References

1. **Hrustalev D. A.** *Mobil'nye telefony Siemens. Principy ustrojstva i remont.* M.: Izumrud, 2004. 256 p.

2. **Zajac A.** *Obzor i testirovanie smartfona Caesar A9600, a takzhe znakomstvo s MT6589 — chetyrehiadernoi SoC MediaTek dlia biudzhetnyh reshenij.* URL: http://ixbt.com/md/pda/ (Data obrashhenija: 03.03.2014.).

3. **Shherbak N.** Programmiruemye radiostancii — budushhee takticheskoj svjazi / N. Shherbak. *Jelektronika: Nauka, Tehnologija, Biznes.* 2001, no. 5, pp. 16—19.

4. **Uhm M.** Adaptivity in Action for SDR and Cognitive Radio. *COTS Journal.* — February, 2006. URL: Rezhim dostupa: http://www.cotsjournalonline.com (Data obrashhenija: 14.10.2014).

5. **Zorin K. M.** Model' i metodika rekonfiguracii logicheskoj struktury integrirovannogo ob'ekta informatizacii. *Izvestija SPbGJeTU "LJeTI".* 2010, no. 6, pp. 20—25.

6. **GOST** R 51275—2006. *Zashhita informacii. Ob'ekt informatizacii. Faktory, vozdejstvujushhie na informaciju. Obshhie polozhenija. Vved.* 2006.12.27. — M.: Federal'noe agentstvo po tehnicheskomu regulirovaniju i metrologii, 2007. 8 p. (Nacional'nyj standart Rossijskoj Federacii).

7. **Chudnov A. M., Barashkov P. N., Tkachenko A. P., Tkachenko K. A.** *Model' sistemy svjazi s upravljaemymi strukturami v konfliktnyh uslovijah.* L.: VAS, 1986.

8. **Sovetov B. Ja., Jakovlev S. A.** Modelirovanie sistem: ucheb. dlja vuzov. M.: Vysshaja shkola, 2007.

9. **Petrov S. V.** Grafovye grammatiki i zadachi grafodinamiki. *Avtomatika i telemehanika.* 1977, no. 10.

10. **Petrov S. V.** Normal'naja forma grafovyh grammatik. *Avtomatika i telemehanika.* 1977, no. 6.

11. **Ajzerman M. A., Gusev L. A., Petrov S. V., Smirnova I. M., Tenenbaum L. A.** Dinamicheskij podhod k analizu struktur, opisyvaemyh grafami (osnovy grafodinamiki) / *Sb. nauch. trudov. Akademija nauk SSSR "Issledovanii po teorii struktur".* M.: Nauka, 1988.

12. **Perez P. P.** *Matrix Graph Grammars: An Algebraic Approach to Graph Dynamics.* VDM Verlag, 2009, pp. 5—80.

13. **Braverman Je. M., Rozonojer L. I.** Shodimost' sluchajnyh processov v teorii obuchenija mashin I, II / Je. M. Braverman. *Avtomatika i telemehanika.* 1969, no. 1.

14. **Cypkin Ja. Z.** *Adaptacija i obuchenija vavtomatizirovannyh sistemah.* M.: Nauka. 1968.

15. **Fermann H. H.** *O nekotoryh podhodah k opredeleniju pravila ostanovki dlja algoritmov adaptacii. Problemy sluchajnogo poiska.* Kn. 4. Pod obshh. red. L. A. Rastrigina. Riga: Zinatne, 1975, pp. 55—59.

УДК 004.942; 004.056.55; 004.384

Д. В. Капулин, канд. техн. наук., зав. каф., e-mail: dkapulin@sfu-kras.ru,
О. В. Дрозд, студент, e-mail: olvldrozd@gmail.com
Сибирский федеральный университет, г. Красноярск

Устройство аппаратного шифрования производственных данных

Предложено устройство, обеспечивающее защищенный обмен производственной информацией с использованием алгоритмов ГОСТ 28147—89. Реализация устройства выполнена с применением ПЛИС Xilinx Spartan-6. Подробно рассмотрены этапы проектирования устройства, проведено имитационное моделирование разработанного устройства в среде Simulink.

Ключевые слова: *аппаратное шифрование, передача данных, защита информации, беспроводная связь, wi-fi*

Введение

Широкое распространение технологий беспроводного *Ethernet* в корпоративном секторе и в секторе электронных устройств для частного пользования закономерным образом приводит к росту внимания к этим технологиям со стороны производителей и интеграторов автоматизированных систем управления технологическими процессами (АСУ ТП). Применительно к АСУ ТП беспроводные сети и устройства передачи данных обладают следующими преимуществами [1]:

- возможность расположения устройств приема-передачи в труднодоступных местах;
- удобство развертывания и обслуживания устройств;
- оперативное добавление устройств в корпоративную сеть или исключение из нее;
- возможность расположения устройств приема-передачи данных на подвижных объектах.

