В.А.ВИШНЯКОВ[1], М.Г.МОЗДУРАНИ ШИРАЗ[2]

МОДЕЛЬ И АЛГОРИТМЫ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ В ОБЛАЧНОЙ СРЕДЕ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

[1]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь

[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

В докладе представлена концепция интнегрированной КИС с использованнием облачных вычислений (ОВ). Проанализированы основные проблемы информационной безопасности (ИБ) при использовании ОВ, механизмы защиты информации с использоваием нейроных сетей [1]. Наиболее распространенной нейросетевой структурой, используемой для решения задач защиты информации,

является многослойный персептрон. Построена обучающая выборка для многослойного персептрона, определяющего, заражена ли данная программа (ее исполняемый файл) вирусом или нет. В ходе работы было проведено обучение данной нейросетевой структуры при помощи специально построенной выборки исполняемых файлов двух состояний: чистых и зараженных вирусами. Обучение проводилось в SPSS Statistics – программе, произведенной компанией IBM. Для обучения многослойного персептрона данные обучающей выборки приведены к десятичному представлению. Для автоматизации решения данной задачи на языке JavaScript был написан конвертер чисел между различными системами счисления [2].

Представлена модель конфигурации многослойного персептрона для определения состояний исполняемых файлов. Bias – это величина, называемая смещением и позволяющая управлять уровнем активации нейрона. Сдвигая активационную функцию вправо или влево вдоль горизонтальной оси, с увеличением смещение, повышается порог активации и искусственно вводится некоторое торможение нейрона, а с уменьшением, как бы подталкивается нейрон.

Рассмотрен нейросетевой подход решения задач защиты информации, состоящий в последовательном объединении двух различных нейронных сетей: рециркуляционной нейронной сети и многослойного персептрона, которые соединялись последовательно. На первом этапе обработки входной информации в данной нейросетевой структуре происходит уменьшение размерности входного вектора входных данных при помощи нелинейной рециркуляционной нейронной сети. Это позволяет перейти от исходного пространства данных к вспомогательному, которое характеризуется меньшей размерностью и большей информативностью исходного пространства. Рециркуляционная нейронная сеть позволяет автоматизировать анализ входных параметров, что, безусловно, упрощает процесс построения обучающей выборки. Второй этап состоит в обнаружении и распознавании атак. Для этого используется многослойный персептрон, который осуществляет обработку сжатого пространства входных образов с целью распознавания класса атаки.

Рассмотрены генетические алгоритмы, которые используются при создании искусственной иммунной системы для защиты информации от вредоносных программ. Начальным этапом построения искусственной иммунной системы является генерация иммунных детекторов, в основе которых лежит многослойный персептрон. Пройдя стадии обучения и отбора, детекторы приобретают способность реагировать на вредоносные программы, сканируя их структуру, и, в то же время, игнорировать чистые файлы.

ЛИТЕРАТУРА

1. Intelligence Community Information Technology Enterprise (ICITE) [Электронный ресурс], режим доступа: http://www.insaonline.org/i/d/a/Resources/ ICITE_Doing.aspx (дата доступа 22.09.2017.

2. Вишняков, В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Монография. / В.А. Вишняков. – Минск: , 2016. – 276 с.