УДК 004.771

И.С. Костромин, И.Г. Мищенко, Д.А. Погибельский, Р.З. Хафизов

Варианты реализации защищённого обмена данными в ЖКХ по стандартам DLMS / COSEM с использованием российской криптографии

Представлен обзор текущей ситуации с используемыми протоколами и решениями по защите информации в жилищно-коммунальном хозяйстве. Приведён анализ подхода к криптографической защите информации, изложенный в стандартах DLMS / COSEM, определены проблемы, препятствующие внедрению российских алгоритмов, а также предложены криптографические наборы, расширяющие стандарт DLMS / COSEM и решающие обозначенные проблемы.

Ключевые слова: ЖКХ, стандартизация, криптография, DLMS, COSEM.
doi: 10.21293/1818-0442-2018-21-4-1-47-52

В настоящее время информационные технологии широко внедряются в сферу жилищно-коммунального хозяйства (ЖКХ). В перспективе это приведёт не только к повышению эффективности управления отраслью, но также расширит возможности злоумышленников по организации различного рода атак с целью шантажа, диверсий или совершения террористических актов.

Надёжность системы должна подтверждаться независимыми средствами проверки, что делает ненадёжным или слишком дорогим поддержку проприетарных механизмов безопасности. Это является предпосылкой к стандартизации используемых протоколов и алгоритмов.

Предлагается множество решений с использованием различных криптографических алгоритмов и протоколов [1–5] и архитектур с использованием вспомогательных серверов аутентификации [6–8]. Среди множества концепций выделяется идея использования Blockchain [9, 10].

Но в наше время типовые IoT-системы используют центральные серверы для управления, координации и хранения данных [11].

Одним из наиболее перспективных протоколов взаимодействия в системах сбора данных и управления в ЖКХ является семейство стандартов DLMS/COSEM (IEC 62056) [12].

Стандарты DLMS/COSEM поддерживаются большим количеством производителей приборов учёта, ряд из которых являются российскими (РиМ, Инкотекс, НПО Мир, Миландр, Энергомера). DLMS/COSEM продвигается ПАО «Россети» как единый стандарт для электросчётчиков в Российской Федерации.

В настоящее время эти стандарты не имеют адаптированных под российские требования решений по защите информации. Выработка таких решений является важной задачей стандартизации в области ЖКХ.

Текущая ситуация

Весь путь данных между конечным устройством (счётчиком, датчиком и т.д.) и сервером сбора данных можно условно разделить на 2 различных (с точки зрения технологий передачи данных) сегмента информационной сети.

Внутри объекта сбора данных (жилой дом, промышленное или офисное здание) передача данных ведётся по сети, организованной эксплуатирующей организацией. Наиболее распространёнными технологиями физической передачи данных при этом являются RS-485, Ethernet, беспроводные сети (как с использованием широкополосной связи в гигагерцовом диапазоне типа WiFi, Bluetooth, так и с использованием узкополосной связи в не лицензируемых субгигагерцовых диапазонах типа LoRa, «Стриж» или проприетарных решениях). Передача данных при этом осуществляется от прибора, выполняющего конечный функционал (счётчик, датчик, запорное устройство) к промежуточному устройству сбора и подготовки данных.

От объекта сбора данных информация передаётся на сервер с использованием существующих широкополосных сетей Интернет. Она может передаваться по беспроводным каналам, предоставляемым операторами сотовой связи, либо по проводным, предоставляемым местными провайдерами Интернет. Решения с передачей информации от объекта сбора данных до сервера по сетям, организованным эксплуатирующей организацией, слабо распространены ввиду существенно большей стоимости развёртывания и эксплуатации.

Защита информации в различных сегментах информационной сети также осуществляется различным образом.

Внутри объекта сбора данных в большинстве существующих решений криптографическая защита информации не применяется, данные передаются в открытом виде. Данный подход имеет право на существование в случае сбора данных с промышленных объектов, имеющих одного собственника и чётко определённый регламент доступа к инженерным коммуникациям, – в этом случае можно рассматривать внутреннюю сеть как одну защищённую зону. Однако в случае жилых построек подобный подход не обеспечивает конфиденциальности, достоверности и целостности передаваемых данных.

