УДК 004.7

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

АНАЛИЗ БИОИНСПИРИРОВАННЫХ ПОДХОДОВ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Котенко И.В., Шоров А.В., Нестерук Ф.Г. **Анализ биоинспирированных подходов для защиты компьютерных систем и сетей.**

Аннотация. В настоящее время в области безопасности компьютерных систем и сетей все чаще упоминаются и рекламируются различные биоинспирированные подходы, то есть подходы, основанные на биологической метафоре. Действительно, традиционные компьютерные методы и системы, как правило, ограничены по своим функциональным возможностям, подвержены частому выходу из строя из-за незначительных ошибок, имеют недостаточную масштабируемость, не обладают способностью к адаптации к условиям функционирования и изменению целей. В противоположность этому, биологические системы, как правило, реализуют развитые механизмы самозащиты, достаточно надежны, обладают высокой масштабируемостью, адаптивны и способны к саморегенерации. Указанные свойства биологических систем стимулируют использование принципов их построения и механизмов их функционирования в технических системах, включая системы защиты информации. В данной статье рассматриваются различные подходы к защите компьютерных систем и сетей, в основе которых лежит биологическая метафора.

Ключевые слова: биологическая метафора, защита компьютерных систем и сетей, иммунокомпьютинг, нейронные сети, гибридные интеллектуальные средства.

Kotenko I.V., Shorov A.V., Nesteruk P.G. **Analysis of bio-inspired approaches for protection of computer systems and networks.**

Abstract. Nowadays more and more different bio-inspired approaches (based on a biological metaphor) for the computer and networks security systems are mentioned and advertised. Traditional computer-based systems and their functionality are often limited by different conditions. Due to frequent minor errors, these systems are subject of failure. They lack scalability, have low adaptation ability to changeable conditions of functioning and its goals. As opposed to traditional computer-based systems, biological systems are often quite reliable. They have great self-protection mechanisms, highly scalable, adaptable and able to self regeneration. These properties of biological systems can be used to construct technical systems (including information security systems). The paper considers different approaches to the protection of computer systems and networks, which are based on a biological metaphor.

Keywords: biological metaphor, protection of computer systems and networks, immunocomputing, neural networks, hybrid intelligent means.

1. Введение. В последние годы много усилий прилагается для создания методов и алгоритмов, которые могли бы обеспечить эффективные механизмы защиты компьютерных систем и сетей.

Одной из важнейших целей построения защищенных систем и сетей является создание механизмов защиты, которые будут устойчивы к сбоям, будут обладать высокой масштабируемостью и адаптивностью

(в том числе смогут самоконфигурироваться и самовосстанавливаться).

Биологические системы, например человек, представляют собой достаточно сбалансированные системы, они в достаточной степени надежны, хотя и намного более сложны, чем современные компьютерные системы. Биологические системы могут приспосабливаться к изменяющимся условиям окружающей среды. Кроме того, биологические системы используют децентрализованные механизмы управления, что позволяет им успешно сохранять работоспособность и бороться с возникающими вредоносными воздействиями.

Во многих исследованиях (например, [48–53, 55–58] и др.) утверждается, что если для защиты компьютерных систем удастся использовать механизмы, которые применяют в процессе своего существования биологические организмы, то можно добиться их высокой устойчивости к атакам, возможности самовосстановления после повреждений, необходимой масштабируемости и других важных свойств.

Создание адаптивных систем защиты информации (СЗИ) должно носить комплексный характер, в том числе предполагается, что биосистемная аналогия должна использоваться начиная с формы представления информации, программирования информационных процессов и заканчивая архитектурой систем с встроенными механизмами обеспечения безопасности.

Эволюция средств обработки информации осуществляется в направлении создания систем с элементами самоорганизации, в которых присутствуют процессы зарождения, приспособления и развития [24]. На названных процессах основаны биологические системы, для которых характерны высокая защищенность, накопление опыта эволюции, селективный отбор.

В данной статье выполнен обзор различных биоинспирированных механизмов защиты компьютерных систем и сетей. Статья не претендует на полноту изложения существующих биоинспирированных механизмов защиты, в частности в ней не рассматриваются использование биологических подходов в области криптографии, однако в ней сделана попытка представить разнообразные подходы, которые могут быть использованы для защиты компьютерных систем и сетей.

В большинстве случаев рассмотренные работы затрагивают лишь определенный класс подходов для защиты компьютерных систем и сетей: использование прямой аналогии с механизмами функционирования живых клеток; защита, базирующаяся на подходе «нервная система сети»; иммуннокомпьютинг; применение генетических алгорит-

мов (ГА), нейронных сетей (НС), нечетких множеств и нечеткой логики (НЛ), эволюционных методик, гибридных систем и др.

В работе в основном рассматриваются биологические подходы, которые можно применить для защиты компьютерных сетей. Хотя гибкость данных механизмов может дать решение и для других задач, лежащих в области защиты компьютерных систем.

Статья организована следующим образом. В разделе 2 рассмотрены основные биологические метафоры и подходы, применимые для защиты компьютерных систем и сетей. Подход к защите компьютерной сети, основанный на механизме работы клеток живого организма, представлен в разделе 3. В разделе 4 даются примеры архитектур систем защиты компьютерных сетей, к которым применима биологическая метафора. В разделе 5 описываются методы защиты компьютерных систем и сетей на основе метафоры иммунных систем и иммунокомпьютинга. В разделе 6 проанализирована обобщенная архитектура системы защиты компьютерной сети, базирующаяся на подходе «нервная система сети». Отказоустойчивые компьютерные системы, основанные на биологических подходах, рассмотрены в разделе 7. В разделе 8 рассматриваются примеры биологических подходов, которые могут использоваться для защиты программного обеспечения. Раздел 9 рассматривает применение нейронных сетей в биоподобных системах защиты информации. В 10 разделе приведены нейроэкспертные системы основанные на биометафоре. В разделе 11 представлены биологические подходы в нейро-нечетких системах. В разделе 12 проанализированы биоподобные эволюционные методы. В разделе 13 приведены гибридные интеллектуальные средства.

В заключении подводятся итоги обзора и указываются основные направления исследований в области применения биологических подходов для защиты компьютерных систем и сетей.

2. Основные биологические метафоры и подходы. На тему использования биологической метафоры написано множество статей и книг. Базовыми работами в данной области являются, например, [79, 100, 115] и др. Существует несколько обзорных работ по данной тематике, например, [5, 6, 78, 79, 95, 103, 108, 118].

Проводится множество международных конференций, например, International Conference on Bio – Inspired Models of Network, Information, and Computing Systems; International Conference on Bio –inspired Systems and Signal Processing; IEEE Symposium on Computational Intelligence in Cyber Security, ACM workshop on Survivable and self – regenerative systems и многие другие.

Опишем основные биологические метафоры и подходы и приведем их классификацию.

Живая природа предоставляет много различных типов механизмов, которые позволяют эффективно защищаться от атак и выживать. Работу таких механизмов можно наблюдать на самых различных уровнях, начиная от механизмов, выполняющих определенные действия на клеточном уровне, заканчивая распределенными кооперативными механизмами, используемыми в нервной и иммунной системах, в живом организме в целом и между различными организмами и их сообществами. Исходя из этого, можно разделить биологические подходы, применимые на микро и макроуровнях.

Заметим, что процессы, происходящие между объектами на различных уровнях, похожи. Так, внутри клетки ее элементы получают информацию, обрабатывают ее и вырабатывают определенную ответную реакцию. Такие же действия выполняются на межклеточном уровне и в различных сообществах организмов [80]. В [35, 36] утверждается, например, что биосфера представляет собой иерархическую информационную систему с единым подходом к способам и методам преобразования, хранения и переноса информации, которые обладают высокой защищенностью.

Таким образом, можно проследить некую аналогию с компьютерными системами, которые подобно биосистемам принимают, обрабатывают, хранят и передают информацию, а также с системами защиты, которые не могут находиться только на одном уровне (например, компьютеров пользователей или уровне локальной сети организации), а должны быть многоуровневыми.

О необходимости многоуровневой системы защиты говорится, например, в статье А.В.Суханова и др. [40], где рассматриваются механизмы защиты информационных систем, работающие по аналогии с биологическими системами, которые имеют различные механизмы наследования, развития, адаптации и эволюции. Биологические организмы обладают развитыми механизмами координации, реализуемыми, например, нервной системой, что позволяет биосистемам координировать свои действия и накапливать опыт. Исследователи предлагают строить системы защиты, например, на основе нейронных сетей, важным атрибутом которых является способность обучаться, что позволяет им адаптироваться к изменяющимся входным данным.

Многообразие различных механизмов, реализуемых биосистемами, вызывает определенные трудности для понимания, какие именно

из них можно использовать на данном этапе развития компьютерных технологий.

В статье Ф.Дресслер и О.Акан [80] описывается три этапа, которые необходимо пройти, чтобы иметь возможность использовать биологический механизм в компьютерных системах:

- нахождение аналогий, т.е. тех структур и методов, которые похожи как в биосистемах, так и в компьютерных системах;
- понимание того, как работает биосистема, так как необходимо наиболее точно описать и построить модель поведения биологической системы;
- использование биологического подхода в компьютерной системе. Требуется упростить модель биологической системы (без потери необходимых свойств) до такого уровня, при котором ее возможно будет реализовать в компьютерных системах.

В работе М.Мейсела и др. [108] приведена классификация биоинспирированных подходов по тем областям исследований компьютерных сетей, где они могут быть использованы. На рис.1 дано графическое представление этой классификации. Выделяется три области возможного применения биологических подходов в компьютерных системах: маршрутизация, безопасность и самоорганизация. В соответствии с областью применения даются варианты биологических подходов, которые можно применить.

Дадим краткий анализ биологических подходов, представленных на рис.1.

«Муравьиные» алгоритмы оптимизации – подход, который используется для оптимизации маршрутизации трафика в сетях. Он основан на свойстве муравьиных колоний находить наиболее короткий путь из муравьиного гнезда к пище. Для достижения этого эффекта муравьи используют так называемые феромоны, представляющие собой биологически активные вещества, вырабатываемые экзокринными железами, а также специальными клетками организма. Основные принципы поведения муравьиной колонии: простота действий каждого муравья; отсутствие централизованного контроля; косвенный обмен информацией с помощью феромона; испарение феромона с течением времени, обеспечивающее адаптивность поведения. В результате колония способна находить кратчайший путь от муравейника к источнику пищи, адаптироваться к изменяющимся условиям, находя новый кратчайший путь, если прежний стал недоступен.

На основе этого подхода был создан алгоритм Ant – based control (ABC) [123], служащий для маршрутизации в телефонных сетях. Ал-

горитмы для маршрутизации в сетях пакетной передачи данных были предложены в [126]. Алгоритм, который был назван AntNet [76], является в настоящее время возможно наиболее известной реализацией маршрутизации, основанной на «муравьиных» алгоритмах оптимизации.

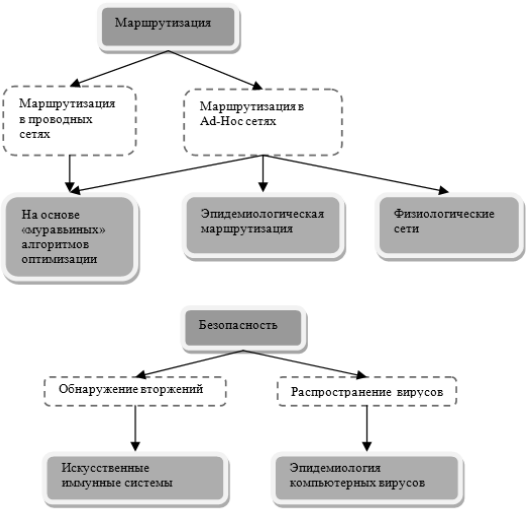


Рис. 1. Классификация биологических подходов по [45].

Метафора искусственных иммунных систем в последнее время получила широкое распространение. Иммунитет играет важную роль для выживания организма в условиях, когда его окружают бактерии и вирусы. Искусственные иммунные системы призваны защитить компьютерные системы от заражения вредоносным программным обеспечением. Комплексная система защиты, использующая метафору иммунных систем, как правило, имеет несколько уровней. Первый уровень включает межсетевой экран, который блокирует атаки, направленные во внутреннюю сеть. На втором уровне находится компонент, который обнаруживает подозрительную активность и проверяет ее на принадлежность уже известным атакам. Третий уровень служит для принятия мер по нейтрализации известных атак или, если атака не известна системе, решает, как ей противодействовать. Если неизвестная атака успешно нейтрализована, система запоминает методы противодействия этому типу угрозы безопасности. Искусственные иммунные си-

стемы, главным образом, предлагаются для реализации в системах обнаружения и противодействия вторжениям.

Ряд исследователей обращаются к подходам, используемым в эпидемиологии. В отличие от эпидемиологии, где изучается распространение инфекционных заболеваний в различных популяциях живых организмов, объектом исследований в области информационных эпидемий является распространение в компьютерных сетях как вирусов и червей, так и полезной информации. В [75] эпидемиологические алгоритмы использованы для актуализации распределенной базы данных. В [139] предложены способы эпидемиологической маршрутизации (epidemic routing). В отличие от протокола, рассмотренного в [75], где данные отправлялись всем узлам в сети, протокол, заданный в [139], обеспечивает доставку сообщения только определенному узлу сети. Исследования в [139] показали, что предложенный протокол эпидемиологической маршрутизации обеспечивал доставку сообщения в 100% случаев, расходуя небольшой объем трафика. Однако позже было обнаружено, что работа протокола очень сильно зависит от топологии сети.

Сегодня Интернет предоставляет множество постоянно меняющихся и вновь разрабатываемых сервисов. Чтобы поддерживать эти сервисы, необходимо использовать сложные информационные системы, которые требуют постоянного контроля и конфигурирования. Из-за того, что сеть Интернет постоянно растет, а предоставляемые ею услуги усложняются, требуется все больше человеческих усилий для поддержания надлежащей работы сети и предоставления сервисов. Для решения данной задачи биологические подходы предоставляют возможность повышения степени автономности сервисов и их способности к самоорганизации. Пример использования данного подхода для решения указанной задачи дан в [140]. В этой работе представлена архитектура сети Интернет, основанная на поддержке жизненного цикла кибернетических объектов. В соответствии с данной архитектурой кибер –объекты, подобно биологическим существам, могут самовоспроизводиться, умирать, мигрировать из одной части сети в другую. Сеть представляет собой множество платформ, где могут функционировать кибер –объекты. Выполняя действия, кибер –объекты потребляют энергию, предоставляя пользователям различные сервисы, например, доступ к веб-страницам. Они тратят энергию, когда используют ресурсы своей платформы, такие как процессорное время или память, или мигрируют на другую платформу.

