DOI:10.19181/kongress.2020.119

Иванова Зинаида Ильинична
Национальный исследовательский Московский
государственный строительный университет,
Москва, Российская Федерация
ivanovazi@mail.ru

Технологии «smart city» для обеспечения безопасности в современном городе

Аннотация. Обсуждается вопрос о необходимости внедрения контроля на улицах городов, в местах скопления людей. Технологии «Smart city» и Интернета вещей (Iot) способны вести наблюдение, собирать необходимую информацию и обрабатывать её в режиме реального времени для быстрого реагирования и предупреждения совершения преступлений и террористических актов. Приводятся примеры реализации таких технологий в европейских и американских городах, разработок в российских правоохранительных органах. Автором отмечаются те преимущества, которые дают «умные» технологии, однако автора больше волнует вопрос о ненадежности и защите программ «Smart city» и «Internet of things» от взлома злоумышленников и использовании в преступных целях. Вывод автора: уже обозначился новый парадокс современности: безопасность самих технологий обеспечения безопасности городской среды. Следовательно, эта проблема должна решаться пересмотром принципиальных подходов к областям и направлениям их применения. Например, в современных условиях технологии слежения необходимы, но внедрять их нужно не ущемляя свободу личности и её права на частную жизнь, учитывая исторические и социокультурные традиции народа.
Ключевые слова: Smart city; цифровизация; безопасность; контроль; преступность; терроризм; свобода личности

Ivanova Zinaida Ilyinichna
National Research Moscow State University of Civil Engineering,
Moscow, Russian Federation
ivanovazi@mail.ru

«Smart city» technologies for safety in a modern city

Abstract. The need to introduce control on the streets of cities, in crowded places is discussed in the article. Smart City and the Internet of Things (Iot) technologies are capable of monitoring, collecting the necessary information and processing it in real time to quickly respond and prevent the commission of crimes and terrorist acts. The author draws examples of the implementation of such technologies in European and American cities, developments in Russian law enforcement agencies. The author notes the advantages of «smart» technologies. However, the author is more concerned about unreliability and protection of the Smart city and Internet of things programs from hacking and using them for criminal purposes. The author's conclusion is: a new paradox of our time has been identified: the safety of the technologies ensuring the safety of the urban environment. This problem should be solved by revising the fundamental approaches to digital technologies' application. For example, tracking technologies are necessary in modern conditions, but they should be

implemented without limiting individual freedom and individual right to privacy, taking into account the historical and socio-cultural traditions of the nation.
Keywords: Smart city; digitalization safety; control; crime; terrorism; personal freedom

Введение

«Умный город» – это не только город высоких технологий, это город, созданный для человека, его интересов, разнообразной жизни, для разных людей» [Катханова, 2014]. Эти слова все чаще звучат в выступлениях политиков, статьях ученых, проектах градостроителей. «Умный город» еще не стал реальностью, но уже появились опасения о последствиях от внедрения «Smart» технологий, Интернета вещей: не приведут ли они к тотальной слежке за каждым горожанином, ограничению свободы, нарушению права на личную жизнь и, в конце концов, к снижению ощущения удовлетворенности жизнью. Многие исследователи предупреждают: программа «умного города» так быстро внедряется в жизнь, что люди оказываются не готовыми принять её ни с психологической, ни с финансовой точки зрения. Цифровые технологии вызваны самим временем, теми процессами и изменениями, которые произошли в последние десятилетия в обществе. Они оказались остро необходимы, в частности, для обеспечения безопасности жителей города, для предупреждения преступлений и террористических актов. Главная задача: как их внедрить, чтобы люди органично встроили цифровые технологии в свой ментальный ценностный ряд, не почувствовали себя «обнаженными», ущемленными в свободе, лишенными приватной территории. «Технократический проект «умного города», не связанный с историческими и социокультурными традициями, требует более серьезной гуманитарной адаптации, чтобы стать привлекательным для горожан. Поэтому сегодня необходимо не только ответить на вопрос, как нам внедрять концепцию «умного города» в России, но и понять, как подготовить население к проживанию в таком городе, сделать его интересным и привлекательным для абсолютного большинства жителей» [Василенко, 2018: 13–19].

