прямоугольников в этих покрытиях значительно меньше, чем в покрытиях, полученных с использованием Алгоритма 3.

Величину перекрытия элементов покрытия в процентном отношении к общей площади покрытия можно оценить следующим образом: для первого и второго алгоритмов примерно 10% независимо от градусной меры острого угла; для алгоритма 3 от 50% при углах, близких к 0°, до 95% при остром угле, близком к 90°.

Заключение. Предлагаемые алгоритмы позволяют находить покрытие элемента топологии микросхем типа шина. Основные характеристики предлагаемых алгоритмов:

- использование технологических и технических ограничений лазерного генератора;
- векторизация координат в процессе исполнения алгоритмов;
- поэтапное формирование покрытия.

Алгоритмы формирования покрытия шины были протестированы на примерах шин из реальных интегральных схем. Нужно подчеркнуть, что выбор элемента топологии – шины – не ограничивает использование предложенных алгоритмов для других видов топологии ИС. Например, для покрытия участков произвольных контуров, содержащих острые углы.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Фейнберг В.З. Геометрические задачи машинной графики больших интегральных схем. - М.: Радио и связь, 1987.- С.117
2. Mark Keil J. Polygon Decomposition //Department of Computer Science University of Saskatchewan, Saskatoon, Sask, Canada - May 14, 1996.
3. O Rourke J. Art Gallery Theorems and Algorithms // Oxford University Press, New York,NY, 1987.
4. Казеннов Г.Г., Осипов Л.Б., Щемелинин В.М. Алгоритм подготовки данных для микрофотонаборных установок // Электронная промышленность.- 1974.- № 6.- С. 84-87.
5. Носова Е.Г., Свердлов А.Г., Фейнберг В.З. Алгоритмы разбиения плоских фигур в системах машинного проектирования интегральных схем // Изв. АН БССР. Сер. физ.- мат. наук. – 1978. № 5. – С. 16-23.
6. Роджерс Д., Адамс Дж., Математические основы машинной графики.– М.: Мир, 2001. – 604 с.
7. Markde Berg, Marcvan Kreveld, Marc Overmarset al. Computational Geometry: algorithms and applications. 2nd edition. Springer-Verlag, 2000 - 367 p.

Материал поступил в редакцию 17.01.08

VORONOV A.A. Algorithms of a covering by rectangulars of objects of topology of microcircuits

The base algorithms of formation of a covering of objects of topology are considered. The purpose of job is the development and realization of algorithms allowing effectively on time and with controlled accuracy to represent (to cover) elements topology of a semi-conductor plate as suitable for exhibiting by the single-channel generator of the images.

Object of research are the one-coherent final areas of a plane - elements of topology of microcircuits in particular trunks.

УДК 004.8.032.26

Безобразов С.В., Головко В.А.

НЕЙРОСЕТЕВОЙ ПОДХОД ДЛЯ КЛАССИФИКАЦИИ КОМПЬЮТЕРНЫХ ВИРУСОВ

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

На сегодняшний день существует большое количество разнообразных компьютерных вирусов, использующие те или иные вредоносные действия и методы заражения компьютерных систем. Некоторые зловредные программы разрабатываются злоумышленниками с целью кражи конфиденциальной информации, другие имеют функцию уничтожения информации, хранящейся на зараженной компьютерной системе, третьи модифицируют информацию с целью дезинформации или требования выкупа за возвращения исходного вида информации. Часть компьютерных вирусов для своего распространения используют локальные и глобальные сети, часть зловредных программ используют функции электронной почты и распространяются в виде вложения в электронные письма, часть вредоносных программ переносятся с устройствами хранения информации.

В зависимости от вредоносных функций и способом распространения компьютерные вирусы принято разделять на классы. И, хотя, на сегодняшний день не существует общепринятой классификации компьютерных вирусов, все их разделяют на несколько больших классов. Зная, к какому классу принадлежит обнаруженный компьютерный вирус, можно сделать предположения о его способе распространения и вредоносных функциях, что позволит своевременно закрыть «дыры» в компьютерной системе безопасности и предотвратить утечку информации.