В биологии таксис означает ответную реакцию организма на раздражитель. Термин дататаксис был сформулирован в [107] для описания движения агентов по направлению к наивысшей концентрации данных. В этой работе datataxis был использован для маршрутизации транспортных агентов. Основная цель агентов — сообща собрать как можно больше данных. Транспортные агенты могут ставить метки на данных, которые они уже собрали. Поэтому агенты, пытающиеся повторно собрать данные, могут определить, что данные уже собраны, и повторный сбор не требуется.

Многие беспроводные сети, например, сенсорные сети, требуют синхронизированного выполнения определенных операции своих сетевых узлов (сенсоров). В живой природе такие действия выполняются в отдельном организме (например, при биении сердца) или в симбиозе организмов (например, при синхронном мигании светлячков). В [109] предложена формальная модель этого явления, которое названо импульсно-зависимым осциллятором (pulse – coupled oscillator). Хотя данная модель накладывает некоторые ограничения на ее применение в реальных беспроводных сетях, она позволяет создавать различные алгоритмы синхронизации для беспроводных сетей.

Физиология изучает внутреннюю работу живого организма. В ряде работ в области беспроводных и сенсорных сетей была сделана попытка создать структуру сети, похожую на физиологическую сеть. Например, в [120] предложена архитектура сенсорной сети, в которой потоки информации циркулируют подобно потокам крови в живом организме. Для каждого соединения поток информации направлен только в одну сторону. Это дает определенные преимущества. Например, всегда доступны дополнительные соединения без необходимости переназначения маршрута для пакетов. В результате в некоторых случаях увеличивается эффективность функционирования компьютерных сетей.

В [80] предлагается выделить классы биологических подходов, которые могут применяться для решения определенных задач в компьютерных системах: оптимизация и распознавание различных сущностей, построение больших распределенных и взаимодействующих систем, например, для распределенного зондирования и разведки, построение эффективных и масштабируемых сетей в условиях неопределенности параметров сети.

Представим ниже наиболее интересные исследовательские работы в области защиты компьютерных систем и сетей, в которых была использована биологическая метафора.

3. Обработка и передача информации на основе аналогии с живыми клетками. В работе Ф.Дресслера [77] за основу механизма защиты компьютерных сетей взята аналогия с живыми клетками. Локальная передача данных осуществляется от клетки к клетке, сигнал попадает на рецептор клетки и приводит к ответной реакции, которая влияет на соседние клетки (рис. 2). Монитор, сканирующий трафик, отправляет собранные данные системе обнаружения вторжений (СОВ), которая после получения и обработки этих данных вносит новые правила в межсетевые экраны.

Обмен информацией с удаленными компьютерами осуществляется похожим образом (рис. 3). Белки (красные и синие фигуры) используются как служебные данные, с помощью которых клетки взаимодействуют друг с другом. Сигналы передаются потоком крови, который переносит белки во все части организма. Таким образом, одни клетки могут вызвать ответную реакцию в других клетках, что позволяет активизировать различные вспомогательные элементы (например, компоненты иммунной системы). При этом информация передается только определенным типам клеток. Это происходит за счет выработки специфического белка, который могут улавливать лишь клетки, обладающие определенным типом рецептора.

Предлагаемый Ф.Дресслером [77] механизм защиты компьютерной сети имеет аналогичный характер. Монитор передает данные определенным блокам защиты, которые, в свою очередь, могут реагировать на возникающие события.

Как видно из данного описания авторы используют здесь слишком обобщенную аналогию.

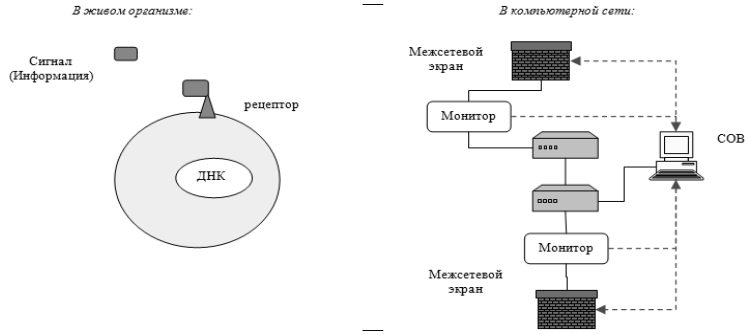


Рис. 2. Локальный обмен информацией: между клетками (слева) и в компьютерной сети (справа).

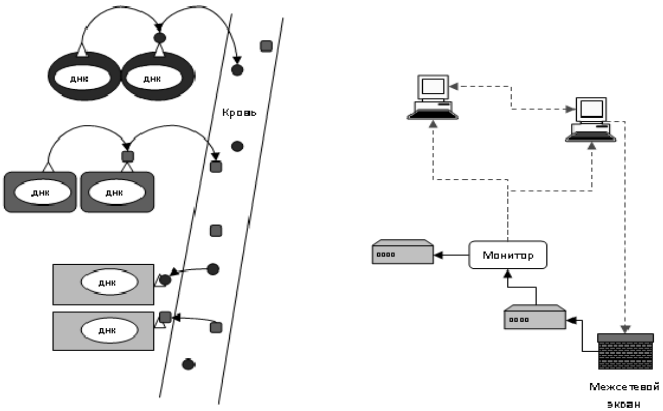


Рис. 3. Удаленный обмен информацией: между клетками (слева) и между сетевыми доменами (справа).

4. Примеры архитектур систем защиты компьютерных сетей, к которым применима биологическая метафора. Пример архитектуры типичной компьютерной сети, включая средства защиты, представлен на рис.4. На рисунке изображены базовые компоненты, которые обычно используются для построения сети организации. Если провести параллель с человеческим организмом и использовать некоторые условности, то можно задать компьютерную сеть как сильно упрощенную модель человеческого организма. Мы можем представить, что информация, поступающая в сеть извне и введенная с помощью различных устройств ввода, является пищей или воздухом, и эта информация необходима различным органам, которые в компьютерной сети соответствуют различным компьютерам и устройствам. В свою очередь, организм должен защитить внутренние органы от болезнетворных бактерий, вирусов и других угроз, поэтому он имеет различные защитные системы, которые препятствуют попаданию в него болезнетворных организмов и уничтожают их после проникновения внутрь. В компьютерной сети такими компонентами системы защиты являются такие компоненты, как межсетевой экран, система обнаружения вторжений (СОВ), антивирусные системы и др. Хотя данные системы достаточно эффективны, уязвимости программного обеспечения, человеческий фактор, несовершенные механизмы защиты и постоянное появление новых видов атак и механизмов их проведения зачастую сводят на нет те усилия, которые принимаются для защиты компьютерных сетей.

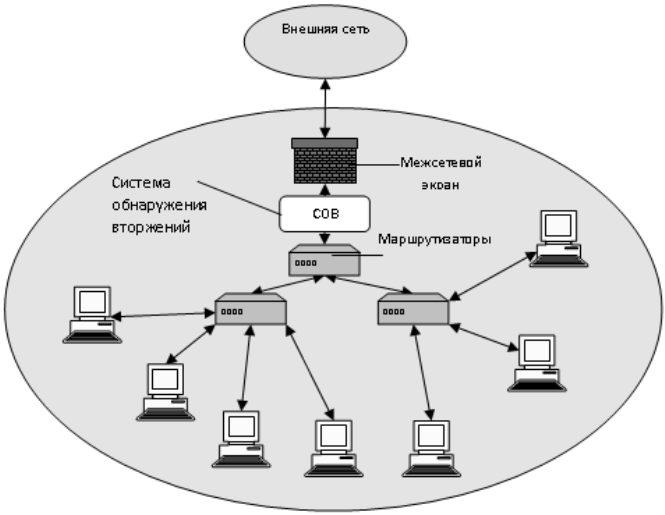


Рис. 4. Пример архитектуры типичной компьютерной сети.

Рассмотрим несколько практических решений, которые используют биологическую метафору.

Компания Hewlett-Packard (HP) пропагандирует технологию ProCurve [127]. В основе технологии 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. При этом главные маршутизаторы (core routers), которые часто выполняют функции по защите сети, заменяются упрощенными аналогами, которые отвечают, в основном, за высокоскоростную маршрутизацию пакетов.

Фирма Cisco, в свою очередь, применяет концепцию самозащищающейся сети (Cisco's Self – Defending Network) [59]. Для защиты передаваемых по сети данных используются защищенные протоколы и технология VPN. Для защиты от внешних угроз задействуется интегрированная система, состоящая из различных компонент защиты, таких как межсетевые экраны, системы предотвращения вторжений, системы защиты от DDoS – атак и др. Для защиты клиента используется специальный программный агент, который служит для конфигуриро-

вания клиента в соответствии с заданной политикой безопасности, используемой в компьютерной сети. Также обеспечивается базовая аутентификация пользователей и проверка на соответствие клиента заданной в сети политики 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.

В работе А.Лукацкого [78] описана концепция самозащищающейся сети и раскрыты причины, из-за которых усилия по построению систем защиты часто терпят неудачу, а также рассматривается подход к защите компьютерной сети по принципу иммунной системы живого организма. Описываются принципы построения инфраструктуры, которая может распознавать компьютеры пользователей по принципу “свой – чужой”, а также защита на основе проверки компьютера на соответствие политикам безопасности, применяемым в системе, к которой производится подключение. В случае несоответствия требуемому уровню защищенности проверяемый компьютер может быть отправлен на карантин, где, если это возможно, путем установки патчей, обновления антивируса и других операций уровень его защищенности будет повышен, или же компьютеру будет предоставлен ограниченный доступ или отказано в доступе. Предлагается внедрять данную технологию в локальные коммутаторы и другое сетевое оборудование.

В статье К.Анагностакиса и др. [51] предлагается кооперативный механизм защиты от вирусов COVERAGE (Cooperative virus response algorithm), основанный на иммунологии. В этой работе была предпринята попытка реализовать такие свойства и механизмы иммунных систем живых организмов как адаптивность, децентрализованная архитектура, механизмы коммуникации.

Авторы работы также попытались оптимизировать стоимость сканирования и фильтрации пакетов для детектирования вирусов несколькими способами.

Во-первых, COVERAGE определяет уровень опасности вирусов и ранжирует их в соответствии с уровнем вредоносности. После этого, если нагрузка на систему сильно возрастает, подобно биологическим системам, COVERAGE принимает решение о том, стоит ли продолжать отслеживать вирусы в соответствии с уровнем их угрозы.

Во-вторых, все агенты COVERAGE, как и клетки живых организмов, обменивается информацией о потенциальном вирусе между собой, для того чтобы построить модель работы вируса, и эмпирически

пытаются определить, соответствует ли информация о вирусе, поступающая от других агентов, тому, что происходит в сети.

В-третьих, агенты COVERAGE определяют частоту опроса друг друга для правильного оценивания вирусной опасности и своевременного обмена новыми данными.

Как и в иммунной системе, в предлагаемой системе защиты нет единого центра управления, и каждый из агентов выбирает другого агента для обмена данными произвольно. Предполагается, что небольшое количество узлов может отправлять ложные сведения. Поэтому узел для коммуникации, выбранный произвольно, предоставляет более надежные данные, так как если агент будет общаться только с определенными агентами, возникнет большая вероятность, что злоумышленник попытается подменить или уничтожить агентов, расположенных на этих узлах. После получения ответа агент обновляет свои данные для того, чтобы знать о текущем состоянии сети и быть готовым к выполнению совместных действий с другими агентами по отражению атак. Информация, поступающая от других агентов, содержит сведения о состоянии удаленного агента и выполнении им сканирования сети. Это позволяет локальному агенту найти агентов, которые выполняют поиск определенных вирусов в сети, а также дает возможность агенту найти зараженные узлы. Авторы различают два типа оценок — прямые и удаленные. Прямые — это те оценки, которые выставляют агенты, непосредственно детектирующие атаку (на него самого, на роутер или другой узел в сети). Удаленные оценки основываются на оценках, полученных от удаленных агентов.

Приведенные примеры архитектур систем защиты компьютерных сетей в сочетании с комбинированием механизмов защиты от сканирования в компьютерных сетях [42, 19] являются перспективным направлением развития в области защиты информации.

5. Искусственные иммунные системы и иммуннокомпьютинг. В последнее время появилось много работ, посвященных искусственным иммунным системам. Искусственные иммунные системы (AISs — Artificial immune systems) [65, 71] и иммуннокомпьютинг (IC — Immunocomputing) [130, 131, 142] часто воспринимаются исследователями как интерпретация генетических алгоритмов [133] и искусственных нейронных сетей (ANNs — Artificial neural networks), которые также называют нейрокомпьютингом [132].

В статье [69] приведено описание моделей и подходов, используемых исследователями для построения искусственных иммунных систем.

Труды СПИИРАН. 2011. Вып. 3(18). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2011. Issue 3(18). ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiras.nw.ru

В таблице 1 даны некоторые модели искусственных иммунных систем.

