СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2017. – № 4 (90).** – 128–143

СООБЩЕНИЯ

УДК 004.492.3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ*

К.А. ДОНСКОЙ[1], Л.С. ЛЕВИН[2], Е.В. ПОПАНТОНОПУЛО[3]

[1] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студент кафедры защиты информации. E-mail: kirdon96@mail.ru*
[2] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студент кафедры защиты информации. E-mail: mynameislev@bk.ru*
[3] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: pev@atlas-nsk.ru*

Данная работа затрагивает проблемы организации информационной безопасности применимо к сфере Интернета вещей. В работе рассматриваются определение Интернета вещей, сформировавшаяся архитектура, используемые технологии реализации, возможные угрозы безопасности и концепция безопасности. Задачей нашей работы является выявление проблем создания защищенной системы в сфере Интернета вещей и пути устранения данных проблем. Проанализировав архитектуру Интернета вещей, обращаем внимание на используемые технологии: сети, операционные системы, техническое исполнение, каналы связи, методы обработки данных, протоколы передачи информации, находим уязвимые места, приводим примеры сценариев атак на устройства семейства Интернета вещей. Исходя из обнаруженных уязвимостей анализируем набор средств и методов обеспечения информационной безопасности и подбираем решения, соответствующие требованиям Интернета вещей. Также мы рассматриваем применение уже существующих технологий и решения компаний лидеров разработки информационных технологий, таких как Cisco. Множество используемых уровней системы Интернета вещей и различия в технологиях не позволяют использовать для защиты единую модель безопасности, поэтому компания Cisco предлагает разграничивать решения безопасности по четырем уровням архитектуры и объединить методы защиты информации в так называемую среду безопасности. Подробное рассмотрение готовых решений и подходов к обеспечению безопасности в сфере Интернета вещей показывает необходимость в разработке стандарта для построения систем Интернета вещей, который бы сузил перечень используемых компонент и технологий, позволив построить единую модель безопасности Интернета вещей, соответствующую концепции безопасности.

* Статья получена 29 июля 2017 г.

Ключевые слова: Интернет, мониторинг, информация, технологии, угрозы, защита, сеть, атаки, канал, архитектура, сценарии, система, безопасность, управление, контроль

DOI: 10.17212/2307-6879-2017-4-128-143

ВВЕДЕНИЕ

IoT (Интернет вещей) – это сеть связанных через Интернет объектов, способных собирать данные и обмениваться данными, поступающими со встроенных сервисов.

Отдел стандартов связи МСЭ (Международный союз электросвязи – International Telecommunication Union) опубликовал Рекомендацию Y.2060, озаглавленную «Обзор Интернета вещей» (Overview of the Internet of Things). В этом документе содержатся следующие определения, описывающие охват IoT.

Интернет вещей (IoT) – глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

Вещь – предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

Устройство – элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

Интернет вещей состоит из слабо связанных между собой разрозненных сетей, каждая из которых была развернута для решения своих специфических задач. В офисных и жилых зданиях устанавливается множество сетей для управления отоплением, вентиляцией, кондиционированием, телефонной связью, безопасностью, освещением. По мере развития Интернета вещей эти и многие другие сети будут подключаться друг к другу и приобретать все более широкие возможности в сфере безопасности, аналитики и управления (рис. 1). В результате Интернет вещей приобретет еще больше возможностей открыть человечеству новые, более широкие перспективы.

