УДК 004.056:332.14

Д. А. Массеров[1], Д. Д. Массеров[1]

[1]*Мордовский государственный университет им. Н.П. Огарёва, г. Саранск, Россия*

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ УМНОГО ГОРОДА В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ ГОРОДСКОЙ СРЕДЫ

Аннотация. Умные города развиваются во всем мире, и правительства многих стран инвестировали и инвестируют большие суммы денег в развитие умных городов. Это развитие не является результатом одномоментного решения, скорее, умные города развивались в течение определенного периода времени, непосредственно от более ранних стадий: от цифрового города к зеленому городу, устойчивому городу, экогороду и т.д. Современная эпоха ознаменовалась появлением высокоскоростной беспроводной связи 5G, быстрых многоядерных серверов на базе GPU, больших данных, облачных вычислений, искусственного интеллекта и аналитики данных. Многие из этих новых технологий способствуют развитию и реализации умных городов. В этом исследовании представляется общий обзор безопасности для умных городов и дается более глубокое понимание того, что мы подразумеваем под обеспечением безопасности умных городов. Авторы обсуждают применимость существующих методов безопасности аутентификации, контроля доступа, шифрования, межсетевых экранов и их пригодность для защиты умного города.

Ключевые слова: умный город, информационно-коммуникационные технологии, обеспечение безопасности, интеллектуальный операционный центр, искусственный интеллект.

D. A. Masserov[1], D. D. Masserov[1]

[1]*Ogarev Mordovia State University, Saransk, Russia*

ENSURING THE CYBER SECURITY OF THE SMART CITY IN THE PROCESS OF DIGITALISATION OF THE URBAN ENVIRONMENT

Abstract. Smart cities are developing all over the world, and many governments have invested and are investing large sums of money in the development of smart cities. This development is not the result of an overnight solution, rather, smart cities have developed over a period of time, directly from earlier stages: from the digital city to the green city, the sustainable city, the eco-city, etc. The modern era has been marked by high-speed 5G wireless, fast GPU-based multi-core servers, big data, cloud computing, artificial intelligence and data analytics. Many of these new technologies are contributing to the development and implementation of smart cities. This study presents a general overview of security for smart cities and provides a deeper understanding of what we mean by security for smart cities. The authors discusses the applicability of existing security methods of authentication, access control, encryption, firewalls and their suitability for smart city security.

Keywords: smart city, information and communication technology, security assurance, intelligent operations center, artificial intelligence.

Введение. Бесспорно утверждение о том, что человечество движется к эре умных городов. Страны по всему миру внедряют умные города, например, в Великобритании, Китае, России и Сингапуре. Умные города – это область, в которой пересекаются информационно-коммуникационные технологии (ИКТ), науки о городах, экологические науки и социальные науки [1]. Эта междисциплинарная область, хотя и сложна в своем составе, но в то же время представляет интерес, так как она изменит жизнь миллионов жителей городов. В тоже время в умных городах появятся угрозы в различных формах, будь то данные, доступ, контроль, услуги, подключение и т.д. Предотвращение угроз всегда является требованием и проблемой для умных городов. Существует также недостаток внимания к кибербезопасности умных городов [2, 3].

Аналогия человека и умного города. Между людьми и городами есть некоторые сходства. Люди живут и работают в городах. Жизнеспособность города связана с его деловой активностью и деятельностью горожан. Если посмотреть, из чего состоит человек, то это мозг, органы чувств и тело. Мозг человека – это интеллектуальный центр, где происходят рассуждения и решения, где обрабатывается и хранится информация. Наши органы чувств

(глаза, уши, нос, кожа и т.д.) позволяют нам собирать информацию и отправлять ее в мозг для обработки. Наконец, человеческое тело обеспечивает все остальные функции, необходимые для поддержания жизнедеятельности. Аналогичным образом, мы можем рассматривать умный город, имеющий подобную человеческому телу форму строения.

Три блока умного города выглядят следующим образом:

1. Мозг – центр управления и принятия решений умного города. Это центральный командный пункт, где анализируются наблюдения, отслеживаются и выявляются аномалии и запускаются соответствующие действия.

2. Органы чувств – входы в системы умного города включают: зрение, звук, показания датчиков и т.д. Зрение принимает форму камер, расположенных в определенных местах. Микрофоны могут использоваться для записи разговоров на местах преступлений и в других случаях. Датчики расхода воды могут использоваться для обнаружения наводнений, а умные счетчики – для учета использования электроэнергии и воды.

3. Тело – тело системы умного города относится как к инфраструктуре, так и к ИКТ-платформам. Под инфраструктурой понимаются здания, дороги, водостоки и т.д. ИКТ представляет собой три основные составляющие: связь, данные и искусственный интеллект (ИИ).

Архитектура системы. С точки зрения ИКТ, умный город имеет четыре основных уровня: датчики или конечные точки, края (шлюзы), платформа (данные, ИИ, управление связью) и их применение.