Таблица 1. **Модели искусственных иммунных систем** [69]

Автор работы, год опубликования и ссылка на работу	**Описание модели или подхода**	**Моделируемые фрагменты биологической иммунной системы (БИС)**	**Тип использованных данных**	**Область применения**
Д.Хант и др., 1999 [96]	Система машинного обучения на основе иммунных систем	Связь AG-AB (антиген-антитело). Иммунные сети	Комбинация цифровых и текстовых данных, категории	Обнаружение обманных действий. Обучение
Д.Дасгупта, 1999 [66]	Агентно-ориентированная система обнаружения вторжений/аномалий и противодействия им	Распределенное управление. Опознание «свой-чужой»	Объекты Java (аплеты)	Защита информации
Д.Дасгупта и др., 1999 [67]	Комбинация иммунных систем и генетических алгоритмов для интерпретации химического спектра	Связь AG-AB. Опознание «свой-чужой»	Бинарные строки	Распознавание химического спектра
П.Уильямс и др., 2001[141]	Мультиагентные вычислительные иммунные системы для обнаружения вторжений	Связь AG-AB. Опознание «свой-чужой»	Строки из ограниченного набора символов	Защита информации
А.Тараканов и Д.Дасгупта, 2000	Формальная модель иммунной системы	Связь AG-AB.	Вектора данных	Моделирование биологических

[128]				иммунных систем
Д.Тиммис, 2000 [134]	Искусственная иммунная система с ограничением ресурсов для анализа данных	Связь AG-AB. Иммунная сеть	Вектора данных	Анализ данных, кластеризация
Л. Де Кастро и Ф. Фон Зубен, 2000 [72]	Система, основанная на вегетативном отборе и созревании аффинности (повышении силы связей антиген - антитело)	Связь AG-AB. Клональная селекция. Созревание аффинности	Бинарные и целочисленные строки	Нахождение одинаковых объектов, оптимизация.
Л. Де Кастро и Ф. Фон Зубен, 2001 [73]	Алгоритм обучения иммунных сетей	Связь AG-AB. Клональная селекция. Созревание аффинности. Иммунные сети	Вектора данных	Анализ данных, кластеризация
С.Хофмейер, С.Форест, 2000 [94]	Архитектура искусственных иммунных систем	Связь AG-AB. Опознание «свой-чужой». Созревание аффинности	Бинарные строки	Защита информации
Д.Бредли, А.Таррелл, 2000 [57]	Машинные отказоустойчивые механизмы, основанные на иммунных системах	Опознание «свой-чужой»	Бинарные строки	Аппаратное обнаружение ошибок и отказоус – тойчивость
Л. Де Кастро и Ф. Фон Зубен, 2001 [74]	Имитация алгоритма восстановления, основанного на иммун-	Опознание «свой-чужой». Иммунное разнооб-	Вектора данных	Задание весов в нейронной сети напрямую

Труды СПИИРАН. 2011. Вып. 3(18). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2011. Issue 3(18). ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiras.nw.ru

	ных системах для инициализации нейронных сетей	разие		
А.Тараканов и Д.Дасгупта, 2002 [129]	Архитектура для построения микросхем на основе модели иммунной системы	Связь AG-AB. Иммунные сети	Вектора данных (состоящие из битов)	Распознавание шаблонов
О.Насраоуи и др., 2002 [113]	Иммунная сеть, основанная на алгоритме, использующем нечеткую логику для моделирования совпадения AG-AB	Связь AG-AB. Иммунная сеть	Вектора данных	Кластеризация, извлечение данных из веб-ресурсов
Е.Харт, П.Росс, 2002 [92]	Система для кластеризации данных с помощью комбинации механизмов	Связь AG-AB. Иммунная память	Бинарные строки, ассоциативная память	Кластеризация
К.Коелло, Н.Корес, 2002 [61]	Подход для управления ограничениями на основе генетической оптимизации	Связь AG-AB. Генетические библиотеки	Бинарные строки	Оптимизация
Д.Ким, П.Бентли, 2002 [102]	Алгоритм для выполнения динамического обучения в изменяющемся пространстве	Связь AG-AB. Клональная селекция. Опознание «свой-чужой»	Бинарные строки	Динамическое обучение
О.Насраоуи и др., 2003 [114]	Модель масштабируемой искусственной иммунной системы	Связь AG-AB. Иммунная сеть	Вектора данных	Кластеризация. Динамическое обучение

	для динамического обучения без учителя, основанная на теории иммунных сетей			
Д.Дасгупта и др., 2003 [68]	Алгоритм многоуровневого иммунного обучения	Отрицательный отбор. Клональная селекция. Антиген-презентирующие клетки (APC).	Различные представления и правила, спектральная оптимизация	Обнаружение аномалий, распознавание шаблонов
А.Икбал, М.Маароф, 2004 [99]	Модель искусственных клеток антигенов	Теория катастроф (Danger Theory)	Строки	Кодоны, детектирующие опасные данные (единицы генетического кода)
С.Степни и др., 2004 [124]	Концептуальные разработки	Иммунная система в целом	Общие положения	Концептуальная модель
З.Джи, Д.Дасгупта, 2004 [101]	Оценивание	Отрицательный отбор	Вектора данных	Общее применение
Д.Галеано и др., 2005 [85]	Модель компьютерной сети	Иммунная сеть	Данные	Обзор
П.Андрюс, Д.Тиммис, 2005 [52]	Опознание «свой-чужой»	Новые теории по иммунным системам	Клеточные автоматы	Общее применение
Т.Стибор, 2005 [125]	Способы применения алгоритма отрицательного отбора	Опознание «свой-чужой».	Вектора данных	Обнаружение аномалий
У.Айкелин, С.Цаузер, 2002 [49]	Теория катастроф (Danger Theory)	Врожденный иммунитет	Строки данных	Защита компьютерных сетей

В [133] определяется, что иммуннокомпьютинг основан на принципах обработки информации белками и иммунными сетями. Так как искусственная нейронная сеть формируется как сеть искусственных нейронов, основное различие между нейрокомьютингом и имунно-комьютингом проявляется в том, что искусственная формальная иммунная сеть (FIN – formal immune network) представляет собой сеть свободного взаимодействия (связей) между формальными белками.

Также в иммуннокомпьютинге используется понятие биомолекулярный иммуннокомпьютер, как компьютер, который контролирует фрагмент природной иммунной системы [87].

Объединение иммуннокомпьютинга с исследованиями мозга помогает обнаруживать глубокое функциональное сходство между мозгом и иммунной системой, включая сети цитокина, рецептор мозаики [50] и нанотрубки в нервных и иммунных синапсах.

Совместное использование иммуннокомпьютинга и ячеистого автомата (CA) [48] дает хорошие результаты в трехмерной компьютерной графике. Последние достижения в разработке реальных программ с использованием иммуннокомпьютинга включают интеллектуальную реконструкцию и моделирование гидрофизических полей, а также обработку сигналов и обнаружение вторжений в компьютерных сетях.

В работе С.Форест и С.Хофмейера [93] представлен подход, основанный на концепции иммуннокомпьютинга и использовании алгоритма отрицательного отбора (Negative Selection Algorithm). Компонент, реализующий этот подход, работает по аналогии с антителами, которые уничтожают все чужеродные объекты в теле человека.

При построении модели пространства объектов и (или) событий разделяются на две части: «свои» (self) и «чужие» (nonself). «Свои» — это все события, которые носят легитимный характер, а «чужие» — это события, которые вызваны злоумышленниками. Система обнаружения аномалий должна отличать эти два класса событий.

На рис. 5 изображена обобщенная схема обнаружения аномалий. Объект, закрашенный темным цветом, относится к «своим», а все пространство вне объекта относится к «чужим». Результат работы системы обнаружения атак с использованием алгоритма отрицательного отбора представлен контурной линией. При выполнении обнаружения атак возможны как ошибки первого, так и второго рода, т.е. ошибки типа «свой» объект определен в качестве

«чужого» (False Positives) и «чужой» объект определен в качестве «своего» (False Negative).

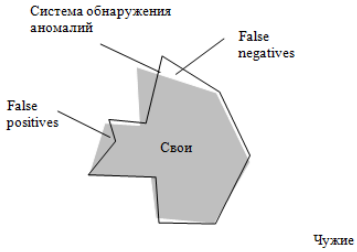


Рис. 5. Схема обнаружения аномалий.

Для того чтобы система могла точно определить, где свой и где чужой, в работе предлагается использовать детекторы, которые реагируют только на «чужие» элементы. Для создания таких детекторов разрабатывается специальный алгоритм обнаружения. Случайно сгенерированный детектор тестируют, проверяя на «правильном» наборе данных. Если детектор срабатывает, его удаляют и генерируют новый. Таким образом, создается набор детекторов, которые срабатывают на «чужих» и не обнаруживают «легитимные» события.

На рис.6 представлена упрощенная схема генерации и проверки детекторов. Генерируемый детектор представляется в виде малого круга, который попадает или не попадает в пространство «своего» объекта, закрашенного темным цветом. В результате образуется набор детекторов, не попадающих в пространство «своего» объекта.

После этого создается распределенная система детектирования, т.е. детекторы распределяются между различными хостами, которые могут взаимодействовать для обнаружения аномалий.

При этом возникает так называемая проблема «дыр». Она состоит в том, что детекторы определенного вида, натренированные на одном типе данных, могут пропускать другие данные, в том числе похожие на те, на которых производилось обучение.

Для устранения данной проблемы предлагается исследовать различные типы наборов данных для генерации детекторов. На рис.7 изображен «свой» объект, на котором тестируют наборы детекторов разного типа, представленных в виде малых кругов и овалов. Наборы детекторов разных типов объединяют.

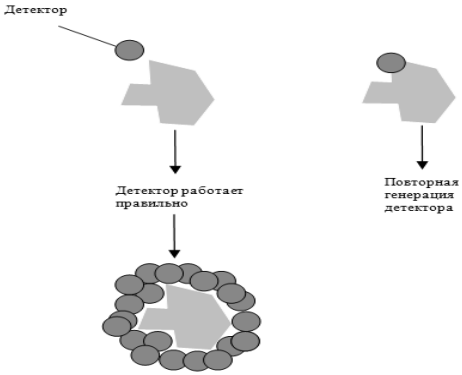


Рис. 6. Генерация и проверка детекторов.

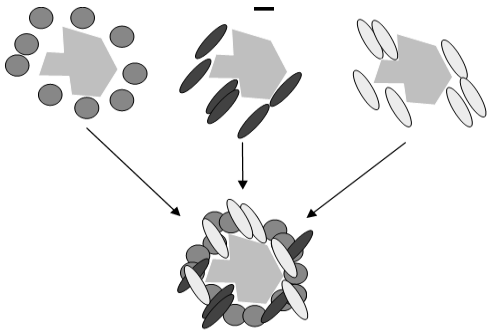


Рис. 7. Объединение наборов детекторов разных типов для обнаружения аномалий.

В работе Д.Дасгупты [70] предлагается использовать различные механизмы защиты, применяемые живыми организмами, и адаптировать их для работы в компьютерных системах. Предлагается многоуровневая система защиты от атак на основе иммунокомпьютинга, различные уровни которой представлены на рис.8.

Предполагается, что межсетевой экран блокирует нежелательный трафик и подозрительные попытки установки соединения, система аутентификации проверяет у пользователя права доступа к сети, механизм контроля доступа обеспечивает разрешение выполнения программ и доступа к данным в соответствии с заданными привилегиями.

Другие компоненты систем защиты обеспечивают активный и пассивный мониторинг работы системы [55, 56].

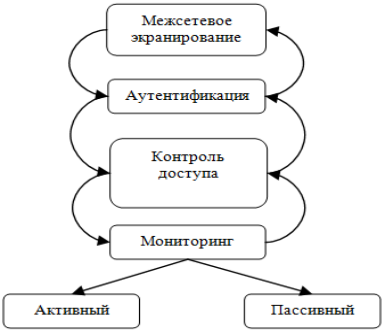


Рис. 8. Многоуровневая система защиты компьютерных сетей.

Выделяется два базовых способа коммуникации в иммунных системах — свободное распространение сигнала и диалог. Свободное распространение сигнала подразумевает то, что сигнал передается от одной клетки к другой без использования обратной связи. Диалоговая схема подразумевает обмен информацией с соседними клетками.

Одной из основных проблем, возникающих при использовании комплексных многоуровневых систем защиты, является то, что отдельные компоненты этих систем часто никак не обмениваются данными и работают независимо, вследствие чего затруднительно сформировать и применять общую согласованную политику безопасности системы. Если бы системы могли также эффективно взаимодействовать и обмениваться информацией, как это делают иммунные системы, можно было бы существенно улучшить эффективность защиты.

Предполагается, что иммунные системы определяют уровень угрозы организму и вырабатывают соответствующую реакцию на основе множества различных поступающих сигналов. Поэтому необходимо использование механизмов слияния и учета информации из разных источников. Подобный механизм детектирования угроз и реагирования на них мог бы оказаться очень полезным для различных компонентов системы защиты.

В [70] утверждается, что для решения задачи классификации угроз иммунные системы используют механизм распределенного управления. В иммунной системе нет единого центра управления работой иммунной системы. Взаимодействие осуществляется с помощью

передачи сигнала от клетки к клетке. Хотя такая система защиты довольно сложна в реализации, но зато позволяет избежать ситуации, в которой при повреждении или уничтожении центра управления система защиты полностью отказывает.

В [70] также сопоставляются процессы, происходящие в биологической и компьютерной системах. Биологические процессы, протекающие в организме, делятся на несколько уровней. К этим уровням можно отнести молекулярный, клеточный, протеиновый и генетический. Для того чтобы поставить диагноз, врач обычно просматривает данные анализов, в которых имеется информация о процессах, происходящих на этих уровнях. Похожим образом компьютерная система защиты может следить за различными уровнями: приложений, пользователя, системным, процессов и пакетов (рис. 9).

Например, система защиты на уровне пользователя будет искать необычный шаблон поведения пользователя, на уровне системы - просматривать применение различных ресурсов системы (процессор, оперативная память, система ввода-вывода), на уровне процессов - проверять наличие запрещенных процессов или процессов, пытающихся получить доступ к закрытым файлам, на уровне пакетов — контролировать потоки информации (число, объем и размер пакетов наряду с источником данных). На основании полученных данных можно сделать вывод о работе системы и принять соответствующие меры по ее улучшению.

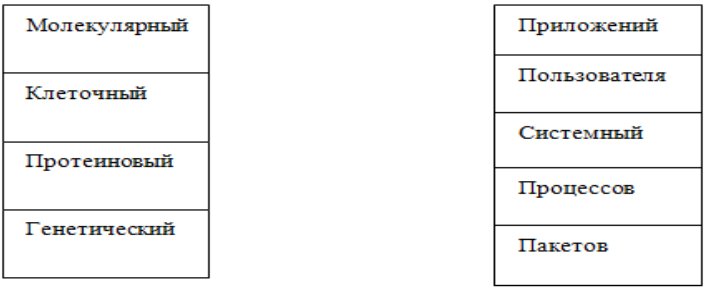


Рис. 9. Пример деления систем на уровни в живой природе (слева) и в компьютерной системе (справа).

В подходе, предлагаемом А.Тараканом [130], используется формальная иммунная сеть (FIN).

В режиме обучения формальная иммунная сеть может формироваться с помощью поступающих сигналов, используя трансформации

(преобразования) дискретного дерева (DTT — discrete tree transform) и/или декомпозиции сингулярного значения (SVD — singular value decomposition).

