УДК 004
JEL коды: D89
08.00.13

Информационная безопасность в мире Интернета вещей
Information security in the world of the Internet of Things

Бушуева Е.С.
к.э.н., Севастопольский государственный университет, Россия.
Bushueva E.S.
Ph.D., Sevastopol State University, Russia.

Аннотация
В работе показано, что «Интернет вещей» противоречив с требованиями безопасности глобальной инфраструктуры. Уязвимости рекомендовано устранять с помощью системного анализа проблем, разработки улучшенных стандартов безопасности (на основе аудита уязвимостей). Рассмотрены некоторые процедуры реализации предложенных принципов. Рассмотрены практические советы.
Abstract
The paper shows that the “Internet of Things” is inconsistent with the security requirements of the global infrastructure. Vulnerabilities are recommended to be eliminated using system analysis of problems, development of improved security standards (based on vulnerability auditing). Some procedures for the implementation of the proposed principles are considered. Considered practical tips.
Ключевые слова: информационная, безопасность, Интернет, вещей, угроза, общество, системный, анализ, сложность, уязвимость, аудит.
Keywords: information, security, Internet, things, threat, society, system, analysis, complexity, vulnerability, audit.

Постановка задачи

«Интернет вещей», «виртуальный умный дом» и другие инновации – результат эволюции цифровых технологий, вещей. Компании стали тяготеть к интеллектуализации продукции (услуг), добавляя ценности для потребителя, завоевывая новые ниши, получая высокую конкурентоспособность, преимущества на рынке, готовясь к вхождению в Индустрию 4.0. Эксперты заявляют, что компании не «пришедшие к цифре в вещах» не способны к выживанию [1, С. 2].

Необходимо предлагать совершенные, интеллектуализированные товары (услуги) без переоснащения потребителя, следует самонастраиваться, поддерживать качество высочайшее, причем на уровне «Включить в розетку». Это атрибут, особенность «Интернета вещей» (далее – IoT, ИВ) [2, С. 10].

Обучающие алгоритмы, чувствительные датчики (реагируют на звук, фон, вибрацию и др.) позволят идентифицировать процессы, объекты, передать на смартфон информацию, если нет дома никого.

Цель исследования – изучение, системный анализ информационной безопасности во взаимодействиях класса «автомат–машина», устойчивости работы и жизнеспособности. Рассмотрены более вероятные для ИВ угрозы (конфиденциальности, доступа, целостности).

Интернет вещей – актуализация задач и проблем безопасности

Официально, категорию «Интернет вещей» определяют как инфраструктуру глобализации общества передовых услуг для связи вещей (физических, виртуальных) посредством совместимых ИКТ [3, С. 8].

IoT-стандарт IEEE 1888 регламентирует протокол контроля сети, универсальный, дистанционного наблюдения, управления с помощью датчиков, мониторов. Развитие их, без участия оператора, несет также и угрозы безопасности [4, С. 27]. Например, удаленное управление «Умным домом» позволит комфортно организовать, обслужить жизненное пространство, но злоумышленник, внедрившийся в систему, увеличивает риски безопасности всей системы.

Основными сложностями безопасного функционирования интеллектуализированных вещей считают, например, сложности авторизации, обмена сообщениями (криптографическими ключами) – из-за энергопотребления, односторонности, сложности для потребителя, континуума «общающихся» вещей, помех, персонализированных данных, мультипротокольных сетей связи, редиректа, фишинга [5, С. 204].

Желание удешевить вещь – основной фактор его небезопасности, его безопасность, как максимум, – на нижнем допустимом стандартами уровне [6, С. 15].

Необходимо эффективное математическое, инфологическое, алгоритмическое и программное обеспечение предобработки, предактуализации данных разнородных протоколов, датчиков (устройств), обрабатываемых «вещью», управляющей и операционной системой (SIEM). Необходимо привести к единообразию, чтобы эффективно, оперативно анализировать «комплексуемые» события, используя метаданные процессов, справочники гетерогенных данных из ИВ, сенсорную сеть WSN [7, С. 20].

Неоднородность, многообразие систем ИВ увеличивает риски угроз безопасности, традиционные подходы к политике безопасности, конфиденциальности неприменимы к технологиям ИВ (например, из-за маломощности вычислительной) [8, С. 23].

Необходимы другие модели, подходы [9, С. 92], [10, С. 2267] методы аутентификации, например, нейроскринкастинга, криптошифрования P2P, M2M, позволяющим пользователю удаленно и безопасно выполнить сеанс с сервером, протоколом распределения сеанс-ключей.

