РАЗДЕЛ I. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НЕЙРОННЫЕ СЕТИ

МЕТОДЫ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ: КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Безобразов С. В.

Брестский государственный технический университет, г. Брест

Введение

С развитием компьютерных наук и компьютерной техники общество столкнулось с проблемой развития киберпреступности. Одним из направлений киберпреступности является создание и распространение вредоносных программ, называемых компьютерными вирусами. На сегодняшний день проблема защиты компьютерных систем от вредоносных программ является одной из основных в области защиты информации. Традиционный подход, основанный на сигнатурном поиске компьютерных вирусов, применяемый для их обнаружения, 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 сотни тысяч компьютеров, 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. Современные исследования в области защиты информации направлены на создание таких систем безопасности, которые были бы способны обнаруживать неизвестные компьютерные вирусы.

Искусственные иммунные системы для защиты информации

Искусственные иммунные системы (ИИС) являются системами, способными обнаруживать неизвестные компьютерные вирусы. 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 [1]. Уникальность БИС является в том, что она способна обнаруживать не только известные вирусы и бактерии, но и неизвестные. Иммунитет основан на способности лимфоцитов распознавать собственные клетки организма от чужеродных клеток. БИС имеют ряд мощных вычислительных возможностей: распознавание, разнообразие, обучение, память, распределенный поиск, саморегуляция, децентрализация, вероятностное обнаружение.

Построенная по основным принципам БИС искусственная иммунная система обладает всеми ее возможностями и, на наш взгляд, является перспективной для построения современной системы компьютерной безопасности. 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. Взаимодействие процессов изображено на рисунке 1.

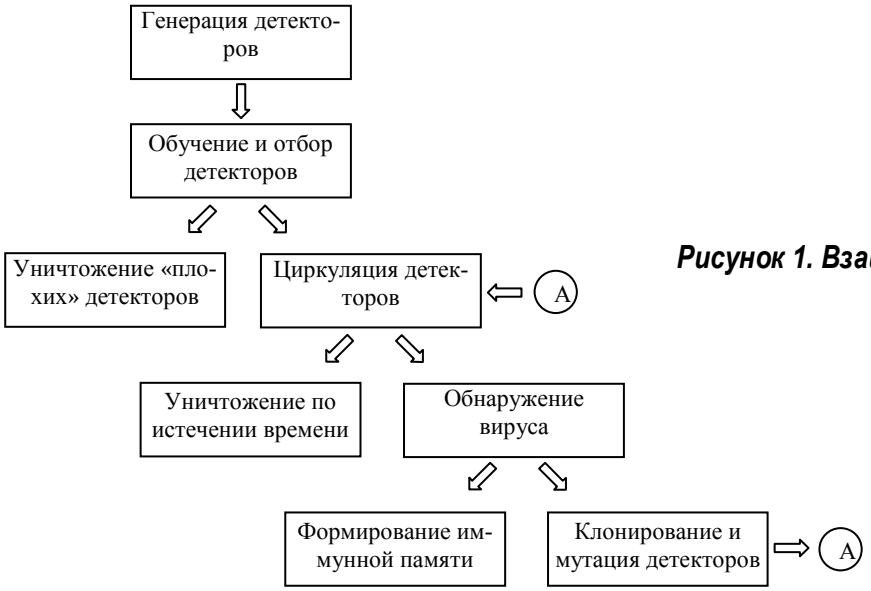

Рисунок 1. Взаимодействие процессов ИИС

Рассмотрим подробней каждый из перечисленных процессов.

Процесс генерации детекторов предназначен для создания иммунных детекторов, которые выполняют функцию обнаружения вредоносных программ. Первоначально детекторы не способны отличать чистые файлы от вредоносных программ. На стадии обучения детекторы обучаются распознавать зловредные программы и не реагировать на чистые файлы. В качестве детекторов мы использовали искусственные нейронные сети, а именно - LVQ сети [2]. На стадии генерации формируется определенное количество детекторов, каждый из которых представляет отдельную нейронную сеть. Структура иммунного детектора, основанного на LVQ, изображена на рисунке 2. На стадии обучения созданные нейронные сети проходят обучение. Для обучения выбирались разнообразные чистые файлы и компьютерные вирусы [3]. Использование разных файлов в процессе обучения позволяет создавать разнообразные иммунные детекторы.

