УДК 004.421.5

Использование стандарта шифрования ГОСТ Р 34.12-2015 для защиты данных в киберфизических системах с ограниченными ресурсами

Грозов В.А.
Университет ИТМО, Санкт-Петербург
Научный руководитель: к.т.н., доцент факультета БИТ Будько Михаил Юрьевич
Университет ИТМО, Санкт-Петербург
vladimirgrozov@mail.ru

Киберфизические системы (КФС) получают все более широкое распространение в различных сферах человеческой деятельности. Важной тенденцией их развития является миниатюризация, необходимая, например, в интернете вещей, в различных малогабаритных робототехнических и беспилотных устройствах и т.д. Особенности таких систем – передача данных по беспроводным каналам связи и существенные ограничения на массогабаритные, энергетические и вычислительные характеристики. Основой защиты данных являются криптографические методы, стойкость которых во многом зависит от качества используемых криптографических примитивов, в том числе генераторов псевдослучайных последовательностей. При этом одной из основных проблем является необходимость обеспечить безопасную передачу данных для низкоресурсных интеллектуальных устройств различного назначения.

Существует особый класс алгоритмов, предназначенных для защиты данных при необходимости минимизации затрат – легковесные криптоалгоритмы. Их использование диктуется необходимостью обеспечивать высокую скорость работы, или малые размеры микросхем, или низкое энергопотребление и др. В некоторых случаях критичным оказывается объем кода программы или размер потребляемой ею оперативной памяти.

Целью работы является развитие техники генерации псевдослучайных последовательностей с использованием компонентов ГОСТ Р 34.12-2015 для повышения защищенности низкоресурсных КФС.

В работе реализованы различные варианты алгоритма ГОСТ Р 34.12-2015, позволяющие уменьшить используемые вычислительные ресурсов и повысить скорость генерации псевдослучайных последовательностей. Проведено сравнение качества генерируемых последовательностей с помощью пакета статистических тестов NIST STS. В качестве эталона для сравнения использовался международный стандарт блочного шифрования AES.

Результаты исследования показали, что использование различных конфигураций криптографических примитивов ГОСТ Р 34.12-2015 позволяет адаптировать алгоритм для генерации псевдослучайных последовательностей с целью улучшения защиты низкоресурсных КФС.