К 2025 году ИВ-узлами, потенциальными целями, могут оказаться все окружающее нас: от чайника до системы наблюдения [11, С. 98].

Метод XOR-проверки изложен в [12, С. 1619] (в [13, С. 112] изложен метод владельцев и сборщиков данных).

Обмен «Пользователь – Вещь» - только при выполнении конкретных действий, с идентификацией (аутентификацией) пользователя, законного владельца данных от вещи. ИВ ведет потоковую обработку, необходимо часто применять многопоточное программирование (например, стандарта POSIX [14, С. 1]).

Необходимы, кроме конфиденциальности, аутентификации и оперативная диагностика, профилактика, оценка нарушений [15, С. 215]. Данные датчиков комбинируемы, если оцениваются риск-процессы или «просто интересны» (например, для полноценного сна в «умном доме»). Психологи, нейрофизиологи, нейроинформатики, нейроматематики решают сложностные задачи по воспроизводимости, управляемости, надежности, принятию решений в воспроизводимой среде, используя DataMining, BigData, различное ПО обработки разноформатных видеоаудиозаписей, данных датчиков.

Инвестиции в инфраструктуру ИВ дают эффекты открытости, транспарентности, инновационности, масштабируемости, аналитичности. Важно учесть безопасность не только вещи, но и его владельца, просто окружения, например, больного в «умном доме», его самоуправляемости через гаджет.

Применение ИВ актуализирует энергоэффективность вещей. Нужны новые возможности управляемости, ресурсобеспеченности, экономичности, экологичности. До 50% ресурсов экономить – вполне решаемая задача. Например, для повышения эффективности кондиционирования «умного дома» ищут решение не в самом кондиционере, а в спецпанелях, наполняемых жидкостью и повышающих эффективность кондиционирования за счет энергии природы. Кондиционирование избавляется от тепла, удаляя из вентиляционного блока горячий воздух. Новая конструкция пропускает его от хладагента через воду (рабочую смесь). Далее жидкость уходит в панель охлаждения на крыше, тепло выходит наружу. В жаркие дни, кондиционирование нужнее, лучи Солнца нагревают жидкость панели. Гибрид-системы станут обыденными, сочетая существующую технологию кондиционирования воздуха с новыми панелями.

Рациональное поведение, ресурсорасходование – качества грамотного ИВ-пользователя.

Эволюция Интернета вещей: системные цели и ориентиры

Ориентиры построения информационного ИВ-ориентированного общества базируются на очень похожих, связанных, но различных категориях «постиндустриальное общество», «знаниевое (на знаниях, компетенциях) общество», «общество информационное» и др. Есть смысл определить эмерджентные свойства моделей развития общества для корректного рассуждения об ИВ.

Постиндустриальное – общество, использованием достижений науки, технологий достигшее такого роста ВВП, доходов населения, что смогло переориентировать экономику (рыночные механизмы) на устойчивое производство услуг, сервис, качество уровня жизни, развитие ИВ. Часто используют обобщенную эмерджентную характеристику такого общества – более половины ВВП идет на формирование качества жизни населения, институтов. В обществе потребления отношения определяются потреблением (индивидуальным, массовым), опосредованно устойчивым рынком, адекватной структурой потребления, ростом доходов, эмерджентное его свойство – потребительские качества, стимулирующие спрос, развивающие производство. В экономике на знаниях, инновационные процессы, образование, знания актуализируются, стимулируются экономически, для конкурентоспособности страны. Такое общество применяет концепцию устойчивого непрерывного компетентносто-ориентированного обучения, к самообучению, научению на базе интеллектуальных систем, институтов (механизмов), интегрируемых в ИВ, ИТ-инновационные сети знаний. Эмерджентное свойство: «ноу-хау», когнитивные технологии, знания определяют эволюцию экономики, массовый прирост знаний, направленный на устойчивый рост, например, индекса HDI.

Первая фаза такого общества – информационное, эволюция информационных потоков (по времени, пространству), саморазвивающихся, самоорганизующихся, устойчиво поддерживаемых государством, имеющего отличия:

- обеспечение общества значимой информацией;

- главенство инфоэкономических механизмов, бизнес-процессов;
- эволюция ИКТ, актуализация открытых потоков, ресурсов;
- эволюция института интеллектуальных услуг, знаний;
- индустриализация производства, потребления информации (товара);
- достаточность, полнота, качественность, надёжность систем связи, их защищённость;
- самоорганизация общества.

