ПРОФОРИЕНТАЦИОННАЯ ШКОЛЬНАЯ ЛАБОРАТОРИЯ ПО ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ В СФЕРЕ ИНТЕРНЕТ ВЕЩЕЙ (IOT)

© Э. Д. Алисултанова, Л. К. Хаджиева, М. З. Исаева

ГГНТУ им. акад. М. Д. Миллионщикова, Грозный, Россия

Данная статья посвящена созданию профориентационной (умной) лаборатории, которая призвана сформировать у школьников базовые представления о технологии Интернет вещей (IoT), угрозах кибербезопасности в этой сфере, мотивировать к получению в будущем профильного образования и построению карьеры в области обеспечения безопасности Интернет вещей (IoT) при функционировании умного производства. Обучение школьников в профориентационной лаборатории, построенное на основе применения интерактивных электронных образовательных ресурсов, прежде всего будет позиционировать карьерные возможности будущих специалистов в сфере обеспечения безопасности Интернет вещей (IoT) при функционировании умного производства. В рамках функционирования лаборатории особое внимание обучающихся сконцентрировано на тематиках правовых аспектов обеспечения кибербезопасности, главных тенденциях развития киберугроз в современном глобальном информационном пространстве и мерах, необходимых для их нейтрализации.

Ключевые слова: лаборатория, технология, Интернет вещей, образовательные ресурсы.

Реализация функционирования профориентационной лаборатории призвана сформировать в регионе детский образовательный центр для внедрения инновационных технологий школьного образования в области кибербезопасности и популяризации профессий, связанных с информационными технологиями.

Создать программно-технические и педагогические условия для ознакомления школьников с угрозами кибербезопасности, способами их устранения и карьерными возможностями в сфере обеспечения безопасности Интернет вещей (IoT) при функционировании умного производства [1].

Интернет вещей (IoT) плотно вошел в нашу жизнь и миллиардов людей по всему миру. Однако рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования – это могут быть даже трубопроводы, доменные печи и установки для выработки элек-

троэнергии. Поскольку ряд таких объектов и систем IoT уже подвергались нападению, и был причинен внушительный ущерб, обеспечение их защиты выходит на первый план.

Безопасность связи. Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, чтобы устройства знали, могут ли они доверять удаленной системе. Здорово, что новые криптографические технологии, такие как ECC (Elliptic Curve Cryptography), работают в десять раз лучше предшественников в слабых 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 – 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 application и firmware 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 харденинг, разграничение доступа к системным ресурсам и файлам, контроль подключений, песочницу, 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. Печально, но уязвимости в устройствах IoT все равно будут, их нужно будет патчить, 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-the-air, OTA) должна быть встроена в устройства до того, как они попадут к покупателям.

Контроль взаимодействий в сети. Некоторые угрозы смогут преодолеть любые принятые 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.

Эволюция парадигмы. Большинство устройств IoT представляют из себя «закрытые системы». Покупатели не смогут добавлять программное обеспечение безопасности после того, как устройства покинут завод. Такое вмешательство аннулирует гарантию, а зачастую попросту не представляется возможным. По этой причине защитные функции должны быть изначально встроены в устройства IoT, чтобы они были безопасными по своей архитектуре. Для большей части индустрии ИБ такая «безопасность внутри», то есть встроенная при изготовлении устройства на заводе – это новый способ обеспечения защиты, это касается и классических технологий безопасности, таких как шифрование, проверка подлинности, проверка целостности, предотвращение вторжений и возможности безопасного обновления. Учитывая тесную связь аппаратного и программного обеспечения в модели IoT, иногда проще, чтобы программы для защиты использовали расширение функций аппаратной части и создавали «внешние» уровни безопасности. Здорово, что многие производители чипов уже встроили функции безопасности в оборудование. Но аппаратный уровень – это всего лишь первый слой, необходимый для комплексной защиты связи и устройств. Комплексная защита требует интеграции функций управления ключами, защиты на основе хоста, инфраструктуры OTA и аналитики безопасности, о чем мы упоминали прежде. Отсутствие даже одного из краеугольных камней в фундаменте безопасности оставит широкий простор действиям злоумышленников. Поскольку промышленный интернет и IoT приносят сетевой интеллект в физические вещи вокруг нас, мы должны внимательно относиться к вопросам их безопасности. Наша жизнь зависит от самолетов, поездов и автомобилей, которые перевозят нас, от

