Цифровая безопасность умных городов

И.А.Соколов, В.П.Куприяновский, В.В. Аленьков, О.Н.Покусаев, Д.И.Ярцев, А.В.Акимов, Д.Е.Намиот, Ю.В.Куприяновская

***Аннотация*— В статье рассматриваются вопросы, связанные с цифровой безопасностью в Умном Городе. Стандарты и реализации моделей Умных городов ориентированы на применение быстро развивающихся цифровых технологий и нацелены на экономические, социальные, экологические и другие положительны эффекты при применении цифровых технологий в городах. Внедрение таких инноваций, фактически, не только трансформирует городской уклад жизни невероятно быстрыми темпами и дает огромные преимущества жителям городов, но и сопровождается совершенно новыми цифровыми угрозами и опасностями. В статье рассматривается стандарт BSI PAS 185 - спецификации для создания и внедрения подхода, ориентированного на безопасность. Таким образом, этот стандарт ориентирован на процесс развития, а не на окончательные решения. Также подробно рассмотрена работа Национального центра кибербезопасности Великобритании.**

***Ключевые слова*—безопасность, Умный Город, BSI, PAS-185.**

I. Введение

В 2016 году журнал INJOIT объявил основной темой издания года «умные города». С того времени в нем было опубликовано значительное число статей на эту тему [17-35,38,39], однако развитие самой большой инфраструктуры человечества продолжается быстрыми темпами и, соответственно, развивается система стандартов умных городов. Значительную роль в этом процессе играют стандарты BSI, многие из которых становятся стандартами ISO и национальными стандартами разных стран и в том числе и России [34]. Поэтому для того, чтобы наши читатели представляли себе возможности этих стандартов, мы обычно публикуем статьи о вышедших стандартах умных городов BSI практически сразу после их официальной публикации. Так в [24] было рассказано о PAS 183, PAS 184 , которые были опубликованы в середине 2017 года. PAS 185 [4] , посвященный безопасности умных городов официально был опубликован в ноябре 2017. Этим, фактически, завершается огромный этап стандартизации умных городов в Великобритании, который, конечно, будет рассматриваться ISO как возможный прообраз мирового стандарта.

Стандарты, реализации и концепции умных городов построены на применении быстро развивающихся цифровых и иных технологий и нацелены на экономические, социальные, экологические и иные положительны эффекты при их применении в городах. 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. В работе [19] был изложен опыт обеспечения цифровой безопасности умных городов на примере США, однако эта тема настоль обширна, что требует и особого внимания и множества исследований. Наука и техника являются агентами изменения и роста. В цифровой экономике новые технологии нарушают существующие бизнес-модели. Это и делает эту экономику более продуктивной. Изменения, которые они приносят, имеют огромный потенциал и затрагивают каждый аспект нашей жизни. Эти изменения приносят большие возможности и могут также принести риски.

Smart Cities - это набор технологических инновации и инициатив, использования датчиков и использование большей возможности подключения для увеличения сбора данных. Основная цель: «Умный город» должен улучшить жизнь граждан более эффективным использованием данных, позволив лучше и устойчивее управлять инфраструктурой и услугами. «Умные города» должны обеспечить безопасность и эти соображения являются краеугольным камнем их системы. Помимо потери данных, другие потенциальные эффекты включат рассмотрение тех, у кого есть злонамеренные намерения дать неверную команду интеллектуальной системе города или создать поставку неточных данных, чтобы преднамеренно нарушать услуги.

Выпуску PAS 185 предшествовали решения правительства Великобритании [7,8,9,13] , на которые этот стандарт прямо или косвенно ссылается. Но на самом деле, основным документом в развитии этой

Статья получена 20 декабря 2017.
И.А.Соколов - Национальный центр цифровой экономики МГУ, ФИЦ «Информатика и управление» РАН (email: isokolov@ipiran.ru)
В.П.Куприяновский - Национальный центр цифровой экономики МГУ (email: vpkupriyanovsky@gmail.com)
В.В. Аленьков - АСЭ ГК Росатом; buildingSmart Россия (email: alenkov@niaep.ru)
О.Н.Покусаев - Центр цифровых высокоскоростных транспортных систем РУТ (МИИТ) (email: oleg@pokusaev.com)
Д.И.Ярцев - BSI (email: dmitry.yartsev@bsigroup.com)
А.В.Акимов - Департамент транспорта и развития дорожно-транспортной инфраструктуры города Москвы (email: akimov_post@mail.ru)
Д.Е.Намиот - МГУ имени М.В. Ломоносова (e-mail: dnamiot@gmail.com)
Ю.В.Куприяновская – Университет Оксфорда (email: Yulia.Kupriyanovskaya@sbs.ox.ac.uk)

