**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

***Кара-Сал А.А., Левченко М.О. Информационная безопасность в сфере Интернета вещей // Академия педагогических идей «Новация». Серия: Научный поиск. – 2017. – № 04 (декабрь). – АРТ 12-эл. – 0,3 п.л. - URL: http://akademnova.ru/series-scientific-search***

***РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ***

**УДК 004.75**

**Кара-Сал Ай-Кат Айдысовна,**
**Левченко Мария Олеговна**
Студентки 3 курс, Факультет математической экономики, статистики и информатики
*Научный руководитель:* Староверова О.В., д.ю.н., доцент
РЭУ им. Г.В. Плеханова
г. Москва, Российская Федерация
wow.letsfight@ya.ru, karasal.97@mail.ru

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ИНТЕРНЕТА ВЕЩЕЙ

*Аннотация:* в рамках концепции Интернета вещей в данной статье рассматривается проблема обеспечения информационной безопасности Интернет вещей и фокусируется внимание на том, как какие меры могут быть применимы для обеспечения такой безопасности.

*Ключевые слова:* Интернет вещей, информационные технологии, процессы, информационные системы, информационная безопасность, управление Интернетом

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

**Kara-Sal Ai-Kat Aidysovna,**
**Levchenko Maria Olegovna**
3 course, Faculty of Mathematical Economics, Statistics and Informatics
Supervisor: Staroverova OV, Associate Professor
Plehanov Russian University of Economics
Moscow, Russian Federation
wow.letsfight@ya.ru, karasal.97@mail.ru

# INFORMATION SECURITY IN THE AREA OF THE INTERNET OF THINGS

*Abstract:* Within the concept of the Internet of things the problem of ensuring information security of the Internet of things is considered and the attention on how what measures can be applicable for ensuring such safety is focused.

*Keywords:* Internet of things, information technologies, processes, information systems, information security, management of the Internet

В настоящее время Интернет вещей имеет огромный потенциал для развития, но основным сдерживающим фактором являются бреши в сфере стандартизации и обеспечения безопасности. Если рассматривать проблему именно с точки зрения конфиденциальности, дальнейшее широкое внедрение датчиков и устройств в современные пространства, такие как дом, автомобиль и даже тело,

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

будет создавать особенные проблемы. Поскольку физические «вещи» в нашей повседневной жизни все чаще находят и обмениваются наблюдениями о нас, то потребители несомненно будут нуждаться в конфиденциальности ещё больше.

Устройства IoT могут стать более распространенными в нашей жизни, чем мобильные телефоны, и будут иметь доступ к нашим самым личным персональным данным, таким как номера социального страхования и банковские реквизиты. Незначительное количество проблем безопасности на одном устройстве, таком как мобильный телефон, могут стремительно переключиться на 50 и более проблем при рассмотрении нескольких устройств ввода-вывода соединенном в доме или бизнесе. И поэтому необходимо выявить потенциальные угрозы безопасности в свете важности доступа к устройствам IoT. Проблемы, связанные с безопасностью мобильных устройств, уже являются проблемой в эпоху всегда подключенных устройств[1]. А теперь подумайте, насколько значительными будут эти проблемы для бизнеса. По мере дальнейшего развития IoT будут миллиарды подключенных устройств - и каждый из них представляет потенциальный вход в вашу

[1] ПАВЛЕКОВСКАЯ И.В., СТАРОВЕРОВА О.В., УРИНЦОВ А.И. ВЛИЯНИЕ НАУЧНО-ТЕХНИЧЕСКОГО ПРОГРЕССА НА РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

ИТ-инфраструктуру, вашу компанию или личные данные.

Мы можем перечислить угрозы IoT по трем категориям: конфиденциальность, безопасность и надёжность. Эксперты утверждают, что угрозы безопасности Интернета вещей могут навредить существующим системам. Так как IoT будет иметь важные компоненты инфраструктуры, это будет являться потенциальной мишенью для национального и промышленного шпионажа.

Также при оценке потребностей в безопасности следует учитывать то, что IoT бесперебойно находится в работе. Появление контекстного обмена данными и автономных действий на основе данной информации позволяет распределить виртуальное присутствие на физический объект. Эти виртуальные присутствия начнут взаимодействовать и обмениваться контекстной информацией, и устройства будут принимать решения на основе этого контекстного устройства. Это приведет к значительным физическим угрозам вокруг национальной инфраструктуры, собственности, окружающей среды и так далее.