В данной статье рассмотрен нейросетевой подход в классификации компьютерных вирусов, обнаруженных искусственной иммунной системой для защиты информации. В первом разделе статьи представлена классификация компьютерных вирусов. В зависимости от классов рассмотрены вредоносные функции компьютерных вирусов и их пути распространения. Второй раздел содержит описание нейросетевого подхода классификации обнаруженных компьютерных вирусов. В третьем разделе представлены результаты исследований.

1. Классификация компьютерных вирусов. На сегодняшний день существует большое количество разнообразных зловредных программ, и хотя в пока еще не существует единой системы классификации вирусов, всех их можно разделить по характерным признакам заражения и распространения на несколько групп. Все многообразие компьютерных вирусов разделяют на следующие группы: сетевые черви, классические компьютерные вирусы, троянские программы, хакерские утилиты [3].

***Безобразов Сергей Валерьевич**, аспирант кафедры «Интеллектуальные информационные технологии» Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

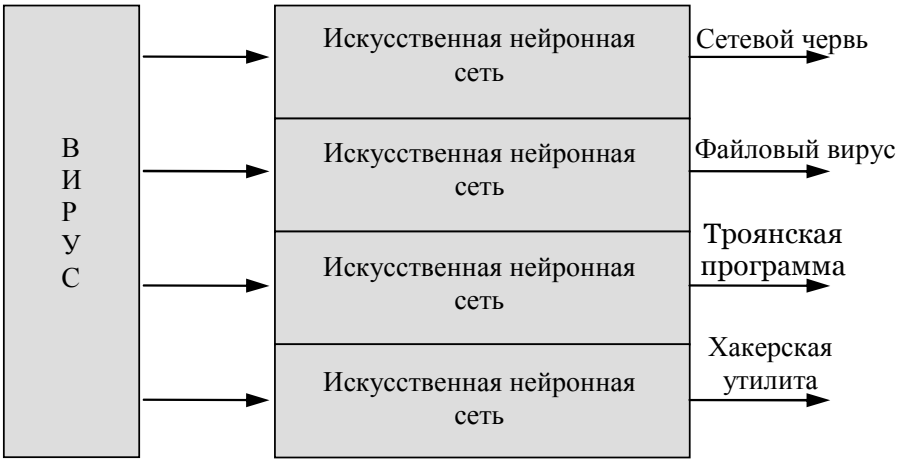

Рис. 1. *Совокупный классификатор обнаруженных компьютерных вирусов*

Таблица 1. *Результаты работы совокупного классификатора*

	Классиф. (Email-Worm)	Классиф. (Net-Worm)	Классиф. (Trojan-PSW)	Классиф. (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.k	-	-	-	Virus.Win32
Email-Worm.Win32.Nyxem	Email-Worm	Net-Worm	-	Virus.Win32

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. И если раньше сетевые черви для своего распространения в основном использовали только компьютерные сети, то сегодня, с развитием новых технологий, появляются и приобретают большую популярность вирусы, которые для своего распространения используют беспроводные и мобильные сети и заражают устройства, работающие в этих сетях. Так, современные сетевые черви используют электронную почту, файлообменные и IRC-сети, сети обмена мгновенного сообщения (такие как icq), беспроводные сети (телефоны, карманные компьютеры и т.д.). В зависимости от используемых технологий сетевые черви подразделяются на: почтовые черви (Email-Worm); черви, использующие интернет-пейджеры (IM-Worm); черви в IRC каналах (IRC-Worm); разнообразные сетевые черви (Net-Worm); черви для файлообменных сетей (P2P-Worm). Для проникновения на компьютер черви используют различные механизмы: ошибки (дыры и уязвимости) в операционных системах и программном обеспечении, ошибки пользователей (к примеру, приводящие к открытию полного доступа к ресурсам компьютерной системы), методы социального инжиниринга (например, тексты писем, призывающие открыть вложенный файл) и т.д.