темы является, по нашему мнению, документ [9], который имеет очень интересное название: «ПРОМЕЖУТОЧНАЯ СТРАТЕГИЯ НАУКИ КИБЕРБЕЗОПАСНОСТИ & ТЕХНОЛОГИИ: БУДУЩАЯ ИЗОЛИРУЮЩАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ». Приведем небольшую цитату из него:

“Кибербезопасность - это проблема, и технологические изменения. Поэтому важно понять, что есть научно-техническая необходимость:

- избегать рисков, связанных с кибератаками
- создавать следующее поколение кибербезопасности продуктов и услуг, которые необходимы цифровой экономики и
- информировать правительство о том, как политика должна адаптироваться к меняющемуся технологическому ландшафту“

Таким образом, в Великобритании (о чем речь пойдет ниже) был запущен целый процесс изучения инноваций в технологии безопасности, который явился пониманием очень простого факта – нет на сегодня готовых «серебряных пуль», способных решить все проблемы безопасности умных городов. На рисунке 1 мы приводим периодическую таблицу кибербезопасности, составленную ведущими компаниями и учеными этого направления в мире, но то, что она останется именно такой, как мы полагаем, никто не сможет поручиться. Скорее всего, эта таблица будет только расти.

Perimeter Controls		Network Controls		Endpoint Controls		Governance Controls		Data Controls		Industry Controls	
1	Intrusion Detect/Prevent	9	CA/PKI Solutions	17	Anti-Malware Tools	26	Brand Protection	35	Application Security	43	Industry Analysis
2	Data Leakage Prevention	10	Cloud Security	18	Endpoint Security	27	Bug Bounty Support	36	Content Protection	44	Information Assurance
3	Firewall Platform	11	DDOS Security	19	HW/Embedded Security	28	Cyber Insurance	37	Data Destruction	45	Managed Security Svcs
4	Network Access Control	12	Email Security	20	ICS/IoT Security	29	GRC Platform	38	Data Encryption	46	Security Consulting
5	Unified Threat Management	13	Infrastructure Security	21	Mainframe Security	30	Incident Response	39	Digital Forensics	47	Security Recruiting
6	Web Application Firewall	14	Network Monitoring	22	Mobile Security	31	Penetration Testing	40	Identity and Access Mgmt	48	Security R&D
7	Web Fraud Prevention	15	Secure File Sharing	23	Password/ Privilege Mgmt	32	Security Analytics	41	PCI-DSS/ Compliance	49	Training/ Awareness
8	Web Security Gateway	16	VPN/ Secure Access	24	Two-Factor Authentication	33	SIEM Platform	42	Vulnerability Management	50	VAR Security Solns
				25	Voice Security	34	Threat Intelligence				

Рис. 1. Периодическая таблица из пятидесяти элементов управления Cyber Security (источник: TAG Cyber])

II Стандарт PAS 185:2017 по безопасности умных городов

С учетом сказанного выше стоит обратить внимание на название этого стандарта - спецификация для создания и внедрения подхода, ориентированного на безопасность. Таким образом, этот стандарт ориентирован на процесс развития, а не на окончательные решения. Он ссылается [4] на определения и концепции, содержащиеся в публикациях британских и мировых стандартов и дополнениях к ним. Он показывает, как общесистемный, стратегический уровень, подход, ориентированный на безопасность, может применяться наряду с развитием умной городской структуры, стратегией умного города и «дорожной картой», рамками для обмена данными и информационными услугами, а также проектами и данными и / или инициативами по обмену информационными услугами. Связь PAS 185 с установленными ключевыми концепциями в каждом из этих сопроводительных документов показана на рисунке 2. Подход, ориентированный на безопасность, включает в себя рутину применение надлежащей и пропорциональной безопасности меры по сдерживанию и / или пресечению враждебных, злонамеренных мошенничеств и преступного поведения или действия. Кроме того, он считает безопасность целостно, глядя на персональные, физические, кибер и межсекторальные вопросы и решения [4].

