

Д.Н. БИРЮКОВ
**АССОЦИАТИВНО-РЕФЛЕКТОРНАЯ ПАМЯТЬ
КИБЕРСИСТЕМЫ ДЛЯ СИНТЕЗА УПРЕЖДАЮЩИХ
РЕАКЦИЙ, НЕЙТРАЛИЗУЮЩИХ ВРЕДНОСНЫЕ
ВОЗДЕЙСТВИЯ**

Бирюков Д.Н. Ассоциативно-рефлекторная память киберсистемы для синтеза упреждающих реакций, нейтрализующих вредоносные воздействия.

Аннотация. В статье предлагается подход к построению и применению ассоциативно-рефлекторной памяти киберсистемы, способной формировать сценарии упреждающего поведения на уровне условных рефлексов.

Ключевые слова: киберсистема, иерархическая временная память, упреждение, условный рефлекс.

Biryukov D.N. **Associative-Reflex Memory of Cybersystem for Synthesis of the Anticipatory Reactions Neutralizing Harmful Influences.**

Abstract. The article shows the approach to construction and use of associative-reflex memory of the cybersystem capable to form scenarios of anticipatory behavior at the level of conditioned reflexes.

Keywords: cybersystem, Hierarchical Temporal Memory, anticipation, conditioned reflex.

1. Введение. В настоящее время пока не разработано единой модели памяти человека, но попытки смоделировать частные аспекты ее функционирования осуществляются все чаще. Так, например, заслуживает внимания частная модель мозга, разработанная Джеффом Хокинсом и Дилипом Джоржом (Numenta, Inc.), которая моделирует некоторые структурные и алгоритмические свойства неокортекса и называется «Иерархическая Временная Память» (Hierarchical Temporal Memory – НТМ) [1]. Неокортекс составляет у человека основную часть коры головного мозга и отвечает за сенсорное восприятие, выполнение моторных команд, осознанное мышление и речь.

НТМ – это система памяти, которая, по заявлению создателей [1], не программируется и не учится алгоритмическому выполнению задач, а «учится» решать проблему в зависимости от данных, подаваемых на сенсоры. Как видится, данная способность системы может быть весьма полезной при организации механизмов формирования условных рефлексов у киберсистемы предотвращения атакующих воздействий на защищаемые информационно-технические ресурсы.

2. Основные положения модели НТМ. Все области коры мозга выглядят похожими друг на друга по своему внутреннему строению, но весьма сильно варьируются по своему размеру и по своему месту в иерархии. Если взять их срез высотой в два миллиметра, то можно обнаружить шесть слоев - пять слоев клеток и один без них (из этого правила есть несколько исключений, но в общем оно соблюдается).

Каждый из нейронных уровней областей коры мозга имеет множество взаимосвязанных клеток, организованных в колонки. Также и регионы НТМ представляют собой слои сильно взаимосвязанных клеток, также организованных в колонки.

Хотя нейроны в коре мозга очень плотно связаны между собой, многочисленные подавляющие нейроны гарантируют, что одновременно будет активен только небольшой процент всех нейронов. То есть, получается, что информация представляется в мозге всегда только небольшим количеством активных нейронов из всех имеющихся. Такой тип кодирования информации называется «разреженное распределенное представление» [1].

Далее предлагается более подробно остановиться на принципах функционирования НТМ.

Первое и наиболее важное – это обучение. Регион НТМ изучает «Внешний Мир» (ВМ) путем нахождения паттернов и их последовательностей во входном потоке данных. Регион, сам по себе, «не знает», что собой представляют эти данные, он работает на статистических принципах, определяя комбинации входных битов, которые часто появляются вместе, и которые называются пространственными паттернами. Потом регион ищет, как эти паттерны образуют последовательности во времени, что называют временными паттернами или просто последовательностями [1]. НТМ способна к непрерывному обучению во время работы. Поэтому нет необходимости в отделении фазы распознавания от фазы обучения, хотя распознавание заметно улучшается при дополнительном обучении.

После того как НТМ выучила паттерны из изучаемой предметной области, она может проводить распознавание новых входных данных. При получении очередного входа НТМ будет сопоставлять его выученным ранее пространственным и временным паттернам.

Важным в распознавании, осуществляемым НТМ, является то, что НТМ позволяет распознавать входные данные, несколько отличающиеся друг от друга, это становится возможным как раз из-за использования разреженных пространственных представлений входных данных в НТМ, что приводит к достаточности сопоставления только некоторой части паттерна, чтобы быть уверенным в существовании всего совпадения.

Каждый регион НТМ хранит в себе последовательности паттернов. Путем их сопоставления с текущими входными данными, регион формирует предсказание насчет своего вероятного следующего входа. Регионы НТМ хранят в себе переходы между распределенными пространственными представлениями. При этом регион НТМ делает раз-

личные предсказания, основываясь на контексте, который в свою очередь может охватывать множество событий и явлений.

