УДК 004.021 DOI: 10.26102/2310-6018/2020.28.1.002

Разработка беспроводной системы управления на основе концепции «интернет вещей»

А.И. Афанасьев, В.Н. Князев
ФГБОУ ВО «Пензенский государственный университет», Пенза, Российская Федерация

Резюме: В статье рассмотрены актуальные вопросы и проблемы разработки беспроводных систем управления на основе концепции «Интернет вещей» («Internet of Things» – IoT). В качестве важных проблем выделены недостаточная гибкость и оперативность выбора каналов связи для передачи данных, недостаточная защищенность каналов связи и предложены способы решения данных проблем. Научная новизна заключается в разработке адаптивного алгоритма выбора канала для передачи данных, отличающегося от известных алгоритмов более высокой гибкостью и надежностью. Гибкость (адаптивность) алгоритма заключается в автоматическом выявлении доступных каналов, а надежность – в обеспечении гарантированной передачи команд управления. Также предложен модифицированный алгоритм шифрования, основанный на комбинированном использовании симметричного алгоритма шифрования ГОСТ 34.12-2015 и ассиметричного алгоритма шифрования на эллиптических кривых, позволяющий повысить уровень надежности защищенного взаимодействия между компонентами системы управления при обеспечении достаточной скорости передачи сообщений. Проведено проектирование беспроводной системы управления с применением, в том числе, онтологического и визуального моделирования. Полученные в ходе проведенного исследования результаты использованы в качестве основы при создании аппаратного и программного обеспечения автоматизированной системы управления IoT-устройствами для частного жилого дома.

Ключевые слова: интернет вещей, умный дом, беспроводное взаимодействие, система управления, канал связи, шифрование, онтологическое и визуальное моделирование.

Для цитирования: Афанасьев А.И., Князев В.Н. Разработка беспроводной системы управления на основе концепции «Интернет вещей». *Моделирование, оптимизация и информационные технологии*. 2020;8(1). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/02/AfanasyevKnyazev_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.002

Development of a wireless control system on the basis of «the internet of things» concept

A.I. Afanasiev, V.N. Knyazev
FSBEI OF HE «Penza State University», Penza, Russian Federation

Abstract. In the article it is discussed current issues and problems of developing wireless control systems based on the concept of «Internet of Things». As important problems here there are an insufficient flexibility and efficiency of the choice of communication channels for data transmission, the insufficient protection of communication channels and the ways to solve these problems were proposed. The scientific novelty is in the development of an adaptive algorithm for selecting a channel for data transmission, which is different from the well-known algorithms by higher flexibility and reliability. The flexibility (adaptability) of the algorithm is the automatic identification of available channels, and the reliability is providing of guaranteed transfer of the control commands. Also there were proposed a modified encryption algorithm based on the combined using of a symmetric encryption algorithm GOST 34.12-2015 and an asymmetric encryption algorithm on elliptic curves, allowing to increase the level of reliability of the protected interaction between the components of the control system while ensuring a sufficient speed of message transmission. There was designed a wireless control system with using an

ontological and visual modelling among other things. The results, which were received in the course of the study were used as the basis for creating hardware and software of an automated control system for «IoT» devices for a private house.

Keywords: Internet of Things, smart house, wireless interaction, control system, communication channel, encryption, ontological and visual modeling.

For citation: Afanasiev A.I., Knyazev V.N. Development of a wireless control system on the basis of «The internet of things» concept. *Modeling, optimization and information technology*. 2020;8(1). Available from: https://moit.vivt.ru/wp-content/uploads/2020/02/AfanasyevKnyazev_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.002 (In Russ).

Введение

Широкомасштабное развитие и применение информационных технологий в Российской Федерации относится к наиболее важным направлениям государственной политики, что подтверждается, в частности, принятием в 2017 году Государственной программы Российской Федерации «Цифровая экономика Российской Федерации», которая способствует «…развитию информационной инфраструктуры Российской Федерации, созданию и применению российских информационно-коммуникационных технологий, а также формированию новой технологической основы для социальной и экономической сферы» [1].

Кроме того, «Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы» предусматривает широкое применение в информационном обществе интернета вещей («Internet of Things» – IoT) и повышение информационной безопасности: «Основными направлениями развития российских информационных и коммуникационных технологий, … являются: … интернет вещей;…, информационная безопасность…» [2].

На фоне данных важных стратегических тенденций имеется актуальная задача разработки собственной эффективной и надежной автоматизированной системы управления (АСУ) с применением IoT-технологий [3].

