DOI 10.37882/2223–2966.2022.10–2.27

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ «УМНЫЙ ГОРОД»

MODERN TECHNOLOGIES IN «SMART-CITY» SYSTEMS

Ahmed Talaat Tawfeeq Tharwat

Summary. This article is devoted to the problems of the development of the concept of smart cities in the Republic of Belarus, the Russian Federation. The main approaches to the definition of the concept of "smart city" are considered, the main characteristics of smart cities are highlighted. The concept of "safe city" is considered, the possible risks associated with the introduction of the concept of "safe city" are reflected. The main ways of ensuring the security of the information and communication system in smart cities are identified. The existing experience of intelligent technologies in smart cities around the world is given. The review of the main intelligent technologies in the field of Internet of Things (IoT), such as a cluster-based authentication process in a smart city, M2M communication technology is carried out. A review of existing smart home systems, such as Arduino1, ZigBee 3.0. protocol has been conducted and their main characteristics have been identified.

Keywords: "smart city", smart-cities, digital environment, "safe city", Internet of Things (IoT), a cluster-based authentication process, M2M communication technology, "smart home", Arduino1, ZigBee 3.0.

Таруат Ахмед Талат Тауфик
Белорусский национальный технический университет
ahmedtharwat6773@gmail.com

Аннотация. Настоящая статья посвящена проблемам развития концепции умных городов в Республики Беларусь, Российской Федерации. Рассмотрены основные подходы к определению понятия «умный город», выделены основные характеристики умных городов. Рассмотрено понятие «безопасный город», отражены возможные риски, связанные с внедрением концепции «безопасный город». Выявлены основные пути обеспечения безопасности информационно-коммуникативной системы в умных городах. Приводится существующий опыт внедрения интеллектуальных технологий в умных городах по всему миру. Проведен обзор основных интеллектуальных технологий в сфере интернет-вещей (IoT), таких как аутентификация пользователей в системах умных городов, основанная на кластерной связи, технология межплатформного программного обеспечения. Проведен обзор действующих систем умного дома, таких как Arduino1, протокола ZigBee 3.0. и выявлены их основные характеристики.

Ключевые слова: «умный город», smart-cities, цифровая среда, «безопасный город», интернет-вещей (IoT), аутентификация, основанная на кластерной связи, технология межплатформного программного обеспечения, «умный дом», Arduino1, ZigBee 3.0.

На современном этапе развития человечества актуальной является проблема создания «умных городов», разработка интеллектуальных технологий в процессе цифрового развития городов с целью улучшения качества жизни населения и эффективного удовлетворения нужд населения. Система «умный город» представляет собой сеть коммуникации, элементы которой взаимодействуют между собой.

Единого определения понятия «умный город» не существует. С точки зрения науки «умный город — безопасный, экологически защищенный и эффективный городской центр будущего с передовой инфраструктурой из сенсоров, электроники и сетей, которая стимулирует устойчивый экономический рост и высокое качество жизни». С точки зрения информационно-технологического аспекта, «в основе умного города находится интеллектуальный обмен информацией, протекающий между большим числом его различных подсистем». Городами с высокоразвитой инфраструктурой являются Амстердам, Стокгольм, Барселона, Сингапур. В России к умным городам относятся Москва, Санкт-Петербург, Казань, Екатеринбург, Самара, Волгоград, Таганрог. Проблема развития таких городов в данный момент заключается в развитии лишь отдельных систем (умный транспорт и т.д.), нехватке инвестиций, ЦОД (центров обработки данных), борьбе с COVID-19 [1].

В настоящее время актуальной является проблема о том, как осуществить активное внедрение концепции умного города в Беларуси. Ускоренному развитию и внедрению инноваций способствует континуальный рост населения.

Стоит учитывать тот факт, что в РБ внедрение smart-технологий осуществляется медленно, так как информатизация все еще не является приоритетной в комплексном городском развитии [2].

