УДК 004.896

А.В. Калач[1], Е.С. Немтина[2]
([1]Воронежский институт Государственной противопожарной службы МЧС России,
[2]Воронежский институт МВД России; e-mail: a_kalach@mail.ru)

ИНТЕЛЛЕКТУАЛЬНЫЕ СРЕДСТВА И МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Показана необходимость придания системам защиты информации в информационных технологиях эволюционных качеств, присущих биосистемам, возможность развития и адаптивность.

Ключевые слова: интеллектуальные системы, нейронные сети, системы защиты информации, биосистемы.

A.V. Kalach, E.S. Nemtina

INTELLECTUAL MEANS AND MODELLING OF SYSTEMS OF PROTECTION OF THE INFORMATION

Given work necessity of giving is shown systems of protection of the information in information technology of the evolutionary qualities inherent in biosystems, possibility of development and adaptability.

Key words: intellectual systems, neural networks, systems of protection of the information, biosystems.

Статья поступила в редакцию Интернет-журнала 9 февраля 2011 г.

В научной литературе часто обсуждается необходимость придания эволюционных качеств системам защиты информации в информационных технологиях, которые свойственны биосистемам (таких как возможность развития и адаптивность). Заявления о применении "технологии активной защиты", основанной на оценке поведения программ с точки зрения их потенциальной опасности, исходят от известных производителей [1]. Такие системы защиты информации при возникновении подозрений в заражении вирусом или проникновении злоумышленника корректируют средства защиты компьютера при изменении его статуса или осуществляют его блокировку. Таким образом, вопрос эволюционного развития систем информационной безопасности является весьма актуальным. В связи с чем, вместе с традиционными средствами защиты корпоративных сетей, такими как антивирусы, детекторы уязвимостей, межсетевые экраны и детекторы вторжений, широко применяются средства автоматизации защиты, включающие корреляторы событий, программы обновлений, средства аутентификации, авторизации и администрирования, системы управления рисками.

Существующие публикации о применении интеллектуальных систем защиты информации [2-6] посвящены системам обнаружения атак, в качестве интеллектуального инструмента в которых используются нейронные сети, системы нечеткой логики и основанные на правилах экспертные системы.

Схемы обнаружения атак включают в себя обнаружение злоупотреблений и аномалий. К первым относятся атаки, использующие известные уязвимости в системах информационных технологий, а деятельность, несвойственную пользователям системы, – ко вторым. Для выявления аномалий анализируется деятельность, отличная от шаблонов, установленных для пользователей. Выявление и обнаружение аномалий связано с формированием базы данных, содержащей профили контролируемой деятельности, а обнаружение злоупотреблений – со сравнением деятельности пользователя с известными шаблонами поведения хакера и применением методов на основе правил, описывающих сценарии возможны атак. В случае, если действия пользователя не совпадают с установленными правилами, то механизм обнаружения идентифицирует потенциальные атаки.

В основе большинства систем обнаружения злоупотреблений и аномалий заложена модель, предложенная Деннингом. Модель поддерживает набор профилей для легальных пользователей, согласовывает записи подсистемы аудита с соответствующим профилем, обновляет профиль и информирует о всех выявленных аномалиях. Для определения аномального поведения применяются статистические методы сравнения используемых пользователем команд с нормальным режимом работы. Поведение пользователя возможно представить в виде модели на основе правил, в терминах прогнозируемых шаблонов или анализа изменения состояния, а для выявления факта атаки используют методы сравнения с образцом.

В системах обнаружения атак можно выделить варианты применения нейронных сетей, к примеру, дополнение нейронной сетью существующих экспертных систем для фильтрации поступающих сообщений с целью снижения числа ложных срабатываний, присущих экспертной системе. Таким образом, чувствительность системы возрастает, так как экспертная система получает данные только о событиях, которые рассматриваются в качестве подозрительных. Если нейронная сеть за счет обучения стала идентифицировать новые атаки, то экспертную систему следует обновить, иначе новые атаки будут игнорироваться экспертной системой, прежние правила которой не способны распознавать данную угрозу.