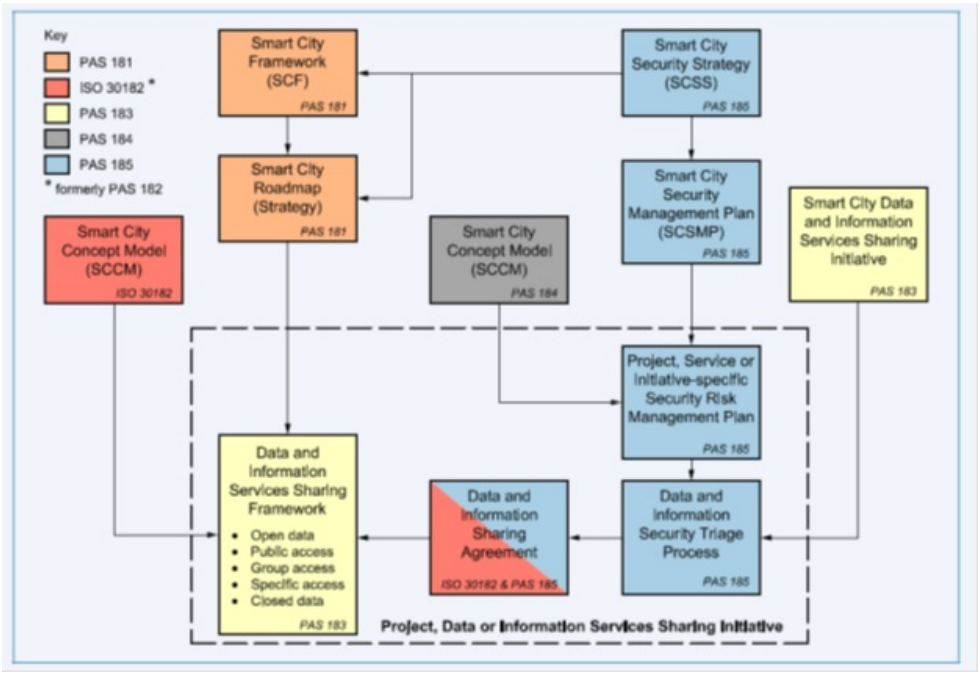

Рис. 2. Интеграция подхода, ориентированного на безопасность [4]

Так как мы затрагиваем в работе тему BIM, приведем прямую цитату из [4]: «PAS 185 также согласуется с изложенным подходом в PAS 1192-5, который относится к управлению информационным моделированием зданий (BIM), цифровым построенным средам и управлению интеллектуальными активами. Такая согласованность обеспечивает совместное использование и раскрытие гео-пространственной, динамической информации об активах для поддержки планирования обслуживания, разработки и предоставления активов и услуг в умных городах.

Если услуга применяется к нескольким активам и / или данным и информация делится или обрабатывается другой городской организацией, этот подход, ориентированный на безопасность установлен в PAS 185. Однако, если служба относится исключительно к построенному активу и данным актива и информация не передается или обрабатывается, другой городской организацией, ряд требований содержащиеся в этом PAS, неприменимы. В тех случаях, когда актив считается чувствительным, ориентированным на безопасность подход, изложенный в PAS 1192-5, может быть реализован».

Так как в 2017 году в России подписана дорожная карта внедрения BIM технологий на уровне правительства, мы посчитали целесообразным привести небольшую выдержку из этого стандарта [5]:

«PAS 1192-5: 2015 - это спецификация для информационного моделирования зданий на основе безопасности (BIM), цифровой строительной среды и интеллектуального управления активами. Она детализирует подход к применению и необходимости соразмерных мер по управлению рисками безопасности, которые влияют на построенный актив в целом или в какой-то его части, а также данные об активах и информации.

Принятие BIM и увеличение использования цифровых технологий в управлении активами, будь то здания или инфраструктура, будет оказывать преобразующей эффект на тех, кто участвует в проектировании, строительстве и управлении. Это будет сделано путем продвижения:

- более прозрачных, открытых способов работы;
- совместной работой разных секторов и обмен информацией; и
- более эффективного управления жизненным циклом активов и работой с данными об их реальном времени использования и состоянии.

PAS 1192-5 описывает процессы, которые помогут организациям в выявлении и реализации соответствующих случаев и принятии соразмерных мер для уменьшения риска потери или раскрытия информации, которые могли бы повлиять на её сохранность и безопасность:

- персонала и других, находящихся в здании лиц, пользователей построенного актива или его сервисов;
- самого построенного актива;
- информации об активах; и / или
- преимущества, которые предоставляет актив

Такие процессы могут быть применены к защите от потери, кражи или раскрытия ценной коммерческой информации и интеллектуальной собственности.