Кроме того, внедрение беспроводных устройств контроля технологических и производственных параметров открывает новые возможности по применению систем автоматики, такие как обеспечение доступа к объекту, контроль периметра объекта, наблюдение за перемещениями персонала на территории предприятия, автоматизация контроля проведения инспекций и технического обслуживания, контроль экологических параметров окружающей среды и т. д.

Разработку контрольно-измерительных приборов АСУ ТП со встроенными беспроводными интерфейсами ведет компания *Yokogawa* с использованием стандарта промышленной беспроводной связи ISA 100/11a. Номенклатура беспроводных измерительных преобразователей *Yokogawa* включает в себя датчики температуры, абсолютного, избыточного и дифференциального давления [2]. Среди производителей промышленных беспроводных точек дос-

тупа следует также отметить компании *Yokogawa* и *Hirschmann* [1].

При использовании беспроводных технологий для организации связи и управления устройствами, входящими в состав АСУ ТП, следует уделять внимание и защите передаваемой информации, которая зачастую носит конфиденциальный характер. Так, компания *Yokogawa* уделяет особое внимание разработке беспроводных устройств контроля и управления системами нефте- и газопроводов, аппаратуры технологического и производственного учета с применением аппаратного шифрования информации. В качестве алгоритмов шифрования в промышленных сетях, построенных с использованием подобного оборудования, наиболее широкое применение находят алгоритмы *DES* и *AES*. Основными недостатками алгоритма шифрования *DES* являются существование слабых ключей, низкая устойчивость алгоритма к прямому перебору ключей, в том числе с использованием аппаратных средств, низкая устойчивость при атаке с использованием дифференциального криптоанализа. В качестве основного недостатка алгоритма шифрования данных *AES* следует отметить недостаточную изученность математического аппарата шифрования [3].

Указанные недостатки алгоритмов шифрования *DES* и *AES* позволяют сделать вывод о недостаточном уровне защищенности каналов беспроводной связи для их массового применения в АСУ ТП, особенно на объектах энергетики и оборонно-промышленного комплекса. Проблема безопасности беспроводных сетей передачи данных в АСУ ТП усугубляется тем, что в России отсутствуют государственные стандарты по информационной безопасности АСУ ТП [4], аналогичные таким стандартам, как ISA SP99, IEEE 1402, IEC 62351 [5—7]. Вместе с тем существует апробированный алгоритм криптографического преобразования, закрепленный стандартом ГОСТ 28147—89 [8].

Постановка задачи

Цель исследования состоит в разработке методов и средств обеспечения безопасной передачи производственных или технологических данных по промышленным беспроводным сетям передачи данных с использованием алгоритма криптографического преобразования (ГОСТ 28147—89). При этом следует отметить наличие различных подходов к реализации данного алгоритма на базе разнообразных аппаратных средств [9—11].

Для постижения поставленной цели предлагается метод проектирования устройства для организации беспроводного защищенного обмена информацией. Реализацию устройства предлагается выполнить с помощью криптографического модуля, сформированного на базе программируемой логической интегральной схемы (ПЛИС) *Xilinx Spartan-6 XC6SLX25* с использованием серийного комплекта разработчика на базе данной ПЛИС. Разрабатываемое устройство должно обеспечивать взаимодействие с мобильными устройствами сторонних производителей посредством протоколов *USB* 2.0 и *IEEE* 802.11.

Описание устройства обмена данными

Рассмотрим процесс разработки устройства для организации защищенного обмена информацией (данными) по промышленным сетям беспроводной связи. На рис. 1 изображена структурная схема устройства защищенной передачи данных. Для защиты канала передачи данных необходимо использовать как минимум два подобных устройства, одно из которых связано с передатчиком и выполняет шифрование передаваемых данных, второе устройство связано с приемником и предназначено для дешифрования полученных данных. При этом устройства аналогичны и взаимозаменяемы.

На рис. 1 приняты обозначения: 1.1 — устройство защищенной передачи данных; 1.2 — проводной *USB* интерфейс; 1.3 — преобразователь интерфейсов *USB*/*UART*; 1.4 — криптографический блок на базе ПЛИС; 1.5 — радиоинтерфейс *IEEE* 802.11 со встроенной радиоантенной 1.7; 1.6 — внешняя радиоантенна (опционально); 1.8 — энергонезависимая память; 1.9 — программатор энергонезависимой памяти; 1.10 — проводной *RS*-232 интерфейс; 1.11 — аккумуляторная батарея; 1.12 — источник электропитания; 1.13 — переключатель режимов работы; 1.14 — генератор тактовых импульсов.