инфраструктуры здравоохранения и гражданской инфраструктуры, которая позволяет нам жить и работать. Нетрудно представить, как незаконное манипулирование светофорами, медицинским оборудованием или бесчисленными другими устройствами может привести к плачевным последствиям. Также ясно, что простые граждане и покупатели IoT не хотят, чтобы незнакомые люди взламывали их дома или машины, чтобы кто-то причинял им вред, устраивая сбои на автоматизированных промышленных объектах. В этой ситуации мы попытаемся предложить такие рекомендации, которые сформируют целостную безопасность для IoT, одновременно сделав ее эффективной и простой в реализации [2].

Безопасность связи. Усиленная модель доверия для IoT. Шифрование, проверка подлинности и управляемость неизменно являются основой устойчивой безопасности. Есть отличные библиотеки с открытым исходным кодом, которые выполняют шифрование даже в устройствах IoT с ограниченными вычислительными ресурсами. Но, к сожалению, большинство компаний по-прежнему подвергаются опасным рискам, допуская ошибки при управлении ключами для IoT. Транзакции на 4 млрд долларов в день электронной торговли защищены простой и надежной моделью доверия, обслуживающей миллиарды пользователей и более миллиона компаний по всему миру. Эта модель доверия помогает системам безопасно проводить проверку подлинности систем других компаний и взаимодействовать с ними по зашифрованным каналам связи. Модель доверия сегодня является критичным фактором безопасного взаимодействия в компьютерных средах и основывается на очень кратком списке надежных центров сертификации (CA). Эти же CA устанавливают сертификаты в миллиарды устройств каждый год. Сертификаты устройств позволяют, например, проверять подлинность мобильных телефонов для безопасного подключения к базовым станциям, проверять подлинность интеллектуальных счетчиков для электроэнергетики, а также приставок в индустрии кабельного телевидения. Надежные CA позволяют легко и безопасно генерировать, выдавать, регистрировать, кон-

тролировать и отзываться сертификаты, ключи и учетные данные, которые имеют решающее значение для надежной проверки подлинности. Учитывая реализуемые объемы сертификатов безопасности для IoT, большинство сертификатов устройств продаются большими партиями за весьма скромную сумму денег за единицу (в долларовом выражении речь идет о десятках центов за сертификат). Почему проверка подлинности имеет значение? Опасно принимать данные от непроверенных устройств или непроверенных сервисов. Такие данные могут повредить или скомпрометировать систему, передать контроль над оборудованием злоумышленникам. Использование надежной проверки подлинности для ограничения нежелательных подключений помогает уберечь системы IoT от подобных опасностей и сохранить контроль над вашими устройствами и сервисами. Независимо от того, соединяется ли устройство с каким-то другим устройством или происходит обмен данными с удаленным сервисом, например облачным, связь всегда должна быть защищена. Все взаимодействия требуют надежной проверки подлинности и взаимного доверия. Исходя из этих соображений, экономия на сертификатах устройств представляется спорной. К счастью, множество стандартов было разработано для упрощения нам с вами развертывания надежной проверки подлинности всех звеньев цепи обмена данными. Стандарты существуют для форматов сертификатов, и надежные центры сертификации поддерживают как стандартные, так и кастомные форматы. В большинстве случаев сертификатами можно легко управлять удаленно (OTA) с помощью стандартных протоколов, таких как Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) и Online Certificate Status Protocol (OCSP). Благодаря надежному центру сертификации, который предоставляет возможность обрабатывать сертификаты, ключи и учетные данные, фактическую проверку подлинности можно делать с помощью мощных стандартов Transport Layer Security (TLS) и Datagram TLS (DTLS) – родственных SSL. Взаимная проверка подлинности, когда обе конечные точки проверяют друг друга, имеет решающее значение для

