления правил. Для оценки качества сети ARTMAP использована классическая задача классификации «круг в квадрате» [12]. При тестировании использовались параметры: α=0,001 (параметр выбора); β=0,8 (скорость обучения); ρ=0,9 (параметр близости); τ=0,5 (порог удаления). С каждым шагом из сети удалялось не более 1/3 от общего числа категорий (табл. 1, рис. 5).

Таблица 1

Результаты выполнения алгоритма порогового удаления категорий в сети ARTMAP

Число векторов обучающей выборки	Шаг алгоритма удаления	Общее число категорий	Качество распознавания (%)	Время обработки тестовой выборки (мс)
100 / 10000	0 1 2	40 28 19	93,5 88,8 88,4	89 68 51
500 / 10000	0 1 2	97 65 36	96,4 93,2 85,7	170 126 94
1000 / 10000	0 1 2	131 88 59	97,2 92,4 89,6	227 162 118
3000 / 10000	0 1 2	189 126 84	98,2 95,3 92,3	314 221 155

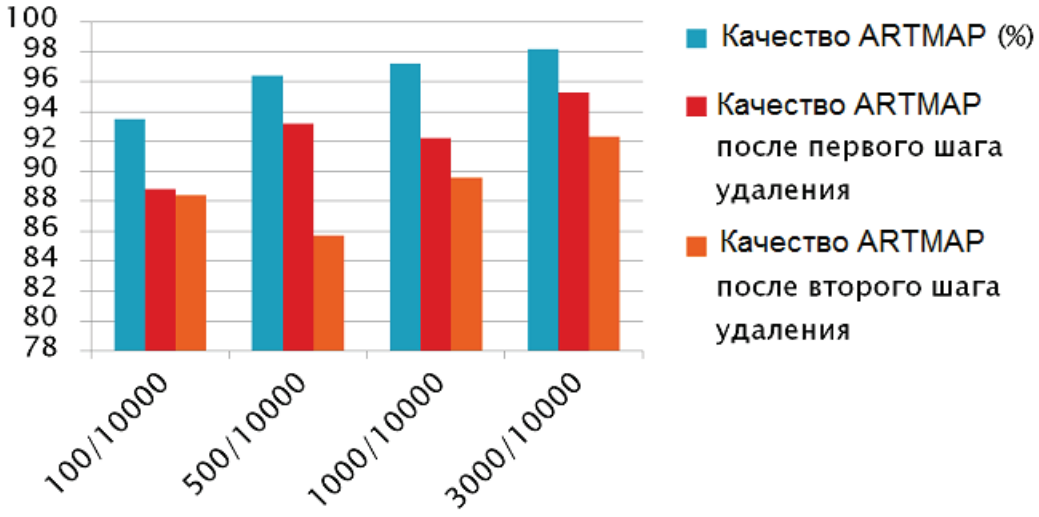


Рис. 5. Динамика качества классификации при пороговом удалении категорий из сети ARTMAP

Оценка производительности АСК. Для тестирования производительности АСК выбрана задача сопоставления угрозам известных методов защиты. База знаний из 17 правил различает 11 видов угроз на основе входных и дополнительных атрибутов, описывающих текущее состояние системы (табл. 2).

База знаний использовалась для выполнения двух функций: 1) инициализации Cascade ARTMAP на подмножестве исходного наборов; 2) генерации тестовых данных на основе имеющихся правил. Для обучения и тестирования создан набор из 1000 входных векторов путем случайного присвоения значений входным атрибутам и получения выходных значений основанных на 17 правилах из БЗ.

Вначале определялось качество классификации АСК без использования правил БЗ. Система обучалась на подмножестве входных векторов из 1000 возможных, и затем тестировалась на оставшихся.

Из табл. 3 следует, что АСК извлекает скрытые закономерности достаточно точно (рис. 6). В среднем создается 18 правил на обучающем наборе из 900 входных векторов.

Для исследования сеть инициализируется подмножеством правил из БЗ, затем обучается и тестируется также, как и в предыдущем эксперименте. После инициализации АСК набором из 5 правил качество классификации составляет только 10,4% на наборе тестовых данных.

Алгоритм уточнения правил (rule refinement) значительно повышает способность сети к распознаванию уже на 100 векторах обучающей выборки. При инициализации АСК набором из 15 правил успешно классифицируются 80,4% тестовых данных.

