В работе приводятся результаты исследования, связанные с цифровой обработкой и распознаванием по изображению кровеносных сосудов глазного дна на основе статистического подхода и энтропийного кодирования. Для этого рассчитывались статистические характеристики изображения сети кровеносных сосудов. Сеть представлялась рядом цифровых последовательностей с числом точек (отсчетов), количество которых определялось размером обрабатываемого фрагмента или длиной линии, описывающей кровеносный сосуд. Определенная степень линейной зависимости между совокупностями данных, описывающих сеть, и применение в качестве дескрипторов распознавания коэффициентов разложения по базису собственных функций позволила уменьшить размерность области распознавания. Фильтрация значений дескрипторов осуществлялась на основе дисперсионного критерия [1]. Такая процедура выбора признаков распознавания позволила упростить процесс правильной классификации, измерения сходства биометрических образцов.

Литература

1. Мультиспектральное наблюдение / А.И. Митюхин // Технические средства защиты информации материалы XI Белорусско-российской науч.-техн. конф. Минск, 4–5 июня 2013 г. – С. 44–45.

ПОДДЕРЖКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

М.Г. Моздурани Шираз, В.А. Вишняков

Наиболее распространенной нейросетевой структурой, используемой для решения задач защиты информации, является многослойный персептрон. Построена обучающая выборка для многослойного персептрона, определяющего, содержит ли данная программа (ее исполняемый файл) вредоносный код или нет. В ходе работы было проведено обучение данной нейросетевой структуры при помощи специально построенной выборки исполняемых файлов двух состояний: «отсутствие вредоносного кода» и «наличие вредоносного кода». 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.

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, и вредоносные коды, которые внедряются в часть файлов из выборки, должны быть более разнообразными.

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС НА БАЗЕ СОВ И МСЭ

М.Г. Моздурани Шираз, В.А. Вишняков

Представлено два подхода к реализации системы предотвращения вторжений: первые при выявлении атаки реконфигурируют активное сетевое оборудование (например, Snort SAM); вторые при выявлении атаки принимают решения, на основе правил, о дальнейшем действии с пакета (например, Snort inline). Недостатком первого подхода является то, что на создание правила, передачу его межсетевому экрану, реконфигурирование самого межсетевого экрана уходит время. Система Snort_inline при обнаружении следов атаки в пакете сама уничтожает пакет, что эффективней первого решения.

Представлена структура защищаемой сети. Сервер работает под управлением Slackware Linux 10.2 с ядром версии 2.4.31. Данная версия ядра является наиболее исследованной, стабильной и содержит минимальное число обнаруживаемых уязвимостей. Сервер защищен с помощью межсетевого экрана IPTables (v1.3.3).

В результате объединения IDS Snort и МСЭ IPTables получается двухуровневая система защиты: на первом уровне iptables проверяет входящий пакет на соответствие своим правилам фильтрации, если пакет получил разрешение на прохождение через межсетевой экран, его проверяет система обнаружения вторжений на наличие вредоносного кода в теле входящего пакета. Представлен скрипт конфигурирующий Snort_inline и IPTables для совместной работы.

ОБ ОДНОЙ МОДИФИКАЦИИ АЛГОРИТМА XOR

И.В. Молчанов, М.А. Калугина

Обратимость логической операции исключающего ИЛИ позволила успешно использовать ее в синхронном шифровании. Однако основанный на ней классический алгоритм XOR рекомендуется применять лишь однократно из-за его уязвимости к криптоанализу при достаточно большом количестве перехваченных зашифрованных данных.

Реализованный в утилите для Windows алгоритм на основе простого XOR предназначен для приложений, использующих уникальный ключ для шифрования каждого конкретного блока информации. Он состоит из шифрования данных простым алгоритмом XOR и добавления «шума» с использованием специальной рекуррентной последовательности псевдослучайных чисел. Эта последовательность формируется заранее по следующей схеме: $a_0=A$, $a_1=B$, $a_{i+1}=\alpha \bullet a_{i-1}+ \beta \bullet a_i$, − где A, B, α, β – псевдослучайные числа, которые вычисляются до исполнения.

Ключ генерируется как последовательность псевдослучайных байтов или как ключевая фраза, задаваемая пользователем (данная реализация включает псевдослучайный ключ на основе вычисления количества байтов в шифруемом файле). Частью ключа являются значения A, B, α, β.

Шифрование. Пусть M , K , E – массивы символов (байтов) в файле ввода, в ключе и в файле вывода соответственно. Тогда $E_i = M_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, $E_i = T$ – псевдослучайный символ, если совпадает. Расшифровка. Пусть E, K, M – массивы символов (байтов) в файле ввода (зашифрованная информация), в ключе и в файле вывода соответственно. Тогда $M_i = E_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, E_i игнорируется, если совпадает.

Таким образом, попытка узнать длину ключа путем циклического сдвига (первый шаг по взлому XOR) не осуществима из-за разных дистанций между a_i и a_{i+1}. Кроме того, при разработке утилиты особое внимание было уделено не только реализации данного алгоритма, но и распространению такого подхода на асинхронный алгоритм шифрования.

ИСПОЛЬЗОВАНИЕ КОДОВ ХЭММИНГА ДЛЯ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБОК В DWDM СЕТЯХ

Б.А. Монич

В системах оптических магистралей, которые работают на терабитных и мультигигабитных скоростях, используется уплотненного волнового мультиплексирования (DWDM). Алгоритм обнаружения и исправления ошибок методом кодов Хэмминга на DWDM транспортной системы Optix OSN 8800 компании Huawei был впервые опробован на одном из 10G каналов. В Республике Беларусь данная транспортная система также является частью сети передачи данных. Функции выявления ошибок реализуются на транспортировке в составе блока избыточной служебной информации, по которой смотрят степень достоверности принятой информации.

Для обнаружения ошибок разработаны и применяются различные алгоритмы. Среди них основными являются следующие.

1. Контроль по паритету. Представляет собой наиболее простой метод контроля данных. Метод заключается в суммировании по модулю 2 всех бит контролируемой информации. Существуют горизонтальный и вертикальный контроль по паритету.

2. Циклический избыточный контроль. Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. В качестве контрольной информации рассматривается остаток от деления этого числа на известный делитель R.