# Особенности защиты информации в Интернете вещей

А.М. Полегенько

***Аннотация*—Вопросы защиты информации становятся все более актуальными с развитием сетевых технологий. Сегодня нас окружает все большее количество гаджетов, способных обмениваться друг с другом данными с участием пользователя или без него. Объединяясь в сеть, различные устройства от фитнес-трекеров до дистанционной системы управления электроснабжением дома, обрабатывают и передают информацию, относящуюся к пользователю. По мере того, как Интернет становится более коммерциализированным, большее внимание уделяется защите персональных данных, финансовых операций и противостоянию киберугрозам. Учитывая особенности устройств, а также их различную природу, вопросы безопасности сетевого взаимодействия требуют рассмотрения новых аспектов. Исследования последних лет показывают, что семь из десяти популярных смарт-устройств уязвимы для потенциальных атак. Большинство выявленных угроз безопасности были связаны с незашифрованными данными, сбором персональных данных, уязвимыми пользовательскими интерфейсами и небезопасными соединениями. Основные проблемы обеспечения безопасности обусловлены тем, что существующие методы и средства защиты изначально разрабатывались для настольных компьютеров, и не учитывали особенности и ограничения устройств Интернета вещей. На сегодняшний день, наряду с адаптацией существующих технологий защиты, важными являются вопросы стандартизации в области Интернета вещей.**

***Ключевые слова*— Интернет вещей, информационная безопасность, смарт-устройства, сетевое взаимодействие, построение системы защиты, стандартизация Интернета вещей**

## I. Введение

Интернет вещей (Internet of Things, IoT) – концепция, предполагающая объедение в сеть устройств (вещей), способных взаимодействовать друг с другом на основе встроенных технологий, которые поддерживаются данной сетью. Устройствами (вещами) являются «умные» гаджеты, «умная» техника и другие сетевые устройства, которые могут быть использованы в обиходе человека или его дома.

Безопасность Интернета вещей становится ключевым аспектом при построении таких сетей. Получив доступ к одному устройству, злоумышленник может проникнуть в сеть, и тогда уже угрозам подвергается любая конфиденциальная информация. Отсюда вытекает актуальность вопросов безопасности информации в подобных сетях, где необходимо учитывать ограничения устройств, входящих в них.

Понятие «Интернет вещей» было предложено Кевином Эштоном, в Массачусетском технологическом институте в 1999 году. С тех пор концепция начала свое стремительное развитие и положила начало для многих стартапов.

Применение традиционных методов защиты устройств Интернета вещей, таких как шифрование, идентификация/аутентификация и внедрение физических мер обеспечения безопасности, требует их существенного реинжиниринга и адаптации, так как устройства имеют множество ограничений. Например, хранение вредоносных сигнатур и «черных списков» может требовать много места на диске, что является не всегда возможным. Интернет вещей, как правило, состоит из портативных устройств с низким электропотреблением, малым форм-фактором и ограниченными возможностями. Так же, чаще всего, устройства являются неуправляемыми, т.е. работают без участия оператора, который мог бы ввести учетные данные или принять решение о том, насколько команда или приложение являются доверенными, поэтому устройства должны самостоятельно принимать подобные решения. Архитектура систем Интернета вещей требует наличия беспроводных сетей и облачной базы данных для связи.

## II. Структура Интернета вещей

Структуру Интернета вещей в общем случае можно представить как совокупность следующих элементов:

- непосредственно сами «вещи» – то есть устройства, датчики и сенсоры, физические объекты, которые в привычном понимании не предназначались для подключения к сети. Такие устройства должны быть однозначно идентифицированы с помощью программно-аппаратных средств – это могут быть RFID-метки, штрих-коды, MAC-адреса и др.;
- сеть – вариации проводных и беспроводных сетей, поддерживающих разные протоколы и стандарты и построенных с помощью маршрутизаторов и шлюзов;
- центры обработки данных – некие хранилища и вычислительные ресурсы, задействованные в сборе, анализе и обработке данных «сети вещей» – например, это могут быть «облака» или «туманные узлы».

Таким образом, подходы к построению системы безопасности должны рассматривать каждый из структурных элементов и еще решать проблемы, вытекающие при объединении нескольких устройств и создании сети.

Исходя из масштабов сети, выделяют 4 уровня Интернета вещей [1]:

- 1 уровень включает отдельные объекты – «вещи»;
- 2 уровень предполагает создание сети «вещей» на уровне отдельных потребителей, объединяя устройства личного пользования (например, смарт-дом);
- 3 уровень охватывает жизнь целых городов, т.е. подразумевает, например, концепцию создания смарт-городов;
- 4 уровень предполагает объединение всего мира посредством Интернета вещей.