Встраивание инструментов обеспечения качественной безопасности может дать конкурентное преимущество коммерческому предприятию за счёт защиты своих ключевых активов и укрепления доверия заинтересованных сторон и клиентов в услугах и продуктах, которые они предоставляют. Для тех, кто участвует в разработке и поставке новых или модифицированных активов, они могут также улучшить

глобальное позиционирование на международном строительном рынке, особенно для высокопрофильных (сложных) и важных проектов».

Стоит также отметить, что PAS 1192-5 был принят, как и PAS 185:2017, сразу после выпуска стандартов на BIM в Великобритании и его взаимодействие с этими стандартами мы приводим на рисунке 3.

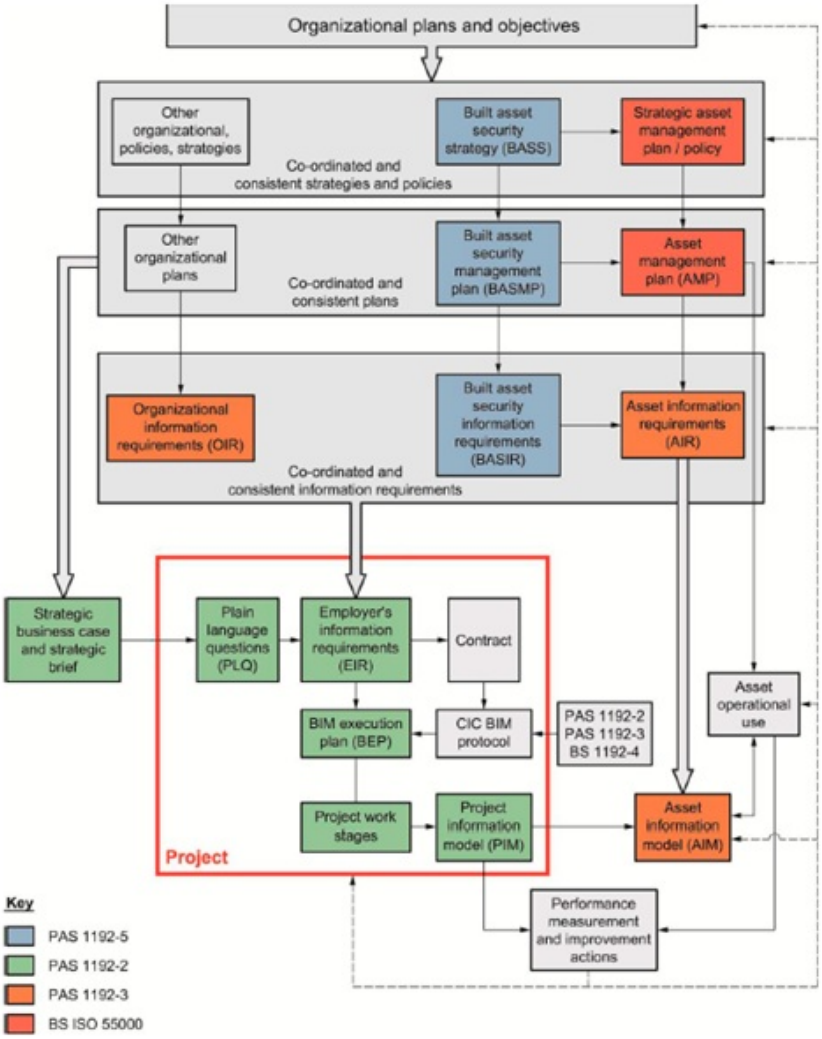

Рис. 3. Взаимодействие PAS 1192-5 с другими стандартами BIM в системе стандартизации Великобритании [5]

Конечно, здания и инфраструктура городов и цифровое знание о них это основа их трансформации в умные города, но основополагающей предпосылкой умных городов является то [4,32], что больше доступности данных и информации, интеграции услуг и систем, а также заключение контрактов на основе этих результатов дают возможность:

a) увеличить пропускную способность, эффективность, надежность и устойчивости и, следовательно, доступности существующих активов для обеспечения расширенного обслуживания своих граждан; а также

b) повысить эффективность проектирования и за счет лучшего понимания на протяжении всего жизненного цикла этих построенных активов уже на месте.