Набирающий в настоящее время все большую популярность интернет вещей представляет собой научную концепцию, которая определяет различные способы взаимодействия физических объектов, систем и устройств с внешней средой и между собой с применением различных стандартов соединения и технологий связи. Широкую популярность и распространение приобретают решения, которые основаны на принципах IoT-технологий применительно к системам управления, имеющих различное назначение [4].

Актуальным и важным применением IoT-технологий является их использование по отношению к системам типа «Умный дом» [5-6].

Материалы и методы

Важное значение для систем типа «Умный дом» имеет применение Wi-Fi-соединений. [7] Однако, имеются причины, которые негативно влияют на уровень качества WiFi- сигнала, и вследствие которых качество связи между устройствами может ухудшиться или связь может даже прерваться, например, при ремонте, при установке новых технических устройств, при неправильной эксплуатации или настройке маршрутизатора и т. д.

Чтобы избежать возможной потери сигнала, и гарантировать доставку сообщений (данных) нужна несколько иная аппаратная организация информационного взаимодействия между устройствами системы [8].

Целесообразно задействовать для связи и другие альтернативные способы беспроводной связи, например радиоканалы и GPRS.

Кроме проблематики межинформационого обмена, существует необходимость обеспечения безопасности передаваемых данных, в целях исключения возможности управления системой злоумышленниками.

На Рисунке 1 рассматривается обобщенная схема взаимодействия между элементами автоматизированной системы управления. Элементы схемы, приведенные на Рисунке 1, представляют собой следующее:

– Client Smartphone – это мобильное устройство на ОС Android, подключенное к OpenVPN серверу;

– Сервер (ПК) - это стационарный пользовательский компьютер, имеющий постоянное подключение к интернету и подключенный к OpenVPN серверу;

– Arduino Server – это плата Arduino серии UNO, подключенная к Сервер (ПК) по соответствующему порту и имеющая несколько беспроводных каналов для связи с платой Arduino Performer с применением модифицированному алгоритма шифрования;

– Arduino Performer – это исполнительная плата Arduino серии UNO, имеющая несколько беспроводных интерфейсов для взаимодействия с Arduino Server с применением модифицированному алгоритма шифрования;

– Исполнительный механизм – это устройство, которое управляется платой Arduino Performer и подразумевает его использование в таких подсистемах умного дома, как отопление, освещение, полив, безопасность, противопожарная система, контроль электропитания, управление дверьми и воротами и т. д.

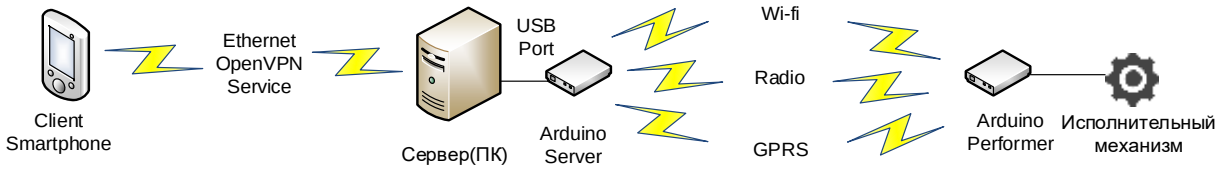

Рисунок 1 – Обобщенная схема взаимодействия между элементами автоматизированной системы управления

Figure 1 – Generalized scheme of interaction between elements of an automated control system

В ходе проектирования общего алгоритма передачи данных, соответствующего адаптивному алгоритму выбора каналов связи и модифицированному алгоритму шифрования, была разработана диаграмма деятельности, представленная на Рисунке 2. При выполнении данного алгоритма Arduino Server ожидает команды со стороны Сервер (ПК), после чего проверяет на доступность каналы связи с необходимым подмодулем в нашем случае Arduino Performer. Так как каналы упорядочены по приоритетности, выбирается первый доступный канал. Далее применяется модифицированный алгоритм шифрования и сформированное зашифрованное сообщение передается подмодулю Arduino Performer. Arduino Performer, получив зашифрованное сообщение, выполняет его расшифрованние, выделяет команду из расшифрованного сообщения и исполняет ее. После выполнения команды, формируется ответное сообщение, которое шифруется с помощью модифицированного алгоритма шифрования и отсылается Arduino Server. При

получении ответного сообщения, Arduino Server выполняет его расшифрование, анализ и далее доведение результата на Сервер (ПК).

