УДК 004.7

И.В. Котенко, Ф.Г. Нестерук, А.В. Шоров

КОНЦЕПЦИЯ АДАПТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ПАРАДИГМ НЕРВНЫХ И НЕЙРОНЫХ СЕТЕЙ

Котенко И.В., Нестерук Ф.Г., Шоров А.В. **Концепция адаптивной защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей.**

Аннотация. Актуальность проблемы защиты информационно-телекоммуникационных систем обусловлена ростом сложности программного и аппаратного обеспечения, высокой динамикой их развития, распределенной и разнородной структурой и множеством других факторов. Очевидна аналогия между эволюцией и естественным отбором в природе и в информационно-телекоммуникационных системах, в том числе системах защиты информации. В работе предлагается концепция адаптивной защиты информационно-телекоммуникационных систем на основе гибридных механизмов, сочетающих парадигмы нервных и нейронных сетей.

Ключевые слова: информационно-телекоммуникационные системы, защита компьютерных систем и сетей, нейронная сеть, нервная система сети.

Kotenko I.V., Nesteruk F.G., Shorov A.V. **Conception of adaptive protection of information and telecommunication systems based on the paradigms of nervous and neural networks.**

Abstract. The relevance of the problem of information and telecommunication systems protection is stipulated by increasing the complexity of hardware and software, high dynamics of their development, distributed and heterogeneous structure and many other factors. Analogy between evolution and natural selection in nature and information and telecommunication systems, including security systems, is obvious. The paper suggests the conception of adaptive protection of information and telecommunication systems which is based on hybrid mechanisms integrating the paradigms of nervous and neural networks.

Keywords: information and telecommunications systems, protection of computer systems and networks, neural network, “nervous network system”.

1. Введение. Актуальность проблемы защиты информационно-телекоммуникационных систем обусловлена ростом сложности программного и аппаратного обеспечения, высокой динамикой их развития, распределенной и разнородной структурой и рядом других факторов. Очевидна аналогия между эволюцией и естественным отбором в природе и информационно-телекоммуникационных системах (ИТКС). 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 придать системам защиты информации (СЗИ) информационно-телекоммуникационных сетей эволюционные свойства, присущие биосистемам, такие как возможность развития (самосовершенствования) и адаптивность (приспособление к текущим условиям обстановки). 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 (инициирования) необходимых функций, сервисов и процессов, их приспособления и развития. На названных процессах основаны биологические системы, для которых характерны высокая защищенность, накопление опыта эволюции, селективный отбор.

Заимствование архитектурных принципов биосистем привело к разработке теорий нейронных сетей (НС), нейро-нечетких систем, 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 адаптивной защиты информационно-телекоммуникационных систем на основе гибридных механизмов, сочетающих парадигмы нервных и нейронных сетей.

Статья организована следующим образом. В разделе 2 дается краткий анализ исследований, основанных на биосистемной аналогии. В разделе 3 рассматривается подход к защите информационно-телекоммуникационных систем на основе гибридного подхода, принципов адаптивной защиты и использования нервных и нейронных сетей. В разделе 4 представлено видение подхода “нервная система сети”, как верхнего уровня системы. В разделе 5 описывается нижний (нейро-нечеткий) уровень системы, и приведен пример его схемотехнической реализации. В заключении делаются выводы по предложенной концепции защиты информации.

2. Анализ исследований, основанных на биосистемной аналогии. Как известно, 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, 8, 19, 22]. Особенно эта задача актуальна для информационно-телекоммуникационных систем критических инфраструктур, которые должны выполнять свое назначение в условиях воздействия нарушителей различных категорий, в том числе террористических актов и воздействия противника.

Поэтому одним из основных направлений развития информационно-телекоммуникационных систем можно считать создание адаптивных СЗИ, реализующих механизмы жизнеобеспечения и защиты биологических систем и базирующихся, в том числе, на технической реализации с привлечением современных наноэлектронных 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 [5, 6]. 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 [5, 6]. 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, уделяется большое внимание.