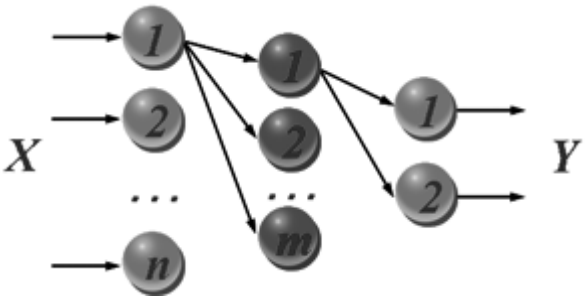

Рисунок 2. Применение LVQ для формирования детектора

После стадии обучения, детекторы проходят стадию отбора. Механизм отбора необходим для предотвращения попадания в компьютерную систему нежелательных детекторов, т.е. тех детекторов, которые реагируют на чистые файлы.

Обученные детекторы циркулируют в компьютерной системе, проверяя и классифицируя файлы. Каждому детектору отводится определенное время, на протяжении которого он может находиться в системе. После истечения выделенного времени детектор, который не произвел обнаружение, уничтожается, а на его место приходит новый. Такой механизм помогает избавиться от слабых детекторов.

При обнаружении вредоносной программы происходит процесс клонирования. Клонирование подразумевает создание большого количества однотипных детекторов (клонируется тот детектор, который обнаружил компьютерный вирус). Процесс клонирования позволяет иммунной системе в кратчайшие сроки избавиться от всех проявлений компьютерного вируса.

Наиболее приспособленный к обнаруженному вирусу детектор трансформируется в детектор иммунной памяти. Иммунная память хранит информацию обо всех вирусах, которые в прошлом заражали компьютерную систему, и предотвращает ее повторное заражение.

Классификация компьютерных вирусов

На сегодняшний день существует большое количество разнообразных зловредных программ, и хотя в настоящее время не существует единой системы классификации вирусов, всех их можно разделить по характерным признакам заражения и распространения на несколько групп. Существует следующая общепринятая классификация компьютерных вирусов: сетевые черви, классические компьютерные вирусы, троянские программы, хакерские утилиты. Компьютерные вирусы, принадлежащие к разным группам, используют различные алгоритмы заражения, различные вредоносные функции, различные предназначения. Зная, к какой категории принадлежит обнаруженная вредоносная программа, можно сделать выводы о пути проникновения ее в компьютерную систему и о тех вредоносных действиях, которые выполняет компьютерный вирус. Такая информация позволит принять оперативные действия по редотвращению утечки и разрушению информации.

Нами была предложена система классификации обнаруженного, с помощью искусственной иммунной системы, неизвестного компьютерного вируса. В качестве классификатора была использована искусственная нейронная сеть (LVQ) – отдельная нейронная сеть на отдельный тип вредоносной программы. Каждая нейронная сеть обучалась на своем типе вирусов, и при поступлении неизвестного образа на вход нейронной сети она соотносила его с эталонным вектором и выдавала решение о принадлежности его к классу [4]. Классификатор вредоносной программы изображен на рисунке 3.

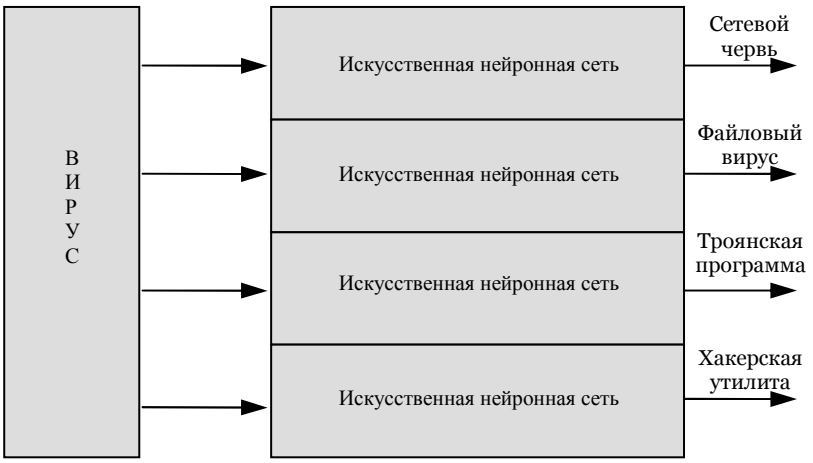

Рисунок 3. Классификация обнаруженного вируса

Выводы

Разработана система классификации обнаруженных при помощи искусственной иммунной системы компьютерных вирусов. Разработанная система позволяет получить общие сведения об обнаруженной зловредной программе и принять оперативные действия для предотвращения утечки и уничтожения информации.

Литература

1. Иммунитет. Энциклопедия «Кругосвет» – http://krugosvet.ru, 2004.
2. Kohonen T. Sell-organised formation of topologically correct feature maps// Biological Cybernetics. - 1982. - N43.-P.59-69.
3. С.В. Безобразов, В.А. Головко. Нейросетевой подход для формирования детекторов в искусственных иммунных системах для защиты информации // Вестник БрГТУ. Физика, математика, информатика.-2006.- №6
4. 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.