Соответственно, можно говорить о возможности масштабирования сетей подобного рода.

## III. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ ВЕЩЕЙ

«Вещами» сегодня являются не только предметы личного пользования обычных потребителей, но и различная техника, активно применяемая во множестве сфер деятельности – торговле, транспорте, медицине, строительстве, банкинге, спорте и др. Отсюда следует, что Интернет вещей чаще всего представляет собой гетерогенную сеть, т.е. устройства различных классов и видов объединяются и взаимодействуют между собой.

Рекомендации по защите информации в сети Интернета вещей направлены на повышение безопасности устройств, сетей и данных.

В первую очередь, устройства Интернета вещей, как правило, за счет своей портативности и мобильности, доступны злоумышленникам физически, и могут быть украдены для получения доступа к конфиденциальным данным и установления связи с другими устройствами сети. Для предотвращения этой угрозы нужно обеспечить физическую защиту, например, путем использования защитных крышек на устройствах или корпусов, предусматривающих ограничения прямого доступа к устройствам. Кроме непосредственного доступа, устройства могут предоставлять удаленный доступ для обновления конфигурационных данных или программного обеспечения. Для защиты от этого, необходимо предусмотреть закрытие программных портов и применение надежных паролей на уровне загрузки и обновления прошивок, которые предотвратят доступ к устройству в случае его компрометации.

При этом, с другой стороны, многие устройства Интернета вещей становятся уязвимыми для кибератак, поскольку их программное обеспечение не обновляется своевременно. Для минимизации подобных рисков рекомендуется внедрять автоматическое обновление по умолчанию, потому как, даже если обновления программного обеспечения выпускаются своевременно, потребители не всегда устанавливают их вручную сразу после выхода.

Так же следует уделять внимание организации хранения данных на самих устройствах, потому как зачастую эта информация имеет отношение к персональным данным пользователя, данным финансовых транзакций и данным о критически важных объектах различных сфер деятельности.

Безопасность должна быть обеспечена как на протяжении всего времени функционирования изделия, так и после вывода его из эксплуатации. Криптографические ключи должны храниться в энергонезависимой памяти устройства не в открытом виде. Кроме этого, можно предусмотреть утилизацию устройств, выведенных из эксплуатации.

Для защиты сетей, во-первых, должны быть предусмотрены методы «сильной аутентификации», включая, например, двухфакторную аутентификацию, присвоение «жестко» заданных уникальных идентификационных и аутентификационных данных, а так же использование современных защищенных протоколов [2]. Криптографические алгоритмы должны быть адаптированы к сети Интернета вещей.

С целью минимизации рисков осуществления в адрес устройств атак типа «отказ в обслуживании» рекомендуется предусматривать ограничения пропускной способности сети устройств Интернета вещей, как на программном, так и на аппаратном уровнях. В случае выявления подозрительного трафика устройства должны обеспечивать возможность сигнализации с последующим анализом выявленной угрозы.

Защита данных, в первую очередь, обеспечивается путем применения криптографических методов, адаптированных под особенности устройств с ограниченными возможностями. В случае компрометации устройства должна быть предусмотрена возможность экстренного стирания ключевой информации, используемой в криптографических операциях.

Устройства Интернета вещей должны передавать и обрабатывать только ту информацию, которая необходима для реализации их основных функций – как правило, это сбор информации о состоянии окружающей их среды или о пользователе. Отсюда следует, что необходимо с вниманием относиться к информации, циркулирующей в сети ИВ, сводя к минимуму риск утечки конфиденциальной информации.

Кроме неоднородности сетей, особенностью Интернета вещей так же является то, что устройства

обладают неодинаковыми вычислительными ресурсами, пропускной способностью и поддерживают разные технологии и протоколы. Отсутствие единых стандартов и протоколов остается серьезной проблемой при построении сети «вещей». Так же многие «вещи» обладают ограниченными возможностями электропитания и должны поддерживать режимы энергосбережения.

Перечисленные особенности Интернета вещей накладывают ограничения и при построении системы безопасности в такой сети. Привычных методов защиты информации в беспроводных сетях может быть недостаточно, или же они не могут быть применимы в связи с ограничениями, которые накладывает сеть Интернета вещей.

Основными методами обеспечения безопасности, как и в традиционных сетях, остаются шифрование, идентификация/аутентификация, внедрение физических мер безопасности.

