И.Е. Кабанова
к.ю.н.
Российская академия народного хозяйства
и государственной службы
при Президенте Российской Федерации, Москва

БЕЗОПАСНОСТЬ В «УМНОМ ГОРОДЕ»: СУЩЕСТВУЮЩИЕ УГРОЗЫ И СПОСОБЫ МИНИМИЗАЦИИ РИСКОВ [1]

I.E. Kabanova
Ph.D. in Law
The Russian Presidential Academy
of National Economy and Public Administration, Moscow

THE SECURITY IN A «SMART CITY»: THE EXISTING THREATS AND WAYS TO MINIMIZE RISKS

Аннотация. Рассматриваются перспективы внедрения комплекса «Безопасный город» и стандарта «Умный город» с учетом имеющихся темпов развития «умной инфраструктуры» в российских муниципалитетах, а также выявляются отдельные угрозы, связанные с цифровизацией городов, и предлагаются способы их минимизации.
Ключевые слова: «умный город», безопасность, угрозы.

Abstract. The prospects for the introduction of the "Security city" and "Smart city" standards, taking into account the existing rates of development of "smart infrastructure" in the Russian municipalities, are considered, as well as certain threats associated with digitalization are identified and ways to minimize them are proposed.
Keywords: "smart city", security, threats

Для управления техногенной средой современного города и обеспечения безопасности для всех пользователей городского пространства применяются новейшие информационные технологии, позволяющие осуществлять постоянный контроль работы всех компонентов городской инфраструктуры, и служащие для предотвращения чрезвычайных ситуаций, а в случае их возникновения немедленного информирования соответствующих служб для оперативного устранения аварий. Примером такой системы является программно-аппаратный комплекс «Безопасный город», предназначенный для обеспечения фото- и видеонаблюдения и фиксации, обеспечения безопасности улиц, дорог, стратегических объектов, жилых домов, общественных зданий и пространств, а также управления объектами жилищно-коммунального хозяйства и другими распределенными объектами в масштабах города. Система направлена на сбор и анализ информации, поступающей от различных городских подсистем, и обеспечение их эффективного совместного функционирования с целью создания комфортной и безопасной городской среды.

«Безопасный город» должен быть внедрен на всей территории России к 2020 году. Начало его созданию было положено в 2015 г. Тогда были запущены работы в пилотных регионах, началась разработка регламентов межведомственного взаимодействия, формирование целевых показателей и т.д. Однако за неполных два года до окончания сроков реализации проекта, по свидетельству представителей

© И.Е. Кабанова, 2019
[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-011-00752.

межведомственной комиссии по внедрению и развитию систем «Безопасного города», только 10 субъектам РФ удалось согласовать технические задания на проведение полного комплекса работ и запустить соответствующие конкурсные процедуры. Подобное положение дел вызывает опасение, что обозначенные сроки будут соблюдены.

Тем не менее, до завершения этого проекта в продолжение работы по цифровизации городского пространства Минстроем России 4 марта 2019 г. были утверждены «Базовые и дополнительные требования к умным городам (стандарт «Умный город»)», включающие 28 мероприятий, которые будут выполнять все города-участники проекта в срок до 2024 года. Стандарт включает мероприятия по восьми направлениям: городское управление, «умное» ЖКХ, инновации для городской среды, «умный» городской транспорт, интеллектуальные системы общественной и экологической безопасности, инфраструктура сетей связи, туризм и сервис. Мероприятия, указанные в стандарте, предусмотрены для реализации в городах с численностью населения свыше 100 тыс. человек и городах, являющихся административными центрами субъектов РФ, но могут быть также реализованы в населенных пунктах с численностью населения менее 100 тыс. человек.

Определенные вопросы вызывает раскоординированность планов по реализации проектов в рамках стандарта «Умный город», и уже намеченных задач по «Безопасному городу», и отсутствие интеграции между этими системами. Чтобы обеспечить взаимодействие систем и подсистем, необходимо создавать интеграционные решения с одним интерфейсом. Сейчас это подменяют квази-интеграцией, когда, например, у оператора «Системы 112» автоматизировано одно рабочее место, но на нем установлено несколько программ, с которыми он работает. И для того, чтобы получать и обрабатывать информацию, оператору надо последовательно открывать и закрывать разные окна, авторизуясь в разных системах. Объектом автоматизации зачастую являются конкретные рабочие места или единые диспетчерские службы, а должны быть – бизнес-процессы, которые обеспечивают интеграцию.

Также отсутствие интеграции систем «Безопасного города» и «Умного города» проявляется на примере использования видеонаблюдения и видеофиксации, поскольку в настоящее время камеры гражданских ведомств не являются доверенным и достоверным источником для силовых и правоохранительных структур. Так, Федеральная служба охраны отказалась использовать данные, передаваемые через «Безопасный город», т.к. не уверена в аутентичности предоставляемого изображения и времени его записи. Более того, в муниципалитетах на одних и тех же точках размещаются разные камеры для нужд различных ведомств.