Формальная иммунная сеть определяется как множество ячеек *(FIN = V1, V2 .. Vn).*

С помощью цитокинов («пересыльщиков белков») выполняются процедуры apoptosis («запрограммированная смерть ячейки») и иммунизации [60]. Результатом такого выделения признаков с помощью формальной иммунной сети является оценка индекса неотделимости.

В режиме распознавания текущие сигналы обрабатываются с использованием трансформации дискретного дерева, передаются в формальную иммунную сеть и распознаются цитокином в самой близкой точке (ячейке) формальной иммунной сети.

На рис.10 показано применение этого подхода. На рисунке представлена общая схема распознавания шаблона с помощью формальной иммунной сети. В режиме обучения на вход системе подают множество обучающих сигналов *(Ag1..n)*. Те значения, которые попали в область *FIN*, будут являться шаблонами для распознавания реальных значений. В режиме распознавания подается сигнал *Agi*. При попадании сигнала в область *FIN* определяется, к какому из тестовых значений он наиболее близок. В представленном случае он наиболее близок к сигналу *Agx*, и, соответственно, система определяет, что сигнал *Agi* принадлежит к тому же классу, что и сигнал *Agx*.

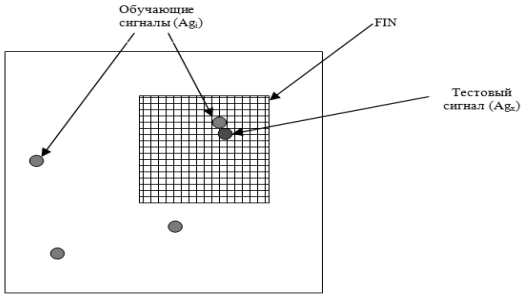


Рис. 10. Распознавание шаблона с помощью формальной иммунной сети.

6. Защита компьютерных сетей на основе подхода «нервная система сети». Нервная система, как адаптивный инструмент управления и взаимодействия со средой, очень важна в эволюции биосистем. Нервная система необходима для создания рефлексов в ответ на воздействия [77]. Рефлексия — продукт верхних уровней системы защиты

информации (СЗИ), а информация о механизмах реализации рефлексов хранится на нижних уровнях СЗИ (в генетической памяти) и является наследуемой.

Поведенческие реакции в биосистеме, определяемые нервной системой, информируют 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, а фиксируется в информационном поле нервной системы [77].

За основу для разработки подхода к защите компьютерных сетей, называемого «нервная система сети», который был предложен, например, в работе Ю.Чена и Х.Чена [60], была взята нервная система человека.

Нервная система пронизывает все тело человека и служит системой сбора, передачи, обработки информации, а также вырабатывает ответную реакцию на различные раздражители [58].

Система защиты, основанная на данном подходе, 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.

Если рассматривать распределенную систему защиты (фрагмента) сети Интернет на основе этого подхода, то ее можно представить как нервную систему человека (рис.11).

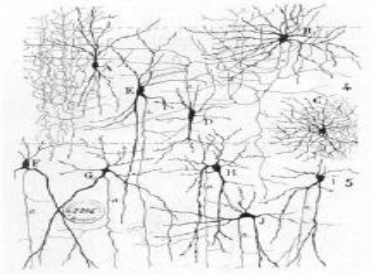


Рис. 11. Нервная система человека.

Предполагается, что сетевые домены Интернета – провайдеров (ISP) или автономные системы (AS) соединены между собой как физи-

чески связанные нейроны. В каждом домене есть специальный сервер (или кластер серверов). Этот сервер выполняет роль сомы в нейроне (сома является центральной частью нейрона, рис. 12), в нем реализуется большая 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).

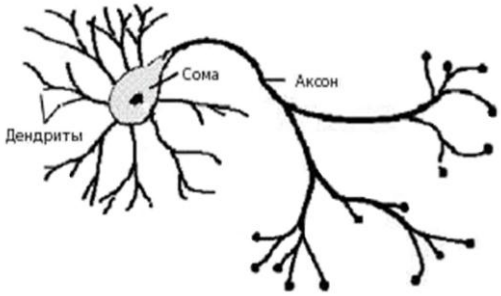


Рис. 12. Биологический нейрон.

Таким образом, на основе метафоры нервной системы сети предлагается адаптивная сетевая инфраструктура, обеспечивающая получение информации, ее передачу на специальный сервер и принятие решений исходя из сложившейся ситуации.

Как и у центрального тела нейронов, у серверов, расположенных в каждой автономной системе, есть и другие функции. Кроме выполнения вычислений по обработке и анализу данных, серверы также отвечают за коммуникацию с другими автономными системами и отправку команд на сетевые устройства, чтобы вовремя принять контрмеры.

Точно так же маршрутизаторы, с одной стороны, выполняют функции распределенных сенсоров в процедуре сбора информации, контролируя состояние сети, а с другой стороны, функционируют как распределенные устройства, которые способны выполнять команды, например, когда им посылается команда принять контрмеры против определенных атак злоумышленников, например, атак «распределенный отказ в обслуживании», рассылки спама и др. [22, 44, 45].

Для обеспечения безопасности системы в [60] предлагается протокол IFSec (infrastructure security protocol), являющийся новым прото-

колом 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 (сомой) в домене. IFSec строится как надстройка IP и работает прозрачно, чтобы транспортировать протоколы более высокого уровня.

В основе предлагаемой многоуровневой системы безопасности лежит механизм обмена информацией под названием “Адаптивное Согласование Доверия и Управление доступом” (Adaptive Trust Negotiation and Access Control — ATNAC), который был предложен в работе Т.Руйтов и др. [121].

Архитектура системы, основанной на данном подходе, представляется следующим образом. Домены сети, которые подключены к нервной системе сети, формируют оверлейную сеть и взаимодействуют между собой через каналы VPN, установленные между специализированными серверами безопасности (рис. 13). Маршрутизаторы, расположенные в разных точках сети, взаимодействуют не только друг с другом, но и со специализированным сервером безопасности в своем домене.

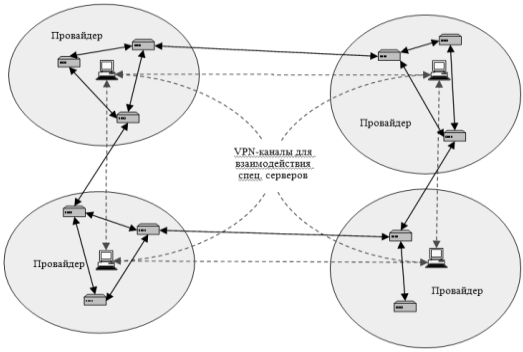


Рис. 13. Обобщенная архитектура компьютерной сети, построенной на основе подхода «нервная система сети».

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.

Идея этой модели возникла из аналогии с нервной системой живых существ. Кооперация распределенных узлов происходит подобно реакции человеческой нервной системы. Одиночные узлы работают не только как исполнители, но так же и как сенсоры. Помимо общей защиты, которая осуществляется ими самостоятельно, они так же предоставляют результаты анализа данных другим узлам и серверам безопасности. Серверы безопасности тоже выполняют две роли. Прежде всего, они функционируют как координаторы, направляя управляющие сигналы к узлам в своих управляющих доменах. Так же они работают как дистрибьюторы, получая полезную информацию от узлов в своих доменах и обмениваясь ею с другими серверами безопасности, распределяя полученную от них информацию собственным узлам.

7. Отказоустойчивые компьютерные системы, основанные на биологических подходах. Одним из важных направлений использования биологических подходов являются отказоустойчивые компьютерные системы (Biologically Inspired Fault – Tolerant Computer Systems).

В работе Э.Тайррелла [135] предлагается концепция использования свойств биологических организмов для создания отказоустойчивых систем. Такие системы позволяют избежать полного отказа оборудования при каких –либо повреждениях таким же способом, как и биологический организм продолжает функционировать при повреждении некоторого не жизненно важного органа.

Разработка методов, обеспечивающих устойчивость к отказам, необходима для увеличения живучести системы, чтобы можно было бы гарантировать работоспособность системы, несмотря на появление сбоев и отказов.

В живых системах достигнуты такие уровни сложности и надежности, которые превосходят уровни, созданные в любой компьютерной системе: в триллионах компонентов, из которых состоит человек, ошибки появляются очень редко, и в большинстве случаев (хотя не всегда, как в случае, когда иммунная система воспринимает свои клетки за чужие) они успешно обнаруживаются и исправляются. В любом живом существе все составляющие его клетки содержат ДНК, чтобы производить белки, необходимые для выживания организма. От того, какая часть (или части) ДНК интерпретируется, зависит физическое расположение клетки и ее отношение к соседям.

В [135] используется понятие эмбриоников (эмбрионной электроники), основывающейся на процессах молекулярной биологии и эмбриональном развитии живых существ. Понимая определенные спо-

собности клеточной организации и перемещая их в мир интегральных схем, те свойства, которые уникальны для живого мира, такие как саморепликация и самолечение, также могут быть применены к искусственным объектам. Самолечение позволяет выполнить частичную реконструкцию в случае незначительной ошибки, в то время как самокопирование (саморепликация) позволяет полностью восстановить исходное устройство в случае если произойдет серьезный сбой.

Основная цель эмбриоников состоит в том, чтобы перенести основные свойства к двумерному миру клеточных массивов, используя специальным образом разработанные программируемые логические интегральные схемы FPGA как строительные блоки.

В любой эмбриональной системе каждая из ячеек, основанных на FPGA, интерпретирует регистр конфигурации, находящийся в ее памяти независимо от специфической логической функции, которую она выполняет. То, какой регистр конфигурации должен интерпретироваться, будет зависеть от координат ячейки, определяемых по ее соседям. Э.Тайррелл [135] также рассмотрел возможность создания иммунных систем на основе аппаратных средств.

Чтобы увеличить потенциальную надежность систем, предлагается использовать также биологические иммунные системы – иммунотроники.

В статье М.Атигетши и П.Пала [53] описываются исследования в области адаптивных и самовосстанавливающихся систем. Авторы используют биологическую метафору, которая, по их мнению, поможет создать новые адаптивные и самовосстанавливающиеся компьютерные системы.

На ранних этапах авторы были нацелены на увеличение защищенности и живучести за счет внедрения систем защиты непосредственно в защищаемые приложения. Механизм защиты должен был определять наиболее потенциально возможные атаки и ранжировать их по степени опасности. Также он должен был определять, в какой очередности могли выполняться атаки на систему.

Затем была создана стратегия автономной защиты компьютерной системы. Была использована концепция реактивной защиты. Для выполнения функций противодействия атакам использовались широко доступные инструменты, такие как межсетевые экраны или антивирусное программное обеспечение. На локальном уровне применялись сенсоры, связанные с механизмом реагирования на различные изменения в окружающей среде. Разработанный механизм защиты имел высокий уровень предсказуемости, что могло бы позволить злоумыш-

леннику (после изучения реакции системы на различные атаки) построить схему нападения таким образом, что система защиты не смогла бы эффективно бороться с ней.

Поэтому авторы внесли элементы изменяющегося поведения. На сетевом уровне были использованы динамические схемы маршрутизации, изменяющаяся информация о компьютерах в сети и изменяющиеся правила в межсетевых экранах. На уровне приложений были введены менеджеры приложений и специальный протокол, которые уничтожали неправильно работающие процессы и запускали их заново. Менеджеры приложений использовали специальный алгоритм голосования, на основе которого принималось решение об уничтожении неправильного работающего процесса, для того чтобы получить более адекватный механизм перезапуска приложений. Все компьютеры в сети были включены в защищенные домены, которые обеспечивают периметр защиты.

Эксперименты показали высокий уровень устойчивости по отношению к атакам, но для управления данной системой защиты требуется высококвалифицированный персонал. Авторы рассматривают полностью автономные системы как следующий уровень самоуправляемых и самовосстанавливающихся систем.

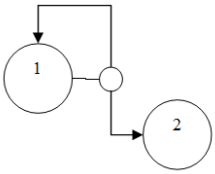
8. Биологические подходы для защиты программного обеспечения. Программное обеспечение, которое обладало бы устойчивостью к возникновению ошибок или возможностью самолечения, могло бы быть очень полезно в ситуациях, когда восстановление системы человеком затруднено или невозможно.

В живых организмах такие процедуры восстановления закодированы в ДНК: организм способен восстанавливать поврежденные части, используя код, заложенный в ДНК, как основу для воссоздания поврежденных тканей. Имея больше знаний о механизмах саморепликации живых организмов, можно разработать новые методы создания программного обеспечения, которые обеспечили бы достижение таких задач как самолечение и самовосстановление. Это повлекло бы создание новых робастных систем, устойчивых как к возникновению внутренних ошибок, так и к атакам на них извне.

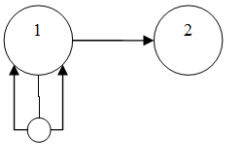
В работе С.Джорджа и др. [86] предлагается модель функционирования программы, основанная на работе клетки живого организма. Исследователи представляют программу жизнедеятельности клетки как автомат, содержащий дискретные состояния и переходы между этими состояниями. На вход каждой клетке подаются параметры среды, в которой она находится, а на выходе выполняется переход в дру-

гое состояние или происходит деление клетки на два (или более) состояний.

На рис.14 состояния показаны большими кругами, а переходы из одного состояния в другое — стрелками. Малыми кругами представлено деление клетки.



А. Деление клетки на две. Клетки находятся в разных состояниях.



Б. После повреждения клетка самовосстанавливается и переходит из одного состояния в другое.

Рис. 14. Пример работы программ,
основанных на жизнедеятельности клетки.

Модель функционирования программы включает следующие

Деление клетки. Клетка может делиться на дочерние клетки, которые могут быть весьма разнородны по своему предназначению и химическому составу, но содержат одинаковую программу (ДНК). Причиной деления клетки на дочерние может явиться различный химический состав клетки и окружающей среды. Поведение дочерних клеток будет отличаться от поведения родительской клетки. Деление клеток моделируется с помощью перехода из одного состояния в другое.

Функционирование клеток. Клетки могут создавать протеины и подавать сигналы с помощью изменения химического состава в зависимости от того, какие гены в данный момент активны. Химикаты, созданные клетками, воздействуют на среду, в которой находятся клетки, а также на окружающие клетки.

Работа генов. Гены могут включаться или выключаться в зависимости от присутствия или отсутствия определенного протеина или

определенной концентрации химикатов. Включение или выключение генов выражается в таких действиях клеток как создание химикатов.

