УДК 621.3.06

А. А. Поликарпов, Н. К. Юрков

ЗАЩИТА ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УЧЕТА ЭНЕРГОРЕСУРСОВ

A. A. Polikarpov, N. K. Yurkov

DATA PROTECTION IN AUTOMATED SYSTEMS OF ENERGY ACCOUNTING

А н н о т а ц и я. Предложен подход к организации автоматизированных систем учета энергоресурсов в промышленности и жилищно-коммунальном хозяйстве для коммерческого и технологического учета на объектах распределения и потребления энергоресурсов. Предлагаемая программно-аппаратная платформа защиты данных с использованием средств криптографического преобразования, которая строится на основе отечественных микроконтроллеров, обеспечивает устойчивую и безотказную работу системы контроля энергоресурсов.

A b s t r a c t. Suggested approach to the Organization of automated energy accounting industry and housing and communal services for commercial and technological integration in the distribution and consumption of energy resources. The proposed hardware and software data protection platform by means of cryptographic transformation, which is built on the basis of domestic microcontrollers that provides a robust and reliable system operation control of energy resources.

К л ю ч е в ы е с л о в а: система учета, энергоресурсы, программно-аппаратная платформа, защита данных.

K e y w o r d s: accounting, energy, software and hardware platform, data protection.

Введение

В настоящее время в связи с реформой жилищно-коммунального хозяйства (ЖКХ) особую актуальность приобретает оперативный учет распределения и энергопотребления как организациями, так и физическими лицами.

Область применения автоматизированных систем учета энергоресурсов (АСУЭ) – промышленность и ЖКХ для коммерческого и технологического учета на объектах распределения и потребления энергоресурсов [1, 2].

Основные функции, выполняемые АСУЭ:

– измерение характеристик потребленных ресурсов: объема и температуры холодной и горячей воды; количества тепловой и электроэнергии; объема и давления природного газа;

– обеспечение автоматизированного сбора информации с объектов распределения и потребления энергоресурсов и ее последующая обработка;

– ведение и хранение баз данных параметров энергоресурсов;

– оповещение о нештатных ситуациях и сбоях различных элементов системы (в том числе через SMS-информирование).

Принцип работы большинства АСУЭ состоит в сборе данных о расходе, температуре, давлении ресурсов индивидуальными приборами учета, преобразовании собранных данных в

цифровую информацию и ее последующей передаче по связующим компонентам в вычислительный центр, в роли которого может выступать сервер и/или автоматизированное рабочее место (АРМ). Вычислительные центры различных уровней иерархии осуществляют обработку собранной информации, производя вычислительные и логические операции, предусмотренные процессом и алгоритмами обработки результатов измерений. По результатам обработки производятся выработка и применение управляющих воздействий, в том числе вывод информации о состоянии объектов [3].

Постановка проблемы создания интеллектуальных систем учета

В связи со стремительным ростом числа подобных систем и увеличением количества интеллектуальных счетчиков, используемых для контроля и учета энергоресурсов, многократно возрастает и количество потенциальных угроз, связанных с навязыванием ложных измерительных данных или выведением системы из строя, к числу которых относятся:

– изменение настроек и программного обеспечения счетчика;

– перехват управления телеметрическими устройствами;

– подача несанкционированных команд на счетчик и управление через счетчик другими устройствами;

– намеренное искажение данных и отключение систем энергоснабжения.

В данный момент на рынке измерительных приборов наблюдается отсутствие защищенных средств измерений, что вызвано нежеланием увеличивать стоимость счетчиков за счет встроенных средств безопасности (использование процессора или микроконтроллера, способного выполнять операции криптографического преобразования), а также сложностью процедуры управления и обслуживания устройств подобного типа (наличие механизма ввода хранения и модифицирования ключа, наличие интерфейса управления устройством для первоначального конфигурирования и последующего контроля конфигурации).

Использование доступных измерительных приборов при построении АСУЭ делает систему уязвимой для вредоносного программного обеспечения.

