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

дизельных двигателей на буровой, что в свою очередь позволяет прямо и косвенно контролировать технологические процессы бурения, формировать ежедневные отчеты о работе дизельных двигателей на буровой и расходе дизельного топлива без участия мастеров.

Для контроля оборотов двигателя на этих дизелях используются электрические тахометры. Удаленный мониторинг работы дизельного двигателя производится по данным полученным с тахометра. Для измерения сигналов тахометра и передачи данных используется контроллер UAB TELTONIKA FM4200. Он содержит аналоговые входы для измерения напряжения тахометров дизельных двигателей, напряжения в электросети буровой установки (контроль дизель электростанции) и GPRS канал для передачи данных.

FM4200 это терминал с GPS и GSM соединением, который способен распознавать координаты и передавать их используя ресурсы GSM сетей. Прибор имеет входные и выходные параметры, которые позволяют следить и управлять другими приборами объекта.

Использование микроконтроллера более надежно, так как процесс полностью автоматизирован, производится экономия материальных средств за счет сокращения рабочих кадров, существует доступ к данным в любой момент времени, данные передаваемые по GRPS каналу доступны только администратору, не играет роли человеческий фактор, тем самым сводится к нулю риск кражи топлива, риск получения ложных данных, процесс может контролироваться удаленно, а также контроллер отличается низким энергопотреблением.

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ УСТРОЙСТВ ФАПЧ

Д.Л. ШИЛИН, М.В. ПОЧЕБУТ

Разработанная система представляет собой симметрично-поточную криптосистему, в которой шифрование проводится над каждым байтом исходного текста с использованием гаммирования. Источником гамма-последовательности является система фазовой автоподстройки частоты, работающая в режиме детерминированного хаоса. Безопасность системы полностью зависит от свойств генератора потока ключей. Если он реализуется на конечном автомате, последовательность со временем повторится. Практически все генераторы псевдослучайных последовательностей за исключением одноразовых блокнотов являются периодическими. Поэтому, поток ключей должен иметь более длинный период, чем количество битов, выдаваемых между сменой ключей. Генератор должен выдавать одну и ту же гамма-последовательность и для шифрования, и для дешифрирования. Поэтому важным моментом является однократное использование гамма-последовательности, следовательно, необходима синхронизация передающего и принимающего устройств. Для этих целей предлагается использовать самосинхронизирующееся потоковое шифрование. Так как внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста, то расшифрующий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором. Последовательности чисел, получаемые при помощи генератора на основе устройства фазовой автоподстройки частоты, работающем в режиме детерминированного хаоса, были протестированы на случайность.

Были использованы статистические NIST, DIEHARD. Также тестирование проводилось по критериям сериальной корреляции, частот, интервалов, серий.