качественной защиты систем IoT. В качестве дополнительного бонуса, однажды выполнив проверку подлинности по TLS или DTLS, две конечные точки могут обмениваться ключами шифрования или получать их для обмена данными, которые невозможно расшифровать подслушивающими устройствами. Для многих приложений IoT требуется абсолютная конфиденциальность данных, это требование легко выполняется использованием сертификатов и протоколов TLS/DTLS. Однако когда конфиденциальность не является обязательным требованием, подлинность передаваемых данных может проверяться любой стороной, если они были подписаны во время их появления на датчике – такой подход не отягощает канал шифрованием, что предпочтительно в архитектурах multi-hop. Часто возникают вопросы касательно стоимости и производительности чипов IoT для криптографических операций. Здесь нужно принять во внимание, что Elliptic Curve Cryptography (ECC) в 10 раз быстрее и эффективнее, чем традиционное шифрование даже в ограниченных вычислительных ресурсах устройствах. Такая скорость и эффективность достигаются без снижения уровня безопасности. ECC даже продемонстрировал уровень защиты industry best practice, эквивалентный RSA 2048, в том числе на чрезвычайно ограниченных в ресурсах чипах – на 8-bit 1-MHz процессорах и 32-bit 1-KHz процессорах, при потреблении лишь микроватт энергии. DTLS, вариант TLS был разработан специально для маломощных устройств, которые периодически работают между циклами сна. И, наконец, цена таких 32-разрядных чипов составляет всего несколько десятков центов (при расчете в долларах), поэтому цену или мощность чипов не получится использовать в качестве аргумента для снижения требований по защите ниже разумных пороговых значений, когда безопасность имеет значение. В силу описанных факторов предлагаются следующие рекомендации по длине ключа для проверки подлинности устройства IoT, где безопасность имеет значение: минимум 224-bit ECC для сертификатов конечных объектов с предпочтением 256-bit и 384-bit; минимум 256-bit ECC для корневых сертификатов с предпочтением 384-bit. Сегод-

ня мы не можем представить себе такое неудобство, как ручную установку сертификатов в наши браузеры для каждого веб-сервера, в то же время, мы не можем представить себе, какой будет ущерб, если слепо верить любому сертификату. Вот почему каждый браузер имеет несколько корней доверия, по которым верифицируются все сертификаты. Встраивание этих корней в браузеры дало возможность масштабировать защиту на миллионы серверов в Интернете. Поскольку миллиарды устройств становятся онлайн ежегодно, в равной степени важно, чтобы в устройства встраивались и корни доверия, и сертификат устройства. Данные, связанные с IoT, должны храниться в безопасности все время. Наша жизнь зачастую зависит от правильности, целостности и надлежащего функционирования этих систем больше, чем от конфиденциальности данных. Проверка подлинности информации, устройств и происхождения информации может иметь решающее значение. Данные зачастую хранятся, кэшируются и обрабатываются несколькими узлами, а не просто передаются из точки А в точку Б. По этим причинам данные всегда должны быть подписаны в тот момент, когда они были впервые зафиксированы и сохранены. Это помогает снизить риски любого вмешательства в информацию. Подписание объектов данных, как только они были зафиксированы, и ретрансляция подписи с данными даже после их дешифрации является все более распространенной и успешной практикой [3].