Различная степень концентрации химикатов, создаваемых клетками, является причиной работы генов. Работа клеток моделируется на основе использования «сообщений». Работа генов моделируется на основе перехода клетки из одного состояния в другое, которое инициируется в результате получения сообщений.

Клеточная программа начинается с клеток в состоянии начальной конфигурации, и все клетки далее следуют правилам перехода из одного состояния в другое. Состояние окружения может изменяться вследствие выполняемых операций. Когда клетки «ощущают» процессы, происходящие в окружающей среде, они могут восстановить или заново создать поврежденные компоненты.

В работе К.Папенфуса и Р.Ботча [119] предлагается подход, названый «оболочкой» (shell – based approach). Их модель защиты состоит из четырех элементов (рис.15): оболочка, токен, методы и данные.

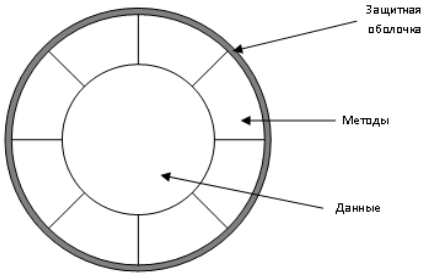


Рис. 15. Структура «оболочки».

Оболочка используется для защиты объекта от доступа неавторизованных пользователей и приложений. Оболочка защищает объект (как данные, так и методы) с помощью шифрования. Это сделано для того, чтобы предотвратить доступ неавторизованных внешних субъектов, которые могут попытаться обойти процесс идентификации. Лишь один метод остается незашифрованным, он назван главным методом. Главный метод – единственный метод, который является активным, в то время как объект находится в оболочке. В любое время объект, который хочет связаться с другим объектом, должен обратиться к главному методу. Все запросы посылаются в виде токенов.

Токен содержит всю информацию, необходимую для того, чтобы один объект мог связаться с другим. Эта информация содержит уникальный идентификационный номер, запрос объекта и сертификат аутентификации объекта. Этот сертификат использует открытый ключ для аутентификации объекта, делающего запрос. Сертификат зашифрован закрытым ключом объекта, делающего запрос. После получения токена главный метод, получивший объект, проверяет сертификат, расшифровывая его с помощью открытого ключа вызывающего объекта. Если этот процесс проходит успешно, главный метод может определить, какой из методов запрашивает объект, возможно, с помощью списка управления доступом главного метода.

Методы используются для получения объектов по запросу и управления их данными. Когда к объекту не обращаются, все его методы являются зашифрованными. Это сделано для того, чтобы предотвратить обход процесса аутентификации другими объектами. Если токен, запрашивающий объект, успешно аутентифицирован, главный метод, получающий объект, должен расшифровать все методы, которые запрашивающий объект может использовать. Расшифрованные методы затем используются для того, чтобы обработать запросы объектов. Данные объекта также должны быть расшифрованы до того, как их сможет использовать метод.

Данные содержатся внутри объектов и могут быть в любом формате, который только может быть использован для хранения и защиты данных. Данные, находящиеся внутри объектов, не могут использоваться пользователем, и только методы могут напрямую работать с объектом.

9. Применение нейронных сетей в биоподобных системах защиты информации. Нейронные сети (НС) являются одним из подходов для организации СЗИ, основанных на биоаналогии. Известны многочисленные применения НС в системах защиты [4, 31–33, 38, 122, 137, 39].

В существующих экспертных системах (ЭС) часто используют нейронную сеть для фильтрации поступающих сообщений с целью снижения числа характерных для ЭС ложных срабатываний. Если НС (после соответствующего обучения) стала идентифицировать новые атаки, то базу знаний ЭС также следует обновить. Иначе новые атаки будут игнорироваться экспертной системой, прежние правила которой не способны распознавать новую угрозу.

Если СЗИ организована на базе НС, то она способна обрабатывать трафик и анализировать поступающую информацию на наличие зло-

употреблений. Информация о любых случаях, которые идентифицируются с указанием на несанкционированный доступ, перенаправляется администратору безопасности или автоматически обрабатывается системой защиты. Этот подход более оперативен по сравнению с предыдущим подходом, так как существует единственный уровень обработки, и СЗИ обладает свойством адаптивности.

Нейронные сети наиболее часто используют для решения задач классификации [7, 8, 62–64, 83, 91]. Доказано, что НС является универсальным аппроксиматором, т. е. любая функция представима в виде многослойной НС из формальных нейронов с нелинейной функцией активации. Формально подтверждена верхняя граница сложности НС, реализующей произвольную непрерывную функцию от нескольких аргументов. Нейронной сетью с одним скрытым слоем и прямыми полными связями можно представить любую непрерывную функцию, для чего достаточно в случае n – мерного входного вектора 2n+1 формального нейрона скрытого слоя с заранее оговоренными ограниченными функциями активации [8, 98].

Основным недостатком НС считают «непрозрачность» формирования результатов анализа [84]. Однако использование гибридных нейро-экспертных или нейро-нечетких систем, а также генетических алгоритмов позволяет явным образом отразить в структуре НС систему правил If – Then, которые автоматически корректируются в процессе обучения НС. Свойство адаптивности НС позволяет решать не только задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, но и автоматически формировать новые правила при изменении поля угроз, а также реализовать систему защиты в целом [29, 34, 116].

НС используются для обнаружения признаков атак в сетевом трафике, идентификации форматов передаваемых данных, динамической идентификации участников обмена, а с использованием генетических алгоритмов — для получения близкого к оптимальному решения в задачах управления маршрутами и параметрами трафика при наличии нечеткости данных, идентификации атаки в условиях дефицита информации или информационного «шума».

Более подробно применение аппарата НС для защиты сетей от программных атак, направленных на нарушение доступности ресурсов, рассмотрено в [4, 12, 16]. Также, нейронные сети очень часто применяют для решения задач классификации и кластеризации [1, 9, 17, 37].

10. Нейро-экспертные системы, основанные на биометафоре. Нейронные сети и экспертные системы различаются по способам представления и обработки информации.

НС ориентированы на распределенную параллельную обработку данных, процесс решения задачи логически «не прозрачен», а накопленные в процессе обучения знания распределены по информационному полю НС, что затрудняет объяснение их конкретного местоположения и делает трудновыполнимым отражение в информационное поле НС априорного опыта квалифицированных специалистов информационной безопасности.

Опыт в экспертных системах представляется в «прозрачных» для пользователя систем правил If-Then, а процесс логического вывода сходен с характером человеческих рассуждений.

НС обладают свойством адаптивности, причем сам процесс обучения достаточно прост и формализуем. Напротив, задача приобретения знаний экспертными системами в значительной мере трудоемка, так как основана на создании непротиворечивой системы правил логического вывода, базирующегося на личном опыте экспертов [15]. Кроме того, ориентированная на достоверные данные ЭС не обладает гибкостью и возможностью самоорганизации.

База знаний нейро-экспертной системы (neural knowledge base, рис.16) организована в виде НС, знания в которой представлены в форме адаптивного распределенного информационного поля.

Топология НС определена реализуемой системой правил, что позволяет разместить опыт экспертов в информационное поле НС [82, 89]. При загрузке системы правил If–Then формируется структура НС и, следовательно, база знаний нейро-экспертной системы, а процесс обучения адаптирует информационное поле НС по обучающим образцам, выявляя скрытые в них закономерности.

Использование нейросетевой базы знаний позволяет устранить основные недостатки, основанные на правилах ЭС, - невозможность оперирования с не вполне достоверной информацией и трудоемкость адаптации базы знаний.

Нейросетевая база знаний корректирует зашумленную или искаженную входную информацию, что эквивалентно активации в правиле If–Then процесса формирования заключения даже в случае неполного выполнения условий в части If правила.

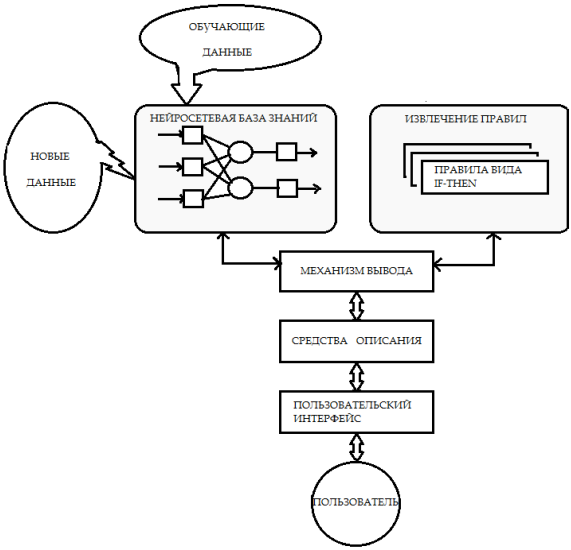


Рис. 16. Нейро-экспертная система.

Активация нейросетевой базы знаний аналогична извлечению знаний (rule extraction), соответствующих правилу If–Then, из информационного поля НС. Изменяются функции блока логического вывода, который оперирует нечеткими рассуждениями, подобными человеческим, исходя из потока данных в нейро-экспертной системе.

11. Применение нейро-нечетких систем. Объединение возможностей нейронных сетей и систем нечеткой логики (НЛ) является перспективным подходом к организации интеллектуальных средств защиты, основанных на биометафоре.

Согласно таблице 2, системы НЛ компенсируют две основные «непрозрачности» НС в представлении знаний и объяснений результатов работы интеллектуальной системы. Нечеткая логика позволяет формализовать качественную информацию, полученную от экспертов, использовать ее в процессе рассуждений в качестве посылок для системы нечетких правил, позволяющих анализировать результаты работы системы.

В механизме классификации адаптивных СЗИ целесообразно использовать сочетание возможностей НС и систем НЛ. Нейронные сети и системы НЛ имеют, с одной стороны, возможность обучения НС, а с другой, процесс решения задач системами НЛ доступен для анализа и

объяснения получаемых выводов. Объединение возможностей НС и систем НЛ в нейро-нечетких системах позволяет сочетать их достоинства.

Как следует из опыта разработки нейро-нечетких классификаторов (таблица 2) [30, 82] нейро-нечеткие сети типа 1 используют для решения задачи отнесения нечеткого входного вектора к четкому классу, а нейро-нечеткие сети типов 2, 3 и 4 применяют для построения нейро-нечетких систем классификации, основанных на системе нечетких правил вывода.

Таблица 2. **Нейро – нечеткие классификаторы**

Нечеткая нейронная сеть	*Веса*	*Входы*	*Цели*
Тип 1	четкие	нечеткие	четкие
Тип 2	четкие	нечеткие	нечеткие
Тип 3	нечеткие	нечеткие	нечеткие
Тип 4	нечеткие	четкие	нечеткие
Тип 5	четкие	четкие	нечеткие
Тип 6	нечеткие	четкие	четкие
Тип 7	нечеткие	нечеткие	четкие

Механизм нечеткого логического вывода используется при описании базы знаний, формируемой экспертами в виде системы правил нейро-нечеткой классификации:

$$П_1 : если \tilde{x}_1 \; есть \; A_{11} \; и .. \tilde{x}_n \; есть \; A_{1n}, то \; \tilde{y} = B_1,$$
$$П_2 : если \tilde{x}_1 \; есть \; A_{21} \; и .. \tilde{x}_n \; есть \; A_{2n}, то \; \tilde{y} = B_2,$$
$$...$$
$$П_к : если \tilde{x}_1 \; есть \; A_{к1} \; и .. \tilde{x}_n \; есть \; A_{кп}, то \; \tilde{y} = B_к,$$

где $\tilde{x}_i \; и \; \tilde{y}_j$ – нечеткие входные переменные и переменные вывода, соответствующие уязвимостям и угрозам, а $A_{ij} \; и \; B_i$, $i = \overline{1,k}, \; j = \overline{1,n}$ – входные и выходные функции принадлежности.

Нейронные сети дают возможность отобразить алгоритмы нечеткого логического вывода в структуре нейро-нечеткого классификатора, фиксируя в информационном поле НС априорную информацию, которая в процессе предэксплуатационного обучения может корректироваться.

Адаптивность нейро-нечетких классификаторов позволяет решать не только задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, но и автоматически формировать новые правила при изменении поля угроз информационной безопасности компьютерной системы.

Нейро-нечеткий классификатор — это НС (рис. 17) [116], которая является адаптивным функциональным эквивалентом нечеткой модели вывода, например, алгоритма Mamdani [23, 82].

Этапы нечеткого логического вывода соответствуют специализации слоев формальных нейронов в нейро-нечетком классификаторе:

слои 1,2 - введение нечеткости (fuzzification) выполняется слоем входных функций принадлежности *A1 – A3, B1 – B3* (input membership functions), осуществляющих преобразование каждого из четких входных значений *x1* и *x2* (crisp inputs) в степень истинности соответствующей предпосылки для каждого правила; $\mu_{Ai}, \mu_{Bi}, i = \overline{1,3}$;

слой 3 - нечеткому логическому выводу соответствует слой нечетких правил *R1 – R6* (fuzzy rules), который по степени истинности предпосылок $\mu_{Ai}, \mu_{Bi}, i = \overline{1,3}$ формирует заключения по каждому из правил, где $\mu_{Ri}, i = \overline{1-6}$ - соответствующие нечеткие подмножества;

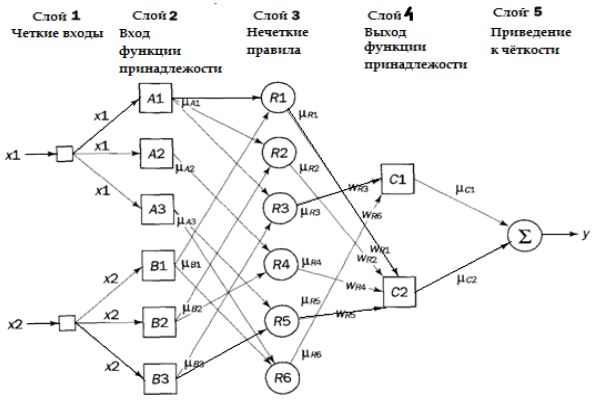


Рис. 17. Нейро-нечеткая сеть.

слой 4 - композиция нечетких подмножеств $\mu_{Ri}, i = \overline{1-6}$ производится слоем выходных функций принадлежности *C1, C2* (output membership functions) с целью формирования нечетких подмножеств $\mu_{Ci}, i = \overline{1,2}$;

слой 5 - объединение (aggregation) нечетких подмножеств $\mu_{Ci}, i = 1,2$, и приведение к четкости (defuzzification) выполняется в выходном слое и приводит к формированию выходного четкого значения y.