Если нейронная сеть представлена в виде отдельной системы обнаружения атак, то при обработке трафика происходит анализ информации на наличие в нем злоупотреблений. Любые возможные случаи, которые идентифицируются с указанием на атаку, используются системой автоматического реагирования на атаки или перенаправляются к администратору безопасности. В сравнении с предыдущим подходом, данный принцип обладает преимуществом в скорости, так как существует только один уровень анализа, а сама система обладает свойством адаптивности. Нейронную сеть применяют также в системах криптографической защиты информации для хранения криптографических ключей в распределенных сетях.

Одним из основных недостатков нейронной сети является "непрозрачность" формирования результатов анализа. Тем не менее, использование гибридных нейро-экспертных или нейро-нечетких систем позволяет отразить в

структуре систему нечетких предикатных правил, которые автоматически корректируются в процессе обучения нейронной сети. Свойство адаптивности нечетких нейронных сетей позволяет решать отдельно взятые задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, автоматически формировать новые правила при изменении поля угроз, а также реализовать систему защиты информации технической системы в целом.

В нашей стране для обнаружения и противодействия несанкционированным действиям используют различные математические методы и интеллектуальные инструменты. В ряде работ по защите информации рассматривается использование интеллектуальных мультиагентных систем: дается обзор инструментов реализации атак, онтология предметной области, определяются структура команды агентов средств защиты информации, механизмы их взаимодействия и координации.

Определенная часть работ рассматривает использование аппарата нейронной сети и генетических алгоритмов для защиты сетей от программных атак, направленных на нарушение доступности ресурсов. В данном случае нейронная сеть используется для обнаружения признаков атак в сетевом трафике, идентификации форматов передаваемых данных, динамической идентификации участников обмена, а генетические алгоритмы – для получения близкого к оптимальному решению в задачах управления маршрутами и параметрами трафика при наличии нечеткости данных идентификации атаки в условиях дефицита информации или информационного "шума". Кроме того, для реализации активного аудита безопасности работы системы информационных технологий применяется аппарат нечетких множеств. Для определения уровня защищенности сетей от угроз несанкционированного доступа, обнаружения злоупотреблений пользователей и программных атак применяются методы интеллектуального анализа данных, работающие по принципу адаптивной защиты от несанкционированного доступа – "анализ – прогнозирование – предупреждение".

Ряд исследований посвящен идентификации и аутентификации пользователя по биометрическим, фонетическим параметрам, которые используют математический аппарат нейронных сетей, комбинированные методы быстрой цифровой обработки сигналов и нейронной сети.

Проведенный анализ приводит к выводу о необходимости решения не конкретных задач защиты информации с применением нейронных сетей, систем нечеткой логики, экспертных систем, а формировании единого подхода к применению интеллектуальных средств для создания комплексной адаптивной защиты систем информационных технологий на основе биоаналогии. Таким образом, проектирование следует осуществлять как единый процесс построения адаптивной системы с внутренне присущими функциями защиты информации.

Для решения поставленной задачи наилучшим сочетанием свойств обладают нечеткие нейронные сети, так как они сочетают в себе достоинства нейронной сети и нечеткой логики, опирающейся на опыт экспертов информационной безопасности. Механизм нечеткого логического вывода позволяет ис-

пользовать опыт экспертов, представленный в виде системы нечетких предикатных правил, для предварительного обучения нечеткой нейронной сети. Дальнейшее обучение нейронной сети на поле известных угроз предоставляет возможность анализа процесса логического вывода для коррекции существующей или синтеза новой системы нечетких предикатных правил средств защиты информации.