Целью данной статьи является обзор «smart» технологий для обеспечения безопасности города и горожан, преимуществ и недостатков, позитивных и негативных проявлений, анализ существующих практик применения данных технологий в европейских и российских городах. Автором применяется метод анализа документов: правительственных решений, зарубежных и российских экспертно-аналитических докладов о применении технологий умного города [Analytical Report, 2017; *Направления внедрения технологий умного города, 2018*], результатов картирования умных городов [Mapping Smart Cities in the EU, 2015], исследовательских статей, материалов дискуссий.

Обзор литературы

Тема внедрения технологий «Smart city» в жизнь городов становится все более актуальной в мировой науке. Множество публикаций в научных изданиях разных стран посвящены разным аспектам внедрения данных технологий в практику. Особо

выделяются статьи, в которых речь идет об обеспечении улучшении здравоохранения и транспортных услуг, борьбе с последствиями изменения климата, создании комфортной среды с помощью разных «умных» электронных систем [Balogun A. L., Marks, Sharma, 2020; Saborido , Alba, 2020]. Тем не менее, вопросы безопасности жизни и собственности горожан, предупреждения преступности во многих случаях игнорируются [Laufs, Borrion, 2020]. Умные города должны обеспечивать индивидуальную конфиденциальность и безопасность, утверждают исследователи из Университета Макгилла в Монреале (Канада) [Braun, Fung, Iqbal, 2018]. Авторы предлагают возможные решения пяти проблем умного города в надежде предвидеть дестабилизирующие тенденции. Среди таких проблем: сохранение конфиденциальности с помощью многомерных данных, защита сети от неожиданных и мощных атак злоумышленников, создание надежных методов обмена данными, правильное использование искусственного интеллекта и уменьшение количества сбоев в интеллектуальной сети. Проблемы уязвимости и риска в функционировании киберфизических систем в умных городах обсуждают авторы из университета Олбани (Олбани, США) и Школы электротехники и информатики (Оттава, Канада) [Habibzadeh, Nussbaum B, Anjomsjoa, 2019]. В статье проводится обзор теоретических и практических задач и возможностей не только с точки зрения их технических аспектов, но также с точки зрения проблем политики и управления.

В российской науке вопросам внедрения технологий «Smart city» и обеспечения их безопасности уделяется недостаточно внимания, однако в последнее время данная тема также актуализируется. Исследователь из Университета ИТМО (Санкт-Петербург, Россия) в соавторстве с коллегой из Университета Олбани (Олбани, США) подвергает анализу конкретные случаи восприятия жителями Санкт-Петербурга инициатив умного города [Vidiasova, Cronemberger, 2020]. Авторы отмечают разрыв в понимании граждан и власти стремлений умного города, разрыв между ожиданиями горожан и результатами, и отмечают, что этот разрыв ставит под угрозу доверие и уровни участия граждан в инициативах «умного города». Иначе говоря, речь идет о риске игнорирования интересов и потребностей различных заинтересованных сторон – городских сообществ и властных групп. Наиболее остро вопрос об учете потребностей горожан, их личной психологической и интеллектуальной готовности к приняттию программ контроля и слежения ставится в статье российского исследователя Василенко И. А. [Василенко, 2018: 13–19].

Результаты исследования

В обоснование необходимости внедрения технологий умных городов, обеспечивающих безопасность, нужно положить, в первую очередь, анализ этапов развития общества с точки зрения форм общественного контроля и изменения общественного сознания. В традиционном обществе (городах и поселениях) люди живут небольшими общинами, каждый человек на виду, он контролируем другими членами своей социальной группы. С развитием индустриального общества большое

количество людей сосредоточивается в городах, на фабриках и заводах. Человек становится анонимным, его труднее контролировать, поэтому создаются институты формального контроля, и одновременно институты гражданского общества. В постиндустриальном обществе усиливается миграция, города становятся мультикультурными со множеством новых городских сообществ, субкультурных, контркультурных групп с разными идеологиями и целями, в том числе, террористическими. Современный город требует постоянного внимания и управления происходящими процессами, соблюдения баланса между естественным и позитивным правом.