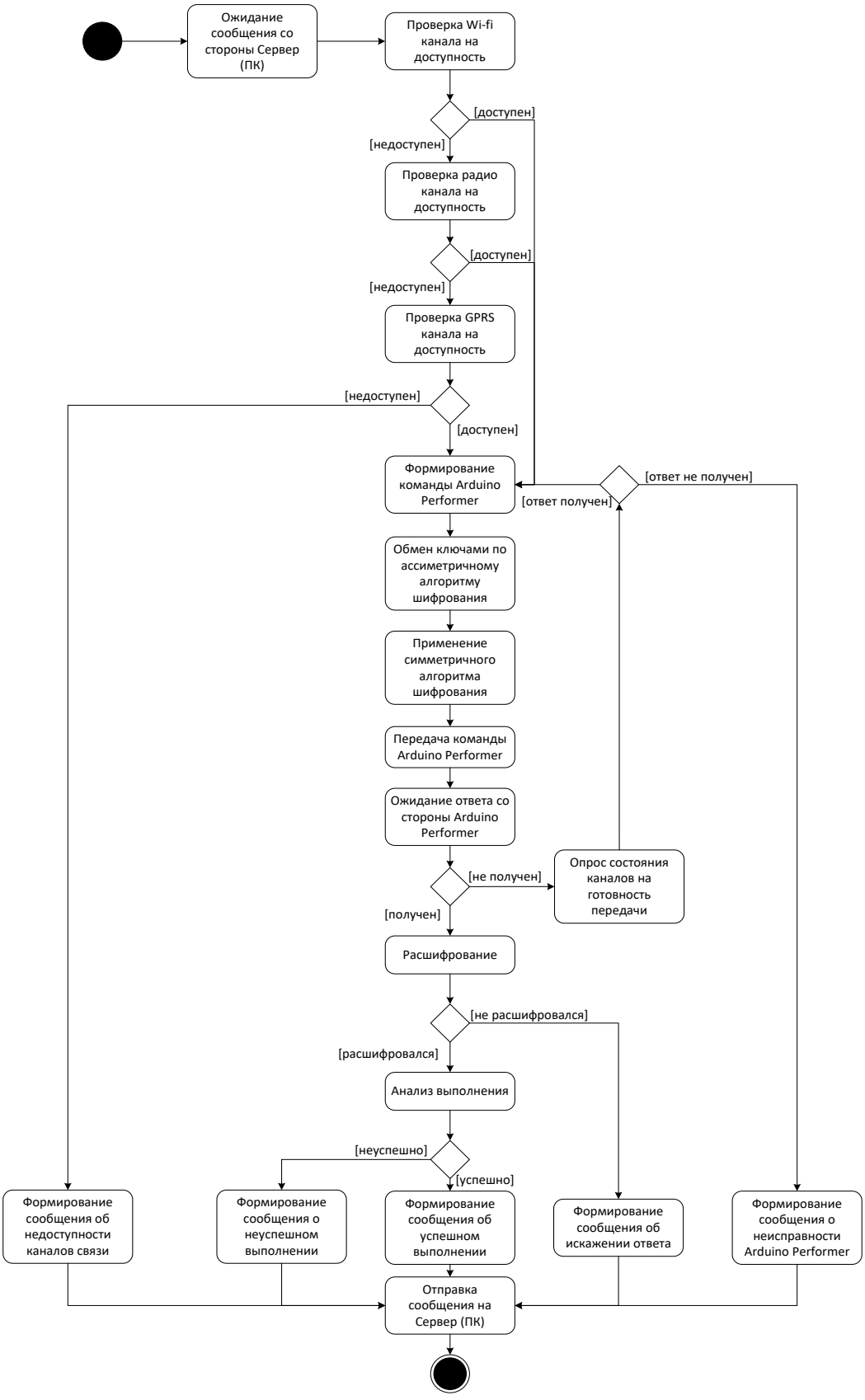

Рисунок 2 – Диграмма деятельности для адаптивного алгоритма выбора канала связи и модифицированного алгоритма шифрования при передаче сообщений
Figure 2 – Activity diagram for an adaptive algorithm for selecting a communication channel and a modified encryption algorithm for transmitting messages

