УДК 004.738.5 DOI: 10.18698/2541-8009-2020-01-570

РОЛЬ АУТЕНТИФИКАЦИИ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Д.В. Братко bdw_@mail.ru
SPIN-код: 4812-3061

В.С. Березин berezin15@yandex.ru
SPIN-код: 2599-0304

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В настоящее время открывается все больше возможностей для оптимального управления ресурсами. Новая технология — Интернет вещей — позволяет измерять и оптимизировать процессы, охватывающие множество областей жизнедеятельности человека. Однако «умные» устройства Интернета вещей часто подвергаются атакам со стороны злоумышленников, в связи с этим был проведен анализ защищенности Интернета вещей на примере реализации системы домашней автоматизации — «Умный дом». В рамках данной проблемы рассмотрена модель угроз каждого компонента системы и приведена логическая форма формализованного представления данной модели угроз. На основе выявленных уязвимостей разработаны меры, направленные на усиление защищенности системы «Умный дом». В ходе анализа установлено, что для решения поставленной задачи необходимо наличие надежной системы доступа и аутентификации, основанной на криптографии. Кроме того, задача обеспечения безопасности не должна изолированно опираться на систему аутентификации, она требует комплексного решения.

Ключевые слова

Интернет вещей, аутентификация, «Умный дом», модель угроз, защищенность, информационно-коммуникационные технологии, автоматизация, облачная платформа

Поступила в редакцию 23.12.2019

Введение. Интернет вещей (англ. *Internet of Things*, *IoT*) — это сеть устройств, которые подключены к Интернету, управляются через него и могут обмениваться данными друг с другом. Это может быть пользовательская электроника — гаджеты (умные часы), домашние устройства (веб-камеры, холодильники, кофеварки и т. д.), и промышленная техника (роботы, датчики и сенсоры).

Интернет вещей открывает большие возможности для оптимального управления ресурсами. Относительно недорогие и подключенные к Интернету датчики позволяют измерять и оптимизировать процессы, для которых ранее это было слишком сложно.

Новая технология охватывает множество областей жизнедеятельности человека. Так, производство в будущем станет более надежным — системы мони-

торинга будут сообщать о проблемных участках до того, как на них произойдут сбои. С помощью подключенных датчиков станет возможным измерять загруженность транспортных каналов и оптимизировать их. Уже сегодня носимые медицинские сенсоры круглосуточно отслеживают жизненные показатели пациентов: пульс, температуру, давление, уровень сахара и кислорода в крови [1].

Однако умные устройства часто становятся объектом интереса хакеров и злоумышленников. Данная область захватывает неопределенное множество протоколов, языков программирования, чипов, следовательно, встает вопрос о проведении полноценного анализа защищенности IoT. Проблема заключается в том, что современный мир не стоит на месте и, пока все силы направляются на изучение одних технологий, им на смену приходят более современные [2].

В данной работе выполнен анализ защищенности IoT на примере одного из вариантов реализации системы домашней автоматизации — «Умный дом».

Обзор Интернета вещей. Интернет вещей — инфраструктура информационного общества, предоставляющая различные виды услуг путем соединения друг с другом вещей (физических и виртуальных) на основе существующих функционально совместимых информационно-коммуникационных технологий (рис. 1).

<table>
<tr><th colspan="2">Интернет вещей</th></tr>
<tr><th>Вещи Интернета вещей</th><th>Сети Интернета вещей</th></tr>
<tr><td rowspan="2">Сенсоры, контроллеры, а также физические объекты, которые изначально не предназначены для подключения к сети.
Каждая вещь должна быть однозначно идентифицирована:
– программно-аппаратными средствами, предусмотренными разработчиками устройств (MAC-адрес сетевого адаптера);
– RFID-метки, радиомаяки, оптические распознаваемые идентификаторы (например, штрих-коды)</td><td>Проводные и беспроводные, в составе которых хабы и шлюзы</td></tr>
<tr><td>Центры обработки данных (ЦОД)
Сбор, хранение, обработка, анализ, визуализация данных, а также выработка прогнозов, рекомендаций и команд устройствам для умного взаимодействия в соответствии с заданными алгоритмами</td></tr>
</table>

Рис. 1. Основные составляющие Интернета вещей

Информационно-коммуникационные технологии обеспечивают связь в любом месте, в любое время, а также связь с любой вещью.