В каждой модели общества приоритет – человеческому потенциалу, инновационным ресурсам, науке, образованию, бизнес-поддержке.

Эволюция общества и безопасности «Интернета вещей»

Имеются несистематизированные данные о подготовке к «глобальной битве» в ИВ. В социально-экономическом плане, риски без жертв, материального ущерба «не считаются». На причастность к непосредственному осуществлению одного взлома часто претендуют сразу несколько злоумышленников. Создается «буферная зона» вокруг объекта (субъекта) воздействия, «мишени» (может быть идентифицирована и Заказчиком), безопасность должна гарантироваться в зоне «благополучия» потребителя.

Для выявления скрытых корреляций следует разработать алгоритмы, сценарии (процедуры) симуляционных воздействий. Например, следующая:

1. риск-объектам придаются веса (путем умножения соответствующих векторов факторов, параметров воздействий на число, большее, чем 1);
2. применяется процедура SVD [16, С. 70] – сингулярное разложение матрицы А векторов факторов, левый (правый) сингулярный вектор, сингулярные числа μ – «предсказатели» риск-ситуаций, асоциального, девиативного поведения:

$$Ax = \mu y, A^* y = \mu x,$$

где A^* – сопряженно-транспонированная матриц к М.

Результатом будет удаление интересующих объектов от начала координат (их выделение). Однако, объекты, имеющие с выделенными заметные корреляции, также будут «вытянуты» вслед за ними, причем степень «вытянутости» зависит от величины корреляции. Можно эффективно выявлять скрытые корреляции.

Успешной является также модель уязвимостей Take-Grant [17, С. 258] анализа прав доступа с построением графа доступов. Разновидность модели используется для подтверждения (опровержения) заявленной степени защищенности по регламенту предъявленных требований. Модель – взвешенный орграф без петель:

$$G =< S, O, E >,$$

O – объектное множество, S – субъектное, $E \in S \times O \times R$ – дуги прав доступа

Рассматриваются правила Активизация(r,x,y,s); Деактивизация(r,x,y,s); Создание(r,x,s); Удаление(r,x,s), где $r \in R, s \in S, x \in O, y \in O$.

Вес типа «стоимость риска» зависит от правил, субъектов применяющих правило, сложности взаимодействий.

ИВ – система глобальная, как и риски, способные разрушить среду. Но готовность граждан противостоять натиску глобального, системного проникновения в их вещи – также растет, прогнозируется, моделируется. Появилось новое движение разработчиков «искусственного интеллекта», способное противостоять рисками ИВ. Ученые полагают, что

именно силами гражданского населения, подготовленного с помощью ИВ, СИИ возможна эффективная борьба.

В РФ, у отечественных силовых структур, спецслужб, «просто рук не хватит» предотвращать в ИВ все, повсеместно успевать, по мере проявления скрытого вредоносного потенциала.

Защитные меры включают ужесточение режимов безопасности, возведение различных технологических барьеров. В их число входят: усиление охранных функций по периметру охраняемых объектов, внедрение в систему охраны датчиков и программ раннего контроля, выпуск различных, более защищенных датчиков, устройств, ПО. Очень часто такие меры препятствуют намерениям злоумышленников, вынуждают отклоняться от намеченного курса и действовать на менее укрепленных участках критических объектов ИВ, всей инфраструктуры в надежде нанести хотя бы второстепенный ущерб.

В противоположность оборонительным мерам, превентивные меры включают прямые воздействия подготовленными специалистами. Узаконенные превентивные меры призваны, как минимум, усилить возможности всей инфраструктуры ИВ. Превентивные меры против нетрадиционного воздействия на локальном уровне стремятся нарушить сложившиеся экономико-социальные отношения [18, С. 60].

Можно предложить модель на основе интегрированных индексов признаков опасности. Они могут включать несколько индексированных факторов, например:

- средства внешнего воздействия (стран, мегаполисов, институтов);
- неэффективных мероприятий региональных и муниципальных властей, снижающих эффективность защиты;
- социальные, организованные воздействия.

Интегрированный индекс признаков динамически пополняется данными клиентов, субъектов и др. Подход, аналогичен методу отбора суждений Терстоуна. Переход к интервальной шкале не требуется, сама шкала – порядковая. Возможно много избыточной, несущественной, случайной информации, поэтому необходимо отфильтровать «шум». Информация о второстепенных факторах, действиях может быть также актуализирована интегрально. Противодействие опасностям ИВ строится с опорой на науку, образование, общественность [19, С. 648].