На более высоком уровне абстракции умный город является аналогом живого существа (ведь без Интернета вещей (IoT) не обойтись) [4]. Компания Alibaba рассматривает умный город как «мозг города» [5], где находится основная часть ИИ, для управления его деятельностью и контролировать все объекты (внутренние и внешние).

Ожидается, что для умного города IoT станет неотъемлемой частью всей городской платформы [6]. «Входами» системы умного города будут датчики, будь то видеокамеры, микрофоны, датчики температуры, водомеры и т.д. Датчики – это устройства, которые взаимодействуют с физическим миром, собирают данные и передают их обратно в точки сбора по различным проводным (оптоволокно, провода и т.д.) или беспроводным (Wi-Fi, Bluetooth, узкополосный IoT и т.д.) каналам связи [7]. Точки сбора обычно называются шлюзами. Датчики обычно используют как телеметрический транспорт с очередью сообщений или как протокол обмена сообщениями с ограниченным прикладным протоколом для отправки данных по беспроводным каналам связи на шлюз. Сообщения обычно представляют собой пакеты небольшого размера и имеют малый вес для экономии энергии, потребляемой датчиками при передаче этих данных. Отдельные секции умного города, расположенные на облачной платформе, могут взаимодействовать со шлюзом через стандартный REST API [8].

Как показано на рисунке, системная архитектура умного города включает четыре горизонтальных и два вертикальных слоя, а их приложение располагаются сверху [3]. Основными четырьмя горизонтальными слоями являются слои устройств и датчиков, за которыми следуют слои подключения, управления IoT и данных ИИ. Первый уровень касается датчиков и других устройств (камер и т.д.), которые обеспечивают входные данные для системы умного города. Данные датчиков затем подключаются к точкам сбора (шлюзам) через слой подключения. Уровень управления соединениями IoT, расположенный на границе, обеспечивает сбор различных данных датчиков, отправленных по различным каналам и различным протоколам, обеспечивая совместимость разнородных устройств и соединений. Наконец, уровень данных ИИ обеспечивает обработку данных и аналитику.

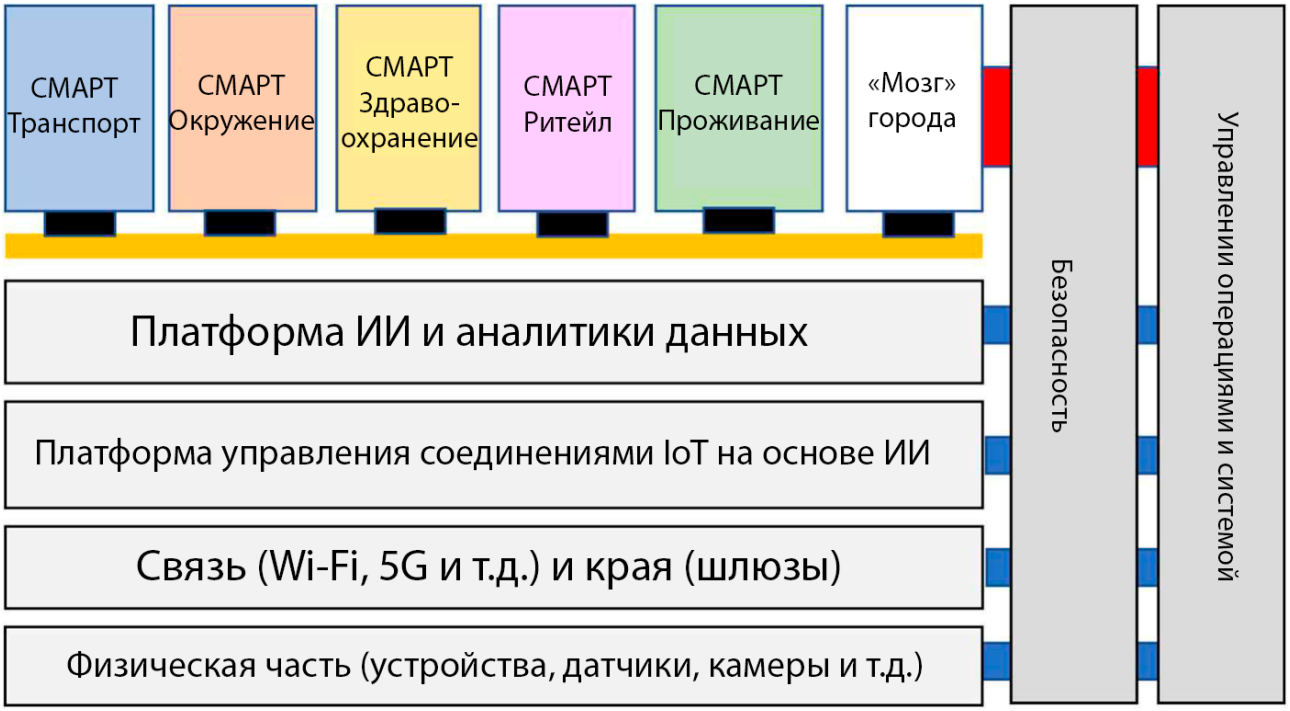

Рисунок. Предполагаемая архитектура системы умного города, в которой безопасность и управление городом охватывают все уровни [3]