Классические компьютерные вирусы отличаются от сетевых червей тем, что не используют компьютерные сети для заражения компьютера. Как правило, такой 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 компьютерной системы, и запрограммированы на срабатывание на определенные действия пользователя либо на конкретную дату. В свою очередь классические вирусы подразделяются на несколько групп, самыми известными из которых являются загрузочные (boot) вирусы и макро-вирусы. Загрузочные вирусы заражают загрузочные сектора жесткого или гибкого дисков и загружаются в оперативную память до загрузки операционной системы. Макро-вирусы для своего запуска используют макрокоманды каких-либо приложений. К примеру, наиболее распространенными макровирусами являются вирусы, разработанные под офисный пакет Microsoft Office. Классические вирусы подразделяются на: файловые вирусы (такие черви используют файловую систему операционной системы); загрузочные вирусы (записывают себя в загрузочный сектор жесткого диска); макровирусы, которые используют макроязыки офисных приложений; вирусы-сценарии, созданные с помощью языков сценария (Java Script, VBScript, PHP и др.). В последнее время классические вирусы практически не встречаются в чистом виде, так как современные преступники преследуют цель кражи информации с последующей ее продажей.

Троянские программы, как правило, осуществляют несанкционированные пользователем действия. Такие вирусы, при заражении компьютерной системы, 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, например, при отсылке собранной информации злоумышленнику. Также троянские программы способны предоставлять злоумышленникам вычислительные ресурсы компьютерной системы, превращая ее в машину «зомби». Нередки случаи организации целой сети, состоящей из «зомби» - машин, которые в дальнейшем используются злоумышленником для организации крупных хакерских атак. Троянские программы различаются по действиям, производимым на компьютере-жертве. Выделяют следующие группы троянских вирусов: троянские утилиты удаленного администрирования (Backdoor); вирусы для воровства паролей (Trojan-PSW); вирусы для несанкционированного обращения к интеренет-ресурсам (Trojan-Clicker); вирусы для организации сетевой распределенной атаки (Trojan-DDoS); вирусы для загрузки из сети Интернет разнооб-

разных компьютерных вирусов (Trojan-Downloader); троянские вирусы для прокси-серверов (Trojan-Proxy).

Хакерские утилиты наименее опасны для пользователя и, в первую очередь, предназначены для конструирования компьютерных вирусов. Такие программы специально разрабатываются для автоматизации создания нового зловредного кода и вредоносного программного обеспечения. Даже неискушенный в области компьютерных вирусов пользователь с помощью таких программ способен сконструировать новый компьютерный вирус, что доставляет немало забот антивирусной индустрии.

Однако на сегодняшний день практически не существует «чистых» классических вирусов, или сетевых червей, или троянцев. Современные компьютерные вирусы содержат разнообразные реализации методов заражения и вредоносных действий. Так, например, классические вирусы используют механизмы распространения сетевых червей для заражения компьютерных систем, а троянские программы позаимствовали методы у классических вирусов. Такой подход при создании вредоносных компьютерных программ значительно усложняет классификацию и обнаружение зловредных вирусов. Анализ тенденции развития вредоносных программ показывает, что сегодня авторы при создании вредоносных программ постепенно отказываются от методов социальной инженерии и все больше предпочитают использование различных уязвимостей для проникновения в компьютерную систему. Статистика показывает, что основная масса разработчиков вирусов сегодня преследует цель зарабатывания денег на краже информации и дальнейшей ее перепродаже [4].

В последние годы доминирующее место среди компьютерных вирусов занимают троянские программы. На втором месте следуют сетевые «черви». Наметился рост вирусов, направленных на нанесение финансового ущерба пользователям. Увеличивается число атак, направленных на компании среднего и крупного бизнеса. Целью таких атак является не только кража информации, но и вымогательство денег. Так, файловый вирус Gpcode, который появился в 2006 году, стал первым вирусом, который использовал достаточно сложный алгоритм шифрования пользовательских данных [5]. Вредоносная программа шифрует файлы на зараженном компьютере, что дает возможность разработчику вымогать деньги за расшифровку. Разработчики вредоносных программ постоянно используют нестандартные пути для заражения компьютеров: системы мгновенного обмена сообщениями через Интернет; большое количество уязвимостей в популярных браузерах. Вредоносные программы постоянно повышают свою технологичность и методы сокрытия своего присутствия в компьютерной системе. Такие методы, как полиморфизм (изменение тела вируса) и руткит-технология (технология сокрытия присутствия вируса в системе) стали достаточно массовыми и применяются практически во всех вредоносных программах [6].

2. Нейросетевой подход для классификации неизвестных компьютерных вирусов. 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 деструктивных действиях, которые выполняет обнаруженный вирус. Такая информация позволит предпринять оперативные действия по предотвращению утечки и разрушения информации, а также выявит слабые места в системе компьютерной безопасности.

