Научная статья
УДК_004.624
DOI: 10.17072/1993-0550-2022-4-68-81

Безопасность применения IoT в сфере здравоохранения

Ксения Леонидовна Поторочина[1], Елена Юрьевна Никитина[2]
[1,2]Пермский государственный национальный исследовательский университет, Пермь, Россия
[1]kseniyapotorochina@gmail.com
[2]neyu@psu.ru, https://orcid.org/0000-0001-6639-9876, AuthorID 147895

Аннотация. Рассмотрены тенденции применения IoT для здравоохранения в мире и связанные с ними проблемы обеспечения безопасности таких устройств. Произведен анализ типовых IoT-систем и распределение наиболее актуальных угроз по основным уровням. На основании выполненного анализа и специфики прикладной сферы предложен перечень рекомендаций по созданию безопасной IoT-системы для здравоохранения.

Ключевые слова: *IoT; IoMT; здравоохранение; интернет вещей; уровень восприятия; транспортный уровень; прикладной уровень; аутентификация; сертификация; стандартизация; технология NTA*

Для цитирования: *Поторочина К. Л., Никитина Е. Ю.* Безопасность применения IoT в сфере здравоохранения // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 68–81. DOI: 10.17072/1993-0550-2022-4-68-81.

Статья поступила в редакцию 21.10.2022; одобрена после рецензирования 11.11.2022; принята к публикации 15.11.2022.

Research article

Security of IoT Applications in Health Care

Kseniya L. Potorochina[1], Elena Yu. Nikitina[2]
[1,2]Perm State University, Perm, Russia
[1]kseniyapotorochina@gmail.com,
[2]neyu@psu.ru, https://orcid.org/0000-0001-6639-9876, AuthorID 147895

Abstract. The trends in global healthcare IoT applications and the associated challenges in securing such devices are examined. An analysis is made of typical IoT-systems and the distribution of the most relevant threats to the main IoT layers. Based on this analysis and the specifics of the application area, a list of recommendations for creating a secure IoT-system for healthcare is proposed.

Keywords: *IoT; IoMT; healthcare; internet of things; sensors; transport layer; application layer; authentication; certification; standardization; NTA technology*

For citation: *Potorochina K. L., Nikitina E. Yu.* Security of IoT Applications in Health Care // Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2022;4(59):68–81. (In Russ.). DOI: 10.17072/1993-0550-2022-4-68-81.

The article was submitted 21.10.2022; approved after reviewing 11.11.2022; accepted for publication 15.11.2022.

Введение

Современное здравоохранение – сфера, в которой интернет вещей (IoMT – Internet of medical things) значительно распространился. К 2022 г. здравоохранение возглавило список сегментов с наибольшим ростом внедрения IoT (IoT – Internet of things), за которым следуют интеллектуальные энергосистемы, подключенные автомобили и приложения для умных городов. IoMT совершенствует и развивает отрасль здравоохранения, помогает реализовать многие функции.

Вопросы безопасности и риски в медицинских системах намного сложнее, чем в других отраслях. Информация о пациентах является чрезвычайно важной и конфиденциальной, а своевременный доступ к информации имеет решающее значение для работников здравоохранения. Однако безопасность устройств IoT часто игнорируется или рассматривается производителями медицинских устройств как нечто второстепенное. В основном это связано с коротким сроком выхода на рынок и снижением затрат, определяющих процесс проектирования и разработки устройств.

1. Возможности применения IoT в здравоохранении

1.1. Мониторинг состояния пациентов, которые находятся в больнице

IoMT помогает осуществлять наблюдение за состоянием оборудования в палатах, отслеживать состояние тяжелых больных с помощью специальных датчиков. Такие устройства контролируют, отслеживают и обновляют данные о состоянии пациента, не привлекая младший медицинский персонал.

Датчики чаще всего располагаются на больничных койках. Например, специальные сенсоры, выпускаемые компанией SMI, которые предупреждают пролежни у тяжелых больных (они измеряют и распределяют давление на матрас). Также существуют устройства, которые мониторят частоту сердечного ритма, дыхания. Они сигнализируют персоналу больницы, если происходят критические изменения [1].

1.2.Удаленный мониторинг состояния пациентов

Такой мониторинг включает в себя сбор данных о состоянии здоровья пациента до визита к врачу, дистанционную консультацию с медицинскими специалистами по неотложным вопросам, составление карты активности больного, проявлений его хронических заболеваний, возможность быстро оказывать помощь в критических случаях (например, при инсультах).

Различные устройства, взаимодействуя с умными приложениями, выполняют базовые действия, которые часто только отнимают время у медицинского персонала. Например, для реабилитации пациентов после инсульта, используются специальные гибкие гаджеты. Они закрепляются на шее, чтобы контролировать способность глотать и отслеживать нарушения речи. Пациент может находиться дома и заниматься повседневными делами. Вся информация отслеживается в режиме реального времени и ускоряет реабилитацию человека [1].

1.3. Оптимизация ухода за больными

Для простоты и быстроты решения вопросов по уходу за пациентами клиники интегрируют в свою работу умные системы. Например, система AutoBed (разработка GE Healthcare) помогает медсестрам не только быстро и эффективно распределить больных по койкам, но и проконтролировать количество пациентов и отследить их перемещения по больнице. Для работы данной системы используются идентификационные метки, инфракрасный порт и компьютерное зрение. Применение IoMT с целью оптимизации ухода за больными позволяет уменьшить время ожидания в два раза – это особенно важно для пациентов, поступивших по системе неотложной помощи [1].

1.4. Умные медицинские приборы

IoT-устройства способны собирать и анализировать информацию о работе самого медицинского учреждения. Оптимизировать работу больниц призвана и система e-Alert от компании Philips. Она помогает комплексно следить за состоянием медицинских устройств, приборов, оборудования. Эта система способна спрогнозировать и предупредить поломки, она сообщает, когда технике необходимы плановый осмотр и замена деталей [1].

1.5. Усовершенствованное управление лекарственными средствами

Благодаря IoMT, в здравоохранении стали использовать и совершенно новые способы мониторинга здоровья и лечения пациентов.

