УДК 004.056.53

Аспекты применения интернет вещей в образовании

Д. Н. Титов[1]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

* e-mail: titov200708@mail.ru

Аннотация. Интенсивный рост информатизации образования приводит к активному применению интернета вещей в нем. Широко используются решения в области процесса управления в образовании, сбора данных в режиме реального времени. Зона покрытия технологии покрывает весь мир. С ростом возможностей растут и угрозы. Рассмотрены вопросы безопасности интернета вещей в областях контроля доступа, программных интерфейсов интернет приложений, шлюзов безопасности, которые выступают в качестве посредника между IoT устройствами и сетью.

Ключевые слова: интернет вещей, контроль доступа, безопасность

Aspects of Using the Internet of Things in Education

D. N. Titov[1]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federatione

* e-mail: titov200708@mail.ru

Abstract: The intensive growth of informatization of education leads to the active use of the Internet of things in it. Solutions in the field of management process in education, data collection in real time are widely used. The coverage area of the technology covers the whole world. As opportunities grow, so do threats. The security issues of the Internet of Things in the areas of access control, Internet application programming interfaces, security gateways that act as an intermediary between IoT devices and the network are considered.

Keywords: internet of things, access control, security

Введение

Сегодня интенсивно осуществляется процесс информатизации общества. В нем принимают участие как образовательные учреждения, так и телекоммуникационные компании, и разработчики телекоммуникационных устройств.

Интернет вещей (Internet of Things, IoT) бурно развивающееся направление информатизации в последние годы. IoT предполагает взаимодействие определенных объектов друг с другом и с внешним миром посредством интернет-технологий. Главная цель IoT — сделать нашу жизнь проще и комфортнее.

Методы и материалы

Сегодня, что угодно имеет шанс стать IoT устройством, при условии, что его можно подключить к сети Интернет и трансформировать таким образом, чтобы передавать информацию. Система Интернета вещей обрабатывает и анализирует эту информацию, затем делает на ее основе какие-то выводы и предпринимает необходимые шаги для достижения поставленной цели.

С каждым годом растет количество подключенных IoT устройств, при том что темпы роста ежегодно растут. По информации с бизнес-портала Statista к 2021 году число устройств выросло до 82,5 млн, показав рост на 31%. В 2022 году 90% произведенных автомобилей будут подключены к интернету. Ожидается увеличение количества смарт-одежды до 24,75 млрд в 2023году. Число IoT устройств к 2025 году вырастет до 75,44 млрд [1].

Какие же решения предлагает современная индустрия IoT в системе образования:

- Улучшение процесса управления. Управлять университетом довольно сложно. Работа со всей документацией, отслеживание движения средств и другие подобные действия отнимают много времени и сил. Цифровизация процессов способна автоматизировать ряд этих задач.

- Сбор данных в режиме реального времени. Приложения IoT в образовании постоянно собирают и обрабатывают данные с разных датчиков. И эти данные могут так или иначе улучшить процесс обучения. Приведем несколько примеров: наблюдение и анализ успеваемости учащихся, следить за профессионализмом учителей, контролируемый доступ к данным об обучении.

- Покрытие по всему миру. Интернет вещей в образовании также означает охват по всему миру. Программное обеспечение, работающее в связке с IoT-устройствами, доступно в любой точке мира. Таким образом, мы получаем возможность объединять программы обучения воедино.

- Цифровизация организационного процесса. IoT-приложения в вузах позволяют автоматизировать многие организационные мероприятия во время обучения таких как внедрение индивидуальных трекеров посещаемости, студенческих облачных журналов, автоматической проверки тестов и других подобных решений.

Интернет вещей сегодня базируется на применении технологий использующих непрерывные вычислительные процессы, а так же известные технологии как:

- радиочастотная идентификация;
- обработка больших объемов;
- кибер-физические системы;
- определения местоположения на основе систем ГЛОНАСС и GPS;
- широкополосной связи G4 и G5;
- и других современных технологий.

Технология RFID применяется для идентификации объектов уже около 40 лет, а остальные из вышеперечисленных технологий относительно "молоды".

Результаты

Концептуально Интернет вещей относятся к классу информационных систем, построение которых должно использовать средства защиты информации, поскольку внесение изменений из вне в работу систем и реализация атак, может привести к последствиям.

Как обезопасить применение IoT-устройств.