Система безопасности должна быть спроектирована так, чтобы предусмотреть защиту для устройств и шлюзов, сети передачи, а также приложений, которые разворачиваются для обеспечения функционирования устройств.

Шифрование является широкоприменяемым, эффективным и достаточно гибким решением для обеспечения конфиденциальности информации и создания системы защиты. Однако любое шифрование, а особенно надежное, требует увеличения производительности и дополнительных вычислительных ресурсов, что является не всегда возможным в условиях Интернета вещей.

Что же касается аутентификации, то исследователями было предложено достаточно большое количество подходов, которые могли быть внедрены для решения проблем безопасности [2, 3]. Одним из распространенных методов является двухфакторная аутентификация. Например, аутентификация на основе одноразовых паролей (OTP). При таком подходе после предоставления идентификационных данных, пользователю или устройству необходимо предъявить еще и одноразовый пароль, сгенерированный центром распределения ключей, тем самым подтверждая свою подлинность. Такой метод не требует от устройств дополнительных вычислительных ресурсов или хранилищ, однако является неприменимым для устройств, которые, например, просто не могут поддерживать возможность ввода полученного одноразового пароля. Такая же проблема актуальна и для метода аутентификации, вторым фактором которого является аппаратный идентификатор.

Другие исследования предлагают использовать при аутентификации концепцию «цифровых воспоминаний», которая решала бы проблему запоминания пользователями сложных паролей. Однако такой метод накладывает ограничения на ресурсы устройств.

Предлагаемые методы так же включают и аутентификацию с применением криптографии на основе эллиптических кривых. Несмотря на то, что в этом случае необходимые базовые параметры эллиптических кривых вычисляются не самими устройствами, после вычисления требуется передача достаточно большого объема данных, что может быть ограничено пропускной способностью сети [2].

Таким образом, различные существующие методы аутентификации являются применимыми для отдельной сети и отдельного класса устройств. Применение единых методов и средств затрудняется отсутствием стандартизации и гетерогенностью подобного рода сетей.

## IV. ПОДХОД К ЗАЩИТЕ НА ОСНОВЕ «ПРОФИЛЕЙ БЕЗОПАСНОСТИ»

Для обеспечения безопасности Интернета вещей может быть предложен подход, который имеет в своей основе концепцию «профилей безопасности». Это означает, что на каждом из уровней Интернета вещей, описанных выше, должна быть обеспечена безопасность в соответствии с неким набором метрик «профиля безопасности». Так как представленные уровни имеют иерархическую структуру, и каждый более высокий уровень можно рассматривать как совокупность элементов более низких уровней, то и «профили безопасности» будут иметь наследственность, т.е., например, для обеспечения безопасности смарт-дома необходимо обеспечить безопасность каждого из устройств и предусмотреть дополнительные меры по защите взаимодействия между узлами.

Вводимые метрики безопасности должны удовлетворять следующим основным показателям:

1) Конфиденциальность и целостность – наиболее важные свойства информации, обеспечиваемые стандартными методами с учетом особенностей устройств сети.
2) Надежность – данная метрика особенно актуальна для критически важных объектов, где сбои в работе могут привести к серьезным последствиям.
3) Масштабируемость – сеть должна поддерживать возможность расширения без ущерба функциональности или безопасности.
4) Поддержка работоспособности (стабильность) – поддерживаемые протоколы, технологии и приложения должны иметь возможность своевременного обновления и сохранения работоспособности устройств.
5) Обнаружение вторжений – в сети должны

быть реализованы меры по своевременному обнаружению атак или любых других попыток нарушения работы.

6) Своевременность – метрики, которые должны выражать способность сети реагировать на происходящие события.

Предлагаемый набор меток является минимальным и может быть дополнен и расширен, в зависимости от рассматриваемых архитектур сети.

Обозначим Интернет вещей 1-го уровня (каждое отдельно взятое устройство) за $X_1$, 2-го уровня (сеть смарт-дома) – за $X_2$, 3-го уровня (смарт-город) – за $X_3$, 4-го уровня (всемирная сеть Интернета вещей) – за $X_4$. Тогда «профили безопасности» можно обозначить как $П$ и представить в виде совокупности метрик безопасности: $П\ \{a_1, a_2, \ldots, a_m\}$, где $a_1, a_2, \ldots, a_m$ – метрики, определяющие необходимые требования безопасности.