В мире появляются умные таблетки со встроенными датчиками – они важны для точности определения информации о состояния человека. Компания AdhereTech создала еще одно умное решение. Их разработка представляет собой смарт-коробочку для лекарственных препаратов: устройство способно напоминать людям, что пришло время пить лекарства, при этом специальные сенсоры фиксируют, когда препарат достают из коробки. Система подает звуковые сигналы, если, согласно графика, этого не произошло или если прием был слишком ранним. Пациент получает информационное уведомление на свой смартфон. При этом данные о приеме лекарств получает и лечащий врач. Это поможет сократить риск рецидивов после лечения, вызванных неправильным приемом медикаментов.

Таким образом, устройства и умные системы призваны не заменить врачей и медсестер, а облегчить и оптимизировать их работу [1].

2. Развитие IoT технологий в Российской федерации

IoT обладает значительным потенциалом для развития отрасли здравоохранения. Пациенты и поставщики получают преимущества по нескольким причинам: снижение затрат, улучшенные результаты лечения, улучшенное управление заболеванием, дистанционный мониторинг хронических заболеваний, улучшенный самоконтроль пациента, усовершенствованное управление лекарственными препаратами, эффективная работа медицинских учреждений.

Масштабное подключение устройств означает, что значительно увеличится количество конфиденциальных данных. В связи с этим медицинские специалисты должны быть уверены, что эти устройства безопасны для пациента и не используются не по назначению, что данные людей, проходящих лечение, защищены, а ошибки обрабатываются своевременно и правильно, чтобы гарантировать безопасность пациентов.

На данный момент глобальный рынок интернета вещей в сфере здравоохранения охватывает пять основных географических регионов – Северную Америку, Азиатско-Тихоокеанский регион, Европу, Ближний Восток и Африку, Латинскую Америку.

По данным компании Statista, объем мирового рынка IoT в 2020 г. составил 389 млрд долларов США. Согласно прогноза к 2030 г. вырастет до более 1 трлн долларов США [2].

В России наметились тенденции в развитии интернета вещей. Однако данные технологии развиваются достаточно медленно. Данный факт характерен не только для применения интернета вещей в области здравоохранения.

Дорожная карта развития интернета вещей в Российской Федерации была утверждена в 2020 г. Она была разработана ГК "Ростех". В соответствии с картой планируется выделить на развитие интернета вещей 10,1 млрд рублей до 2024 г. Наблюдательный совет АНО "Цифровая экономика", координатор государственной программы "Цифровая экономика РФ", в октябре 2021 г. утвердил стратегию развития до 2024 г. В качестве приоритетных задач бизнеса и государства заявлены: развитие интернета вещей, а также цифровой инфраструктуры 5G, широкополосного доступа и центров обработки. Чтобы реализовать поставленные цели, формируется план опережающего развития безопасной открытой инфраструктуры [3].

К 2025 г. планируется, что в Российской Федерации будет 1 млрд устройств интернета вещей. Достижение такого показателя дает возможность превысить среднемировые показатели проникновения устройств интернета вещей и обеспечить эффективное изменение важных отраслей (здравоохранение, транспорт, сельское хозяйство) за счет обеспечения их необходимыми данными, полученными при помощи IoT [4].

По данным компании МТС, в 2021 г. объем рынка IoT в России составил 117 млрд рублей, что стало возможным за счет активного внедрения интернета вещей в ЖКХ и промышленности. Согласно прогноза компании МТС, объем рынка IoT будет расти со среднегодовым темпом 16,5 % до 2023 г. включительно. Экономический эффект от реализации технологий IoT в сфере здравоохранения в России составит до 536 млрд рублей до 2025 г. (по прогнозу PWC) [1,2].

3. Уровни IoT-системы и угрозы

При всех преимуществах применение IoT сопряжено с вероятностью новых атак безопасности и уязвимостей в системах здравоохранения.

Типовая IoT-система состоит из трех уровней: восприятие, транспортировка, применение. Каждый из этих уровней системы имеет свои специфические технологии, которые создают проблемы и некоторые возможные слабые места с точки зрения информационной безопасности.

3.1. Уровень восприятия

Первый уровень связан с физическими датчиками IoT для реализации сбора и обработки данных при помощи различных распространенных технологий, таких как RFID, WSN, RSN и GPS. Этот уровень включает датчики и исполнительные устройства для отслеживания в реальном времени местоположения медицинского оборудования, измерений температуры, давления, уровня глюкозы, количества кислорода в крови и т.д. Для данного уровня существуют следующие угрозы безопасности, описанные в [9].

3.1.1. Физические атаки

Данные виды атак направлены на аппаратные компоненты системы IoT, и атакующему необходимо физически находиться рядом или в системе IoT, чтобы атаки сработали. Злоумышленник может нанести ущерб узлу, физически заменив его или часть его оборудования, чтобы получить доступ и изменить конфиденциальную информацию, такую как общие криптографические ключи или таблицы маршрутизации. Злоумышленник может компрометировать узел, физически внедрив в него вредоносный код, который даст ему доступ к системе IoT [9].

3.1.2. Бесконтактные атаки

Атаки могут осуществляться и без установления соединения с граничным узлом. Реализовать такую атаку можно при подключении к линии питания или при измерении уровня излучаемых помех либо вибрации на незащищенном устройстве. Используя недокументированное поведение или неполадки, например, искусственно вызвав скачок напряжения, можно перевести устройство в незарегистрированное незащищенное состояние [9, 13].

3.1.3. Сетевые атаки

Такие веб-инструменты, как Shodan, могут сканировать сеть, идентифицируя каждый незащищенный узел. Несмотря на то, что TLS-защита важна и эффективна, могут оставаться тонкие уязвимости из-за ошибок в реализации TLS для граничного узла, плохого использования случайных чисел в криптоалгоритмах, необнаруженного вредоносного ПО, агрессивных протокольных атак с установленных экспертных узлов и даже из-за слабых мест самих протоколов [9, 13].

3.1.4. Атаки на порты

Небольшой граничный узел, который не использует ПО, может иметь только одно подключение – сетевой порт (проводной или беспроводной). Сложные граничные узлы, однако, могут быть оснащены, например, модульными портами для подключения различных датчиков, USB- или другими (даже беспроводными) портами для подключения периферийных устройств, расходных материалов (например, чернильных картриджей) или для тестирования и отладки оборудования. Каждый порт предоставляет возможность доступа к граничному узлу. Атака может проходить через неиспользуемый порт. В отличие от сетевого порта для защиты этих портов не существует установленного стандарта [13].

