computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

КОНЦЕПЦИЯ ГИБРИДНОЙ АДАПТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Игорь Котенко, Филипп Нестерук, Андрей Шоров

Лаборатория проблем компьютерной безопасности СПИИРАН
14 линия, 39, Санкт-Петербург, 199178, Россия
ivkote@iias.spb.su, 08p@mail.ru, ashorov@comsec.spb.ru
http://comsec.spb.ru

Резюме: *в работе предлагается концепция гибридной адаптивной защиты информационно-телекоммуникационных систем на основе биометафоры нервных и нейронных сетей. Верхний уровень системы защиты, основанный на подходе «нервная система сети», базируется на распределенном механизме сбора и обработки информации, который координирует действия основных устройств компьютерной сети, идентифицирует атаки и принимает контрмеры. Реализацию информационных процессов на нижнем уровне предлагается выполнять с привлечением «информационно-полевого» программирования, которое позволяет описывать распределенные информационные поля в виде пакетных нейросетевых программ.*

Ключевые слова: *компьютерная безопасность, гибридная защита, нервная система, нейронные сети.*

CONCEPTION OF A HYBRID ADAPTIVE PROTECTION OF INFORMATION SYSTEMS

Igor V. Kotenko, Filipp G. Nesteruk, Andrey V. Shorov

Laboratory of computer security problems SPIIRAS
39, 14th Liniya, St. Petersburg, 199178, Russia
ivkote@iias.spb.su, 08p@mail.ru, ashorov@comsec.spb.ru
http://comsec.spb.ru/en

Abstract: *The paper suggests the conception of a hybrid adaptive protection of information and telecommunication systems which is based on a biometaphor of nervous and neural networks. A top level of a protection system, based on an approach of "nervous system network" is a distributed mechanism for collecting and processing information. We suggest to implement the information processes on the low level with the assistance of an "information field" programming. It allows specifying the distributed information fields in the form of neural network software packages.*

Keywords: *Data mining, malware, detection.*

1. ВВЕДЕНИЕ

Актуальность проблемы защиты информационных систем, продиктована сложностью программного и аппаратного обеспечения, обуславливающей наличие уязвимостей, прогрессирующей динамикой их развития, распределенной и разнородной структурой и многими другими факторами. Очевидна аналогия между эволюцией и естественным отбором в природе и информационно-телекоммуникационных системах. Живые организмы существуют и эволюционируют, в том числе благодаря совершенной защите от различных угроз, выработанной веками, используя информацию, циркулирующую в их распределенной структуре на основе реализации различных механизмов защиты.

Поэтому представляется, что необходимо наделять системы защиты информации (СЗИ) информационно-телекоммуникационных сетей эволюционными свойствами, присущими биосистемам, такими как возможность развития

(самосовершенствования), адаптивность (приспособление к текущим условиям обстановки), репродукция и наследование. Этот тезис подтверждается текущими тенденциями в индустрии программных систем – известные производители программного обеспечения заявляют, например, о необходимости применения технологий активной адаптивной защиты, основанной на оценке поведения программных компонентов с точки зрения их потенциальной опасности.

В свете современных представлений постановка задачи разработки моделей, методик и алгоритмов создания адаптивных СЗИ носит комплексный характер и может основываться на биосистемной аналогии. Эволюция средств обработки информации осуществляется в направлении создания систем с элементами самоорганизации, в которых присутствуют процессы зарождения (запуска) необходимых функций, сервисов и процессов, их приспособления и развития. На названных процессах основаны биологические системы, для которых характерны высокая защищенность, накопление опыта эволюции и селективный отбор.

Заимствование архитектурных принципов биосистем привело к разработке теорий нейронных сетей (НС), нейро-нечетких систем (ННС), иммунокомпьютинга и эволюционных методик, лежащих в основе искусственных интеллектуальных систем, базирующихся на распределенной нейросетевой обработке информации и использовании принципов иммунной защиты биосистем.

В настоящей работе предлагается концепция гибридной адаптивной защиты информационных систем на основе гибридных механизмов, сочетающих биометафоры нервных и нейронных сетей. Статья организована следующим образом. В разделе 2 дан краткий анализ исследований, основанных на биосистемной аналогии и гибридных подходах. В разделе 3 представлено видение подхода «нервная система сети», как верхнего уровня системы защиты. В разделе 4 описывается нижний, нейро-нечеткий уровень системы, и приводится пример его схемотехнической реализации. В разделе 5 верхний и нижний уровни рассматриваются в совокупности с целью описания концепции гибридного адаптивного подхода к защите информационных систем на основе нервных и нейронных сетей. В заключении, разделе 6, обобщены выводы по предложенной концепции.

2. АНАЛИЗ ИССЛЕДОВАНИЙ

Биосистемы обладают многоуровневой иерархической системой жизнеобеспечения, реализованной с использованием комплекса механизмов информационной избыточности, защиты и иммунитета. Механизмы защиты информации по возможностям далеки от биологических прототипов, поэтому разработка технологии создания адаптивных систем с встроенными функциями жизнеобеспечения и защиты, основанных на биосистемной аналогии, представляется актуальной [1–5]. Особенно эта задача актуальна для информационных систем критических инфраструктур, которые должны выполнять свое назначение в условиях воздействий угроз всевозможных категорий.

Одним из основных направлений развития информационных систем можно считать создание гибридных адаптивных СЗИ, реализующих механизмы жизнеобеспечения и защиты биологических систем, базирующихся на технической реализации с привлечением современных технологий в виде сверхбольших интегральных схем (СБИС).

Особую роль в эволюции биосистем играет нервная система как адаптивный инструмент взаимодействия со средой. Нервная система необходима для формирования рефлексов в ответ на воздействия. Рефлексия – продукт верхних уровней информационных систем, а информация о механизмах реализации рефлексов хранится на нижних уровнях (в генетической памяти) и наследуется. Поведенческие реакции в биосистеме – результат функционирования нервной системы, свидетельствующий о развитии связи между воздействиями и реакцией организма. Отмечают разделение информации между носителями различной природы: ДНК и нервными клетками – нейронами. Поведенческая информация формируется на основе механизмов, передаваемых через ДНК, и фиксируется в информационном поле нервной системы. Биосистемам свойственно накопление жизненного опыта и передача его потомкам через обучение [6, 7]. Целенаправленность поведения биосистемы развивает форму памяти в виде адаптивного информационного поля нейронной сети нервной системы.

