10. Kuznecov A.A., Permyakov S.A., Sushkova L.T. Izuchenie vzaimosvyazi pokazatelej variabel'nosti diagramm ritma serdca i diagramm amplitud sistolicheskogo potenciala ritma serdca u zdorovyx lyudej [Study of heart rate diagram and systolic amplitude diagram parameters in healthy persons]. *Fizika i radioehlektronika v medicine i ehkologii: Doklady 12-j mezhd. nauchn.-tekhn. kofn., book 1*. [Proc. 12th Int. Conf. "Physics and radioelectronics in medicine and ecology", book 1]. Vladimir, 2016, pp. 294-297
11. Permyakov S.A, Kuznecov A.A., Sushkova L.T. Issledovanie mexanizma sopryazheniya generacii sistolicheskogo potenciala i ritma serdca [Investigation of coupling mechanism of systolic potentical generation and heart rate] *Fiziologiya, medicina, farmakologiya. Vysokie tekhnologii, teoriya, praktika. Sb. statej IV mezhdunarodnoj nauchno-prakticheskoj konferencii «Vysokie tekhnologii, fundamental'nye i prikladnye issledovaniya v fiziologii i medicine»* [Physioligy, medicine, pharmacology. High techonoligies, theory, practice, Proc. 4th Int. Sc.-pract. Conf. «High technologies, fundamental and applied researches in physiology and medicine»]. Saint Petersburg, 2012, pp. 86-88.
12. Kuznecov A.A, Permyakov S.A. O estestvennoj normalizacii diagrammy ritma serdca [About the natural normalization of heart rate diagram]. *Trudy Nizhegorodskogo gosudarstvennogo tekhnicheskogo universiteta im. R.E. Alekseeva*, 2012, vol. 78, no. 4, pp. 363-368.
13. Ventcel' E. S. *Teoriya veroyatnostej: ucheb. dlya vuzov* [Probability theory. Textbook for universities]. Moscow, Vyssh. shkola Publ., 1999. 576 p.
14. Permyakov S.A. e.a. *Analizator funkcional'nogo sostoyaniya organizma* [Analising tool for organism functional state]. Patent RF, no.165751, 2015.

*Received 10.09.2017*

УДК 004.057.4

# МЕТОД АУТЕНТИФИКАЦИИ УСТРОЙСТВ В СЕНСОРНЫХ СЕТЯХ

*Васин Н.Н., Чигирь Р.В.*
*Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ*
*E-male: rwch63@mail.com*

Сенсорные сети (peer-to-peer) предназначены для автоматизации производственных процессов и процессов мониторинга. Поэтому элементы сенсорных сетей характеризуются как наличием централизованного управления, так и возможностью взаимодействия между собой напрямую. Важным критерием работы сенсорной сети является оперативность её реагирования на изменение внешних факторов. Время выполнения служебных операций при взаимодействии сенсоров должно быть минимальным. В настоящей статье рассматриваются известные методы аутентификации, используемые для обеспечения защищенности протекающих процессов обмена сообщениями по сети. Представлен анализ их эффективности, указаны тенденции современного развития протоколов. Определена проблема сравнительно длительного времени аутентификации при использовании существующих методов, а также предложен метод сокращения времени выполнения процедуры аутентификации. Проведен эксперимент и сравнительный анализ быстродействия существующих и предложенного алгоритмов аутентификации, в ходе которого выявлено преимущество предложенного метода, позволившего сократить время аутентификации более чем в семь раз.

***Ключевые слова:*** аутентификация; сенсорные сети; алгоритм

## Введение

Современные сенсорные сети (peer-to-peer) строятся, как правило, на принципе централизованного управления, с элементами самоорганизации, когда сетевые элементы могут взаимодействовать между собой напрямую без обращения к серверам управления. Для корректной работы всей сети требуется обеспечить минимальное время установления сеанса связи между ее структурными элементами. Таким образом, необходима система аутентификации, которая позволяет участникам сети проводить как прямое взаимодействие друг с другом, так и оставаться под контролем централизованного управления с сохранением равной степени защищённости. Для этого требуется и соответствующая процедура аутентификации элементов.