Еще одним положительным эффектом работы НТМ на этапе предсказания является то, что когда НТМ предсказывает, что будет дальше, это предсказание может повлиять на распознавание всей системой того, что было предсказано. Т.е., система в состоянии заполнить пропущенные или искаженные данные, поступающие от сенсоров, так как система находится в состоянии ожидания определенных данных и по контексту зачастую может восполнить пропущенные или искаженные данные.

Всю работу НТМ можно разделить на следующие три основных шага: (1) формирование в регионе НТМ пространственного распределенного представления входных данных; (2) формирование представления входных данных в контексте предыдущих входов; (3) формирование предсказания региона НТМ на основе текущего входа в контексте предыдущих входов.

Далее предлагается рассмотреть каждый из этих шагов более подробно.

1) Формирование пространственно распределенного представления входа. Первым делом регион НТМ конвертирует свой вход в пространственное разреженное представление. Регион НТМ логически состоит из множества *колонок*. Каждая колонка состоит из одной или более клеток (аналогов биологических нейронов). Совокупность колонок региона можно представлять в виде некоторого двухмерного массива. Каждая колонка в регионе воспринимает свою уникальную область входных битов (обычно они перекрываются между собой, но никогда полностью не совпадают для двух разных колонок). В результате, различные паттерны на входе региона приводят к активации различных колонок региона. При этом колонки с более высоким уровнем активации подавляют (ингибируют) близлежащие колонки с меньшим уровнем активации в определенном (изменяемом) радиусе.

Процесс подавления можно пояснить на простом примере. Например, человек ожидает наступления определенного события, но ожидаемое событие может принадлежать одному из альтернативных классов. В этом случае целый ряд клеток находится в состоянии предсказания. С наступлением конкретного события, активными становятся только часть клеток, совпавших с предсказываемым событием, а остальная часть клеток деактивируется.

Распределенное представление текущих входных сигналов кодируется тем, какие колонки являются активными, а какие нет, после

описанной деактивации. На рисунке 1 показана часть региона с примером представления пространственно распределенного входа.

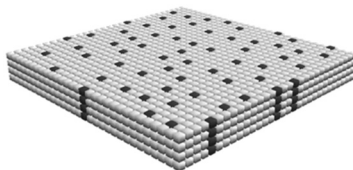


Рис. 1. Часть региона НТМ после активации колонок пространственно распределенным входом

2) *Формирование представления входа в контексте предыдущих входов.* Следующая функция, которую выполняет регион НТМ, конвертирует описанное колончатое представление текущего состояния входа региона в новое представление, которое включает в себя состояния региона из прошлого (или контекст). Это новое представление формируется путем активации только некоторого подмножества клеток из каждой колонки, при этом, обычно, это будет только одна клетка из всей колонки.

Каждая колонка в регионе НТМ состоит из нескольких клеток. И каждая из клеток может быть активной или пассивной. Выбирая различные активные клетки в каждой активной колонке, возможно по-разному представить один и тот же вход региона в различных контекстах.

Когда колонка становится активной, она активирует в себе все клетки, если данный вход был для нее неожиданным (не предсказанным в ней самой заранее). Но если некоторые из клеток колонки уже находились в состоянии предсказания (см. рисунок 2), то активными будут только они, а остальные – нет.

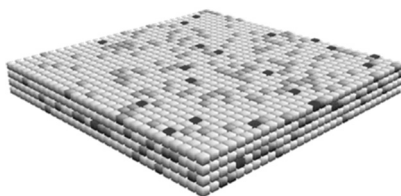


Рис. 2. Регион НТМ, отражающий память с контекстом, и находящийся в режиме ожидания (предсказания)

Путем активации некоторого подмножества клеток в каждой активной колонке, регион НТМ может отобразить (представить) один и

тот же вход в различных контекстах. Все колонки активируют в себе только предсказывающие клетки. Колонки без таких клеток активируют все свои клетки. На рисунке 3 показано несколько колонок с одной активной клеткой и колонка со всеми активными клетками.

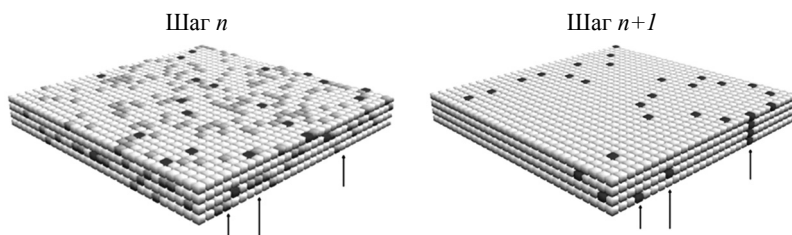


Рис.3. Пример активации нейронов

Если клетка активна благодаря прямому воздействию на нее входных сигналов, то ее называют «активной». Если же клетка стала активна благодаря своим латеральным связям с соседними клетками, то она находится в состоянии «предсказания».

3) *Формирование предсказания на основе входа и контекста предыдущих входов.* Финальным шагом алгоритма для региона является выработка предсказания того, что должно произойти далее. Это предсказание вырабатывается на основе представления, сформированного на шаге 2, которое включает в себя и контекст от предыдущих входов. Когда регион создает такое предсказание, он активирует все клетки, которые вероятно станут активными благодаря последующему прямому воздействию (в одно и то же время может быть сделано несколько предсказаний).