Требования, предъявляемые к IoT:

1) обеспечение соединения между вещами в IoT на основе идентификатора этой вещи;

2) функциональная совместимость в целях предоставления и потребления разных видов информации и услуг;

3) поддержка организации автономных сетей;

4) поддержка возможностей определения местоположения;

5) безопасность соединения, предполагающая защиту от таких угроз, как нарушение аутентичности, конфиденциальности, целостности;

6) защита неприкосновенности частной жизни.

Выделим несколько существенных элементов, общих для IoT.

Сенсоры и контроллеры. Звук, движение, наблюдаемые и окружающие объекты, освещенность, температура — эти и другие параметры определяют состояние вещи и ее взаимодействие с окружающей средой. Если от вещи предполагается действие, она также содержит контроллер — регулятор или управляющее устройство. Так, дверь может распознать посетителя по биометрическим параметрам и открыть замок, если эти параметры соответствуют хозяину жилища.

Отсутствующий пользовательский интерфейс. Большинство вещей получают информацию от сенсоров и управляющих серверов. Взаимодействие с пользователем часто происходит опосредованно, через управляющие серверы с интерфейсом порталов, или на основе приложений, с помощью которых пользователь может получить информацию о статусе объектов и задать определенные установки.

Программируемый интеллект. По существу, вещь, подключенная к Интернету, — это материализованное приложение. И как для обычного приложения, ее функциональность может быть улучшена и расширена.

Связность. Использование Интернета для обеспечения связности вещей позволяет им не только обмениваться информацией друг с другом или с центральной системой. Интернет обеспечивает доступность вещей вне зависимости от расположения хозяина. Можно управлять отопительной системой дома из салона автомобиля, а климатической системой автомобиля — перед выходом из дома.

Автоматизация. Индустриальные сенсорные управляющие системы появились задолго до Интернета вещей. Уникальность сегодняшнего явления заключается в том, что оно принесло автоматизацию в массы, позволяя автоматизировать повседневные бытовые задачи. Благодаря открытой коммуникационной инфраструктуре с помощью этих систем путем автоматизации могут быть решены широкомасштабные задачи — от построения интеллектуальной транспортной системы до разработки системы интеллектуального городского освещения [3].

Для того чтобы перейти к анализу защищенности IoT на примере реализации системы домашней автоматизации, рассмотрим базовые понятия, связанные с наиболее важным для данной системы механизмом безопасности — аутентификацией.

Понятие аутентификации. *Аутентификация* — это процесс, состоящий из процедур, включающих подтверждение подлинности предъявленного претен-

дентом (субъектом доступа) идентификатора (идентификационной информации) и проверку принадлежности аутентификационной информации (фактора аутентификации, секрета) и идентификатора (идентификационной информации) конкретному субъекту или объекту доступа.

Фактор аутентификации — вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа при аутентификации.

Выделяют следующие факторы аутентификации:

– фактор знания (пароль, PIN-код и т. п.);

– фактор владения (данные, хранимые в техническом (аппаратном) устройстве);

– биометрический фактор (биометрические данные физического лица);

– фактор поведения (поведенческая модель).

Способы аутентификации:

– однофакторная аутентификация (используется один фактор аутентификации);

– многофакторная аутентификация (используется два и (или) более различных факторов аутентификации);

– односторонняя аутентификация (доверие к идентификационным данным другой стороны обеспечивается только лишь для одной из взаимодействующих сторон);

– взаимная аутентификация (для каждой из сторон обеспечивается определенный уровень доверия к идентификационным данным другой стороны и к тому, что другая сторона является той, за кого себя выдает).

Доверие к результату аутентификации субъекта или объекта — это уверенность в том, что субъект или объект доступа, предъявляющий конкретную идентификационную и аутентификационную информацию, на самом деле является тем субъектом или объектом, за который себя выдает.