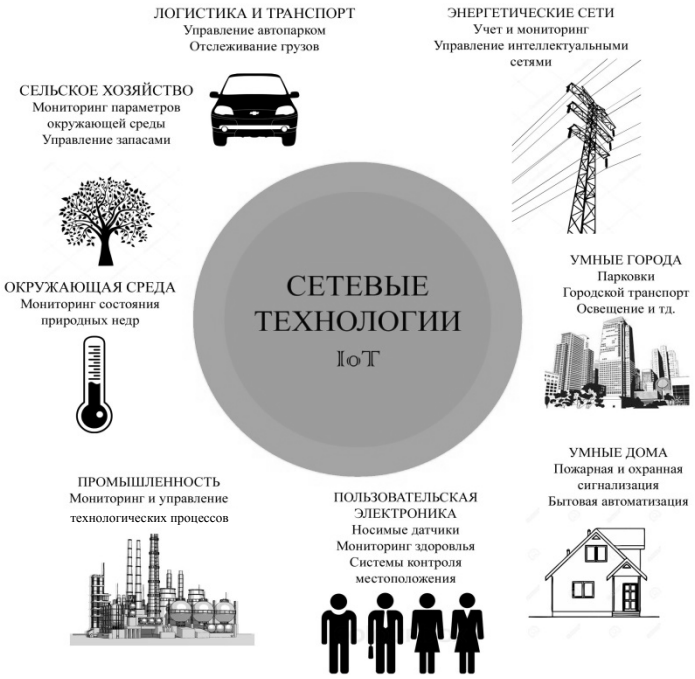

Рис. 1. Разнообразие областей применения

1. АРХИТЕКТУРА IoT

Архитектура IoT состоит из четырех уровней:

- устройства,
- связь,
- обработка,
- управление данными.

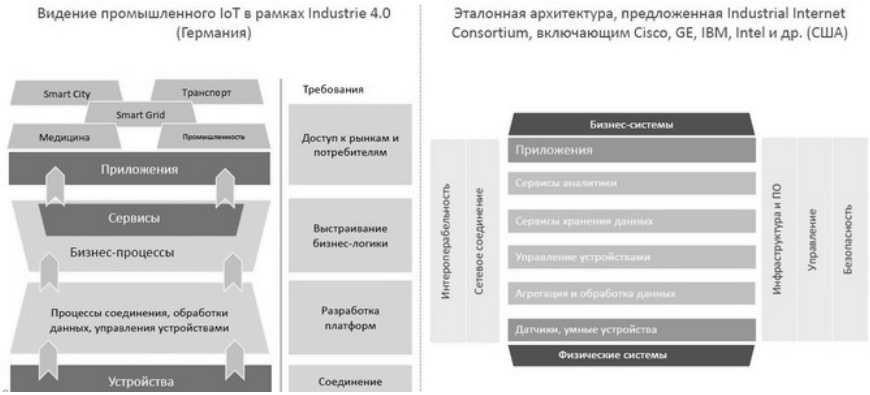

Рис. 2. Эталонные модели Германии, США

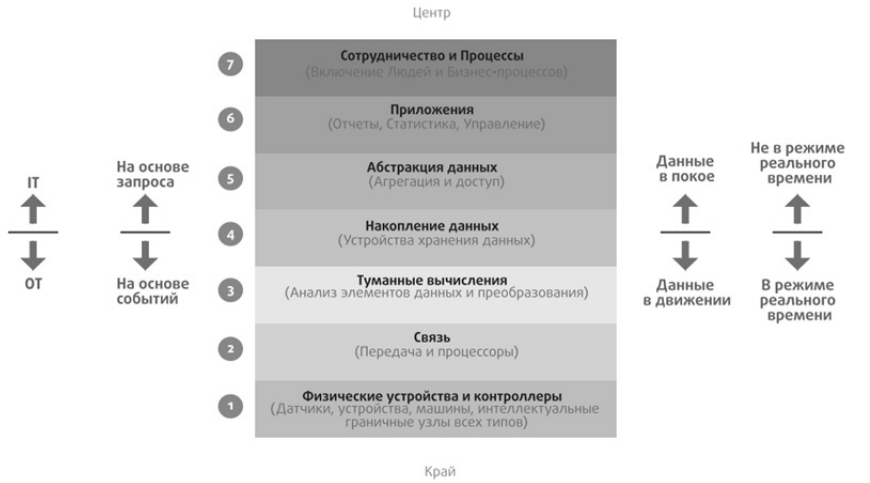

Рис. 3. Эталонная модель Всемирного форума IoT

2. УГРОЗЫ БЕЗОПАСНОСТИ IOT

Слабые места IoT:

- стандартные учетные записи от производителя, слабая аутентификация;
- отсутствие поддержки со стороны производителя для устранения уязвимостей;

- трудно или невозможно обновить ПО и ОС;
- использование текстовых протоколов и ненужных открытых портов;
- используя слабость одного гаджета, хакеру легко попасть во всю сеть;
- использование незащищённых мобильных технологий;
- использование незащищённой облачной инфраструктуры;
- использование небезопасного ПО.

