

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.