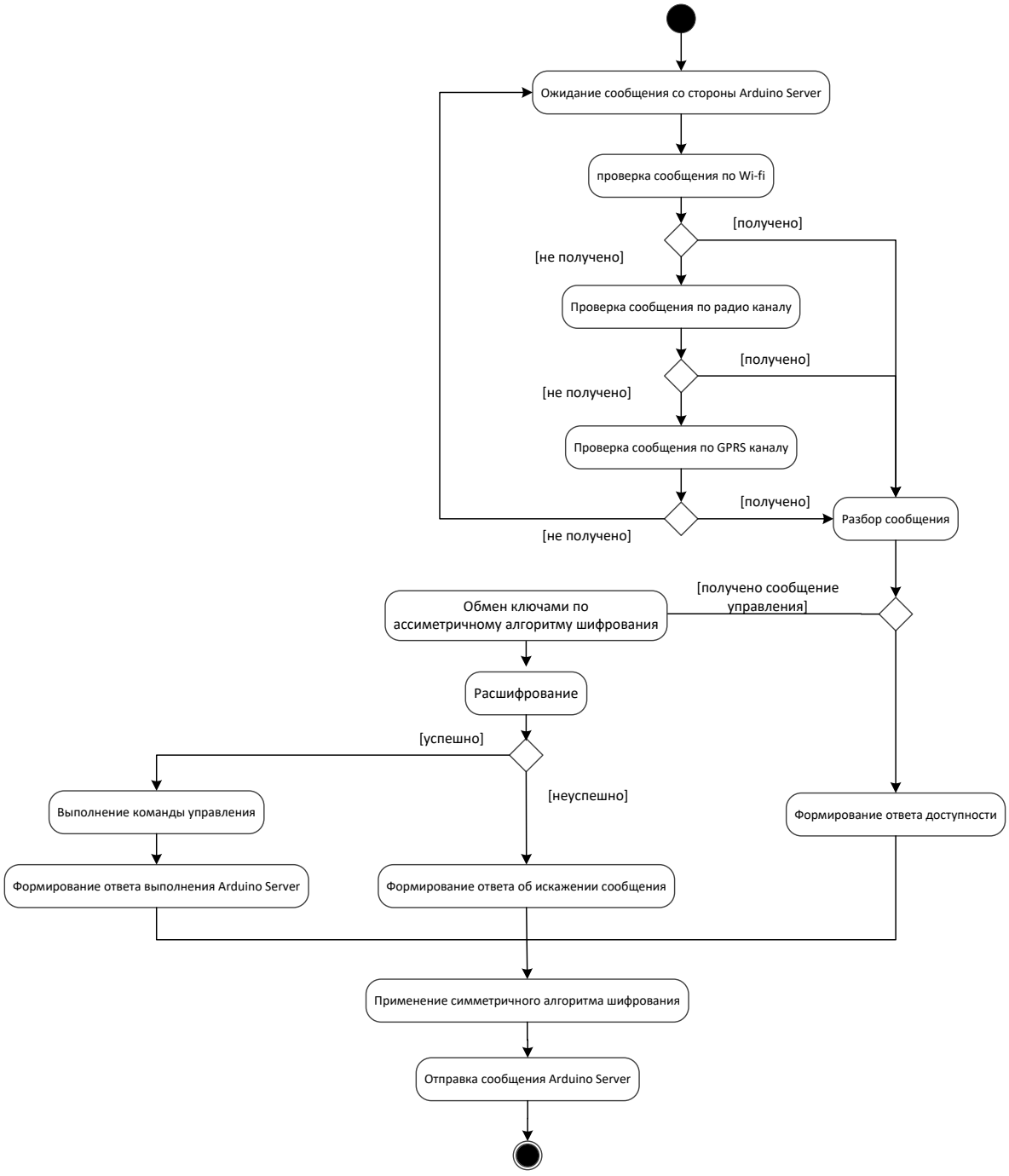

Рисунок 3 – Диаграмма деятельности для алгоритма передачи данных со стороны Arduino Performer
Figure 3 – Activity diagram for the data transmission algorithm by Arduino Performer

На Рисунке 3 приведена диаграмма деятельности для алгоритма передачи данных со стороны Arduino Performer.

Для обеспечения безопасного взаимодействия между Arduino Server и Arduino Performer предлагается модифицированный алгоритм комбинированного использования

симметричного (ГОСТ 34.12-2015) и ассиметричного (на эллиптических кривых) алгоритмов шифрования с целью увеличения надежности [9, 10]. Приведем список основных преимуществ модифицированного алгоритма:

- смена ключей, основанная на эллиптических кривых, повышает надежность работы симметричного алгоритма;
- криптографический алгоритм на эллиптических кривых использует меньшую длину ключа по сравнению с иными ассиметричными алгоритмами, что приемлемо при работе на устройствах с ограниченными ресурсами;
- скорость работы алгоритмов на эллиптических кривых гораздо выше, чем у классических ассиметричных алгоритмов, что объясняется как размерами поля, так и применением более близкой для компьютеров структуры бинарного конечного поля;
- из-за малой длины ключа и высокой скорости работы, алгоритмы ассиметричной криптографии на эллиптических кривых могут использоваться в смарт-картах и других устройствах с ограниченными вычислительными ресурсами;
- потенциальный нарушитель не сможет получить доступ управления к Arduino Performer с учетом особенностей формирования общего секретного ключа.

Алгоритм обмена сообщениями между Arduino Server и Arduino Performer с использованием модифицированного алгоритма шифрования состоит из двух этапов, представленных на Рисунках 4 и 5.