Приступая к исследованию вопроса о том, каким должен быть умный город, стоит отметить, что одним из первостепенных направлений инновационной и научно-технической деятельности на 2021–2025 в Республики Беларусь является концепция умного города в рамках программы «Цифровое развитие Беларуси». Взаимодействие внешних ИС и ИР, внешних сервисов, ЦОД, регулятора, координационного центра, администрации, населения, бизнес-сообщества, IoT-платформ

способствует эффективному функционированию цифровой платформы. В рамках программы одной из задач является повышение уровня комфорта и безопасности жителей с помощью smart-технологий, видеоаналитики, удаленного мониторинга и т.д. Разработка и апробация цифровой платформы осуществляется в первую очередь в Орше, Барановичах, Пинске, Новополоцке, Полоцке, Мозыре, Лиде, Борисове, Солигорске, Молодечно, Бобруйске.

Минск занимает 111-е место в рейтинге умных городов в индексе Cities in Motion бизнес-школы Наварры [3].

Таким образом концепция умного города характеризуется технологичностью, интеллектуализацией и концентрацией внимания на стиле жизни. В 2019 году был запущен пилотный региональный проект «Кричев-малый умный город», подразумевающий использование IT-технологий на предприятиях. В рамках программы «Безопасный город» в целях профилактики правонарушений в общественных местах установлены системы видеонаблюдения. Была внедрена АСДУ (автоматизированная система диспетчерского управления движением автобусов). Солнечные батареи и аккумуляторы установлены на газорегуляторных пунктах, система GPRS фиксирует показатели на компьютеры. На газопроводах используется дистанционный лазерный детектор утечек метана Sewerin RMLD [4].

К синонимам понятия «умный город» относятся «безопасный город», «цифровой город», «комфортный город». В вопросе обеспечения безопасности в «умном городе» существует так называемый «угрозный универсум». Все риски в данной среде условно можно разделить на умышленные и «остальные». Перечень возможных угроз в умных городах бесконечен, и ущерб от них неограничен. Невозможно предсказать и учесть все предстоящие риски, а значит невозможно обеспечить исчерпывающую безопасность в таких городах. Существует три стратегии реагирования на появление умышленных угроз: предотвращение с целью устранения источников угроз; отражение с целью прекращения воздействия угроз и устранения их последствий; минимизация последствий. Задачами на данном этапе исследования является использование результатов имитационного моделирования систем безопасности в разработке обучающих выборок для систем поддержки принятия решений на интеллектуальном уровне [5].

В Российской Федерации актуальным является развитие концепции «Безопасный город», направленной на прогнозирование, реагирование, мониторинг и предупреждение угроз, устранение их последствий. С целью реализации данной концепции необходимым является использование цифровых средств, обеспечивающих процессы поддержки принятия управленческих решений в режиме реального времени. К возможным угрозам относятся природные явления или процессы, которые могут привести к возникновению чрезвычайных ситуаций (ЧС); техногенные опасные ситуации, имеющие вредное физическое, химическое и механическое воздействия на окружающую среду; биолого-социальные ситуации, представляющие угрозу жизни и здоровью людей; конфликтные ситуации; ситуации, связанные с киберпреступностью и информационной войной и т.д. [6].

Немаловажным аспектом развития «Безопасного города» является информационная безопасность. К основным проблемам работы систем относятся проблемы в проектировании, эксплуатации, хранении, обработки и передачи данных. Также интернет-вирусы, угрозы со съемных носителей, email-угрозы, программы-вымогатели. Для борьбы с угрозами используются стандартизированные протоколы передачи данных в системах (протоколы IP, TCP/IP, UDP, FTP, DNS, HTTP, NTP, SSH); гомоморфное шифрование; защита данных зашифрованных пакетов в cloud-хранилищах; разделение сети умного города и всемирной паутины; автоматизация и управление чрезвычайно важных объектов инфраструктуры города; использование комплексных решений, а не заказной разработки IoT-вещей; встроенная защита в процессы производства, внедрение продукции OEM-производителями; тестирование программных средств [7].

