рецептов, рекомендаций по выбору, анализу и разделению объектов, относящихся к АПС, на множества по единственному критерию «принадлежит — не принадлежит». Несмотря на кажущуюся простоту критерия, задача разработки алгоритма для таких систем достаточно трудоемкая и сложная. Для решения этой задачи разработана модель обеспечения безопасности эксплуатации АПС, с помощью которой алгоритм и разрабатывался эвристическими методами с выполнением рутинных работ, связанных с перебором вариантов, с использованием стандартного программного обеспечения.

С. Д. Жилкин

ВЫЯВЛЕНИЕ АНОМАЛИЙ РАБОТЫ ПО С ПОМОЩЬЮ МОДЕЛЕЙ ПОВЕДЕНИЯ

Предпосылкой к ведению работ в данном направлении является сложившаяся ситуация в сфере информационной безопасности. На данный момент существует множество программных средств, препятствующих выполнению вредоносного кода. Однако куда меньшее внимание уделено проблеме выявления и локализации недекларированных возможностей (НДВ) ПО, проявляющихся при различных предпосылках и вызывающих аномальное поведение. Так, некоторое ПО может начать вести себя необычным образом вследствие определенной последовательности действий. При этом программный код, провоцирующий такое поведение, сам по себе может не являться вредоносным. В данной работе решается задача выявления заранее неизвестных атак.

Одним из подходов выявления компьютерной атаки, не базирующихся на экспертных знаниях о том, как эта атака совершается, является мониторинг и анализ состояния узлов и серверов информационной системы с целью выявления отклонений от некоторого так называемого штатного, или эталонного, состояния [1, 2].

О поведении приложения можно судить по его взаимодействию с операционной системой: обращение к жесткому диску, сетевым ресурсам, вызовы функций драйверов, работа с реестром и прочее. Для того чтобы получать информацию такого рода о поведении ПО, требуется дополнительная система мониторинга. Она может основываться на журнальных файлах операционной системы (система мониторинга верхнего уровня) или, например, на более подробных данных, полученных на уровне драйверов ОС (системы мониторинга низкого уровня), как проиллюстрировано на рис. 1. При реализации методов моделирования ПО, приведенных в данной работе, для сбора информации о поведении ПО использовалась система «Инсайдер» компании «Праймтек». С помощью модулей конвертации можно осуществить поддержку других систем мониторинга. Таким образом, на основании данных от системы мониторинга возможно создание моделей поведения, описывающих штатную работу контролируемого ПО.

Так как при построении модели и анализе используется математический аппарат, необходимо описывать поведение ПО некоторым набором числовых значений — вектором координат. Предлагается описывать поведение процесса количественными, логическими и статистическими характеристиками. Количественные характеристики могут включать в себя такие параметры, как число обращений к системным файлам, библиотекам и прочим ресурсам системы. Логические характеристики описывают общее поведение ПО: создавались ли сетевые соединения, порождались ли дополнительные процессы и прочее. Статистические характеристики могут показывать частоту выделения дополнительной памяти, обращений к жесткому диску и другие частотные параметры. Чем более подробной будет информация о взаимодействии процесса с операционной системой,

тем более развернутым будет вектор, описывающий поведение ПО, и тем более точными будут результаты моделирования и анализа.

В рамках данной работы разработаны три типа модели поведения: общая, точная и нейронная. Продемонстрированы преимущества и недостатки, а также показана область применения каждой модели. Представлены результаты выявления НДВ различного уровня сложности, заложенных в тестовый набор прикладного ПО с открытым кодом.

СПИСОК ЛИТЕРАТУРЫ:

1. *Марков А. С., Миронов С. В., Цирлов В. Л.* Выявление уязвимостей в программном коде // Открытые системы. М., 2005. № 12.
2. Круглый стол «Вестника Связи» // Вестник Связи. 2006. № 12. С. 4–18.

В. Г. Иваненко, С. В. Родченко

ВСТРАИВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АУДИОСИГНАЛЫ

В связи с бурным распространением сети Интернет весьма важной становится проблема защиты авторских прав на аудиоданные. Любой человек может разместить любые аудиофайлы в Сети, предварительно заявив, что он имеет права на них и является законным владельцем данной аудиопродукции. Для защиты соответствующих авторских прав возможно использование цифровой стеганографии, в частности технологии цифровых водяных знаков [1].

Цифровой водяной знак (ЦВЗ) — это специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контроля его распространения. При этом ЦВЗ, содержащий информацию о законном владельце и правообладателе, встраивается в защищаемый аудиофайл для осуществления возможности проверки авторства, закрепленного за ним. Сама встроенная информация изменяет параметры аудиофайла незначительно (эти изменения «невидимы» для слушателя, что является важнейшей особенностью алгоритма встраивания), и при этом данная информация встраивается таким образом, чтобы злоумышленнику было трудно ее извлечь или разрушить, значительно не повредив при этом сам контейнер. Целевое же извлечение встроенной информации не представляет серьезных сложностей, поскольку другой стороне известны параметры встраивания.

Существует пять основных методов встраивания информации в аудиосигналы: методы кодирования наименее значащих бит, методы фазового кодирования, методы расширения спектра, методы маскирования цифровых водяных знаков, методы встраивания информации с использованием эхо-сигнала [2].

Методы кодирования наименее значащих бит по сравнению с другими перечисленными методами имеют худшие показатели стойкости для встраиваемых ЦВЗ.

В методах фазового кодирования, в зависимости от внедряемых данных, происходят модификация фазы начального сегмента аудиосигнала и согласование с ним фазы последующих сегментов для сохранения разности фаз. ЦВЗ, встроенный посредством данного метода, лишь частично переживает двойное цифро-аналоговое и аналого-цифровое преобразование. Возникают проблемы извлечения после перестановки сэмплов в аудиосигнале. Метод имеет достаточно хороший показатель невидимости встроенного ЦВЗ.