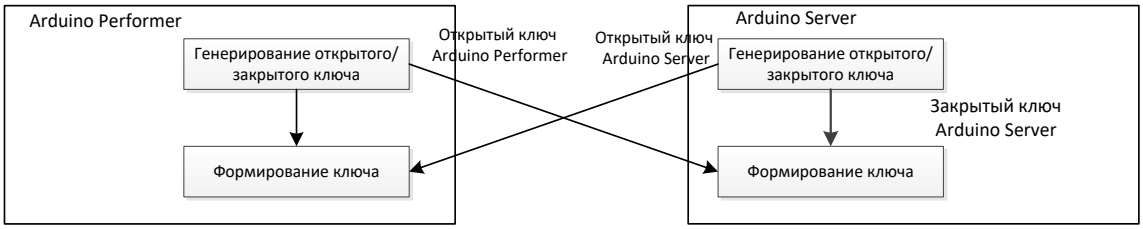

Рисунок 4 – Первый этап алгоритма обмена сообщениями между Arduino Server и Arduino Performer

Figure 4 – The first step of the messaging algorithm between Arduino Server and Arduino Performer

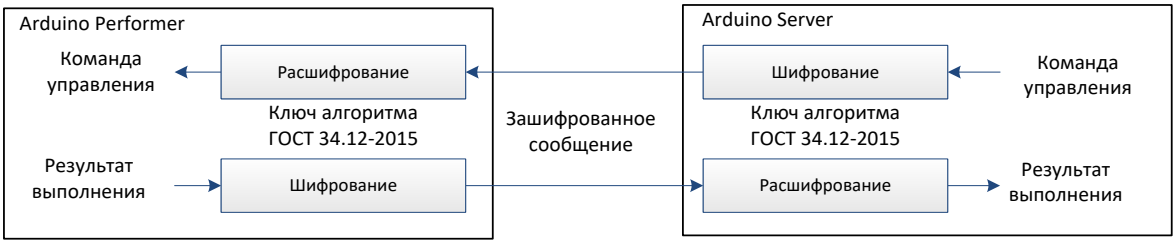

Рисунок 5 – Второй этап алгоритма обмена сообщениями между Arduino Server и Arduino Performer

Figure 5 – The second stage of the messaging algorithm between Arduino Server and Arduino Performer

На первом этапе Arduino Server выступает инициатором информационного обмена. В начале работы и далее перед отправкой новой команды он генерирует и отсылает открытый ключ к Arduino Performer. После получения открытого ключа Arduino Performer так же формирует свой открытый и закрытый ключи и отсылает свой открытый ключ обратно Arduino Server. Далее Arduino Server и Arduino Performer формируют 256 битный ключ, который далее используется в симметричном алгоритме шифрования ГОСТ 34.12-2015.

Обобщенный алгоритм симметричного шифрования ГОСТ 34.12-2015 представлен на Рисунке 6.

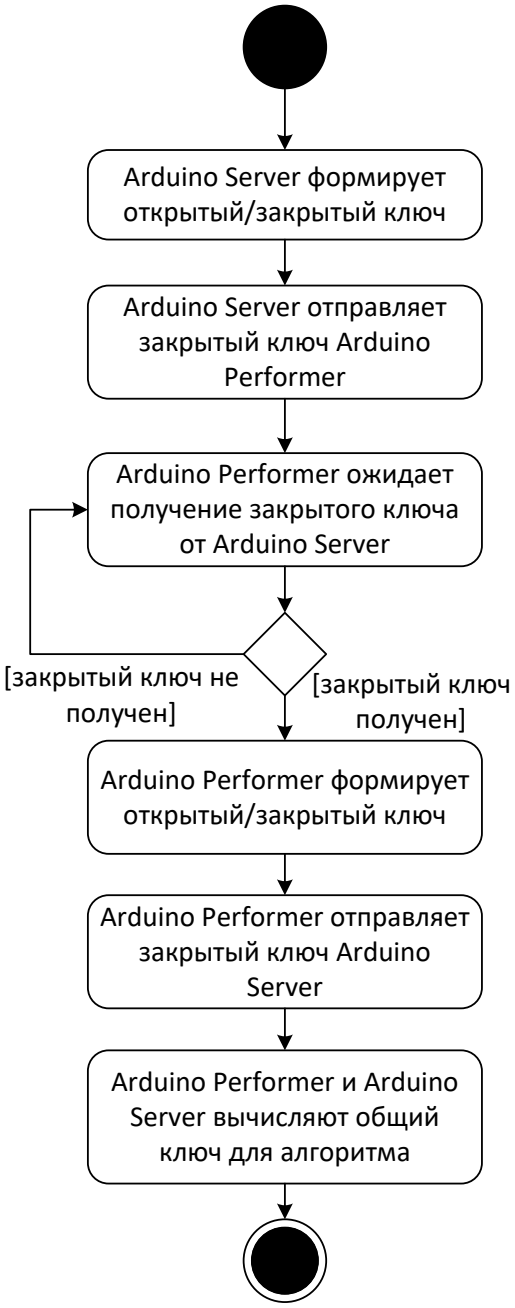

Рисунок 6 – Диаграмма деятельности обобщенного алгоритма симметричного шифрования ГОСТ 34.12-2015