Основная цель умного города - объединить конкретные вертикальные сектора (например, коммунальные услуги, транспорт, здравоохранение и т. д.) через организационные границы в целый город и это подход к созданию, доставке и использованию городом пространств и услуг. Эти изменения должны дать возможность в городе:

1) лучше учитывать потребности текущих и будущих граждан;

2) интегрировать физическое и цифровое планирование;

3) более эффективно и устойчиво идентифицировать, предвидеть и реагировать на возникающие проблемы, в том числе аварийные ситуации; а также

4) увеличить пропускную способность для предоставления услуг и инноваций, которая, в свою очередь, увеличивают производительность и эффективность.

Продвижение в области цифровой техники, информации и коммуникационных технологий являются важными для этих изменений. Однако более широкое использование и зависимость от этих технологий, особенно когда они применяются в сочетании с гораздо более широким использованием и применением городских данных и информации, а также новые модели предоставления услуг, также создает значительные

уязвимости и связанные с ними проблемы с безопасностью. Угрозы, связанные с: организованной преступностью; несанкционированное приобретение личных данных, интеллектуальной собственности и коммерчески чувствительных данных или информации; терроризм; и злонамеренные действия, включая саботаж, которые нарушают или повреждают данные / информацию и / или систем, может использовать эти уязвимости для того, чтобы поставить под угрозу ценность, долговечность и постоянное использование построенных в городе активов и услуг, а также безопасности, как города, так и его граждан [4].

Поэтому подход умного города, ориентированный на безопасность, отличается от любых политик и процессов по безопасности, которые могут уже существовать в пределах отдельных местных органов власти или другой службы поскольку он должна реагировать на новые или расширенные уязвимости, созданные изменениями существующих способов работы. К числу этих уязвимостей относятся [4]:

«i) увеличение объема данных и информации, которые генерируются, собираются, используются и хранятся, включая личные данные, интеллектуальную собственность и коммерчески чувствительные данные и информацию;

ii) более широкое разделение (совместное использование) и распространение данных и информации внутри и между организациями с существующими различными договорными механизмами;

iii) потенциальное агрегирование данных и информации из более широкого круга источников; а также

iv) потенциальные различные организационные приоритеты, механизмы управления политиками и процессами, пониманием проблем безопасности, а также возрастание рисков.

Однако важно, чтобы для любого отдельного и особенного города, ориентированного на этот подход к безопасности он являлся уместным и пропорциональным рискам и не мешал реализации целей города. Кроме того, индивидуальные организационные стратегии и процессы, ориентированные на безопасность следует, в случае необходимости, поддерживать и дополнять этот более широкий подход.

Если умный город должен получить и поддерживать доверие его граждан, то он должен быть способен реагировать на повышение осведомленности граждан и потенциальных проблем о том, как их личные данные используются, и создавать механизмы для предотвращения утери потенциального доверия. Хотя PAS специально написан для умного города и для лиц, принимающих решения, и сотрудников служб умных городских данных, независимо от того, из государственного, частного или третьего секторов они, он может также иметь отношение к тем, кто заинтересован в использовании данных и информации для эффективного достижения целей интеллектуального города».

Для знакомства читателя с подходами, изложенными в PAS 185:2017 [4], которые построены на оценках рисков и их снижении, приведем рисунок 4 о процессе управления рисками для разработки стратегии интеллектуального управления рисками города, и неразрывно с ним связанный рисунок 5 об общем жизненным цикле данных и информации.