Когда входной паттерн изменяется с течением времени, различные наборы колонок и клеток становятся последовательно активными. А когда любая клетка становится активной, то она формирует соединения с подмножеством клеток, которые были активны непосредственно до этого. После этого, все, что нужно сделать клетке, это отследить по этим сформированным связям совпадающую во времени активность. Если эти соединения вдруг стали активны, то клетка может предположить, что она тоже вскоре может стать активной (как это уже было ранее), и она переходит в состояние предчувствия своей активации. В любой момент времени некоторые клетки региона НТМ будут активны благодаря прямому воздействию входных сигналов (показаны темно-серым цветом на рисунке 2). При этом другие клетки, получающие латеральные воздействия от активных клеток, будут переходить в состоянии предсказания (показаны светло-серым цветом). Ито-

говым выходом всего региона является активность всех его клеток (как из-за прямых воздействий, так и из-за латеральных).

3. Модель представления данных в ассоциативно-рефлекторной памяти проектируемой киберсистемы с учетом наблюдаемых контекстов. Для хранения данных в рамках ассоциативно-рефлекторной памяти [2] и работы с ними, предлагается использовать некоторые положения, представленные в модели НТМ [1].

В основе работы НТМ заложена идея использования совокупности определенным образом организованных нейронов. Именно система нейронов участвует в процессе восприятия данных, поступающих из «Внешнего Мира» (ВМ), накоплении этих данных, их обработки и порождения ответных реакций.

Окружающий познающую систему «Внешний Мир» состоит из процессов. Каждый процесс состоит из совокупности событий (событие – то, что происходит в некоторый момент времени и рассматривается как изменение состояния мира). Отдельное событие может быть распознано по одному, а чаще по ряду обнаруженных и измеренных свойств события. Для измерения свойств наблюдаемых событий применяются сенсоры. Чем более разнообразны и точны сенсоры, тем более точно можно регистрировать наблюдаемые события, а следовательно, в дальнейшем, и более точно их распознавать.

Для дальнейшего изложения следует определить, что совокупность сенсоров функционирует дискретно и позволяет строить последовательность «кадров» наблюдаемого «Внешнего Мира» (далее – Сенсорные Кадры (СК)). Для хранения СК и работы с ними, предлагается использовать модифицированную модель НТМ.

Последовательность СК, формируемых на выходе сенсоров, необходимо хранить, чтобы сформировать и развивать сенсорную память. Следует заметить, что СК может формироваться сенсорами различных типов, т.е. в одном СК могут быть отражены сразу несколько свойств наблюдаемого события. Это приводит к тому, что формируемый СК представляет собой совокупность взаимосвязанных (ассоциируемых) концептов.

Важным элементом для работы сенсоров в связке с памятью является время, так как время играет критически важную роль в обучении, распознавании и предсказании. Чтобы проектируемая система могла обучаться (накапливать опыт о наблюдаемых событиях), ей нужно подавать переменный во времени поток данных – меняющиеся СК. Запоминание и распознавание последовательностей СК является основой для выработки предсказаний на уровне функционирования ассоциативно-рефлекторной памяти. После того как система (память)

выучит какие паттерны скорее всего следуют за какими, она сможет предсказывать появление следующих паттернов на основе предыдущих и текущих входных данных.

Основным, на что хотелось бы обратить внимание при моделировании ассоциативно-рефлекторной памяти (АРП) является то, что именно АРП должна позволять формировать условные рефлексы (УР). В основе формирования УР должно лежать обучение. Система с реализованной в ней АРП должна быть способной изучать «Внешний Мир» (ВМ) путем нахождения паттернов и их последовательностей во входном потоке данных. Очевидно, что система не всегда способна интерпретировать (семантически осмыслить) поступающие данные, что, однако, не должно мешать ей запоминать последовательности СК во времени. Подобно биологическим системам, проектируемая интеллектуальная система должна быть способной к обучению «на лету», то есть к непрерывному обучению в ходе регистрации каждого СК.

Таким образом, память системы должна хранить в себе последовательности паттернов. И путем их сопоставления с текущими входными данными, АРП должна формировать предсказание насчет вероятного следующего входа. На самом деле система должна хранить в себе переходы между распределенными пространственными представлениями входных данных, поскольку СК, как было указано выше, представляет собой совокупность взаимосвязанных концептов (каждый из которых также может быть представлен пространственно распределенным паттерном). В некоторых случаях эти переходы могут выглядеть как линейные последовательности, но в общем случае, в один момент времени, может быть предсказано много вероятных последующих входов. При этом система должна делать различные предсказания, основываясь на текущем контексте событий, который может простираться далеко в прошлое. Основная часть АРП должна отводиться именно хранению переходов между пространственными паттернами, которые (переходы) можно интерпретировать как «далее следует».

Пусть $SK(\tau_i)$ – данные, поступающие на вход системы через систему сенсоров в момент времени τ_i . При этом τ_i – относительное время регистрации Сенсорного Кадра (время задает порядок следования СК через параметр i).