Рассмотрим следующие свойства нечетких нейронных сетей, необходимые для адаптивных средств защиты информации:

- распределенный параллелизм вычислений;
- адаптивность нейро-нечетких средств защиты информации (системы нечетких правил);
- возможность классификации угроз;
- "прозрачность" для анализа структуры;
- функциональная устойчивость и защищенность элементной базы.

Самовоспроизведение путем передачи генетической информации является целью жизни. Важно, чтобы в период жизни структуры она успевала построить хотя бы одну свою копию. Копии содержат в себе определенное количество "информационных дефектов" – мутаций, что является важным условием процесса эволюции. Метаболизм (обновление), самовоспроизведение, мутабильность, молекулярные механизмы переноса информации и наследования в организмах обеспечивают совершенствование живых информационных систем [6].

Биосфера – иерархическая информационная система с единым подходом к методам и способам преобразования, хранения, переноса информации, которые обладают высокой степенью защищенности. Многообразие различных видов и форм существования жизни можно сравнить с многообразием специализированных подсистем системы информационных технологий, которые различаются по свойствам и сложности структурной организации. Иерархия биосферы подразделяется на уровни системной организации генетического материала: нуклеотидный, триплетный, генный (образуют молекулярный уровень), хромосомный, клеточный уровень, тканевый уровень, органный уровень, организменный уровень, популяционный уровень, видовой уровень, биоценотический уровень, глобальный (биосферный уровень). Начиная с молекулярного уровня, каждому уровню иерархии присуща генетическая преемственность и информационная защищенность структур. Биосфера является сложной информационной системой, подсистемы которой обладают набором механизмов и свойств, которые придают высокую информационную защищенность. Высокий уровень защищенности и жизнеспособности видов обусловлен надежностью способа кодирования, хранения и передачи информации (в процессе размножения) – генетического кода вида.

Придание положительных качеств биосистем, отвечающих за защищенность информационных процессов, системам информационных технологий связано с наличием:

- информационно-защищенных механизмов сохранения и передачи информации;
- свойств сложной кибернетической системы;

- иерархии функционально разнородных подсистем с развитыми функциями защиты;

- эволюционных качеств (способности к зарождению, росту и развитию, обучению и адаптации в динамической внешней среде).

Механизмы наследственности и изменчивости носят информационный характер и обеспечивают защищенность биосистемы. Генетический материал биообъектов – это ДНК (дезоксирибонуклеиновая кислота).

Популяции сохраняются благодаря размножению, которое основывается на передаче внутри вида генетической информации при помощи ДНК, которая является универсальным и защищенным носителем информации. ДНК имеет двойственный характер: с одной стороны – защищенный носитель информации, а с другой – сама информация в виде генетического кода. Молекулы ДНК – это линейные макромолекулы, которые имеют вид двойных цепей полимеров, составленных из нуклеотидов, каждый из них содержит по одной молекуле фосфорной кислоты и сахара, одно из четырех азотистых оснований: аденин, гуанин, цитозин и тимин. Сочетания трёх нуклеотидов в цепи ДНК – генетический код. Нарушения последовательности нуклеотидов в цепи ДНК приводят к мутациям (наследственным изменениям в организме). ДНК точно воспроизводится при делении клеток, обеспечивает передачу в поколениях наследственных признаков и специфических форм обмена веществ. Надежность структуры ДНК объясняется силой водородных связей между цепями, а уникальность – разнообразием видов аминокислот, входящих в генный код.

В соответствии с правилом комплементарности в ДНК двойные цепи полимеров соединены между собой водородными связями: каждый кодон имеет только один антикодон, способный связаться с ним по всем водородным связям. Устойчивость структуры ДНК объясняется силой водородных связей между цепями полимеров: аденин и тимин образуют между собой две водородные связи, а гуанин и цитозин – три. Двойная связь слабее чем тройная, увеличение отношения ограничивает количество кодов, следовательно, чем меньше вариантов, тем проще закодированная в геноме организация вида.