На верхнем уровне различные части умного города будут по-разному использовать данные и идеи, а также инициировать соответствующие действия (например, вызов полиции на место преступления для обеспечения безопасности умного города). Технологии искусственного интеллекта могут быть использованы для анализа данных и прогнозирования правильных результатов (например, распознавание лиц для идентификации преступника, находящегося под следствием). Таким образом, уровни данных и обработки присутствуют в каждом разделе умного города. В идеале можно создать один общий уровень платформы данных и ИИ для обслуживания всех возможных разделов умного города, но в реальности этого трудно достичь, учитывая тот факт, что существуют различные административные домены управления (когда транспортный уровень может не разрешить, например, уровню здравоохранения доступ и обмен данными), а централизованный уровень платформы может привести к узкому месту во время сбоев [9].

Вертикальные уровни архитектуры касаются безопасности, эксплуатации и управления контролем. Поскольку некоторые фрагменты умного города разрабатываются для частных лиц, например, для частных домовладений или частных бизнес-зданий, они считаются самостоятельными системами, практически не требующими взаимодействия с другими разделами умного города. Однако некоторые из них (например, умный транспорт, здравоохранение и окружающая среда) обслуживают население и создаются правительством, следовательно, нуждаются в управлении операциями и системой, взаимосвязи и совместимости между собой, комплексной защитой. Например, интеллектуальный операционный центр (IOC) [10] или центр командования и управления – это структура, которая позволяет правительству централизованно управлять различными подсистемами умного города (транспорт, окружающая среда, общественная безопасность и т.д.). Такая конструкция также позволит соединять и взаимодействовать различным правительственным частям умного города. Другой пример, в случае преступления, произошедшего на дорожной развязке, полиции потребуется доступ к таким «приложениям», как «умный транспорт», «умный перекресток» и «умные фонарные столбы», чтобы собрать все данные, связанные с преступлением [5]. Она также должна иметь возможность управлять камерами, расположенными вблизи или на месте преступления.

Таким образом, для государственных отделов умного города необходимо, чтобы эти отделы взаимодействовали друг с другом и обеспечивали обмен соответствующими данными.

Система умного города и все ее части должны быть защищены, а средства безопасности должны быть встроены в каждый уровень платформы умного города, из конца в конец, чтобы обеспечить целостность, предотвратить вторжение и злонамеренные атаки. Это объясняет, почему безопасность охватывает все горизонтальные слои. Устройства должны быть защищены, чтобы обеспечить их защиту от взлома. Данные датчиков, передаваемые по защищенному проводному или беспроводному каналу связи, должны быть зашифрованы. Доступ к устройствам должен предоставляться только авторизованному персоналу, как локально, так и удаленно. Данные должны надежно храниться в распределенном хранилище. Доступ к данным должен быть предоставлен только в авторизованном виде. Данные, связанные с каждым аспектом умного города, могут рассматриваться как отдельная сущность, надежно хранящаяся в частном или публичном облаке. Они могут быть общими или храниться в секрете. Многие страны разработали политику, связанную с управлением данными, и в зависимости от места хранения данных власти имеют юрисдикцию над данными и их неправильным использованием.

Рассмотрение проблемы безопасности. Безопасность умных городов относится к более широкой проблеме, и ее не следует рассматривать изолированно. Под изолированностью мы подразумеваем разработку решений безопасности для конкретных сегментов умного города, таких как «умный транспорт», «умное здравоохранение», «умная окружающая среда», «умная жизнь» и т. д. [6]. Следует рассмотреть и понять, каковы основополагающие факторы, которые будут способствовать безопасной работе умного города.

В сущности, необходимо обеспечить безопасность «мозга», «тела» и «органов чувств» умного города в дополнение к обеспечению безопасности каждой части умного города. Это требует комплексного и полного решения вопроса безопасности для защиты умного города. Это не только защитит город от злоумышленников за его пределами, но и защитит его внутреннее пространство – инфраструктуру, связь и сервисы.

Что следует защищать? При разработке решений по обеспечению безопасности для «умных» городов необходимо изучить: что нужно защищать, каковы конечные цели злоумышленников и типы атак. Чтобы понять, что нужно защищать в умном городе, необходимо рассмотреть его активы. Активы умного города – это его ресурсы, люди и услуги. Под ресурсами подразумеваются финансовые активы – деньги, товары (золото и т.д.), другие активы (акции и т.д.), инфраструктуру – телекоммуникации, интернет, центры обработки данных, офисы, дома и т. д. и предметы первой необходимости – воду, электричество, продукты питания, медицинские препараты и т. д.