В качестве преобразователя интерфейсов *USB*-*UART* используется микросхема *FT*232*R* (производитель *FTDI Chip*, корпус *SSOP*-28). Взаимодействие с внешними устройствами осуществляется посредством проводного интерфейса *USB* (1.15 на рис. 1). Для обеспечения взаимодействия с устройствами по

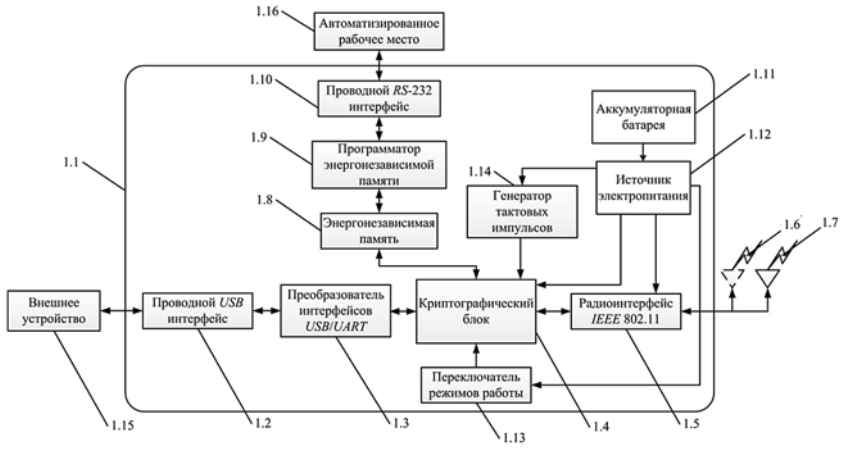

Рис. 1. Структурная схема устройства обеспечения защищенной передачи данных

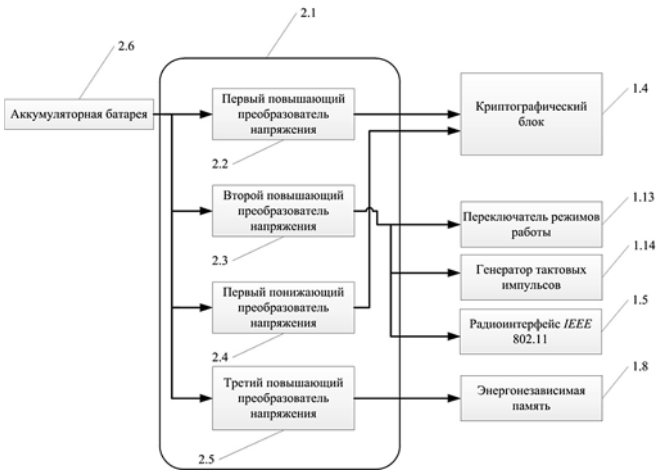

Рис. 2. Структурная схема источника электропитания

беспроводным каналам связи используется модуль *WizFi* 220 (производитель *WIZnet Co.*) со встроенной антенной, также возможно подключение внешней антенны через разъем стандарта *U.FL*. Модуль *WizFi* 220 поддерживает стандарты беспроводной передачи данных *IEEE* 802.11*b/g/h*, протоколы безопасности *WEP* и *WPA/WPA*2. Взаимодействие между модулем и внешними устройствами может осуществляться посредством интерфейсов *UART*, *SPI* и I^2C.

В качестве ключевого запоминающего устройства используется микросхема электрически стираемого перепрограммируемого постоянного запоминающего устройства 24*LC*02 (производитель *Microchip*, корпус *SOP*-8L) емкостью 2048 бит, что позволяет хранить восемь секретных ключей по 256 бит каждый. Взаимодействие между ключевым запоминающим устройством и внешними устройствами осуществляется посредством интерфейса I^2C. Программатор энергонезависимой памяти построен по схеме, предложенной Клаудио Ланконелли [12], взаимодействие с автоматизированным рабочим местом специалиста по информационной безопасности (1.16 на рис. 1) осуществляется посредством интерфейса *RS*-232. В качестве генератора тактовых импульсов используется генератор тактовых импульсов *KXO-V*97 (производитель *Geyer*, Германия).

Рассмотрим систему электропитания устройства (рис. 2). В состав источника электропитания 2.1 входят три повышающих преобразователя напряжения 2.2; 2.3; 2.5 и один понижающий преобразователь напряжения 2.4. В качестве повышающих преобразователей напряжения используются повышающие преобразователи напряжения *MAX*1675 (производитель *Maxim*, корпус *UMAX*10), в качестве понижающего преобразователя напряжения используется понижающий преобразователь напряжения *LM*3674 (производитель *National Semiconductor*, корпус *SOT*-23). Понижающий преобразователь напряжения используется для обеспечения ПЛИС питающим напряжением 1,2 В, для обеспечения питания всех остальных потребителей используются повышающие преобразователи напряжения, кроме преобразователя интерфейсов, питание которого осуществляется через цепи питания и общего провода разъема *USB*. В качестве аккумуляторных батарей 2.6 используются два литий-ионных аккумулятора формфактора 18650 емкостью по 3200 мА·ч, для управления процессом заряжания аккумуляторных батарей используется контроллер заряда *bq*24002 (производитель *Texas Instruments*, корпус *R-PDSO-G*20). Процесс заряда аккумуляторных батарей осуществляется через цепи питания и общего провода разъема *USB*, таким образом заряжать аккумуляторные батареи можно от персонального компьютера или ноутбука. Заряда двух аккумуляторных батарей достаточно для 48 ч непрерывной работы при максимальном энергопотреблении, притом что модуль *WizFi* 220 будет работать только в режиме передачи.