Пример угроз для частных лиц

Если говорить про системы автоматизации для частных лиц, то из описанного выше наиболее важными представляются вопросы обеспечения контроля доступа к системе, безопасных коммуникаций между ее элементами, а также устойчивости к атакам. При этом по финансовыми причинам часто приходится идти на компромисс между стоимостью оборудования и уровнем защиты. К сожалению, адекватно оценить риски, особенно если речь идет о системах жизнеобеспечения дома, в данном случае очень сложно.

Дополнительно стоит отметить желательность использования надежных каналов связи и резервных линий коммуникаций, гибкие возможности системы при работе в автономном режиме, а также обеспечение конфиденциальности. Еще одним вопросом, который, к сожалению, редко решается производителями массового оборудования, является мониторинг работы, анализ и уведомления о нештатных ситуациях.

Конфиденциальность личных данных сегодня часто обсуждается в применении ко многим областям, но, пожалуй, именно в современных гаджетах и носимой электронике проблема защиты персональных данных особенно актуальна. В частности, подавляющее большинство фитнес-трекеров работают совместно с собственными облачными сервисами для хранения и обработки данных, и пользователям необходимо соглашаться с многостраничными документами условий использования сервисов, если они хотят воспользоваться данным устройством.

Примеры угроз для бизнеса

IoT встречается не только в частном секторе, но и в множестве коммерческих областей, включая транспорт, системы автоматизации, мониторинг окружающей среды и медицину. В каждой из них потребители могут встретиться с уникальными угрозами. Например, отслеживание транспорта может раскрыть бизнес-стратегии компании, а неверные показания датчиков могут привести к аварии и порче дорогостоящего оборудования.

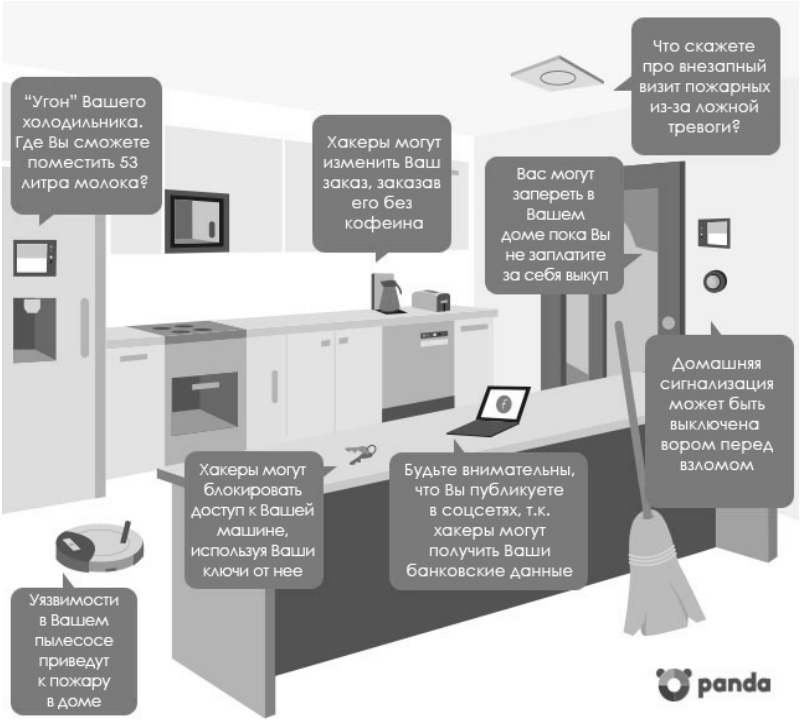

Рис. 4. Сценарии хакерских атак на IoT

В общем случае схема системы с использованием IoT состоит из конечных устройств, опциональных шлюзов, сети и вычислительных центров. Если предположить, что в существующей инфраструктуре серверов и основных коммуникаций уже реализованы все необходимые технологии (в частности, для корпоративных сетей и баз данных), то для IoT необходимо задуматься о стратегии защиты конечных точек, шлюзов и их коммуникаций. Конечные точки чаще всего работают в условиях ограниченных ресурсов, включая вычислительные мощности, объемы памяти и энергопотребление. Для них может быть очень сложно или даже невозможно использовать такие технологии, как выделенные чипы безопасности, контроль привилегий, защиту памяти или виртуализацию. Кроме того, недостаток ресурсов может приводить к слабой устойчивости к атакам, направленным на отказ в обслуживании. Вопрос дополнительно усложняется тем, что все чаще устройства основаны на собственных достаточно сложных микроконтролле-

