Данная работа выполнена при поддержке РФФИ, проект № 07-07-00139-а.

Список литературы

1. Бердичевский М.Н., Дмитриев В.И. Обратные задачи магнитотеллурики в современной постановке // Физика Земли. 2004. № 4. С. 12-29.
2. Шимелевич М.И., Оборнев Е.А., Гаврюшов С.А. Техника построения нейронных сетей для решения многопараметрических обратных задач магнитотеллурического зондирования // Изв. вузов. Геология и разведка. 2001. № 2. С. 129-137.
3. Доленко С.А., Доленко Т.А., Персианцев И.Г., Фадеев В.В., Буриков С.А. Решение обратных задач оптической спектроскопии с помощью нейронных сетей // Нейрокомпьютеры: разработка, применение. 2005. № 1-2. С.89-97.
4. Доленко С.А., Оборнев Е.А., Персианцев И.Г., Шаров С.А., Шимелевич М.И., Шугай Ю.С. Применение адаптивной нейросетевой классификации и кластеризации данных при решении обратной задачи электроразведки // Нейроинформатика-2007. IX Всероссийская научно-техническая конференция. Сборник научных трудов. Ч. 2. С. 234-241. – М., МИФИ, 2007.
5. Доленко С.А., Орлов Ю.В., Персианцев И.Г., Шугай Ю.С.. Адаптивное построение иерархических нейросетевых классификаторов // Нейрокомпьютеры: разработка, применение. 2005. № 1-2. С. 4-11.

С.В. БЕЗОБРАЗОВ
Брестский государственный технический университет, Республика Беларусь
bescase@gmail.com, gva@bstu.by

ИСКУССТВЕННЫЕ ИММУННЫЕ СИСТЕМЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ: ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Проблема защиты компьютерных систем от вредоносных программ является одной из главных проблем защиты информации. Широко применяемый метод сигнатурного поиска не способен обнаруживать новые, неизвестные компьютерные вирусы. Искусственные иммунные системы для защиты информации являются неплохой альтернативой эвристическим методам обнаружения новых зловредных программ. В данной статье представлены методы обнаружения компьютерных вирусов и их классификации, основанные на применении искусственных нейронных сетей в искусственных иммунных системах. Представлены и проанализированы результаты исследований.

Введение. С развитием компьютерных наук и компьютерной техники общество столкнулось с проблемой развития киберпреступности. Одним

из направлений киберпреступности является создание и распространение вредоносных программ, называемыми компьютерными вирусами [1]. На сегодняшний день проблема защиты компьютерных систем от вредоносных программ является одной из основных в области защиты информации. Традиционных подход, основанный на сигнатурном поиске, применяемый для обнаружения компьютерных вирусов, достаточно хорошо позволяет обнаруживать известные вирусы, однако совершенно не подходит для обнаружения неизвестных вредоносных программ. С момента появления нового компьютерного вируса до его обнаружения специалистами антивирусной индустрии проходит некоторое, иногда продолжительное время (от нескольких часов до нескольких дней). За это время современные вредоносные программы способны заразить миллионы компьютеров по всему миру, вызвать настоящие вирусные эпидемии и привести к огромным убыткам. Компьютерные системы с устаревшими антивирусными базами не способны противостоять новой угрозе. Эвристические анализаторы, применяемые для обнаружения неизвестных компьютерных вирусов, на сегодняшний день далеки от совершенства, и зачастую классифицируют чистый, незараженный файл как вредоносную программу, или наоборот, не замечают зловредную программу. По некоторым подсчетам эвристические анализаторы обнаруживают только 25 – 30 процентов компьютерных вирусов, при этом требуют больших затрат процессорного времени и имеют высокий уровень ложных срабатываний [2]. Современные исследования в области защиты информации направлены на создание таких систем безопасности, которые были бы способны достаточно хорошо обнаруживать неизвестные компьютерные вирусы.