Сети предоставляют злоумышленникам огромные возможности удаленного управления чужими IoT-устройствами. Поскольку сети включают как цифровые, так и физические компоненты, локальная безопасность IoT должна учитывать оба типа доступа к сети. Защита сети IoT включает в себя обеспечение безопасности портов, отключение переадресации портов и контролируемое открытие портов по необходимости; использование антивирусных программ, брандмауэров и систем обнаружения и предотвращения вторжений; блокировка неавторизованных IP-адресов и обеспечение исправлений и обновлений систем.

Контроль доступа к сети может помочь идентифицировать и инвентаризировать IoT - устройства, подключающиеся к сети. Это обеспечит основу для отслеживания и мониторинга устройств.

Сегментация. Устройства IoT, которым необходимо напрямую подключаться к Интернету, должны быть сегментированы в свои собственные сети и иметь ограниченный доступ к корпоративной сети. Сегменты сети должны отслеживать аномальную активность, где могут быть предприняты действия в случае обнаружения проблемы.

Шлюзы безопасности. Выступая в качестве посредника между устройствами IoT и сетью, шлюзы безопасности обладают большей вычислительной мощностью, памятью и возможностями, чем сами устройства IoT, что дает им возможность реализовывать такие функции, как брандмауэры, чтобы гарантировать, что хакеры не смогут получить доступ к устройствам IoT, которые они подключают.

Программный интерфейс приложения (API) являются основой большинства сложных веб-сайтов. Например, они позволяют собирать и анализировать информацию о успеваемости обучающихся. К сожалению, хакеры могут скомпрометировать эти каналы связи, что делает безопасность API необходимой для защиты целостности данных, отправляемых с устройств IoT в серверные системы, и обеспечения связи с API только авторизованных устройств, разработчиков и приложений. Например, утечка данных компании T-Mobile в 2018 году пример последствий плохой безопасности API [2]. Из-за «дырявого API» мобильный гигант раскрыл личные данные более 2 миллионов клиентов.

Заключение

Исходя из всего выше сказанного можно сделать вывод, что IoT устройства позволят качественно усилить систему образования университета и существенно улучшить систему его управления, но для этого потребуется проведение ряда работ по выстраиванию сетевой архитектуры университета с применением современных систем обеспечения сетевой безопасности, а также постоянная работа над программным интерфейсом приложения реализующего взаимодействие экосистемы университета с IoT устройствами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ITUT Y.2060 (06/2012) Overview of the Internet of things [Электронный ресурс. — Режим доступа: http://www.itu.inl/itut/recommendations/ rec.aspx?rec=Y.2060/.

2. Louchez A. An overview of loT technologies [Электронный ресурс]. Режим доступа: htlps://itunews.itu.int/ru/Note.aspx?Note=4373/.
Harmessing the Internet of Things for Global Development [Электронный ресурс]. Режим доступа: http://www.itu.int/net/pressoffice/press_releases/ 2016/02.aspx#. Vr7VU8]P3g.

3. Regulation and the Internet of Things. Global Symposium for Regulators. ITU News. 2015. № 4 IЭлектронный ресурс. Режим доступа: https://itunews.itu.int'/rv/Note.aspx?Note=6060/.

4. Короткова Т. Фонд развития интернет инициатив будет инвестировать в проекты в области "больших данных", носимых устройств и Интернета вещей [Электронный ресурс]. Режим доступа: http://bigdata.cnews.ju/news/line/frii_budet_in vestirovat_proekty_v.

5. ITU press releases 19/01/2016 [Электронный ресурс]. Режим доступа: www.itu.int/net/ pressoffice/press_releases/2016/pdf/ 02ru.pdf.
Golovanov V. B., Sabanov A. G. International standards of entities identification review И Elect rosvyaz. 2015. № 10. P. 3237.

6. Location matters Spatial standards for the Internet of Things. ITU News. 2013. № 9. Technology Watch [Электронный ресурсj. Режим доступа: https://itunews.itu.int/ru/ Note.aspx?Note=4574/.

7. ITU Internet Reports (2005), The Internet of Things [Электронный ресурс]. Режим доступа: https://www.itu. int/net/wsis/tunis/.../stats/Thc Internetof Things2005.pdf.

8. Левенков О. И., Сабанов А. Г. Применение электронной подписи на SIM-карте для обеспечения юридической силы электронным документам в системах M2M с использованием спутниковой системы ГЛОНАСС И Защита информации. Инсайд. 2015. №4.С. 5255.

9. Стандарты Интернета вещей [Электронный ресурс]. Режим доступа: http://iot.ru/ standartiinternetaveshey/.