СОЗДАНИЕ ПОДСИСТЕМЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВИРУСНЫХ АТАК

Романов А.Н. ИУС-06м
e-mail: romanov.andrey.nickolaevich@googlemail.com
Руководитель доцент Меркулова Е.В.

Сеть Интернет представляет собой одновременно объект и средство IT-преступлений. Самым распространенным видом этих преступлений является незаконное копирование информации. С точки зрения противодействия IT-преступлениям такого вида, информационная безопасность сети Internet является актуальной проблемой.

Объект исследования – автоматические системы проектирования защиты информации. Предметом исследования являются алгоритмы проактивной защиты.

Суть технологии проактивной защиты в том, что анализу подвергаются не алгоритмы копирования и удаления информации, а вредоносные действия.

В качестве защищаемой в работе была выбрана информационная аналитическая система для построения трёхмерных моделей залегания угольных пластов, а так же построение трёхмерных моделей сети горных выработок[1]. Работа информационной аналитической системы это сложный математический процесс, сопровождающийся изменением массива данных в которых содержаться расчеты. Информация о промежуточных расчетах находится в файлах и значимость этой информации а следовательно и важность файлов где хранится данная информация приобретают высокую ценность. Именно по этому предъявляются высокие требования безопасности доступа к этим файлам. Структура создаваемой подсистемы защиты

аналитической системы изображена на рисунке 1.

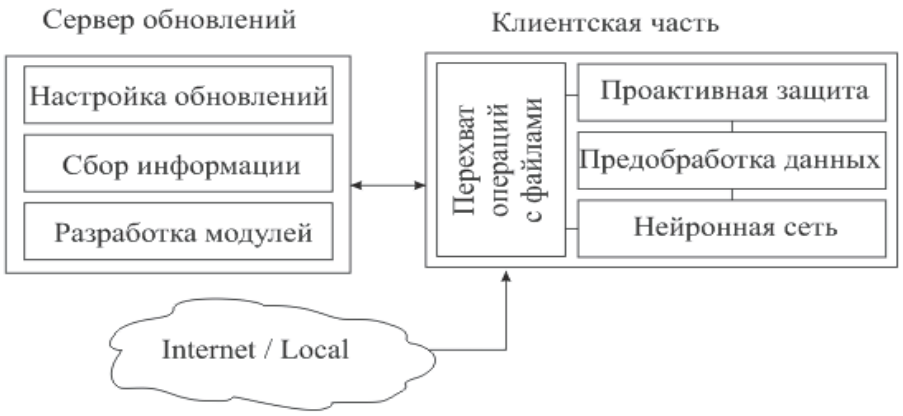

Рисунок 1 - Структура подсистемы защиты

Клиентская часть подсистемы безопасности состоит из ядра и набора модулей, выполняющих перехват операций с файлами. Разработанное ядро спроектировано таким образом, чтобы обновление модулей не влияло на работу ядра и других модулей. Мгновенная выгрузка и загрузка модулей в оперативную память происходит в моменты времени, когда подсистема безопасности бездействует.

Серверная часть подсистемы безопасности состоит из ядра, набора утилит необходимых для работы сервера и конструктора модулей для клиентской части. Для передачи пакетов от сервера к клиентам и наоборот используется сетевой протокол - набор правил для специфического типа связи.

Задачу защиты информации можно представить как совокупность ряда подзадач:

- выделение защищаемых файлов;

- отслеживание обращения к файлам;

- анализ совокупности действий обращения;

- сопоставление анализа и политики безопасности.

Данного рода задачи решаются с использованием превентивных методов защиты информации. Превентивных методов обнаружения существует достаточно много и в работе рассмотрено два самых перспективных из них:

- поведенческий блокиратор;

- эвристический анализатор.

Эвристическим анализатором называется набор методов, которые анализируют код исполняемых файлов. Однако для эвристических анализаторов с высоким уровнем обнаружения характерен высокий уровень ложных срабатываний[2].

Основная идея поведенческого блокиратора - это анализ поведения и блокировка выполнения любых опасных действий и последовательности действий. Теоретически поведенческий блокиратор может предотвратить распространение любого, как известного, так и неизвестного вируса[2].

В обоих рассмотренных превентивных методах есть два общих и весомых недостатка:

- высокий процент ложных обнаружений;

- отсутствие экспертных решений.