## Методы аутентификации на сенсорных сетях

На практике используются несколько типов аутентификации на сенсорных сетях [1]: ACL (Access Control List), динамическая аутентификация пользователей на основе легковесного

пароля с использованием хэш-функции, двухфакторная аутентификация с смарт-карты или биометрией, аутентификация пользователей в беспроводных сетях на основе криптографии эллиптических кривых.

Протокол ACL использует списки управления доступом [2]. Способ основывается на проверке наличия записи по каждому участнику сети в базе данных (БД) на центральном элементе. В случае наличия записи об участнике в списке проверяются права его доступа и, согласно этим правам, выдается разрешение на установление связи между элементами. Как видно из алгоритма работы данного протокола (см. рис.1), взаимодействие идет через сервер управления, обеспечивая централизованность управления, но при этом автономность данной системы практически отсутствует. На первом этапе клиент «А» отправляет свои данные на сервер для регистрации в сети, сервер сверяет полученные данные от «А» со списками доступа и в ответ выдает подтверждение или отказ в регистрации. После этого «А» отправляет запрос серверу управления на доступ к клиенту «Б». Сервер сверяет полученный запрос со списками доступа и в случае подтверждения прав доступа к «Б» отправляет «А» сеансовый ключ для взаимодействия с «Б».

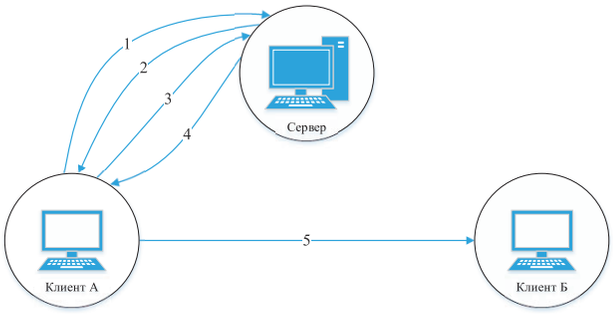


Рис. 1. Алгоритм работы ACL

Протокол динамической аутентификация пользователей на основе легковесного пароля с использованием хэш-функции [3] протекает в несколько этапов (см. рис. 2). На первом этапе происходит регистрация нового абонента в сети: для этого регистрируемый элемент «А» отправляет на центральный сервер свой идентификатор и хэш пароля доступа к запрашиваемой сети и специальной метки. Обрабатывающий шлюз принимает полученную информацию, и данный абонент регистрируется в сети. При этом остальным участникам сети приходит уведомлении о появлении нового элемента «А».

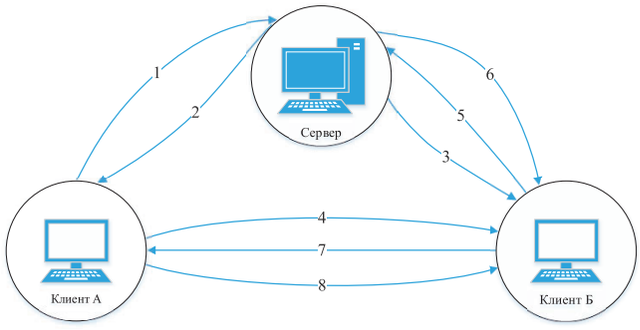


Рис. 2. Алгоритм динамической аутентификации на основе легковесного пароля с использованием хэш-функции

После регистрации узел «А» запрашивает доступ к необходимым для его функционирования другим участникам сети. Получив данный запрос, узел «Б» сенсорной сети перенаправляет его на сервер для проверки подлинности обратившегося элемента «А» и его прав доступа к нему. После проверки центральный узел выдает информацию по запрашиваемым правам доступа и на основании полученных данных делается подтверждение о начале сеанса между конечными элементами сети.

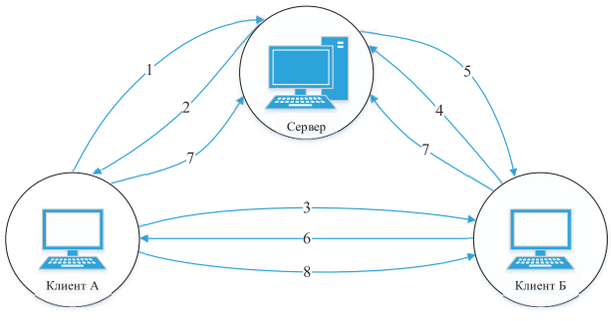


Рис. 3 Алгоритм работы двухфакторной аутентификации

В протоколе с двухфакторной аутентификацией (см. рис. 3) шлюз (сервер управления) создает два мастер-ключа $X$ и $Y$ для клиента «А» и «Б» соответственно [4]. Предполагается, что шлюз и узлы датчиков используют общий долгосрочный общий секретный ключ, вычисляемый как хэш-функция от ключей «А» и «Б» с их метками.