Таблица 2

База знаний для сопоставления угрозам известных методов защиты

	Атрибуты	База знаний в виде правил
Возможные угрозы	X1 Отказ в обслуживании X2 Хищение информации X3 Присвоение личности X4 Модификация информации X5 Попытка взлома пароля пользователя X6 Вирусная атака X7 Поиск остаточной информации X8 Несанкционированный запуск программ X9 Изменение конфигурации СЗИ X10Несанкционированное уничтожение данных X11 Несанкционированное открытие файлов	R1: IF (X1, Z2, Z7) THEN Y2; R2: IF (X1, Z2, Z7) THEN Y2; R3: IF (X2, Z4, Z7) THEN Y2; R4: IF (X3, Z4) THEN Y8; R5: IF (X4, Z1) THEN Y4; R6: IF (X5, Z3) THEN Y6; R7: IF (X6, Z1) THEN Y3; R8: IF(X7,Z4,Z5,Z6,Z7) THEN Y5; R9: IF (X8, Z4) THEN Y1; R10: IF (X9,Z1) THEN Y8; R11: IF (X10, Z5) THEN Y7; R12: IF (X11, Z4, Z7) THEN Y2; R13: IF (X11, Z5) THEN Y7; R14: IF (X11, Z4, Z7) THEN Y2; R15: IF (X5, Z7) THEN Y2; R16: IF (X11,X8,X5,Z5,Z7) THEN Y10; R17: IF (X3, X9, Z4) THEN Y9
Состояния системы	Z1 Установленное ПО и обновления к нему Z2 В системе присутствуют сетевые сервисы Z3 Система поддерживает многозадачность Z4 Поддержка многопользовательского режима Z5 Установлены устройства ввода/вывода Z6 Наличие устройств горячей замены Z7 Наличие внешних каналов связи	
Методы противодействия	Y1 Идентификация и аутентификация Y2 Блокирование бесконтрольного доступа Y3 Защита от вирусов Y4 Контроль целостности данных Y5 Уничтожение остаточных данных Y6 Защита программ от исследования Y7 Резервирование информации Y8 Восстановление и самовосстановление Y9 Проверка сертификата безопасности Y10 Блокировка запуска программ	

В процессе обучения АСК формирует 2 правила и классифицирует 100% тестовых данных.

E1 : IF (X5, X11, Z5, Z7) THEN Y10 E2 : IF (X9, Z4) THEN Y9

Правило E1 соответствует правилу R16, а E2 является обобщением пропущенного правила R17.

Таблица 3

Качество классификации АСК (усредненный результат по 10 запускам программы)

НС	Обучающая/тестовая выборки	Эпох обучения	Категории (правила)	Распознано (%)
Cascade ARTMAP без инициализации правилами (Fuzzy ARTMAP)	100/900 500/500 900/100	2,2 2,6 2,4	13,4 17,1 18,2	95,3 97,9 99,7
6 правил без обучения Cascade ARTMAP с 6 правилами (R1 – R3, R12 – R15)	0/1000 100/900 500/500 900/100	0 2,2 2,2 2,3	5 13 18,4 19,4	10,4 96,2 99,3 99,9

(Продолжение табл. 2)

10 правил без обучения Cascade ARTMAP с 10 правилами (R1 – R5, R11 – R15)	0/1000 100/900 500/500 900/100	0 2,2 2,2 2,2	10 14 18 17,4	37,4 96,7 99,4 100,0
15 правил без обучения Cascade ARTMAP с 15 правилами (за исключением R16, R17)	0/1000 100/900 500/500 900/100	0 2,0 2,0 2,0	15 15 17 17	80,4 98,7 100,0 100,0

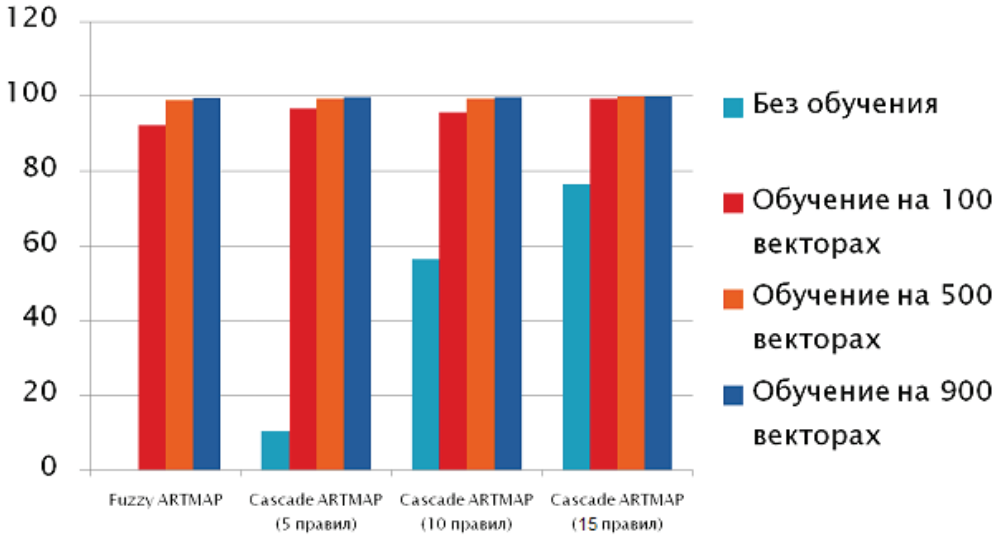


Рис. 6. Влияние предобучения на качество классификации АСК

ВЫВОДЫ

Из проведенного исследования следует, что использование сетей теории адаптивного резонанса, в частности Cascade ARTMAP, является перспективным для применения в составе СЗИ.