Люди формируют кадровый резерв и рабочую силу города, они поддерживают бизнес–операции и двигают экономику города. Наконец, под городскими службами имеется в виду здравоохранение, водо- и электроснабжение, санитарные и канализационные службы, полицию, скорую помощь и т.д.

Все это – важные активы для умного города. У злоумышленников может возникнуть соблазн украсть такие активы. Однако не все из них соблазняются на кражу. Другие конечные цели включают злоумышленников, которые больше заинтересованы в создании хаоса путем нарушения или прекращения работы служб. Кроме того, большинство атак являются злонамеренными, и они, как правило, делятся на следующие две категории: 1) атаки, нарушающие жизнь жителей города и 2) атаки, нарушающие бизнес–операции в городе. Обе эти конечные цели травмируют жизнь и экономическое благосостояние города.

Кроме того, тип атак может определяться местом. Локальные атаки – физическое присутствие на месте или поблизости от места атаки. Именно здесь командные центры с видеонаблюдением помогают захватить нападающих и идентифицировать их. Удаленные атаки – находятся вдали от места проведения атаки, но используют подключение к Интернету для получения контроля над компьютерными системами, чтобы нарушить работу городских

служб. Такие злоумышленники обычно проживают за пределами города, и их необходимо выслеживать по сетевым адресам интернет-протокола (IP) [11].

Следует определить, какие ресурсы и услуги являются более критичными по сравнению с другими. Критически важные ресурсы и услуги – это те, которые необходимы для повседневной нормальной работы города, которые поддерживают жизнь граждан и ведение бизнеса. Исходя из этого, авторами были определены следующие шесть наиболее критических ресурсов и служб, которые необходимо защитить. Ресурсы: вода, электроэнергия, связь, данные, IOC («мозг» умного города) и финансовые активы. Службы: обеспечение правопорядка, здравоохранение (медицинские услуги), пожарно-спасательные службы, транспортные услуги, услуги ЖКХ .

Защита водоснабжения. Важнейшим элементом для выживания человека является вода, поэтому она имеет наивысший приоритет. Город не может существовать без наличия воды, как для личного потребления, так и для бизнеса (в ресторанах и т.д.). Нападения на источник воды и водный транспорт могут нарушить водоснабжение. Опять же, такие атаки могут быть совершены физически злоумышленниками на месте, отключением насосов и разрывом труб для транспортировки воды в цепи поставок. Нападения, совершаемые на месте, обычно предотвращаются присутствием охранников и видеонаблюдением.

Однако кибератаки, которые осуществляются злоумышленниками, находящимися на удалении (за пределами города), бывает трудно поймать. Через киберпространство они получают контроль над системой управления водоснабжением, чтобы отключить или сократить подачу воды в город. Наблюдательные программы должны присутствовать 24 часа в сутки 7 дней в неделю, чтобы постоянно отслеживать аномалии в системе водоснабжения, а удаленный доступ к системе управления водоснабжением должен быть ограничен или даже запрещен.

Защита электроэнергии. Большинство современных приложений для «умных городов» работают от электричества. Без электроэнергии большинство систем и предприятий умного города перестанут работать, и город останется в темноте. Следовательно, обеспечение безопасности источника электроэнергии и ее доставки имеет решающее значение для умных городов. Выработка электроэнергии может быть остановлена путем физического разрушения объекта или прерывания процесса выработки электроэнергии. Исходя из этого, требуется строгая безопасность объекта, чтобы гарантировать, что производство электроэнергии не будет прервано, и что существует резервное питание во время перебоев. Атаки на любой из таких компонентов, как линии электропередачи, трансформаторы, реле, переключатели и электростанции, могут прервать подачу электроэнергии, что приведет к сбоям в работе всех приложений умного города. Важно разработать комплексную стратегию и структуру для обеспечения безопасности как производства электроэнергии, так и ее доставки в город.

Кроме того, поскольку система энергетической инфраструктуры объединена в сеть, существует вероятность цепочки сбоев, что многократно усиливает воздействие одной локализованной атаки. Это может привести к массовым отключениям электроэнергии в нескольких городах. Умные города должны обладать встроенной надежностью и возможностью изоляции для противодействия таким атакам.

Обеспечение безопасности средств связи. Инфраструктура умного города требует подключения датчиков, камер, центров обработки данных и т. д. Подключение может осуществляться через проводную и беспроводную сетевую инфраструктуру. Также можно рассматривать защиту средств связи как обеспечение безопасности IoT. Безопасность IoT включает в себя безопасность устройств, данных и соединений. Безопасность устройств включает в себя аппаратную безопасность (защиту от взлома), контроль доступа и аутентификации. Безопасность данных достигается шифрованием, а безопасность соединения – использованием легких защищенных сквозных транспортных протоколов.