В данной статье представлено описание системы обнаружения неизвестных компьютерных вирусов на основе искусственных иммунных систем. Также представлен метод классификации обнаруженных неизвестных компьютерных вирусов. В первом разделе статьи рассмотрена связь биологической иммунной системы с искусственными иммунными системами, и представлен механизм обнаружения вирусов при помощи ИИС. Второй раздел содержит описание метода классификации обнаруженных компьютерных вирусов. В третьем разделе представлены результаты исследований.

1. Применение метода искусственных иммунных систем для обнаружения компьютерных вирусов. Механизмы, использующиеся в искусственных иммунных системах, позволяют обнаруживать неизвестные компьютерные вирусы. Искусственные иммунные системы (ИИС) базируются на основных принципах биологической иммунной системы (БИС).

БИС является уникальной системой, которая ежедневно борется с болезнетворными бактериями и вирусами, защищая организм от инфекций [3]. Уникальность БИС заключается в том, что она способна обнаруживать не только известные вирусы и бактерии, но также и неизвестные. Иммунитет основан на способности лимфоцитов распознавать собственные клетки организма от чужеродных клеток. Основными элементами иммунной системы являются лимфоциты – белые клетки [3]. Лимфоциты образуются из стволовых клеток костного мозга. Незрелые лимфоциты не способны отличать свои клетки от чужеродных, и для того чтобы выполнять иммунологическую функцию они должны пройти стадии обучения и отбора. После синтеза незрелые лимфоциты направляются к органам, в которых происходит их созревание: тимусу (вилочковой железе) и лимфатическим узлам. Лимфоциты в зависимости от места их созревания делятся на В-лимфоциты и Т-лимфоциты. Зрелые лимфоциты имеют на своей поверхности детекторы, которые способны обнаруживать специфический антиген (вредные бактерии, вирусы). Антитела связываются с бактериями, образуя химическую связь, за счет комплементарного соответствия между молекулярной структурой на поверхности бактерии и структурой антитела. Эволюцию лимфоцитов можно проследить на рис. 1.

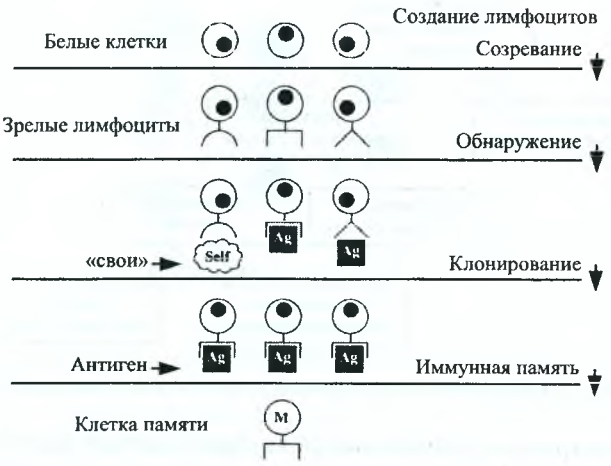

Рис. 1. Эволюция лимфоцитов

БИС имеет ряд мощных вычислительных возможностей, такие как: распознавание, разнообразие, обучение, память, распределенный поиск, саморегуляция, децентрализация, вероятностное обнаружение.

Построенная по основным принципам биологической иммунной системы, искусственная иммунная система обладает всеми ее возможностями и, на наш взгляд, является перспективной для построения современной системы компьютерной безопасности для защиты от вредоносных программ. ИИС состоит из следующих процессов: создание детекторов, обучение и отбор детекторов, уничтожение нежелательных детекторов, циркуляция иммунных детекторов в компьютерной системе, уничтожение детекторов по истечении времени, обнаружение вредоносной программы, клонирование и мутация детекторов, формирование иммунной памяти [4], [5]. Взаимодействие процессов представлено на рис. 2. Все перечисленные процессы находятся в тесном взаимодействии. Еще одной отличительной способностью ИИС является отсутствие единого центра управления.