Программно-аппаратная платформа системы энергоучета

Предлагаемая программно-аппаратная платформа предназначена для защиты данных с использованием средств криптографического преобразования по ГОСТ 28147–89, построена с применением отечественных микроконтроллеров ЗАО ПКК «Миландр» (гарантировано отсутствие закладок на этапе производства), для обеспечения устойчивой защищенной работы сети используется режим простой замены.

Для зашифрования в этом режиме 64-битовый блок открытых данных (от прибора учета) сначала разбивается на две половины (младшие биты – A, старшие биты – B). На i-м цикле используется подключ K_i: $A_{i+1} = B_i \oplus f(A_i, K_i)$ ($\oplus$ – двоичное «исключающее или»); $B_{i+1} = A_i$.

Для генерации подключей исходный 256-битовый ключ (ключ хранится в энергонезависимой памяти и загружается при монтаже устройства) разбивается на восемь 32-битовых блоков: $K_1 \ldots K_8$. Ключи $K_9 \ldots K_{24}$ являются циклическим повторением ключей $K_1 \ldots K_8$ (нумеруются от младших битов к старшим). Ключи $K_{25} \ldots K_{32}$ являются ключами $K_8 \ldots K_1$ (ключ вырабатывается на один сеанс передачи данных).

Расшифрование выполняется так же, как и зашифрование, но инвертируется порядок подключей K_i.

Функция $f(A_i, K_i)$ вычисляется следующим образом: A_i и K_i складываются по модулю 2^{32}.

Для обеспечения защищенной передачи данных о потреблении энергоресурсов от индивидуальных приборов учета к центру сбора информации предполагается использование модуля криптографического преобразования для индивидуального прибора учета. В данном модуле реализованы возможность подключения к прибору учета по стандартному интерфейсу (импульсный RS-485/RS-232 (ModeBus), возможна также реализация других перспективных интерфейсов, таких как I2C, SPI для приборов учета нового типа), преобразование данных в соответствии с алгоритмом ГОСТ 28147–89 (алгоритм приведен выше) и передача в центр сбора информации по проводному интерфейсу, использование беспроводных интерфейсов для передачи данных внутри одного объекта при дополнительном использовании GSM или Wi-Fi модуля передачи данных (рис. 1).