Поскольку различные объекты становятся частью взаимосвязанной области, мы должны учитывать, что эти устройства могут потерять физическую безопасность, так как они будут расположены в неблагоприятной среде. Это позволит злоумышленникам перехватывать,

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

извлекать или изменять данные, и они могут вмешиваться в системы управления и изменять функциональность.

Безопасность должна строиться как основа систем IoT, с тщательной проверкой достоверности, аутентификацией, проверкой данных и всеми данными, которые необходимо зашифровать. На уровне приложений организациям, занимающимся разработкой программного обеспечения, необходимо лучше писать код, который является стабильным, устойчивым и заслуживающим доверия, с лучшими стандартами разработки кода, обучением , анализом угроз и тестированием. Поскольку системы взаимодействуют друг с другом, важно иметь согласованный стандарт совместимости, который безопасен и действителен.

На сегодняшний день существуют организации, занимающиеся разработкой стандартов в сфере Интернета вещей. На данном этапе развития IoT уже утверждены первые рекомендации МСЭ-Т[2], посвященные специально Интернету вещей: Y.2060 «Обзор Интернета вещей», Y.2063 «Основа WEB вещей» и Y.2069 «Термины и определения Интернета вещей» и др.

[2]Рекомендация МСЭ-Т Y.2060 (06/2012). Международный союз электросвязи (ITU-T) – Internet of Things Global Standards Initiative Focus Group

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

В рекомендации Y.2060 прописаны следующие возможности обеспечения безопасности: общие возможности обеспечения безопасности и специализированные возможности обеспечения безопасности.

Общие возможности обеспечения безопасности не зависят от приложений и включают:

- на уровне приложения: авторизацию, аутентификацию, защиту конфиденциальности и целостности данных приложения, защиту неприкосновенности частной жизни, аудит безопасности и антивирусную программу;
- на уровне сети: авторизацию, аутентификацию, конфиденциальность данных об использовании и данных сигнализации, а также защиту целостности данных сигнализации;
- на уровне устройства: аутентификацию, авторизацию, проверку целостности устройства, управление доступом, защиту конфиденциальности и целостности данных.

Специализированные возможности обеспечения безопасности тесно связаны с требованиями приложений, например, требованиями безопасности мобильных платежей.

Проанализировав содержание стандарта, были выявлены узкие места: отсутствие числовых данных,

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

описывающих определённые характеристики устройств (например, частота); отсутствие подробного описания процессов, обеспечивающих безопасность устройств (например, как должна осуществляться аутентификация или защита целостности данных).

Без сплошной структуры нижнего уровня создается больше угроз с каждым устройством, добавленным в IoT. Необходим безопасный и надежный IoT с защитой конфиденциальности, жестким компромиссом и отлаженной работой.

Нами были предложены способы обеспечения безопасности, связанные не только с технической стороной защиты устройств, но и непосредственно с жизненным циклом «вещи»:

- Мониторинг безопасности с первого дня
- Жизненный цикл устройства, проверка обновлений
- Контроль доступа и аутентификация устройства
- Подготовка к будущим потенциальным нарушениям безопасности

Четкий акцент на безопасности необходим с первого дня, если речь идет о незрелых технологиях и слаборазвитых рынках. Если планируется развивать свою собственную инфраструктуру IoT или развертывать существующее решение, необходимо проводить

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

исследования и всегда быть информированным о развития данной сферы.

В спешке, чтобы вывести на рынок новые продукты и услуги, многие компании не обращают внимание на долгосрочную поддержку. Крупные продавцы телефонов не обновляют программное обеспечение на телефонах, которые были закуплены и не были проданы в течение 2-3 лет, поэтому представьте, что произойдет с устройствами стоимостью 20 долларов, которые могут быть в вашей сети в течение многих лет.