Реализация в инкрементных классификаторах ART процедуры сокращения малозначащих и повторяющихся кластеров позволяет увеличить производительность построенных на их основе адаптивных средств защиты информации как в режиме работы, так и в процессе обучения, а, следовательно, в полной мере реализовать режим функционирования СЗИ, близкий к реальному масштабу времени.

Благодаря тому, что Cascade ARTMAP сохраняет символьное представление правил, извлеченные правила сохраняют форму и могут быть непосредственно сопоставлены с оригиналом. Кроме того, фактор доверия, ассоциированный с каждым правилом, дает возможность более тонкой настройки НС.

СПИСОК ЛИТЕРАТУРЫ

1. Нестерук Г.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов / Г.Ф. Нестерук, Л.Г. Осовецкий, А.Ф. Харченко.– СПб.: Изд-во СПбГУЭФ, 2003
2. Адаптивные средства обеспечения безопасности информационных систем / Ф.Г. Нестерук, А.В. Суханов, Л.Г. Нестерук, Г.Ф. Нестерук. – СПб.: Изд-во Политех. универ., 2008.
3. Carpenter G. A., Grossberg S., & Reynolds J. H. ARTMAP: Supervised Real-Time Learning and Classification of Nonstationary Data by a Self-Organizing Neural Network // Neural Networks, 4, 1991
4. Salom T., Bersini H. An algorithm for self-structuring neural net classifiers // Proc. 2nd IEEE Conf. On Neural Network (ICNN'94), 1994
5. Negnevitsky M. Artificial intelligence: a guide to intelligent systems. - Addison-Wesley, 2002
6. Tan A.-H. Cascade ARTMAP: Integrating Neural Computation and Symbolic Knowledge Processing. // IEEE Trans.on Neural Networks, 1997, vol. 8, n.2
7. Granger E., Rubin M. A., Grossberg S., Lavoie P. A what-and-where fusion neural network for recognition and tracking of multiple radar emitters, Neural Networks, vol. 3, 2001

8. Carpenter G. A. and Tan A.-H. Rule extraction: From neural architecture to symbolic representation. // Connection Science, 1995, 7(1)
9. Bharadwaj M. Semi-Supervised Learning in Exemplar Based Neural Networks // A thesis submitted of the requirements for the degree of Master of Science in the Department of Electrical and Computer Engineering in the College of Engineering at the University of Central Florida, Orlando, Florida. 2003
10. Carpenter G.A., Grossberg S., Markuzon N., Reynolds J.H., Rosen D.B. Fuzzy ARTMAP: An adaptive resonance architecture for incremental learning of analog maps. // Proc. of the Int. Joint Conf. on Neural Network. 1992
11. Татаринов А.Ю. Исследование и разработка нейросетевых средств классификации для систем защиты информации / А.Ю. Татаринов: Дипломная работа – СПб.: СПбГУ ИТМО, 2010.
12. Zhou Z., Chen S., Chen Z. FANNC: A Fast Adaptive Neural Network Classifier. // Knowledge and Information Systems. 2000.

Надійшла до редакції 21.11.2010р.

НЕСТЕРУК ФИЛИПП ГЕННАДЬЕВИЧ – к.т.н, старший научный сотрудник научно-исследовательского отдела проблем информационной безопасности СПИИРАН, Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН), г. Санкт-Петербург, Российская Федерация, тел.: (+7)(812)328-51-85, E-mail: nest_pg@mail.ru .

ТАТАРИНОВ АЛЕКСЕЙ ЮРЬЕВИЧ - студент кафедры «Безопасные информационные технологии» СПбГУ ИТМО, Санкт-Петербургский государственный университет информационных технологий, механики и оптики (СПбГУ ИТМО), г. Санкт-Петербург, Российская Федерация, тел.: +7(812) 233 86 51, E-mail: gore00@gmail.com .

НЕСТЕРУК ГЕННАДИЙ ФИЛИППОВИЧ – д.т.н., доцент, профессор кафедры системного программирования СПбГУ, Санкт-Петербургский государственный университет (СПбГУ), г. Санкт-Петербург, Российская Федерация. тел.: +7(812)-428-71-09, E-mail: nest_g_p@yahoo.com