Как и в случае нейро-экспертных систем необходима коррекция информационного поля НС путем предэксплуатационного обучения.

Знания квалифицированных специалистов, представленные в форме нечетких правил логического вывода, могут быть отражены в структуре нейро-нечеткого классификатора. Последующее обучение классификатора позволяет настроить веса связей (т.е. откорректировать достоверность отдельных правил) и устранить противоречивость системы правил в целом.

Например, нейросеть Cascade ARTMAP (Adaptive resonance theory mapping - отображение адаптивной теории резонанса) [90] позволяет включать в НС априорное знание об исследуемой проблеме в виде правил If–Then. Включение предопределенных правил в НС до обучения не только позволяет повысить эффективность обучения, но и включить знания, не охваченные обучающими примерами. Неполные или частично достоверные правила могут быть откорректированы нейронной сетью в процесс обучения.

В соответствии с алгоритмом извлечения правил обученная нейросетевая система может быть преобразована обратно в компактный набор правил. Это позволяет непосредственно сравнить исходные знания и откорректированные нейронной сетью правила (рис. 18).

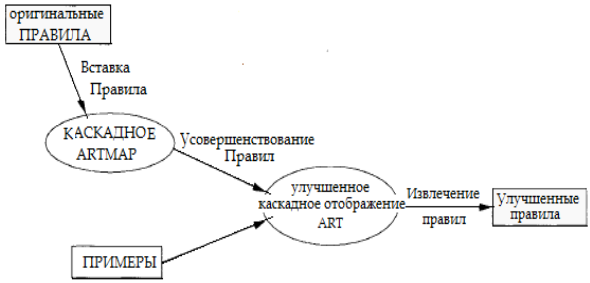


Рис. 18. Использование Cascade ARTMAP для доработки исходных правил.

В нейронную сеть Cascade ARTMAP возможно добавление не только правил, связывающих набор входных признаков с набором выходных атрибутов, но также и каскадов правил. Набор правил образует

каскад (или цепочку) правил, если следствие одного правила является посылкой для другого правила. Атрибуты, одновременно выполняющие роль как следствий, так и посылок, называются промежуточными атрибутами. Пример каскада, состоящего из двух правил:

Правило 1: If A и B, Then C,

Правило 2: If C и D, Then E.

Результаты экспериментов показали, что априорное знание увеличивает точность классификации, особенно при небольшом наборе обучающих примеров [66].

Лучшим сочетанием качеств обладают нейро-нечеткие схемы классификации с элементами принятий решений со следующими свойствами:

- функциональная устойчивость и защищенность нейросетевой элементной базы;
- возможность формирования и поддержания базы знаний в виде системы нечетких правил логического вывода;
- возможность классификации и кластеризации угроз;
- адаптивность нейро-нечетких классификаторов;
- «прозрачность» для анализа структуры связей нейро-нечетких классификаторов и системы нечетких правил логического вывода;
- возможность работы в режиме реального времени.

Также с нейросетевыми и нейро-нечеткими средствами обнаружения атак активно используются многоагентные методы для обнаружения вторжений в компьютерные сети и моделирования процессов проведения атак, которые также можно рассмотреть с точки зрения биометафоры.

В ряде работ [1, 9–11, 17, 18, 41, 117, 136, 138] рассматривается использование интеллектуальных многоагентных систем для защиты информации. В частности, дается обзор инструментов реализации атак, онтология предметной области, определяется структура команды агентов СЗИ, механизмы их взаимодействия и координации.

12. Биоподобные эволюционные методы. Эволюционные методы используются для решения оптимизационных задач [2, 54, 81]. Обычно это задачи многопараметрической оптимизации некоторой целевой функции от n переменных $f(x_1,x_2,..x_n)$ (в терминах эволюционных методик — функции соответствия), у которой необходимо найти глобальный максимум или минимум.

Применительно к интеллектуальным средствам СЗИ необходимо обеспечить автоматическую и оперативную реакцию системы защиты на изменение характера уязвимостей компьютерной системы или изменение поля угроз, что сводится к решению задачи адаптации базы знаний СЗИ к динамике внешнего окружения.

Эволюционный подход к машинному обучению интеллектуальных средств основан на вычислительных моделях естественного отбора и генетики. Методы эволюционных вычислений включают генетические алгоритмы, эволюционные стратегии и генетическое программирование. Все эти методы моделируют эволюцию, используя процессы отбора, мутации и воспроизводства [110].

В нейросетевых СЗИ эволюционные методы и генетические алгоритмы (ГА), в частности, используют для минимизации ошибки обучения НС на заданной обучающей выборке [3, 4, 46, 47].

Генетические алгоритмы как метод оптимизации сложных систем, основанный на биологической аналогии, были закономерным продолжением теории эволюции Дарвина, теории естественного отбора Вейсмана и генетической концепции Менделя, однако их широкое применение в искусственных системах [97] в значительной степени обусловлено возрождением интереса к нейросетевой тематике [88].

Известные методы ГА, используемые для обучения НС путем оптимизации весов межнейронных связей нейронной сети, можно подразделить на методы оптимизации весов связей при неизменной топологии сети и методы оптимизации топологии НС в соответствии с заданной функцией соответствия.

Типовой ГА для оптимизации весов связей НС (рис.19) [116] включает этапы кодирования хромосом, задания функции соответствия, по которой осуществляется отбор отдельных нейронных сетей в процессе эволюции НС, и выбора генетических операторов для моделирования эволюции, таких как пересечение, инверсия и мутация.

Вначале нумеруют узлы НС, начиная с входного слоя, и представляют топологию НС в виде квадратной матрицы связей, число строк (столбцов) которой равно количеству узлов в нейронной сети. При этом каждый элемент матрицы соответствует отдельной межнейронной связи и равен значению веса связи. Для отсутствующих межнейронных связей значение элемента матрицы равно 0 [111].

В рассматриваемом случае в качестве генов выбираются значения весов связей, ассоциированные с входами формальных нейронов, – это группа весов, расположенная в отдельной строке матрицы весов, в качестве функции соответствия – обратная величина евклидова расстоя-

ния между расчетным и целевым значениями выходов, а в качестве генетических операторов — пересечение и мутация.

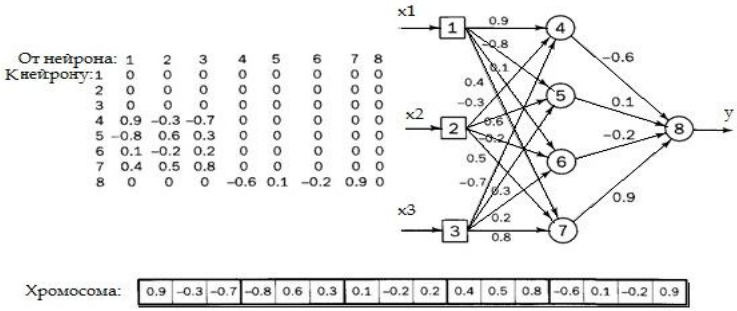


Рис. 19. ГА для оптимизации весов связей НС.

Оператор пересечения создает пару дочерних хромосом из генетического материала обоих родителей путем обмена одноименными (случайно выбранными) генами, а оператор мутации в весе случайно выбранного гена хромосомы вызывает незначительное случайное изменение значения в заданном диапазоне. В каждом эволюционном цикле рассчитываются значения выходов НС и функции соответствия. Отбор хромосом в следующую популяцию производится с учетом функции соответствия. Затем производится следующая эволюционная попытка до тех пор, пока хотя бы одна из хромосом не удовлетворит требованиям по допустимой ошибке обучения НС.

Аналогичным образом ГА используют для оптимизации топологии НС, т. е. числа нейронов и межнейронных связей в сети [112]. Составляется матрица связей сети, каждый элемент которой отмечается нулем, если связь в НС отсутствует, либо единицей в противном случае. Хромосома образуется путем последовательного соединения строк матрицы связей.

В [116] эволюционный процесс включает следующие этапы:

1. Задается размер популяции хромосом, вероятности выполнения операторов пересечения и мутации, число циклов обучения НС.

2. Выбирается функция соответствия для процедуры эволюционного отбора, например, обратная величина евклидова расстояния между расчетным и целевым значениями выходов НС.

3. В качестве начальной популяции выбирается случайным образом сгенерированная совокупность хромосом.

4. Выбирается одна из хромосом популяции и вычисляется значение функции соответствия.

5. Действия по п. 4 повторяются для всей популяции хромосом.

6. В соответствии со значением функции соответствия случайным образом выбирается пара хромосом, и с применением операторов пересечения и мутации создается пара дочерних хромосом. Оператор пересечения случайным образом выбирает гены в родительских хромосомах и производит взаимный обмен генами, а оператор мутации с низкой вероятностью (порядка 0,005.) инвертирует один или два бита в случайно выбранном гене.

7. Формируется новая популяция путем включения в нее дочерних хромосом.

8. Действия по п.п. 6, 7 повторяются, пока размер новой популяции хромосом не достигнет размера исходной популяции.

9. Действия с п. 4 повторяются до тех пор, пока не сменилось заданное число популяций.

Генетические алгоритмы предоставляют эффективные средства оптимизации адаптируемых параметров интеллектуальных средств в составе СЗИ, в частности, взвешенных связей нейронной сети.

13. Гибридные интеллектуальные средства. В гибридных интеллектуальных средствах сочетаются достоинства различных подходов. В каждом из подходов имеются как сильные, так и слабые стороны (таблица 3) [116, 82]. Сравнение экспертных систем (ЭС), систем с нечеткой логикой (НЛ), искусственных нейронных сетей (ИНС) и генетических алгоритмов (ГА) позволяет выделить нейронные сети, системы нечеткой логики и генетические алгоритмы по критерию возможности решения задач с использованием не вполне достоверных входных данных, что свойственно большинству систем защиты.

Недостатком нейронных сетей, не позволяющим анализировать процесс формирования классификационных заключений, считается не вполне «прозрачное», с точки зрения администратора безопасности, представление знаний в информационном поле НС. Для устранения отмеченного недостатка целесообразно сочетание НС с системами нечеткой логики либо с экспертными системами. Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет явным образом отразить в структуре нейронных сетей систему нечетких правил вывода, которые автоматически корректируются в процессе обучения НС.

Заключение. Традиционные компьютерные системы имеют ряд недостатков, таких как низкая надежность и адаптивность, ограниченная масштабируемость. Биологические системы, напротив, обладают высокой надежностью, умеют адаптироваться к окружающей среде и

обладают высокой масштабируемостью. Следовательно, компьютерные системы, которые строятся с применением биологических подходов, должны получить такие преимущества как масштабируемая архитектура, самоорганизация, самолечение и устойчивость к ошибкам.

Таблица 3. **Сравнение подходов**

	ЭС	*НЛ*	*ИНС*	*ГА*
Представление знаний	3	4	1	2
Толерантность к неопределенности	3	4	4	4
Толерантность к неточности	1	4	4	4
Приспособляемость	1	2	4	4
Способность к обучению	1	1	4	4
Возможность объяснения	4	4	1	2
Добыча знаний	1	2	4	3
Возможность коррекции	1	3	4	3

Примечание: Оценка по 4-х бальной шкале: 1 – плохо, 2 – скорее плохо, 3 – скорее хорошо, 4 – хорошо.

В данной статье проведен общий анализ некоторых из существующих подходов к защите компьютерных систем с использованием биологической метафоры, начиная от компьютерных сетей и заканчивая защитой программного обеспечения. Конечно, далеко не все из них сегодня можно полностью реализовать, однако многие из представленных подходов могут оказаться жизнеспособными и дать новый толчок в развитии перспективных систем защиты информации.

В настоящее время биоинспирированная концепция реализуется авторами статьи в виде различных моделей, алгоритмов и программных модулей [13, 14, 20, 21, 43, 104–106].

Исходя из анализа существующих подходов, использующих биологическую метафору, авторы выделяют такие базовые задачи для дальнейшей работы, как разработка основ теории и методологии проектирования адаптивных средств защиты информации и практическая реализация отдельных адаптивных средств защиты информации.

Литература

1. *Алексеев А. С., Котенко И. В.* Командная работа агентов по защите от распределенных атак “отказ в обслуживании” // Сб. докл. VI Международной конф. SCM’2003. – СПб.: СПГЭТУ, 2003. т. 1. С. 294 -297.

2. *Баранюк Т. Н., Нестерук Г. Ф., Молдовян У. А*. Эволюционные методы обучения нейро-нечетких средств классификации несанкционированной деятельности в ЛВС // SCM'2005. — СПб.: СПбГЭТУ «ЛЭТИ». 2005, т.1. С. 258 - 262.
3. *Бочков М.В., Крупский С.А., Саенко И.Б*. Применение генетических алгоритмов оптимизации в задачах информационного противодействия сетевым атакам // Сб. докл. Всероссийская научная конф. Управление и информационные технологии. Т.2. СПб.: ЛЭТИ, 2003. – С.13 - 16.
4. *Бочков М. В.* Реализация методов обнаружения программных атак и противодействия программному подавлению в компьютерных сетях на основе нейронных сетей и генетических алгоритмов оптимизации // Сб. докл. VI Междунар. конф. SCM'2003. – СПб.: СПГЭТУ, 2003. т. 1. С. 376-378.
5. *Варшавский В.И., Поспелов Д.А.* Оркестр играет без дирижера: размышления об эволюции некоторых технических систем и управлении ими. М.: Наука, Главная редакция физико-математической литературы, 1984. 208с.
6. *Гаазе-Рапопорт М.Г., Поспелов Д.А.* От амебы до робота: модели поведения. М.: Наука, 1987. 286 с.
7. *Горбань А. Н*. Обучение нейронных сетей. - М.: СП ПараГраф. 1991
8. *Горбань А. Н., Дунин-Барковский В. Л., А. Н. Кирдин и др.* Нейроинформатика. // - Новосибирск: Наука. Сиб. отд-ние, 1998.
9. *Городецкий В. И., Котенко И. В.* Командная работа агентов-хакеров: применение многоагентной технологии для моделирования распределенных атак на компьютерные сети // КИИ-2002. VIII Национальная конференция по искусственному интеллекту. Труды конференции. М.: Физматлит, 2002.
10. *Городецкий В. И., Карсаев О. В., Котенко И. В.* Программный прототип многоагентной системы обнаружения вторжений в компьютерные сети // ICAI'2001. Международный конгресс "Искусственный интеллект в XXI веке". Труды конгресса. Том 1. М.: Физматлит, 2001.
11. *Городецкий В. И., Котенко И. В.* Командная работа агентов в антагонистической среде // Сб. докл. V Междунар. конф. SCM'2002. – СПб.: СПГЭТУ, 2002. т. 1. С. 259-262.
12. *Гриняев С. Н.* Интеллектуальное противодействие информационному оружию. М.: СИНТЕГ, 1999
13. *Коновалов А.М., Котенко И.В., Шоров А.В.* Моделирование функционирования команд интеллектуальных агентов бот-сетей и систем защиты // Двенадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2010: Труды конференции. Т. 3. – М.: Физматлит, 2010. С. 44-51.
14. *Коновалов А.М., Котенко И.В., Шоров А.В.* Среда моделирования для имитации сетевых атак и механизмов защиты // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.38-39.
15. *Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В.* Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2001
16. *Костин А. А., Нестерук Г. Ф., Фахрутдинов Р. Ш*. О иерархии адаптивных средств обнаружении компьютерных атак на ЛВС // Фундаментальные исследования в технических университетах: Материалы IX всероссийской конференции по проблемам науки и высшей школы, 18 - 19 мая 2005 г. - СПб: Изд-во Политехнического университета, 2005. С. 169 – 170.