Для защиты информации, циркулирующей с использованием публично доступных проводных или беспроводных сетей передачи данных, используются стандартные технологии защищённой передачи данных SSL/TLS [13]. Предпосылками такой тенденции является простота реализации стека протоколов для данной технологии на Linux платформах, совместимость с клиентскими и серверными системами. В настоящее время существуют сформулированные стандарты и коммерчески доступные решения по защите информации с использованием TLS и российской криптографии. При соблюдении всех необходимых процедур и наличии необходимого оборудования данный подход обеспечивает достаточный уровень защиты информации. Однако на практике процедуры (генерация и управление ключами, аудит безопасности) игнорируются, а оборудование и программное обеспечение (сертифицированные криптопровайдеры, проверенные версии Linux) заменяются на дешёвые или бесплатные решения, безопасность которых зачастую не обеспечивается.

Таким образом, можно констатировать, что текущая система сбора данных и управления в ЖКХ не защищена от информационных атак, доступных злоумышленникам даже с низкой квалификацией.

В публичном сегменте сети существующие решения обеспечивают иллюзию безопасности, т.к. предлагаемые решения обладают рядом уязвимостей, а скорость исправления известных проблем безопасности недопустимо низка.

Объективная необходимость стандартизации протоколов сбора данных и управления в системе ЖКХ привела к началу внедрения международных стандартов, таких как DLMS/COSEM в сетях управления и сбора данных. Крупные игроки рынка, такие как ПАО «Россети», начинают использование данного решения в своих схемах развёртывания и продвигают его как национальный стандарт.

Защита информации в стандартах DLMS/COSEM

Устройства, выполненные согласно DLMS/COSEM, имеют 3 возможных уровня защиты данных: без ограничений (публичные данные), ограничения доступа по паролю и криптографическая защита данных.

Аспекты, касающиеся доступа к публичным данным и доступа по паролю, не требуют изменений при переходе к требованиям российских государственных регуляторов.

В стандартах DLMS/COSEM криптографическая защита информации вынесена на уровень приложения. Это позволяет использовать различные варианты передачи данных на физическом уровне. В стандарте описаны особенности передачи данных по наиболее распространённым промышленным интерфейсам RS-485 и Ethernet.

Так как защита информации инкапсулируется на уровне приложения, то возможна организация сквозного (end-to-end) шифрования чувствительных данных. Это позволит не накладывать дополнительных требований на промежуточные звенья передачи данных – возможно использование или отсутствие любых дополнительных уровней защиты (MacSec, IPsec, SSL/TLS) с использованием как российских, так и зарубежных криптографических алгоритмов, что не снизит общий уровень защищённости.

Используемые криптографические алгоритмы в стандартах DLMS/COSEM определены в так называемых криптографических наборах. Эти наборы описывают преобразования, используемые для шифрования, цифровой подписи, согласования ключей, хэш-функции и передачи ключей.

В текущей версии стандарта определяется 2 набора криптографических алгоритмов: на основе шифра AES и эллиптической криптографии. Остальные наборы криптографических преобразований могут быть определены в дальнейшем.

Данная архитектура документа позволяет легко адаптировать его для использования новых криптографических стандартов или механизмов.

Проблемы применения DLMS/COSEM

Несмотря на то, что зафиксированные в существующих криптографических наборах DLMS/COSEM алгоритмы близки к российским, механическая замена зарубежных алгоритмов российскими не представляется возможной по нескольким причинам: используемый режим криптографического преобразования, длина блока блочного шифра, подход к использованию ключей, полученных в результате согласования по алгоритмам Диффи–Хеллмана.

По длине блока и длине ключа алгоритм ГОСТ Р 34.12-2015 «Кузнечик» соответствует используемому в существующих криптографических наборах AES-256. Миграция с одного алгоритма на другой при соответствии этих параметров представляет наименьшую сложность – в протоколе одно криптографическое преобразование может быть заменено на другое. Препятствием для использования только алгоритма «Кузнечик» является его слабая поддержка производителями средств криптографической защиты информации для коммерческого использования.

Также проблемы возникают при использовании наиболее распространённой схемы с сессионным симметричным ключом, выводимым по процедуре согласования ключа из асимметричных ключей по алгоритму Диффи–Хеллмана. Данная схема в неизменном виде не соответствует DLMS/COSEM. В стандарте описаны возможности вывода ключа согласования для замены ключей и криптографическая схема с эфемерными ключами.

В схеме с эфемерными ключами симметричный ключ вырабатывается для каждого сообщения индивидуально. Эта схема является простой и надёжной, но требует большого объёма вычислений, что для дешёвых устройств с низкой производительностью обернётся высоким временем выполнения команд.