Анализ источников научно-технической информации показал, что исследованию средств, основанных на распределенной нейросетевой обработке информации и принципах иммунной защиты биосистем, гибридным подходам, уделяется большое внимание.

Компания HP пропагандирует технологию ProCurve, в основе которой лежит попытка

интеллектуализации таких сетевых устройств как коммутаторы, маршрутизаторы, точки доступа к беспроводной сети. В частности, делается попытка наделить эти устройства функциями, отвечающими за безопасность сети, например, такими как проверка и фильтрация пакетов, защита от вирусов, шифрование данных.

Компания Cisco применяет концепцию самозащищающейся сети (Cisco's Self-Defending Network). Для защиты передаваемых по сети данных используются защищенные протоколы и технология VPN. Для защиты от внешних угроз задействуется интегрированная система, состоящая из различных компонентов защиты, таких как межсетевые экраны, системы предотвращения вторжений, системы защиты от DDoS-атак и др. Для защиты клиента используются специальные программные агенты, которые служат для конфигурирования клиента в соответствии с заданной политикой безопасности, используемой в компьютерной сети. Также обеспечивается базовая аутентификация пользователей и проверка на соответствие клиента заданной в сети политике безопасности. На основе полученных данных пользователь может получить доступ в сеть или ему может быть отказано в доступе. Имеется возможность создания зон карантина, куда перенаправляются пользователи, не удовлетворяющие условиям, которые требуются для получения доступа в сеть.

Перспективной считается концепция самозащищающейся сети, которая может распознавать все объекты по принципу "свой-чужой", а также защита на основе проверки сетевых объектов на соответствие применяемым политикам безопасности. В случае несоответствия требуемому уровню защищенности, проверяемый объект (компьютер, программа, файл) может быть отправлен на карантин, где, если это возможно, путем установки патчей, обновления антивируса и других операций, уровень его защищенности будет повышен, или же объекту будет предоставлен ограниченный доступ либо отказано в доступе.

Гибридный принцип, или принцип гибридности, зачастую заключается в сочетании, казалось бы, несочетаемого, вследствие чего традиционные системы, приобретают совершенно новые свойства и становятся уникальными в своём роде и области. Так, например, лидер японского автопрома Toyota, выпускает с заката прошлого века гибридные модели Prius [8], позволяющие существенно снизить потребление топлива при соизмеримых мощности, скорости, массе и характеристиках аналогичных моделей машин. Неоспоримы успехи исследователей в области биологии по отбору, селекции, скрещиванию и получению новых полезных гибридов [9]. Продукт «Лаборатории Касперского» Kaspersky Internet Security 2012, в котором реализован принцип гибридности, основан на сочетании классических антивирусных и новейших поведенческих и облачных технологий защиты, что позволяет не только минимизировать время реакции на угрозы, но и снизить нагрузку на компьютеры [10].

В настоящее время сложился определенный задел в области нейросетевой обработки и иммунокомпьютинга, имеется ряд результатов, реализующих нейросетевые средства интеллектуального анализа данных, применимых для защиты информации. Отметим здесь работы [11–20], важные для исследуемой области.

Рассмотрим ниже сначала отдельно два различных биоинспирированных подхода, предлагаемых авторами работы, а затем сформулируем предлагаемую концепцию гибридной адаптивной защиты, которая базируется на использовании этих подходов на различных уровнях представления системы защиты.

3. МЕХАНИЗМЫ РЕАЛИЗАЦИИ ВЕРХНЕГО УРОВНЯ СЗИ

Нервная система человека была взята как основа подхода к защите компьютерных сетей, называемого "нервная система сети", предложенного, наприме р, в работе Ю.Чена и Х.Чена [21].

На основе биоаналогии, подход "нервная система сети" использует распределенный механизм сбора и обработки информации для обнаружения атак и противодействия им. Подобно биологической нервной системе, множество компонентов защиты связаны между собой, что позволяет оперативно обмениваться информацией, координировать действия узлов входящих в "нервную систему", детектировать атаки и принимать меры для их нейтрализации.

Структура данной системы повторяет структуру нервной системы человека (рис. 1). Механизм работы нервной системы сети – распределенный, т.е. предполагается, что нет единого центра, который координирует действия всей сети.

Предполагается, что сетевые домены Интернет-провайдеров (ISP) или автономные системы (AS) соединены между собой как физически связанные нейроны. В каждом домене есть специальный сервер (или кластер серверов).