Умный и безопасный город – это умная политика градорегулирования. Важное направление организации городской среды с учетом процесса роста городов и городского населения – применение технологий «Smart city» (системы цифрового наблюдения, считывание, технологии предиктивного обнаружения, система экстренного оповещения, централизованные станции контроля и др.). Десятки и сотни тысяч датчиков и видеокамер собирают информацию о ситуации на дорогах, в общественных местах и зданиях, на спортивных мероприятиях и территориях с ограниченным доступом, чтобы вовремя заметить угрозу, проанализировать её и передать информацию соответствующим службам. Они позволяют эффективно управлять городом и его отдельными районами и обеспечивать безопасность среды. Система новейших сенсоров и технология видеоаутентификации делают возможным сбор широкого спектра данных, охватывающих все сферы городской жизни. Эти данные можно эффективно визуализировать, собирать и использовать в самых различных ситуациях. При этом в настоящее время от фиксации правонарушений комплексы безопасности все больше переходят к аналитике в режиме реального времени и предиктивной аналитике [Analytical Report 8, 2017]. Например, в Чикаго используются высокопроизводительные вычисления для определения лиц преступников, зафиксированных посредством специальных камер. Для оперативного коллективного использования полученных данных в полицейской среде (патрульных служб, службы расследования преступлений и криминологических экспертов, оперативных полицейских сил) Министерством юстиции США установлены стандарты и правила создания целостного информационного пространства: Национальная Информационная Модель Обмена Информацией (NIEM) и Глобальная Архитектура Ссылок (GRA).

Многие города мира уже создают единые Аналитические центры сбора и обработки информации. Однако пока только столица Каталонии Барселона остается единственным городом, где функционирует общая платформа для сбора информации со всех датчиков. Всего около 550 датчиков собирают информацию и контролируют обстановку в городе. Здесь установлены наиболее продвинутые системы датчиков.

В системе видеонаблюдения в Лондоне все камеры, направленные на общественное пространство, находятся в распоряжении полиции. Камеры, которые наблюдают, далеко не всегда помогают предотвращать преступления, однако дают возможность всем структурам полиции работать слаженно и эффективно, в реальном

времени и направлять обработанные данные людям, ответственным за принятие решений.

Еще одна возможность осуществлять постоянный контроль скоплений людей, толп и проявлений возможной агрессии – crowdsensing. В данном случае информация собирается сенсорами (видео-камерами) на устройствах пользователей. В качестве таких устройств могут использоваться видео-регистраторы в автомобилях, социальные сети. Полицейские могут быть снабжены носимыми камерами, видео с которых тоже может попадать в полицейское облако. Подобные системы уже используются в городах Балтимор и Окленд в США [Куприяновский и др., 2016].

Системам видеонаблюдения уделяется особое внимание в концепции «Smart City», разработанной в Казахстане. В программу будут внедрены модули обнаружения подозрительного поведения, оставленных подозрительных предметов, стихийного скопления больших людских масс и т.д. Биометрическая видеоаналитика позволит распознавать лица по биометрическим признакам лица. Таким образом, могут быть обнаружены лица, находящиеся в розыске или вызывающие подозрение. Данные о передвижении подозреваемого с камер видеонаблюдения будут отправляться ближайшим дежурным патрульным на Аппаратно-программный комплекс «Правонарушение», которыми те будут оснащаться [Альмухамедова, 2018].

В России таких комплексных систем класса «умная полиция» пока нет, однако есть разработки типа СОРМ (Система технических средств для обеспечения функций оперативно-розыскных мероприятий) – комплекс технических средств и мер для эффективной работы правоохранительных органов, включая возможность прослушивания телефонных разговоров с разрешения суда.

В феврале 2019 г. Минстрой России утвердил стандарт «Умный город», большинство мероприятий которого планируется реализовать к 2024 г. К базовым положениям стандарта относится внедрение интеллектуального видеонаблюдения с распознаванием лиц и развитие систем информирования граждан о чрезвычайных ситуациях через мобильные средства связи. В 19 пилотируемых российских городах появятся цифровые технологии обеспечения общественной безопасности: постоянный мониторинг проблемных районов (в том числе и мест сосредоточения мигрантов и беженцев), подозрительных лиц и подозрительного поведения в целях предупреждения преступных действий.