$X(\tau_i) = \langle x_1(\tau_i), x_2(\tau_i), \dots, x_n(\tau_i) \rangle$ – паттерн СК, зарегистрированного от системы сенсоров в момент времени τ_i .

Элемент паттерна $x_l(\tau_i)$, зарегистрированного в момент времени τ_i , может быть связан с элементом паттерна $x_m(\tau_{i+1})$, зарегистрированного в момент времени τ_{i+1} , ролью с семантическим обозначением «далее следует».

$H(\tau_{i+1}) = H(H(\tau_i), X(\tau_i)) = \bar{X}(\tau_{i+1})$ – функция прогноза СК (через прогнозируемый паттерн) с учетом контекста (с учетом ранее зарегистрированных СК). В основу данной функции может быть положена, например, Хеш-функция.

$\bar{X}(\tau_{i+1}) = \langle \langle x_1(\tau_{i+1}), h_1 \rangle, \langle x_2(\tau_{i+1}), h_2 \rangle, \dots, \langle x_n(\tau_{i+1}), h_n \rangle \rangle$ – паттерн, который прогнозируется получить в момент времени τ_{i+1} с учетом контекста.

$h_i \in \{1, \overline{N}\}$, где N – максимальное количество возможных различных интерпретаций x_i с учетом различных контекстов, а само значение h_i задает номер интерпретации.

$ars = ARS(X(\tau_i), X(\tau_{i+1}))$ – сила ассоциации двух явлений, наблюдаемых последовательно.

ars_{\min} – минимальное значение ars , при котором осуществляется распространение ассоциативного сигнала по ассоциативной сети, функционирующей в рамках ассоциативно-рефлекторной памяти.

Тогда обобщенную схему прогнозирования паттернов в рамках ассоциативно-рефлекторной памяти можно представить следующим образом: см. рисунок 4.

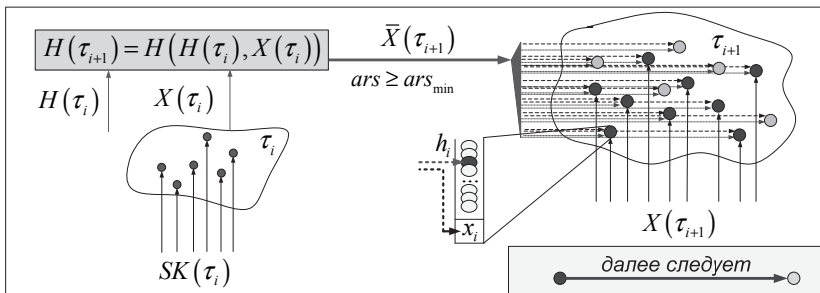


Рис. 4. Обобщенная схема прогнозирования паттернов в АРП

4. Модель функционирования ассоциативно-рефлекторной памяти в ходе порождения спецификаций предупреждающих реакций. Все указанное в работе [1] относительно НТМ может быть полезно для организации работы с контекстами, для работы в условиях шума и пропусков, а также, возможно, для реализации в той или иной мере способности системы к обучению и предсказанию. Стоит однако отметить, что настроить подобную систему до этапа ее непосредственной эксплуатации по назначению, как видится, достаточно сложно, а если система сложная, как система обеспечения информационной безопасности (ИБ), то скорее и вовсе невозможно, так как описание всех связей между многочисленными нейронами практически нереализуемо.

НТМ не предполагает самообучение при отсутствии входных данных от сенсоров, а данная способность просто необходима для интеллектуальных систем. Так, человек способен самостоятельно строить нейронные связи, но естественно при этом процессе он оперирует не нейронами и связями, а воображаемыми событиями, образами, процессами и т.п. Манипуляции с воображаемыми отдельными событиями и целыми процессами человек осуществляет при ретроспективной и перспективной рефлексии. Поэтому предлагается надстроить более высокий уровень в иерархии регионов, содержащий данные о событиях и их последовательностях, т.е. о процессах (см. рисунок 5). Далее его предлагается называть «Уровень Процессов» (УП).