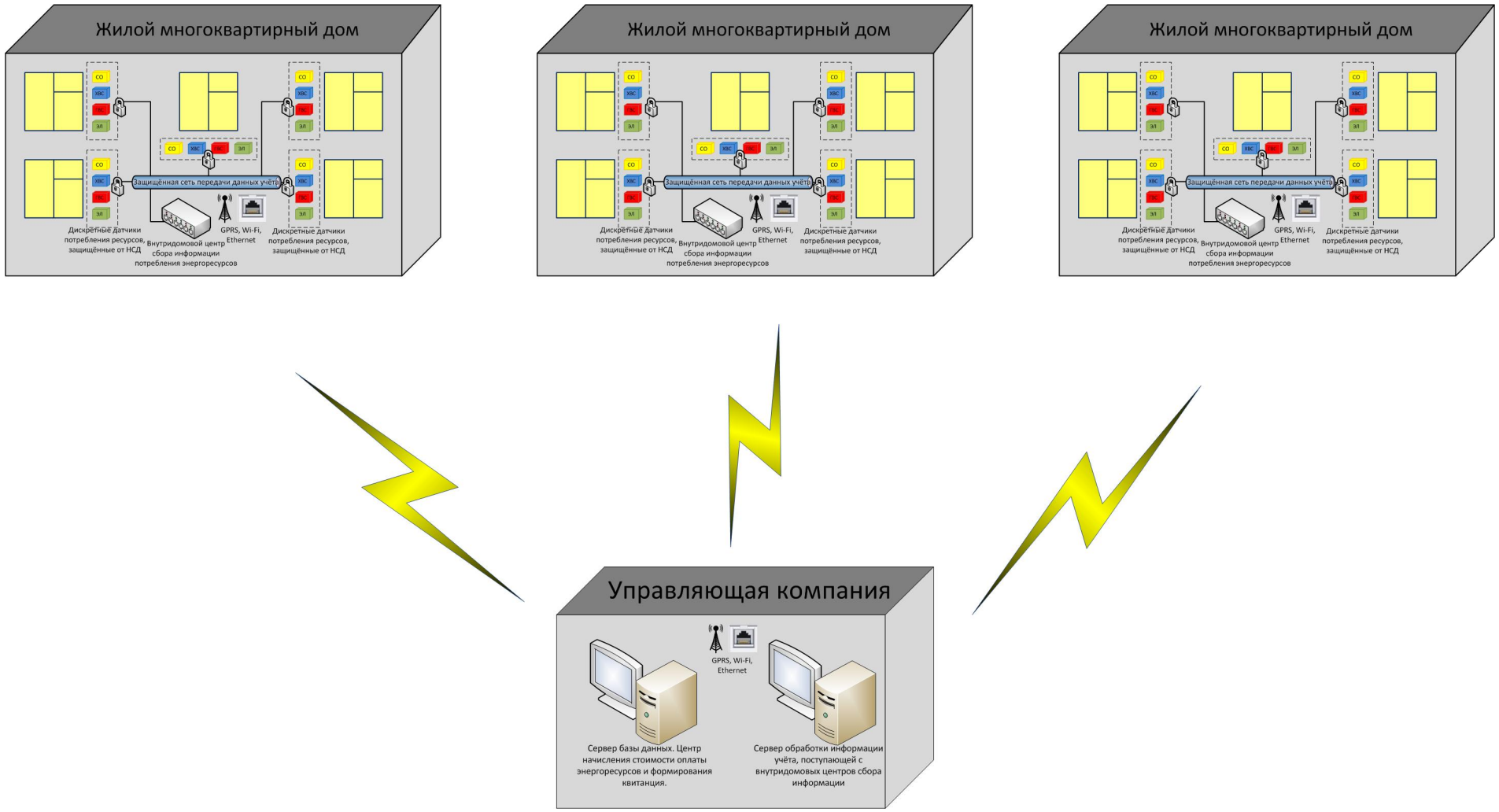

Рис. 1. Базовая структура сети

Настройка параметров модуля осуществляется при монтаже системы.

В модуле предусматривается автономное питание от батареи, что позволяет использовать его со всеми типами счетчиков (в том числе теми, где использование общественной сети электропитания является невозможным в соответствии с требованиями). Расчетное время работы от батареи 5 лет (исходя из диапазона рабочих температур 0…+40 °С).

Центр сбора и обработки информации построен на базе микроконтроллера. В состав прибора входит GSM модуль приема/передачи информации (с возможностью работы по беспроводному каналу связи по протоколу GPRS). Центр сбора информации производит периодический мониторинг подключенных модулей приборов учета, осуществляет сбор данных о потреблении и их передачу диспетчерскому центру с использованием криптографического алгоритма по ГОСТ 28147–89.

Алгоритмом работы устройства предусматривается рассылка аварийных SMS-сообщений в случае обнаружения сбоев в системе или при попытке несанкционированного доступа к устройству.

Каждый узел системы опечатывается пломбой от НСД и получает уникальный адрес-идентификатор для защиты от отключения.

Модуль для индивидуального прибора учета имеет малые габариты и низкое энергопотребление (размер и габариты определяются использованием микроконтроллера MDR32F9Q2 размером 10×10 мм и статическим потреблением 10 мкА). Модуль конструктивно объединяется корпусом с прибором учета и обеспечивает защиту от несанкционированного доступа. На рис. 2 показан вид устройства со снятой крышкой.