Другой проблемой представляется использование в существующих криптографических наборах

режима GCM (Galois/Counter Mode счётчик с аутентификацией Галуа). Процедура получения шифротекста в этом режиме соответствует таковой в режиме гаммирования, описанном в ГОСТ Р34.13-2015. Однако параллельно с вычислением шифротекста ведётся вычисление имитовставки, причём для этого вычисления используется тот же ключ, что и для шифрования. Различия между режимами наглядно показаны на рис. 1. (Обозначения: IV – инициализационный вектор; I_n – дополненный инициализационный вектор; $CTR_{1,2}$ – значения счётчика; $P_{1,2}$ – значения открытого текста; $C_{1,2}$ – значения шифротекста; T_S – результаты шифрования блока; Auth – аутентификационное сообщение; Len – длина обработанного сообщения; MAC – имитовставка; e_K – шифрование на ключе K; mult – преобразование (умножение) Галуа с ключом хэширования H).

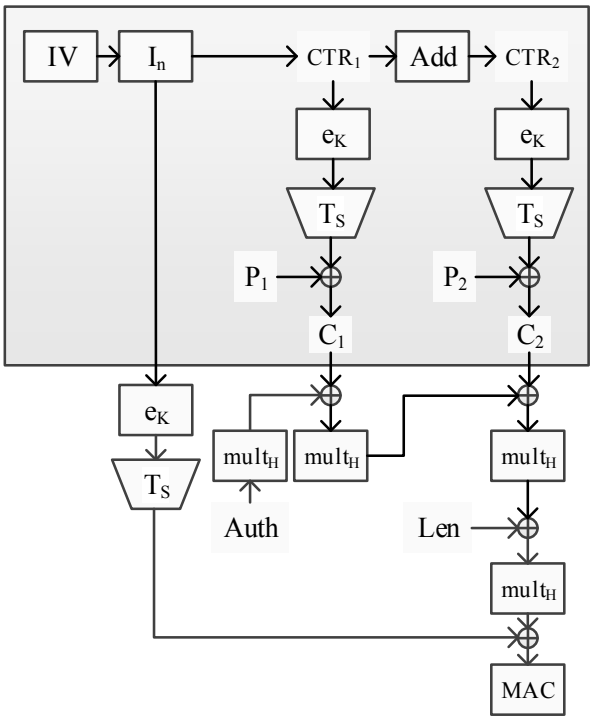

Рис. 1. Различия между алгоритмами «гаммирование» и «счётчик с аутентификацией Галуа», в сером прямоугольнике – общая часть

ГОСТ Р 34.13-2015 описывает только один возможный вариант вычисления имитовставки («режим выработки имитовставки»), соответствующий CMAC в зарубежной литературе. При этом «настоятельно не рекомендуется» для вычисления имитовставки использовать тот же ключ, что и для шифрования.

Предлагаемое решение

На основании спецификаций DLMS/COSEM [14, 15], а также в ходе консультаций с участниками ТК26 были выработаны предложения по расширению списка криптографических наборов, которые позволят создать устройства, обеспечивающие безопасность передаваемых данных с использованием российских криптографических алгоритмов.

Использование одного ключа для формирования имитовставки и шифротекста недопустимо. Чтобы не вводить дополнительного ключа, не имеющего своего отражения в DLMS/COSEM, было предложено использовать существующий ключ аутентификации K_{GAK}. Уровень нагрузки на этот ключ допускает его использование для этих целей как для алгоритма «Кузнечик», так и для алгоритма «Магма». Возможность обновления ключей на независимом ключе шифрования ключей K_{KEK} позволяет дополнительно контролировать нагрузку на ключ.

Конфиденциальность сообщения обеспечивается шифрованием открытой команды в режиме гаммирования на сессионном ключе.

Целостность сообщения выполняется в режиме выработки имитовставки (CMAC) на ключе K_{GAK}.

Информационный обмен начинается с процесса генерации сессионного ключа, на котором в дальнейшем будет закрыт безопасный канал. Процесс согласования безопасного канала соответствует описанному в DLMS.

Данный процесс состоит из 4 шагов (все данные при передаче защищаются на глобальных ключах шифрования K_{GUEK} и аутентификации K_{GAK}):

1. Клиент случайным образом генерирует сессионный ключ SK и случайное число, после чего передаёт их серверу.
2. Сервер расшифровывает запрос и извлекает сессионный ключ SK, после чего передаёт клиенту своё случайное число.
3. Клиент проверяет правильность ответа, подготавливает параметры безопасного канала и отправляет их серверу.
4. Сервер проверяет допустимость параметров, формирует подтверждающее сообщение и отправляет его клиенту.