Участники процесса аутентификации:

– субъект доступа (аппликант, претендент, заявитель);

– центр регистрации (ЦР) — устанавливает и фиксирует связь субъекта и его уникального секретного признака — аутентификатора. В роли такого центра может выступать, например, удаленный ЦР удостоверяющего центра (УЦ), связанный доверительными отношениями с УЦ;

– доверяющая сторона — владелец того ресурса, к которому претендует получить доступ субъект доступа. Он проверяет по протоколу аутентификации факт владения субъектом доступа соответствующим аутентификатором — секретом, который выдан субъекту ЦР;

– проверяющая сторона (центр валидации) — выполняет проверку наличия фиксированной ЦР связи «субъект доступа — аутентификатор» [4–9].

Анализ угроз системы, включающей элементы IoT. Защита IoT-устройств призвана гарантировать, что в решении используется набор доверенных

устройств и что эти устройства могут доверять пользователю или приложению, управляющими ими.

Чтобы понять риски, связанные с IoT, рассмотрим архитектуру такой системы. В качестве примера возьмем наиболее общий вариант домашней автоматизации — «Умный дом», представленный на рис. 2.

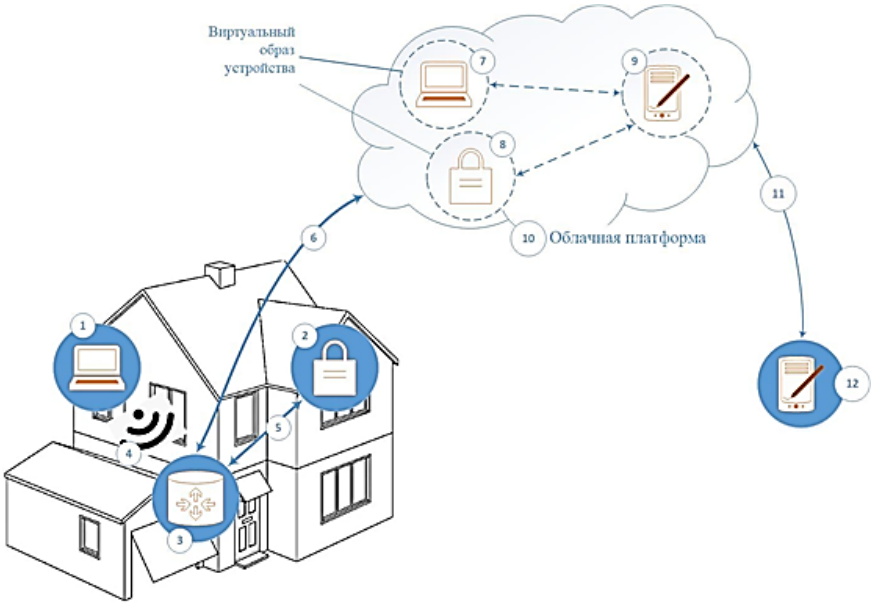

Рис. 2. Реализация системы «Умный дом»

На рис. 2 показаны уязвимые места системы «Умный дом»: устройства IoT — ноутбук, подключенный к сети по Wi-Fi (1) и датчик открытия двери (2); шлюз или маршрутизатор (3), обеспечивающий опосредованное подключение этих устройств к Интернету и доступ к облачным услугам; облачная платформа, обеспечивающая создание (регистрацию) и управление устройствами IoT. После регистрации устройства платформа создает виртуальный образ физического объекта IoT (7, 8, 9), обеспечивая вычислительные ресурсы и память, необходимые для его работы и автоматизации, а также приложения удаленного доступа (12), предоставляющие пользовательский интерфейс взаимодействия с облачными приложениями для управления объектами IoT.

Угрозы, которым могут подвергаться отдельные компоненты системы, представим в сводной таблице.