рах и поддерживают удаленное обновление встроенного программного обеспечения. Так что встают задачи по обеспечению контроля корректности работающего на устройствах кода. В качестве одного из вариантов здесь предлагаются системы обеспечения доверенной среды исполнения, основанные на аппаратно-программных решениях.

Предлагаемый некоторыми компаниями дополнительный уровень в виде локальных шлюзов в определенных ситуациях может способствовать повышению уровня безопасности. В этом случае конечные устройства не подключены непосредственно к сети, а общаются исключительно с мостом, что позволяет упростить защиту их локальных коммуникаций. При этом шлюз, обладая существенно большими вычислительными ресурсами, уже способен реализовать традиционные технологии защиты коммуникаций при обмене данными с вычислительным центром.

Когда речь заходит о безопасных коммуникациях, стоит учитывать такой немаловажный фактор, как удобство использования. Очень желательно обеспечивать установление связей без сложной ручной настройки, но при этом не в ущерб уровню защиты, согласованно с политиками безопасности и под контролем системы управления ИТ. Для решения этой задачи можно предложить современные протоколы для аутентификации и шифрования трафика, требующие адаптации для повышения эффективности работы на платформах IoT. Отметим, что при подготовке программного обеспечения iRidium данным вопросам было уделено особое внимание. В частности, для связи панелей и серверов между собой используются защищенные протоколы.

При этом решение должно корректно отрабатывать и нештатные ситуации (например, потерю связи). Учитывая все большее распространение специализированных алгоритмов и аналитики, здесь важно обеспечить корректность и согласованность получаемых данных. Кроме двух описанных выше вопросов есть и еще один, возможно, не менее важный. Речь идет о жизненном цикле продуктов. Технологии обеспечения безопасности необходимы на всех этапах, начиная от разработки и создания и заканчивая утилизацией.

Основные инструменты безопасности, необходимые для защиты IoT:

- идентификация и аутентификация;
- защита технических каналов связи;
- сертификация с использованием шифрования;
- репликация и защита баз данных;
- контроль процесса релизов и изменений;
- использование средств доверенной загрузки;
- встроенная верификация платформы;

- контроль жизненного цикла системы;
- аудит безопасности.

Для бизнес-сегмента ключевым моментом будет удобное и эффективное отслеживание всех устройств в системе, мониторинг их состояния и диагностика. Администратор должен контролировать, в частности, такие вопросы, как установленное на устройствах программное обеспечение и его конфигурация. Решение должно учитывать следующие особенности: масштабируемость для использования в системе сотен, тысяч и более устройств; установка конечных точек в удаленных неконтролируемых местах; обеспечение требуемого уровня доступности и физической безопасности.

3. КОНЦЕПЦИЯ ЗАЩИТЫ IoT

Безопасность связи

Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, чтобы устройства знали, могут ли они доверять удаленной системе. Новые криптографические технологии, такие как ECC (EllipticCurveCryptography), работают в десять раз лучше предшественников в слабомощных чипах IoT 8-bit 8MHz. Не менее важной задачей здесь является управление ключами для проверки подлинности данных и достоверности каналов их получения. Ведущие центры сертификации (CA) уже встроили «сертификаты устройств» в более чем миллиард устройств IoT, предоставив возможность выполнять проверку подлинности широкого спектра устройств, включая сотовые базовые станции, телевизоры и многое другое.