В данных методах результатом отсутствия экспертных решений является высокий процент ложных обнаружений. В качестве альтернативы базы знаний для экспертной системы в работе предложено применить искусственную нейронную сеть, которая будет интеллектуальным недостающим звеном. Однако требуется выбрать метод обучения нейронной сети.

При выборе метода обучения искусственной нейронной сети необходимо учитывать особенность самой системы безопасности и анализируемых данных. В работе выбран метод обучения без учителя, который самостоятелен, что является подходящим для решения поставленной задачи. Обучение без учителя является более правдоподобной

моделью обучения в биологической системе. Процесс обучения заключается в подстраивании весов синапсов. Сеть не нуждается в целевом векторе для выходов и, следовательно, не требует сравнения с предопределенными идеальными ответами. Обучающее множество состоит только из входных векторов. Обучающий алгоритм подстраивает веса сети так, чтобы получались согласованные выходные векторы, т. е. чтобы предъявление достаточно близких входных векторов давало одинаковые выходы. Сигнальный метод обучения Хебба заключается в изменение весов по правилу:

(1)

Дифференциальный метод обучения Хебба:

(2)

Неполный укрупненный алгоритм обучения Хебба с применением формул (1) и (2):

Шаг 1. На стадии инициализации всем весовым коэффициентам присваиваются небольшие случайные значения;

Шаг 2. На входы сети подается входной образ, и сигналы возбуждения распространяются по всем слоям согласно принципам классических прямопоточных сетей, то есть для каждого нейрона рассчитывается взвешенная сумма его входов, к которой затем применяется передаточная функция нейрона, в результате чего получается его выходное значение;

Шаг 3. На основании полученных выходных значений нейронов по формуле (1) или (2) производится изменение весовых коэффициентов;

Шаг 4. До тех пор пока выходные значения сети не застабилизируются с заданной точностью происходит повторение. Применение этого нового способа определения завершения обучения, отличного от использовавшегося для сети обратного распространения,

обусловлено тем, что подстраиваемые значения синапсов фактически не ограничены[3].

Отдельным этапом является подготовка входных данных для искусственной нейронной сети. Для предобработки данных разработан алгоритм, укрупненный вид которого можно представить следующим образом:

Шаг 1. Получение уравнений в зависимости от времени. Процесс получения новых данных в защищаемой компьютерной системе строго определенный и выполняется линейно по шагам. В один момент времени могут быть изменены только одни данные;

Шаг 2. Проводится нумерация защищаемых файлов с учетом расстояний по Хеммингу. Именно эти номера в бинарном виде формируют вектор входных значений;

Шаг 3. Строятся временные диаграммы с учетом изменений защищаемых объектов (см. рисунок 2). На рисунке 2 по оси ординат идут номера файлов, а по оси абсцисс время.

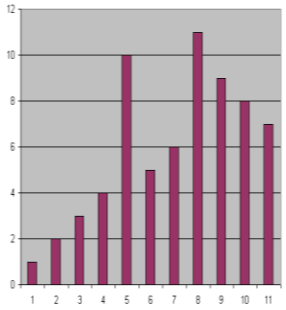

Рисунок 2 – Гистограмма изменения файлов во времени

На вход искусственной нейронной сети подается вектор, состоящий из номеров файлов. Номера файлов следуют в той же последовательности, как и происходило обращение к ним.

На выходе искусственной нейронной сети получается числовое значение, находящееся в строго определенном диапазоне (0; 1). Предполагается, что количество значений ограничится двумя. Первое – разрешение доступа, второе – запрет доступа к файлам.

Для использования в задаче защиты информации предлагается использовать:

- в качестве превентивного метода - поведенческий блокиратор;
- искусственную нейронную сеть с обучением без учителя;
- для обучения нейронной сети метод Хебба.

Рассмотрены и аргументированы выбранные методы, используемые при решении поставленной задачи. В статье рассмотрена структура разработанной подсистемы информационной безопасности.

Перечень ссылок

1. Пилюгин В.И., Збощик М.П., Кочин А.Е., Романов А.Н., Комплекс мер по прогнозированию месторасположений аномальных зон тектонического происхождения при отработке пологих угольных пластов Донбасса. – Донецк: ДонНТУ, 2007.-20с.

2. Никишин А., Проактивная защита как она есть

Способ доступа URL: www.viruslist.com/ru/downloads/vlpdfs/wp_nikishin_proactive_ru.pdf

3. Короткий С., Нейронные сети

Способ доступа URL: lii.newmail.ru/NN/KOROTKY/N3/kor_nn3.htm