Протокол состоит из этапа регистрации по логину и паролю, фазы аутентификации и фазы обновления пароля. При подключении клиент «А» запрашивает доступ к центральному узлу по открытому каналу. Центральный узел запрашивает подтверждение знания секрета. Клиент «А» преобразует полученную метку и отправляет обратно. Если преобразование верно, клиенту «А» выдается ключ $X$ для взаимодействия с сервером управления.

После этого «А» отправляет запрос доступа к клиенту «Б», передавая свой идентификатор. Абонент «Б» перенаправляет запрос на шлюз с указанием своего идентификатора и идентификатора, полученного от «А». Сервер сверяет права доступа между «А» и «Б» и по результатам в ответ высылает ключ, вычисленный на основе ключей $X$ и $Y$. Затем «Б» передает «А» полученный от сервера новый сеансовый ключ. После получения всеми сторонами сеансового ключа идет уведомление сервера о начале работы «А» и «Б» по сеансовому ключу. По завершении данных процедур начинается обмен данными между «А» и «Б», при котором обе стороны считаются достоверными.

Протоколы двухфакторной аутентификации со смарт-карт или биометрией [5-6] используют вышеописанный метод двухфакторной аутентификации с внесением корректировок на то, что для процедуры регистрации на сервере или же генерирования ID клиента привлекается дополнительная информация со смарт-карты либо используются биометрические данные в качестве своеобразной подписи для формирования индивидуального ключа с более высокими параметрами аутентичности.

Аутентификация пользователей в беспроводных сетях на основе криптографии эллиптических кривых [7] строится на принципах протокола двухфакторной аутентификации, с той разницей, что используется шифрование с более сильной криптографией. Процедуру можно разделить на четыре этапа, а именно: фаза регистрации пользователя в системе, фаза получение обновления информации об участниках сети, фаза аутентификации между конечными узлами и фаза получения сеансового ключа между конечными узлами.

В ходе аутентификации клиент «А» отсылает запрос доступа клиенту «Б». Клиент «Б» перенаправляет запрос на сервер для определения прав доступа. В случае положительного результата проверки клиента «Б» создает сеансовый ключ и передает его абоненту «А». После получения данного ключа абонентом «А» начинается передача данных между конечными узлами «А» и «Б».

Опыт применения вышеописанных типов аутентификации показал их основные недостатки [8-10], заключающиеся в невысокой скорости выполнения процедур и избыточной зависимости от центрального узла, без которого невозможно проведение процедур аутентификации между конечными узлами сенсорной сети, что в большей степени относится к методу аутентификации через списки доступов. Сегодня ведутся проработки алгоритмов в направлении повышения защищенности каналов обмена данных в момент проведения процедуры аутентификации. Также оптимизируются потоки информации между сервером и конечными узлами. Однако алгоритмов, предоставляющих возможность конечным устройствам сенсорной сети проводить процедуру аутентификации без участия посредника и с высокой скоростью выполнения операций, в настоящий момент не создано.

## Предлагаемый алгоритм аутентификации

Разработанный алгоритм аутентификации решает задачу аутентификации узлов сенсорных сетей между собой без участия центрального узла управления, а также позволяет сократить время, необходимое для выполнения данной операции. Для этого необходимо провести в два этапа аутентификации каждого узла на сенсорной сети (см. рис. 4). Сначала элемент «А» регистрируется на центральном сервере, тем самым создавая централизованный канал управления данным узлом. Регистрация проходит путем подтверждения запрашиваемой стороной знания общего секрета через преобразование случайной метки. После чего абонент «А» отсылает свои данные, подтверждающие его права доступа к серверу.

В случае успешного подтверждения сервером данных абонента «А» он отправляет клиенту «А» его идентификатор (ID), определяющий данного абонента в сети, создаются уникальные клиентские пароли для централизованного канала управления, а также регистрирующемуся абоненту передаётся информация об уже зарегистрированных участниках сети.