Криптографическая защита информации в зависимости от значения управляющего байта может состоять из только защиты целостности (рис. 2), только защиты конфиденциальности (рис. 3) либо защиты и целостности и конфиденциальности (рис. 4). Обозначения на рисунках: Tag, Len – тег и длина команды; SC – security control; IC – счётчик сообщений; P – команда в открытом виде; Sys-T – system title (уникальный код устройства DLMS); MAC – имитовставка сообщения; AK – ключ K_{GAK}; SK – сессионный ключ; C – команда в зашифрованном виде.

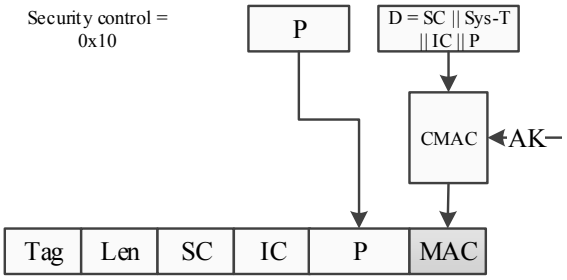

Рис. 2. Схема с защитой только целостности команды DLMS/COSEM

Для использования асимметричной криптографии последовательность действий несколько отличается.

Было предложено решение, не противоречащее спецификации DLMS/COSEM и позволяющее использовать асимметричную криптографию однократно при установлении сессии. Для этого выполняется согласование ключа обновления ключей на основании асимметричной криптографии, после чего клиент генерирует и загружает в сервер (обновляет) комплект симметричных ключей. В дальнейшем схема аналогична схеме для симметричной криптографии.

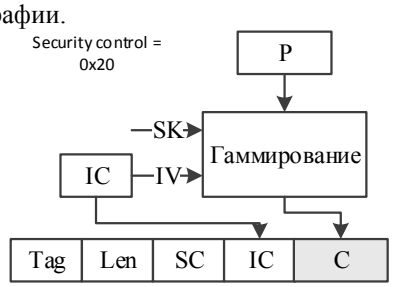

Рис. 3. Схема с защитой только конфиденциальности команды DLMS/COSEM

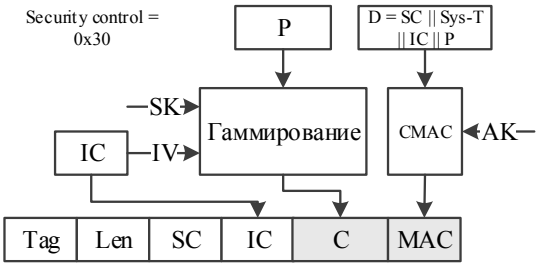

Рис. 4. Схема с защитой только целостности команды DLMS/COSEM

Это позволяет снизить вычислительную нагрузку на удалённое устройство (сервер), при этом сохранив высокий уровень защищённости и удобства при использовании асимметричной криптографии.

Предлагаемые криптографические наборы с использованием российской криптографии сведены в таблицу.

Предлагаемые криптографические наборы DLMS/COSEM

Индекс набора	Имя набора	Шифрование	Цифровая подпись	Согласование ключа	Хэш-функция	Передача ключей
3	KUZ-256	«Кузнечик» (ГОСТ Р 34.12–2015), 256 бит	–	–	–	«Кузнечик» (ГОСТ Р 34.12–2015), 256 бит
4	G341012-KUZ-256-STR-256	«Кузнечик» (ГОСТ Р 34.12–2015), 256 бит	ГОСТ Р 34.10–2012 на эллиптических кривых	ГОСТ Р 34.10-2012 на эллиптических кривых	«Стрибог» ГОСТ Р 34.11–2012, 256 бит	«Кузнечик» (ГОСТ Р 34.12–2015), 256 бит
5	MAG-256	«Магма» (ГОСТ Р 34.12–2015), 256 бит	–	–	–	«Магма» (ГОСТ Р 34.12–2015), 256 бит
6	G341012-MAG-256-STR-256	«Магма» (ГОСТ Р 34.12–2015), 256 бит	ГОСТ Р 34.10–2012 на эллиптических кривых	ГОСТ Р 34.10-2012 на эллиптических кривых	«Стрибог» ГОСТ Р 34.11–2012, 256 бит	«Магма» (ГОСТ Р 34.12–2015), 256 бит

Заключение

Предлагаемое решение позволяет использовать российские криптографические алгоритмы в системах сбора данных, основанных на стандартах DLMS/COSEM. Возможность выбора используемого криптографического набора позволит использовать предполагаемое решение в широком круге устройств.