3.2. Транспортный уровень

Транспортный уровень в основном обеспечивает повсеместный доступ к среде для уровня восприятия. Целью этого уровня является передача собранной информации, полученной от уровня восприятия, в любую конкретную систему обработки информации через существующие сети связи. Как правило, на этом уровне основными угрозами безопасности являются: атаки на маршрутизацию (промежуточные вредоносные узлы могут изменять правильные пути маршрутизации в процессе сбора и пересылки данных), DoS-атаки (самый распространенным методом является сетевой флуд, создание огромного потока запросов на разных уровнях, с которыми физически не может справиться принимающий узел) [9].

3.3. Уровень применения (приложений)

Прикладной уровень предоставляет услуги, запрашиваемые клиентами. На этом уровне может быть реализована система "Умное здравоохранение". Основными угрозами безопасности на этом уровне являются те, что описаны в [9].

3.3.1 DoS-атаки

Атаки направлены на уязвимости в приложениях и операционных системах (Apache, Windows, OpenBSD и т.п.). Они приводят к неработоспособности какого-либо приложения

или ОС в целом. Среди таких атак: Slowloris, атаки нулевого дня и прочие. Такие атаки состоят из запросов и требуют малое количество ресурсов от атакующего. Лимит одновременных подключений на атакуемом сервере весьма быстро заканчивается, и он перестает принимать полезные запросы. Атаки прикладного уровня, реализованные с помощью DoS, также могут быть ориентированы на стирание памяти или информации с диска, извлечение и использование данных из БД [5].

3.3.2 Проблемы в механизмах аутентификации

Уязвимость обусловлена неограниченным количеством попыток войти в аккаунт, возможностью аутентификации только по паролю. Злоумышленник может воспользоваться перебором комбинаций "логин/пароль" [14].

3.3.3 Низкая осведомленность пользователей

Для реализации могут использоваться USB-устройства с заманчивым для простого сотрудника названием (годовой отчет, финансовый план), в которые внедрен эксплойт. Возможен вариант, когда злоумышленник приходит на собеседование и просит распечатать секретаря резюме со своего USB-устройства, которое он якобы забыл. Пользователи также привыкли доверять письмам, полученным по электронной почте. Письмо от руководителя не вызывает сомнения у пользователя, но может содержать вложение с вшитым эксплойтом или ссылку на HTML-страницу, с заранее размещенным инструментом проникновения [6].

4. Особенности требований и обеспечения безопасности IoT-систем

4.1. Базовые требования к безопасности

Для определения требований безопасности к IoT системам рассмотрим традиционную модель CIA относительно сферы здравоохранения. Данная модель основана на использовании трех основных областей, которыми являются: конфиденциальность, целостность и доступность данных.

Конфиденциальность гарантирует, что система IoT запрещает неавторизованным лицам (пользователям и устройствам) раскрывать медицинскую информацию [8, 10].

Целостность относится к полноте и точности данных на протяжении всего жизненного цикла системы. Целостность гарантирует, что медицинские данные пациентов не будут изменены, удалены или искажены злоумышленником, что приведет к ошибочному диагнозу или неправильному назначению [8, 11].

Доступность гарантирует, что медицинские данные и устройства будут доступны для авторизованных пользователей, когда это необходимо. Это означает непрерывность служб безопасности и предотвращение любых сбоев устройств и сбоев в работе. В частности, в процессе лечения, когда врачам должны быть доступны своевременные данные о пациентах [8, 11].

4.2. Сравнение традиционной ИТ безопасности и безопасности IoT

Основная проблема заключается в том, что традиционных требований к безопасности недостаточно, а традиционные методы защиты ИТ не работают в отношении IoT. Это происходит ввиду некоторых особенностей IoT-систем:

1) большинство IoT-устройств являются "закрытыми", поэтому клиенты не могут обеспечить безопасность программного обеспечения после того, как устройства были отправлены с завода. По этим причинам безопасность должна быть встроена в IoT-устройства;

2) IoT-система состоит из узлов с ограниченными аппаратными и программными ресурсами, в то время как традиционные ИТ в основном основаны на богатых ресурсами устройствах. Таким образом, в мире IoT в большинстве случаев можно использовать только легкие алгоритмы, чтобы найти правильный баланс между более высокой безопасностью и меньшими возможностями;

3) для устройств IoT характерна широкая гетерогенность, она легко наблюдается в каждом функциональном элементе (идентификация, зондирование, связь, вычисления, сервис и семантика). Большое количество разнородных данных увеличивает поверхность атаки [8, 9] (см. таблицу).

Сравнение традиционной ИТ безопасности и безопасности IoT

Критерий сравнения	Традиционная ИТ-безопасность	Безопасность IoT
Способ обеспечения защиты	Дополнительная безопасность	Встроенная система безопасности
Сложность алгоритмов защиты	Сложные алгоритмы	Легкие алгоритмы для устройств с ограниченными ресурсами
Возможность контроля	Пользовательский контроль собираемой информации	IOT часто собирают информацию автоматически, без постоянного контроля пользователя
Уровень технологической неоднородности	Небольшая технологическая неоднородность	Большая технологическая неоднородность, следовательно, большая площадь атаки
Тип среды (открытая/закрытая)	ИТ- устройства расположены в закрытых средах	IOT устройства расположены также в открытых средах

4.3. Дополнительные требования к безопасности IoT

Основываясь на отличительных особенностях IoT-систем и специфике сферы здравоохранения, обозначим дополнительные требования к безопасности:

1) идентификация и аутентификация: идентификация гарантирует идентичность всех объектов (пациентов, врачей, устройств и т. д.) перед тем, как разрешить им взаимодействовать с ресурсами системы IoT. Аутентификация устройств и приложений может доказать, что взаимодействующая система не является злоумышленником, а данные, которыми обмениваются в сетях, являются законными [10, 11].

2) авторизация (контроль доступа): после проверки личности пользователя должны быть определены права доступа или привилегии к ресурсам, чтобы разные пользователи могли получить доступ только к тем ресурсам, которые требуются в зависимости от их задач. Например, у врача должен быть больший доступ к данным пациентов, чем у других поставщиков медицинских услуг [10, 11].

3) отчетность: в системе интернета вещей в здравоохранении: отчетность должна гарантировать, что организация или физическое лицо обязаны нести ответственность за свои действия в случае кражи данных или другого неправомерного события [12].

4) актуальность данных: актуальность данных означает, что отображаемые данные должны быть полученными на текущий момент времени. Например, врачу необходимо знать текущую информацию пациента о его электрокардиографии (ЭКГ) [10].