Далее происходит установление сеанса между зарегистрированным узлом «А» и абонентом «Б», находящимся в сети, с которым необходимо связаться. Для этого абонент «А» отсылает запрос доступа на узел «Б», одновременно запрашивая его ID. Получив данный запрос, клиент «Б» отправляет свой ID. После чего передает тестовую метку абоненту «А» для проверки его подлинности путем подтверждения знания общего секрета. Метка преобразовывается узлом «А» и передается обратно. Если все процедуры выполнены корректно, то вырабатывается сеансовый ключ между конечными узлами «А» и «Б».

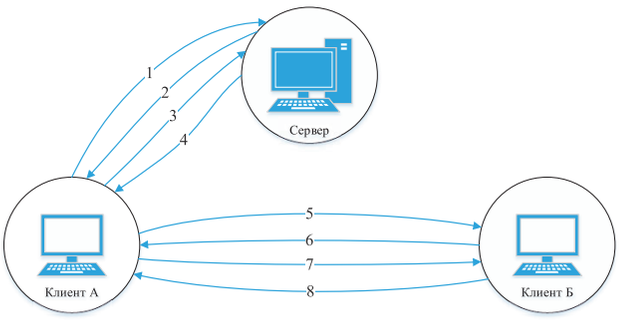


Рис. 4. Предлагаемый алгоритм аутентификации между узлами сенсорной сети

## Результаты экспериментального сравнения эффективности алгоритмов

В ходе изучения быстродействия алгоритмов аутентификации на сенсорных сетях был поставлен эксперимент по их сравнительному анализу. Аутентификация проводилась между узлами, уже зарегистрированными в сети. Таким образом, не учитывалось время, затрачиваемое сенсором при первичном подключении к сети, а лишь измерялось время, необходимое для проведения процедуры аутентификации между конечными узлами. Результаты тестирования отображены в таблице 1, приведенной ниже.

Таблица 1. Сравнительный анализ затрачиваемого времени на выполнение процедуры аутентификации между конечными узлами

| Исследуемый алгоритм аутентификации | Время аутентификации |
|---|---|
| ACL | 106 мс |
| На основе легковесных паролей | 60 мс |
| Двухфакторная аутентификация | 60 мс |
| На основе эллиптических кривых | 60 мс |
| Предложенный алгоритм аутентификации | 8 мс |

По результатам эксперимента выявлено, что применяемые в настоящее время методы аутентификации не имеют временных преимуществ относительно друг друга, так как в их основе используются схожие принципы работы. Алгоритм аутентификации по спискам доступа показывает самые плохие временные показатели, так как вся процедура аутентификации проходит через сервер управления. Разработанный алгоритм аутентификации показывает наилучшие результаты по быстродействию. Сравнительный анализ показывает, что предлагаемый алгоритм имеет выигрыш по быстродействию более чем в семь раз.

## Заключение

Разработанный метод проведения аутентификации элементов сенсорных сетей позволяет снизить нагрузку на центральный узел сети, тем самым повышая автономность его работы. Обеспечивается высокая отказоустойчивость сети, так как нагрузка распределяется между всеми элементами сети. Данный алгоритм обладает наивысшими показателями быстродействия среди проанализированных. По завершении процедуры аутентификации реализуется рабочая автономная система с возможностью централизованного управления. Таким образом, предлагаемый алгоритм отвечает всем требованиям, предъявляемым для работы на сенсорных сетях.

## Литература

1. Куан Ж., Чунминг Т., Ксиангхан Ж., Чунминг Р. Безопасный протокол аутентификации пользователей для сети датчиков при захвате данных. Журнал облачных компьютерных вычислений, систем и приложений. №4:6, 16 февраля 2015 // URL: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-015-0030-z (д.о. 10.02.2017). doi: 10.1186/s13677-015-0030-z.
2. Списки управления доступом (ACL) и правила уровня связывания ACL. Центр знаний IBM. Посл. обновл. 12. 2013 // URL: http://www.ibm.com/support/knowledgecenter/ru/SSRS7Z_8.5.0/com.ibm.programmingcm.doc/dcmcm035.htm (д.о. 13.02.2017).
3. Шах И.Д., Гала Ш.Х., Шекокар Н.М. Легковесный протокол аутентификации, используемый в беспроводной сенсорной сети. Материалы МНК «Схемы, системы, коммуникационные и информационные технологии применения (CSCITA)», опубл. 19.06.2014 // URL: http://ieeexplore.ieee.org/document/6839249/ (д.о. 15.02.2017). doi: 10.1109/CSCITA.2014.6839249.
4. Ньянг Дае-Хан, Ли Мун-Ку. Совершенствование двухфакторного протокола аутентификации Даса в безпроводных сенсорных сетях. Архив по криптологии ePrint. Доклад № 631, 21.12. 2009 // URL: http://eprint.iacr.org/2009/631.pdf (д.о. 21.02.2017).
5. Лал Дас М. Двухфакторная аутентификация пользователей в беспроводных сенсорных сетях // Труды IEEE по беспроводной связи.