Для обеспечения безопасности информационно-коммуникативной системы и разработки СППР используются следующие механизмы: а) идентификация и аутентификация; б) управление доступом; в) протоколирование и аудит; г) криптография; д) межсетевое экранирование. Адаптивная сетевая безопасность включает в себя: 1) технологию анализа безопасности или поиска уязвимостей (ручное или автоматическое устранение неполадок сети); 2) технологию обнаружения атак (с помощью анализа или журналов регистрации операционной системы и прикладного программного обеспечения, или сетевого трафика в реальном времени); 3) адаптивный компонент (серия тестов по обнаружению уязвимостей) 4) управляющий компонент. Наиболее популярными являются протоколы TCP/IP и т.д., позволяющие эффективно проверять защищенность корпоративной сети, работающей в данном сетевом окружении, независимо от того, какое программное обеспечение функционирует на более высоких уровнях [8].

В данный момент активно разрабатываются и внедряются интеллектуальные технологии и цифровые решения «умных городов» по всему миру.

С 1 января 2020 года в г. Москва повсеместна была установлена интеллектуальная система распознавания лиц, камеры с HD-качеством.

В рамках пилотного проекта «SmartAqkol» в Казахстане был проведен Wi-Fi общего доступа, составлена цифровая 3D-карта города, включающая в себя более 18-ти слоев на карте — инженерные системы и сети, камеры, освещение), установлено около 70 видеокамер.

В городе Сонгдо (Южная Корея) с помощью внедрения сенсоров в улицы, здания и дороги каждый объект подключен к сети; датчики отправляют данные в главный пункт управления для выполнения анализа о неисправностях, состоянии объектов, температуре и т.д. Сонгдо является ярким примером создания «умного города» с нуля [9].

Технологические аспекты современных городов подразумевают оптимизацию телекоммуникационной сети в густонаселенных городских районах, оценку технологий на основе блокчейна для приложений Интернета вещей (IoT), оптимизацию транспортных средств для распределения грузов, оценку качества жизни в устойчивых городах, анализ перспектив совместного энергетического сообщества в Европе, а также предложения о совместной беспроводной передаче энергии и информации в сценариях Интернета вещей [10].

Исследуя облачные вычисления в сфере интернета-вещей, необходимо упомянуть, что физическое расстояние между облаком и конечным пользователем достаточно большое, соответственно увеличиваются задержка передачи и время сигнала. Существует пограничный сервер, который может облегчить обработку и хранение данных другого сервера; сервер обслуживания для каждой службы (например, службы экстренной медицинской помощи); и центральный сервер для умного города. Каждый пользователь взаимодействует с пограничным сервером, который расположен в населенном пункте пользователя. Пользователь может получать обслуживание с любого сервера обслуживания через кластерную связь. Все пользователи сервера обслуживания будут зарегистрированы с помощью пограничных серверов.

При регистрации пользователя сначала оценивается “доверие” пользователя. Сначала необходимо определить уровни доверия (LT) и связанные с ними диапазоны значений. Когда пользователь выполняет регистрацию через direct trust, ему/ей присваивается значение “mid (M)” [0.41,0.50] как первоначальное значение доверия. Таким образом, когда пользователь выполняет регистрацию через direct trust, ему/ей присваивается значение “low (L)”. В результате он/она получает случайное значение в качестве начального доверительного значения. При использовании процесса аутентификации на основе кластера каждый сервер обслуживания получает номер, сгенерированный центральным сервером, и он уникален для каждого сервера обслуживания. Аналогично, каждый пограничный сервер получает номер, сгенерированный соответствующим сервером обслуживания, и каждому пользователю пограничного сервера присваивается номер, сгенерированный пограничным сервером. Эти номера называются номерами аутентификации, которые используются для генерации ключей и аутентификации для каждого идентификатора (пользователя, пограничного сервера и сервера служб).