«Внедрение таких инноваций, фактически, трансформирует городской уклад жизни невероятно быстрыми темпами и дает огромные преимущества жителям городов, но и сопровождается совершенно новыми цифровыми угрозами и опасностями» [Соколов, 2018: 104–118]. Теперь многие горожане задаются вопросом, не принесут ли подобные «новшества» к сбоям в электронных системах, вмешательству хакеров, подмене и преступном использовании информации. Может ли, например, хакер парализовать работу всей городской инфраструктуры? Может ли

преступник, внедрившись в Аппаратно-программный комплекс, единый центр, куда стекается вся информация городской территории, использовать такую информацию в террористических целях? Может ли он подменить биометрическую информацию и спасти преступника от правосудия? Насколько надежны программы цифрового города? И какими нашими личными данными мы позволим распоряжаться властями и полицией? Не находимся ли мы круглосуточно под всевидящим Оком Большого брата, под тотальным контролем властей?

Такие опасения вполне обоснованы. Уязвимость подобных систем уже выявлена, в частности, на улицах Вашингтона [Интеллектуальные города. Умные города, 2020]. В Москве мы также встречаемся со случаями кражи банковских данных, взлома паролей и увода денег со счетов вкладчиков. Контроль личной переписки и СМС-сообщений – уже для нас не новость. Можно также ожидать от злоумышленников совершения откровенных преступлений – дать неверную команду интеллектуальной системе города или организовать поставку неточных данных и нарушения движения транспорта, намеренно организовать ДТП, создать перебои в подаче электроэнергии, осуществить кражу электроэнергии и т.д. Как отмечают специалисты, некоторые системы Smart city чрезвычайно уязвимы к кибератакам, в некоторых городах финансирования систем защиты недостаточно, им нужны более значительные инвестиции. Некоторым городам не хватает опытных специалистов или соответствующей коммуникационной инфраструктуры. Злоумышленники могут идти впереди создателей программ и из-за недостатка у них знаний о методах социальной инженерии. Речь идет о сложных кибератаках, ведущих к взлому коммуникаций между устройствами, блокировке систем с помощью вымогательского программного обеспечения, изменение данных датчиков и др.

Современные процессы урбанизации приводят к росту больших городов, увеличению числа мегаполисов. В некоторых странах Европы численность городских жителей уже более 80 %, в России 74 % населения живут в городах. Столь быстрый рост городского населения, рост городского пространства и усложнение его технической и социальной структуры вызывает все более острую необходимость в эффективности управления городами. Автомобили и поезда метро без водителей, видеоконтроль с помощью технологии распознавания лиц, расширение сферы он-лайн финансовых расчетов. Все это сегодня не просто вызывает опасения у людей, но и превращается в пугающую перспективу.

По мнению Стивена Вебба, вице-президента исследовательского департамента компании Frost & Sullivan, наиболее подвержены угрозам кибератак крупные города – мегаполисы, которые требуют постоянного совершенствования и усложнения программ безопасности. Это чрезвычайно актуально и для российских городов [Вебб, 2015]. Чемпионат мира по футболу в 2018 г. подтолкнул правительство России к финансированию новых систем безопасности. Модернизированы командно-оперативные центры, усовершенствованы аналитические системы, а также обновлены

существующие программы видеонаблюдения, но необходимого финансирования для новейших систем контроля и аналитики пока недостаточно.

Выводы

Итак, у технологий «Smart city» есть две противоположные стороны:

1) повышение комфорта городской среды, быстрое получение нужной информации, широкий доступ к самоуправлению, контроль и снижение уровня преступности;

2) возможность злонамеренного проникновения в программы управления городскими процессами и совершение тяжких массовых преступлений; вторжение в личную жизнь, попадание конфиденциальных данных в руки злоумышленников и совершение преступлений против личности, недостаточная степень защищенности программ.

Не находимся ли мы в эйфории от ожидания решения всех проблем с помощью Smart-технологий. Вся человеческая история показывает, что новые открытия сопровождаются новыми проблемами, которые оказываются гораздо сложнее, чем предыдущие. С нашей точки зрения, появился новый парадокс современности – безопасность самих технологий обеспечения безопасности городской среды, благополучия и жизни горожан. Проблему повышения безопасности программ «Smart city» решить гораздо сложнее, нужны принципиально новые подходы к направлениям и возможностям цифровизации, но как показывает недолгая история электронной эпохи, такой процесс бесконечен: любое действие неизменно порождает противодействие.