Формализация модели угроз. Для формализации модели угроз введены следующие функции:

1) функция угроз, направленная на устройства IoT:

$$F_1 = \mu \{K_i\},$$

где K_i — множество возможных угроз, направленных на устройства Iot;

Модель угроз для каждого компонента системы «Умный дом»

№ п/п	Компонент системы «Умный дом»	Уязвимость	Способ реализации угрозы
1	Устройства IoT (рис. 2, позиции 1, 2)	Низкая защита доступа; отсутсвие механизма автоматического обновления программного обеспечения (ПО)	Использование ПО устройств IoT через маскировку под зарегистрированного пользователя; дефекты и уязвимости программного обеспечения устройств IoT; внесение программных закладок; применение вирусов или другого вредоносного программного кода
2	Коммуникационные протоколы (беспроводная связь, протоколы верхнего уровня) (рис. 2, позиции 4, 11)	Отсутсвие надежной системы аутентификации и шифрования данных	Атака Man In The Middle (MITM); атака повторного воспроизведения (replay attack)
3	Шлюз/маршрутизатор (рис. 2, позиция 3)	Низная защита доступа	Несанкционированный доступ к защищаемой информации путем подключения к сети «Умный дом» через шлюз/маршрутизатор
4	Облачные услуги (рис. 2, позиции 7–10)	Отсутствие надежной системы аутентификации; низкий уровень защищенности данных при регистрации устройства; низкий контроль доступа к различным функциям устройства	Несанкционированное управление через Интернет; кража информации через облачные системы
5	Приложения удаленного доступа (рис. 2, позиция 12)	Использование незащищенных протоколов (HTTP вместо HTTPS); слабая система аутентификации	Установка вредоносных приложений

2) функция угроз, направленная на сети Интернета вещей:

$$F_2 = \mu \{K_j\},$$

где N_j — множество возможных угроз, направленных на среду передачи данных;

3) функция угроз, направленная на центр обработки данных (облачную платформу):

$$F_3 = \mu \{M_l\},$$

где M_l — множество возможных угроз, направленных на облачную платформу.

Таким образом, логическая форма формализованного представления модели угроз в системе «Умный дом» имеет вид [10]

$$F_{\text{угроз}} = F_1 \wedge F_2 \wedge F_3.$$

Данная модель является основой для моделирования злоумышленных воздействий на систему «Умный дом» и затрагивает все составляющие Интернета вещей (см. рис. 1).

Защищенность системы «Умный дом». Для усиления защищенности компонентов системы «Умный дом» предназначены следующие меры.

Устройства IoT:

1) надежная система доступа и аутентификации, основанная на криптографии. Для защиты связи между устройствами IoT необходимо шифрование, и для этого нужны криптографические идентификаторы устройств. Требуется использовать доверенные сертификаты, выпущенные с помощью УЦ как для устройств с коротким сроком службы, так и для устройств IoT, рассчитанных на десятилетия. Также необходимо убедиться, что доступ к подключенным устройствам получают только авторизованные пользователи;

2) криптографическая защищенность ПО. Использование системы PKI для подписания кода и проверки его аутентичности;

3) обновление ПО на протяжении всего жизненного цикла устройств. Важно, чтобы обновление могло осуществляться автоматически, без участия владельца устройств.

Сети IoT:

1) криптографическая защита данных;

2) отсутствие критических зависимостей от связности. Сохранение системой критической функциональности даже при отсутствии связи;

3) создание дополнительной спецификации устройства, детально описывающей требуемую политику безопасности для конкретного устройства (перенаправление портов, допустимые источники трафика и его характеристики). Данная спецификация может быть реализована на домашнем маршрутизаторе. Проект этого решения — Manufacturer Usage Description (MUD). Контроллер MUD, который может являться частью домашнего маршрутизатора или экрана безопасности, скачивает файл с сервера и соответствующим образом конфигурирует списки доступа и т. п. Предполагается, что файл MUD предоставляется производителем устройства и защищен электронной подписью, позволяющей контроллеру проверить подлинность спецификации.