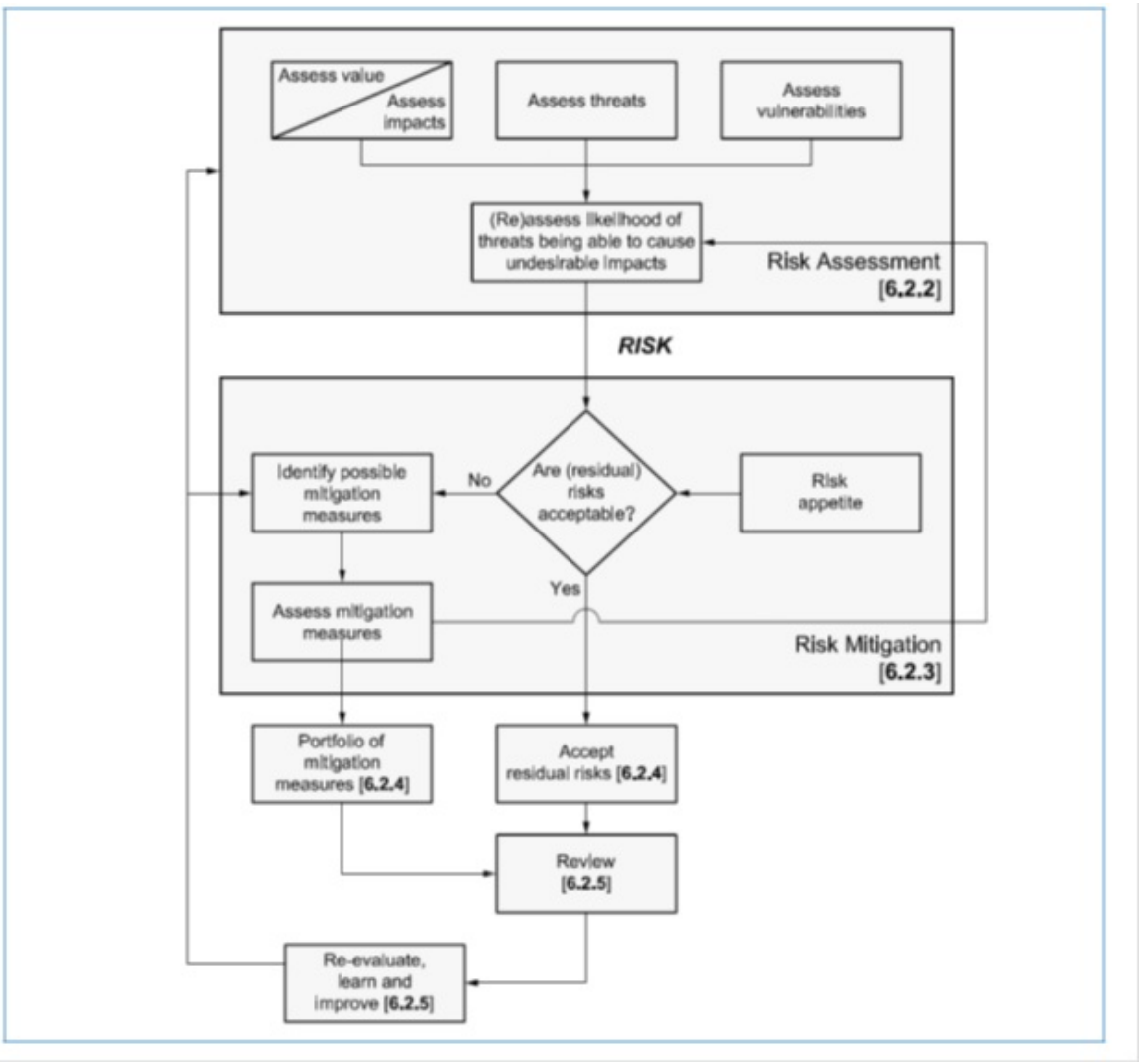

Рис. 4. Процесс управления рисками для разработки стратегии интеллектуального управления рисками города [4]

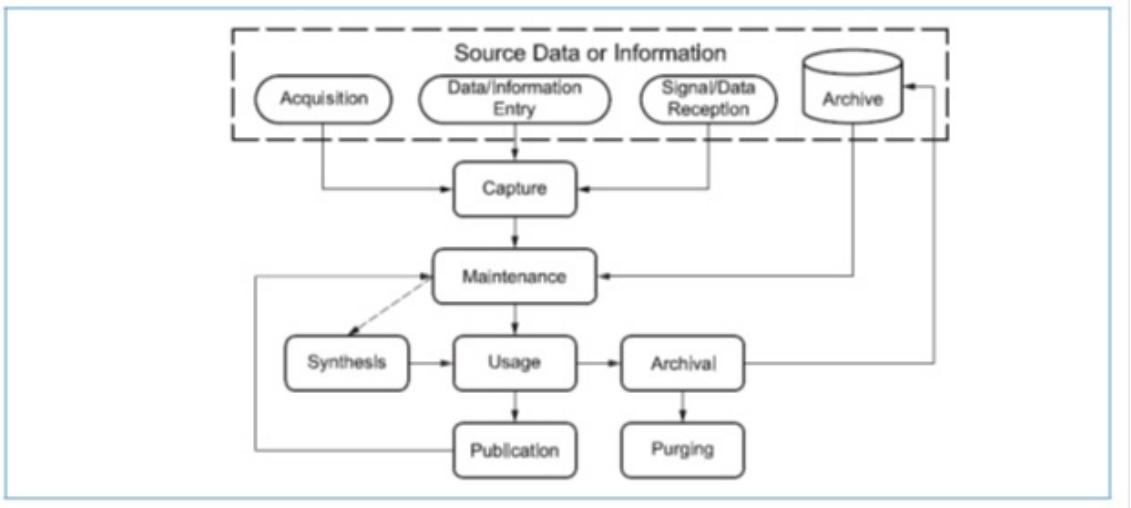

Рис. 5. Общий жизненный цикл данных и информации [4].