Для обеспечения информационной защищенности процесса передачи и хранения информации в ДНК используется принцип избыточности. Чем сложнее организм, тем большая избыточность кода в геноме. В ядрах клеток высших организмов много избыточной ДНК, так как геном состоит из тысяч повторяемых участков, чередующихся с уникальными последовательностями оснований. Основные особенности кода ДНК, обеспечивающие информационную защищенность и функциональную устойчивость биосистем: информационная избыточность и комплементарность кодирования, равномерность распределения масс и уравновешенность системы связей по молекуле ДНК.

Один из основных принципов для обеспечения информационной защищенности генома из-за значительной избыточности – клеточный принцип построения биосистем. Достаточно одной клетки, чтобы на основе наследственной информации восстановить организм с его видовыми и индивидуальными особенностями. Биосистема – сложная система, состоящая из иерархии специализированных автономных компонентов, которые осуществляют общесистем-

ные функции по хранению всей наследственной информации, обрабатывают и декодируют определенную часть общей информации, связанную с функциями данных компонентов.

Из градации организмов по степени сложности следует, что чем проще система (меньше структурная избыточность и защищенность), тем интенсивнее процесс передачи информации, большая избыточность за счет высокой скорости размножения. Большие объемы компенсируют возможную потерю или модификацию информации при передаче. Наоборот, чем сложнее система, тем больше структурная избыточность и меньше скорость размножения. Используется избыточность самих информационных сообщений – большое число повторяющихся последовательностей нуклеотидов в кодах. Клетка – это наименьшая структура, в которой хранится и декодируется информация. Общая организация процессов декодирования информации внутри клетки обладает повышенной информационной защищенностью: декодирование триплетного кода ведется по принципу сопоставления – каждый кодон имеет только один антикодон, способный связаться с ним по всем водородным связям. В таком случае ядро представляется как компонент системы, которое осуществляет только процессы копирования и хранения информации, оригинальная генетическая информация не покидает ядра и не претерпевает изменений (свойство стабильности). Дубликат информации в дальнейшем преобразуется с возможностью фиксации изменений во вновь созданных компонентах системы (свойство пластичности).

Основные особенности клетки как защищенной системы по обработке и хранению информации заключаются в следующем:

- декодирование генома производится над дублем системной информации вне ядра специальными обрабатывающими структурами, которые используют при декодировании принцип сопоставления при соблюдении комплементарности кода;

- генетическая (системная) информация хранится в обособленной структуре – ядре, защищающем ее от внешних воздействий.

Таким образом, отдельные клетки и биологические организмы в целом благодаря иерархической организации, методам и принципам хранения, кодирования и декодирования информации являются информационно защищенными системами, а моделирование систем защиты информации и оценки уровня защищенности систем информационных технологий – необходимый этап для автоматизации процедур анализа уязвимостей и выявления атак на корпоративную систему с целью придания эволюционных свойств адаптивности и развития.

Нередко модели защиты являются важной частью системы управления рисками. Учитываются следующие параметры: актуальные угрозы, имеющиеся ошибки в программном обеспечении, важность, интервал и время простоя различных ресурсов, вероятность атаки, варианты защиты и возможная величина ущерба. Система управления рисками в системе информационных технологий позволяет просчитывать существующие риски, моделировать оптимальный комплекс контрмер, автоматически разрабатывать профиль защиты, оценивать остаточные риски.

В структуре защиты систем биосистемная аналогия базируется на иерархии средств защиты информации, встроенных механизмах иммунной защиты и накопления опыта. Наиболее известные системы, ограничиваются реализацией функций нижнего уровня системы защиты и антивирусной направленностью средств иммунной защиты [7]. Около 70 % вирусных атак осуществляется извне через точку входа в защищаемую сеть, только около 30 % изнутри. К внешним угрозам жизнедеятельности системы относятся первые, к внутренним угрозам – вторые. В каждом случае задействуется иммунная защита биосистемы. Реализация идеи информационной иммунной системы заключается в том, что в случае обнаружения в сети признаков заражения происходит отправка образа нового вируса в антивирусный центр, спустя некоторое время получается обновление антивирусной базы, которое распространяют по корпоративной сети прежде, чем успеет распространиться вирус.