Figure 6 – Activity diagram of the generalized symmetric encryption algorithm GOST 34.12-2015

Автоматизированные системы управления с использованием IoT-технологий характеризуются отсутствием нормативно установленных определений, строгой классификации технологий. Системы на основе IoT постоянно развиваются, что отражается в расширении, изменении понятийной системы. Создание формальной онтологии для такой предметной области является важной задачей [11]. В соответствии с этим в среде Protégé [12] был разработан необходимый для задачи набор классов,

свойств этих классов, а также набор связей и взаимодействий между ними. Список созданных классов представлен на Рисунке 7.

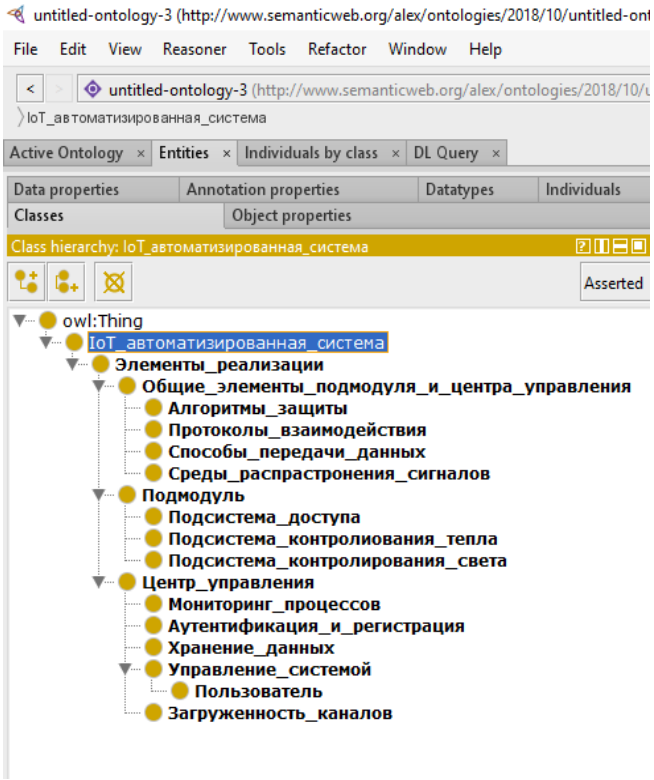

Рисунок 7 – Основной набор классов в дереве наследования
Figure 7 – The main set of classes in the inheritance tree

Для данной онтологии был построен онтологический граф, который представлен на Рисунке 8 .