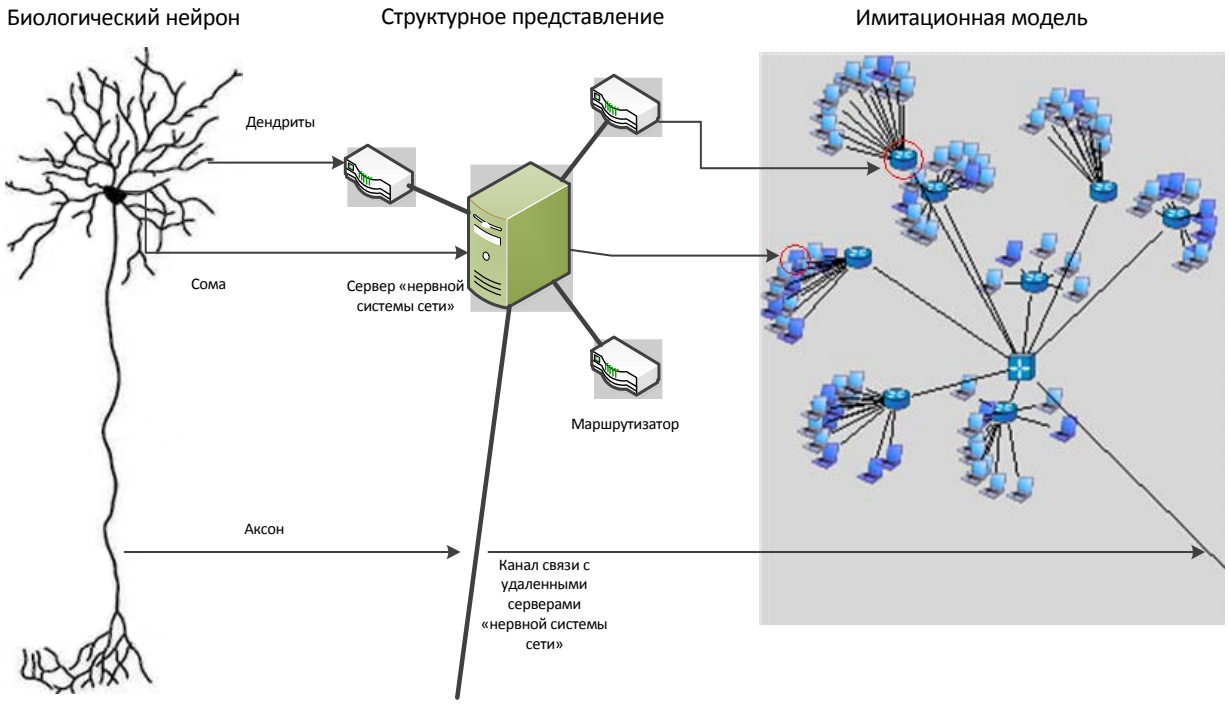

Рис. 1 – Представление биологического нейрона в модели компьютерной сети

Этот сервер исполняет роль сомы в нейроне. Сома является центральной частью нейрона, она реализует большую часть процессов обработки и анализа информации.

Другие сетевые устройства (маршрутизаторы) функционируют как дендриты нейрона, которые передают большую часть информации нейрону. Виртуальная частная сеть (VPN), к которой подключены все серверы, соответствует аксону, передающему сигналы от сомы к другим нейронам (доменам), а также получает информацию от этих нейронов (доменов).

Для обеспечения безопасности системы в [21] предлагается протокол IFSec (InFrastructure Security protocol). Этот протокол работает на сетевом уровне (уровень 3) и определяет формат и механизм шифрования, которые поддерживают безопасный обмен информацией между доменами (нейронами), а также между маршрутизаторами (дендритами) и сервером (сома) в домене. IFSec строится как надстройка IP и работает прозрачно, чтобы транспортировать протоколы более высокого уровня.

Протокол IFSec предоставляет три уровня коммуникации.

Самый низкий уровень дает возможность маршрутизаторам в одном домене обмениваться информацией для контроля состояния сети.

Второй уровень — коммуникация между маршрутизаторами и сервером, расположенными в одном домене.

На самом высоком уровне сервер обменивается информацией с другими серверами, расположенными в других доменах.

Таким образом, протокол IFSec работает в трех различных слоях. Слой 1 служит для коммуникации между одиночными узлами. Слой 2 реализует взаимодействие между узлами и их сервером. Слой 3 объединяет серверы в разных доменах.

Архитектура системы, основанной на данном подходе, представляется следующим образом. Домены сети, которые подключены к нервной системе сети, формируют оверлейную сеть и взаимодействуют между собой с помощью протокола IFSec. Маршрутизаторы, расположенные в разных точках сети, взаимодействуют не только друг с другом, но и со специализированным сервером безопасности в своей подсети [22 – 26].

Функциональные возможности данной архитектуры могут быть представлены на двух уровнях: локальная обработка поступившей информации на отдельных устройствах и обработка информации в масштабе распределенной кооперации провайдеров.

Конкретный процесс по обеспечению защиты осуществляется локально, т.е. в каждом отдельном узле. Крупномасштабная кооперация выполняется для реализации защищенного обмена информацией как внутри домена (от маршрутизатора к маршрутизатору, от маршрутизатора к серверу), так и между доменами (от сервера к серверу). В этом случае

информация автоматически распределяется по различным узлам сети. Своевременное получение информации позволяет более эффективно реагировать на различные внешние угрозы.

Каждый узел состоит из функциональных блоков со стандартным интерфейсом передачи данных, что обеспечивает большую гибкость при динамическом обновлении и обслуживании узлов.

Для начала представим общую архитектуру «нервной системы сети» (рис. 2). В подсети 1 компьютерной сети имеется сервер «нервной системы сети». Он связан с серверами «нервной системы» в других подсетях.

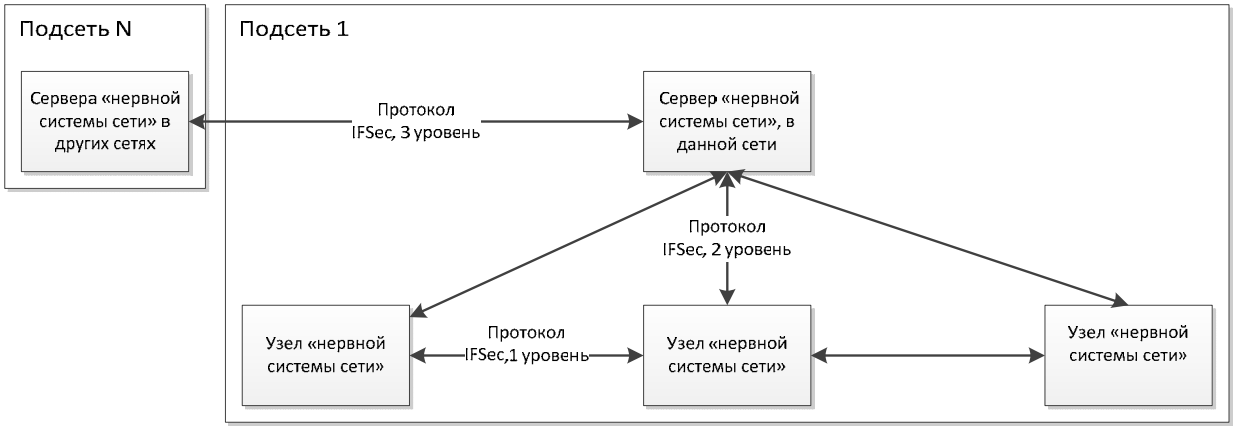

Рис. 2 – Структурное представление «нервной системы сети»

К каждому серверу подключены узлы «нервной системы сети», находящиеся в одной подсети с главным сервером. Кроме того, каждый из узлов имеет связи с другими узлами «нервной системы» в данной подсети. На основе предложенной архитектуры отобразим компонентную структуру «нервной системы сети». В частности раскроем компоненты сервера и узла «нервной системы сети».