Есть известные практические методы, которые могут стать эффективными в обеспечении ИВ-безопасности, как и воздействия. Рассмотрим некоторые такие воздействия.

Практика профилактики и противодействия

Спуфинг, spoofing - предъявление при идентификации ложной информации: цель - несанкционированный доступ, созданием ситуации, когда по недостоверному ip-адресу пытаются подключиться к «прокси», «экрану». Пользуясь уязвимостями механизма аутентификации. Идет присвоение данных пользователей, подмена.

Аутентификация IP-адресов поддерживается серверами ИВ. Управление доступом IP-адресами легко в небольших группах, по адресу же бывает громоздкой, при объеме публичных серверов. Аутентификация чувствительна к спуфингу по IP, атаке DNS: проблема спуфинга достаточно актуальна. Защита сетей от взлома, доступа - важная проблема. Полностью (на уровне приложения) - нерешаемая. Всегда есть у них уязвимые места.

Правила снижающие уязвимости:

- анализировать лог-файлы, сетевые, спецприложениями;
- отдать аутсорсингу безопасность, если своих ресурсов мало.

DNS поможет идентифицировать владельца домена, адрес. Тестирование – увидеть хосты, функционирующие в ИВ. Получив их список, злоумышленник сканирует порты, добывая информацию, используемую при взломе объекта ИВ.

1. Руткит. Это код, программа, комплекс:

- маскировки (объект, файл, процесс);
- управления (события);
- сбора параметров (данные).

Руткит - программа (комплекс) скрытия присутствия вредоносной программы (злоумышленника) в ИВ. Руткит прячется глубоко в ОС, избегая обнаружения антивирусом. Root - «корень» (обозначение роли пользователя), Kit – «набор», т.е. набор неограниченного доступа.

Классификация по привилегиям:

- пользовательские (внедряются в запущенные процессы, используя их области памяти);
- операционные, ядра (на уровне ОС, максимального доступа, практически безграничного).

По действиям, – изменяющие алгоритм, функции или структуру данных в системе.

Базовый арсенал методов отлова руткитов:

- сигнатурный поиск - по сигнатуре (цепочке битов), характерной для вредоноса;
- эвристический анализ - по подозрительности процессов и др.;
- аудит целостности (контрольные суммы, ЭЦП файлов).

Наиболее распространенные руткиты:

- LRK - с 1997 г., встречается в уязвимых системах, подменяет файлы (исполняемые);
- Knark - сильно скрытный, располагающийся в ядре;
- Beastkit - для дистрибутивов RedHat, имеет модификацию Illogic (права администратора);
- другие - Sneakin, Devil и др.

Руткит позволяет удаленно, полно контролировать ОС, следовательно, ИВ. Новые руткиты устанавливают свои SSL-сертификаты, расшифровывают HTTP-трафик (с цель доступа к кредитным картам), организуют атаки. Поэтому IT-персонал должен быть квалифицирован, предпринимать защитные меры.

2. Реверс-инжиниринг. Защищаться в ИВ актуально стало и для приложений мобильных средств. Особенно, «андроидных», чьи приложения часто легко взламываются, чтобы не только вникнуть в код (что непросто), а и в механизм работы, идею. Это позволит воспроизвести, сымитировать работу приложения. Такой подход называется реверс-инжиниринг (обратный инжиниринг). Используют к Android для извлечения «исходника», ресурсов APK-файла. Противодействующим можно воспользоваться соответствующими инструментами (например, dex2jar, JAD и др.).

Полной защиты нет, но максимально усложнить взломщикам процесс взлома – возможно [20, С. 436]. Как, каким инструментарием? Обычно, следующими:

- применение ProGuard, который позволяет анализировать, оптимизировать код, идентифицировать, удалять неиспользуемые атрибуты, поля, классы, переименовывать остальные с использованием бессмысленных коротких имен, это уменьшит базу кода, повысит его эффективность, понизит расшифровываемость, после верификации информация добавляется в классы JavaMicroEdition, Java-6, др.;
- перемещением «ответственности на сервер», наиболее важные компоненты, фрагменты сервиса стоит переместить из клиентского приложения на веб-сервис, веб-сервер, например, уникальный алгоритм защищаем перемещением его для обработки данных (удаленно) на веб-сервере, само приложение уже обеспечивается самими данными работы алгоритма;
- перемещением «ответственности на компилятор» (C++), применяя изначально NDK при разработке алгоритмов в so-файлы, можно добиться более редкой декомпиляции (сравнительно с APK), можно комплектовать, используя SSL взаимодействий типа «устройство-сервер» и, хотя есть вероятность разбора ассемблер-код (дизассемблирования), реверс-инжиниринг объемной библиотеки assembly трудоемок (на Java – декомпиляция легче);
- применением SSL, взаимодействия типа «устройство-сервер» лучше организовать с помощью SSL (может понадобиться сертификат), чтобы не потерять конфиденциальных данных (передаваемых SSL/TSL-протоколом), снизить уязвимость от MitM-атак, при этом, имея «самозаверенный» сертификат SSL, злоумышленник может нарушить конфиденциальность соединений.

Исследования показывают, что не менее 30% мобильных приложений реализуют соединения некорректно. Поэтому, рекомендуется:

- проверка сертификата, устанавливая соединение SSL/TLS;
- использование X509TrustManager-стандарта;
- принимая самозаверенный сертификат, создавать свою X509TrustManager-реализацию;
- указывать сертификаты для принятия, отклонять остальные.

Важно не сохранять значения необработанных форматов. Для сохранения на устройстве данных не использовать такие. Например, чтобы сохранить валютный баланс можно сохранить их закодированные значения (по некоторому алгоритму кодирования).

Важно также правильно вести учетные данные, минимизировать темп запросов приложением данных, минимизировать фишинг-атаки, их успешность. Имя, пароль – не хранить (если возможно) на устройстве. Авторизацию (аутентификацию) – с помощью маркера авторизации.

Выводы

В работе показано, что «Интернет вещей» противоречив с требованиями безопасности глобальной инфраструктуры. Уязвимости рекомендовано устранять с помощью системного анализа проблем, разработки улучшенных стандартов безопасности (на основе аудита уязвимостей). Рассмотрены некоторые процедуры реализации предложенных принципов. Рассмотрены практические советы.

Работа эволюционируема. Как и у всех, затрагивающих проблемы ИВ, нерешенной остаются проблемы соотношения риска-гарантий, естественных и вызванных

вмешательством человека изменений, сохранения устойчивости ИВ. Законченной теории нет, некоторые структурные параметры инфраструктуры могут динамически видоизменяться с недопустимой степенью точности.

Литература

1. Найдич А. «Интернет вещей» – реальность или перспектива? [Электронный ресурс] // КомпьютерПресс, 2013. № 12. URL: http://compress.ru/article.aspx?id=24290 (дата доступа 05.06.2018).

2. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] // Открытые системы. 2013. № 4. URL: http://www.osp.ru/os /2013/04/13035551 (дата доступа 05.06.2018).

3. Internet of Things Global Standards Initiative [Электронный ресурс]. – URL: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата доступа: 05.06.2018).

4. Шиков С. А. Проблемы информационной безопасности: интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40. DOI: 10.15507/0236-2910.027.201701.027-040

5. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы.-СПб.: Символ-Плюс, 2009.-560с.

6. Печенкин А.И., Полтавцева М.А., Лаврова Д.С. Подход к нормализации данных интернета вещей для анализа безопасности // Программные продукты и системы // Software & Systems №2(114), 2016.

7. Grieco L.A., Alaya M.B., Monteil T, Drira K.K. Architecting information centric ETSI-M2M systems // IEEE PerCom, -2014.

8. Weber R.H. Internet of things – new security and privacy challenges // Comput. Law Secur. Rev, 2010, v.26, №1, pp. 23–30.

9. Feng H, Fu W. Study of recent development about privacy and security of the internet of things / International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp.91–95.

10. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things // Comp. Networks, 2013, v.57, № 0, pp.2266–2279.

11. Turkanovi M., Brumen B., Holbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion // Ad Hoc Networks, 2014, Vol. 20, pp. 96–112.

12. N. Ye N, Zhu Y, Wang R-C., Malekian R., Lin O-M. An efficient authentication and access control scheme for perception layer of internet of things//Appl. Math. Inf. Sci., 2014, v.8, №4, pp.1617–1624.

13. Alcaide A., Palomar E., Montero-Castillo J., Ribagorda A. Anonymous authentication for privacy-preserving iot targetdriven applications //Comput. Secur., 2013, v.37, pp.111–123.