Защита устройств

Защита устройств – это в первую очередь обеспечение безопасности и целостности программного кода. Тема безопасности кода выходит за рамки этой статьи, заострим внимание на целостности. Подписание кода требуется для подтверждения правомерности его запуска, также необходима защита во время выполнения кода, чтобы атакующие не перезаписали его во время загрузки. Подписание кода криптографически гарантирует, что он не был взломан после подписания и безопасен для устройства. Это может быть реализовано на уровнях приложений и рабочей платформы (прошивки) и даже на устройствах с монолитным образом прошивки. Все критически важные устройства, будь то датчики, контроллеры или что-то еще, должны быть настроены на запуск только подписанного кода. Устройства должны быть

защищены и на последующих этапах, уже после запуска кода. Здесь поможет защита на основе хоста, которая обеспечивает повышение защищенности, разграничение доступа к системным ресурсам и файлам, контроль подключений, защиту от вторжений, защиту на основе поведения и репутации. Также в этот длинный список возможностей хостовой защиты входят блокирование, протоколирование и оповещение для различных операционных систем IoT. В последнее время многие средства хостовой защиты были адаптированы для IoT и теперь хорошо проработаны и отлажены, не требуют доступа к облаку и бережно расходуют вычислительные ресурсы IoT-устройств.

Контроль устройств

К сожалению, уязвимости в устройствах IoT все равно будут, их нужно будет исправлять, и это может происходить в течение длительного времени после передачи оборудования потребителю. Даже код с применением обфускации в критичных системах в конце концов реконструируется, и злоумышленники находят в нем уязвимости. Никто не хочет, а зачастую и не может отправлять своих сотрудников для очного визита к каждому устройству IoT для обновления прошивки, особенно если речь идет, например, о парке грузовиков или о сети датчиков контроля, распределенных на сотни километров. По этой причине «управляемость по воздуху» (over-theair – OTA) должна быть встроена в устройства до того, как они попадут к покупателям.

Контроль взаимодействий в сети

Некоторые угрозы смогут преодолеть любые предпринятые меры независимо от того, насколько хорошо все защищено. Поэтому крайне важно иметь возможности аналитики безопасности в IoT. Системы для аналитики безопасности помогут вам лучше понять вашу сеть, заметить подозрительные, опасные или злонамеренные аномалии.

4. ПРИМЕР РЕШЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ IOT

Компания CiscoSystems играет ведущую роль в разработке модели Всемирного форума IoT, разработала фреймворк безопасности IoT, ставший полезным дополнением к эталонной модели Всемирного форума IoT. На рис. 5 показана среда безопасности, связанная с логической структурой IoT.

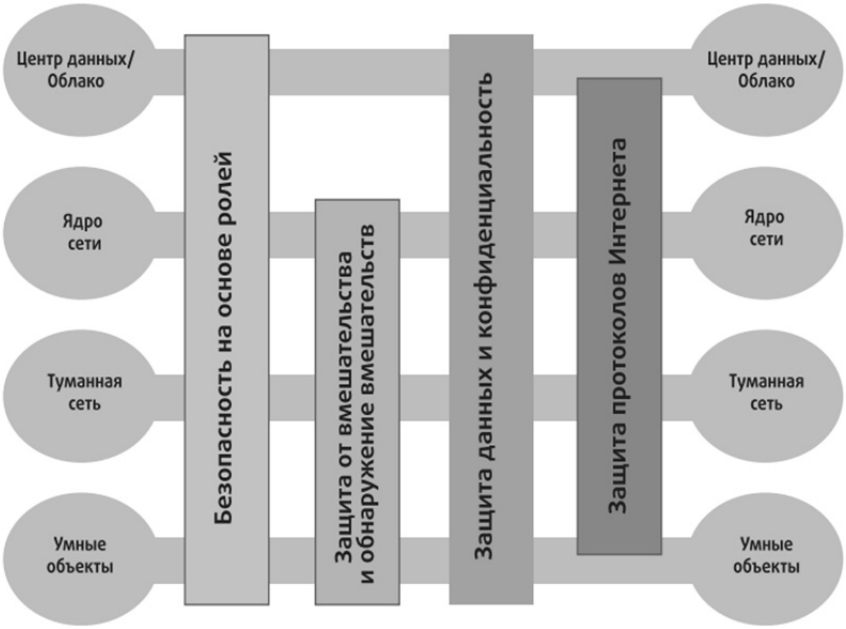

Рис. 5. Среда безопасности IoT

С помощью этой четырехуровневой архитектуры модель Cisco определяет четыре общие возможности безопасности, охватывающие несколько уровней.