В процессе аутентификации на основе кластера существует другой кластер, членами которого являются все серверы служб, а мастер кластера — центральный сервер или сервер аутентификации, подключенный к центральному серверу. Этот кластер используется для аутентификации сервера служб, когда требуется межсервисная связь. Например, служба server SSb хочет получить сервис от сервера service SSc. В этой ситуации SSc использует приватный ключ и отправляет зашифрованное сообщение на центральный сервер для аутентификации SSb. Затем центральный сервер отправит SSb сообщение с просьбой отправить его идентификатор и адрес. Затем SSb отправляет свой идентификатор и AT в виде зашифрованного текста, используя свой секретный ключ. Центральный сервер открывает его и проверяет подлинность SSB, если его AT находится на центральном сервере [11]

На данном этапе помимо интернет-вещей в разработке находится технология machine-to-machine (M2M) для межплатформного программного обеспечения. Данная технология предусматривает передачу данных как путем проводного, так и беспроводного соединения. Экосистема M2M состоит из провайдера устройства, интернет-провайдера, провайдера платформы, сервис-провайдера и пользователей услуг. На прикладном уровне используются такие протоколы как HTTP, MQTT, CoAP, AMQP, XMPP. К протоколам транспортного уровня относятся TCP, UDP. Сетевой уровень включает в себя протоколы IPV4, IPV6, IPSec, ICMP, 6LowPAN. Уровень передачи данных и физический уровень объединяют в себе протоколы ZigBee, BLE, Wi-Fi, LoRa, NFC, Cellular, Z Wave.

M2M технология использует низкоскоростные беспроводные персональные сети (LR-WPAN), например, ZigBee, internet engineering task force (IETF). Также беспроводные персональные сети с поддержкой IPv6 с низким энергопотреблением (6LoWPAN), протокол маршрутизации для сетей с низким энергопотреблени-

ем и потерями (RPL), протокол ограниченных приложений (CoAP), ISA100.11a и WirelessHART, M-BUS, беспроводная M-BUS, KNX, связь по линии электропередачи (PLC) и IPv4/IPv6. В персональной сети (PAN) / домашней сети (HAN) / локальной сети (LAN) / полевой сети (FAN) используются технологии беспроводной связи с низким энергопотреблением, такие как Wi-Fi, Bluetooth low energy (BLE), ZigBee и 6LoWPAN, Z-wave также могут использоваться для подключения узла шлюза связи между машинами к главному серверу. С помощью сети LPWAN (Sigfox и LoRa) передаются данные очень малого размера. IPv6-адресация может предоставить возможность охватить миллиарды устройств, которые могут быть подключены к интернет-протоколу (IP). CoAPis отвечает потребностям передачи гипертекста, реализует методы HTTP retrieve, post, post и delete, исключающие неправильное толкование при общении с клиентами, включает в себя безопасность транспортного уровня дейтаграмм (DTLS), обеспечивающую передачу данных Интернета вещей, а также безопасный обмен данными через транспортный уровень. Units per transaction (UPT), позволяет использовать меньший объем полосы пропускания, помогая поддерживать высокие скорости связи при одновременном использовании минимального объема полосы пропускания [12].

Одним из направлений сети умного города является система умного дома. Датчики системы Arduino1 позволяют определять движение в зоне 0–7 м. Для передачи данных и управления используется GSM-модуль связи. Однако данный модуль не определяет источники энергии небольшой мощности. Функция потокового сканирования позволяет сократить количество датчиков движения и записать отрезок спектра активных частот для поиска преступника. Основой разработки модуля датчика Arduino служит амплитудный детектор СВЧ-колебаний. «Если амплитуда принятого сигнала на VD1 диод достаточно велика, то выходное напряжение детектора откроет VT1 транзистор. Следовательно, возникает импульс высокого логического уровня длительностью приблизительно 10 мс на выходе элемента DD1.1, образующего с элементом DD1.2 простой генератор одиночного импульса (одновибратор). Он разрешит работу мультивибратора с элементами DD1.3, и DD1.4 на частоте приблизительно 1,5 кГц. Пакет импульсов, усиленных по мощности VT2 и VT3 транзисторами, будет воспроизведен пьезоэлектрическим капсюлем HA1 (или динамической головкой вместо капсюля) как громкий щелчок. Так прибор отреагирует на выход сотового телефона в эфир даже на очень короткое время» [13].