4.4. Градация основных уровней типовой IoT-системы по степени уязвимости

Анализируя уровни типовой IoT-системы по модели CIA и дополнительным характеристикам, можно сделать следующие выводы:

1) уровень восприятия является самым уязвимым и наиболее сложным для защиты. Это происходит из-за того, что граничные узлы представляют, как правило, небольшие недорогие интеллектуальные устройства, которые отличаются очень ограниченными ресурсами. Зачастую ошибочно полагают, что они малоуязвимы для атак. В то время как серверы, к которым устройства обращаются, и сети, которые их соединяют, оснащены проверенными средствами обеспечения безопасности, граничные узлы обычно не защищены, по крайней мере, пока. Задача состоит в том, чтобы обеспечить безопасность граничных узлов, оставаясь в узких пределах доступных ресурсов – с точки зрения вычислительной мощности, памяти и энергопитания, а также в рамках бюджета. Важно также учитывать проблему использования только одного вида технологии безопасности, так как существует технологическая неоднородность IoT-устройств.

2) транспортный уровень можно отнести к более низкому уровню риска, по сравнению с уровнем восприятия, из-за известных недостатков стандартных технологий беспроводной передачи данных, а также известных угроз в сетях доступа. Преимуществом этого уровня является интенсивное исследование уязвимостей и постоянная разработка новых методов защиты.

3) на прикладном уровне вопросы конфиденциальности являются не менее сложными, поскольку в сфере здравоохранения сохранение частной информации о пациенте является принципиальным вопросом. На данном уровне также серьезную проблему составляют Dos-атаки, поскольку они чрезвы-

чайно узко направлены, благодаря чему могут создать серьезные проблемы атакуемому при малых затратах ресурсов атакующего.

5. Основные проблемы и их актуальность

5.1. Примеры атак на медицинские IoT-устройства

Проблемы безопасности, характерные для устройств интернета вещей, вызваны быстрым ростом спроса на них. Если обратиться к статистике, то можно узнать, что между 2008 и 2010 гг. количество любых продуктов, подключенных к интернету, превысило население планеты. Прогнозируется, что к 2025 г. число IoT-устройств превысит 75 млрд. Рынок интернета вещей будет расти к 2027 г. до более чем 2,4 триллиона долларов в год. Большое распространение данной технологии означает большее количество атак.

"Атаки становятся все более изощренными. Наблюдался резкий всплеск атак на медицинские устройства во время COVID-19", – сказал Кристиан Рено, директор по исследованиям IoT в 451 Research, входящей в S&P Global Market Intelligence. "Мы наблюдаем рост атак на устройства IoT в целом, но особенно в секторе здравоохранения".

В 2018 г. на Black Hat многие исследователи высказались о значительных недостатках в безопасности IoMT. Джонатан Баттс (директор QED Secure Solutions) и Билли Риос (основатель WiteScope – фирмы по обеспечению безопасности) показали, каким образом злоумышленники смогут удаленно получить контроль над кардиостимулятором Medtronic и назначать или отменять разряды для пациентов.

Одной из самых известных атак на систему здравоохранения в последние годы, начиная с 2017 г., стала программа-вымогатель WannaCry. В результате атак на уязвимости в ОС Windows хакерам удалось заблокировать доступ медицинских работников к уязвимым устройствам [7, 15, 16].

В 2022 г. компанией Palo Alto Networks была сделана публикация об исследовании медицинских насосов. Данное исследование реализовалось при помощи решения интернета вещей Security for Healthcare.

В результате сканер показал, что 75 % медицинских инфузоматов содержат одну или более из 40 известных программных уязвимостей или "один, или более из 70 известных дефектов безопасности IoT-устройств". 52 % из всех исследованных инфузоматов содержат две уязвимости, раскрытые в 2019 г., то есть более двух лет назад. Причем из десяти самых часто встречающихся уязвимостей шесть являются критическими, их степень угрозы составляет 9,8 балла.

Такой уязвимостью является – CVE-2019-12255 (переполнение буфера в TCP-компоненте Wind River VxWorks), она была выявлена в 2019 г. Остальные пять уязвимостей были определены в 2020 г. Инфузоматы относятся к числу тех устройств, от которых может напрямую зависеть жизнь пациентов, поэтому важно, как можно скорее устранить в них критические уязвимости [17].

5.2. Основные препятствия в создании безопасной IoMT-системы

Основываясь на проделанном исследовании, определим актуальные на данный момент факторы, оказывающие негативное влияние на информационную безопасность IoT-устройств:

1) большинство IoT-устройств не получают достаточного количества обновлений, а некоторые вообще не получают критических обновлений безопасности. Поэтому когда-то безопасные устройства становятся уязвимыми, незащищенными и в итоге подвергаются хакерским атакам. Для производителей IoT приоритетом является экономия ресурсов и быстрая поставка, что плохо сочетается с серьезным обеспечением безопасности. Большая часть производителей предлагает обновления прошивки лишь в течение небольшого периода времени;

2) большинство IoT-устройств являются "закрытыми", поэтому клиенты в принципе не могут обеспечить безопасность программного обеспечения после того, как устройства были отправлены с завода;

3) ограниченные аппаратные и программные ресурсы граничных узлов требуют легких и простых алгоритмов защиты, что отличается от стандартных возможностей защиты ИТ;

4) проблема паролей по умолчанию. Данная проблема возникает, если после поставки устройств с паролями по умолчанию потребителей не предупредили о необходимости и важности смены паролей после получения. На данный момент не существует юридических последствий, которые могли бы побудить производителей более внимательно относиться к данной ситуации.

Таким образом, любое учреждение, которое использует заводские учетные данные по умолчанию на своих устройствах, подвергает своих пациентов и их ценную информацию риску;

5) нехватка навыков в области IoT. В наше время многие компании утверждают, что существует большой пробел в навыках специалистов по безопасности IoT, нехватка программ обучения и курсов повышения квалификации. Это касается как специалистов, так и конечных пользователей, которые могут неосознанно облегчить атаку злоумышленников;

6) проблема управления IoMT. При использовании IoMT-устройств в здравоохранении было обнаружено большое количество уязвимостей в разнообразном наборе подключенных объектов. Сочетание традиционных подключенных устройств и устаревших систем, таких как аппараты искусственной вентиляции легких, мониторы пациента, светильники, инфузионные насосы с низким уровнем безопасности, подвержены хакерским атакам.