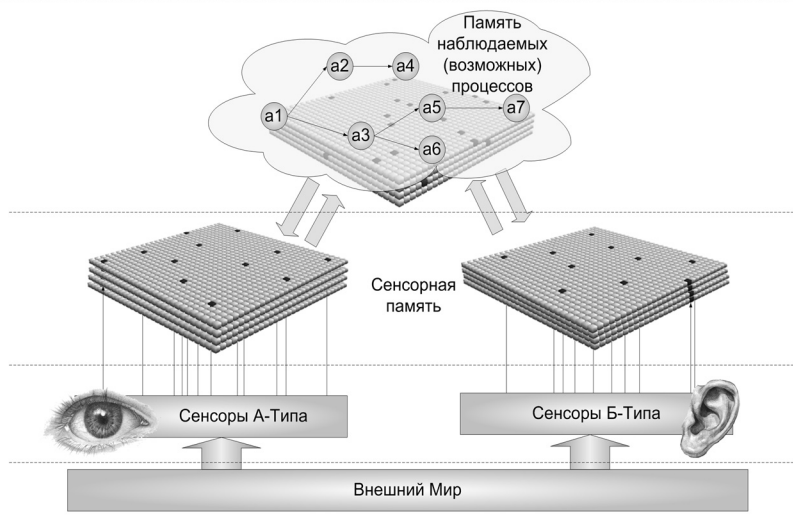


Рис. 5. Связь УП с уровнем, реализующим сенсорную память

На УП система должна быть в состоянии строить деревья возможных процессов, опираясь на предыдущий опыт и правила построения процессов. Также на УП на все множество процессов должны накладываться ограничения, порождаемые спецификой предметной области, знанием о сенсорах и эффекторах (т.е. об их возможностях и недостатках), решаемыми системой задачами и т.п. После того, как на УП построится определенный фрагмент наблюдаемого процесса, система должна выбрать на него ответную реакцию. Ответная реакция может выбираться как на основе предыдущего опыта, так и на основе анализа возможных реакций, описание которых построено в ходе рефлексии системы. Процесс – ответная реакция далее должен активировать выполнение последовательности действий эффекторами.

Таким образом, предлагается представить взаимодействие УП, содержащего последовательность предполагаемых действий, с эффекторами так, как это представлено на рисунке 6.

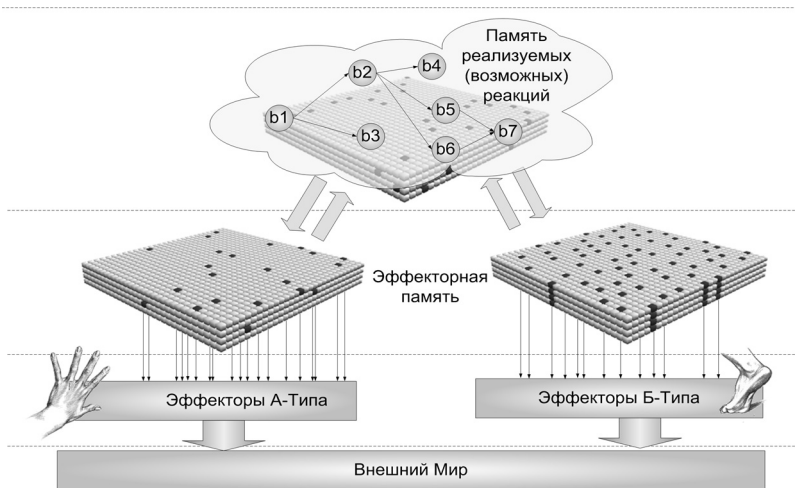


Рис. 6. Настройка уровня, содержащего данные о реализуемых (возможных) реакциях системы

Далее предлагается замкнуть работу сенсоров с работой эффекторов через соответствующие регионы на УП и через “Синтезатор” [3].

На долю “Синтезатора” предлагается отнести задачи, связанные с интеллектуальной обработкой наблюдаемых процессов из ВМ и формированием обоснованных реакций, оформленных в виде совокупности действий, реализуемых имеющимися эффекторами, и направленных либо на изменение ВМ, либо на изменение самой систе-

мы, осуществляемое через эффекторы. Однако решение указанных задач относится уже к работе ассоциативно-семантической памяти (АСП), которая должна быть рассмотрена отдельно и более детально.

Исходя из уже описанного, уровни функционирования памяти информационно-технической системы, обладающей свойством антиципации, могут быть представлены следующим образом – см. рисунок 7: область (I) обозначена область принятия решений на уровне АРП, а область (II) – на уровне АСП.

Для пояснения схемы, представленной на рисунке 7, предлагается рассмотреть обобщенную методику функционирования абстрактной киберсистемы, обладающей свойствами антиципации.



Рис. 7. Уровни функционирования памяти киберсистемы, обладающей свойством антиципации

Ниже приводятся основные этапы функционирования системы, основанные на применении механизмов, реализованных на уровне ассоциативно-рефлекторной памяти. Поскольку функционирование АРП также связано и с функционированием ассоциативно-семантической памяти (на уровне “Синтезатора”), то предлагается отразить и эту взаимосвязь. Тогда функционирование ассоциативно-рефлекторной памяти в ходе порождения спецификаций упреждающего поведения можно представить в виде нижеприведенной последовательности мероприятий.

1. Система воспринимает окружающий “Внешний Мир” и себя через конечную совокупность сенсоров различного, но определенного типа.

– Сенсоры регистрируют свойства событий, происходящих во ВМ и в самой системе (очевидно, что не все события и их свойства известны системе априорно).

– Регистрируемые свойства событий представляются в виде Сенсорных Кадров, помещаемых в аналог Иерархической Временной Памяти.

– СК представляют собой разреженную совокупность активных нейронов, располагающихся в различных Регионах АРП.

– Меняющиеся во времени СК, поступающие от сенсоров, позволяют построить связи между последовательно активизируемыми нейронами, что в свою очередь обуславливает организацию сенсорной памяти.