Задачи создания профориентационной лаборатории заключались в следующем:

- 1) мониторинговые исследования уровня базовых знаний и представлений школьников об угрозах кибербезопасности в сфере IoT для построения индивидуальных траекторий обучения;
- 2) формирование программно-технической части профориентационной школьной лаборатории по кибербезопасности на базе ГГНТУ;
- 3) создание условий проведения регулярных занятий очной формы и онлайн-обучения со школьниками в рамках внеурочной кружковой работы на базе ГГНТУ, в том числе на платформе дистанционного обучения ГГНТУ;

4) заключение договоров с профильными ГБОУ и с муниципальными департаментами образования в регионе, а также с компаниями 1С и Cisco о сотрудничестве в области развития цифровых навыков школьников;

5) разработка и размещение в дистанционно-образовательной среде ГГНТУ учебно-методические материалы для обучения школьников в профориентационной лаборатории по кибербезопасности;

6) организация волонтерской деятельности студенческой молодежи и молодых преподавателей института прикладных информационных технологий (ИПИТ) ГГНТУ в деле наставничества по организации и реализации учебной работы профориентационной школьной лаборатории кибербезопасности в сфере Интернет-вещей;

7) непрерывное освещение в СМИ и социальных сетях деятельности профориентационной школьной лаборатории в целях популяризации IT-специальностей в профессиональном выборе школьников и дальнейшего построения карьеры в области обеспечения кибербезопасности.

Методология реализации.

1. Проведение анкетирования и вводного семинара для исследования представления школьников об угрозах кибербезопасности в сфере IoT и выяснения их реального уровня знаний и интереса к данной тематике.

2. Формирование банка электронных учебно-методических материалов и их экспертиза (консультанты 1С и Cisco) для обучения в профориентационной лаборатории школьников.

3. Подготовка профориентационной лаборатории школьников для запуска – подготовка помещений, создание рабочих мест учеников на базе действующей лаборатории ГГНТУ по информационной безопасности и приобретению дополнительного программно-технического оснащения, подключение лаборатории и электронных учебных материалов к платформе дистанционного обучения ГГНТУ [3].

4. Подбор и утверждение состава волонтерских студенческих групп и наставников.

5. Проведение обучения в дистанционном и очном форматах для получения школьни-

ками базовых понятий о сфере IoT в целом и угрозах кибербезопасности.

6. Реализация дополнительных учебно-тренировочных мероприятий со школьниками, развивающими познавательный интерес к информационным технологиям в области приобретения цифровых навыков обеспечения кибербезопасности.

Требования к оборудованию лабораторных ПК:

- Компьютер с ОЗУ не менее 4 и 8 Гб свободного дискового пространства;

- Высокоскоростной доступ к Интернету для загрузки программного обеспечения и работы с интерактивными средствами, например Blockly.

Дополнительные требования к аппаратному обеспечению:

Помимо необходимых лабораторных работ, в рамках данного курса имеются дополнительные лабораторные работы повышенной сложности, которые могут выполняться студентами, желающими углубленно изучить создание прототипов. Для выполнения лабораторных работ повышенной сложности студентам потребуется следующее оборудование:

- Prototyping Lab Kit (PL-Kit)
- Приложение Prototyping Lab App (PL-App) Launcher
- Файл образа Prototyping Lab App (PL-App)
- Проводное или беспроводное подключение (Ethernet или Wi-Fi) к локальной сети с использованием DHCP
- Raspberry Pi с адаптером питания
- Google Chrome или другой современный веб-браузер

Структура курса I2IoT 2.0

Этот курс предоставляет исчерпывающую вводную информацию о том, какую ценность несет взаимодействие элементов цифровизации и Интернета вещей для организаций, компаний, государственных органов и отраслей. Студенты узнают, как устройства, которые ранее не подключались к сети, станут подключенными и будут играть важную роль в системе Интернета вещей. Курс поможет студентам понять роли и обязанности для ИТ-профессий, связанных с Интернетом вещей, и узнать, как

можно создать собственную работу в сфере Интернета вещей.