Сервер «нервной системы сети» имеет модули обмена данными с подчиненными ему узлами, а также с серверами, находящимися в других подсетях. Модули обмена данными соединены с компонентом, отвечающим за анализ данных и принятие решений.

С помощью него, они получают команды и данные для отправки на узлы и другие сервера «нервной системы» и доставляют ему информацию о событиях, происходящих в сети.

К модулю анализа и принятия решений подключена база данных, которая служит хранилищем данных, полученных из внешних источников, и поставляет ранее сохраненную информацию.

В модуле анализа и принятия решений данные, полученные от модулей обмена информацией с узлами и серверами «нервной системы сети», попадают в модуль приоритезации, где в соответствии с установленными политиками классифицируются события, и определяется, насколько важна та или иная информация, на основе чего принимается решение об очередности выполнения действий в следующих блоках.

Затем данные попадают в модуль корреляции, который, в соответствии с приоритетом, выбирает события и запрашивает похожие события из базы данных (БД) с помощью компонента «обмен данными с БД».

После чего происходит сопоставление набора событий, и определяется уровень угрозы. Для обнаружения источника атаки используется алгоритм на основе подхода «множество изменяемых деревьев» [4].

После этого в блоке «решение о блокировке» на основе политик и порогов определяется реакция на текущую ситуацию в сети.

В данном модуле проверяется, превысил ли подозрительный IP-адрес пороговое значение. Если превысил, то принимается решение о блокировке адреса атакующего, которое отправляется всем подчиненным узлам, а также удаленным серверам «нервной системы сети».

Узел «нервной системы сети» является модулем для первичной обработки данных, поступающих с сенсоров, и управления режимами их работы. В качестве сенсоров могут выступать как простые мониторы трафика, так и более сложные механизмы защиты.

На первом этапе обработки узел с помощью блока перенаправления потоков распределяет потоки трафика, исходя из IP-адреса отправителя. Далее, используя блок классификации пакетов, он определяет типы пакетов, отправляемых источником. После этого производится анализ трафика, полученного после обработки. К модулю анализа и

противодействия подключена база данных, из которой он получает информацию, на основе чего производится анализ трафика.

Если узел обнаружил, что трафик – вредоносный, он передает информацию об этом вместе с данными о вредоносном трафике модулю сдерживания атак. Легитимный трафик возвращается в сеть. Модуль сдерживания атак, с помощью компонентов обмена данными, пересылает эту информацию серверу и узлам, а также получает информацию от них и обновляет базу данных правил и сигнатур.

В модуле анализа и противодействия пакеты из модуля классификация попадают в компонент «анализ на основе правил», где на базе правил фильтрации принимается решение о блокировке трафика.

Далее трафик проходит модули поиска аномалий и сигнатурного анализа. Если какой-либо модуль принял решение о блокировке трафика, пакет, не проходя через последующие фильтры, попадает на модуль блокировки, который в случае положительного решения удаляет пакет и передает информацию о нем в модуль сдерживания атак. В случае если пакет легитимный, он возвращается в сеть. Если узел обнаруживает вредоносные потоки трафика, он отправляет сообщение об этом серверу «нервной сети», с которым он связан.

Серверы «нервной системы сети» постоянно анализируют информацию, поступающую от подключенных к ним узлов и других серверов, вследствие чего принимаются решения об ограничении работы тех или иных пользователей вычислительной сети.

4. МЕХАНИЗМЫ РЕАЛИЗАЦИИ НИЖНЕГО УРОВНЯ СЗИ

В качестве базы для построения адаптивных СЗИ может быть использован технический аналог биосистемы в виде взаимосвязанных интерфейсом нейросетевых командных пулов, управляемых потоком данных [27].

В соответствии с принципами монолитности исполнения и многофункциональности, обработку данных целесообразно организовывать в командных пулах путем выполнения операций чтения, модификации и записи.

Формальная модель процессов, протекающих в информационных полях нейросетевых средств защиты информации в основных режимах работы, необходима для адекватного задания методов проектирования и верификации адаптивных СЗИ, специфицируемых с помощью пакетных нейросетевых программ.

Программирование информационных полей нейронных сетей (и нейро-нечетких систем) в СЗИ можно свести к описанию структуры информационных полей с помощью пакетных нейросетевых программ [27], что позволяет детализировать и исследовать процессы, происходящие в нейронных сетях различных уровней систем адаптивной защиты путем моделирования взаимодействия оперативных данных с распределенными избыточными информационными полями нейронных сетей.

Адаптивность СЗИ предлагается обеспечить использованием функционально устойчивой элементной базы – обычных и логарифмических формальных нейронов, способных к обучению. Адаптивные средства СЗИ согласно принципу биоаналогии следует представлять в виде описания информационных полей нейронных сетей иммунного и рецепторного уровней защиты. Нейронная сеть представляется в виде совокупности взаимосвязанных командных пакетов, которая размещается в командных пулах. При описании нейронных сетей пакетными нейросетевыми программами возможна различная степень детализации: командный пакет может соответствовать одной из функций нейросетевого логического базиса, функции формального нейрона, слоя из формальных нейронов или нейронной сети в целом.

Важным принципом биосистемной аналогии является представление жизненно важных функций и информации в форме топологии, например, генома биологического вида [27]. Известен подход представления топологии информационной системы в виде совокупности командных пакетов, каждый из которых соответствует отдельному фрагменту топологии и определяет реализуемую фрагментом функцию, а также местоположение источников исходных данных и приемников результатов [28]. Пакеты данных предназначены для передачи результатов обработки информации от одних командных пакетов (источников) другим командным пакетам (приемникам). Данный подход соответствует потоковым вычислениям, а подобные информационной системы называют машинами, управляемыми потоком данных.

