Архитектура системы безопасности сетей связи 3G (UMTS) представляет собой многоуровневую структуру. Одной из неотъемлемых функций архитектуры является поддержка требований по наблюдаемости и конфигурируемости системы защиты информации на основе анализа состояний мобильный станций, оконечных мобильных устройств, каналов передачи, сетевой инфраструктуры. Априорное знание этих состояний, в сочетании с точными географическими параметрами (широта, высота, долгота), позволяют оценить степень конфиденциальности и произвести оценку целостности всей инфраструктуры сети. Перспективным инструментом анализа в этом отношении являются методы основанные на фрактальных вейвлетных моделях.

В данной работе предполагается использование программно-аппаратного комплекса базирующегося на высокотехнологичном радиоизмерительном оборудовании — модульной измерительной системе компании National Instruments, основанной на открытом промышленном стандарте PXI. для использования своих модульных измерительных систем, компания National Instruments предлагает использовать среду графического программирования NI LabVIEW. в состав NI LabVIEW входят специализированные модули для имитации и записи реального сигнала UMTS и измерения различных технических параметров сигнала.

КОДОВАЯ КОРРЕКЦИЯ СМЕЩЕНИЯ В ГЕНЕРАТОРАХ СЛУЧАЙНЫХ ЧИСЕЛ

С.Б. САЛОМАТИН, Т.А. АНДРИАНОВА

Основными элементами в инфраструктуре формирования ключевого пространства является генераторы случайных чисел. Одним из недостатков генераторов такого рода является возможность появления постоянного смещения e в распределениях случайных последовательностей чисел.

Для предотвращения появления смещения можно использовать метод кодовой коррекции работы генератора случайных чисел. Суть метода состоит в дополнительном кодировании данных, формируемых генератором случайных чисел.

Кодовые корректоры смещения можно разделить на два вида: линейные и нелинейные.

Линейный кодовый корректор отображает n бит входных данных в m бит выхода с величиной смещения $e/2$. Смещение любой ненулевой комбинации выходных бит будет не больше $e^d/2$, где d — минимальное кодовое расстояние линейного кода, задаваемого порождающей матрицей G.

Действие линейного корректора удобно описать с помощью (n, m, t)-устойчивой функции. Под (n, m, t)-устойчивой функцией будем понимать функцию, отображающую n битов входа в m битов выхода таким образом, что если t входных битов имеют фиксированные значения, то не происходит никаких изменений на выходе.

Нелинейный корректор отображает n бит в m бит. При этом ненулевая линейная комбинация выхода определяется как вектор булевой функции. Величина смещения может быть вычислена с помощью таблицы истинности. Используя преобразования Уолша, можно оценить смещение с помощью функции веса кода.

В качестве примера рассматривается применение кода БЧХ с параметрами (256, 21, 111) и дуального кода (256, 234, 6) с порождающим полиномом $h(x)$, имеющего степень 21 Вектор из 255 символов представляется в полиномиальном виде $m(x)$. Далее выполняется кодирование $m(x)$ mod $h(x)$. При этом происходит

отображение элементов поля F_2^{255} в поле F_2^{21}. При входном смещении равном 0,25 теоретическая оценка смещения выхода не превосходит 2^{-111}. Энтропия выхода близка к 21.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ОБЛАЧНЫХ СЕРВИСОВ

П.В. ШЕЛЕСТОВИЧ

С ростом популярности облачных сервисов для определенных видов вычислений все острее встает вопрос обеспечения безопасности данных в «облаке» и их постоянной доступности. Например, пользователи мобильных устройств регулярно синхронизируют свои данные с персональными компьютерами посредством облачных служб, то выступает потенциальной угрозой для важных рабочих данных.

Были проведены исследования мероприятий по обеспечению безопасности облачных вычислений. Эта задача лежит как на операторе облака, так и на пользователе. Создание условий для функционирования средств защиты информации в первую очередь подразумевает формирование доверенной среды. Для облачной платформы это означает тотальную организацию процессов развертывания и корректного завершения доверенных контейнеров (виртуальных машин или приложений) внутри. Внутри доверенной среды такие сервисы защиты информации, как подпись, аутентификация, идентификация и другие, также становятся облачными сервисами, доступными всем доверенным пользователям на общих основаниях. Перенос основных сервисов защиты информации в облачную среду снимает с участника сложную инфраструктурную часть средств защиты информации и предъявляет практически единственное требование к пользователю среды облачных вычислений — доверенность среды компьютера (устройства, терминала), который подключается к облаку.

Полученные результаты исследований выявили: использование облачной безопасности для защиты информации имеет смысл и результат. Таким образом, облачная безопасность больше всего подходит именно для пользователей, которые с ее помощью могут обезопасить свою деятельность куда более действенно и актуально, нежели локальными решениями.