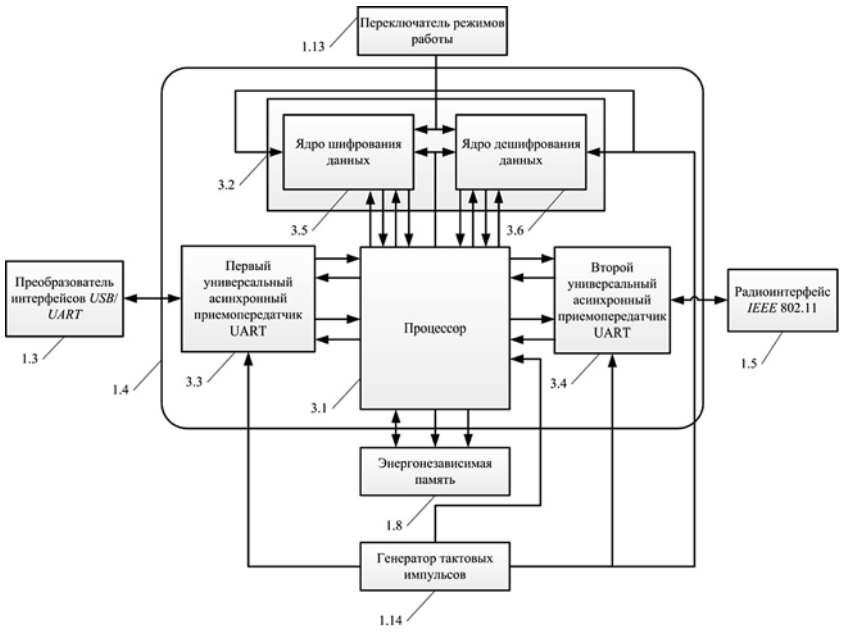

Рис. 3. Структурная схема криптографического блока

Рассмотрим структуру криптографического блока и назначение модулей, входящих в его состав (рис. 3). Криптографический блок реализован на базе ПЛИС *Xilinx Spartan*-6 *XC*6*SLX*25 с использованием серийного комплекта разработчика *SK-iMX*53-*XC*6*SLX* [13]. В качестве языка реализации алгоритма шифрования выбран язык описания аппаратуры *Verilog*.

Криптографический блок состоит из процессора 3.1, криптографического сопроцессора 3.2, первого универ-

сального асинхронного приемопередатчика *UART* 3.3, второго универсального асинхронного приемопередатчика *UART* 3.4. В состав криптографического сопроцессора входит ядро шифрования данных 3.5 и ядро дешифрования данных 3.6.

Основной задачей первого универсального асинхронного приемопередатчика является прием пакетов открытых данных от внешних устройств и передача пакетов открытых данных внешним устройствам, при этом непосредственным приемником и передатчиком данных является преобразователь интерфейсов *USB*/*UART*, с которым, в свою очередь, взаимодействуют мобильные устройства, подключенные посредством проводного *USB* интерфейса. Также первый универсальный асинхронный приемопередатчик обеспечивает управление процессом передачи и приема данных.