Существующие телекоммуникационные сети, используемые для поддержки фиксированных широкополосных и мобильных сотовых сетей, достаточно надежно защищены, и случаи перехвата соединения единичны. Однако для умного города требования к безопасно-

сти должны быть выше, поскольку люди ожидают, что умный город будет более защищенным, чем обычные города.

1. Безопасность Wi-Fi. Защита беспроводных сетей требует защиты беспроводного канала. Для этого необходим защищенный протокол управления доступом к среде (MAC), где доступ к каналу будет контролироваться. В Wi-Fi защищенный доступ Wi-Fi (WPA) был разработан Wi-Fi Alliance для обеспечения более сложных возможностей шифрования данных и лучшей аутентификации пользователей по сравнению с проводным эквивалентом конфиденциальности (WEP), который был первоначальным стандартом безопасности Wi-Fi.

2. Безопасность Bluetooth. Bluetooth [12] предлагает несколько режимов безопасности: 1, 2, 3, 4, и производители устройств определяют, какой режим включить в гаджет с поддержкой Bluetooth. Почти во всех случаях пользователи Bluetooth могут создавать «доверенные устройства», которые могут обмениваться данными, не спрашивая разрешения. Когда любое другое устройство пытается установить соединение с гаджетом пользователя, пользователь должен решить, разрешить ли ему это. Безопасность на уровне сервиса и безопасность на уровне устройства работают вместе, чтобы защитить устройства Bluetooth от несанкционированной передачи данных. Методы безопасности включают процедуры авторизации и идентификации, которые ограничивают использование услуг Bluetooth зарегистрированным пользователем и требуют от пользователей осознанного решения при открытии файла или принятии передачи данных. Пока эти меры включены на телефоне пользователя или других устройствах, несанкционированный доступ маловероятен. Пользователь также может просто переключить свой режим Bluetooth на «необнаруживаемый» и, таким образом, полностью избежать соединения с другими небезопасными устройствами Bluetooth.

3. Безопасность LORAWAN. Дизайн безопасности LoRaWAN [13] придерживается самых современных принципов: использование стандартных, хорошо проверенных алгоритмов и сквозная безопасность. Безопасность сети LoRaWAN включает в себя: (a) взаимную аутентификацию, (b) защиту целостности и (c) конфиденциальность. Взаимная аутентификация устанавливается между конечным устройством LoRaWAN и сетью LoRaWAN как часть процедуры присоединения к сети. Это гарантирует, что только подлинные и авторизованные устройства будут подключены к подлинным и аутентичным сетям. MAC–адреса LoRaWAN и сообщения приложений аутентифицированы по происхождению, защищены от нарушения целостности, защищены от повторного воспроизведения и зашифрованы. Эта защита в сочетании с взаимной аутентификацией гарантирует, что сетевой трафик не был изменен, исходит от законного устройства, не понятен подслушивающим лицам и не был перехвачен и воспроизведен мошенниками. Безопасность LoRaWAN также реализует сквозное шифрование полезной нагрузки приложений, обменивающихся между конечными устройствами и серверами приложений. В системе безопасности LoRaWAN используется криптографический примитив расширенного стандарта шифрования (AES) в сочетании с несколькими режимами работы: CMAC2 для защиты целостности и CTR3 для шифрования. Каждое устройство LoRaWAN персонализируется с помощью уникального 128–битного ключа AES (называемого AppKey) и глобально уникального идентификатора (DevEUI на основе EUI–64), оба из которых используются в процессе аутентификации устройства.

4. Безопасность SIGFox. SIGFox [14] – это маломощное недорогое решение для подключения датчиков и устройств. Радиосвязь между базовыми станциями и облаком SIGFox, а также само облако SIGFox защищены с помощью аутентификации на основе подписи и виртуальной частной сети (VPN). Пользователи подключаются к облаку SIGFox с помощью защищенных интерфейсов протокола передачи гипертекста (HTTPS). SIGFox имеет встроенный брандмауэр, который запрещает доступ в Интернет устройствам SIGFox без прохождения через основную сеть SIGFox, и данные защищены как в пути, так и в состоянии покоя. Безопасность данных в движении достигается за счет аутентификации сообщений и предотвращения повторного воспроизведения. Благодаря использованию маркера сообщения и ключа аутентификации, проверка маркера гарантирует аутентификацию отправителя и целостность сообщения. Для обеспечения безопасности данных в состоянии покоя базовые

станции и опорная сеть SIGFox используют модуль доверенной платформы, также известный как ISO/IEC 11889, для защиты оборудования с помощью встроенных криптографических ключей.