Центр обработки данных (облачная платформа):

1) контроль доступа к ресурсам устройств. Приложение объявляет набор ресурсов, к которым оно хотело бы получить доступ, платформа же

предоставляет список устройств с этими ресурсами. Соответственно, пользователь получает возможность выбрать, к каким устройствам и их возможностям данное приложение может иметь доступ, тем самым авторизуя приложение и открывая ему доступ также к другим возможностям, которые могут быть использованы злоумышленником;

2) технология двухфакторной аутентификации. Двухфакторная аутентификация пользователей при входе в различные компьютерные системы и сети обеспечивает в них заметное повышение уровня защиты информации, благодаря чему эта технология все шире применяется в мобильных устройствах и в Интернете. Способы двухфакторной защиты от несанкционированного доступа, применяемые в человеко-машинном взаимодействии, конечно, можно было бы перенести в область межмашинного взаимодействия (M2M) в IoT, но они слишком сложны для низкопроизводительных процессоров IoT-устройств, обладающих к тому же небольшими объемами памяти. Пути решения данной проблемы в данный момент находятся на стадии разработки;

3) верификация приложений «магазинами приложений». Предварительная проверка приложений на предмет наличия вредоносного кода.

Заключение. В работе были рассмотрены пути повышения безопасности отдельных компонентов структуры IoT (устройства IoT, сети IoT, центры обработки данных) на примере реализации системы домашней автоматизации — «Умный дом».

В ходе анализа было выявлено, что критически важным механизмом безопасности в такой структуре является наличие надежной системы доступа и аутентификации, основанной на криптографии. Кроме того, как видно из анализа угроз системы IoT, проблема безопасности не должна изолированно опираться только на систему аутентификации, а требует комплексного решения. Чем больше «открыта» система, тем выше становятся требования к исполнителям, ответственным за безопасность системы — от производителей оборудования IoT, разработчиков программного обеспечения до провайдеров облачных структур и самих владельцев «умных» устройств. Более того, недостаточная защищенность хотя бы одного из элементов может существенно ослабить безопасность системы в целом.

Литература

[1] Что такое интернет вещей. *tadviser.ru: веб-сайт*. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%B5_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_%28Internet_of_Things%2C_IoT%29 (дата обращения: 20.08.2019).

[2] Кантышев П. Интернет вещей открывает киберпреступникам новое поле деятельности. *vedomosti.ru: веб-сайт*. URL: https://www.vedomosti.ru/technology/articles/2016/02/29/631753-internet-veschei-otkrivaet-kiberprestupnikam-novoe-pole-deyatelnosti (дата обращения: 26.09.2019).

[3] Робачевский А.М. Умные и опасные? (Вопросы безопасности IoT). *Интернет изнутри*, 2017, № 5. URL: http://internetinside.ru/umnye-i-opasnye-voprosy-bezopasnosti-i/ (дата обращения: 20.08.2019).

[4] Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам. *Вестник Нижегородского университета им. Н.И. Лобачевского*, 2013, № 2(1), с. 45–51.

[5] Грушо А.А., Забежайло М.И., Смирнов Д.В. и др. О комплексной аутентификации. *Системы и средства информатики*, 2017, т. 27, № 3, с. 4–11. DOI: https://doi.org/10.14357/08696527170301

[6] Сабанов А.Г. Критерии доверия к результатам идентификации субъектов доступа. *Электросвязь*, 2019, № 3, с. 54–60.

[7] Сабанов А.Г. Способ определения строгости аутентификации. *Электросвязь*, 2016, № 8, с. 56–61.

[8] Сабанов А.Г. Формирование уровней доверия к идентификации и аутентификации субъектов при удаленном электронном взаимодействии. *Электросвязь*, 2015, № 10, с. 46–51.

[9] Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 1, 2. *Защита информации. Инсайд*, 2016, № 2, с. 84–87, № 3, с. 70–73.

[10] Овчинников Н.А., Мисюрина К.В., Рудикова М.Н. и др. Формализованная модель информационной безопасности «Умный дом». *Апробация*, 2016, № 1(40), с. 49–51.

