цифровых устройств при их реализации на ПЛИС, защита цифровых устройств от клонирования на идентичных ПЛИС, защита цифровых устройств от несанкционированных изменений.

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ФАЗОВОЙ СИНХРОНИЗАЦИИ

Д.Л. ШИЛИН, С.С. БЫВШЕВ, М.В. ПОЧЕБУТ

Авторами предлагается способ шифрования данных с использованием систем фазовой синхронизации (СФС), работающих в режиме детерминированного хаоса. Данный режим работы является нерегулярным. Причина нерегулярности определяется свойством нелинейных систем экспоненциально быстро разводить первоначально близкие траектории. Поэтому не представляется возможным предсказать поведение таких систем, так как реально начальные условия можно задавать лишь с конечной точностью, а ошибки экспоненциально возрастают.

Предлагается на основе ранее разработанной имитационной модели СФС создать систему шифрования информации для передачи последней по открытым каналам связи. В качестве случайных последовательностей будут использоваться значения фазы и частоты сигнала на выходе блока фильтров модели. Будет использован симметричный алгоритм шифрования, в котором шифрование и дешифрование отличается только порядком выполнения и направлением некоторых шагов. В этом алгоритме авторами предлагается использовать один и тот же секретный ключ — физические параметры работы модели. С точки зрения простоты реализации, наиболее привлекательным является двоичное (битовое) гаммирование. Обычно, при использовании гаммирования, если гамма короче, чем открытое сообщение, она повторяется требуемое число раз. В нашем случае, в этом нет необходимости, так как возможно сгенерировать гамма последовательность необходимой длины. Этот аспект позволяет построить поточную систему шифрования данных, которая сможет передавать поток данных, каждый символ которых должен быть зашифрован и отправлен куда-либо, не дожидаясь последующих данных (обмен текстовыми и голосовыми сообщениями по сети).

При кодировании файла целиком (без учета структуры), снижается криптостойкость шифра. Это объясняется тем, что многие файлы помимо основных данных, хранят однородные данные о формате. Поэтому для некоторых форматов файлов целесообразно шифровать только основные данные.

СИСТЕМА КОНТРОЛЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ БУРОВОЙ УСТАНОВКИ

М.В. ПОЧЕБУТ, Ю.В. ВОРОБЬЕВА

Для обеспечения операций бурения используются дизельные двигатели большой мощности. Ежедневно мастер готовит отчет о работе технологического оборудования на буровой установке и по телефону докладывает информацию в диспетчерскую службу бурового предприятия. Такой контроль сложно назвать надежным, так как присутствует человеческий фактор, влияющий на достоверность передаваемой информации.

Целью данного проекта является проектирование системы по обеспечению оперативного мониторинга и контроль в режиме ON-LINE работы, к примеру, всех