– Регионы АРП, с которыми связаны сенсоры, имеют связь с Регионами АРП, с которыми связаны эффекторы. Эта связь необходима для организации взаимодействия между нейронами, активируемыми раздражителями из ВМ, и нейронами, которые связаны с эффекторами, через которые система в состоянии оперативно реагировать на эти раздражители (данная связь между регионами АРП сенсоров и регионами АРП эффекторов позволяет реализовать механизм безусловных рефлексов системы).

2. Совокупность СК, построенных в регионах АРП сенсоров, сопоставляется с конкретными событиями, информация о которых хранится на более высоком уровне АРП – на уровне наблюдаемых и теоретически возможных процессов (УП), либо оформляется в виде нового события на УП.

– Совокупность сенсорных кадров через систему нейронных связей активирует распределенные нейроны на УП, содержащие данные об обнаружении конкретного события. Если регулярно появляющаяся совокупность СК не может быть соотнесена с конкретным событием из ВМ, то на УП формируется новое событие.

– Меняющиеся во времени события, отражаемые в нейронах УП, позволяют построить связи между последовательно активизируемыми нейронами, что в свою очередь обуславливает организацию памяти на уровне последовательностей событий.

3. Система определяет то, каким образом необходимо реагировать на события, регистрируемые ею через систему сенсоров.

– Регионы АРП, с которыми связаны СК, имеют связь с Регионами АРП, в которых реализована память о том, каким образом (на уровне процессов) нужно реагировать на происходящие события. Эта связь необходима для организации взаимодействия между нейронами, содержащими данные о наблюдаемых системой процессах, и нейрона-

ми, хранящими данные о том, какие действия необходимо предпринять для достижения системой желаемого ею будущего состояния (правильная конфигурация данного взаимодействия нейронов позволит как предугадывать следующее за текущим событием из ВМ, так и активировать соответствующие нейроны, отвечающие за управление эффекторами, деятельность которых направлена на предотвращение ожидаемого события).

– Возможные последовательности возможных событий, наблюдаемых системой, также как и возможные последовательности возможных реакций, могут строиться как на основе опыта системы, так и на основе результатов, полученных «Синтезатором». И в том и в другом случае результатом будет построение определенных связей между нейронами и регионами нейронов в системе Памяти киберсистемы.

4. Система воздействует на ВМ или изменяет свою конфигурацию, осуществляя определенные действия эффекторами.

– Регионы памяти, в которых хранится информация о возможном поведении системы, имеют связь с Регионами памяти, в которых реализована эффекторная память. Эта связь необходима для того, чтобы система была в состоянии активизировать последовательность Эффекторных Кадров (ЭК), инициирующих определенным образом имеющиеся эффекторы, для выполнения того действия, которое было выбрано системой в ответ на события, регистрируемые сенсорами и представленные в виде событий в Регионе с сенсорной памятью, либо на события, прогнозируемые сенсорной памятью.

– Эффекторы воздействуют/не воздействуют на «Внешний Мир» и/или саму систему для достижения желаемого будущего системой.

5. Важным элементом интеллектуальной информационно-технической системы, обладающей свойствами антиципации, является «Синтезатор», который:

– осуществляет анализ цепочек регистрируемых событий,
– строит цепочки событий потенциально реализуемые во «Внешнем Мире» и относящиеся к рассматриваемой предметной области,

– накладывает ограничения на возможные цепочки событий, исходя из решаемых системой задач и априорных знаний о правилах протекания процессов во ВМ,

– осуществляет анализ действий системы и их последовательностей, осуществляемых системой ранее, либо заложенных на этапе ее проектирования,

– строит цепочки действий, потенциально реализуемые системой,

– накладывает ограничения на возможные цепочки действий системы, исходя из решаемых ею задач и априорных знаний о правилах протекания процессов во ВМ,

– сопоставляет наблюдаемые и возможные процессы во «Внешнем Мире» с последовательностью возможных действий системы,

– организует нейронные связи между регионами памяти, содержащими данные о наблюдаемых событиях из ВМ, и регионами, содержащими последовательности потенциально реализуемых действий системы, направленных на достижение желаемого системой будущего.

Таким образом, как можно увидеть из выше приведенного описания, киберсистема, способная осуществлять синтез сценариев упреждающего поведения в ходе предотвращения атакующих воздействий на защищаемые ресурсы, должна быть способной моделировать упреждающее поведение на двух основных уровнях: на уровне АРП и АСП (как указывалось ранее [2]).

5. Метод синтеза сценариев упреждения на основе ассоциативно-рефлекторного поведения. Одним из основных этапов процесса синтеза сценариев упреждения является этап прогнозирования [3,4]. Процесс формирования прогноза на уровне ассоциативно-рефлекторного поведения состоит из этапов, в ходе выполнения которых осуществляется:

– получение информации о входных паттернах, которые были зарегистрированы ранее – на предыдущих этапах функционирования системы (при этом глубина ретроспективы может быть различной, и зависит от необходимой точности учета контекста);

– получение данных о сформированном входном паттерне: $X(\tau_i)$;

– формирование прогноза относительно паттерна (паттернов), который ожидается получить в следующий момент времени с учетом имеющегося контекста и полученных данных ($\bar{X}(\tau_{i+1})$), а также учитывая силу ранее выработанных ассоциативных связей (*ars*);