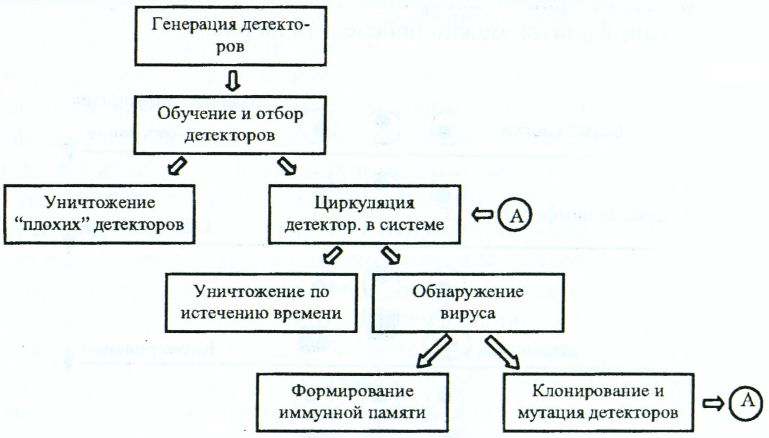

Рис. 2. Взаимодействие процессов искусственной иммунной системы

Рассмотрим подробней каждый из перечисленных процессов.

Процесс генерации детекторов предназначен для создания иммунных детекторов, которые являются основными элементами ИИС и выполняют функцию обнаружения вредоносных программ. Для построения иммунных детекторов мы использовали искусственные нейронные сети, а имен-

но, LVQ сеть (обучающийся векторный квантователь) [6]. В процессе генерации формируется определенное количество детекторов, каждый из которых представляет отдельную нейронную сеть [5]. Структура иммунного детектора, основанного на LVQ, изображена на рис. 3.

Первоначально детекторы не способны отличать чистые файлы от вредоносных программ. Поэтому необходим процесс обучения иммунных детекторов. На стадии обучения иммунные детекторы обучаются распознавать зловредные программы и не реагировать на чистые файлы. Обучение детекторов проходит по следующему алгоритму:

- случайным образом выбирается некоторое количество чистых файлов (например, утилиты операционной системы) и некоторое количество вредоносных программ;
- из выбранных файлов также случайным образом выбирается несколько фрагментов определенной длины (размерность фрагментов зависит от количества входов искусственной нейронной сети, которая формирует детектор);
- выбранные фрагменты образуют обучающую выборку для ИНС и подаются на ее вход.

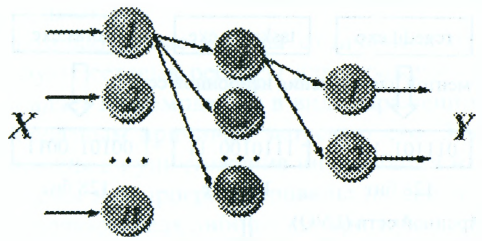

Рис. 3. Искусственная нейронная сеть для векторного квантования

Использование разнообразных файлов и вредоносных программ для формирования обучающей выборки позволяет создавать разнообразные иммунные детекторы, способные обнаружить вероятные вредоносные программы. Механизм обучения нейронной сети, на основе которой формируется иммунный детектор, представлен на рис. 4.

После обучения детекторы проходят стадию отбора. Механизм отбора необходим для предотвращения попаданию в компьютерную систему нежелательных детекторов. Нежелательным детектором называется такой детектор, который реагирует на чистые файлы. Такой детектор должен быть уничтожен.

Обученные иммунные детекторы циркулируют в компьютерной системе, проверяя и классифицируя файлы. Каждому детектору отводится определенное время, на протяжении которого он может находиться в компьютерной системе. После истечения выделенного времени детектор, который не обнаружил вредоносной программы, уничтожается, а на его место приходит новый детектор. Механизм выделения времени для существования детектора и уничтожения по истечении выделенного времени позволяет ИИС избавляться от слабых иммунных детекторов и поддерживает принцип постоянного обновления детекторов.

При обнаружении иммунным детектором вредоносной программы происходит процесс клонирования. Клонирование подразумевает создание большого количества однотипных детекторов (клонируется тот детектор, который обнаружил вредоносную программу). Зачастую, при попадании компьютерного вируса в систему, он заражает большое количество файлов, путем внедрения копии своего тела в файлы-жертвы. Процесс клонирования позволяет иммунной системе в кратчайшие сроки избавиться от всех проявлений обнаруженного компьютерного вируса.