Внедряемая профориентационная лаборатория предназначена для слушателей, которые хотят работать в сфере ИТ, со специализацией по информационной безопасности. В этом вводном курсе слушатели знакомятся с основными понятиями кибербезопасности. Программа курса включает такие темы, как: безопасность в Интернете, разные типы вредоносного ПО и атак, меры, предпринимаемые организациями для ослабления атак, а также возможности для профессионального роста и развития в сфере ИТ.

Программа рассчитана на слушателей с разным уровнем образования, обучающихся в различных учебных заведениях, в том числе в средней и высшей школах, университетах, колледжах, профессиональных и технических училищах [4].

Обзор программы:

Слушатели узнают об основных правилах поведения в сети для обеспечения безопасности.

Слушатели познакомятся с разными типами вредоносного ПО, атак и способов защиты организаций от этих атак.

Слушатели изучают карьерные возможности в сфере кибербезопасности.

Все понятия в данном курсе излагаются простым доступным языком, специально, чтобы они были понятны слушателям с любым уровнем образования, а включенные в курс интерактивные задания помогают лучше усвоить материал.

Задания включают лабораторные работы (в бумажном виде), видео и контрольные работы, в них использованы разные стили обучения, что помогает стимулировать процесс обучения и способствует удержанию знаний.

Методология реализации. Проведение анкетирования и вводного семинара для исследования представления школьников об угрозах кибербезопасности в сфере IoT и выяснения их реального уровня знаний и интереса к данной тематике.

Анкетирование проходит в формате заполнения формы с вопросами в электронном виде.

Общий срок разработки формы, проведение анкетирования, анализ результатов – 1 месяц.

Проведение обучения в дистанционно-очном формате для получения школьниками базовых понятий о сфере IoT в целом и угрозах кибербезопасности в частности. В процессе обучения используются электронные образовательные ресурсы (теория), а также оборудование лаборатории (практика). В процессе обучения школьники получают представление об экономических возможностях, которые открывает текущая цифровая трансформация, узнают, как благодаря IoT изменяются стандартные бизнес-процессы, как происходит сбор, хранение, анализ и визуализация данных, полученных от систем IoT, познакомятся с основами сетевых технологий, попробуют свои силы в выборе стратегии по снижению рисков, связанных с угрозами безопасности для IoT-систем, а также получают представление об их комплексной защите.

Этапы обучения включают в себя практическую часть, в рамках которой эксперты-преподаватели продемонстрируют на реальном оборудовании, наглядно имитирующем различные технологические процессы умного производства (или города), типичные угрозы кибербезопасности.

Проведение хакатона (креатона), в рамках которого школьники будут выявлять возможные угрозы кибербезопасности в сфере IoT, моделировать ситуации с использованием реального оборудования лаборатории и искать пути устранения выявленных угроз.

Хакатон (креатон) может быть рассчитан на один или несколько дней. В рамках хакатона (креатона) школьники совместно с экспертами-преподавателями смогут проверить свои предположения о возможных угрозах кибербезопасности и путях их устранения.

В рамках хакатона (креатона) перед школьниками выступят работающие в индустрии специалисты по кибербезопасности с примерами реальных кейсов, представители системы государственного и вендорского образования с информацией о возможностях получения образования в этой области, а также сотрудники HR (кадровых) департаментов крупных работодателей и кадровых агентств с целью рассказать

о востребованности вакансий для специалистов по кибербезопасности в различных отраслях промышленности.

Выводы. Внедрение данной профориентационной лаборатории актуально, в первую очередь, и в связи с тем, что системы IoT бывают очень сложными, им требуются комплексные меры защиты, покрывающие уровни облаков и подключений, также необходима поддержка устройств IoT с ограниченными вычислительными ресурсами, которых недостаточно для поддержки традиционных решений безопасности. Безопасность должна быть всесторон-

ней, иначе атакующие просто воспользуются самым слабым звеном. Конечно, традиционные IT-системы, как правило, передают и обрабатывают данные из систем IoT, но сами системы IoT обладают своими уникальными потребностями в защите.

