программных системах, установленных на компьютере, а также вычисляет три характеристики производительности системы.

С помощью утилиты msinfo32.exe — сведения о системе.

Используемый нами метод привязки программного обеспечения пользователя к характеристикам персонального компьютера работает следующим образом:

Программный продукт:

1) анализирует параметры оборудования;

2) анализирует лицензионную информацию;

3) при несоответствии принимает меры ограничения (программа не запускается).

Модуль-регистратор:

1) анализирует параметры оборудования;

2) генерирует регистрационный ключ;

3) передает ключ пользователю продукта.

Простая реализация метода защиты программного обеспечения привязкой к параметрам персонального компьютера [2] сводит анализ лицензионной информации, сгенерированной модулем-регистратором к ее сравнению с необходимой, полученной в результате анализа параметров реального оборудования программным продуктом. Нейтрализация защиты в данном случае сводится к поиску и замене инструкции сравнения на безусловный переход.

Надежность защиты может быть увеличена путем использования криптозащиты. Шифрование должно применяться совместно с защитой от статического и динамического анализа кода программы и «изощренным программированием», т.е. стилем, позволяющим получить сложный и запутанный исполняемый модуль [3].

В программных и аппаратно-программных методах основанных на привязке защищаемого программного обеспечения к его непосредственному носителю возникает дополнительная задача. Эта задача заключается в сокрытие от злоумышленника алгоритмов защищенного программного обеспечения, в которых реализована проверка наличия объекта привязки. Для сокрытия алгоритмов получили распространение следующие методы:

1) метод запутывания;

2) метод виртуального процессора;

3) метод мусора.

Литература

1. *Шалатонин И.А., Коваленко П.П.* Международный конгресс по информатике: информационные системы и технологии: материалы международного научного конгресса 31 окт. – 3 нояб. 2011 г. : в 2 ч. Ч. 2. Минск: БГУ, 2011. С. 146–150.

2. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. М., 2005.

3. *Абашеев А.А., Жуков И.Ю., Иванов М.А. и др.* Ассемблер в задачах защиты информации. М., 2004.

МЕТОД БЛОЧНОГО МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ СИНУСОИДАЛЬНЫХ РЕШЕТОК

А.А. БОРИСКЕВИЧ, Ю.А. КОЧЕТКОВ

Традиционные двумерные штрих-коды (QR-коды) не несут визуальной информации и ограничены по информационной емкости.

В связи с этим предложен метод блочного маркирования изображений и оптоэлектронного извлечения сообщения, основанный на внесение избыточности в информационное бинарное сообщение и его зашифровании, генерации двумерных синусоидальных решеток с различными идентификационными параметрами (частота, ориентация, размер) для кодирования информационного сообщения, перцептуальном гибридном внедрении маркирующей синусоидальной маски, формирование контура обнаружения маркируемого изображения, обнаружение контура для оптического захвата

изображения, эффективной пространственной обработки маркированного изображения, декодировании сообщения с использованием параметров внедренных решеток, расшифровке сообщения и коррекции ошибок, возникающих в процессе оптического считывания. Данный алгоритм позволяет формировать устойчивые кодовые образы, несущие как визуальную, так и скрытую информацию, воспринимаемую мобильными телефонами с экрана монитора и печатной продукции.

Результаты моделирования показывают, что данный алгоритм обеспечивает высокое субъективное и объективное качество маркированного изображения (PSPNR и WPSNR>29 дБ), высокую точность декодирования решеток и значительное увеличение емкости внедрения по сравнению с QR-кодами.

АЛГОРИТМ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ НА ОСНОВЕ ВЕЙВЛЕТ-АНАЛИЗА

Л.А. РУИС, М.А. МЛАГИ, А.А. БОРИСКЕВИЧ

В качестве альтернативы традиционному подходу обнаружения аномалий сетевого поведения использование современных методов обработки сигналов позволит эффективно проводить анализ сетевого трафика с целью выявления новых или неизвестных вторжений. Технологии обнаружения вторжений делятся на две категории: обнаружение злоупотреблений и обнаружения аномалий. Подходы обнаружения злоупотреблений ограничиваются известными атаками, поэтому выявления новых атак или вариантов известных атак является одной из трудных проблем, с которыми сталкиваются методы обнаружения злоупотреблений.

В связи с этим целью работы является разработка эффективного алгоритма обнаружения сетевых аномалий, основанный на использовании современной технологии вейвлет-анализа, аппроксимационной авторегрессионной модели и технологии обнаружения выбросов.

Моделирование нормального сетевого трафика состоит из следующих двух этапов: вейвлет-декомпозиции и генерации авторегрессионной модели. Исходный сигнал сетевого трафика преобразуется в множество аппроксимационных вейвлет-коэффициентов, которые используются для построения модели предсказания нормального трафика сети. Данная модель используется для формирования сигнала состояния сетевого поведения, идентификации пиков которого осуществляется с помощью алгоритма обнаружения выбросов, и принятия решения о типе вторжений. Для реализации вейвлет-анализа сетевого трафика были использованы следующие базисные вейвлет-функции: Haar, Bior5.3, Bior9.7, Coiflet и Symlet. Установлено что, вейвлет-функция Haar является наилучшей по критерию быстродействия и точности обнаружения различных сетевых атак при использовании базы пакетов сетевых трафиков 1999 DARPA.

АЛГОРИТМ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ ГЛАВНЫХ КОМПОНЕНТ И ОПОРНЫХ ВЕКТОРОВ

К.В. ГОНСАЛЕС, Л.А. РУИС, А.А. БОРИСКЕВИЧ

Информационные технологии обрабатывают огромный объем трафика информации, что требует ускорение процессов обработки для оперативности и управления доступа к информации и услугам. В этом случае ускорение управления доступа состоит в уменьшении объема обрабатываемого трафика на основе определения главных компонент множества пакетов данных, что позволит применить эффективный метод идентификации с использованием классификаторов, основанных на опорных векторах пониженной размерности.