5. Безопасность долгосрочной эволюции (LTE). LTE – это ключевая технология сотовой связи 4G, которая сегодня используется во всем мире для поддержки широкополосной мобильной сотовой связи. Что касается безопасности LTE [15], который охватывает: (a) безопасность аппаратного обеспечения, (b) криптографию, (c) безопасность воздушного интерфейса, (d) безопасность E–UTRAN, (e) безопасность транзита и (d) безопасность основной сети. Компоненты инфраструктуры LTE (например, развитый узел B, организация управления мобильностью, обслуживающий шлюз) могут использовать аппаратное, микропрограммное и программное обеспечение, что делает их восприимчивыми к общеизвестным дефектам программного обеспечения. Защита проводных сетей также требует обеспечения безопасности проводного соединения. Большинство проводных соединений осуществляется через Ethernet, по коаксиальным кабелям или оптоволокну. Ничто не мешает кому-то прослушивать проводное соединение, чтобы посмотреть на текущие осциллограммы и попытаться извлечь данные, но, если сигналы зашифрованы, извлечение данных затруднено.

6. Безопасность протокола. В дополнение к «безопасности соединения», существует также необходимость в безопасности, встроенной в протокол, т.е. «безопасность протокола». Доступ к Интернету и предоставление услуг являются ключевыми для многих домашних и бизнес-пользователей. Нарушение предоставления интернет-услуг может привести к остановке многих бизнес-операций и т.д.

Защита данных. Большинство сегментов умного города будут собирать, обрабатывать и анализировать данные, чтобы получить рациональные выводы и использовать их для создания осмысленных служб и услуг. Например, «умные» транспортные приложения будут собирать данные о транспортных средствах, водителях, дорожном движении и пассажирах, а «умные» медицинские приложения будут собирать данные о пациентах и врачах. Независимо от уровней умного города, в рамках платформы умного города будут генерироваться данные, которые должны быть защищены как в содержании, так и в хранении. Такие данные могут быть защищены несколькими способами [11]:

(a) Контроль доступа – запрет несанкционированного доступа к данным;

(b) Шифрование – защита содержимого;

(c) Аутентификация – проверка подлинности источника;

(d) Подписи – подтверждают достоверность данных;

(e) Конфиденциальность – отделить данные от идентификации и местоположения пользователя.

Обеспечение безопасности «мозга» умного города. Система умного города должна быть защищена и доступ к ней должен иметь только уполномоченный персонал. Защита доступа к устройствам, сетям и платформам имеет решающее значение для обеспечения безопасности умных городов. Многие города по всему миру используют концепцию централизованного центра управления и контроля умного города.

Компания Huawei, например, создала IOC – интеллектуальный операционный центр [10], выполняющий функции мониторинга, контроля и реагирования в умном городе, поддерживаемый захватом изображений в режиме реального времени, прямыми видеотрансляциями, картами с информацией о состоянии дорог, передвижении людей и т.д.

Вопросы безопасности, связанные с IOC, по мнению авторов, включают следующее:

• Проблема удаленного взлома: людей, имеющих права удаленного доступа к IOC, должно быть не более нескольких, чтобы можно было определить виновных в случае удаленной атаки.

• Украденные пароли: пароли доступа уполномоченного персонала на сайте IOC могут быть украдены с помощью вредоносных программ и фишинговых методов. Чтобы справиться с этим типом слабости, многофакторный контроль доступа может помочь сузить круг злоумышленников и предотвратить их проникновение.

• Операционные нарушения: IOC должна иметь возможность контролировать и отслеживать неправомерные действия персонала IOC. Все события, происходящие в IOC, отслеживаются в режиме реального времени и регистрируются в хранилище данных для последующего отслеживания и расследования.

• Резервное копирование и контроль захвата: если в IOC вторгаются, его необходимо быстро отключить. Вывод из строя может быть осуществлен в виде отключения питания IOC или отключения его соединений с вычислительными системами, системами хранения данных, сетью, датчиками и всеми внешними интерфейсами. Также может быть установлен режим «ведущий-ведомый», при котором скомпрометированный IOC становится ведомым (следовательно, подчиняется ведущему IOC), а ведущий может полностью отключить функции ведомого IOC.

Обеспечение безопасности финансовых активов умного города. Финансовые активы включают как материальные, так и нематериальные активы жителей города, бизнес-корпораций и правительства. Большая часть этих финансовых активов хранится в финансовых учреждениях, будь то банки, фирмы по ценным бумагам или кредитные союзы. Возможные атаки включают: отключение финансовых услуг (таких как онлайн-банкинг, онлайн-трейдинг и т.д.) – финансовые кражи (кража денег, акций и т.д.) – кража информации о счетах (пользовательских и финансовых данных).