Таким образом, общую схему наследственности «профилей безопасности» в Интернете вещей можно представить в следующем виде:

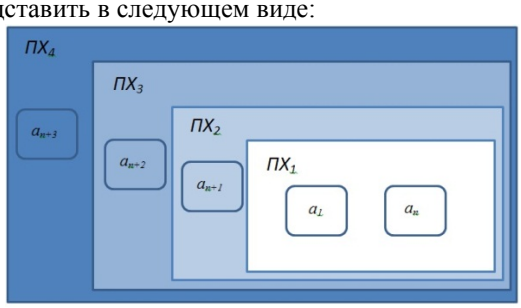


Рис.1 Профили безопасности

Для обеспечения безопасности отдельных смарт-устройств необходимо предусмотреть выполнение требований $[a_1;a_n]$. В случае, если в устройстве обеспечивается выполнение заданных требований, мы можем о говорить о «профиле безопасности» устройства – $ПХ_1$. Для обеспечения безопасности «смарт-дома» необходимо, чтобы все устройства, включенные в него, обладали «профилями безопасности», а также выполнялось дополнительное требование $a_{n+1}$, касающееся безопасного взаимодействия данных устройств.

Такая наследственность позволила бы оптимизировать создание систем безопасности в концепции Интернета вещей, особенно для высших уровней.

## V. ЗАКЛЮЧЕНИЕ

Таким образом, для обеспечения безопасности устройств Интернета вещей, в первую очередь, необходим комплексный подход, который предусматривал бы не только внедрение актуальных методов защиты, но и учитывал ограничения, накладываемые особенностями функционирования подобных устройств. Существующие методы защиты, такие как шифрование, аутентификация, физическая защита от несанкционированного доступа должны быть применены для каждого «профиля безопасности» по предлагаемому набору метрик. Предполагается, что внедрение подхода на основе «профилей безопасности» позволит обеспечивать непрерывность защиты на протяжении всего жизненного цикла устройств.

Подход на основе «профилей безопасности» на практике может быть затруднен, опять же, в связи с отсутствием единых стандартов, а также принятых нормативно-правовых документов. Однако, 17 октября 2017 года представителями Минкомсвязи России, «Росатома», «Ростелекома», Университета ИТМО и МГУ им. М.В. Ломоносова подписан меморандум о создании Национального консорциума развития и внедрения цифровых технологий в сфере городского управления, одной из основных задач которого является реализация концепции «Умные города России». В апреле 2018 года Ассоциация интернета вещей (АИВ), созданная фондом развития интернет-инициатив (ФРИИ), внесла в Росстандарт проект нового стандарта связи для интернета вещей – Narrow Band Fidelity (NB-FI). В 2019 году планируется проведение первого заседания, посвященного вопросам стандартизации в области Интернета вещей в России, что положит начало развития подобного рода сетей в нашей стране.

## БИБЛИОГРАФИЯ

[1] DB Best Technologies [Электронный ресурс]. – The Internet of Things (IoT) explained. – Электрон.данные. – Redmond, 2016. – режим доступа: https://www.dbbest.com/blog/the-internet-of-things/.

[2] Preethy Wilson. Inter-Device Authentication Protocol for the Internet of Things [Текст]: диссертация / Preethy Wilson; University of Victoria, 2017 – 4-10 с.

[3] M. A. Crossman and H. Liu. Study of authentication with IoT [Текст]: материалы конференции/ M. A. Crossman and H. Liu; 2015 IEEE International Symposium, 2015 – 1–7 с.

Полегенько А.М., аспирант Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики. email: polegenko@telros.ru

# Specificity of information security in the Internet of Things

A.M. Polegenko

***Abstract* – Information security issues are becoming more relevant with the network technologies developing. Today we are surrounded by an increasing number of gadgets that can share data with each other with or without the user. By connecting to the network, various devices from fitness trackers to remote control system of power supply at home, process and transmit information related to the user. As the Internet becomes more commercialized, more attention is paid to the protection of personal data, financial transactions and countering cyber threats. Given the characteristics of the devices, as well as their different nature, network security issues require consideration of new aspects. Studies in recent years show that seven out of ten popular smart devices are vulnerable to potential attacks. Most of the security threats identified were related to unencrypted data, personal data collection, vulnerable user interfaces, and insecure connections. The main security concerns stem from the fact that existing security methods and tools were originally developed for desktop computers and did not take into account the characteristics and limitations of IOT devices. Today, along with the adaptation of existing protection technologies, the issues of standardization in the field of the Internet of things are important.**

***Keywords* – Internet of things, information security, smart devices, network interaction, building a security system, standardization of the Internet of things**