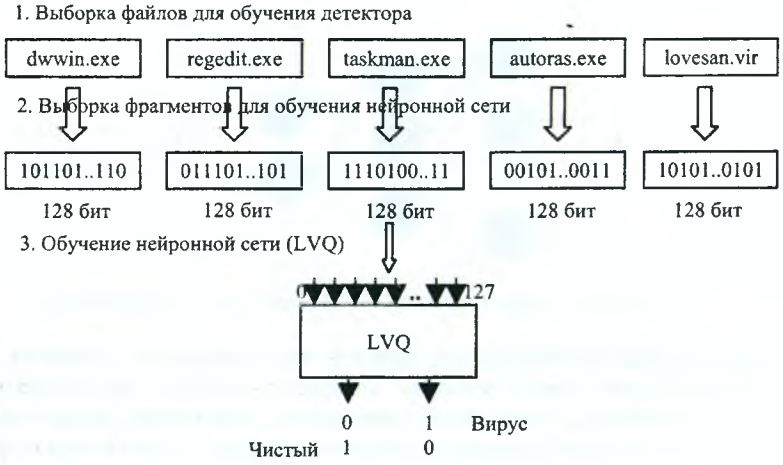

Рис. 4. Механизм обучения иммунного детектора (LVQ)

После избавления компьютерной системы от вредоносной программы выбирается наиболее приспособленный к обнаруженному вирусу детектор и трансформируется в детектор иммунной памяти. Иммунная память

хранит информацию обо всех вирусах, которые когда-либо заражали компьютерную систему. Детекторы иммунной памяти существуют в компьютерной системе достаточно долгий промежуток времени и позволяют оперативно реагировать на повторное заражение.

2. Классификация компьютерных вирусов в искусственных иммунных системах для защиты информации. На сегодняшний день существует большое количество разнообразных зловредных программ, и, несмотря на то, что пока не существует единой системы классификации вирусов, всех их можно разделить по характерным признакам заражения и распространения на несколько основных групп. Существует следующие группы компьютерных вирусов: сетевые черви, классические компьютерные вирусы, троянские программы, хакерские утилиты [7]. Компьютерные вирусы, принадлежащие к разным группам, используют различные алгоритмы заражения, различные вредоносные функции, имеют различные предназначения.

К сетевым червям относятся зловредные программы, которые распространяют свои копии по локальным или глобальным сетям для проникновения на удаленные компьютеры, запускают себя на зараженном компьютере и используют зараженный компьютер для дальнейшего распространения на другие компьютеры.

Классические компьютерные вирусы отличаются от сетевых червей тем, что не используют сетевые ресурсы для заражения компьютера. Как правило, вирус попадает на компьютер в виде зараженного файла и пользователь по разнообразным причинам запускает его. Зачастую классические вирусы направлены на уничтожение информации и нарушения работоспособности системы и запрограммированы на срабатывание на определенные действия пользователя либо на конкретную дату.

Троянские программы, как правило, осуществляют несанкционированные пользователем действия. Такие вирусы собирают информацию о компьютере или пользователе и передают ее злоумышленнику, разрушают или модифицируют информацию, нарушают работоспособность компьютерной системы и т.д. Как правило, такие вирусы не заметны для пользователя и проявляют себя исключительно редко – при отсылке собранной информации злоумышленнику. Также троянские программы способны предоставлять злоумышленникам вычислительные ресурсы компьютерной системы, превращая ее в машину «зомби».

Знание о том, к какой категории принадлежит обнаруженная вредоносная программа, дает возможность сделать выводы о пути проникновения вируса в компьютерную систему и о тех вредоносных или деструк-

тивных действиях, которые выполняет обнаруженный вирус. Такая информация позволит принять оперативные действия по предотвращению утечки и разрушения информации.