- Безопасность на основе ролей: системы управления доступом на основе ролей (Role-BasedAccessControl – RBAC) назначают права доступа ролям, а не отдельным пользователям. Пользователям, в свою очередь, предписывают различные роли либо статически, либо динамически соответственно обязанностям. RBAC широко используется в коммерческих облачных и корпоративных системах. Этот инструмент, понятный администраторам, может использоваться для управления доступом к IoT-устройствам и генерируемым ими данным.
- Защита от вмешательства и обнаружение вмешательств – эта функция особенно важна на уровне устройств и туманной сети, но распространяется также и на уровень ядра сети. Все эти уровни могут использовать компоненты, физически находящиеся вне физически охраняемой территории предприятия.
- Защита данных и конфиденциальность – эти функции охватывают все уровни архитектуры.

• Защита протоколов Интернета – защита «данных в движении» от подслушивания и перехвата, важна для всех уровней.

На рис. 5 отмечены конкретные функциональные области безопасности поверх четырех уровней модели IoT. Перечислим четыре компонента безопасности.

• Аутентификация – охватывает элементы, инициирующие доступ, и первым делом идентифицирует устройства IoT. В отличие от типичных корпоративных сетевых устройств, для которых идентификация может осуществляться по идентификационным признакам человека (таким как имя/пароль или бейдж), оконечные устройства IoT должны оснащаться такими методами аутентификации, которые не требуют вмешательства человека. К таким методам относятся радиочастотные метки, сертификаты x.509 или MAC-адреса оконечных устройств.

• Авторизация – управляет доступом к устройству через структуру сети. Этот элемент включает в себя контроль доступа. Вместе с уровнем аутентификации он вырабатывает необходимые параметры для того, чтобы разрешить обмен информацией между устройствами и между устройствами и прикладными платформами, тем самым обеспечивая работу IoT-служб.

• Сетевая политика – охватывает все элементы, осуществляющие маршрутизацию и транспортировку трафика с оконечных устройств по инфраструктуре, будь то контроль, управление или собственно трафик данных.

• Аналитика безопасности, включая видимость и контроль – все функции, необходимые для централизованного управления устройствами IoT. В первую очередь видимость IoT-устройств, означающая то, что центральные функции управления безопасно оповещены о парке распределенных устройств IoT, включая идентичность и атрибуты каждого устройства. На основе такой видимости возникает способность осуществлять контроль, включая конфигурацию, патчи и обновления, а также контрмеры для пресечения угроз.

ЗАКЛЮЧЕНИЕ

Интернет вещей – это пока еще новая область развития информационных технологий, и вопросы защиты информации здесь наиболее актуальны. Исходя из архитектуры, технологий и концепции безопасности мы делаем вывод, что добиться безопасности в сфере IoT единообразно невозможно из-за большого расхождения в реализации каналов связи, платформ и методов обработки данных в конкретных продуктах. Для решения вопросов защиты информации Интернета вещей необходимо привести стандарт разработки систем в

данном направлении. В данный момент каждое решение требует индивидуального подхода обеспечения безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность интернета вещей (Internet of Things) [Электронный ресурс]. – 2017. – URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things) (дата обращения: 12.11.2017).

2. Что такое интернет вещей Internet of Things, IoT [Электронный ресурс]. – 2017. – 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_(Internet_of_Things,_IoT) (дата обращения: 12.11.2017).

3. Еще один взгляд на безопасность Интернета вещей [Электронный ресурс]. – 2015. – URL: https://geektimes.ru/company/iridiummobile/blog/267760/ (дата обращения: 12.11.2017).

4. Интернет вещей: сетевая архитектура и архитектура безопасности [Электронный ресурс]. – 2017. – URL: http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/ (дата обращения: 12.11.2017).

5. Эталонная архитектура безопасности интернета вещей (IoT). Ч. 1 [Электронный ресурс]. – 2017. – URL: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (дата обращения: 12.11.2017).