№8 (3), 16.03.2009 // URL: http://ieeexplore.ieee.org/abstract/document/4801450/ (д.о. 21.02.2017). doi: 10.1109/TWC.2008.080128.
6. Юань Д., Джианг Ч., Янг Ж. Аутентификация пользователей по биометрической базе на беспроводных сенсорных сетях // Журнал Естественных Наук университета Вухань. Т.3, №15, 2010. – С. 272-276. doi: 10.1007/s11859-010-0318-2.
7. Венбо Ш, Гонг П. Новый протокол аутентификации пользователей в беспроводных сенсорных сетях на основе криптографии эллиптических кривых. Журналы SAGE. 01.01. 2013 // URL: http://journals.sagepub.com/doi/full/10.1155/2013/730831 (д.о. 7.03.2017). doi: 10.1155/2013/730831.
8. Хан М.К., Альхазбар Х. Криптоанализ и улучшение безопасности «двухфакторной аутентификации пользователей в беспроводных сенсорных сетях» // Сенсоры. Т.3, №10, 2010. – С. 2450-2459. doi: 10.3390/s100302450.
9. Сю-Лянь Йе, Тянь-Хо Чен, Пинь-Чуань Лю, Тай-Ху Ким, Синь-Уэн Вей. Протокол обеспечения аутентификации в беспроводных сенсорных сетях на основе криптографии эллиптических кривых // Сенсоры. Т.5, №11, 2011. –С. 4767-4779. doi: 10.3390/s110504767.
10. Хан В. Уязвимости защищенного протокола аутентификации в беспроводных сенсорных сетях на основе криптографии эллиптических кривых. Архив по криптологии ePrint. Доклад №293, 15.05.2014 // URL: http:// eprint.iacr.org/2011/293. (д.о. 21.03.2017).

*Получено 28.06.2017*

**Васин Николай Николаевич**, д.т.н., профессор, заведующий Кафедрой систем связи (СС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-846-332-08-05. E-mail: vasin@psuti.ru

**Чигирь Роман Викторович**, аспирант Кафедры СС ПГУТИ. Тел. 8-927-603-20-38. E-mail: rwch63@mail.ru

## DEVICE AUTHENTICATION METHOD FOR SENSOR NETWORKS

*Vasin N.N., Chigir R.W.*
*Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia*
*E-mail: rwch63@mail.com*

Peer-to-peer sensor networks are used for autonomous operation control and monitoring. The elements of sensor network are required to interact both with a central controller and with each other. An important characteristic of sensor network is its adaptation speed when responding to external changes. When performing service operations interaction time between sensors should be minimal. In this article, existing authentication methods currently utilized to protect information exchange in the network are examined. The results of an analysis of their effectiveness are presented, along with the tendencies of modern protocols evolution. The problem of a relatively long authentication time when using existing methods is identified, and a solution for its shortening is proposed. The results of an experiment and comparative analysis of the authentication speed for both existing and proposed algorithms are presented, which show the advantage of the proposed method that leads to shortening of authentication time by more than 7 times.

***Keywords:*** authentication; sensor networks; algorithm

**DOI:** 10.18469/ikt.2017.15.3.09

**Vasin Nicolai Nicolaevich**, Povolzhsky State University of Telecommunication and Informatics, 23 Lev Tolstoy str., Samara 443010, Russian Federation; the Head of Department of Communication Systems, Doctor of Technical Science, Professor. Tel. +78463320805. E-mail: vasin@psuti.ru

**Chigir Roman Wiktorovich**, Povolzhsky State University of Telecommunication and Informatics, 23 Lev Tolstoy str., Samara 443010, Russian Federation; PhD Student of the Department of Communication Systems. Tel. +79276032038. E-mail: rwch63@mail.ru.