Например, 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, в свою очередь, 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.

В настоящее время сложился определенный задел в области нейросетевой обработки и иммунокомпьютинга, имеется ряд изобретений, реализующих нейросетевые средства интеллектуального анализа данных, применимых для защиты информации. Отметим здесь работы [10, 12 - 18, 24, 25], важные для исследуемой области.

3. Подход к защите информации на основе гибридного подхода. Представляется, что концептуальные и архитектурные решения по построению адаптивных СЗИ должны быть основаны на принципах биоаналогии [10]. В качестве базы для построения адаптивных СЗИ

может быть использован 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 следует учитывать, 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 (рис. 1).

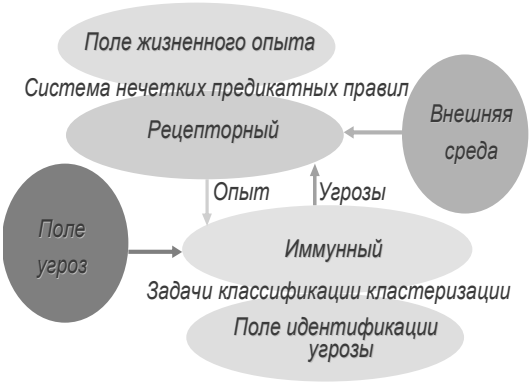

Рис. 1. Иерархия адаптивной СЗИ.

Выделим в качестве базовых три следующих принципа построения адаптивных СЗИ, основанные на биологической метафоре.

1. Интеллектуальная обработка информации, в том числе интеллектуальный анализ информации (ИАИ):

- обеспечение иерархии элементов обработки информации;
- на нижних уровнях иерархии осуществляется хранение и анализ генетической информации, реализация механизмов мутации, распределенного преобразования информации, разделение сообщений в соответствии с распределенным 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 и накопление опыта в распределенных информационных полях нервной системы;

- изменение генетической информации связывается с изменением не формы представления, а содержания информации;
- защита информации в биосистеме 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, как поля идентифицирующего угрозы, и вверху иерархии, как 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;
- 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 ИАИ:

- возможность наследования ранее накопленного опыта адаптивной ИС 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.

Нейронные и нейро-нечеткие сети представляют собой нижний уровень (НУ) СЗИ, предназначенный для обмена информацией с внешней средой и передачи ее на верхний уровень (ВУ) СЗИ, приема

информации от ВУ, а также формирования ответных реакций на воздействия.

Верхний уровень адаптивных СЗИ представлен “нервной системой сети” и предназначен для управления процессами системы и взаимодействия с элементами и блоками НУ.

ВУ и НУ работают как единое целое, обеспечивая постоянное информационное взаимодействие и согласование решений в режиме реального времени.

Выделяется как минимум два условных состояния СЗИ:

- режим бодрствования – основной режим работы (сенсоры НУ активны, верхний уровень, взаимодействуя с НУ, анализирует информацию, полученную в этом режиме);
- режим сна (сенсоры нижнего уровня отключаются, верхний уровень, взаимодействуя с НУ, анализирует информацию, полученную в режиме бодрствования, и вырабатывает инструкции, накапливая базу данных).

Количество уровней и режимов работы СЗИ может быть увеличено при необходимости.

4. Механизмы реализации верхнего уровня СЗИ на основе подхода “нервная система сети”. За основу подхода к защите компьютерных сетей, называемого “нервная система сети”, который был предложен, например, в работе Ю.Чена и Х.Чена [11], была взята нервная система человека.

Нервная система является элементом организма, и состоит из нервных клеток (нейронов), и комплекса вспомогательных клеток (нейроглии). Количество нейронов в центральной нервной системе человека $\approx 4*10^{11}$ [26]. В ответ на воздействие (например, внешнее посредством рецепторов), нейрон генерирует сигнал (импульс), передаваемый по нервной системе в головной мозг, где происходит процесс восприятия, трактовки и выдачи ответных инструкций, и снова, но уже как ответная реакция, по узлам нервной системы проходит ответный импульс (реакция на воздействие).