Для реализации проекта «Умный дом для пожилых людей» используется ZigBee 3.0. Он включен в спецификацию Zigbee Pro 2017 (R22). Данный протокол имеет ряд преимуществ: ячеистая структура, обеспечивающая надежность для человека, позволяющая не поддаваться влиянию других технологий передачи, низкое энергопотребление благодаря «спящему режиму».

В системе используются две камеры, записывающие видеоданные в реальном времени. При условии, что запись происходит 12 часов в сутки, видео записывается в разрешении 1920x1080, 30 кадров в секунду, битрейт такого видеопотока составляет в среднем 3 Мбит/с. Средняя нагрузка ввода-вывода для каждого видеопотока составляет в среднем 60 операций ввода-вывода при условии, что размер блока составляет не менее 8 КБ. Таким образом, система хранения данных должна обрабатывать архивирование потока данных 3*2/70% = 8,6 Мбит/с, с размером блока 8 КБ и выше, и 60*2/70% = 171,4 операций ввода-вывода. Для таких требований достаточно 2 жестких дисков SATA в RAID-1 (зеркальных). Для хранения информации в течение как минимум одной недели, 7 (дней) * 12 (часов) * 3600 (секунд) * 2 (камеры) * 3 (Мбит/с)/8 (бит) = 226 800 МБ = 226,8 ГБ. В настоящее время производство жестких дисков малой емкости практически остановлено. Для улучшения и повышения надежности, компактности и производительности системы предлагается использовать 2 твердотельных 2,5-дюймовых твердотельных накопителя емкостью 480 ГБ каждый. Это позволит хранить архивные данные либо в течение двух недель, либо в течение недели с непрерывной записью. Ограничение на количество перезаписей ячеек твердотельного накопителя с памятью TLC составляет от 1500 до 3000 циклов, что в среднем позволит использовать этот тип SSD в системе не менее 1500*480(ГБ)/226,8(ГБ)*7/365 = 66,9 лет. Предлагается использовать накопители SATA 3. Типичная пропускная способность этих накопителей составляет 450 Мбит/с последовательного чтения и 350 Мбит/с последовательной записи при размере блока 8 КБ, что позволит организовать дополнительные сервисы, такие как удаленный просмотр записей и синхронизация с удаленным облачным хранилищем, не влияя на производительность основного сервиса. Для реализации функциональности ZigBee используется микроконтроллер Texas Instrument CC2652R, который поддерживает протоколы Zigbee 3.0, Bluetooth mesh, Bluetooth 5.1 и другие. Также модули разработки с припаянным чипом и его вспомогательной схемой, а также антенным разъемом.

Для обеспечения связи между устройствами в локальной сети, а также для обеспечения доступа в Интернет используется маршрутизатор Mikrotik hEX Po E. Что касается интерфейсов подключения к Интернету, то маршрутизатор имеет порт Gigabit Ethernet, порт SFP для установки оптических модулей и порт USB, поддерживающий USB-модемы. Операционная система это-

го маршрутизатора позволяет настроить VPN-сервер на маршрутизаторе для входящих VPN-подключений.

Технология «умный дом» для пожилых людей в целом позволяет автоматизировать рутинные процессы [14].

Исходя из вышесказанного, создание цифрового пространства, строительство «умных городов», разработка и внедрение smart-технологий способствует технологическому, социально-экономическому развитию городов, улучшению качества и уровня жизни населения, появлению новых рабочих мест. Приоритетной задачей развития «цифровых городов» является эффективное управление интеллектуальными технологиями, повышение безопасности и разработка систем поддержки принятия решений с целью минимизации возможных рисков. Стоит учитывать, что реализация и развитие концепции «умного города» является отсроченным во времени процессом.