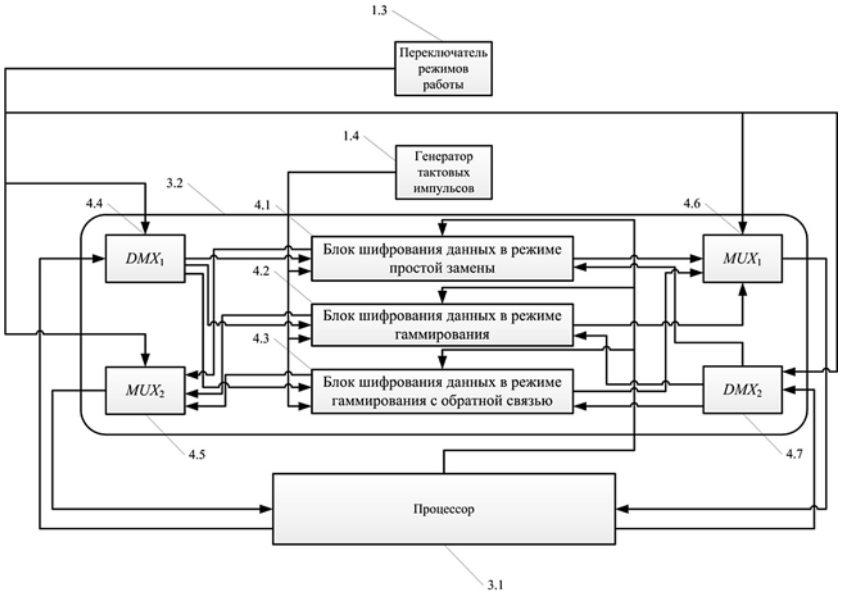

Рис. 4. Структурная схема ядра шифрования данных

Задача второго универсального асинхронного приемопередатчика — прием пакетов закрытых данных от внешних устройств и передача пакетов закрытых данных внешним устройствам, при этом непосредственным приемником и передатчиком данных является радиоинтерфейс *IEEE* 802.11 на базе модуля *WizFi* 220, с которым взаимодействуют мобильные устройства посредством беспроводного канала связи стандарта *IEEE* 802.11. Также второй универсальный асинхронный приемопередатчик обеспечивает управление процессом передачи и приема данных.

На рис. 4 представлена структурная схема ядра шифрования данных, при этом структуры ядра шифрования и дешифрования данных аналогичны. Ядра предназначены соответственно для осуществления процедур шифрования и дешифрования последовательностей двоичных данных в соответствии с алгоритмом шифрования согласно ГОСТ 28147—89. Ядра шифрования и дешифрования данных включают в себя блоки выполнения криптографических преобразований в режиме простой замены 4.1, режиме гаммирования 4.2 и режиме гаммирования с обратной связью 4.3. В состав ядер шифрования и дешифрования данных также входят мультиплексоры 4.5, 4.6 и демультиплексоры 4.4, 4.7, предназначенные для коммутации внутренних каналов передачи данных в зависимости от выбранного режима работы криптографического сопроцессора.

Выбор режима шифрования/дешифрования данных осуществляется с помощью переключателя режимов работы. Переключатель режимов работы представляет собой *DIP*-переключатель на три контактные группы, размещаемый на поверхности печатной платы устройства. С помощью переключателя режимов работы выполняется переключение криптографического сопроцессора, входящего в состав криптографического блока, на иные режимы работы. Первая контактная группа соответствует режиму простой замены, вторая контактная группа соответствует режиму гаммирования, третья контактная группа соответствует режиму гаммирования с обратной связью.

Основными функциями процессора является обеспечение:

- считывания информации из энергонезависимой памяти, что включает в себя также адресацию памяти и управление процессом чтения информации;
- взаимодействия с первым и вторым универсальными асинхронными приемопередатчиками *UART*, что включает в себя прием данных, передачу данных, управление процессом приема данных, управление процессом передачи данных;
- взаимодействия с криптографическим сопроцессором, что включает в себя передачу и прием как открытых, так и закрытых данных, управление процессами приема и передачи как открытых, так и закрытых данных, передачу криптографическому процессору секретных ключей, предварительно считанных из энергонезависимой памяти.

Выработка секретных ключей осуществляется с использованием программного продукта, реализующего линейный конгруэнтный метод для генерации псевдослучайных чисел. Возможна разработка аппаратного генератора случайных чисел с использованием таких процессов, как тепловой шум полупроводниковых приборов, фотоэлектрический эффект и неравномерность в задержках логических элементов [14].

Таблица 1

Параметры реализации алгоритма криптографического преобразования по ГОСТ 28147-89 на базе ПЛИС

Семейство ПЛИС	Модель ПЛИС	Число логических ячеек	Задержка, нс	Потребляемая мощность, Вт	Частота, МГц	Пропускная способность, Мбит/с
Artix-7	*XC7A200*	3808	131,0860	0,0730	7,6286	61,0286
Spartan-6	*XC6SLX25*	3808	161,3270	0,0290	6,1986	49,5887

В табл. 1 представлены некоторые параметры реализации шифроалгоритма ГОСТ 28147—89 на базе ПЛИС. Для рассматриваемого случая представлены параметры реализации 32 раундов шифрования данных в режиме простой замены.

Методика проектирования устройства защищенного обмена информацией

Исходя из приведенной структуры разработанного криптографического блока сформулируем методику проектирования подобного рода устройств шифрования на базе ПЛИС. Основная идея предлагаемой методики проектирования состоит в интеграции основных этапов проектирования (математическое моделирование, аппаратная реализация, отладка в составе системы) в единый итерационный цикл проектирования на основе включения в него дополнительных этапов проектирования и автоматизации процесса передачи формализованных описаний проектируемого устройства и данных, получаемых при моделировании и системной интеграции между этапами проектирования.

Предлагаемая методика проектирования состоит из следующих этапов.

1. Формализация технического задания на систему и устройства на базе ПЛИС. Разработка структурной схемы как для системы, так и для устройства.

2. Разработка идеализированной (линеаризованной) математической модели системы с использованием формата чисел с плавающей запятой, выполнение численного моделирования в среде *MATLAB/Simulink* и отладка разработанной модели.