Реализация контроля безопасного доступа и аутентификации устройств очевидно. Данный вопрос уже был рассмотрен Международным союзом электросвязи. Создание элементов управления доступом и методов аутентификации, которые могут быть реализованы на дешевых и компактных устройствах IoT без ущерба для пользовательского интерфейса или добавления ненужного оборудования, сложнее, чем кажется. Несомненно, недостаток вычислительной мощности является еще одной проблемой, поскольку самые передовые методы шифрования просто не смогут работать очень хорошо, если вообще будут.

Также важно изучить угрозы и потенциальных злоумышленников, прежде чем бороться за безопасность IoT. Уровень угрозы не является одинаковым для всех устройств: кто-то взломал плюшевого мишку вашего соседа, а у вас взломали машину. Необходимо снизить

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

риск взлома данных и правильно защищать каналы передачи данных. Однако, чтобы осуществить это, вам сначала нужно изучить угрозу.

Появление Интернета Вещей открывает широкие возможности в изучении насущных проблем в сфере защиты правовых интересов пользователей. Более глубокое понимание различий между сетью, операционными системами вещей, прикладным программным обеспечением и их применением позволит создать широкий набор практических методов для множества заинтересованных сторон как в виртуальном, так и в физическом мире.

На основании всего вышесказанного можно выделить основные угрозы и сдерживающие факторы развития интернета вещей:

- Отсутствие согласованных стандартов: государство и международные организации должны провести системную работу по адаптации технологических стандартов и протоколов к новым технологическим условиям;
- Недостаточно проработанное правовое поле для применения ряда технологических решений: появляется возможность отслеживать местоположение людей, и возникает риск, что воспользоваться этой информацией смогут злоумышленники;

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

- Неполноценное обеспечение кибербезопасности: недостаточная защита данных в глобальных сетях и вторжение IoT в частную жизнь;
- Отсутствие понимания необходимости рассмотрения безопасности «вещей» с точки зрения жизненного цикла.

Поэтому возможными направлениями в обеспечении безопасности Интернета вещей являются:

- Создание единого пространства, специализирующегося на соединении непосредственно самих «вещей». Проектом данной сети является Mongoose OS[3]- полноценная экосистема для подключения и взаимодействия между собой разнообразных физических устройств, от кружек и холодильников до микроволновых печей и автомобилей;
- Создание единых стандартов. Проектом стандарта Интернета вещей в России является Narrow Band Fidelity (NB-FI), разработанный Ассоциацией интернета вещей (АИВ). NB-FI является стандартом сотовой связи для устройств телеметрии с низкими объёмами обмена данными. В нём предложены: частота работы устройств; расстояние, на котором передатчики могут обмениваться данными; срок службы устройств;
- Повышение качества существующих продуктов и сервисов за счет обеспечения бесперебойности их

[3] Тотальный интернет: кто строит единую сеть для всех девайсов в мире

**Всероссийское СМИ**
**«Академия педагогических идей «НОВАЦИЯ»**
**Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.**
**(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)**

**Сайт:** akademnova.ru
**e-mail:** akademnova@mail.ru

работы, превентивного устранения возможных неполадок, оптимизации использования сырья и сокращения влияния человеческого фактора.

- Таким образом, была освещена проблема обеспечения безопасности устройств Интернета вещей и рассмотрены возможные пути её решения, которые на наш взгляд являются наиболее перспективными и достаточно легко осуществимыми.

**Список использованной литературы:**

1. Барсков А. «IoT как инструмент цифровой экономики» /
   - https://www.osp.ru/lan/2017/05/13052169 (дата обращения: 18.11.2017).
2. Рекомендация МСЭ-Т Y.2060 (06/2012)
3. Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns / https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things (дата обращения: 22.11.2017).
4. Тотальный интернет: кто строит единую сеть для всех девайсов в мире https://www.rbc.ru/magazine/2017/12/5a0b34be9a79476c6a7dfcbf (дата обращения: 09.11.2017).
5. А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков ИНТЕРНЕТ ВЕЩЕЙ. Самара –: 2015. 10 с.
6. ПАВЛЕКОВСКАЯ И.В., СТАРОВЕРОВА О.В., УРИНЦОВ А.И. ВЛИЯНИЕ НАУЧНО-ТЕХНИЧЕСКОГО ПРОГРЕССА НА РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА. Москва –: 2017.

***Дата поступления в редакцию: 08.12.2017 г.***
***Опубликовано: 15.12.2017 г.***