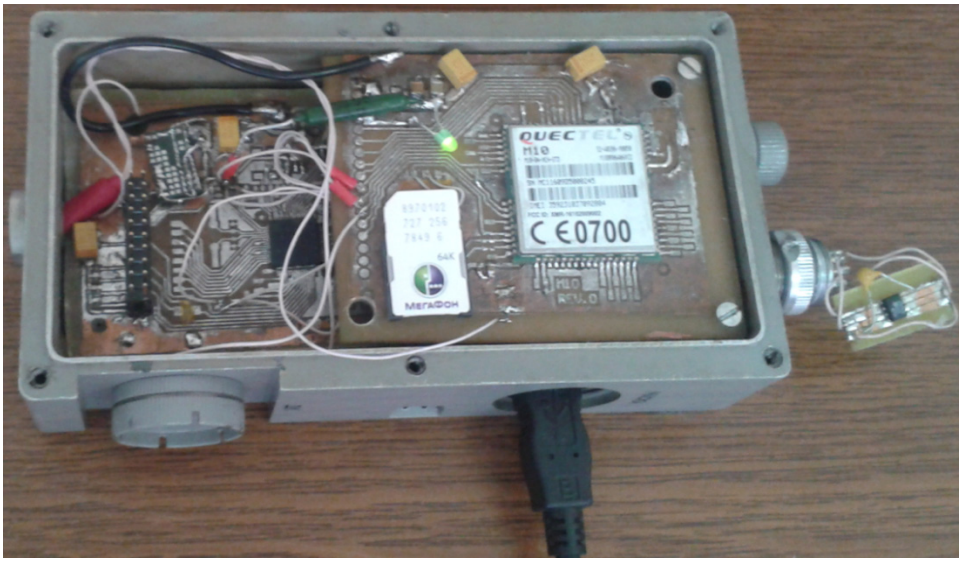

Рис. 2. Вид устройства со снятой крышкой

Макетирование работы устройства на базе контроллера MDR32F9Q2 и GSM-модуля Quectel M10 позволяет сделать вывод о наличии достаточной производительности микроконтроллера для решения задачи обеспечения защищенной передачи данных в системах учета и распределения энергоресурсов.

Характеристики и преимущества:

– использование отечественного микроконтроллера обеспечивает независимость от внешних поставщиков и позволяет использовать устройство для техники специального назначения;

– низкая стоимость комплектующих изделий и высокая аппаратная гибкость платформы позволяют использовать устройство как для индивидуального бытового применения, так и для промышленных комплексов;

– программная среда может быть адаптирована в короткие сроки для любого типа оборудования управления по требованию заказчика;

– имеется возможность выпуска различных модификаций устройства на базе разработанной платформы, адаптированных для специфических применений заказчиков (например,

по специальному заказу возможно нанесение на корпус устройства гравировок с контактной информацией служб экстренной помощи и телефонов доверия, а также информации рекламного характера).

Вывод

Предлагаемая система учета распределения и энергопотребления обеспечивает бесперебойный контроль, сбор, первичную обработку и передачу информации в вышестоящую автоматизированную систему управления работой энергосистем. Производство подобных систем экономически оправдано, сроки эксплуатации удовлетворяют соответствующим требованиям.

Список литературы

1. Салдыркин, И. В. Учет количества электроэнергии в распределительных сетях 6–10 кВ / И. В. Салдыркин, И. В. Толкачев // Промышленная энергетика. – 2006. – № 10. – С. 2–14.
2. Опыт внедрения АСКУЭ потребителей / С. Г. Лесняк, О. Д. Молчан, Д. Г. Жданов, П. Б. Федотов // Электрические станции. – 2002. – № 5. – С. 68–70.
3. Система мониторинга и учета энергоресурсов. – URL: http://www.ipmce.ru/custom/sensornetworks/products/energo/

Поликарпов Александр Алексеевич
соискатель ученой степени
кандидата технических наук,
Пензенский государственный университет
E-mail: ski10@mail.ru

Polikarpov Aleksandr Alekseevich
applicant for a degree
of candidate of technical sciences,
Penza State University

Юрков Николай Кондратьевич
доктор технических наук, профессор,
заведующий кафедрой
конструирования
и производства радиоаппаратуры,
Пензенский государственный университет
E-mail: yurkov_nk@mail.ru

Yurkov Nikolay Kondrat'evich
doctor of technical sciences, professor,
head of sub-department of radio equipment
design and production,
Penza State University

УДК 621.3.06
Поликарпов, А. А.
Защита данных в автоматизированных системах учета энергоресурсов / А. А. Поликарпов, Н. К. Юрков // Измерение. Мониторинг. Управление. Контроль. – 2013. – № 2(4). – С. 25–29.