Программирование в биосистемах носит избыточный распределенный характер, что обеспечивает высокую функциональную устойчивость информационных процессов. Отдельные искажения информации, с одной стороны, компенсируются избыточностью информационных полей, а, с другой, – создают предпосылки для реализации механизма мутаций и эволюционных процессов развития и отбора.

Для исследования информационных процессов в адаптивных СЗИ можно использовать пакетные нейросетевые программы, которые позволяют описывать топологию избыточных распределенных информационных полей НС [29].

Командные пулы организуются в виде многофункциональной регулярной вычислительной структуры, в которой размещены пакетные нейросетевые программы. В качестве средства формализации выбран язык графического описания объектов, а в качестве механизма управления вычислениями – машины, управляемые потоком данных, которые обеспечивают безопасность хранимой информации: операция записи данных производится не по конкретному адресу памяти, а по содержанию; отсутствует операция выборки данных из памяти и, следовательно, непосредственный доступ к информации. Готовые к обработке данные, представленные в виде пакетов, извлекаются из памяти автоматически (без управления извне).

Объединение функций хранения и обработки информации в многофункциональных пулах упрощает их структуру за счет исключения части коммуникационных цепей, предназначенной для передачи готовых к обработке командных пакетов от локальных пулов команд к процессорным узлам, и снижает загрузку интерфейса. Минимизация потоков данных между командными пулами позволяет использовать простейшие виды интерфейсов для передачи пакетов данных. По мере повышения функциональной мощности командных пакетов наблюдается снижение объема передачи пакетов и функциональная специализация командных пулов. И наоборот, снижение функциональной мощности командных пакетов приводит к универсальности командных пулов, интенсификации трафика передачи сообщений, что предъявляет повышенные требования к скоростным возможностям интерфейса.

Наличие современной технологической базы делает целесообразным использование командных пакетов, соответствующих уровню детализации командный пакет – слой формальных нейронов. Для реализации командных пулов на базе СБИС с программируемой структурой следует ограничиться уровнем командного пакета – формальных нейронов, а минимизацию информационного обмена обеспечивать путем размещения пакетных нейросетевых программ в пределах базового блока (ряда базовых блоков) для замыкания информационных потоков между слоями или формальными нейронами НС в рамках отдельных СБИС.

Средства адаптивной защиты могут быть распределенными по базовым блокам, либо локализованными в отдельном базовом блоке. Предложен схемотехнический вариант реализации адаптивной нейросетевой вычислительной среды, отличающийся организацией интерфейса между памятью командных пакетов и операционными блоками [27]. Отмечена взаимосвязь структуры базовых блоков с уровнем детализации описания процессов в НС, формой представления и порядком поступления пакетов данных.

Реализацию информационных процессов на нижнем уровне предлагается выполнять с привлечением так называемого “информационно-полевого” программирования, которое позволяет описывать избыточные распределенные информационные поля в виде пакетных нейросетевых программ [27, 30]. Адаптивные процессы в информационных полях позволяют СЗИ развиваться и накапливать опыт при расширении множества угроз, а наследование опыта сводится к передаче информационных полей в аналогичные по назначению системы.

В качестве базы для создания адаптивной системы защиты информации (технический аналог живого организма) можно использовать нейросетевую среду – взаимосвязанные интерфейсом командные пулы, используемые для размещения пакетных нейросетевых программ и выполнения распределенной обработки за счет взаимодействия оперативных данных с адаптивным избыточным информационным полем НС.

Для обеспечения целостности информации в нейросетевых СЗИ можно использовать аппаратные способы защиты информации, например, на основе организации командных пулов в виде накопителей, не имеющих внешних шин записи/чтения, в которых доступны только входная и выходная очереди, что затрудняет осуществление несанкционированных действий, нарушение целостности и конфиденциальности информации, в сочетании с комбинированием различных механизмов защиты, например, с комбинированием обнаружения сканирования в компьютерных сетях [31].

5. ГИБРИДНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ

Предполагается, что концептуальные и архитектурные решения по построению адаптивных СЗИ, должны быть основаны на

принципах биоаналогии [11]. Предлагаемая концепция гибридной адаптивной защиты информационных систем формируется путем объединения представленных выше подходов.

В качестве базы для построения адаптивных СЗИ предлагается использовать технический аналог структуры биосистемы в виде взаимосвязанных нейросетевых командных пулов (центров), управляемых на основе поступающих данных о состоянии системы.

Архитектурной особенностью биосистем является внутрисистемный характер механизмов защиты. Поэтому в процессе проектирования СЗИ предполагается, что функции защиты информации должны быть внутренними функциями проектируемой системы.

Иерархия адаптивной СЗИ отражает разделение функций защиты на иммунные, проверяющие форму представления информации, и рецепторные, реализующие взаимодействие со средой и накопление опыта.

Выделим, в качестве базовых, пять следующих принципов построения гибридных адаптивных СЗИ, основанных на биологической метафоре.

1. Интеллектуальная обработка информации, интеллектуальный анализ информации:

- обеспечение иерархии элементов обработки информации необходимыми ресурсами;
- на нижних уровнях иерархии осуществляется хранение и анализ генетической информации, реализация механизмов мутации и распределенного преобразования информации, разделение сообщений в соответствии с анализом по критерию “свой/чужой”, накопление опыта по идентификации патогена в иммунологической памяти;
- на верхних уровнях иерархии реализуется связь системы со средой через “органы чувств” (сенсоры) и накопление опыта в распределенных информационных полях нервной системы;
- изменение генетической информации связывается с изменением не формы представления, а содержания информации;
- защита информации обеспечивается, в том числе, за счет реализации свойства адаптивности – приобретения жизненного опыта, позволяющего успешно оперировать ситуациями, в частности, распознавать своих и чужих, выбирать поведение в сложной изменяющейся обстановке.