Литература

1. Choo K.-K.R. Cryptographic Solutions for Industrial Internet-of-Things. Research Challenges and Opportunities / K.-K.R. Choo, S. Gritzalis, J.H. Park // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14(8). – P. 3567–3569.

2. Keke G. Blend Arithmetic Operations on Tensor – Based Fully Homomorphic Encryption Over Real Numbers / G. Keke, Q. Meikang // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3590–3598.

3. Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things / D. He, M. Ma, Sh. Zeadally, N. Kumar, K. Liang // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14(8). – P. 3618–3627.

4. Lightweight Searchable Public - Key Encryption for Cloud – Assisted Wireless Sensor Networks / P. Xu, Sh. He, W. Wang, W. Susilo, H. Jin // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3712–3723.

5. File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things / R. Zhou, X. Zhang, X. Du, X. Wang, G. Yang, M. Guizani // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3648–3658.

6. A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things / X. Li, J. Niu, Md Z.A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3599–3609.

7. Karati A. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments / A. Karati, SK H. Islam, M. Karuppiah // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3701–3711.

8. A Novel Latin-Square-Based Secret Sharing for M2M Communications / J. Shen, T. Zhou, X. Liu, Y.-C. Chang // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 14 (8). – P. 3659–3668.

9. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks / P.K. Sharma, S. Singh, Y.-S Jeong, J.H. Park // IEEE Communications Magazine. – 2017. – Vol. 55. – P. 78–85.

10. DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network / P.K. Sharma, S. Rathore, J.H. Park // IEEE Consumer Electronics Magazine. – 2018. – Vol. 7 (4). – P. 55–64.

11. Kim D.-Y. Remote Software Update in Trusted Connection of Long Range IoT Networking Integrated with Mobile Edge Cloud / D.-Y. Kim, S. Kim, J. H. Park // IEEE Access. – 2017. – Vol. 6. – P. 66831–66840.

12. Конев А.А. Модуль аутентификации в системах интернета вещей / А.А. Конев, Д.С. Никифоров, А.В. Шилер // Информационные и управляющие системы на транспорте и в промышленности: матер. II Всерос. науч.-техн. конф. – Омск, 2018. – С. 141–149.

13. Антонов М.М. Организация защищенной гетерогенной сети в автоматизированных системах коммерческого учета энергоресурсов / М.М. Антонов, А.А. Конев, Д.С. Никифоров, С.А. Черепанов // Доклады ТУСУР. – 2016. – Т. 19, №3. – С. 107–110.

14. DLMS User Association, Blue book, COSEM interface classes and OBIS identification system. Ed. 12.2 [Электронный ресурс]. – Режим доступа: https://www.dlms.com/files/Blue-Book-Ed-122-Excerpt.pdf, свободный (дата обращения: 16.12.2018).

15. DLMS User Association, Green book, DLMS/COSEM Architecture and Protocols. Ed. 8.3 [Электронный ресурс]. – Режим доступа: https://www.dlms.com/files/Green-Book-Ed-83-Excerpt.pdf, свободный (дата обращения: 16.12.2018).

Костромин Игорь Сергеевич
Нач. отд. встраиваемого программного обеспечения
ЦППО АО «ПКК Миландр»
Георгиевский пр-т., д. 5, Зеленоград, г. Москва, Россия, 124498
Тел.: +7 (495-9) 81-54-33, доб. 572
Эл. почта: kostromin.i@milandr.ru

Мищенко Игорь Геннадьевич
Нач. отд. интеграционных систем ЦППО
АО «ПКК Миландр»
Георгиевский пр-т., д. 5, Зеленоград, г. Москва, Россия, 124498
Тел.: +7 (495-9) 81-54-33, доб. 433
Эл. почта: mishchenko.i@milandr.ru

Погибельский Дмитрий Александрович
Канд. физ.-мат. наук, рук. лаб. сложных
организационно-технологических систем МФТИ
Институтский пер., д. 9, г. Долгопрудный,
Московская обл., Россия, 141701
Тел.: +7-916-852-88-80
Эл. почта: Pogibelskii.da@mipt.ru

Хафизов Рашит Закирович
Канд. физ.-мат. наук, зам. ген. директора
по стратегическому планированию и маркетингу
АО «ПКК Миландр»
Георгиевский пр-т., д. 5, Зеленоград, г. Москва, Россия, 124498
Тел.: +7 (495-9) 81-54-33, доб. 115
Эл. почта: hafizov.r@milandr.ru

Kostromin I.S., Mishchenko I.G.,
Pogibelskiy D.A., Khafizov R.Z.