Для защиты финансовых IT-систем от посторонних лиц в основном используются межсетевые экраны, а также системы обнаружения и предотвращения вторжений. Безопасность с точки зрения контроля доступа пользователей, многофакторной аутентификации пользователей, шифрования данных, защищенных сетевых и транспортных соединений, защиты от вредоносных программ и вирусов, проверки журналов, защиты конечных точек и т.д. – все это необходимо для защиты финансовых активов умного города.

Заключение. Развитие умных городов началось по всему миру и поставило перед промышленностью и странами серьезные задачи. Умный город неполноценен без комплексной системы безопасности и механизмов защиты его граждан, предприятий, операций и услуг. В данном исследовании подчеркивается важность безопасности для умного города, приводится список возможных атак и определяются области для обеспечения безопасности и защиты, таких ресурсов как вода, энергия, данные, связь (интернет), городской «мозг» и критически важные городские службы (полиция, пожарные, банки, здравоохранение и транспорт). Безопасность умных городов – это новая актуальная тема, которая требует более глубоких и дальнейших исследований, и проблему следует рассматривать как безопасность систем, начиная с устройств и заканчивая провайдерами и пользователями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Намиот Д.Е., Куприяновский В.П., Самородов А.В., Карасев О.И., Замолодчиков Д.Г., Федорова Н.О. Умные города и образование в цифровой экономике // International Journal of Open Information Technologies. 2017. V. 5. N 3. P. 56–71.

2. Власова Н.Ю. От безопасного города к умному городу: стратегический подход // Экономико–правовые проблемы обеспечения экономической безопасности: материалы Всероссийской научно–практич. конф. Екатеринбург: Изд–во Екатер. ун–та, 2018. С. 163–166. URL: https://elibrary.ru/item.asp?id=36888260

3. Cybersecurity in smart cities. Master thesis, Lund University, Sweden.Available at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8950557&fileOId=8950904

4. Строев П. В., Решетников С. Б. Умный город как новый этап городского развития // Экономика промышленности. 2017. Том 10. № 3. URL: https://doi.org/10.17073/2072–1633–2017–3–207–214

5. Challenges of cybersecurity for smart cities. Available at https://personalpages.manchester.ac.uk/staff/m.dodge/Dodge_Kitchin_Challenges_of_Cybersecurity_for_Smart_Cities.pdf

6. Грибков Р.В., Мухин М.А. Умный город: концептуальный подход к созданию платформы умного города на муниципальном уровне // Развитие менеджмента в индустрии 4.0: Переход к киберфизическим организациям и формирование их систем управления: материалы XI Российской научно–практич. конф. (с междунар. участием). Пермь: Изд–во Перм. ун–та, 2018. С. 49–51. URL: https://elibrary.ru/item.asp?id= 37043748.

7. Пахомов Е.В. Технологическая основа умного города // Инженерный вестник Дона. 2017. № 3. URL: http://ivdon.ru/uploads/article/pdf/IVD_109_Pakhomov1.pdf_0b44ff1497.pdf

8. Цибарева М.Е., Васяйчева В.А. Оценка эффективности внедрения элементов умного города в процессе цифровизации городской среды // Вестник Самарского университета. Экономика и управление. 2020. № 11(2). С.83–91.

9. Шалагинов А. Концепция SMART / SAFE CITY от «А» до «Я» // Технологии и средства связи. 2016. № 3 (114). С. 23–25.

10. Huawei Intelligent Operations Center (IOC). Available at https://e.huawei.com/en/solutions/industries/government/smart-city/ioc

11. Серёдкин С.П. Безопасность критической информационной инфраструктуры (краткий обзор современных подходов) // Информационные технологии и математическое моделирование в управлении сложными системами. 2021. № 4(12). С.30–38. DOI: 10.26731/2658–3704.2021.4(12).30–38

12. Bluetooth security. Electronic Notes. Available at https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php

13. LoRaWAN Security Whitepaper. LORA Alliance, 2017. Available at https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

14. Make things come alive in a secure way. SIGFOX, Technical White Paper, 2017. Available at

15. Guide to LTE security. NIST, 2017. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

REFERENCES

1. Namiot D.Ye., Kupriyanovskiy V.P., Samorodov A.V., Karasev O.I., Zamolodchikov D.G., Fedorova N.O. *Umnyye goroda i obrazovaniye v tsifrovoy ekonomike* [Smart cities and education in the digital economy].International Journal of Open Information Technologies. 2017. v. 5. no. 3. pp. 56–71.

