АСПЕКТЫ ПРЕПОДАВАНИЯ ТЕХНИЧЕСКИХ ДИСЦИПЛИН ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г.А. Власова

Стремительное развитие информационных технологий и их внедрение во все сферы жизнедеятельности человека требует подготовки все большего количества технических специалистов. В то же время рост потребности рынка труда не должен приводить к снижению качества подготовки кадров.

Базовыми навыками при подготовке специалистов по информационной безопасности являются умение представлять в аналитическом виде модели сигналов, осуществлять расчет временных и спектральных характеристик сигналов, знание математических моделей сигналов и принципов передачи сигналов по каналам связи и умение применять эти знания для решения теоретических и практических задач. Однако классические учебники, содержащие монохромные статические зависимости, тяжелы для усвоения современными студентами. Информация, содержащаяся в таких учебниках, воспринимается учащимися как устаревшая и сложная для восприятия. Поэтому для изучения математических моделей сигналов разработаны и используются в учебном процессе компьютерные программы для вуализации базисных функций, исследования их свойств и особенностей разложения различных сигналов в базисе данных функций. Рассматриваются следующие негармонические ортогональные нормированные полиномы: полиномы Чебышева 1-го рода; полиномы Лагерра, Лежандра и Эрмита. Программы позволяют: выбрать число базисных функций, увидеть значение каждой функции при произвольном значении аргумента на интервале определения, задать сигнал в виде функции и увидеть его представление во временной области и в виде спектра в выбранном базисе.

Использование в учебном процессе данных программ вызывает интерес у студентов, помогает изучить вопрос множественности спектров, формирует способность анализировать и оценивать собранные данные, навыки работы с компьютерной техникой, системного и сравнительного анализа, оптимизации параметров элементов и систем защиты информации.

АСПЕКТЫ ПРОЕКТИРОВАНИЯ УСТРОЙСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ДАТЧИКОВ И ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ IoT

Г.А. Власова

Интернет вещей (Internet of Things, IoT), рассматриваемый Советом Европы как основной путь развития информационных технологий, постепенно становится производственной системой. В том числе и на критически важных объектах информатизации: атомных станциях, нефтеперерабатывающих заводах, газопроводах, системах электроснабжения и т.д. Однако многочисленные примеры успешных атак на системы IoT говорят об их уязвимости. Значительная потенциальная опасность последствий, которые могут возникнуть в результате сбоев в работе системы, делают актуальной проблему обеспечения информационной безопасности IoT. Эффективным методом обеспечения защиты является применение криптографии. Однако не существует универсального решения для различных областей применения криптографических методов.

Для датчиков и исполнительных устройств в системе IoT характерны малые объемы передаваемой информации, низкое быстродействие (во многих случаях до 30 с). При этом требуются низкая стоимость (меньше стоимости датчиков), что влечет низкий объем доступной памяти, низкую потребляемую энергию (небольшая экономия на одном устройстве оборачивается большой для сети таких устройств). Однако надежность (криптостойкость) должна снижаться незначительно. Согласно рекомендациям американского Национального института стандартов и технологий (NIST) гарантированно обеспечивают высокий уровень безопасности симметричные алгоритмы с длиной ключа не менее 128 бит и асимметричные алгоритмы с длиной ключа не менее 3072 бит. Проведенные измерения для алгоритмов RSA-3072 , AES-128 и ECIES-256 на симуляторе микроконтроллера показали следующие

результаты. Алгоритмы RSA-3072 и AES-128 значительно (примерно в 3 раза) меньше используют память программ по сравнению с ECIES-256. Однако для памяти данных AES-128 уже не имеет такого значительного преимущества по сравнению с ECIES-256 (выигрыш приблизительно в полтора раза). RSA-3072 требует в 3,5 раз больше памяти данных по сравнению с ECIES-256 и в 5,4 раза больше по сравнению с AES-128. Для успешного запуска RSA-3072 требуются микроконтроллеры с минимум 32 КБ памяти.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНАХ И ПОДРАЗДЕЛЕНИЯХ ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ БЕЛАРУСЬ

С.Ю. Воробьёв, В.А. Русак

В XXI веке трудно найти какую-либо область из жизни общества, где бы не использовались способы обработки и передачи информации [1]. Информационная сфера Республики Беларусь стремительно развивается. По мере совершенствования и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых информационных технологий [2]. Наибольшую общественную опасность представляют правонарушения, связанные с неправомерным доступом к компьютерной информации. Требования к обеспечению технической защиты информации в органах и подразделениях по чрезвычайным ситуациям Республики Беларусь изложены в приказе МЧС от 11.03.2016 № 64 «Об информационной безопасности». Необходимо отметить усиление опасности несанкционированного доступа к компьютерной информации в связи с ростом различного способа использования компьютерных систем и сетей в органах государственного управления и государственных организациях.

Список литературы

1. Лемешевский О.О. Актуальные вопросы информационной безопасности на факультете внутренних войск МВД Республики Беларусь // Матер. междунар. науч.-практ. конф. «Теоретические и прикладные проблемы информационной безопасности». Минск, 18 мая 2018 г. С. 36–38.

2. Чижиков Э.Н. Защита информации в информационных системах МЧС России // Темат. сб. «Информационные технологии, связь и защита информации МВД России». Москва, 2012. С. 14–17.

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ

А.А. Гавришев, А.П. Жук

Авторами в работе [1] разработан обобщенный алгоритм защищенного информационного обмена в беспроводных системах безопасности. В работе [2] на основании работы [1] разработан усовершенствованный алгоритм защищенного информационного обмена с усложненной имитовставкой, состоящий из следующих шагов. 1. Инициализация генератора ПСП-1 управляющего блока. 2. Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока, и его отправка на генератор ПСП-2 блока контроля и в блок логической операции XOR. 3. Выбор из таблицы уникальных идентификационных данных (УИД) одного уникального значения, присвоенного каждому контролируемому объекту. 4. Сложение по правилу XOR значений первой ПСП-1 блока контроля и УИД выбранного контролируемого объекта. 5. Отправка полученного значения в накопитель хаотической последовательности (НХП), где оно перемножается с хаотическим сигналом (ХС), и передача полученного произведения на контролируемый объект. 6. Декодирование в контролируемом объекте полученного сигнала с помощью накопителя копии хаотической последовательности (НКХП), идентичного НХП в управляющем блоке. 7. Поступление декодированного сигнала в блок логической операции XOR контролируемого объекта, в который одновременно с этим приходит индивидуальное