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

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ В ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ СИСТЕМЕ УПРАВЛЕНИЯ

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

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

Свойства нечетких нейронных сетей (НС), необходимые для адаптивных средств защиты информации (ЗИ): параллелизм вычислений; адаптивность; возможность классификации угроз; «прозрачность» для анализа структуры; функциональная устойчивость. Направлением в системах защиты информации является использование интеллектуальных средств, работающих в распределенной КИС с облачными вычислениями (ОВ). Предлагается усовершенствовать схему защиты КИС добавлением системы обнаружения зараженных файлов на базе НС и системой обнаружения вторжений, которая дополнит систему защиты возможностью обнаружения и блокирования атак с использованием знаний в виде правил.

Разработана концепция интегрированных КИС (ИКИС), разделенных по технологиям применения ОВ: малые − на базе SaaS, средние − IaaS, больши е на базе PaaS. Создавая инструментальные платформы бизнес-процессов в ИКИС, корпорации могут приобрести возможности для инноваций, повышения производительности и удовлетворения спроса, предъявляемого рынками.

Представлена модель 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 торможение нейрона, а с уменьшением, как бы подталкивается нейрон [2].

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 [2].

Исследована эффективность работы нейронной сети с помощью контрольной выборки исполняемых файлов после ее обучения. Относительная погрешность классификации файлов составила 5 %, однако следует отметить, что при обучении данной нейронной сети использовалась относительно небольшая выборка исполняемых файлов; для использования же нейронной сети при решении реальных задач защиты информации, например, во внутрикорпоративных системах, выборка файлов должна быть больше [2].

С целью повышения надёжности защиты информации в корпоративной сети предприятия была разработана и внедрена система обнаружения вторжений на базе СОВ Snort. Для осуществления поставленной цели в ходе работы были выполнены задачи: смоделирована виртуальная компьютерная сеть; проанализированы возможные ее уязвимости; настроена и подготовлена к работе система обнаружения вторжений в данную виртуальную сеть (использованы знания в виде правил); произведена проверка работоспособности СОВ путем моделирования различных атак и зондирований сети. Смоделированная СОВ может использоваться для обеспечения защиты информации и контроля данных в КИС для малых и средних предприятий, имеющих в своём составе локальную вычислительную сеть. [2].

ЛИТЕРАТУРА

1. 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.

2. Вишняков, В.А. Модели обнаружения атак с использованием интеллектуальных технологий / В.А. Вишняков, М. Г. Моздурани Шираз. – Доклады БГУИР, № 8, 2017. – С. 76-81.