Данный принцип противоречит биосистемной аналогии, а именно с внутрисистемной реализацией иммунной защиты, так как в рассмотренной системе антивирусной защиты (в отличие от биосистемы) большая часть механизмов иммунной защиты находится в антивирусном центре, расположенном за пределами корпоративной сети.

В том случае, когда антивирусный центр размещен за пределами защищаемой системы информационных технологий, злоумышленники могут сформировать канал для загрузки вирусов и вредоносных программ под видом обновления антивирусной базы, получить доступ к конфиденциальной информации в случае автоматической отправки на анализ подозреваемых на наличие вируса файлов. Реакция подобной иммунной защиты в лучшем случае измеряется часами, что, учитывая перечисленные возможности реализации каналов несанкционированного доступа, неприемлемо для большинства критических приложений. Следовательно, область применения подобного подхода ограничена только восстановлением выведенной из строя корпоративной сети, как аналог процесса реанимации больной биосистемы с помощью инъекций [8].

Реализации совокупности механизмов наследования, развития, адаптации и отбора в эволюционных процессах, свойственных биосистемам, лежит в основе биосистемной аналогии систем информационных технологий. Разрабатываемые интеллектуальные средства выявления атак и несанкционированных информационных процессов в корпоративной сети уделяют основное внимание свойству адаптивности при построении перспективных систем, причем системы уровня почтовых шлюзов и межсетевых экранов ориентированы в большей мере на выявление внешних атак, а системы серверного уровня – на нейтрализацию внутренних угроз в корпоративной системе.

Как правило, известные интеллектуальные системы защиты информации, реализуют лишь механизмы оперативной реакции и нейтрализации угроз жизнедеятельности системы информационных технологий, при этом практически не уделяя внимание координирующей роли, которую играет нервная система – верхний уровень иерархии защиты биологических систем в реализации эволюционного процесса накопления жизненного опыта системы.

Литература

1. ***Голосовая*** текстонезависимая система аутентификации, идентификации пользователя / Бабенко Л.К., Макаревич О.Б., Федоров В.М., Юрков П.Ю. // Нейрокомпьютеры: разработка и применение, 2003, № 12.

2. ***Ивахненко А.Г., Ивахненко Г.А., Савченко Е.А.*** Самоорганизация дважды многорядных нейронных сетей для фильтрации помех и оценки неизвестных аргументов // Нейрокомпьютеры: разработка применение, 2001, № 12.

3. ***Лукацкий А.В.*** Системы обнаружения атак // "Банковские технологии", 1999. С. 54-58.

4. ***Медведовский И.Д., Платонов В.В., Семьянинов П.В.*** Атака через Интернет. С.-Пб.: НПО Мир и семья, 1997.

5. ***Милославская Н.Г., Толстой А.И.*** Интрасети: Доступ в Интернет, защита. М.: ЮНИТИ, 2000.

6. ***Нейронные*** сети в системах криптографической защиты информации / Червяков Н.И., Малофей О.П., Шапошников А.В., Бондарь В. // Нейрокомпьютеры: разработка и применение, 2001, № 10.

7. ***Бочков М.В., Крупский С.А., Саенко И.Б.*** Применение генетических алгоритмов оптимизации в задачах информационного противодействия сетевым атакам // Сборник докладов всероссийской научной конференции "Управление и информационные технологии", Том 2. С.-Пб.: ЛЭТИ, 2003. С. 13-16.

8. ***Осовецкий Л.Г., Нестерук Г.Ф., Бормотов В.М.*** К вопросу иммунологии сложных информационных систем // Изв. вузов. Приборостроение. 2003. Т. 46, № 7. С. 34-40.