УДК 426.33

ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ «УМНЫЙ ГОРОД»

[1]Рыбак В. А., [2]Римарев И. М., [3]Таруат А. Т.
[1]Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, rbk@mail.ru,
[2] Белорусская государственная академия связи, Минск, Беларусь, rimaev@mail.ru,
[3]Белорусский национальный технический университет, Минск, Беларусь, tayrat@mail.ru

Аннотация. Хотя 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». Согласно городскому взгляду, «умный город является продвинутым и высокотехнологичным городом, который объединяет людей, информацию и элементы городской инфраструктуры». С точки зрения информационно-технологического аспекта, «в основе умного города находится интеллектуальный обмен информацией, протекающий между большим числом его различных подсистем». Основными подходами к реализации концепции умного города являются проектирование и создание городов [1].

Исходя из вышесказанного следует подчеркнуть, что немаловажным аспектом развития цифровой среды является эффективное взаимодействие инструментов технических систем умных городов и пользователей. Такое взаимодействие можно назвать интерфейсом умного города. Такие технологии должны быть актуальными, уникальными, доступными, удобными, понятными населению и функциональными в использовании, соответствовать потребностям населения. Именно интерфейсы умного города, то есть взаимосвязь пользователей и интеллектуальных систем, являются основой его социально-технического развития. Актуальным на данный момент является создание человеко-машинных интерфейсов (human-machineinterfaces, HMI) с целью обеспечения рабочих мест в рамках технологических систем. Существуют также человеко-компьютерный интерфейс (humancomputerinterfaces, HCI), мобильный интерфейс в рамках разработки и использования мобильных приложений населением. Стандартами качества цифровых систем являются ISO 9241, ISO / TR 16982: 2002, ISO / IEC 25010: 2011.

Цифровая среда в свою очередь включает в себя технологии умного города (центры обработки данных, сети передачи данных, умные устройства); компоненты (умное управление, умная городская среда, умная экономика, умные люди, умная мобильность, умная окружающая среда); каналы (служба-

поддержки, онлайн встречи, email, официальный сайт, мессенджер/чат, socialmedia, мобильные приложения, C2C платформы, онлайн-трансляции); интерфейсы, пользователи smart-городов (государственные частные, общественные организации, население) [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 CitiesinMotion бизнес-школы Наварры. «Умный город» в Беларуси предполагает собственно город вместе с прилегающими территориями. При этом крупные предприятия чаще всего располагаются за пределами города, уровень жизни населения в РБ в таких городах ниже среднего по сравнению с мировой практикой, однако стоит учитывать особенности жизни в сельской местности [3, 4].

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). На ЖД вокзале станции «Кричев» действует платежно-справочный терминал самообслуживания. В поликлиники используется программа МАПСОФТ для выдачи талонов. В УО действуют программные комплексы управленческой деятельности «ПараГраф», системы электронного составления меню «Крошка». Солнечные батареи и аккумуляторы установлены на газорегуляторных пунктах, система GPRS фиксирует показатели на компьютеры. На газопроводах используется дистанционный лазерный детектор утечек метана SewerinRMLD [5].

К синонимам понятия «умный город» относятся «безопасный город», «цифровой город», «комфортный город». 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 исследо-

вания является использование результатов имитационного моделирования систем безопасности в разработке обучающих выборок для систем поддержки принятия решений на интеллектуальном уровне [6].

Довольно важным аспектом обеспечения безопасности умного города является использование интеллектуальных технологий для обеспечения комфорта жителей. Например, использование интеллектуального освещения на улицах города. Автоматическая система интеллектуального управления AmplexAmpLight экономит до 35 % электроэнергии. СУНО «Луч-2» обеспечивает функционирование в 4 режимах работы: в режиме автоматического управления, в режиме телеуправления, в телекаскадном режиме, в режиме ручного управления. Или, например, автоматизированная система управления уличным освещением «Гелиос» [7].

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; экологические ситуации, такие как критические показатели атмосферного воздуха, воды и почв; ситуации, связанные с безопасностью на транспорте (терроризм, преступность, происшествия и аварии); конфликтные ситуации, приводящие к социальным взрывам, криминогенным и террористическим угрозам; эскалация экстремистской деятельности; разжигание национальных и религиозных конфликтов и др.; ситуации, связанные с киберпреступностью и информационной войной; управленческие (операционные) риски и ситуации, приводящие к нарушением жизнедеятельности населения [8].

Единая информационная цифровая среда в рамках концепции «Безопасный город» на территории Российской Федерации достигается в том числе посредством использования интеллектуальных систем видеонаблюдения, датчиков и эффективных технологий удаленного доступа к ним («интернет-вещей»); экономичном хранении и обработке информации в «облачной» среде; разработки в области информационно-аналитических технологий, таких как «искусственный интеллект», «большие данные», разрешение видеокамер до 4К, 5G-технологии и др. Координация работы государственной власти и местных органов самоуправления способствует эффективному функционированию комплексной системы обеспечения безопасности жизнедеятельности населения [9].

Немаловажным аспектом развития «Безопасного города» является информационная безопасность. Источниками цифровой угрозы могут являться разработчики систем, обслуживающий персонал, сами пользователи, а также злоумышленники. 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 Io-вещей; встроенная защита в процессы производства, внедрение продукции OEM-производителями; тестирование программных средств. Так, например, в банковской сфере существуют банковский интернет сервис для устранения аномальных учетных записей, когнитивные технологии для оценивания потенциальных заемщиков [10].

Таким образом, что автоматизация и цифровизация современных городов не является самоцелью и должна, прежде всего, служить повышению комфорта всех жителей, а также обеспечению приемлемого уровня безопасности.

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. Семячков, К. А. Особенности развития интерфейсов умного города / К. А. Семячков // Экономика и бизнес: теория и практика. – 2021. – № 6–2. – С. 185–201.

3. Инструкция для градоначальников, или дорожная карта умного города / Н. Кошаровский // 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.

4. 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.

5. Кричев: ИТ-подъем с переворотом / Д. В. Бочков // Веснік сувязі: научно-производственный журнал для специалистов в области связи и информационных технологий / Министерство связи и информатизации Республики Беларусь, Белорусский профессиональный союз работников связи. – 2019. – № 3. – С. 20–27.

6. 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.

7. Кузнецов, А. И. Автоматизированное управление эффективностью систем освещения на базе светодиодных источников света / А. И. Кузнецов. – Челябинск: ЮУрГУ, 2020. – 123 с.

8. 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.

9. Качанов, С. А. О месте АПК «Безопасный город» в концепции «Умный город» / С. А. Качанов, А. П. Попов // Технологии гражд. безопасности. – 2019. – Т. 16, № 3. – С. 4–9.

10. 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.