17. *Котенко И. В., Карсаев А. В., Самойлов В. В.* Онтология предметной области обучения обнаружению вторжений в компьютерные сети // Сб. докл. V Междунар. конф. SCM'2002. – СПб.: СПГЭТУ, 2002. т. 1. С. 255-258.
18. *Котенко И. В.* Модели противоборства команд агентов по реализации и защите от распределенных атак «Отказ в обслуживании» // Тр. междунар. конф. IEEE AIS'03 и CAD-2003. – М.: Физматлит, 2003. т. 1. С. 422 - 428.
19. *Котенко И.В., Чечулин А.А., Нестерук Ф.Г.* Комбинирование механизмов обнаружения сканирования в компьютерных сетях // Вопросы защиты информации №3, 2011.
20. *Котенко И.В., Коновалов А.М., Шоров А.В.* Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.42-45.
21. *Котенко И.В., Коновалов А.М., Шоров А.В.* Агентно-ориентированное моделирование функционирования бот-сетей и механизмов защиты от них // Защита информации. Инсайд, 2010. № 4, С.36-45. № 5, С.56-61.
22. *Котенко И.В., Шоров А.В.* Использование биологической метафоры для защиты компьютерных систем и сетей: предварительный анализ базовых подходов // Защита информации. Инсайд, 2011. № 1-2.
23. *Круглов В. В., Борисов В. В.* Искусственные нейронные сети. Теория и практика.- 2-е изд., стереотип. – М.: Горячая линия - Телеком, 2002.
24. *Кузнецова В. Л., Раков М. А.* Самоорганизация в технических системах. – Киев: Наук. думка,1987.
25. *Лачинов В. М., Поляков А. О.* Информодинамика или Путь к Миру открытых систем. / Изд. 2-е, перераб. и доп. – СПб.: Издательство СПбГТУ, 1999.
26. *Лобашев М.Е.* Генетика. – Л.: Изд-во ленинградского университета, 1969.
27. *Лукацкий А.В.* Иммунная система вашей сети // Защита информации. Конфидент, №2, 2006. С.20-21.
28. *Мелик-Гайназян И.В.* Информационные процессы и реальность. М.: Наука, 1998. - 192 с.
29. *Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф.* Информационная безопасность и интеллектуальные средства защиты информационных ресурсов. (Иммунология систем информационных технологий). – СПб.: Изд-во СПбГУЭФ, 2003, 364 с.
30. *Нестерук Г.Ф., Осовецкий Л.Г., Нестерук Ф.Г.* О применении нейро-нечетких сетей в адаптивных системах информационной защиты// Нейроинформатика. 2005. С. 163.
31. *Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Костин А.А., Воскресенский С.И.* Организация иерархической защиты информации на основе интеллектуальных средств нейронечеткой классификации.//Вопросы защиты информации. 2005. № 3. С. 16-26.
32. *Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Воскресенский С.И., Костин А.А.* Повышение избыточности информационных полей адаптивных классификаторов системы информационной безопасности.//Специальная техника. 2006. № 1. С. 60.
33. *Нестерук Г.Ф. Баранюк Т.Н. Фахрутдинов Р.Ш. Молдовян У.А.* К мониторингу недекларированных возможностей ОС средствами нечеткой логики и нейронных сетей // SCM'2005: Сборник докладов Международной конференции по мягким вычислениям и измерениям 27-29 июня 2005 г. Т.1. - СПб: СПбГЭТУ «ЛЭТИ», 2005. С. 263 – 267.
34. *Нестерук Ф. Г., Осовецкий Л. Г., Нестерук Г. Ф., Баранюк Т. Н. и др*. Отчет по научно-исследовательские работе «Разработка и исследование адаптивной систе-

мы информационной безопасности для корпоративных информационных сетей», шифр 2006-РИ-19.0/001/811, этап 2. – СПб.: СПбГУ ИТМО. 2006.
35. *Нестерук Ф.Г., Нестерук Г.Ф., Осовецкий Л.Г.* Основы организации адаптивных систем ЗИ. СПб.: СПбГУ ИТМО, 2008. С. 112.
36. *Нестерук Ф. Г., Суханов А. В., Нестерук Л. Г., Нестерук Г.Ф.* Адаптивные средства обеспечения безопасности информационных систем / Под ред. Л. Г. Осовецкого. – СПб.: Изд-во Политехн. ун-та, 2008.– 626 с.
37. *Нестерук Ф.Г., Молдовян А.А., Нестерук Г.Ф., Нестерук Л.Г.* Квазиологические нейронные сети для решения задачи классификации в системах защиты информации.// Вопросы защиты информации. 2007. № 1. С. 23-31.
38. *Осовецкий Л.Г., Нестерук Г.Ф., Бормотов В.М.* К вопросу иммунологии сложных информационных систем.// Известия высших учебных заведений. Приборостроение. 2003. Т. 46. № 7. С. 34.
39. *Пантелеев С. В.* Решение задач идентификации динамических объектов с использованием нейронных сетей // Сб. докл. VI Международной конф. SCM'2003. – СПб.: СПГЭТУ, 2003. т. 1. С. 334-336.
40. *Суханов А.В., Нестерук Л.Г., Нестерук Ф.Г.* Мониторинг безопасности информационных систем на основе модели адаптивной защиты // Журнал "Безопасность информационных технологий", выпуск 3, 2008. С.33-38.
41. *Степашкин М. В., Котенко И. В.* Классификация атак на Web-сервер // VIII Санкт-Петербургская междунар. конф. "Региональная информатика-2002" Материалы конференции. Ч. 1. СПб., 2002.
42. *Чечулин А.А., Котенко И.В.* Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы, 2010, № 12, С.21-27. ISSN1684-8853.
43. *Шоров А.В., Коновалов А.М., Котенко И.В.* Исследовательское моделирование ботсетей и механизмов защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XVIII Общероссийской научно-технической конференции. Санкт-Петербург. Издательство Политехнического университета. 2009. С.132.
44. *Шоров А.В.* Анализ биологических подходов для защиты компьютерных сетей от инфраструктурных атак // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)». 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.145.
45. *Шоров А.В., Котенко И.В.* Защита компьютерной сети от инфраструктурных атак на основе реализации "нервной системы сети" // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.118-119.
46. *Ярушкина Н. Г.* Гибридные системы, основанные на мягких вычислениях: определение, архитектура, возможности // Программные продукты и системы, № 3, 2002.
47. *Ярушкина Н. Г.* Гибридизация интеллектуальных систем // Тр. междунар. научно-технич. конф. IEEE AIS'03 и CAD-2003. – М.: Физматлит, 2003. т. 1. С. 115 - 130.
48. *Adamatzky A.* Identification of Cellular Automata, London, Taylor & Francis, 1994.
49. *Aickelin U., Cayzer S.* The Danger Theory and Its Application to Artificial Immune Systems // Proceedings of 1st International Conference on Artificial Immune Systems (ICARIS), University of Kent at Canterbury, UK, 2002.
50. *Agnati L., Tarakanov A., Guidolin D.* A simple mathematical model of cooperativity in receptor mosaics based on the symmetry rule // BioSystems, Vol. 80, No.2, 2005, P.165–173.

51. *Anagnostakis K., Greenwald M., Ioannidis S., Keromytis A., Li D*. A Cooperative Immunization System for an Untrusting Internet // ICON2003. The 11th IEEE International Conference on Networks, 2003. P.403–408.
52. *Andrews P., Timmis J.* Inspiration for the next generation of artificial immune systems // ICARIS, 2005. P. 126–138.
53. *Atighetchi M., Pal P.* From Auto-adaptive to Survivable and Self-Regenerative Systems Successes, Challenges, and Future // Proceedings of the 2009 Eighth IEEE International Symposium on Network Computing and Applications, IEEE Computer Society, 2009. P. 98–101.
54. *Back T., Fogel D.B., Michalewicz, Z., eds*. Handbook of Evolutionary Computation. – NY: Institute of Physics Publishing, Bristol, Philadelphia and Oxford University Press. 1997
55. *Bass T.* Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems. Invited Paper // IRIS National Symposium on Sensor and Data Fusion, 1999.
56. *Barrus J., Rowe N. A* Distributed Autonomous-Agent Network-Intrusion Detection and Response System // Proceedings of the Command and Control Research and Technology Symposium, 1998.
57. *Bradley D., Tyrrell A.* Immunotronics: Hardware fault tolerance inspired by the immune system // Proceedings of the 3rd International conference on Evoluable Systems (ICES2000), vol. 1801. Springer-Verlag, Inc., 2000. P.11–20.
58. *Cajal S., Pasik P., Pasik T.* Texture of the Nervous System of Man and the Vertebrates: Vol. 1, Springer, 1999.
59. Cisco's Self-Defending Network Architecture Reference Model. 2005.
60. *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.
61. *Coello C., Cores N*. A parallel implementation of the artificial immune system to handle constraints in genetic algorithms: Preliminary results // Proceedings of the 2002 Congress on Evolutionary Computation (CEC 2002), 2002. P. 819–824.
62. *Carpenter, G. A., Grossberg, S., & Reynolds, J. H.* ARTMAP: Supervised Real-Time Learning and Classification of Nonstationary Data by a Self-Organizing Neural Network // Neural Networks, 4, 1991, p. 565 - 588
63. *Carpenter, G. A., Grossberg, S., Markuzon, N., Reynolds, J. H., & Rosen, D. B.* Fuzzy ARTMAP: A Neural Network Architecture for Incremental Supervised Learning of Analog Multidimensional Maps // IEEE Trans. on Neural Networks, 3 (5), 1992, p. 698 - 713
64. *Carpenter, G. A., Grossberg, S., & Rosen, D, B.* Fuzzy ART: Fast Stable Learning and Categorization of Analog Patterns by an Adaptive Resonance System // Neural Networks, 4, 1991, p. 759 - 771
65. *Dasgupta D.* Artificial Immune Systems and Their Applications. Springer, Berlin, 1999.
66. *Dasgupta D.* Immune-based intrusion detection system: A general framework // Proceedings of the 22nd National Information Systems Security Conference (NISSC), 1999.
67. *Dasgupta D., Cao Y.,Yang C*. An immunogenetic approach to spectra recognition // Proceedings of Genetic and Evolutionary Computational Conference (GECCO 1999), vol. 1, 1999. P. 149–155.
68. *Dasgupta D., Yu S., Majumdar N*. MILA—multilevel immune learning algorithm // Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2003), LNCS 2723, Springer, 2003. P. 183–194.
69. *Dasgupta D.* Advances in Artificial Immune Systems. IEEE Computational Intelligence Magazine, 2006.

70. *Dasgupta D.* Immuno-inspired autonomic system for cyber defense // Information Security Tech. Report archive, Vol.12, No.4, 2007. P.235-241.
71. *De Castro L. N., Timmis J*. Artificial Immune Systems: A New Computational Intelligence Approach. Springer, London, 2002.
72. *De Castro L., Von Zuben F.* The clonal selection algorithm with engineering applications // Proceedings of GECCO 2000, 2000. P. 36–39.
73. *De Castro L., Von Zuben F*. aiNet: An artificial immune network for data analysis // Data Mining: A Heuristic Approach, H.A. Abbass, R.A. Sarker, and C.S. Newton, Eds. Idea Group Publishing, USA, 2001. P. 231–259.
74. *De Castro L., Von Zuben F*. An immunological approach to initialize feedforward neural network weights // International Conference on Artificial Neural Networks and Genetic Algorithms (ICANNGA '01), 2001. P. 126–129.
75. *Demers A., Greene D., Hauser C., Irish W., Larson J., Shenker S., Sturgis H., Swinehart D., Terry D.* Epidemic algorithms for replicated database maintenance, in: PODC'87 // Proceedings of the sixth annual ACM Symposium on Principles of distributed computing, 1987, P. 1-12.
76. *Di Caro G., Dorigo M*., AntNet: Distributed Stigmergetic Control for Communications Networks // Journal of Artificial Intelligence Research №9, 1998. P.317-365.
77. *Dressler F.* Bio-inspired mechanisms for efficient and adaptive network security // Service Management and Self-Organization in IP-based Networks, 2005.
78. *Dressler F.* Benefits of Bio-inspired Technologies for Networked Embedded Systems: An Overview // Organic Computing - Controlled Emergence. Dagstuhl Seminar Proceedings, Schloss Dagstuhl, Germany, 2006.
79. *Dressler F*., Carreras I. (Eds.), Advances in Biologically Inspired Information Systems - Models, Methods, and Tools // Studies in Computational Intelligence (SCI), vol. 69. Berlin, Heidelberg, New York, Springer, 2007.
80. *Dressler F., Akan O. A* Survey on Bio-inspired Networking // Elsevier Computer Networks, 2010.
81. *Davis L.* Handbook on Genetic Algorithms. – NY: Van Nostrand Reinhold. 1991.
82. *Fuller R.* Neural Fuzzy Systems. - Abo: Abo Akademi University, 1995
83. *Fu L.M*. Neural Networks in Computer Intelligence. - McGraw-Hill Book, Inc. 1994
84. *Fu L.* A Neural Network Model for Learning Rule-Based Systems // Proc. of the International Joint Conference on Neural Networks. 1992. P. 343-348.
85. *Galeano J., Veloza-Suan A., Gonzalez F.* A comparative analysis of artificial immune network models // GECCO 2005: Proceedings of the 2005 conference on Genetic and evolutionary computation, Washington DC, USA: ACM 320 Press, vol. 1, 2005. P. 361–368.
86. *George S., Evans D., Davidson L*. A Biologically Inspired Programming Model for Self-Healing Systems // Workshop on Self-healing systems, 2002. P. 102–104.
87. *Goncharova L., Jacques Y., Martin-Vide C., Tarakanov A., Timmis J*. Biomolecular immune-computer: Theoretical basis and experimental simulator // LNCS, Vol. 3627, 2005. P.72–85.
88. *Goldberg D.* Genetic Algorithms in Machine Learning, Optimization, and Search. - Addison-Wesley, 1988.
89. *Gallant S.I.* Neural Network learning and Expert Systems. MIT Press, Cambridge, MA, 1993.
90. *Granger E., Rubin M. A., Grossberg S. and Lavoie P.* A what-and-where fusion neural network for recognition and tracking of multiple radar emitters // Neural Networks, vol. 3, 2001, p. 325 - 344.