2. Vlasova N.Yu. *Ot bezopasnogo goroda k umnomu gorodu: strategicheskiy podkhod* [From a safe city to a smart city: a strategic approach]. *Ekonomiko–pravovyye problemy obespecheniya ekonomicheskoy bezopasnosti* [In: Economic and legal problems of ensuring economic security: proceedings of the All–Russian Research and Practical Conference]. Ekaterinburg: Izd–vo Ekater. un-ta, 2018, pp. 163–166. Available at: https://elibrary.ru/item.asp?id=36888260

3. Cybersecurity in smart cities. Master thesis, Lund University, Sweden.Available at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8950557&fileOId=8950904

4. Stroyev P. V., Reshetnikov S. B. *Umnyy gorod kak novyy etap gorodskogo razvitiya* [Smart city as a new stage of urban development]. *Ekonomika promyshlennosti* [Economics of Industry]. 2017. v. 10. no. 3. URL: https://doi.org/10.17073/2072–1633–2017–3–207–214

5. Challenges of cybersecurity for smart cities. Available at https://personalpages.manchester.ac.uk/staff/m.dodge/Dodge_Kitchin_Challenges_of_Cybersecurity_for_Smart_Cities.pdf

6. Gribkov R.V., Mukhin M.A. *Umnyy gorod: kontseptual'nyy podkhod k sozdaniyu platformy umnogo goroda na munitsipal'nom urovne* [Smart city: conceptual approach to creating digital platform for smart city at the municipal level]. *Razvitiye menedzhmenta v industrii 4.0: Perekhod k kiberfizicheskim organizatsiyam i formirovaniye ikh sistem upravleniya* [Management Development in Industry 4.0: Transition to Cyberphysical Organizations and the Formation of Their Management Systems: materials of the XI Russian Research and Practical Conference (with internation-

al participation)]. Perm: Izd-vo Perm. un-ta, 2018, pp. 49–51. Available at: https://elibrary.ru/item.asp?id=37043748

7. Pakhomov E.V. *Tekhnologicheskaya osnova umnogo goroda* [Technological basis of a smart city]. *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don]. 2017. no. 3. URL: http://ivdon.ru/uploads/article/pdf/IVD_109_Pakhomov1.pdf_0b44ff1497.pdf

8. Tsibareva M.E., Vasyaicheva V.A. *Otsenka effektivnosti vnedreniya elementov umnogo goroda v protsesse tsifrovizatsii gorodskoy sredy* [Evaluation of the effectiveness of the implementation of smart city elements in the process of digitalization of the urban environment]. *Vestnik Samarskogo universiteta. Ekonomika i upravleniye* [Bulletin of the Samara University. Economics and Management]. 2020. no. 11(2). pp. 83–91.

9. Shalaginov A. *Kontseptsiya SMART / SAFE CITY ot «A» do «YA»* [The concept of SMART / SAFE CITY from «A» to «Z»].*Tekhnologii i sredstva svyazi* [Technologies and means of communication]. 2016. no. 3 (114). pp. 23–25.

10. Huawei Intelligent Operations Center (IOC). Available at https://e.huawei.com/en/solutions/industries/government/smart-city/ioc

11. Seredkin S.P. *Bezopasnost' kriticheskoy informatsionnoy infrastruktury (kratkiy obzor sovremennykh podkhodov)* [Security of critical information infrastructure (a brief overview of modern approaches)]. *Informatsionnyye tekhnologii i matematicheskoye modelirovaniye v upravlenii slozhnymi sistemami* [Information technologies and mathematical modeling in the management of complex systems]. 2021. no. 4(12). pp.30–38. DOI: 10.26731/2658–3704.2021.4(12).30–38

12. Bluetooth security. Electronic notes. Available at: https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php

13. LoRaWAN Security Whitepaper. LORA Alliance, 2017. Available at: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

14. Make things come alive in a secure way. SIGFOX, Technical White Paper, 2017. Available at

15. Guide to LTE security. NIST, 2017. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

Информация об авторах

Дмитрий Александрович Массеров – к. э. н., доцент, географический факультет, Мордовский государственный университет им. Н.П. Огарёва, г. Саранск, e-mail: masserow@yandex.ru

Даниил Дмитриевич Массеров – студент направления подготовки «Инфокоммуникационные технологии и системы связи», Мордовский государственный университет им. Н.П. Огарёва, г. Саранск, e-mail: masserovggg@gmail.com

Authors

Dmitriy Alexandrovich Masserov – PhD in Economics, Associate Professor, Faculty of Geography, Ogarev Mordovia State University, Saransk, e-mail: masserow@yandex.ru

Daniil Dmitrievich Masserov – student of the direction «Info-communication technologies and communication systems», Ogarev Mordovia State University, Saransk, e-mail: masserovggg@gmail.com

Для цитирования

Массеров Д.А., Массеров Д.Д. Обеспечение кибербезопасности умного города в процессе цифровизации городской среды // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №1(13). – С. 32-41 – DOI: 10.26731/2658-3704.2022.1(13).32-41 – Режим доступа: http://ismm-irgups.ru/toma/113-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 26.04.2022)

For citation

Masserov D.A., Masserov D.D. Ensuring the cyber security of the smart city in the process of digitalisation of the urban environment // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 1(13). P. 32-41. DOI: 10.26731/2658-3704.2022.1(13).32-41. [Accessed 26/04/22]