

в применении прикладного TCP/IP сервера для управления набором правил пакетного фильтра (в GNU/Linux используется iptables) на маршрутизаторах. Для запуска приложения TCP/IP сервера при появлении трафика на детерминированных портах предлагается использовать суперсервер xinetd (extended Internet daemon). Метод позволяет централизованно и быстро вносить изменения в правила пакетных фильтров на все маршрутизаторы в сети. Использование распределенного межсетевых экранов обеспечивает низкую уязвимость к DoS-атакам, отсутствие единой точки отказа, высокую пропускную способность сети и делает возможным применение локальных и глобальных политик.

АНАЛИЗ БОРТОВЫХ СИСТЕМ ВИДЕОФИКСАЦИИ ДЛЯ ОХРАНЫ РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А.А. ЖУРАВЛЕВ, В.Ю. ЦВЕТКОВ

Произведен анализ существующих систем видеofиксации, предназначенных для беспилотных летательных аппаратов (БПЛА) и обеспечивающих мониторинг территорий и распределенных объектов с целью выявления незаконной деятельности вблизи критически важных объектов. Выявлены основные параметры систем видеofиксации, определяющие выбор метода эффективного кодирования для сжатия видеоданных, фиксируемых на борту БПЛА. Установлено, что при выборе метода видеокodирования необходимо учитывать угол наклона камеры, абберации оптической системы, а также разрешающую способность матрицы видеокamеры. Последний параметр особенно важен, так как определяет качество воспроизведения видеоданных после декодирования. Увеличение размера матрицы позволяет повысить качество воспроизведения видеоданных, но только при увеличении скорости передачи. Если полоса канала ограничена, увеличение размера матрицы ведет к необходимости повышения коэффициента сжатия видеоданных, что вызывает снижение качества их воспроизведения. С другой стороны, использование оптического увеличения для повышения детальности формируемых на борту БПЛА видеоданных приводит к уменьшению площади перекрытия соседних кадров и снижению эффективности методов сжатия, основанных на блочной компенсации движения.

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

Ю.А. СЕЛИВАНОВА, В.Ю. ЦВЕТКОВ

Проведен анализ защищенности сервисов в коммуникационных системах Microsoft Lync Server 2010, Skype и ooVoo. Установлено, что данные системы используют следующие технологии информационной безопасности. В Microsoft Lync Server 2010 для аутентификации пользователей и серверов используются протоколы TLS и MTLS с криптографическими алгоритмами RSA-RC4-128-SHA. Пользователи локальной сети аутентифицируются средствами протокола Kerberos, а внешние — с использованием TLS-DSK или NTLMv2. SIP-каналы шифруются средствами TLS. Трафик аудио и видео защищается протоколом SRTP с применением AES-128. Трафик веб-конференций шифруется в HTTPS-канале. в Skype для аутентификации пользователей используется протокол TLS, для шифрования и защиты целостности

– AES-256 блочный шифр, криптографические стандарты открытого ключа RSA, ISO 9796-2 система подписи, SHA-1 систему хэширования и RC4 шифрование потока. В ooVoo аутентификация пользователей осуществляется по защищенному каналу TLS (RSA-RC4-128-MD5), аудио и видео трафик передается в открытом виде. Таким образом, Microsoft Lync Server 2010 и Skype используют схожие технологии информационной безопасности и предоставляют более защищенные сервисы по отношению к ooVoo.

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА

Кодовые структуры, обладающие стойкостью к раскрытию, используют как компоненты систем защиты информации. Одним из эффективных средств защиты от ошибок и преднамеренных воздействий является комплексная кодовая защита. Объектом исследования являлись алгебро-геометрические коды Эрмита, мощность которых превосходит аналогичный показатель кодов эллиптических кривых.

Основными критериями, предъявляемыми к разработке и исследованию эффективности криптоалгоритмов, являются такие показатели, как нелинейность преобразований, сбалансированность криптографической функции, линейная сложность шифрующей последовательности. Автокорреляционная функция (АКФ) предоставляет возможность описания критериев безопасности через оценку вероятностных параметров.

Криптографический анализ проведён на примере алгебро-геометрического кода (32, 64), заданного кривой Эрмита в поле GF(16). Оценка АКФ указывает на близость исследуемых последовательностей к случайным. Значения компонент спектра Уолша-Адамара эквивалентных сопряжённых последовательностей кодированных векторов отражают уровень нелинейности (от 106 до 104 при верхней границе 120), что указывает на высокую степень удалённости последовательностей от линейных, а значит, высокую степень устойчивости к линейному криптоанализу. Значения нулевых компонент спектров имеют отклонения от нуля, что указывает на определенную несбалансированность структуры кода. Уровень линейной сложности шифрующих последовательностей оценён с помощью алгоритма Берлекемпа-Мессис и составляет от 120 до 124, т.е. криптосистемы, использующие подобные последовательности, устойчивы к вскрытию, и криптоаналитик не может предсказать ни следующий, ни предыдущий бит последовательности.

МОНИТОРИНГ СИСТЕМЫ БЕЗОПАСНОСТИ СЕТИ 2G/3G (UMTS)

Д.Н. ПИСКУН

Системы связи UMTS требуют осуществления глобального роуминга, высокой скорости передачи информации и оказания электронных услуг различного вида. Все эти функции должны быть поддержаны системой защиты информации, одной из опций которой является анализ состояний мобильных станций и сетевой структуры.

Целью данной работы является разработка моделей и алгоритмов анализа состояния системы связи в режиме мониторинга зон покрытия, а также написание программного обеспечения системы защиты информации.