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. 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). 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 [11] предлагается протокол IFSec (InFrastructure Security protocol), являющийся новым протоколом безопасности сетевой инфраструктуры. 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, рас-

положенные в разных точках сети, взаимодействуют не только друг с другом, но и со специализированным сервером безопасности в своей подсети [2, 3, 4, 20, 21].

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.

5. Механизмы реализации нижнего уровня СЗИ. Реализацию информационных процессов на нижнем уровне предлагается выполнять с привлечением “информационно-полевого” программирования, которое позволяет описывать избыточные распределенные информационные поля в виде пакетных нейросетевых программ (ПНП) [7, 23]. 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 ПНП 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 [7], 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 конфиден-

циальности информации, в сочетании с комбинированием механизмов обнаружения сканирования в компьютерных сетях [9].

Для реализации компонента адаптивной СЗИ (рис. 2) структура командных пулов [7] претерпевает минимальные изменения, связанные с необходимостью формирования входного вектора для адаптивных средств защиты информации и выполнения операции параллельного сравнения поступившего входного вектора с функциональными параметрами нейронов–прототипов. Выходные цепи мультиплексора MS модифицированы, за счет размещения аппаратных схем контроля IV (Input Vector), призванной выделить распределенную по полям пакетов данных системную информацию о комплементарности, равномерности распределения масс и уравновешенности системы связей.

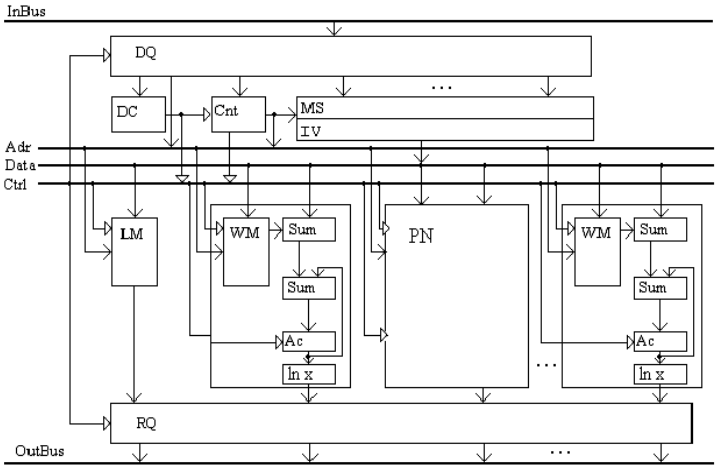

Рис. 2. Архитектура компонента адаптивной СЗИ.

Кроме того, в структуре нейропроцессорного узла PN следует отключить функциональный преобразователь ex, так как при выполнении операции сравнения поступившего входного вектора с функциональными параметрами нейронов–прототипов (первый сумматор Sum) отпадает необходимость в умножении входного вектора на вектор весовых коэффициентов. В рассматриваемой структуре PN второй сумматор Sum совместно с аккумулятором Ac используется для накопления значений несовпадений входного вектора с функциональными параметрами каждого из нейронов-прототипов так, что после просмотра всех полей входного вектора на выходах PN сформируется вектор

несовпадений, определяющий степень близости входного вектора к каждому из нейронов-прототипов.

Заключение. В статье предложена общая концепция адаптивной защиты информационно-телекоммуникационных систем на основе гибридных механизмов, сочетающих парадигмы нервных и нейронных сетей.

На основе метафоры “нервной системы” в работе предлагается адаптивная сетевая инфраструктура, обеспечивающая получение информации, ее передачу и принятие решений, исходя из сложившейся ситуации в соответствии с аналогией с нервной системой 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.