– получение Сенсорного Кадра от Системы Сенсоров и преобразование его во входной паттерн: $X(\tau_{i+1})$;

– сравнение результатов прогноза с полученными данными; если элемент паттерна совпал с прогнозируемым элементом ($\langle x_i(\tau_{i+1}), h_i \rangle$), то активируется только прогнозируемый элемент (у массива x_i активируется элемент, относящийся к интерпретации h_i), если элемент вход-

ного паттерна не совпал с прогнозируемым элементом, то активируется весь массив, совпадающий с входным элементом паттерна;

- деактивация прогнозированных, но не активированных входным паттерном элементов;
- укрепление ассоциативных связей между элементами, которые активировались в следующие друг за другом промежутки времени.

На рисунке 8 приведена одна итерация применения метода построения прогноза Сенсорных Кадров (входных паттернов), которые могут поступить на вход через Систему Сенсоров. Осуществление прогноза – это только один аспект ассоциативно-рефлекторного поведения, лежащего в основе упреждения. Вторым важным аспектом, лежащим в основе упреждения, построенного на уровне ассоциативно-рефлекторного поведения, является возможность осуществлять само-модификацию и изменение объектов во «Внешнем Мире».

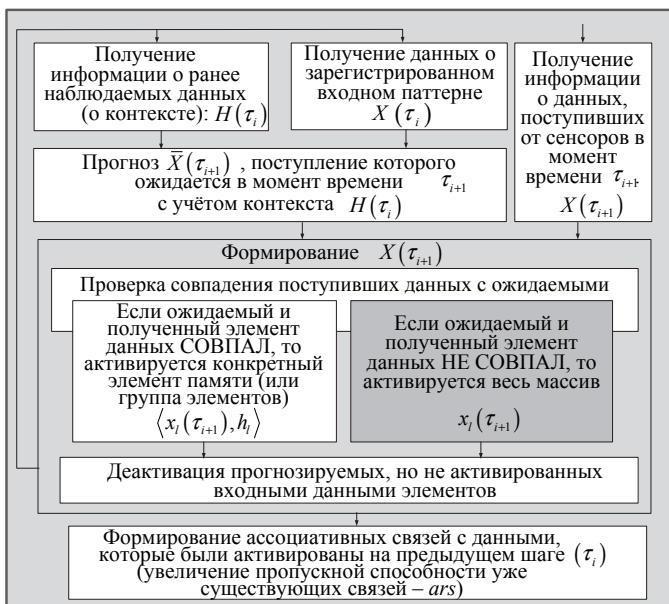


Рис. 8. Итерация метода построения прогноза наблюдаемых Сенсоров Кадров (входных паттернов)

Для того чтобы воспринимаемые данные смогли инициировать определенные выходные реакции, паттерны, которые формируются по результатам восприятия СК, должны быть связаны с паттернами, формирующими конкретные Эффекторные Кадры, которые осуществляют

управление Системой Эффекторов, способной оказывать преобразующие воздействия на «Внешний Мир» и саму систему. Эта связь необходима для организации взаимодействия между областью памяти, содержащей данные о наблюдаемых системой процессах, и областью памяти, хранящей данные о том, какие действия необходимо предпринять для достижения системой желаемого будущего состояния (правильная конфигурация данного взаимодействия позволит как предугадывать следующее за текущим событие из ВМ, так и активировать соответствующие паттерны, отвечающие за управление эффекторами, деятельность которых направлена на предотвращение ожидаемого события).

Следует заметить, что не все системы могут самостоятельно «обучиться» во время своего непосредственного функционирования. Это может быть связано с тем, что не всякая система сможет «дожить» до состояния обученности, либо процедура самообучения может быть непомерно дорогой или долгой. Ввиду этого, подход, предложенный в [1], не всегда применим для его практической реализации и требует доработки, связанной, например, с учетом возможности реализации процедур обучения системы без накопления ею опыта через систему сенсоров. Для того чтобы выполнение таких процедур стало возможным, предлагается уже на уровне АРП при описании процессов использовать семантически окрашенные именованные концепты предметной области [5], с которой имеет дело система в процессе своего функционирования. Это позволит оператору не только заранее вносить необходимые связи между паттернами, представляющими Сенсорные и Эффекторные Кадры, но и проверять, а при необходимости и править, выработанные системой в процессе ее функционирования условные рефлексy.

6. Заключение. Предложенный метод синтеза сценариев упреждения, построенный на основе ассоциативно-рефлекторного поведения, может быть положен в основу систем обнаружения и предотвращения вторжений, способных формировать различные ответные реакции на одни и те же атакующие воздействия, зависящие от того, в каких условиях и каким образом атакующие воздействия осуществляютcя, т.е. – в зависимости от контекста.

Литература

1. Иерархическая темпоральная память (HTM) и ее кортикальные алгоритмы обучения. Numenta, Inc. URL: <http://numenta.com/assets/pdf/whitepapers/hierarchical-temporal-memory-cortical-learning-algorithm-0.2.1-ru.pdf> (дата обращения: 18.12.2014).
2. Бирюков Д.Н., Ломако А.Г., Сабиров Т.Р. Многоуровневое моделирование сценариев упреждающего поведения // Проблемы информационной безопасности.