2. Биосистемная аналогия:

- информация в элементах обработки информации хранится в виде структурированных информационных полей: внизу иерархии – поля идентифицирующего угрозы, вверху иерархии – поля опыта, ставящего в соответствие полю известных угроз механизмы защиты информации;
- нижние (иммунные) уровни средств защиты осуществляют проверку соответствия формы передаваемых в системе сообщений по критерию “свой/чужой”;
- идентифицирующая информация – своя для каждой системы и связана с формой, но не содержанием информации; (как, например, паспорта различных государств, содержащих идентифицирующую информацию, такую как фотографический образ, имя, личную подпись, дату и место рождения, идентификационный номер присвоенный органом государственной регистрации, адрес проживания, и т.п., по принятыми, законами конкретных стран формам, но не несущих полную информацию о владельце паспорта)
- верхние (рецепторные) уровни защиты необходимы для связи с внешней средой и накопления опыта;
- перенос и наследование информации – передача иерархии информационных полей, сформированных в процессе жизненного цикла адаптивной информационной системы, в последующие реализации системы.

3. Поддержание свойств, необходимых для реализации функций интеллектуального анализа информации:

- возможность наследования ранее накопленного опыта адаптивной информационной системы в виде иерархии информационных полей;
- возможность решения задач классификации и кластеризации с оперативной адаптацией информационных полей;
- коррекция жизненного опыта информационной системы на основе коррекции и расширения системы нечетких правил, адаптация информационных полей иерархии уровней системы;
- возможность анализа, коррекции и переноса (наследования) информации в другие информационной системы.

4. Нейронные и нейро-нечеткие сети представляют собой нижний уровень СЗИ, предназначенный для обмена информацией с внешней средой и передачи ее на верхний уровень СЗИ, приема информации от верхнего уровня, а также формирования ответных реакций на воздействия.

5. Верхний уровень адаптивных СЗИ представлен “нервной системой сети” и предназначен для управления процессами системы и взаимодействия с элементами и блоками нижнего уровня. Верхний и нижний уровни работают как одно целое, в постоянном информационном взаимодействии и согласовании решений в режиме реального времени.

6. ЗАКЛЮЧЕНИЕ

В статье предложена общая концепция гибридной адаптивной защиты информационных систем, сочетающая биометафоры нервных и нейронных сетей.

На основе метафор нервной и нейронной сети в работе предлагается гибридная адаптивная сетевая инфраструктура, обеспечивающая получение, передачу, хранение и защиту информации, принятие решений, исходя из сложившейся ситуации, в соответствии с аналогией работы нервной и нейронной систем живых существ.

Кооперация распределенных компонентов происходит подобно реакции человеческой нервной системы. Одиночные компоненты работают не только как исполнители, но также и как сенсоры. Помимо общей защиты, которая осуществляется ими самостоятельно, они также предоставляют результаты анализа данных другим компонентам системы.

Планируется в результате исследований разработать технологию создания сетевых компонентов со встроенными функциями защиты, отличающуюся представлением структуры компонента в виде иерархии компонентов, выполненных с различной степенью детализации, описанием информационной структуры с помощью графического языка, функциональным блокам которой соответствуют командные пакеты, информационным потокам – пакеты данных.

Достоинствами такого подхода являются применение подхода управления потоком данных для организации распределенных вычислений, а также средств интеллектуального анализа данных в составе адаптивной системы защиты информации для обеспечения оперативной реакции на изменение множества угроз и условий эксплуатации.

Будущая работа связана с моделированием компонентов представленного концептуального подхода к построению гибридных адаптивных систем защиты.

Работа выполняется при финансовой поддержке Министерства образования и науки РФ (государственный контракт 11.519.11.4008), РФФИ (проект №13-01-00843-а), программы фундаментальных исследований ОНИТ РАН (проект №2.2), проектов Евросоюза SecFutur и MASSIF.

7. СПИСОК ЛИТЕРАТУРЫ

[1] D. Dasgupta, H. Bersini, et al., *Artificial Immune Systems and Their Usage*, D. Dasgupta (Eds.), translated from English under edit. of A.A. Romanyiukha, M.: FIZMATLIT, 2006, 344 p. (in Russian)

[2] R.M. Khaitov, *Physiology of Immune System, Moscow,* VINITI RAN, 2001, 223 p. (in Russian)

[3] N.K. Jerne, *Towards a network theory of the immune system*, *Ann. Immunol. (Inst. Pasteur),* (125) (1974), pp. 435-441.

[4] G. Miller, P. Todd, S. Hedge, Designing neural networks using genetic algorithms, *Proc. 3rd Int. Conf. on Genetic Algorithms,* (1989), pp. 379-384.

[5] I.V. Kotenko, F.G. Nesteruk, A.V. Shorov, Methods of computer networks defense on the base of bio-inspired approaches, *Voprosi zaschiti informacii,* (2) (2012), pp.35-46. (in Russian)

[6] M.E. Lobashev, *Genetics*, Leningrad, LGU Publishers, 1969, 357 p. (in Russian)

[7] I.V. Melik-Gaynazya, *Information Processes and Reality*, Moscow, Nauka, 1998, 137 p. (in Russian)

[8] Electronic resource. Access mode – URL: http://www.toyotacenter.ru/ (in Russian)

[9] Electronic resource. Access mode – URL: http://rudocs.exdat.com/docs/index-227356.html (in Russian)

[10] Electronic resource. Access mode – URL: http://www.kaspersky.ru/news?id=207733674 (in Russian)

[11] L.B. Booker, D.E. Goldberg, I.E. Holland, Classifier systems and genetic algorithms, *Artificial Intelligence,* Elsevier, (40) (1989), pp. 235-282.

[12] G. Deffuant, *Reseaux Connectionistes Auto-construits*, These D'Etat, 1992, 141 p.

[13] M. Dorigo, H. Bersini A comparative analysis of Q-learning and classifier systems, *Proc. SAB'94, MIT Press, (*1994), pp. 248-255.

[14] S. Fahlman, C. Lebiere, The cascade-correlation learning architecture, *Advances in Neural Information Processing System*, Morgan Kaufman, (2) (1990), pp. 524-532.

[15] M. Fombellida, Methodes heuristiques et methodes d'optimalisation non contraintes pour l'apprentissage des perceptrons multicouches, *Proc. 5th Int. Conf. on Neural Networks and their Application: Neuro-Nimes, (*1992), pp. 349-366.

[16] D.E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison-Wesley, 1989, 432 p.

[17] Y. Hirose, K. Yamashita, S. Hijiya, Back-propagation algorithm which varies the number of units, *Neural Networks,* (4) (1991), pp. 61-66.