6. Сетевые технологии Интернета вещей [Электронный ресурс]. – 2017. – URL: https://habrahabr.ru/company/ericsson_ru/blog/301494/ (дата обращения: 12.11.2017).

7. Что такое IoT или интернет вещей? [Электронный ресурс]. – 2017. – URL: https://coinspot.io/beginners/chto-takoe-iot-ili-internet-veshhej/ (дата обращения: 12.11.2017).

8. Новости интернета вещей [Электронный ресурс]. – 2017. – URL: https://iot.ru/ (дата обращения: 12.11.2017).

9. Интернет вещей: как изменится вся наша жизнь на очередном витке развития Всемирной сети [Электронный ресурс]. – 2017. – URL: https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (дата обращения: 12.11.2017).

10. Что такое интернет вещей (Internet of Things, IoT) [Электронный ресурс]. – 2017. – URL: http://edurobots.ru/2016/04/internet-veshhej/ (дата обращения: 12.11.2017).

11. «Интернет вещей» – реальность или перспектива? [Электронный ресурс]. – 2017. – URL: http://compress.ru/Article.aspx?id=24290 (дата обращения: 12.11.2017).

12. Защита IoT-устройств и шлюзов [Электронный ресурс]. – 2017. – URL: https://www.ibm.com/developerworks/ru/library/iot-trs-secure-iot-solutions1/index.html (дата обращения: 12.11.2017).

13. Интернет вещей (IoT). Защита устройств и обязанность вендоров [Электронный ресурс]. – 2017. – URL: https://www.securitylab.ru/blog/personal/aodugin/334725.php (дата обращения: 12.11.2017).

14. Интернет вещи (iot) и их безопасность [Электронный ресурс]. – 2017. – URL: http://www.cleper.ru/articles/description.php?n=589 (дата обращения: 12.11.2017).

15. IoT нуждается в информационной безопасности [Электронный ресурс]. – 2017. – URL: http://www.comnews.ru/content/109250/2017-08-25/iot-nuzhdaetsya-v-informacionnoy-bezopasnosti (дата обращения: 12.11.2017).

Донской Кирилл Александрович, студент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – современные системы информационной безопасности. E-mail: kirdon96@mail.ru

Левин Лев Сергеевич, студент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – современные системы информационной безопасности. E-mail: mynameislev@bk.ru

Попантонопуло Евгений Владимирович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – современные системы информационной безопасности. E-mail: pev@atlas-nsk.ru.

Information security of internet things *

K.A. Donskoy[1], L.S. Levin[2], E.V. Popantonopulo[3]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, student of the information security department. E-mail: kirdon96@mail.ru*
[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, student of the information security department. E-mail: mynameislev@bk.ru*
[3] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630087, Russian Federation, postgraduate of the information security department. E-mail: pev@atlas-nsk.ru*

This operation touches on issues of the organization of information security is applicable to the sphere of the Internet of things. In operation determination of the Internet of things, the created architecture, the used technologies of implementation, possible security risks and the concept of safety is considered. The task of our operation is detection of problems of creation of secure system in the sphere of the Internet of things and a way of elimination of these problems. Having analyzed architecture of the Internet of things, paying attention to the used technologies: networks, operating systems, workmanship, communication links, data handling methods, information transfer protocols, we find weak spots, we give examples of scenarios of the attacks to family devices the Internet of things. Proceeding from the found vulnerabilities, we analyze a set of means and methods of support of information security and we select the decisions conforming to requirements of the Internet of things. Also we consider use of already existing technologies and the decision of the companies of leaders of development of information technologies such as Cisco. The set of the used levels of system of the Internet of things and difference in technologies do not allow to use for protection uniform model of safety therefore the Cisco company suggests to differentiate solutions of safety on four levels of architecture and to integrate information security methods in the so-called environment of safety. Detailed reviewing of ready decisions and approaches to safety in the sphere of the Internet of things shows us need for development of the standard for creation of systems of the Internet of things which would narrow the list of the used components and technologies, having allowed to construct the uniform model of safety of the Internet of things corresponding to the concept of safety.