III Развитие подходов к решению вопросов по безопасности умных городов в Великобритании и США

Учитывая огромное число угроз (рисунок 1), мы попробуем пояснить ситуацию на примере нескольких технологий, мировая стандартизация которых сегодня уже разворачивается, и те направления, работа с которыми выделена в Великобритании и в США [10-12] для решения проблем безопасности умных городов. Необходимо сказать, что развитие в США и Великобритании этого направления проходит очень скоординировано. Целью политики Великобритании и США является достижение [9] «безопасного по умолчанию состояния в устройствах, которые могут быть захвачены или нарушены, что приведет к утечке

данных или дестабилизированным сетям». В следующих разделах мы приведем те технологические направления, на которых сосредоточены усилия Великобритании и США по достижению цифровой безопасности умных городов.

A. Интернет вещей («IoT»)

Умные устройства, подключенные к Интернету - «Интернет вещей» («IoT») - делают жизнь более удобной, улучшая заводскую эффективность и уже спасают жизни. IoT устройства включаются в потребительские товары, такие как центры домашней автоматизации, видеорегистраторы и сетевые маршрутизаторы, а также заводские системы автоматизации, которые контролируют машины и системы автоматизации зданий, которые регулируют климат здания, управляют различными функциями, включая энергопотребление, бойлерами, аварийными отказам, подачей воды, лифтами и безопасностью контроля доступа. Низкая стоимость и удобство устройств IoT взрывной рост и недавние оценки предполагающие, что более 50 млрд. IoT элементов к 2020 году будут подключены как устройства и по большей части к интернету.

Поскольку эти устройства подключены в Интернете, ими могут быть расположены манипулировать злонамеренные субъекты, также как их законные операторы. Быстрый рост числа устройств IoT ставит подрывные задачи для органов национальной безопасности и обороны, поскольку IoT-устройства представляют новые типы целей, а также новое оружие, угрожающее экономической и физической безопасности. Конечно, огромную роль играет их число и вездесущность.

Эти разрушительные проблемы трудно соотнести с традиционными политиками обороны и безопасности. И цели, и оружие, созданные IoT обычно находятся в частных руках – они не принадлежат, эксплуатируются или даже доступны государственным учреждениям. Когда эти частные системы атакуют или используют для запуска атак, экономические и политические последствия могут быть серьезным, и вне текущих полномочий национальных оборонных властей. Для того чтобы представить уже текущее состояние данных из устройств Интернета (IoT) ,делающие возможными действия и решения влияющие на безопасность мы приводим рисунок 6. Дополнительные сведения можно посмотреть в [18,21]