**References**

1. Quan Zh., Chunming T., Xianghan Zh., Chunming R.A secure user authentication protocol for sensor network in data capturing. *Journal for Cloud Computing*, 2015, vol. 4, no. 6. doi: 10.1186/s13677-015-0030-z.
2. Access control lists (ACL) and ACL binding level rules. IBM Knowledge Center. (In Russian) Available at: http://www.ibm.com/support/knowledgecenter/ru/SSRS7Z_8.5.0/com.ibm. programmingcm.doc/dcmcm035.htm (accessed 13.02.2017).
3. Shah M.D., Gala Sh.N., Shekokar N.M. Lightweight authentication protocol used in Wireless Sensor Network. *International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)*, 2014, pp. 138-143. doi: 10.1109/CSCITA.2014.6839249.
4. DaeHun Nyang, Mun-Kyu Lee. Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks. *Cryptology ePrint Archive. Report 2009/631*. Available at: http://eprint.iacr.org/2009/631.pdf (accessed 21.02.2017).
5. Das M.L. Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2009, vol. 8, no. 3. doi: 10.1109/TWC.2008.080128.
6. Yuan J., Jiang Ch., Jiang Z. A biometric-based user authentication for wireless sensor networks. *Wuhan University Journal of Natural Sciences*, 2010, vol. 15, no. 3, pp. 272-276. doi: 10.1007/s11859-010-0318-2.
7. Wenbo Shi, Gong P.A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *SAGE journals*, 2013. doi: 10.1155/2013/730831
8. Khan M.K., Alghathbar K. Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'. *Sensors*, 2010, vol. 10, no. 3, pp. 2450-2459. doi: 10.3390/s100302450.
9. Hsiu-Lien Yeh, Tien-Ho Chen, Pin-Chuan Liu, Tai-Hoo Kim, Hsin-Wen Wei. A Secured Autentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors*, 2011, vol. 11, no. 5, pp. 4767-4779. doi: 10.3390/s110504767.
10. Han W. Weakness of a Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Cryptology ePrint Archive. Report 2011/293*. Available at: http://eprint.iacr.org/2011/293 (accessed 21.03.2017).

*Received 28.06.2017*

# ТЕХНОЛОГИИ РАДИОСВЯЗИ, РАДИОВЕЩАНИЯ И ТЕЛЕВИДЕНИЯ

УДК 621.396

## ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ СИСТЕМ РАДИОСВЯЗИ С ОРТОГОНАЛЬНЫМ ЧАСТОТНЫМ МУЛЬТИПЛЕКСИРОВАНИЕМ СИГНАЛОВ НА ОСНОВЕ ИХ ЭКСТРАПОЛЯЦИИ ПО КАЛМАНУ

*Воронков Г.С., Кузнецов И.В., Султанов А.Х.*
*Уфимский государственный авиационный технический университет, Уфа, РФ*
*E-mail: voronkov.gs@net.ugatu.su*

В статье рассмотрен вопрос энергоэффективности систем подвижной радиосвязи. Предложен метод ее повышения на основе дифференциального преобразования сигналов систем, использующих ортогональное частотное мультиплексирование, с использованием экстраполяции сигналов. Сформулированы требования к экстраполятору, предложена структурная схема формирования и приёма сигналов, реализующая указанный метод. Показано, что в качестве экстраполятора может быть использован фильтр Калмана, представлена математическая формулировка задачи его синтеза. Получено решение дифференциального уравнения фильтра Калмана для сигналов синфазного и квадратурного каналов для случая синхронной работы системы. Показана ортогональность разностных сигналов. Получено условие устойчивости системы восстановления сигналов, показано, что условие выполняется для полученного решения. Продемонстрировано повышение энергоэффективности системы HSPA+ при использовании предложенного метода. На примере усилителей производства компании Analog Devices показано, что использование предложенного метода позволяет снизить мощность, потребляемую оконечным усилительным каналом передатчика, что увеличивает время автономной работы систем беспроводной связи.

***Ключевые слова:*** дифференциальное преобразование сигналов, экстраполяция сигналов, фильтр Калмана, повышение энергоэффективности, уменьшение динамического диапазона, системы беспроводной связи OFDM