Variants of secure data exchange implementation in housing and communal services according to DLMS/COSEM standards using Russian cryptography

In this paper the authors review a commonly used protocols and security concepts, that are used in housing in Russia. Main problems to implement Russian domestic cryptography in DLMS / COSEM systems and defined a solution that could met requirements from DLMS / COSEM standard are specified as well as a security requirements from Russian government.

Keywords: housing, standardization, cryptography, DLMS, COSEM.
doi: 10.21293/1818-0442-2018-21-4-1-47-52

References

1. Choo K.-K.R.; Gritzalis, S.; Park J.H. Cryptographic Solutions for Industrial Internet-of-Things. Research Challenges and Opportunities. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14(8), pp. 3567–3569.

2. Keke, G.; Meikang, Q. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3590–3598.

3. He, D.; Ma, M.; Zeadally, S.; Kumar, N.; Liang, K. Certificateless Public Key Authenticated Encryption with Keyword Search for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3618–3627.

4. Xu, P., He, S., Wang W., Susilo W., Jin H. Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3712–3723.

5. Zhou R., Zhang X., Du X., Wang X., Yang G., Guizani M. File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3648–3658.

6. Li X., Niu J., Bhuiyan Md Z.A., Wu F., Karuppiah M., Kumari S. A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3599–3609.

7. Karati A., Islam SK.H., Karuppiah M. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environment. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3701–3711.

8. Shen J., Zhou T., Liu X., Chang Y.-C. A Novel Latin-Square-Based Secret Sharing for M2M Communications. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14 (8), pp. 3659–3668.

9. Sharma P.K., Singh S., Jeong Y.-S., Park J.H. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Communications Magazine*, 2017, vol. 55 (9), pp. 78–85.

10. Sharma P.K., Rathore S., Park J.H. DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network. *IEEE Consumer Electronics Magazine*, 2018, vol. 7 (4), pp. 55–64.

11. Kim D.-Y., Kim S., Park J. H. Remote Software Update in Trusted Connection of Long Range IoT Networking Integrated with Mobile Edge Cloud. *IEEE Access*, 2017, vol. 6, pp. 66831–66840.

12. Konev A.A., Nikiforov D.S., Shiler A.V. Authentication module in internet systems of things. *Information and control systems in transport and industry*, Omsk, 2018, pp. 141–149.

13. Antonov M.M., Konev A.A., Nikiforov D.S., Cherepanov S.A. Development of a protected network for an automated system of energy control and accounting. *Proceedings of TUSUR University*, 2016, pp. 107–110 (in Russ.).

14. *DLMS User Association, Blue book, COSEM interface classes and OBIS identification system.* Ed. 12.2 [Electronic resource]. Available at: https://www.dlms.com/files/Blue-Book-Ed-122-Excerpt.pdf, свободный (accessed: December 16, 2018).

15. *DLMS User Association, Green book, DLMS/COSEM Architecture and Protocols.* Ed. 8.3 [Electronic resource]. Available at: https://www.dlms.com/files/Green-Book-Ed-83-Excerpt.pdf, свободный (accessed: December 16, 2018).

Igor S. Kostromin
Head of embedded software department, Milandr company,
5, Georgievskiy pr., Zelenograd, Moscow, 124498
Phone: +7 (495-9) 81-54-33, ext. 572
Email: kostromin.i@milandr.ru

Igor G. Mishchenko
Head of integration software department, Milandr company,
5, Georgievskiy pr., Zelenograd, Moscow, 124498
Phone: +7 (495-9) 81-54-33, ext. 433
Email: mishchenko.i@milandr.ru

Dmitriy A. Pogibelskii
Candidate of Physics and Mathematics,
Head of the Laboratory for Complex systems, MIPT
9, Institutskiy per., Dolgoprudny, Moscow Region, 141701
Phone: +7-916-852-88-80
Email: Pogibelskii.da@mipt.ru

Rashit Z. Khafizov
Candidate of Physics and Mathematics,
Deputy general director for strategic planning and marketing, Milandr company,
5, Georgievskiy pr., Zelenograd, Moscow, 124498
Phone: +7 (495-9) 81-54-33, ext. 115
Email: hafizov.r@milandr.ru