6. Модель безопасности для IoT-систем в здравоохранении

Создание безопасной IoMT-системы требует комплексного подхода. IoT состоит из нескольких уровней, распределение которых по росту уязвимости имеет следующий вид: транспортный уровень, уровень применения, уровень восприятия. Основываясь на этом, выдвинем несколько предложений, которые положительно повлияют на безопасность всей системы, но будут реализованы преимущественно на уровнях восприятия и применения.

6.1. Идентификация и аутентификация граничных узлов

Для создания безопасной системы здравоохранения на основе IoT необходимо обнаруживать и идентифицировать граничные узлы. До обеспечения шифрования и защиты транспортного уровня (при помощи TLS/SSL протоколов) нужно определить, кто именно хочет подключиться к сети. Это важно, поскольку злоумышленник может получить контроль над граничным узлом, не затрагивая сеть. В таком случае, несмотря на надежную защиту канала связи между сервером и конечным узлом, TLS/SSL не помогут.

В связи с этим IoMT-устройства должны иметь личный сертификат или некий секретный ключ, который позволит стойко аутентифицировать устройство. При этом безопасность системы здравоохранения будет определяться тем, насколько хорошо хранятся ключи. Поскольку граничный узел – это устройство с ограниченными ресурсами (память, энергопитание, вычислительная мощность, бюджет), то производителям IoMT устройств необходимо предложить такие инструменты для разработки, которые снизили бы затраты на внедрение безопасности в конечные изделия на этапе его проектирования и производства, в частности, зашифрованное хранение ключей в защищенном оборудовании при помощи аппаратных модулей безопасности (HSM).

В качестве решения можно предложить – криптоэлементы – микросхемы на основе схем с коррекцией ошибок, которые должны соответствовать криптографическому протоколу ECDH (Elliptic-curve Diffie–Hellman). Необходимо, чтобы такая микросхема была оснащена защищенным аппаратным хранилищем секретных ключей, а также алгоритмами эллиптической криптографии ECDSA (Elliptic Curve Digital Signature Algorithm) для обеспечения функций ассиметричной аутентификации [21, 22].

Микросхема является компактной и может быть добавлена в любой IoMT-узел, позволяя обеспечить аутентификацию, целостность и конфиденциальность для всей системы, с учетом ограниченных ресурсов конечных узлов. Внедрение данного решения не требует высоких затрат.

Для обеспечения дополнительной безопасности граничных устройств можно также экранировать устройство сеточным рисунком металлизации. Благодаря такому решению можно создать барьер для электромагнитного излучения, что позволит преградить детектирование внутренних сигналов, а также создать визуальную защиту от тех злоумышленников, которые вскрывают корпус с целью изучения работы устройства. При этом экран необходимо подключить к остальной части схемы, для того чтобы устройство перестало работать в случае повреждения экрана [21, 23].

Для обеспечения безопасности граничных узлов важно развитие микроэлектронной продукции, а именно технологий TEE, TPM. TPM – это аппаратное обеспечение, специально созданное для крипто-вычислений, физически изолировано от остальной части си-

стемы обработки и часто является отдельной интегральной схемой на материнской плате. TEE – это область на чипсете, которая работает как TPM, но физически не изолирована от остальной части чипа. Технологии TEE активно развиваются и представляют перспективную альтернативу, представленной выше HSM [24].

6.2. Стандартизация и сертификация

При создании системы "Умного здравоохранения" появляется проблема в организации взаимодействия устройств от разных производителей. В целом большинство медицинских устройств являются гетерогенными по своей природе и подключаются к различным системам или сетям, обмениваются данными по сети. Высокая конкуренция производителей "умных" устройств для медицинских учреждений и постоянное развитие технологий беспроводной связи усложняют введение стандартов.

На данный момент в России утвержден национальный стандарт интернета вещей: "Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi) ", вступивший в силу с 2019 г. В 2021 году был утвержден также стандарт для протокола LoRaWAN (Long Range Wide Area Networks) в форме предварительного национального стандарта (ПНСТ) "Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением". Существует также первый международный стандарт промышленного интернета вещей, разработка которого велась по инициативе "Ростелекома". Однако эти стандарты не могут полностью решить проблему организации безопасного взаимодействия IoT-устройств. Поэтому приведем меры, которые могли бы положительно повлиять на текущую ситуации [20, 25]:

• формулировка минимальных критериев для совместимости устройств от различных производителей;

• реализация экспертиз граничных устройств на их совместимость перед продажей. Проверка на соответствие требованиям минимальных критериев, то есть процесс сертификации;

• реализация тестирования устройств с четырех областей: тестирование компонент, тестирование функциональности, нагрузочное тестирование, тестирование безопасности. На сегодняшний день не существует единого подхода и стандарта по тестированию IoMT [26, 27].

Сертификация может заставить производителей пересмотреть свое отношение к безопасности, выпускаемых ими устройств. Прохождение проверки и получение соответствующего сертификата будет гарантировать медицинскому учреждению определенную защиту от покушений злоумышленников. Главное условие такой процедуры, чтобы она была доступна производителям и не превратилась в чистую формальность.

Сформулируем набор требований и критериев для разработчиков, производителей IoT-устройств и поставщиков услуг, который направлен на улучшение безопасности:

1) уведомление медицинской организации о том, может ли устройство получать обновления безопасности и способе получения уведомлений, требуемые действия пользователей;

2) обеспечение наличия механизма автоматизированного безопасного предоставления обновлений ПО. Обновления должны быть подтверждены каким-либо образом, как исходящие из надежного источника;

3) все IoMT-устройства и связанные с ними приложения должны поддерживать общепринятые протоколы безопасности и криптографии;

4) обновления не должны изменять пользовательские настройки, параметры безопасности и конфиденциальности без уведомления пользователя – особенно важно для устройств удаленного мониторинга состояния пациентов;

5) проектирование устройств в соответствии с минимальными требованиями, необходимыми для работы в медицинском учреждении. Например, порты USB или слоты для карт памяти следует включать только в том случае, если они необходимы для работы и обслуживания устройства. Неиспользуемые порты и службы должны быть отключены;

6) проведение оценки рисков при использовании IoT-устройств;

7) обязательное осуществление проверки, IoMT-устройств и связанных с ними приложений на тщательное тестирование;