Предполагается, что в результате исследований будет разработана технология создания сетевых компонентов со встроенными функциями защиты, отличающаяся представлением структуры компонента в виде иерархии топологий, выполненных с различной степенью детализации, описанием информационной структуры с помощью графического языка, функциональным блокам которой соответствуют командные пакеты, информационным потокам – пакеты данных. Основными достоинствами такого подхода являются применение подхода управления потоком данных для организации распределенных вычислений, 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 отдельных компонентов и общего концептуального подхода к построению адаптивных систем защиты, а также с реализацией прототипов компонентов системы защиты, строящейся на основе представленной концепции.

Литература

1. *Дасгупта Д., Берсини Х., и др.* Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты. Пер. с англ. под ред А.А. Романюхи. М.: ФИЗМАТЛИТ, 2006. 344 с.
2. *Котенко И.В., Коновалов А.М., Шоров А.В.* Моделирование бот-сетей и механизмов защиты от них // Системы высокой доступности, № 2, 2011. С.107-111.
3. *Котенко И.В., Коновалов А.М., Шоров А.В.* Исследовательское моделирование бот-сетей и механизмов защиты от них // Приложение к журналу “Информационные технологии”, № 1, 2012, 32 с.

4. *Котенко И.В., Шоров А.В., Нестерук Ф.Г.* Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. Вып.3 (18). СПб.: Наука, 2011. С.19–73.
5. *Лобашев М.Е.* Генетика. – Л.: Изд-во ленинградского университета, 1969.
6. *Мелик-Гайназян И. В.* Информационные процессы и реальность. М.: Наука, 1998.
7. *Нестерук Ф.Г, Суханов А. В, Нестерук Л. Г, Нестерук Г. Ф.* Адаптивные средства обеспечения безопасности информационных систем. Монография. СПб.: Изд-во Политехнического университета, 2008. 626 с.
8. *Хаитов Р. М.* Физиология иммунной системы. – М.: ВИНИТИ РАН, 2001. 223 с.
9. *Чечулин А.А., Котенко И.В.* Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы, 2010, № 12, С.21-27. ISSN1684-8853.
10. *Booker L.B, Goldberg D.E., Holland I.E.* Classifier systems and genetic algorithms // Artificial Intelligence 40. Elsevier, 1989. P. 235-282.
11. *Chen Y., Chen H.* NeuroNet: An Adaptive Infrastructure for Network Security // International Journal of Information, Intelligence and Knowledge, Vol.1, No.2, 2009. P.143–168.
12. *Deffuant G.* Reseaux connectionistes auto-construits. These D'Etat, 1992. P. 141.
13. *Dorigo M., Bersini H.* A comparative analysis of Q-learning and classifier systems // Proc. SAB'94. MIT Press, 1994. P. 248-255.
14. *Fahlman S., Lebiere C.* The cascade-correlation learning architecture // Advances in Neural Information Processing System, V. 2. Morgan Kaufman, 1990. P. 524-532.
15. *Fombellida M.* 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. P. 349-366.
16. *Goldberg D.E.* Genetic algorithms in search, optimization and machine learning // Addison-Wesley, 1989. P. 432.
17. *Hirose Y., Yamashita K., Hijiya S.* Back-propagation algorithm which varies the number of units // Neural Networks. 1991. V. 4. P. 61-66.
18. *Holland J.H., Holyoak K.J., Nisbett R.E., Thagard P.R.* Induction: Processes of inference, learning and discovery. Cambridge: MIT Press, 1986. P. 386.
19. *Jerne N.K.* Towards a network theory of the immune system // Ann. Immunol. (Inst. Pasteur). 1974. V. 125C. P. 435-441.
20. *Kotenko I., Konovalov A., Shorov A.* 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. P.21-44.
21. *Kotenko I., Konovalov A., Shorov A.* Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience, Vol. 24, Issue 6, 25 April 2012. P. 573-588.
22. *Miller G., Todd P., Hedge S.* Designing neural networks using genetic algorithms // Proc. 3rd Int. Conf. on Genetic Algorithms, 1989. P. 379-384.
23. *Nesteruk F.G., Nesteruk L.G., Nesteruk G.F.* Application of the Formal Model for Describing Processes of Adaptive Information Security in Computer-aided Systems// Automation and Remote Control, 2009, Vol. 70, № 3. P. 491–501.
24. *Salom T., Bersini H.* An algorithm for self-structuring neural net classifiers // Proc. 2nd IEEE Conf. On Neural Network (ICNN'94), 1994. P. 1307-1312.
25. *Sutton R.S.* Reinforcement learning architectures for animats // Proc. 1st SAB Conference (Eds. J.-A. Meyer and S.W. Wilson). MIT Press, 1990. P. 288-296.
26. *http://victor-male1.livejournal.com/17783.html*