Таким образом, ключевыми проблемами развития единого информационного пространства в области обеспечения безопасности жизнедеятельности до сих пор являются межведомственная разобщенность, неспособность быстро договариваться, согласовывать соответствующие регламенты, своевременно готовить технические решения и регулировать новые общественные отношения.

Объем рынка технологических решений для «Умного города» в России по итогам 2018 года увеличился на 8%, превысив 81 млрд руб. [1]. При всем потенциале и привлекательности рынка он не только не показывает взрывного роста, но и может сократиться в ближайшие годы. Практически весь российский рынок решений «умного города» представлен Москвой (см. о первом этапе цифровизации Москвы [2]): на столицу приходится 93% рынка, на Санкт-Петербург – 2%, на все остальные регионы – 5%. Частные инвестиции рынок практически не привлекает. Незаинтересованность частных инвесторов в проектах «Умного города» объясняется тем, что зачастую такие вложения не становятся высокодоходными. Более того, в ряде сфер внедрение решений в принципе не может считаться инвестицией, например, в сфере

обеспечения общественной безопасности или в области социальной защиты. Такие системы приносят социальные эффекты и являются некоммерческими по своей сути.

Еще одной существенной проблемой исследуемых проектов является недостаточное обеспечение кибербезопасности устройств систем «Безопасного города» и «Умного города». Например, терминалы, используемые для оплаты парковок, аренды велосипедов, покупки билетов, получения справочной информации, организации электронной очереди и записи на прием к врачу, являются одними из самых вероятных мишеней для хакеров именно из-за своей доступности и доверия к ним со стороны пользователей. И на сегодняшний день уровень их защиты недостаточно высок. Существует несколько типов уязвимостей, которым подвержены такие устройства. Все они позволяют получить как доступ к операционной системе, управляющей терминалом, а затем исследовать содержимое его жесткого диска в поисках ценных данных, так и выходить в Интернет, устанавливать различные приложения, в том числе вредоносные. Кроме того, один терминал может использоваться для взлома других, ведь они часто объединены в сеть.

Существуют уязвимости и в операторских сетях стандартов 4G и 5G, которые используются для управления городской инфраструктурой, в частности, интеллектуальными светофорами, дорожными табло и т.д. Во многих городах для оптимизации дорожного трафика внедряются «умные» светофоры, объединенные в сеть. Взлом такой сети и отказ в обслуживании даже нескольких светофоров чреват авариями и транспортным коллапсом.

В то же время, принимая во внимание все риски, связанные с функционированием «умной» городской инфраструктуры, важно учитывать, что подобные системы действительно способны повлиять на изменение поведенческих моделей, способствуя формированию режима правопорядка. Так, с появлением камер видеонаблюдения было отмечено повышение водительской дисциплины при соблюдении ПДД, в частности, скоростного режима в населенных пунктах и пропуска пешеходов на переходах. Однако такое влияние нелинейно. Эксперты отмечают, что прямой взаимосвязи между количеством установленных устройств для фиксации нарушений ПДД и мест концентрации аварий не выявлено. На снижение очагов аварийности влияет целый комплекс мер, который не ограничивается установкой устройств видеонаблюдения и фиксации правонарушений. В качестве примера приводится опыт Сыктывкара, где мэром было принято решение поставить перед перекрестком отбойники и отодвинуть на три метра стоп-линии. В результате смертность на перекрестках в городе упала до нулевой отметки, что подтвердило: снижению смертности (а это один из важнейших показателей безопасности в городе) способствует не только размещение средств фото- и видеофиксации нарушений ПДД, но и другие меры, в т.ч. не относящиеся к «умной» инфраструктуре.

В качестве рекомендации для сокращения уязвимости подсистем «Безопасного города» и «Умного города» наряду с техническими решениями, рекомендуемыми экспертами по обеспечению кибербезопасности (сегментация интеллектуальной сети, обеспечение целостности данных, биометрические решения), можно предложить увеличить самостоятельность муниципалитетов в вопросах определения конкретных направлений цифровизации для целей обеспечения безопасного развития муниципального образования (как показывает пример Сыктывкара, далеко не всегда для этого требуются «умная» инфраструктура), и предусмотреть в рамках федеральных программ создание муниципальных центров реагирования на киберинциденты, поскольку именно муниципальный уровень позволит оперативно обеспечивать стабильное и безопасное обновление программного обеспечения, учитывать срок службы умной инфраструктуры муниципалитетов, регулировать общественные каналы коммуникации внутри муниципального сообщества.

Список использованных источников

1. «Умный город» нуждается в бюджете // Газета «Коммерсантъ» № 46 от 18.03.2019, с. 10 // https://www.kommersant.ru/doc/3915458 (дата обращения: 09.04.2019).

2. Зотов В.Б. Информационные технологии как инструмент повышения эффективности управления городом // Управленческие науки. 2012. № 1. С. 4 – 12.