[18] J.H. Holland, K.J. Holyoak, R.E. Nisbett, P.R. Thagard, *Induction: Processes of Inference, Learning and Discovery*, Cambridge: MIT Press, 1986, 386 p.

[19] T. Salom, H. Bersini, An algorithm for self-structuring neural net classifiers, *Proc. 2nd IEEE Conf. on Neural Network* (ICNN'94, 1994), pp. 1307-1312.

[20] R.S. Sutton, Reinforcement learning architectures for animats, *Proc. 1st SAB Conference* (Eds. J.-A. Meyer and S.W. Wilson). MIT Press, (1990), pp. 288-296.

[21] Y. Chen, H. Chen, NeuroNet: An Adaptive Infrastructure for Network Security, *International Journal of Information, Intelligence and Knowledge,* (1) 2 (2009), pp.143-168.

[22] I.V. Kotenko, A.M. Konovalov, A.V. Shorov, Modeling of botnets and tools of defense against them, *Sistemi visokoi dostupnosti*, (2) (2011), pp.107-111. (in Russian)

[23] I.V. Kotenko, A.M. Konovalov, A.V. Shorov, Researchers modeling of botnets and defense against them, *Prilojenie k jurnalu "Informacionnie technologii*", (1) (2012), pp. 32. (in Russian)

[24] I.V. Kotenko, A.V. Shorov, F.G. Nesteruk, Analysis of bio-inspired approaches for defense of computer systems and networks, *Trudy SPIIRAN,* (3) 18 (2011), pp. 19-73. (in Russian)

[25] I. Kotenko, A. Konovalov, A. Shorov, Agent-based Modeling and Simulation of Botnets and Botnet Defense, *Conference on Cyber Conflict. Proceedings 2010.* CCD COE Publications. Tallinn, Estonia, (June 15-18, 2010), pp. 21-44.

[26] I. Kotenko, A. Konovalov, A. Shorov, Agent-based simulation of cooperative defense against botnets, *Concurrency and Computation: Practice and Experience,* (24) 6 (2012), pp. 573-588.

[27] F.G. Nesteruk, A.V. Suhanov, L.G. Nesteruk, G.F. Nesteruk, *Adaptive Means of Information Systems Safety Supplying,* Monograph. SPb.: Polytechnic University Publishing, 2008, 626 p. (in Russian)

[28] J.B. Dennis, J.B. Fossin, J.P. Linderman, *Scheme of data flow*, Teoriya programmirivaniya, Novosibirsk: VC SO AN SSSR, (1972), Part. 2. pp. 7-43. (in Russian)

[29] G.F. Nesteruk, M.S. Kupriyanov, F.G. Nesteruk, About developing of language means for neural networks structure programming, *Proceedings of V International Conference SCM'2002.* SPb, (2002), Vol. 2. pp. 52-55. (in Russian)

[30] F.G. Nesteruk, L.G. Nesteruk, G.F. Nesteruk, Application of the Formal Model for Describing Processes of Adaptive Information Security in Computer-aided Systems, *Automation and Remote Control,* (70) 3 (2009), pp. 491-501.

[31] A.A. Chechulin, I.V. Kotenko, Combining of defense tools against scanning in computer networks, *Informacionno-upravliauschie sistemi,* (12) *(*2010), pp. 21-27. (in Russian)

Игорь Витальевич Котенко, *Заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Закончил с отличием ВИКИ им. А.Ф. Можайского (1983 г.) и Военную академию связи (1987 г.). В 1990 г. защитил кандидатскую диссертацию, а в 1999 г. – докторскую. В 2001 г. присвоено ученое звание профессор по кафедре "Телекоммуникационные системы". Автор более 450 научных работ. Область научных интересов – информационная безопасность, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, ложные информационные системы, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер-терроризму; искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение.*

Филипп Геннадьевич Нестерук, *Старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Закончил ОМГТУ (2000 г.) Поступил в аспирантуру СПбГУЭиФ, в 2005 г. защитил кандидатскую диссертацию по теме «Разработка модели адаптивной системы защиты информации на базе нейро-нечетких сетей», специальность 05.13.19, в СПбГУ ИТМО.*

Андрей Владимирович Шоров, *Научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Окончил Санкт-Петербургский Государственный Инженерно-Экономический Университет (2008 г.), в 2012 г. защитил кандидатскую диссертацию по теме «Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “Нервная система сети”» (Специальность: 05.13.19 — Методы и системы защиты информации, информационная безопасность), в СПИИРАН.*

computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

CONCEPTION OF A HYBRID ADAPTIVE PROTECTION OF INFORMATION SYSTEMS

Igor V. Kotenko, Filipp G. Nesteruk, Andrey V. Shorov

Laboratory of computer security problems SPIIRAS
39, 14th Liniya, St. Petersburg, 199178, Russia
ivkote@iias.spb.su, 08p@mail.ru, ashorov@comsec.spb.ru
http://comsec.spb.ru/en

Abstract: *The paper suggests the conception of a hybrid adaptive protection of information and telecommunication systems which is based on a biometaphor of nervous and neural networks. A top level of a protection system, based on an approach of "nervous system network" is a distributed mechanism for collecting and processing information. We suggest to implement the information processes on the low level with the assistance of an "information field" programming. It allows specifying the distributed information fields in the form of neural network software packages.*

Keywords: *Data mining, malware, detection.*

1. INTRODUCTION

There is an analogy in evolution and natural selection in nature and technical systems. Living organisms exist and evolve through improved protection against a variety of threats by using information circulating in their distributed structure and implementing various security mechanisms.

Therefore, it seems that it is necessary to endow the information security systems by evolutionary properties inherent biological systems. These properties are the possibility of progress (self-improvement), adaptability (accommodation to the current conditions of the situation), reproduction and inheritance.

This thesis is confirmed by the latest trends in the industry of software systems. For example, known software vendors claim that they need active adaptive security technologies, based on an assessment of the behavior of software components in terms of their potential danger.

In the paper we propose the conception of adaptive protection of information systems based on hybrid mechanisms that combine bio-metaphors of nervous and neural networks.

