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.

Библиотека БГУИР