Нами была предложена система классификации обнаруженного с помощью искусственной иммунной системы неизвестного компьютерного вируса. В качестве классификатора была использована совокупность искусственных нейронных сетей – отдельная нейронная сеть на отдельный тип вредоносной программы. Для обучения нейронной сети на ее вход подаются образцы зловредных программ, относящиеся к той категории, для классификации которой предполагается использование данной нейронной сети. Каждая нейронная сеть обучается на отдельной категории вирусов. При поступлении неизвестного образа на вход обученной нейронной сети она соотносит его с эталонным вектором и принимает решение о принадлежности или непринадлежности его к классу. Классификатор вредоносной программы изображен на рис. 5.

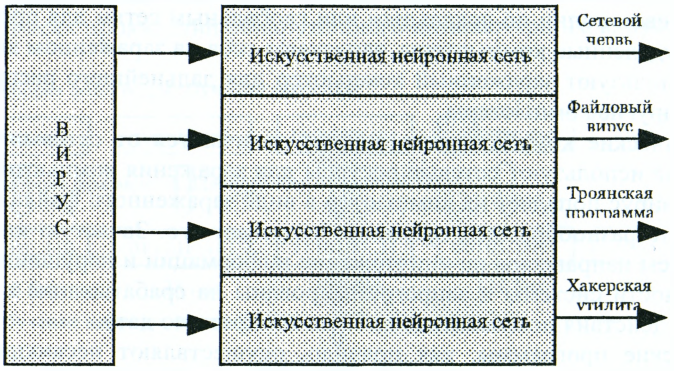

Рис. 5. Применение ИНС для классификации компьютерного вируса

3. Результаты исследований. Нами была разработана модель системы компьютерной безопасности, предназначенной для обнаружения компьютерных вирусов, на основе искусственных иммунных систем [5]. Были проведены ряд тестов.

В первом тесте представлен сравнительный анализ результатов обнаружения компьютерных вирусов различными антивирусными продуктами и модели ИИС. Для теста были выбраны следующие антивирусные продукты: антивирус Касперского версии 5 с актуальными вирусными базами; антивирус Касперского версии 5 с устаревшими вирусными базами;

NOD 32 с отключенными вирусными базами, но с эвристическим анализатором; и разработанная нами модель ИИС для обнаружения компьютерных вирусов. Эксперимент разрабатывался с целью показать незащищенность компьютерной системы с неактуальными вирусными базами, продемонстрировать несовершенство эвристических алгоритмов, и способность искусственных иммунных систем к обнаружению вредоносных программ. Табл. 1 отображает результаты проведенного эксперимента.

Таблица 1

Сравнительный анализ различных антивирусных продуктов

Имя файла	Антивирус Касперского (актуал. базы)	Антивирус Касперского (устар. базы)	NOD32 (эвристическ. анализатор)	ИИС (4 детектор-ов)	ИИС (500 детекторов)
Backdoor.Win32.Agent.lw	Backdoor	OK	OK	OK	Вирус
Backdoor.Win32.Agobot	Backdoor	Backdoor	Win32/Agobot	Вирус	Вирус
Email-Worm.BAT.Maddas	Email-Worm	Email-Worm	OK	Вирус	Вирус
Email-Worm.JS.Gigger	Email-Worm	Email-Worm	OK	Вирус	Вирус
Email-Worm.VBS.Loding	Email-Worm	Email-Worm	OK	Вирус	Вирус
Email-Worm.Win32.Zafi.d	Email-Worm	OK	NewHeur_PE	Вирус	Вирус
Net-Worm.Win32.Bozori.a	Net-Worm	OK	Win32/Bozori	Вирус	Вирус
Net-Worm.Win32.Mytob.a	Net-Worm	OK	Win32/Mytob	Вирус	Вирус
Trojan-Downl.JS.Psyme.y	Trojan	OK	OK	Вирус	Вирус
Trojan-Downl.Win32.Bagle	Trojan	OK	Win32/Bagle	Вирус	Вирус
Trojan-Proxy.Win32.Agent	Trojan	Trojan	OK	Вирус	Вирус
Trojan-Proxy.Daemonize	Trojan	Trojan	OK	OK	Вирус
Trojan-Proxy.Mitglieder	Trojan	Trojan	Win32/Trojan	Вирус	Вирус
Trojan-PSW.LdPinch	Trojan	Trojan	Win32/PSW	Вирус	Вирус
Virus.Win32.Gpcode.ac	Virus.Win32	OK	OK	Вирус	Вирус
Exploit.Win32.DebPloit	Exploit	OK	OK	OK	Вирус