Котенко Игорь Витальевич — д.т.н., проф.; заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, 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, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений, телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Kotenko Igor Vitalievich — Prof. of Computer Science; head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism, artificial intelligence, including multi-agent frameworks and systems, agent-based modeling and simulation, soft and evolutionary computing, machine learning, data mining, data and information fusion, telecommunications, including decision making and planning for telecommunication systems. The number of publications — 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Нестерук Филипп Геннадьевич — старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: адаптивные системы защиты информации, интеллектуальный анализ данных, нейронные сети, нечеткая логика, экспертные системы, генетические алгоритмы, искусственный интеллект, извлечение знаний, комплексные системы защиты информации. Число научных публикаций — более 100. 08p@mail.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Nesteruk Filipp Gennadyevich — PhD. of Computer Science, Senior researcher of Laboratory of Computer Security Problems, SPIIRAS. Research interests: adaptive systems of information security, data mining, neural networks, fuzzy logic, expert systems, genetic algorithms, artificial intelligence, knowledge extraction, complex systems of information security. The number of publications — over 100. 08p@mail.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Шоров Андрей Владимирович — аспирант лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: имитационное моделирование, безопасность компьютерных сетей, обнаружение вторжений. Число научных публикаций — 18. ashorov@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Shorov Andrey Vladimirovich — Ph.D. student of Laboratory of Computer Security Problems, SPIIRAS. Research interests: modeling and simulation, computer network security, intrusion detection. The number of publications — 18. akonovalov@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00826, 12-07-13119-офи_м_РЖД), программы фундаментальных исследований ОНИТ РАН (проект № 2.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и Massif, а также в рамках других проектов.

Рекомендовано СПИИРАН, лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 12.01.2012.

РЕФЕРАТ

Котенко И.В., Нестерук Ф.Г., Шоров А.В. **Концепция защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей.**

Актуальность защиты информационных систем связана с их высокой скоростью развития, ростом сложности, и распределенной структурой. Существует аналогия между эволюцией и естественным отбором в природе, и системами информационных технологий.

В работе предлагается концепция адаптивной защиты информационно-телекоммуникационных систем на основе гибридных механизмов, сочетающих парадигмы нервных и нейронных сетей.

Система защиты, основанная 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. Структура данной системы повторяет структуру нервной системы человека. Механизм работы нервной системы сети - распределенный, т.е. нет единого центра, который координирует действия всей сети.

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

SUMMARY

Kotenko I.V., Nesteruk F.G., Shorov A.V. **Conception of adaptive protection of information and telecommunication systems based on the paradigms of nervous and neural networks.**

The relevance of the problem of information and telecommunication systems protection is stipulated by increasing the complexity of hardware and software, high dynamics of their development, distributed and heterogeneous structure and many other factors. Analogy between evolution and natural selection in nature and information and telecommunication systems, including security systems, is obvious.

The paper suggests the conception of adaptive protection of information and telecommunication systems which is based on hybrid mechanisms integrating the paradigms of nervous and neural networks.

Protection system, based on the approach “nervous system network” is based on a distributed mechanism for collecting and processing information. It coordinates the activities of main computer network devices, identifies attacks and takes countermeasures. The structure of this system follows the structure of the human nervous system. The mechanism of the nervous system is distributed, i.e. there is no single center, which coordinates the activities of the network.

We suggest implementing the information processes on the lower level with the assistance of an “information field” programming. 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.