Нами был предложен алгоритм 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 классификации использовалась нейронная сеть для векторного квантования (LVQ) [7], [8]. Для обучения искусственной нейронной сети на ее вход подаются образцы зловредных программ, относящиеся к той категории, для классификации которой предполагается использование данной нейронной сети. Каждая искусственная нейронная сеть обучается распознавать отдельную категорию 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. Таким образом, при обучении, искусственная нейронная сеть выделяет особенности структуры класса компьютерных вирусов, которые позволяют ей корректно классифицировать обнаруженные при помощи искусственной иммунной системы компьютерные вирусы. Совокупный классификатор обнаруженных компьютерных вирусов изображен на рисунке 1.

3. Результаты экспериментов. Нами был произведен ряд тестов, демонстрирующих работу совокупного классификатора. Результаты экспериментов отображены в таблице 1.

Для проведения данного теста были выбраны типичные для каждого класса вредоносных программ компьютерные вирусы. Как видно из полученных результатов, классификатор достаточно успешно и корректно классифицирует практически все компьютерные вирусы, за исключением вируса *Email-Worm.Win32.Nyxem*. В случае классификации компьютерного вируса *Email-Worm.Win32.Nyxem* сразу несколько классификаторов обнаружили характеристики класса компьютерных вирусов, которые они обучены классифицировать. На самом деле, классификация компьютерного вируса *Email-Worm.Win32.Nyxem* как вируса, принадлежащего к разным классам, не является ошибкой совокупного классификаторы. *Email-Worm.Win32.Nyxem* является очень опасным компьютерным вирусом, который сочетает в себе функции сразу нескольких классов вредоносных программ: распространение по компьютерным сетям; распространение по электронной почте в виде вложенного файла, нарушение целостности информации, хранящейся на зараженной машине.

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. Разработан метод классификации обнаруженных с помощью искусственной иммунной системы [9] компьютерных вирусов. Классификация производится на основе совокупного классификатора, построенного с применением методов искусственных нейронных сетей. Классификация обнаруженных компьютерных вирусов позволяет предпринять оперативные действия по предотвращению утечки и разрушения информации, а также выявлять слабые места в системе компьютерной безопасности.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Почему не срабатывают антивирусы – http://www.i2r.ru, 2003.
2. Касперский Е. Компьютерные вирусы: происхождение, реальная угроза и методы защиты / Е. Касперский // Наука и жизнь [Электронный ресурс]. – 2006. – Режим доступа: http://www.delphihelp.org/vir_begginers.html – Дата доступа: 27.03.2006.
3. Е. Касперский. Компьютерное зловредство. – СПб.: Питер, 2007. - 208 с.
4. Spivey M. Practical hacking techniques and countermeasures / M.D. Spivey. - Auerbach Publications, 2007. – 752 p.
5. Virus.Win32.Gpcode.ad // Интернет безопасность [Электронный ресурс]. – 2006. – Mode of access: http://www.viruslist.com/ru/viruses/encyclopedia?virusid=118344 – Дата доступа: 14.04.2006.
6. Хоглунд Г. Руткиты. Внедрение в ядро Windows / Г. Хоглунд, Д. Батлер. – СПб.: Питер, 2007. – 288 с.
7. Kohonen T. Sell-organised formation of topologically correct feature maps// Biological Cybernetics. - 1982. - N43.-P.59-69.
8. В.А. Головко. Нейронные сети: обучение, организация и применение. Кн. 10: Учеб. пособие для вузов / Общая ред. А. И. Галушкина. - М.: ИПРЖР, 2000. –С.114-129.
9. С.В. Безобразов. Применение искусственных иммунных систем для обнаружения вирусов // Вестник БрГТУ. Физика, математика, информатика.-2005.- №5(35).-С. 66-70.

Материал поступил в редакцию 25.02.08

BEZOBRAZOV S.V., GOLOVKO V.A. Neural network approach for malware classification

Neural network approach for malware classification is described. Malware detection method of artificial immune systems for information security is applied. Malware classification and their harmful activity is present. Classifications system based on collective neural classifier is developed. Research results are submitted.