Реализация профориентационной лаборатории должна способствовать формированию в регионе детского образовательного центра для внедрения инновационных технологий школьного образования в области кибербезопасности и популяризация профессий, связанных с информационными технологиями.

ЛИТЕРАТУРА

1. *Росляков А. В.* Интернет вещей: учебное пособие / *А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков.* Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. 135 с. ISBN 2227-8397. Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. URL: <http://www.iprbookshop.ru/71837.html> (дата обращения: 16.12.2019). Режим доступа: для авторизир. пользователей.
2. *Семенов Ю. А.* Процедуры, диагностики и безопасность в Интернет / *Ю. А. Семенов.* Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. 581 с. ISBN 978-5-94774-708-9. Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. URL: <http://www.iprbookshop.ru/62827.html> (дата обращения: 16.12.2019). – Режим доступа: для авторизир. пользователей.
3. *Семенов Ю. А.* Процедуры, диагностики и безопасность в Интернет / *Ю. А. Семенов.* Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. 581 с. ISBN 978-5-94774-708-9. Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. URL: <http://www.iprbookshop.ru/62827.html> (дата обращения: 16.12.2019). Режим доступа: для авторизир. пользователей.
4. <https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1>

VOCATIONAL SCHOOL LABORATORY ON THE BASIS OF CYBER SECURITY IN THE FIELD OF THE INTERNET OF THINGS (IOT)

© E. D. Alisultanova, L. K. Khadzhieva, M. Z. Isaeva
GSTOU named after acad. M. D. Millionshchikov, Grozny, Russia

This article is devoted to the creation of a career-oriented (smart) laboratory, which is designed to formulate in schoolchildren basic ideas about the Internet of Things (IoT) technology, cyber security threats in this area, motivate to receive specialized education in the future and build a career in the field of Internet things (IoT) security with the functioning of smart manufacturing.

The training of schoolchildren in a vocational guidance laboratory, based on the use of interactive electronic educational resources, will primarily position the career opportunities of future specialists in the field of Internet of Things (IoT) security in the operation of smart manufacturing.

Within the framework of the functioning of the laboratory, special attention of students is concentrated on the topics of the legal aspects of ensuring cyber security, the main trends in the development of cyber threats in the modern global information space and the measures necessary to neutralize them.

Keywords: laboratory, technology, Internet of things, educational resources

REFERENCES

1. Roslyakov, A. V., Vanyashin, S. V. and Grebeshkov A. Yu. (2015) Internet veshchei: uchebnoe posobie. Tekst: elektronnyi // Elektronno-bibliotchnaya sistema IPR BOOKS. [Internet of things: a training manual]. Available at: <http://www.iprbookshop.ru/71837.html> (accessed: 16.12.2019). Access mode: for authorized users. Samara: Volga State University of Telecommunications and Informatics. ISBN 2227-8397. P. 135.
2. Semenov, Yu. A. (2016) Protsedury, diagnostiki i bezopasnost' v Internet. Tekst: elektronnyi // Elektronno-bibliotchnaya sistema IPR BOOKS: [sait]. [Procedures, diagnostics and security on the Internet]. Available at: <http://www.iprbookshop.ru/62827.html> (accessed: 16.12.2019). Access mode: for authorized users. Samara: Volga State University of Telecommunications and Informatics. ISBN 978-5-94774-708-9. P. 581.
3. Semenov, Yu. A. (2016) Protsedury, diagnostiki i bezopasnost' v Internet. Tekst: elektronnyi // Elektronno-bibliotchnaya sistema IPR BOOKS: [sait]. [Procedures, diagnostics and security on the Internet]. Available at: <http://www.iprbookshop.ru/62827.html> (accessed: 16.12.2019). Access mode: for authorized users. Moscow: Internet University of Information Technologies (INTUIT). ISBN 978-5-94774-708-9. P. 581.
4. Available at: <https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1>