3. Преобразование идеализированного алгоритма, реализованного в формате с плавающей точкой, в алгоритм с представлением чисел с фиксированной точкой. Оптимизация разрядностей по критерию минимизации аппаратных затрат.

4. Замена блоков проектируемого устройства на библиотечные компоненты, ориентированные на дальнейшую реализацию в аппаратуре с использованием пакетов *Altera DSP Builder*, *Xilinx System Generator* или *MATLAB HDL Coder* [15].

5. Аппаратно-программное моделирование созданного устройства.

6. Отладка и анализ параметров разработанного устройства на базе ПЛИС в реальном системном окружении.

Преимуществами предлагаемой методики проектирования устройств на базе ПЛИС по сравнению с классической методикой проектирования [16] являются:

- снижение влияния человеческого фактора при переходе от математической модели устройства к аппаратной реализации;
- непрерывность процесса проектирования устройства;
- получение в процессе проектирования отлаженной математической модели, которая является прототипом для создаваемого устройства и может быть использована не только в процессе проектирования, но и для дальнейшей оптимизации алгоритма работы устройства на основе данных, полученных из реального системного окружения проектируемого устройства.

Апробация методики проектирования проведена с использованием отладочного комплекса, включающего в себя серийный комплект разработчика *SK-iMX53-XC6SLX* и четыре отладочных модуля, реализующих ключевые узлы разработанного устройства (рис. 5). Узлы комплекса реализованы в соответствии со структурными схемами, приведенными на рис. 1—4. В состав отладочного комплекса входят модуль преобразователя интерфейсов *USB-UART*; модуль радиоинтерфейса *IEEE* 802.11, в состав которого входит модуль *WizFi* 220 со встроенной антенной; модуль, включающий в себя энергонезависимую память и программатор энергонезависимой памяти; модуль, включающий в себя аккумуляторную батарею и источник электропитания.

Моделирование устройства защищенной передачи данных выполнено в среде *MATLAB/Simulink*.

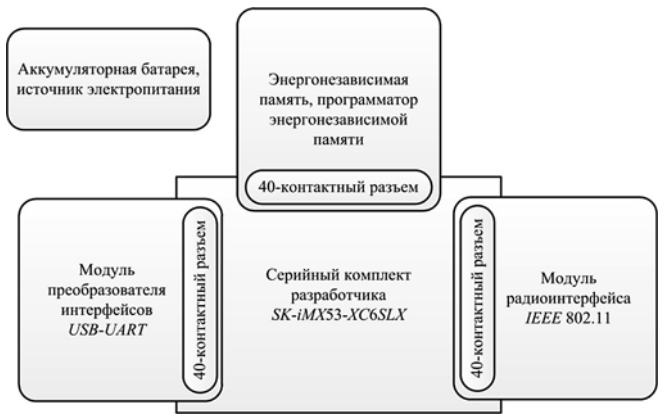

Рис. 5. Структурная схема отладочного комплекса

Устройство было представлено в виде трехканальной (три потока шифрования) системы массового обслуживания (СМО) с параметрами, соответствующими различным стандартам обмена информации. Анализ результатов моделирования, приведенных в табл. 2, показывает, что устройство обеспечивает надежную обработку и передачу данных с использованием большинства стандартных интерфейсов. Применение устройства совместно с интерфейсом *USB* 3.0 возможно при организации обработки поступающих пакетов данных в промежуточных накопителях (при одновременном снижении скорости обработки).

Рассматриваемая методика проектирования предлагаемого устройства обмена информацией может быть представлена в виде диаграммы *IDEF3*, приведенной на рис. 6.

Применение методики проектирования для разработки устройства аппаратного шифрования информации заканчивается его тестированием и отладкой. Предварительно должны быть проведены схемотехническое проектирование, размещение и трассировка элементов на печатной плате. Для устройства, рассматриваемого в настоящей работе, такие операции выполнены с использованием системы автоматизированного проектирования *Altium Designer*.

Таблица 2

Результаты моделирования устройства для обмена закрытой документальной информацией

Стандарт	Время работы СМО, мкс	Число поступивших заявок	Число обслуженных заявок	Число необслуженных заявок
802.11*g*	100	56	56	0
802.11*n*	100	156	156	0
802.11*ac*	100	1364	1362	2
Gigabit Ethernet	100	1040	1038	2
Fast Ethernet	100	104	104	0
USB 1.0	100	12	12	0
USB 2.0	100	498	497	1
USB 3.0	100	1915	1872	43