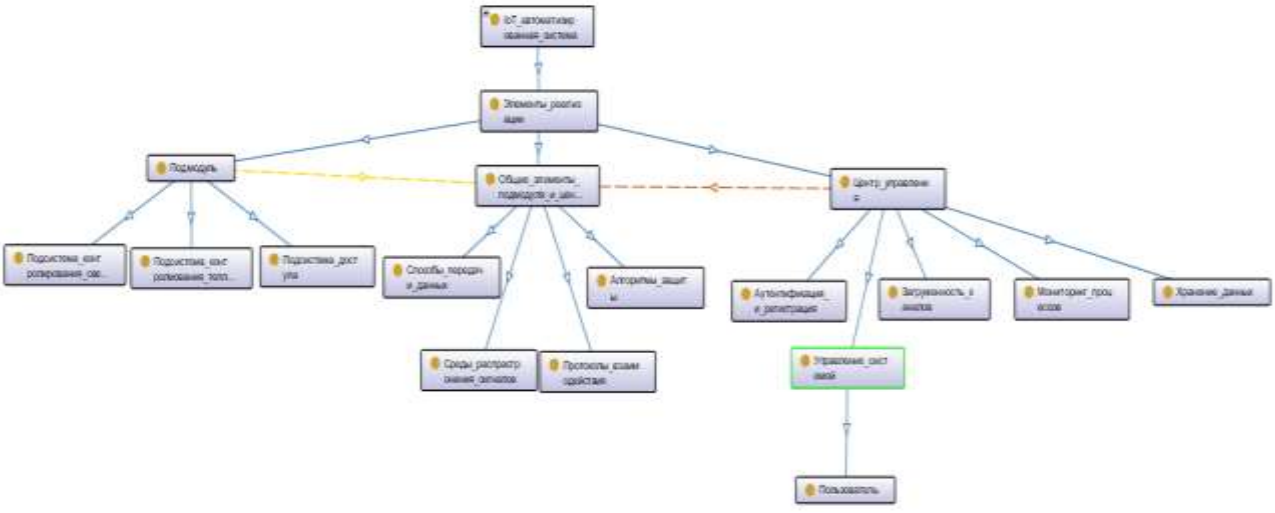

Рисунок 8 – Граф онтологии
Figure 8 – Ontology graph

После разработки онтологической модели было проведено визуальное моделирование с применением унифицированного языка моделирования UML,

являющегося одним из главных средств современной информационной технологии RUP [13].

После проведения проектирования автоматизированной системы управления с использованием IoT-технологий был осуществлен выбор аппаратных, языковых и инструментальных программных средств разработки.

Для реализации серверной части использован стационарный персональный компьютер с операционной системой Ubuntu Linux [14]. В качестве микроконтроллера как исполнителя команд управления использован микроконтроллер Mega328P на базе отладочной платы Arduino Uno. Для реализации Wi-fi канала связи выбран микроконтроллер ESP8266 [15].

Для создания серверного приложения выбрано использование среды разработки IDE Eclipse, поскольку данная среда включает в себя компилятор языка C/C++ и имеет возможность установки расширений, которые дополняют среду Eclipse диспетчерами для работы с серверами приложений, базами данных и т. д. Для реализации клиентского приложения выбрано использование инструментальной среды разработки Microsoft Visual Studio в связи с удобством использования и её распространённостью.

Полученные в ходе исследования результаты на основе предлагаемого подхода организации работы автоматизированной системы управления с применением различных по типу каналов связи для повышения надежности и безопасности передачи данных и модифицированного алгоритма шифрования использованы в создании аппаратного и программного обеспечения автоматизированной системы управления IoT-устройствами для частного жилого дома.

Заключение

В статье рассмотрены актуальные и перспективные вопросы и проблемы разработки беспроводных систем управления на основе концепции «Интернет вещей» («Internet of Things», IoT). В качестве важных проблем определены такие, как недостаточная гибкость и оперативность выбора каналов связи для передачи данных, недостаточная защищенность каналов связи и предложены способы решения данных проблем.

Предложен адаптивный алгоритм выбора канала для передачи данных, отличающегося от известных алгоритмов более высокой гибкостью и надежностью. Гибкость (адаптивность) алгоритма заключается в автоматическом выявлении доступных каналов, а надежность – в обеспечении гарантированной передачи команд управления.

Также предложен модифицированный алгоритм шифрования, основанный на комбинированном использовании симметричного алгоритма шифрования ГОСТ 34.12-2015 и ассиметричного алгоритма шифрования на эллиптических кривых, позволяющий повысить уровень надежности защищенного взаимодействия между компонентами системы управления при обеспечении достаточной скорости передачи сообщений.

Проведено проектирование беспроводной системы управления с применением, в том числе, онтологического и визуального моделирования.

Полученные в ходе проведенного исследования результаты использованы в качестве основы при создании аппаратного и программного обеспечения автоматизированной системы управления IoT-устройствами для частного жилого дома.

ЛИТЕРАТУРА

1. *Программа «Цифровая экономика Российской Федерации».* Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р.

[Электронный ресурс]. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 16.04.2019).
2. *Распоряжение Президента Российской Федерации* от 9 мая 2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы» [Электронный ресурс]. – URL: http://zmedu.hostedu.ru/files/ykaz_7668.pdf (дата обращения: 16.04.2019).
3. Афанасьев А.И., Князев В.Н. Программные средства АСУ с применением IoT-технологий. Сборник научных статей V Всероссийской межвузовской научно-практической конференции: *Информационные технологии в науке и образовании. Проблемы и перспективы*. Под ред. Л.Р. Фионовой. Пенза, Изд-во ПГУ. 2018:133-135.
4. Кранц М. *Интернет вещей. Новая технологическая революция*. М., Изд-во БОМБОРА. 2018:336.
5. Дементьев А.И. *«Умный дом» XXI века*. М., Изд-во Ridero. 2016:142.
6. Петин В.А. *Создание умного дома на базе ARDUINO*. М., Изд-во ДМК-Пресс, 2018:180.
7. Росс Д. *Беспроводная компьютерная сеть Wi-Fi своими руками.* М.: Наука и техника. 2015:384.
8. Руденков Н.А., Долинер Л.И. *Основы сетевых технологий*. Екатеринбург, Изд-во УФУ. 2011:377.
9. *Информационная технология. Криптографическая защита информации. Блочные шифры.* - ГОСТ Р 34.12 – 2015. [Электронный ресурс]. – URL: https://files.stroyinf.ru/Data/603/60339.pdf (дата обращения: 16.04.2019).
10. Пастухов Д.Ф., Пастухов Ю.Ф., Синица П.Р. *Шифрование данных на базе эллиптических кривых*. Новополоцк, Изд-во ПГУ. 2016:72.
11. Палагин А.В., Крывый С.Л., Петренко Н.Г. *Онтологические методы и средства обработки предметных знаний: монография*. Луганск: Изд-во ВНУ. 2012:324.
12. Муромцев Д.И. *Онтологический инжиниринг знаний в системе Protégé*. СПб ГУ ИТМО. 2007:62.
13. Ларман К. *Применение UML 2.0 и шаблонов проектирования. Введение в объектно-ориентированный анализ, проектирование и итеративную разработку*. М.: Издательство «Вильямс». 2013:736.
14. Негус К., Каэн Ф. *Ubuntu и Debian Linux для продвинутых: более 1000 незаменимых команд*. СПб, Питер. 2014. 384 с.
15. Шварц М. *Электроника. Интернет вещей с ESP8266*. М.: BHV. 2018:192.