Keywords: internet, monitoring, information, technology, threats, protection, network, attacks, channel, architecture, scenarios, system, security, management, control

DOI: 10.17212/2307-6879-2017-4-128-143

REFERENCES

1. *Informatsionnaya bezopasnost' interneta veshchei (Internet of Things)* [Information security of the Internet of things (Internet of Things)]. 2017. Available at: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0

* *Received 29 July 2017.*

%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_ (Internet_of_Things) (accessed 11.12.2017).

2. *Chto takoe internet veshchei Internet of Things, IoT* [What is the Internet of things, IoT]. 2017. Available at: 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_ (Internet_of_Things, _IoT) (accessed 11.12.2017).

3. *Eshche odin vzglyad na bezopasnost' Interneta veshchei* [One more view of safety of the Internet of things]. 2015. Available at: https://geektimes.ru/company/iridiummobile/blog/267760/ (accessed 11.12.2017).

4. *Internet veshchei: setevaya arkhitektura i arkhitektura bezopasnosti* [Internet of things: network architecture and architecture of safety]. 2017. Available at: http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/ (accessed 11.12.2017).

5. *Etalonnaya arkhitektura bezopasnosti interneta veshchei (IoT)*. Ch. 1 [Reference architecture of safety of the Internet of prophetic (IoT). Pt. 1]. 2017. Available at: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (accessed 11.12.2017).

6. *Setevye tekhnologii Interneta veshchei* [Network technologies of the Internet of things]. 2017. Available at: https://habrahabr.ru/company/ericsson_ru/blog/301494/ (accessed 11.12.2017).

7. *Chto takoe IoT ili internet veshchei?* [What is IoT or Internet of Things?]. 2017. Available at: https://coinspot.io/beginners/chto-takoe-iot-ili-internet-veshhej/ (accessed 11.12.2017).

8. *Novosti interneta veshchei* [News of the Internet of things]. 2017. Available at: https://iot.ru/ (accessed 11.12.2017).

9. *Internet veshchei: kak izmenitsya vsya nasha zhizn' na ocherednom vitke razvitiya Vsemirnoi seti* [Internet of things: How will our whole life change at the next round of development of the World Wide Web]. 2017. Available at: https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (accessed 11.12.2017).

10. *Chto takoe internet veshchei (Internet of Things, IoT)* [What is the Internet of Things, IoT]. 2017. Available at: http://edurobots.ru/2016/04/internet-veshhej/ (accessed 11.12.2017).

11. *"Internet veshchei" – real'nost' ili perspektiva?* ["Internet of things" – reality or perspective?]. 2017. Available at: http://compress.ru/Article.aspx?id=24290 (accessed 11.12.2017).

12. *Zashchita IoT-ustroistv i shlyuzov* [Protection of IoT-devices and gateways]. 2017. Available at: https://www.ibm.com/developerworks/ru/library/iot-trs-secure-iot-solutions1/index.html (accessed 11.12.2017).

13. *Internet veshchei (IoT). Zashchita ustroistv i obyazannost' vendorov* [Internet of things (IoT). Device protection and vendor responsibility]. 2017. Available at: https://www.securitylab.ru/blog/personal/aodugin/334725.php (accessed 11.12.2017).

14. *Internet veshchi (iot) i ikh bezopasnost'* [Internet of things (IoT) and their protection]. 2017. Available at: http://www.cleper.ru/articles/description.php?n=589 (accessed 11.12.2017).

15. *IoT nuzhdaetsya v informatsionnoi bezopasnosti* [IoT needs information security]. 2017. Available at: http://www.comnews.ru/content/109250/2017-08-25/iot-nuzhdaetsya-v-informacionnoy-bezopasnosti (accessed 11.12.2017).

Для цитирования:

Донской К.А., Левин Л.С., Попантонопуло Е.В. Информационная безопасность интернет вещей // Сборник научных трудов НГТУ. – 2017. – № 4 (90). – С. 128–143.

For citation:

Donskoy K.A., Levin L.S., Popantonopulo E.V. Informatsionnaya bezopasnost' internet veshchei [Information security of internet things]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2017, no. 4 (90), pp. 128–143.