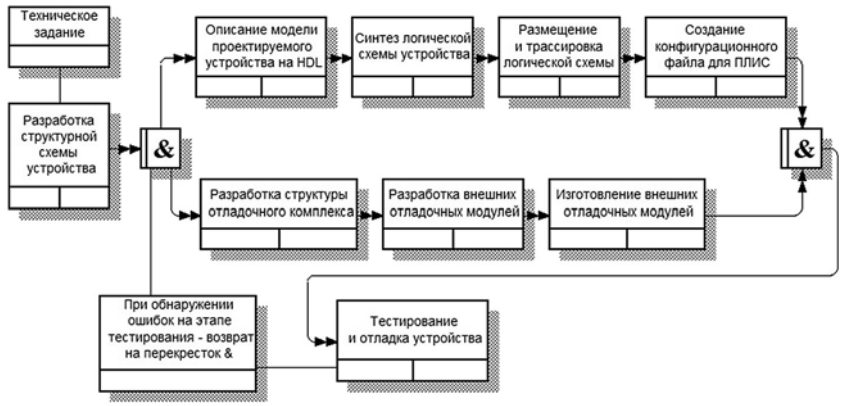

Рис. 6. Алгоритм проектирования устройства защищенного обмена информацией

Заключение

В результате проведенного исследования предложена и апробирована методика проектирования, а также предложена и реализована структура устройства аппаратного шифрования данных по алгоритму криптографического преобразования ГОСТ 28147—89. Разработанное устройство предназначено для безопасного обмена производственной и технологической информацией по промышленным беспроводным сетям передачи данных. Структура устройства спроектирована таким образом, чтобы была обеспечена возможность совместной работы с приборами (в том числе и с мобильными) сторонних производителей, поддерживающими интерфейсы *USB* и *IEEE* 802.11, что имеет особое значение при построении беспроводных сетей передачи данных в АСУ ТП на объектах промышленности, энергетики и оборонно-промышленного комплекса.

Работа выполнена при поддержке Красноярского краевого фонда поддержки научной и научно-технической деятельности.

Список литературы

1. **Беспроводные** точки доступа Hirschmann BAT [Электронный ресурс]. URL: http://www.hirschmann.ru/industrial/catalog/bat54/bat.series (дата обращения: 12.01.2015).

2. **Беспроводные** контрольно-измерительные приборы Yokogawa [Электронный ресурс]. URL: http://yokogawa.kippostavka.ru/wiriless.htm (дата обращения: 12.01.2015).

3. **Синьковский А. В.** Разработка эффективных решений по защите информации с использованием фрактального моделирования в условиях автоматизированного проектирования и производства: Автореф. дис. канд. техн. наук. М., 2007. 28 с.

4. **Лукацкий А. В.** Безопасность АСУ ТП: от слов к делу [Электронный ресурс]. URL: http://www.gosbook.ru/node/61562 (дата обращения: 12.01.2014).

5. **ISA99,** Industrial Automation and Control Systems Security [Электронный ресурс]. URL: https://www.isa.org/isa99/ (дата обращения: 12.01.2015).

6. **P1402** — Standard for Physical Security of Electric Power Substations [Электронный ресурс]. URL: http://standards.ieee.org/develop/project/1402.html (дата обращения: 12.01.2015).

7. **Core** IEC Standards [Электронный ресурс]. URL: http://www.iec.ch/smartgrid/standards/ (дата обращения: 12.01.2015).

8. **ГОСТ 28147—89.** Системы обработки информации. Защита криптографическая. Введ. впервые; дата введ. 01.07.90. М.: Изд-во стандартов, 1996. 26 с.

9. **Rabie A. M., Magdy S. A.** Metamorphic-Key-Hopping GOST Cipher and Its FPGA Implementation // The International Journal of Computer Science and Communication Security. 2013. Vol. 3. P. 51—60.

10. **Коробицын В. В., Ильин С. С.** Реализация симметричного шифрования по алгоритму ГОСТ—28147 на графическом процессоре // Информационные технологии. 2008. № 10. С. 46—51.

11. **Коробицын В. В., Ильин С. С.** Реализация симметричного шифрования по алгоритму ГОСТ—28147 на графическом процессоре с использованием технологи CUDA // Информационные технологии. 2011. № 4. С. 41—46.

12. **Lanconelli** Open Systems [Электронный ресурс]. URL: http://www.lancos.com/index.html (дата обращения: 12.01.2015).

13. **Отладочная** плата SK-iMX53-XC6SLX [Электронный ресурс]. URL: http://www.starterkit.ru/html/index.php?name=shop&op=view&id=76 (дата обращения: 12.01.2015).

14. **Саранча С. Н.** Методика определения параметров аппаратного генератора случайных чисел, реализованного в ПЛИС архитектуры FPGA // Автоматизированные системы управления и приборы автоматики: Всеукраинский межведомственный научно-технический сб. Харьков, 2011. Вып. 157. С. 89—94.

15. **FPGA** and ASIC Design with HDL Coder and HDL Verifier [Электронный ресурс]. URL: http://www.mathworks.com/fpga-design/solutions.html (дата обращения 12.01.2015).