ЛИТЕРАТУРА

1. Алферов, О.Л. Концепция «Умный город» — проект интеллектуальной инфраструктуры среды обитания людей / О.Л. Алферов // Соц. и гуманитар. знания. Отечеств. и зарубеж. лит. Сер. 4, Государство и право. — 2021. — № 1. — С. 140–150.
2. Инструкция для градоначальников, или дорожная карта умного города / [Кошаровский Н.] // Веснік сувязі: научно-производственный журнал для специалистов в области связи и информационных технологий / учредители: Министерство связи и информатизации Республики Беларусь, Белорусский профессиональный союз работников связи. — 2019. — № 6. — С. 24—30.
3. Каким должен быть умный город и как его построить? / С.В. Кругликов, С.В. Потетенко // Веснік сувязі: научно-производственный журнал для специалистов в области связи и информационных технологий / учредители: Министерство связи и информатизации Республики Беларусь, Белорусский профессиональный союз работников связи. — 2021. — № 3. — С. 16—21.
4. Кричев: ИТ-подъем с переворотом / [Д.В. Бочков] // Веснік сувязі: научно-производственный журнал для специалистов в области связи и информационных технологий / учредители: Министерство связи и информатизации Республики Беларусь, Белорусский профессиональный союз работников связи. — 2019. — № 3. — С. 20—27.
5. Грищенко, Л.Л. «Умные» технологии при обеспечении безопасности в «умном городе» / Л.Л. Грищенко, С.М. Ревин, Ю.В. Коротаев // Муницип. акад. — 2020. — № 2. — С. 186–191.
6. Зацаринный, А.А. Целеполагание в аппаратно-программном комплексе «Безопасный город»: задачи и реалии / А.А. Зацаринный, А.П. Сучков // Технологии гражд. безопасности. — 2020. — Т. 17, № 3. — С. 69–74.
7. Щербонос, Е.Б. Аспекты проработки системы безопасности умного города / Е.Б. Щербонос, А.Б. Шукенбаев, Н.Ш. Шукенбаева // REDS: Телекоммуникационные устройства и системы. — 2022. — Т. 12, № 1. — С. 51–55.
8. Яблочкин, Н.С. Разработка системы поддержки принятия решений для повышения безопасности информационно- коммуникационных систем / Н.С. Яблочкин // Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств: материалы X Всероссийской науч.-техн. конф., Самара, 21–22 марта 2017 г. / Самарский гос. техн. ун-т; отв. ред. А.И. Никонов. — Самара, 2017. — С. 153–156.
9. Абламейко, С. Использование систем искусственного интеллекта при обеспечении общественной безопасности в «Умном городе»: юридические аспекты / С. Абламейко, Н.В. Шакель, Р.П. Богуш // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. — 2021. — № 5. — С. 84–92.
10. Advanced technologies in Smart Cities [Electronic resource]: Energies 15(13). — Mode of access: https://www.researchgate.net/publication/361621028_Advanced_Technologies_in_Smart_Cities. — Date of access: 03.09.2022.
11. Cluster-Based Authentication Process in a Smart City [Electronic resource]: Hindawi. — Security and Communication Networks. — Mode of access: https://www.hindawi.com/journals/scn/2022/5186376/. — Date of access: 03.09.2022.
12. Machine to machine communication enabled internet of things: a review [Electronic resource]: International Journal of Reconfigurable and Embedded Systems (IJRES) 11(2). — Mode of access: https://www.researchgate.net/publication/361672707_Machine_to_machine_communication_enabled_internet_of_things_a_review. — Date of access: 03.09.2022.
13. Жданов, Н.В. Применение датчиков перемещения источников СВЧ-сигналов в системах «умного» дома и города / Н.В. Жданов // Актуальные проблемы радио- и кинотехнологий: материалы V Международной научно-технической конференции, посвященной 140-летию со дня рождения выдающегося физика и создателя первой русской усилительной радиолампы Н.Д. Папалекси. В 2 частях., 2021 / Санкт-Петербургский гос. ин-т кино и телевидения. — Санкт-Петербург, 2012. — С. 60–63.
14. Stepanov M.S. The using of ZigBee protocol to organize the "smart home" system for aged people / M.S. Stepanov, L.S. Poskotin, D.V. Shishkin, Timur Turgut, A.R. Muzata // T-COMM. — 2021. — Vol. 15. — № 10. — P. 64–70.

Журнал «Современная наука: актуальные проблемы теории и практики»