Таблица 2

Результаты работы классификатора вирусов

	Классификатор (Email-Worm)	Классификатор (Net-Worm)	Классификатор (Trojan-PSW)	Классификатор (Virus)
Email-Worm.Win32.Brontok.q	Email-Worm	-	-	-
Email-Worm.Win32.Warezov.a	Email-Worm	-	-	-
Email-Worm.Win32.Zafi.d	Email-Worm	-	-	-
Net-Worm.Win32.Lovesan.a	-	Net-Worm	-	-
Net-Worm.Win32.Maslan.a	-	Net-Worm	-	-
Net-Worm.Win32.Mytob.a	-	Net-Worm	-	-
Trojan-PSW.Win32.Antigen.a	-	-	Trojan-PSW	-
Trojan-PSW.Win32.CrazyBilets	-	-	Trojan-PSW	-
Trojan-PSW.Win32.Coced	-	-	Trojan-PSW	-
Virus.Win32.Gpcode.ac	-	-	-	Virus.Win32
Virus.Win32.Neshta.a	-	-	-	Virus.Win32
Virus.Win32.Delf.lk	-	-	-	Virus.Win32

Анализируя полученные результаты, представленные в табл. 2, можно сделать вывод, что антивирус с актуальными вирусными базами обнаружил все вирусы, которые использовались в эксперименте. Это объясняется тем, что в базах содержались сигнатуры данных вирусов. Антивирус с устаревшими вирусными базами обнаружил только половину присутствующих вирусов, что явно отражает угрозу компьютерной системы перед новыми компьютерными вирусами. Антивирус NOD 32, который для обнаружения использовал эвристический анализатор, обнаружил только семь вирусов, что отражает несовершенство современных эвристических алгоритмов для обнаружения неизвестных вирусов. Искусственная иммунная система, которая использовала только четыре детектора, не обнаружила три вируса, однако с увеличением количества детекторов все присутствующие вирусы были обнаружены.

Второй тест отображает результаты работы модуля классификации обнаруженных вирусов. Для проведения данного теста были выбраны классические компьютерные вирусы, каждый из которых характеризует свой класс вирусов. Как видно из полученных результатов, классификатор достаточно успешно и корректно классифицирует компьютерные вирусы. Однако следует обратить внимание на то, что большое количество современных вредоносных программ разработаны с использованием различных и смешанных технологий. К примеру, сетевые черви могут иметь функции трояна и классического вируса. Такой подход значительно усложняет классификацию вредоносных программ.

Выводы. Разработана модель системы безопасности компьютерной системы на основе искусственных иммунных систем для обнаружения вредоносных программ. Разработанная модель позволяет обнаруживать неизвестные компьютерные вирусы. Разработан метод классификации обнаруженных с помощью ИИС компьютерных вирусов.

Список литературы

1. Michael Erbschloe. Trojans, worms and spyware. A computer security professional's guide to malicioius code.

2. Проактивная защита как она есть - http://www.viruslist.com/ru/analysis/.

3. Иммунитет. Энциклопедия «Кругосвет» – http://krugosvet.ru, 2004.

4. Forest S., Perelson A., Allen L., Cherukuri R.: Self-Nonself Discrimination in a Computer. Proceedings IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press. P. 202–212, 1994.

5. Искусственные иммунные системы для защиты информации: применение LVQ сети // IX Всероссийская научно-техническая конференция «Нейроинформатика - 2007»: Сборник научных трудов. В 3-х ч. Ч. 2. - М.: МИФИ, 2007

6. Kohonen T. Sell-organised formation of topologically correct feature maps// Biological Cybernetics. - 1982. - N 43. - P. 59-69.

7. Описание вредоносных программ - http://www.viruslist.com/ru/viruses/.