8) IoMT-система должна поддерживать отправку предупреждений о любых попытках

обновления, получения административного доступа, несанкционированного доступа, изменения настроек, связанных с обработкой конфиденциальных данных пациентов;

9) обеспечение общепринятых механизмов восстановления паролей учетных записей пользователей для приложений на основе IoMT;

10) поддержка многофакторной проверки и аутентификации (электронная почта, телефон и т.д.) личности пользователя для контроля доступа к учетной записи в приложениях на основе IoMT;

11) обеспечение мер для защиты от подбора паролей, выполнение блокировки учетной записи пациента или медицинского персонала после разумного количества неверных попыток входа в аккаунт;

12) уведомление пользователей о необходимости смены заводских паролей на устройствах IoMT личными паролями. Внедрение специальных методов защиты, которые при первом включении устройства потребуют от пользователя сменить установленный пароль на новый;

13) реализация на этапе производства получения каждым IoMT-устройством уникального пароля с сохранением требования о смене заводского пароля;

14) обеспечение доступности политик конфиденциальности, безопасности и поддержки. Медицинская организация в качестве предполагаемого клиента должна иметь возможность ознакомиться с ними перед покупкой и активацией;

15) оповещение пользователей о продолжительности периода поддержки безопасности и наличия обновлений, а также их прекращения.

16) ознакомление пользователей с информацией о том, какие типы личных и конфиденциальных данных пациентов собираются и как они используются. Ограничение сбора информации теми данными, которые необходимы для оказания медицинских услуг. Обязательное предоставление потребителем согласия на использование данных для любых других целей. [28].

6.3. Применение технологии NTA

На конечные устройства IoMT невозможно поставить антивирусное ПО и обеспечить дополнительные механизмы защиты после того, как они были отправлены с завода. Единственной точкой контроля является сеть. Для сферы здравоохранения хорошо подходит технология NTA (Network Traffic Analysis), позволяющая выявить аномальное поведение сетевого трафика. Такое решение дает возможность контролировать трафик как между корпоративной сетью и интернетом, так и трафик, циркулирующий внутри медицинского учреждения.

Для выявления атак используются разные техники (поведенческий анализ, машинное обучение). NTA может применяться в сетях любого масштаба, равно как и любой архитектуры: локальной, облачной, гибридной. Реализуется также хранение трафика, благодаря чему можно исследовать инциденты безопасности. Технология позволяет получить представление обо всем трафике, независимо от того, зашифрован он или нет. Поэтому независимо от того, является организация небольшой частной медицинской клиникой или медицинским учреждением государственного уровня инструмент безопасности на основе NTA снижает риск воздействия на конфиденциальные данные пациентов, умные медицинские приборы [18, 19].

6.4. Обучение медицинского персонала

Широкое распространение IoT-технологий в сфере здравоохранения требует от сотрудников как определенного уровня знаний и навыков по работе с умными устройствами, так и в целом компьютерной грамотности.

Необходимо разработать и реализовывать программу по повышению квалификации медицинского персонала с учетом следующих особенностей:

1) большая часть обучающихся – это взрослые люди, которые имеют определенные барьеры восприятия нового материала. Проблемой может стать утрата навыков обучения, низкая мотивация и заинтересованность, страх перед новыми и непонятными технологиями, сложившиеся привычки и стереотипы;

2) отсутствие базового технического образования – для таких пользователей начальный курс должен быть направлен на овладение основными навыками по работе с компьютером;

3) молодые специалисты после обучения в вузе имеют навыки в "медицинской информатике", поэтому для них обучающие

курсы должны быть ориентированы преимущественно на ознакомление с необходимыми вопросами информационной безопасности.

Любое медицинское учреждение, которое хочет создать безопасную систему на основе IoT, должно иметь инструкцию с базовыми правилами информационной безопасности. Необходимо выдавать ее каждому новому сотруднику и периодически напоминать уже работающим специалистам о важности соблюдения изложенных в ней правил.

Заключение

В последнее время сектор здравоохранения стал местом для внедрения широкого спектра устройств и приложений IoT. Количество устройств интернета вещей с каждым днем увеличивается и помогает совершенствовать медицину во всем мире. Значительное распространение новой технологии увеличивает поверхность для всевозможных атак. Устройства IoT имеют дело с жизненно важной и частной информацией, такой как личные медицинские данные, и могут стать мишенью для злоумышленников. Отличие требований к безопасности IoT от требований к стандартным ИТ тормозит развитие и распространение новых технологий, а также делает процесс защиты интернет-устройств затруднительным. На данный момент продолжают существовать нерешенные проблемы и трудности в безопасном использовании IoMT.

Список источников

1. *IoT* в медицине: как интернет вещей совершенствует сферу здравоохранения. URL: https://tallinn.mhealth.events/ article/iot-v-meditsine-kak-internet-veshchey-sovershenstvuet-sferu-zdravoohraneniya-97414 (дата обращения: 05.04.2022).
2. *Интернет* медицинских вещей (IoMT): новые возможности для здравоохранения. URL: https://niioz.ru/upload/iblock/ 8e2/8e2ecff098ac4476c2142d8b7e450be7.pdf (дата обращения: 05.04.2022).
3. *Правительство* РФ утвердило дорожную карту развития 5G. URL: https://rostec.ru/upload/iblock/e01/e01f016e946493a3c9d18a5a25a52c8d.pdf (дата обращения: 06.04.2022).
4. *Новости* – правительство России. URL: http://government.ru/news/43542/ (дата обращения: 06.04.2022).
5. *DDoS* великий и ужасный. URL: https://habr.com/ru/company/ua-hosting/blog/233903/ (дата обращения: 06.04.2022).
6. *Анатомия* таргетированной атаки / Блог Касперского. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 08.04.2022).
7. *Healthcare* IoT security risks and what to do about them. URL: https://www.techtarget.com/iotagenda/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them (дата обращения: 07.04.2022).
8. *Islam SMR., Kwak D., Kabir M.H., Hossain M., Kwak K.S.* The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access. 2015;3:678–708.
9. *Frustaci M., Pace P., Aloi G., Fortino G.* Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet Things J. 2018;5(4):2483–2495.
10. *Jaigirdar F.T., Rudolph C., Bain C.* Acm. Can I Trust the Data I See? A Physician's Concern on Medical Data in IoT Health Architectures; Proceeding of Proceedings of the Australasian Computer Science Week Multiconference. 2019 Jan 29-31; 2019; Sydney, NSW, Australia. New York. Association for Computing Machinery (ACM). P. 1–10.
11. *Alsubaei F., Shiva S., Abuhussein A.* Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment; Proceeding of 2017 Ieee 42nd Conference on Local Computer Networks Workshops. 2017 Oct 9; 2017; Singapore, Singapore. IEEE. P. 112–120.
12. *Dogaru D.I., Dumitrache I.* Cyber security in healthcare networks; Proceeding of The 6th IEEE International Conference on E-Health and Bioengineering Conference (EHB). 2017 Jun 22–24; 2017; Sinaia, Romania. IEEE. P. 414–417.
13. *Электроника* НТБ: науч.-техн. журнал. Электроника НТБ – Повышение уровня безопасности граничных узлов интернета вещей с помощью микросхем ATECC608A компании MICROCHIP. URL: https://www.electronics.ru/journal/article/7695#:~:text=Используя%20недокументированное%20поведение%20или%20неполадки%2C,для%20изучения%20содержимого%20встроенной%20памяти (дата обращения: 10.04.2022).