И. Аукен, министр экологии Дании, выступая на сессии Мирового экономического форума, заявила, что к 2030 году приватность полностью исчезнет из человеческой жизни. Не будет собственности, личного транспорта, привычной работы. По мнению датского министра, подобный образ жизни позволит человечеству избавиться от таких серьезных проблем, как изменение климата, миграционный кризис, ухудшение экологии, безработица и перенаселение городов [Интеллектуальные города. Умные города, 2020]. Большинству современников эти слова кажутся взятыми из антиутопических произведений фантастов, вряд ли люди согласятся находиться постоянно под всевидящим Оком Большого брата, быть под тотальным контролем даже в целях безопасности.

Библиографический список

Альмухамедова Н. SMART CITY: Умные технологии улучшают жизнь казахстанцев. [Электронный ресурс] // Strategy 2050: [веб-сайт]. URL: https://strategy2050.kz/ru/news/52068 (дата обращения: 29.05.2020).

Василенко И. А. «Умный город» как социально-политический проект: возможности и риски смарт-технологий в городском ребрендинге// Власть. 2018. № 3. С. 13–19.

Вебб С. Безопасность умных городов (Smart Cities safety)// Технологии и средства связи. 2015. № 3. С. 30–33.

Интеллектуальные города. Умные города [Электронный ресурс] // Государство. Бизнес. ИТ./URL: http://www.tadviser.ru/index.php (дата обращения: 29.05.2020).

Катханова А. Мультиформатное двухдневное мероприятие **Smart City Ground-Up** в рамках проекта Smart in the City [Электронный ресурс] // Междисциплинарный лекторий «Контекст»: [веб-сайт]. *URL:* http://www.contextfound.org/events/y2014/m11/n97 (дата обращения: 29.05.2020).

Куприяновский В. П., Буланча С. А., Намиот Д. Е., Синягов С. А. Умная полиция в умном городе// International Journal of Open Information Technologies. 2016. Vol 4, № 3. ISSN: 2307–8162.

Направления внедрения технологий умного города в российских городах. Экспертно-аналитический доклад. Центр стратегических разработок Северо-Запад. М., 2018. 164 с.

Соколов И. А., Куприяновский В. П., Аленьков В. В. и др. Цифровая безопасность умных городов// International Journal of Open Information Technologies. Vol. 6, № 1. 2018, С. 104–118. ISSN: 2307–8162.

Analytical Report 8: The Future of Open Data Portals [Электронный ресурс] // European Data Portal: [веб-сайт]. URL: https://www.europeandataportal.eu/sites/default/files/edp_analyticalreport_n8.pdf (дата обращения: 29.05.2020).

Balogun A. L., Marks D, Sharma R. Assessing the Potentials of Digitalization as a Tool for Climate Change Adaptation and Sustainable Development in Urban Centres. Sustainable Cities and Society, Vol. 53, 2020, 101888. https://doi.org/10.1016/j.scs.2019.101888.

Braun T., Fung B. C. M., Iqbal F. et al. Security and privacy challenges in smart cities// Sustainable Cities and Society, 2018, Vol. 39, P. 499–507. https://doi.org/10.1016/j.scs.2018.02.039.

Habibzadeh H., Nussbaum B. H., Anjomsjoa F. et al. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities// Sustainable cities and Society, 2019, Vol. 50, 101660. https://doi.org/10.1016/j.scs.2019.101660.

Laufs J., Borrion H., Bradford B. Security and the smart city: A systematic review// Sustainable Cities and Society, 2020, Vol. 55, 102023. https://doi.org/10.1016/j.scs.2020.102023Get rights and content.

Mapping Smart Cities in the EU [Электронный ресурс] // [веб-сайт]. URL: https://www.unece.org/fileadmin/DAM/hlm/prgm/urbandevt/Measuring_Progress__Achieving_Smarter_Cities_/Presentations/Catriona_Manville.pdf (дата обращения: 29.05.2020).

Saborido R., Alba E. Software systems from smart city vendors// Cities, 2020, Vol. 101, 102690. https://doi.org/10.1016/j.cities.2020.102690.

Vidiasova L., Cronemberger F. Discrepancies in perceptions of smart city initiatives in Saint Petersburg, Russian Federation// Sustainable Cities and Society, 2020, Vol. 59, 102158. https://doi.org/10.1016/j.scs.2020.102158.