14. Романенко А.А. Введение в POSIX threads. URL: http://ccfit.nsu.ru/arom/data/PP_ICaG/03_pthreads_txt.pdf (дата доступа 02.06.2018).

15. Леонов А.В. Интернет-вещей: проблемы безопасности // Омский научный вестник, №2(140)б 2015, с.215-218.

16. Harrington P. Machine Learning in Action.-Shelter Island, 2012.-pp.280.

17. Миронова В.Г., Шелупанов А.А. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Томск. Ун-та систем управления и радиоэлектроники.–2010.–№2(22).–с.257–259.

18. Круз Л. Интернет вещей и информационная безопасность: защита информации // Инсайд. 2013. №6. С.60–61.

19. Suo H. Security in the Internet of Things // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. -2012, pp.648–651.

20. Ивлиев С.Н. Интернет вещей: новые угрозы информационной безопасности // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики, XII Всерос. науч.-техн. конф. (28–29 мая 2015 г.).-Саранск, 2015, с.435–441. URL: http://elibrary.ru/item.asp?id=24179239 (дата доступа 02.06.2018).

References

1. Naiditsch A. “Internet of Things” - reality or perspective? [Electronic resource] // ComputerPress, 2013. № 12. URL: http://compress.ru/article.aspx?id=24290 (access date 05.06.2018).

2. The Internet of Things: New Challenges and New Technologies [Electronic resource] // Open Systems. 2013. No. 4. URL: http://www.osp.ru/os / 2013/04/13035551 (access date 05.06.2018).

3. Internet of Things Global Standards Initiative [Electronic resource]. - URL: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (access date: 06/05/2018).

4. Shikov S. A. Problems of Information Security: the Internet of Things // Bulletin of the Mordovia University. 2017. V. 27, No. 1. P. 27–40. DOI: 10.15507 / 0236-2910.027.201701.027-040

5. Sutton M., Green A., Amini P. Fuzzing: a study of vulnerabilities by brute force.-SPb .: Symbol-Plus, 2009.-560s.

6. Pechenkin A.I., Poltavtseva M.A., Lavrova D.S. Approach to the normalization of Internet of Things data for security analysis // Software products and systems // Software & Systems №2 (114), 2016.

7. Grieco L.A., Alaya M.B., Monteil T, Drira K.K. Architecting information centric ETSI-M2M systems // IEEE PerCom, -2014.

8. Weber R.H. Internet of things - challenges. // Comput. Law Secur. Rev, 2010, v.26, No. 1, pp. 23–30.

9. Feng H, W. W. Fundamentals, Sanya, 2010, pp.91–95.

10. Roman R, Zhou J, Lopez J. Comp. Networks, 2013, v.57, No. 0, pp. 2266–2279.

11. Turkanovi, M., Brumen, V., and Holbl, M. A, Ad Hoc Networks, 2014, Vol. 20, pp. 96–112.

12. N. Ye N, Zhu Y, Wang R-C., Malekian R., Lin O-M. The Internet of Things // Appl. Math Inf. Sci., 2014, v.8, №4, pp.1617–1624.

13. Alcaide A., Palomar E., Montero-Castillo J., Ribagorda A. Anonymous authentication for privacy-preserving iot targetdriven applications // Comput. Secur., 2013, v.37, pp.111–123.

14. Romanenko A.A. Introduction to POSIX threads. URL: http://ccfit.nsu.ru/arom/data/PP_ICaG/03_pthreads_txt.pdf (access date 02.06.2018).

15. Leonov A.V. Internet of things: security problems // Omsk Scientific Herald, №2 (140) b 2015, p.215-218.

16. Harrington R. Machine Learning in Action.-Shelter Island, 2012.-pp.280.

17. Mironova V.G., Shelupanov A.A. Pre-project design of personal data information systems as a stage of information security audit. Dokl. Tomsk. University of Control Systems and Radioelectronics. – 2010. – №2 (22). – P.257–259.

18. Cruz L. The Internet of Things and Information Security: Information Protection // Inside. 2013. №6. P. 60–61.

19. Suo H. Security in the Internet of Things // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. -2012, pp. 648–651.

20. Ivliev S.N. The Internet of Things: New Threats to Information Security // Problems and Prospects for the Development of Domestic Lighting, Electrical and Power Engineering, XII Vseros. scientific and technical conf. (May 28-29, 2015) .- Saransk, 2015, p.435-441. URL: http://elibrary.ru/item.asp?id=24179239 (access date 06/02/2018).