14. *Как защитить* веб-приложение от атаки перебором Блог Касперского. URL: https://www.kaspersky.ru/blog/username-enumeration-attack/28049/https: //www.peerbits.com/blog/biggest-iot-security-challenges.html (дата обращения: 10.04.2022).
15. *Интернет* вещей, IoT, M2M (мировой рынок). URL: https://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT,_M2M_ (мировой_рынок) (дата обращения: 10.04.2022).
16. *Всемирная* хакерская конференция Black Hat собирает таланты / Блог Касперского. URL: https://www.kaspersky.ru/blog/black-hat-vzlamyvaem-vse-vokrug/1484/ (дата обращения: 11.04.2022).
17. *Palo* Alto Networks (PAN). URL: https://www.tadviser.ru/index.php/Компания: Palo_Alto_Networks_(PAN) (дата обращения: 08.04.2022).
18. *Системы* анализа трафика (NTA) – Сравнение и выбор. URL:https://www.anti-malware.ru/security/network-traffic-analysis (дата обращения: 24.05.2022).
19. *Функции* и различия межсетевых экранов / SberCloud. URL: https://sbercloud.ru/ru/warp/blog/raznovidnosti-mezhsetevyh-ekranov (дата обращения: 24.05.2022).
20. *В России* принят первый национальный стандарт интернета вещей – Cnews. URL: https://www.cnews.ru/news/top/2019-02-05_v_rossii_prinyat_pervyj_natsionalnyj_standart (дата обращения: 24.05.2022).
21. *Интернет* вещей / Технология микрочипов. URL: https://www.microchip.com/en-us/solutions/internet-of-things (дата обращения: 24.05.2022).
22. *Кривченко И.* Аппаратно защищенные микросхемы семейства Crypto-Authentica-tion: потенциальные применения ATECCx08A // Компоненты и технологии. 2015. № 11.
23. *Средства* экранирования электромагнитных полей – Студопедия. URL: https://studopedia.ru/18_70437_sredstva-ekranirovaniya-elektromagnitnih-poley.html (дата обращения: 28.05.2022).
24. *Trusted* computing - Difference between TPM, TEE and SE - Information Security Stack Exchange. URL: https://security.stackexchange.com/questions/122738/difference-between-tpm-tee-and-se#:~:text=TPM-это%20аппаратное%20обеспечение%2C%20специально%20созданное,изолирована%20от%20остальной%20части%20чипа (дата обращения: 28.05.2022).
25. *Новости.* URL: https://www.rst.gov.ru/ portal/gost/home/presscenter/news?portal:componentId=88beae40-0e16-414c-b176-d0ab5de82e16&navigationalstate=JBPNS_rO0ABXczAAZhY3Rpb24AAAABAA5zaW5nbGVOZXdzVmlldwACaWQAAAA-BAAQ3NTE5AAdfX0VPRl9f (дата обращения: 01.06.2022).
26. *Мартюшов М.В.* Стандартизация в сфере Интернета вещей: состояние, проблемы и перспективы // Инновации и инвестиции. 2019. № 6. Р. 340–343.
27. *Куприяновский В.П., Намиот Д.Е., Куприяновский П.В.* Стандартизация Умных городов, Интернета Вещей и Больших Данных. Соображения по практическому использованию в России // International Journal of Open Information Technologies. 2016. Vol. 4, № 2. P. 34-40.
28. *Internet* of Things (IoT) Trust Framework v2.5 – Internet Society. URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/#_edn2 (дата обращения: 05.06.2022).

References

1. *IoT* v medicine: kak internet veshchej sovershenstvuet sferu zdravoohraneniya. URL:https://tallinn.mhealth.events/article/iot-v-meditsine-kak-internet-veshchey-sovershenstvuet-sferu-zdravoohraneniya-97414 (access date: 05.04.2022). (In Russ.).
2. *Internet* medicinskih veshchej (IoMT): novye vozmozhnosti dlya zdravoohraneniya. URL: https://niioz.ru/upload/iblock/8e2/8e2ecff098ac4476c2142d8b7e450be7.pdf (access date: 05.04.2022). (In Russ.).
3. *Pravitel'stvo* RF utverdilo dorozhnuyu kartu razvitiya 5G. URL: https://rostec.ru/upload/iblock/e01/e01f016e946493a3c9d18a5a25a52c8d.pdf (access date: 06.04.2022). (In Russ.).
4. *Novosti*- pravitel'stvo Rossii. URL: http://government.ru/news/43542/ (access date: 06.04.2022).
5. *DDoS* velikij i uzhasnyj. URL: https://habr.com/ru/company/ua-hosting/blog/233903/ (access date: 06.04.2022). (In Russ.).