16. **Proakis J. G., Salehi M.** Communication systems engineering / New Jersey: Prentice-Hall, 2002. 801 p.

D. V. Kapulin, Head of Chair, e-mail: dkapulin@sfu-kras.ru,
O. V. Drozd, Student, e-mail: olvldrozd@gmail.com, Siberian Federal University, Krasnoyarsk

Hardware-Based Encryption Production Data Device

This Research is devoted to the analysis of methods and techniques of data hardware encryption for production and technological information. The main objective of this paper is developing and applying the automated design method for hardware encryption tools and devices to establish the secure data channels in industrial wireless networks. The paper proposes a method of designing an electronic device, providing secure data transmission in industrial wireless data networks using cryptographic transformation algorithm GOST 28147—89. Using the proposed method, the device for data exchange with protected data is developed. The designing of the device is hold on the FPGA Xilinx Spartan-6 XC6SLX25, hardware description language — Verilog. Simulation of the developed device in a queuing system is run in Matlab/Simulink. This device is able to wireless protected data transmission between any tools, support USB and IEEE 802.11.

Keywords: *hardware encryption, data transfer, data protection, wireless, wi-fi*

References

1. **Besprovodnye** *tochki dostupa Hirschmann BAT,* URL: http://www.hirschmann.ru/industrial/catalog/bat54/bat.series (accessed 12.01.2015).

2. **Besprovodnye** *kontrol'no-izmeritel'nye pribory Yokogawa*, URL: http://yokogawa.kip-postavka.ru/wiriless.htm (accessed 12.01.2015).

3. **Sin'kovskii A. V.** *Razrabotka effektivnykh reshenii po zashchite informatsii s ispol'zovaniem fraktal'nogo modelirovaniya v usloviyakh avtomatizirovannogo proektirovaniya i proizvodstva* (The development of effective solutions to data protection using fractal simulation in a computer-aided design and manufacturing), Candidate's thesis abstract, Moscow. 2007. 28 p. (in Russian).

4. **Lukatskii A. V.** *Bezopasnost' ASU TP: ot slov k delu*. URL: http://www.gosbook.ru/node/61562 (accessed 12.01.2014).

5. **ISA99,** *Industrial Automation and Control Systems Security*. URL: https://www.isa.org/isa99/ (accessed 12.01.2015).

6. **P1402** — *Standard for Physical Security of Electric Power Substations.* URL: http://standards.ieee.org/develop/project/1402.html (accessed 12.01.2015).

7. **Core** *IEC Standards.* URL: http://www.iec.ch/smartgrid/standards/ (accessed 12.01.2015).

8. **GOST 28147—89.** *Sistemy obrabotki informatsii. Zashchita kriptograficheskaya*. (Information processing systems. Cryptographic protection, State Standart 28147—89). Moscow: Standarty, 1996, 26 p. (in Russian).

9. **Rabie A. M., Magdy S.** A Metamorphic-Key-Hopping GOST Cipher and Its FPGA Implementation. *The International Journal of Computer Science and Communication Security*. 2013, vol. 3, pp. 51—60.

10. **Korobitsyn V. V., Il'in S. S.** Realizatsiya simmetrichnogo shifrovaniya po algoritmu GOST—28147 na graficheskom protsessore (Implementation of the symmetric encryption algorithm GOST—28147 on the GPU). *Informatsionnye tekhnologii*. 2008, no. 10, pp. 46—51 (in Russian).

11. **Korobitsyn V. V., Il'in S. S.** Realizatsiya simmetnchnogo shifrovaniya po algoritmu GOST—28147 na graficheskom protsessore s ispol'zovaniem tekhnologi CUDA (Implementation of the symmetric encryption algorithm GOST—28147 on the GPU with CUDA). *Informatsionnye tekhnologii*. 2011, no. 4, pp. 41—46 (in Russian).

12. **Lanconelli** *Open Systems.* URL: http://www.lancos.com/index.html (accessed 12.01.2015).

13. **Otladochnaya** *plata SK-iMX53-XC6SLX.* URL: http://www.starterkit.ru/html/index.php?name=shop&op=view&id=76 (accessed 12.01.2015).

14. **Sarancha S. N.** Metodika opredeleniya parametrov apparatnogo generatora sluchainykh chisel, realizovannogo v PLIS arkhitektury FPGA (Method of parameter's definition for the hardware random number generator implemented in the FPGA). *Avtomatizirovannye sistemy upravleniya i pribory avtomatiki, Vseukrainskii mezhvedomstvennyi nauchno-tekhnicheskii sbornik*. Kharkiv. 2011, iss. 157, pp. 89—94 (in Russian).

15. **FPGA** *and ASIC Design with HDL Coder and HDL Verifier*, URL: http://www.mathworks.com/fpga-design/solutions.html (accessed 12.01.2015).

16. **Proakis J. G., Salehi M.** *Communication systems engineering.* NJ.: Prentice-Hall, 2002. 801 p.