91. *Granger, E., Rubin, M. A., Grossberg, S., & Lavoie, P.* Classification of Incomplete Data Using the Fuzzy ARTMAP Neural Network // Proc. Int'l Joint Conference on Neural Networks, vol. IV, 2000, p. 35 - 40.
92. *Hart E., Ross P*. Exploiting the analogy between immunology and sparse distributed memories: A system for clustering non-stationary data // Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS), 2002. P. 49–58.
93. *Hofmeyr S., Forrest S.* Immunizing Computer Networks: Getting All the Machines in Your Network to Fight the Hacker Disease // In Proceedings of the 1999 IEEE Symposium on Security and Privacy, 1999. P. 9–12.
94. *Hofmeyr S., Forrest S.* Architecture for an artificial immune system // Evolutionary Computation, vol. 8, no. 4, 2000. P. 443–473.
95. *Hordijk W.* An Overview of Biologically Inspired Computing in Information Security // Proceedings of the National Conference on Information Security, Coimbatore, India, 2005. P.1–14.
96. *Hunt J., Timmis J., Cooke D., Neal M., King C*. Jisys: The development of an Artificial Immune System for real world applications // Applications of Artificial Immune Systems, D. Dasgupta Ed., Pub. Springer-Verlag, ISBN 3-540-64390-7, 1999. P. 157–186.
97. *Holland J.* Adaptation in Natural and Artificial Systems. - University of Michigan Press, 1975.
98. *Hecht-Nielsen R.* Kolmogorov's Mapping Neural Network Existence Theorem // IEEE First Annual Int. Conf. on Neural Networks, San Diego, 1987, V. 3, P. 11-13.
99. *Iqbal A., Maarof M*. Towards danger theory based artificial APC model: Novel metaphor for danger susceptible data codons // Proceedings of Third International Conference on Artificial Immune Systems (ICARIS 2004), 2004. P. 161–174.
100. *Ishida Y*. Immunity-Based Systems. A Design Perspective. Springer Verlag, 2004.
101. *Ji Z., Dasgupta D.* Real-valued negative selection algorithm with variable-sized detectors // LNCS 3102, Proceedings of GECCO, 2004. P. 287–298.
102. *Kim J., Bentley P*. Toward an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection // Proceedings of the 2002 Congress on Evolutionary Computation (CEC 2002), 2002. P. 1244–1252.
103. *Kim J., Bentley P.J., Aickelin U., Greensmith J., Tedesco G., Twycross J*. Immune System Approaches to Intrusion Detection - A Review // Natural Computing, 6 (4), 2007. P.413-466.
104. *Kotenko I., Chechulin A., Doynikova E.* Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems // Information Fusion and Geographic Information Systems. Proceedings of the Fourth International Workshop. Brest, France, 2011. Lecture Notes in Geoinformation and Cartography. Springer. 2011.
105. *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.
106. *Kotenko I., Konovalov A., Shorov A.* Simulation of Botnets: Agent-based approach. Intelligent Distributed Computing IV. Studies in Computational Intelligence, Springer-Verlag. 2010, Volume 315. P.247-252.
107. *Lee U., Magistretti E., Gerla M., Bellavista P., Lio P., Lee K.-W*. Bio-inspired multi-agent data harvesting in a proactive urban monitoring environment // Ad Hoc Networks №7, 2009. P. 725-741.
108. *Meisel M., Pappas V., Zhang L.* A Taxonomy of Biologically Inspired Research in Computer Networking // Computer Networks (Special Issue on Interdisciplinary Paradigms for Networking). 2009.

109. *Mirollo R., Strogatz S*. Synchronization of pulse-coupled biological oscillators // SIAM J. Appl. Math 50, 1990. P.1645-1662.
110. *Mitchell M*. An Introduction to Genetic Algorithms. - Cambridge, MA: MIT Press. 1996
111. *Montana D.J., Davis, L*. Training feedforward networks using genetic algorithms. Proceedings of the 11th International Joint Conference on Artificial Intelligence, Morgan Kaufmann, San Mateo, CA, 1989. P. 762-767.
112. *Miller G.F., Todd P.M., Hedge, S.U.* Designing neural networks using genetic algorithms // Proc. of the 3-d International Conference on Genetic Algorithms. Morgan Kaufmann, San Mateo, CA, 1989. P. 379-384.
113. *Nasraoui O., Gonzalez F., Dasgupta D*. The fuzzy ais: Motivations, basic concepts, and applications to clustering and web profiling // IEEE International Conference on Fuzzy Systems, 2002. P. 711–717.
114. *Nasraoui O., Gonzalez F., Cardona C., Rojas C., Dasgupta D.* A scalable artificial immune system model for dynamic unsupervised learning // Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2003), ser. LNCS 2723. Chicago, IL: Springer, 2003. P. 219–230.
115. *Negoita M., Neagu D., Palade V.* Computational Intelligence Engineering of Hybrid Systems. Springer Verlag. 2005.
116. *Negnevitsky M*. Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.
117. *Noureldien A. N*. Protecting Web Servers from DoS/DDoS Flooding Attacks. A Technical Overview // International Conference on Web-Management for International Organisations. Proceedings. Geneva, October, 2002.
118. Panel: The Future of Biologically-Inspired // NSPW 2007: New Security Paradigms Workshop 2007, North Conway, New Hampshire USA. 2007.
119. *Papenfus C., Botha R.* A shell-based approach to information security // SAICSIT, 1998. P.15–19.
120. *Pappas V., Verma D., Ko B.-J., Swami A*. A circulatory system approach for wireless sensor networks // Ad Hoc Networks In Press, Corrected Proof. 2008.
121. *Ryutov T., Zhou L., Neuman C., Leithead T., Seamons K*. Adaptive Trust Negotiation and Access Control // ACM Symposium on Access Control Models and Technologies (SACMAT'05), 2005.
122. *Ryan J., Lin M., Miikkulainen R.* Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAIWorkshop (Providence, Rhode Island), pp. 72-79. Menlo Park, CA: AAAI. 1997.
123. *Schoonderwoerd R., Bruten J., Holland O., Rothkrantz L.* Ant-based load balancing in telecommunications networks // Adapt. Behav. Vol. 5, No.2, 1996. P. 169-207.
124. *Stepney S., Smith R., Timmis J.* Towards a conceptual framework for artificial immune systems // Proceedings of Third International Conference on Artificial Immune Systems (ICARIS 2004), 2004. P. 53–64.
125. *Stibor T., Timmis J., Eckert C.* A comparative study of real-valued negative selection to statistical anomaly detection techniques // ICARIS, 2005. P. 262–275.
126. *Subramanian D., Druschel P., Chen J*. Ants and reinforcement learning: A case study in routing in dynamic networks // Proceedings of IJCAI, Morgan Kaufmann, 1997. P. 832-838.
127. The ProCurve Networking, Adaptive EDGE Architecture. Technical White Paper, 2006.
128. *Tarakanov A., Dasgupta D*. A formal model of an artificial immune system // BioSystem, vol. 55, 2000. P. 151–158.

129. *Tarakanov A., Dasgupta D.* An immunochip architecture and its emulation // 2002 NASA/DoD Conference on Evolvable Hardware, Alexandria, VA, USA, 2002. P. 261–265.
130. *Tarakanov A.* Immunocomputing for Intelligent Intrusion Detection // Computational Intelligence Magazine, IEEE Vol. 3, No. 2, 2008. P. 22–30.
131. *Tarakanov A., Skormin V., Sokolova S.* Immunocomputing: Principles and Applications. Springer, New York, 2003.
132. *Tarakanov A., Tarakanov Y.* A comparison of immune and neural computing for two real-life tasks of pattern recognition // LNCS, Vol. 3239, 2004. P.236–249.
133. *Tarakanov A., Tarakanov Y.* A comparison of immune and genetic algorithms for two real-life tasks of pattern recognition // International Journal of Unconventional Computing, Vol. 1, No. 4, 2005. P.357–374.
134. *Timmis J.* Artificial immune systems: A novel data analysis technique inspired by the immune network theory, Ph.D. dissertation, University of Wales, Aberystwyth, UK, 2000.
135. *Tyrrell A.* Biologically Inspired Fault-Tolerant Computer Systems // Lecture Notes In Computer Science, Vol. 2485, 2002. P.88–89.
136. *Tambe M., Pynadath D. V.* Towards Heterogeneous Agent Teams // Lecture Notes in Artificial Intelligence. V.2086, Springer Verlag, 2001.
137. *Tan K.* The Application of Neural Networks to UNIX Computer Security //Proc. of the IEEE International Conf. on Neural Networks, 1995. V.1. P. 476-481.
138. Understanding DDOS Attack, Tools and Free Anti-tools with Recommendation. SANS Institute. April 7, 2001.
139. *Vahdat A., Becker D.* Epidemic routing for partially-connected ad hoc networks, Tech. Rep. CS-2000-06, Duke University, 2000.
140. *Wang M., Suda T.* The bio-networking architecture: A biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications // Applications and the Internet, IEEE/IPSJ International Symposium, 2001.
141. *Williams P., Anchor K., Bebo J., Gunsh G., Lamont G.* Cdis: Towards a computer immune system for detecting network intrusions // Lecture notes in Computer Science, vol. 2212, 2001. P. 117–133.
142. *Zhao W.* Review of Immunocomputing: Principles and Applications // ACM SIGACT News, Vol. 36, No. 4, 2005. P.14–17.

Котенко Игорь Витальевич — д.т.н., проф.; заведующий лабораторией проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургского института информатики и автоматизации РАН (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, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (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.

Шоров Андрей Владимирович — аспирант лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (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. Научный руководитель — И.В. Котенко.

Shorov Andrey Vladimirovich — Ph.D. student of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (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. Scientific adviser — I.V. Kotenko

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 Philipp Gennadyevich — PhD. of Computer Science, Senior researcher of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science. 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.

Поддержка исследований. Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект № 3.2), Министерства образования и науки Российской Федерации (государственный контракт 11.519.11.4008), Комитета по науке и высшей школе Правительства Санкт-Петербурга и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Рекомендовано СПИИРАН, лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 21.09.2011.

РЕФЕРАТ

Котенко И.В., Шоров А.В., Нестерук Ф.Г. **Анализ биоинспирированных подходов для защиты компьютерных систем и сетей.**

Одной из важнейших целей построения защищенных систем и сетей является создание механизмов защиты, устойчивых к сбоям, обладающих высокой масштабируемостью и адаптивностью (в том числе способных самоконфигурироваться и самовосстанавливаться).

В статье проведен общий анализ некоторых из существующих подходов к защите компьютерных систем с использованием биологической метафоры. Конечно, далеко не все из них сегодня можно полностью реализовать. Однако многие из представленных подходов могут оказаться жизнеспособными и дать новый толчок в развитии перспективных систем защиты информации.

В статье приведен обзор следующих основных аспектов использования биологической метафоры для защиты компьютерных систем и сетей:

- основные биологические метафоры и подходы, применимые для защиты компьютерных систем и сетей;
- подход к защите компьютерной сети, основанный на механизме работы клеток живого организма;
- архитектуры систем защиты компьютерных сетей, к которым применима биологическая метафора;
- методы защиты компьютерных систем и сетей на основе метафоры иммунных систем и иммунокомпьютинга;
- обобщенная архитектура системы защиты компьютерной сети, базирующаяся на подходе “нервная система сети”;
- отказоустойчивые компьютерные системы, основанные на биологических подходах;
- примеры биологических подходов, которые могут использоваться для защиты программного обеспечения;
- применение нейронных сетей в биоподобных системах защиты информации;
- нейро-экспертные системы, основанные на биометафоре;
- применение нейро-нечетких систем;
- биоподобные эволюционные методы;
- гибридные интеллектуальные средства;
- итоги обзора, основные направления исследований в области применения биологических подходов для защиты компьютерных систем и сетей.

SUMMARY

Kotenko I.V., Shorov A.V., Nesteruk P.G. **Analysis of bio-inspired approaches for protection of computer systems and networks.**

One of the major goals for building of secure systems and networks is creation of protection mechanisms which are fault-tolerant, have high scalability and adaptability (including the ability to self repairing and self healing).

The paper contains a general analysis of some existing approaches to the computer systems protection based on biological metaphor. Not all of them can be fully realized nowadays, of course. However, many of these approaches can be viable and can give new impetus to the development of advanced information security systems.

The paper gives an overview of the following main issues of using of bio-inspired approaches for protection of computer systems and net-works:

- basic biological metaphors and approaches that are applicable to the protection of computer systems and networks;
- approach to protecting a computer network, based on the mechanism of living organism cells;
- architectures of computer network security systems that use the biological metaphor;
- methods of protecting of computer systems and networks based on the metaphor of immune systems and immunocomputing;
- generalized architecture of a computer network security system based on the "nervous system network" approach;
- fault-tolerant computer systems based on biological approaches;
- examples of biological approaches, which can be used for software protection;
- application of neural networks in bio-based information protection systems;
- neuro-expert systems based on biological metaphor;
- application of neuro-fuzzy systems;
- bio-inspired evolutionary methods;
- hybrid intelligent tools;
- conclusion of the review, main research directions in the area of application of biological approaches to protect computer systems and networks.