6. *Anatomiya* targetirovannoj ataki | Blog Kasperskogo. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (access date: 08.04.2022). (In Russ.).
7. *Healthcare* IoT security risks and what to do about them. URL: https://www.techtarget.com/iotagenda/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them (access date: 07.04.2022).
8. *Islam SMR, Kwak D., Kabir M.H., Hossain M., Kwak K.S.* The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access. 2015;(3):678–708.
9. *Frustaci M., Pace P., Aloi G., Fortino G.* Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet Things J. 2018;(5(4)):2483–2495.
10. *Jaigirdar F.T., Rudolph C., Bain C.* Acm. Can I Trust the Data I See? A Physician's Concern on Medical Data in IoT Health Architectures; Proceeding of Proceedings of the Australasian Computer Science Week Multiconference. 2019 Jan 29–31; Sydney, NSW, Australia. New York. Association for Computing Machinery (ACM); 2019. 1–10.
11. *Alsubaei F., Shiva S., Abuhussein A.* Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment; Proceeding of 2017 Ieee 42nd Conference on Local Computer Networks Workshops. 2017 Oct 9; 2017; Singapore, Singapore. IEEE; 2017. 112–120.
12. *Dogaru D.I., Dumitrache I.* Cyber security in healthcare networks; Proceeding of The 6th IEEE International Conference on E-Health and Bioengineering Conference (EHB). 2017 Jun 22–24; 2017; Sinaia, Romania. IEEE; 2017. 414–417.
13. *Elektronika* NTB – nauchno-tekhnicheskij zhurnal – Elektronika NTB – POVYSHENIE UROVNYA BEZOPASNOSTI GRANICHNYH UZLOV INTERNETA VESHCHEJ S POMOSHCH'YU MIKROSKHEM ATECC608A KOMPANII MICROCHIP. URL: https://www.electronics.ru/journal/article/7695#:~:text=Ispol'zuya%20nedokumentirovannoe%20povedenie%20ili%20nepoladki%2C,dlya%20izucheniya%20soderzhimogo%20vstroennoj%20pamyati (access date: 10.04.2022). (In Russ.).
14. *Kak zashchitit*' veb-prilozhenie ot ataki pereborom / Blog Kasperskogo. URL: https://www.kaspersky.ru/blog/username-enumeration-attack/28049/https: //www.peerbits. com/blog/biggest-iot-security-challenges.html (access date: 10.04.2022). (In Russ.).
15. *Internet* veshchej, IoT, M2M (mirovoj rsnok). URL: https://www.tadviser.ru/ index.php/Stat'ya:Internet_veshchej,_IoT,_M2M_(mirovoj_rynok) (access date: 10.04.2022). (In Russ.).
16. *Vsemirnaya* hakerskaya konferenciya Black Hat sobiraet talanty / Blog Kasperskogo. URL: https://www.kaspersky.ru/blog/black-hat-vzlamyvaem-vse-vokrug/1484/ (access date: 11.04.2022). (In Russ.).
17. *Palo* Alto Networks (PAN). URL: https://www.tadviser.ru/index.php/Компания:Palo_Alto_Networks_(PAN) (access date: 08.04.2022).
18. *Sistemy* analiza trafika (NTA) – Sravnenie i vybor. URL: https://www.anti-malware.ru/security/network-traffic-analysis (access date: 24.05.2022). (In Russ.).
19. *Funkcii* i razlichiya mezhsetevyh ekranov | SberCloud. URL: https://sbercloud.ru/ru/warp/blog/raznovidnosti-mezhsetevyh-ekranov (access date: 24.05.2022). (In Russ.).
20. *V Rossii* prinyat pervyj nacional'nyj standart interneta veshchej – CNews. URL: https://www.cnews.ru/news/top/2019-02-05_v_rossii_prinyat_pervyj_natsionalnyj_standart (access date: 24.05.2022). (In Russ.).
21. *Internet* veshchej / Tekhnologiya mikrochipov. URL:https://www.microchip.com/en-us/solutions/internet-of-things (access date: 24.05.2022). (In Russ.).
22. *Krivchenko I.* Apparatno zashchishchennye mikroskhemy semejstva Crypto-Authentica-tion: potencial'nye primeneniya ATESSx08A. Komponenty i tekhnologii. 2015;(11). (In Russ.).
23. *Sredstva* ekranirovaniya elektromagnitnyh polej – Studopediya. URL: https://studopedia.ru/18_70437_sredstva-ekranirovaniya-elektromagnitnih-poley.html (access date: 28.05.2022). (In Russ.).
24. *Trusted* computing – Difference between TPM, TEE and SE – Information Security Stack Exchange. URL: https://security. Stackexchange.com/questions/122738/ difference-between-tpm-tee-and-se#:~:text=TPM-eto%20apparatnoe %20obespechenie%2C%20special'no%20sozdannoe,izolirovana%20ot%20ostal'noj% 20chasti%20chipa (access date: 28.05.2022).

25. *Novosti.* URL: https://www.rst.gov.ru/portal/gost/home/presscenter/news?portal:componentId=88beae40-0e16-414c-b176-d0ab5de82e16&navigationalstate=JBPNS_rO0ABXczAAZhY3Rpb24AAAABAA5zaW5nbGVOZXdzVmlldwACaWQAAAABAAQ3NTE5AAdfX0VPRl9f (access date: 01.06.2022). (In Russ.).
26. *Martyushov M.V.* Standartizaciya v sfere Interneta veshchej: sostoyanie, problemy i perspektivy Innovacii i investicii. 2019;(6):340–343.
27. *Kupriyanovskij V.P., Namiot D.E., Kupriyanovskij P.V.* Standartizaciya Umnyh gorodov, Interneta Veshchej i Bol'shih Dannyh. Soobrazheniya po prakticheskomu ispol'zovaniyu v Rossii // International Journal of Open Information Technologies. 2016;(4:2):34–40. (In Russ.).
28. *Internet* of Things (IoT) Trust Framework v2.5 – Internet Society. URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/#_edn2 (access date: 05.06.2022).

Информация об авторах:

Е. Ю. Никитина – кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности и систем связи Пермского государственного национального исследовательского университета (614068, Россия, г. Пермь, ул. Букирева, 15), neyu@psu.ru, https://orcid.org/0000-0001-6639-9876, AuthorID 147895;

К. Л. Поторочина – студент кафедры информационной безопасности и систем связи Пермского государственного национального исследовательского университета (614068, Россия, г. Пермь, ул. Букирева, 15), kseniyapotorochina@gmail.com.

Information about the authors:

E. Yu. Nikitina – Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Information Security and Communication Systems, Perm State University (15, Bukireva street, Perm, Russia, 614068), neyu@psu.ru, https://orcid.org/0000-0001-6639-9876, AuthorID 147895;

K. L. Potorochina – Student, Department of Information Security and Communication Systems, Perm State University (15, Bukireva street, Perm, Russia, 614068), kseniyapotorochina@gmail.com.