First we outline a brief analysis of investigations based on the bio-metaphors and different hybrid approaches. Then we define an approach "network nervous system" as the top-level protection system, determine the lower protection level as neuro-fuzzy system, and present an example of their realization.

2. TOP LEVEL PROTECTION MECHANISMS

One of approaches for protection of computer networks is a bio-inspired approach "nervous network system" [1-3].

The protection system is based on a distributed mechanism for collecting and processing information, which coordinates the activities of the main devices of the network, detected of attack and take countermeasures.

The structure of the "nervous network" follows the structure of the human nervous system (Fig.1). The mechanism of the "nervous network" is distributed, i.e. no single center which coordinates the activities of all network.

The protection system consists of two main components – the server of the "nervous network system" and the node of the "nervous network system". Servers are installed in different subnets and implement most functions of information processing and analysis, as well as the coordination of nearby network devices.

Nodes are used for data collection, initial processing and transmission of network status information to servers. Nodes can be installed on routers. Servers are located in different subnets and exchange information on the status of their subnets.

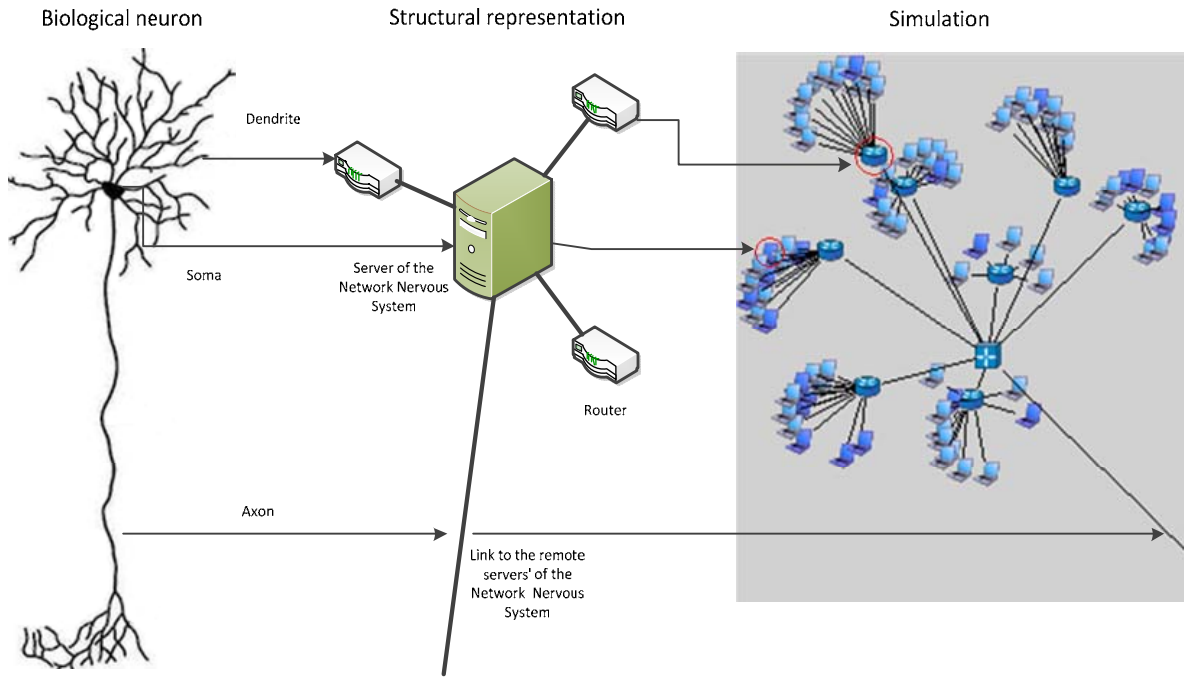

Fig.1. – Metaphor of the biological neuron in the computer network model

Thus, based on the metaphor of the "nervous network system", the paper proposes an adaptive network infrastructure which provides information collection and its transfer to the special server and making decisions based on the current situation.

3. LOWER LEVEL PROTECTION MECHANISMS

We suggest implementing the information processes on the lower level with the assistance of an "information field" programming [4, 5].

It allows specifying the distributed information fields in the form of neural network software packages.

Adaptive processes in the information fields allow developing the security systems which can evolve and gain experience when expanding the set of threats. In this case the inheritance of the experience is reduced to transferring of information fields.

4. HYBRID APPROACH FOR PROTECTION MECHANISMS

It is assumed that the conceptual and architectural solutions for building adaptive hybrid information protection systems should be based on the principles of bio-analogy. The proposed concept of a hybrid adaptive protection of information systems is formed by combining two above approaches.

This research is being supported by the state contract 11.519.11.4008 of Ministry of education and science of Russia, grant of Russian Foundation of Basic Research (Project No. №13-01-00843-a), program of fundamental research of the Department for Informational Technologies and Computation Systems of the Russian Academy of Sciences (contract No 2.2), Russian Science Support Foundation and partly funded by the EU as part of the MASSIF project and SecFutur project.

5. REFERENCES

[1] Y. Chen, H. Chen, NeuroNet: An Adaptive Infrastructure for Network Security, *International Journal of Information, Intelligence and Knowledge,* (1) 2 (2009), pp. 143-168.

[2] I. Kotenko, A. Konovalov, A. Shorov Agent-based Modeling and Simulation of Botnets and Botnet Defense, *Conference on Cyber Conflict. Proceedings 2010.* CCD COE Publications. Tallinn, Estonia, (June 15-18, 2010), pp. 21-44.

[3] I. Kotenko, A. Konovalov, A. Shorov Agent-based simulation of cooperative defence against botnets, *Concurrency and Computation: Practice and Experience,* Vol. 24, Issue 6, (25 April 2012), pp. 573-588.

[4] F.G. Nesteruk, A.V. Suhanov, L.G. Nesteruk, G.F. Nesteruk, *Adaptive Means of Information Systems Safety Supplying,* Monograph. SPb.: Polytechnic University Publishers, 2008, 626 p. (in Russian)

[5] F.G. Nesteruk, L.G. Nesteruk, G.F. Nesteruk, Application of the Formal Model for Describing Processes of Adaptive Information Security in Computer-aided Systems, *Automation and Remote Control,* (70) 3 (2009), pp. 491-501.