REFERENCES

1. *The program «Digital Economy of the Russian Federation»*. It was approved by the order of the Government of the Russian Federation dated July 28, 2017:1632. [Electronic resource]. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (access date: 16.04.2019).
2. The order of the President of the Russian Federation dated May 9, 2017 No. 203 «*The strategy for the development of the information society in the Russian Federation for 2017 2030*» [Electronic resource]. URL: http://zmedu.hostedu.ru/files/ykaz_7668.pdf (access date: 16.04.2019).
3. Afanasyev A.I., Knyazev V.N. Software for automated control systems using IoT technologies. *Collection of scientific articles of the Vth All-Russian Intercollegiate*

Scientific and Practical Conference: Information Technologies in Science and Education. Problems and prospects. Ed. L.R. Fionic. Penza, PGU Publishing House. 2018:133-135.
4. Krantz M. *Internet of Things. New technological revolution*. M., BOMBOR Publishing House. 2018:336.
5. Dementiev A.I. *«Smart home» of the XXI century.* M., Ridero Publishing House. 2016:142.
6. Petin V.A. *Creation of a smart home based on ARDUINO*. M., Publishing House DMK-Press. 2018:180.
7. Ross D. *DIY wireless computer network Wi-Fi. M.: Science and Technology*. 2015:384.
8. Rudenkov N.A., Doliner L.I. *Fundamentals of network technologies*. Yekaterinburg, Publishing House of UFU. 2011:377.
9. *Information technology. Cryptographic protection of information. Block ciphers.* - GOST R 34.12 – 2015. [Electronic resource]. URL: https://files.stroyinf.ru/Data/603/60339.pdf (access date: 04/16/2019).
10. Pastukhov D.F., Pastukhov Yu.F., Tit P.R. *Data encryption based on elliptic curves.* Novopolotsk, PSU Publishing House. 2016:72.
11. Palagin A.V., Kryvy S.L., Petrenko N.G. *An ontological methods and means of processing subject knowledge: monograph.* Lugansk: VNU publishing house V. Dahl. 2012:324.
12. Muromtsev D.I. *Ontological knowledge engineering in the Protégé system*. St. Petersburg State University ITMO. 2007:62.
13. Larman K. *The Use of UML 2.0 and Design Patterns. The introduction to object-oriented analysis, design and iterative development*. M.: Williams Publishing House. 2013:736.
14. Negus K., Caen F. *Ubuntu and Debian Linux for advanced: more than 1000 indispensable teams*. St. Petersburg, Peter. 2014:384.
15. Schwartz, M. *Electronics. The Internet of Things with ESP8266*. M.: BHV. 2018:192.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATIONS ABOUT AUTHORS

Афанасьев Алексей Игоревич, студент магистратуры кафедры «Математическое обеспечение и применение ЭВМ», Пензенский государственный университет, Пенза, Российская Федерация.
email: alegy1996@gmail.com
ORCID: 0000-0002-7822-3875

Alexey I. Afanasiev, Master Student Of The Department Mathematical Support And Computer Application, Penza, Russian Federation.

Князев Виктор Николаевич, кандидат технических наук, доцент кафедры «Математическое обеспечение и применение ЭВМ», Пензенский государственный университет, Пенза, Российская Федерация.
email: knyazev@sura.ru

Victor N. Knyazev, Candidate Of Technical Sciences, Department Of Mathematical Support And Computer Application, Penza, Russian Federation.