Компьютерные системы. С-Пб.: Издательство Политехнического университета. 2014. №4. С. 41–50.

3. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. С-Пб.: Издательство Политехнического университета. 2013. №2. С. 13–19.
4. *Бирюков Д.Н., Ломако А.Г.* Построение систем информационной безопасности: от живых организмов к киберсистемам // Защита информации. INSIDE. 2013. №2. С. 2–6.
5. *Бирюков Д.Н., Ломако А.Г.* Формализация семантики для представления знаний о поведении конфликтующих сторон // Материалы 22-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”. С-Пб.: Издательство Политехнического университета. 2013. С. 8–11.

References

1. Ierarhicheskaja temporal'naja pamjat' (HTM) i ee kortikal'nye algoritmy obuchenija. [Hierarchical temporal memory (HTM) and its cortical algorithms of training. Numenta, Inc.]. Available at: <http://numenta.com/assets/pdf/whitepapers/hierarchical-temporal-memory-cortical-learning-algorithm-0.2.1-ru.pdf> (accessed 18.12.2014).
2. Biryukov D.N., Lomako A.G., Sabirov T.R. [Multilevel modeling of scenarios of anticipatory behavior]. *Problemy informatsionnoy bezopasnosti. Kompyuternie sistemy – Problems of information security. Computer systems.* SPB: St. Petersburg Polytechnical University 2014. vol. 4. pp. 41–50. (In Russ).
3. Biryukov D.N., Lomako A.G. [Approach to creation of system of cyber-threats preventing]. *Problemy informatsionnoy bezopasnosti. Kompyuternie sistemy – Problems of information security. Computer systems.* SPB: St. Petersburg Polytechnical University 2013. vol. 2. pp. 13–19. (In Russ).
4. Biryukov D.N., Lomako A.G. [Design and construction of information security from living organisms to cybersystems]. *Zashita informatiyi – Data protection. INSIDE.* 2013. vol. 2. pp. 2–6. (In Russ).
5. Biryukov D.N., Lomako A.G. [Formalization of semantics for representation of knowledge of behavior of conflicting parties]. *Materialy 22 nauchno-prakticheskoy konferenciyi “Metody i tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 22nd scientific and practical conference “Methods and Technologies for Information Security Provision”]. SPB: St. Petersburg Polytechnical University 2013. pp. 8–11. (In Russ).

Бирюков Денис Николаевич — к-т техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, защита информации, интеллектуальная поддержка принятия решений. Число научных публикаций — 70. Biryukov.D.N@yandex.ru; ул. Ждановская, д. 13, г. Санкт-Петербург, 197198; p.t.: +7(812) 237-19-60.

Biryukov Denis Nikolaevich — Ph.D., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, IT-Security, intelligent decision support. The number of publications — 70. Biryukov.D.N@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Бирюков Д.Н. **Ассоциативно-рефлекторная память киберсистемы для синтеза упреждающих реакций, нейтрализующих вредоносные воздействия.**

Проведенные исследования показали, что в настоящее время не разработано единой модели памяти человека, но есть отдельные, заслуживающие внимания и доведенные до практических реализаций, наработки. Так, например, для реализации в проектируемой системе возможностей формирования условных рефлексов, предлагается использовать усовершенствованную модель «Иерархической Временной Памяти» (НТМ; Numenta, Inc.).

Представленная в статье модель функционирования ассоциативно-рефлекторной памяти, а также метод синтеза сценариев упреждения на основе ассоциативно-рефлекторного поведения, позволяют реализовать в проектируемой системе способность формировать различные ответные реакции на одни и те же атакующие воздействия, в зависимости от контекста, в котором эти атакующие воздействия осуществляются.

Также предложено уже на уровне ассоциативно-рефлекторной памяти использовать семантически окрашенные именованные концепты предметной области, с которой имеет дело система в процессе своего функционирования. Это должно позволить оператору проверять, а при необходимости и править, выработанные системой условные рефлексы.

SUMMARY

Biryukov D.N. **Associative-Reflex Memory of Cybersystem for Synthesis of the Anticipatory Reactions Neutralizing Harmful Influences.**

The conducted researches showed that now isn't developed uniform model of memory of the person, but is separate, deserving attention and brought to practical realization, an operating time. So, for example, for realization in the designed system of opportunities of formation of conditioned reflexes, it is offered to use advanced model "Hierarchical Temporal Memory" (HTM; Numenta, Inc.).

The model of functioning of associative-reflex memory presented in article, and also method of synthesis of scenarios of anticipation on the basis of associative-reflex behavior, allow to realize ability to form various responses to the same attacking influences, depending on a context in which these attacking influences are carried out in the designed system.

It is already also offered to use at the level of associative and reflex memory semantic painted names of concepts of subject domain with which the system in the course of the functioning deals. It has to allow the operator to check, and if necessary and to govern, the conditioned reflexes developed by system.