Братко Дарья Владимировна — студентка кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Березин Вячеслав Сергеевич — студент кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:

Братко Д.В., Березин В.С. Роль аутентификации в системах Интернета вещей. *Политехнический молодежный журнал*, 2020, № 01(42). http://dx.doi.org/10.18698/2541-8009-2020-01-570

THE ROLE OF AUTHENTICATION IN THE IOT SYSTEMS

D.V. Bratko bdw_@mail.ru
SPIN-code: 4812-3061

V.S. Berezin berezin15@yandex.ru
SPIN-code: 2599-0304

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Currently, more and more opportunities are opening up for optimal resource management. A new technology — the Internet of things — allows one to measure and optimize processes that span many areas of human life. However, "smart" devices of the Internet of things are often attacked by cybercriminals. Thus, an analysis of the security of the Internet of things was carried out using the example of implementing a home automation system — Smart Home. In the framework of this problem, the threat model of each component of the system is considered and the logical form of a formalized representation of this threat model is given. Based on the identified vulnerabilities, measures have been developed aimed at enhancing the security of the Smart Home system. In the course of the analysis, it was found that in order to solve the problem, a reliable access and authentication system based on cryptography is necessary. In addition, the task of ensuring security should not be isolated from the authentication system; it requires a comprehensive solution.

Keywords

Internet of things, authentication, Smart Home, threat model, security, information and communication technologies, automation, cloud platform

Received 23.12.2019

References

[1] Chto takoe internet veshchey [What is Internet of things]. *tadviser.ru: website* (in Russ.). URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%B5_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_%28Internet_of_Things%2C_IoT%29 (accessed: 20.08.2019).

[2] Kantyshev P. Internet veshchey otkryvaet kiberprestupnikam novoe pole deyatel'nosti [Internet of things opens new territory for cybercriminals]. *vedomosti.ru: website* (in Russ.). URL: https://www.vedomosti.ru/technology/articles/2016/02/29/631753-internet-veschei-otkrivaet-kiberprestupnikam-novoe-pole-deyatelnosti (accessed: 26.09.2019).

[3] Robachevskiy A.M. Smart and dangerous? Security problems of the Internet of things. *Internet iznutri*, 2017, no. 5 (in Russ.). URL: http://internetinside.ru/umnye-i-opasnye-voprosy-bezopasnosti-i/ (accessed: 20.08.2019).

[4] Sabanov A.G. Some features of authentication when accessing cloud services. *Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo* [Vestnik of Lobachevsky University of Nizhni Novgorod], 2013, no. 2(1), pp. 45–51(in Russ.).

[5] Grusho A.A., Zabezhaylo M.I., Smirnov D.V., et al About complex authentication. *Sistemy i sredstva informatiki* [Systems and Means of Informatics], 2017, vol. 27, no. 3, pp. 4–11. DOI: https://doi.org/10.14357/08696527170301 (in Russ.).
[6] Sabanov A.G. Assurance criteria to access claimant identification results. *Elektrosvyaz'*, 2019, no. 3, pp. 54–60 (in Russ.).
[7] Sabanov A.G. The method of authentication stringency level determination. *Elektrosvyaz'*, 2016, no. 8, pp. 56–61 (in Russ.).
[8] Sabanov A.G. User identification and e-authentication assurance levels forming. *Elektrosvyaz'*, 2015, no. 10, pp. 46–51 (in Russ.).
[9] Sabanov A.G. General analysis of international standards on identification and authentication. Part 1, 2. *Zashchita informatsii. Insayd*, 2016, no. 2, pp. 84–87, no. 3, pp. 70–73 (in Russ.).
[10] Ovchinnikov N.A., Misyurina K.V., Rudikova M.N., et al. "Smart home" formalized model of informational security. *Aprobatsiya*, 2016, no. 1(40), c. 49–51 (in Russ.).

Bratko D.V. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Berezin V.S. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Bratko D.V., Berezin V.S. The role of authentication in the IOT systems. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2020, no. 01(42). http://dx.doi.org/10.18698/2541-8009-2020-01-570.html (in Russ.).