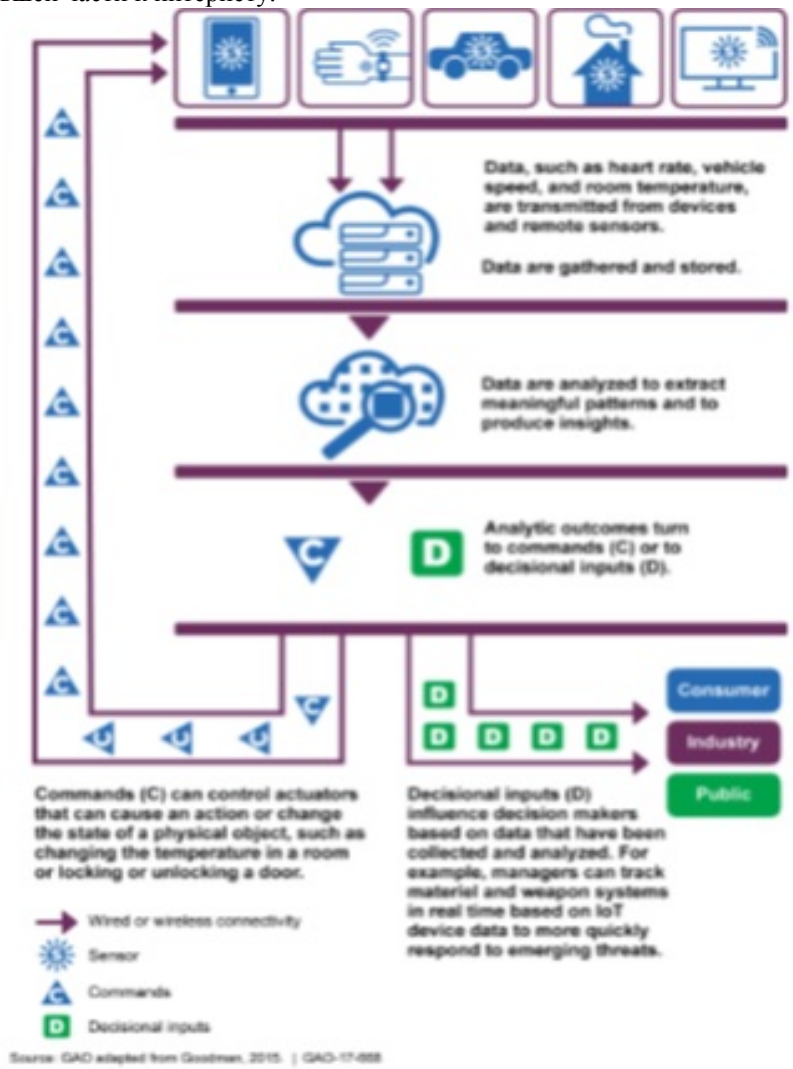

Рис. 6. Данные из устройств Интернета (IoT), делающие возможными действия и решения влияющие на безопасность (источник – GAO)

A. Данные и информация

Вездесущность подключенных устройств будет генерировать огромное количество данных, связанных с ними рисков и возможностей. Данные и информация являются центральными в нашем цифровом обществе. Огромный объем данных и созданные типы данных порождают новые проблемы, и это также верно для информации, которая может быть получена из этих данных.

Большие данные относятся к данным, поступающим с высокой скоростью, в разном диапазоне форматов и в большом количестве, например, данные спутников GPS и радиотелескопов, твиты из Twitter, онлайн-блоги и видеоролики, размещенные на YouTube.

Данные (и информация), которые придут из нашего гиперсвязного мира [17], представят огромные возможности для проведения анализа который революционизирует использование инфраструктуры. Очевидно, что произойдет увеличение сбора данных в частном секторе, вызванного как прямой необходимостью совершенствования бизнес-аналитики и рынка, позволяющего монетизировать такие данные.

С расширением IoT, как средства цифровых трансформаций, это будет только расти. Как эти данные, так и поток информации, который контролируется, и у кого есть доступ к нему, предоставляют ряд возможностей и угроз. Общественность должна иметь уверенность, что данные обрабатываются правильно. В то же время мы не должны уклоняться от использования инструментов, которые мы должны предоставлять общественности и управлять общественной инфраструктурой как можно более эффективнее.

Некоторые ключевые проблемы кибербезопасности в части данных:

- данные должны рассматриваться через весь жизненный цикл - включая соответствующие хранение, защиту, использование и удаление
- данные, собранные для одной цели, могут впоследствии найти другую альтернативу и получить изначально непреднамеренное использование
- данные будут получены из новых и необычных источников, и происхождение этих данных может быть сомнительным.

B. Автоматизация, машиностроение и искусственный Интеллект (AI)

Чтобы в полной мере использовать эти данные, обществу будет необходимо все больше полагаться на автоматизацию, Машиноведение и искусственный интеллект (AI). Автоматизация - это потребность ограничения взаимодействия человека или его полное исключение [36,37].

Это может применяться к системам управления, таким как электростанций и заводы, а также к другим ИТ и процессам, связанных с данными. Автоматизация сочетает датчики и системы управления с тем, чтобы разрешить сложные последовательности операций выполненных во многих разных ситуациях. В данный момент, они варьируются от программ на стиральных машинах до систем автопилота.

Автономные системы - это машины и системы, которые были автоматизированы.

Системы дополненной реальности или автоматизированные системы - это системы со степенью автономии, но где человеческое взаимодействие по-прежнему требуется. Круиз-контроль или автостоянки на автомобиле являются примерами этого. Как автономные, так и расширенные системы будут приобретать все большее значение.

Машинное обучение фокусируется на алгоритмах, которые могут учиться и делать прогнозы на основе данных. Такие алгоритмы работают путем построения модели из данных, чтобы сделать прогнозы или получить решения. Машинное обучение является мощным средством автоматизации. AI шире, чем машинное обучение и является одновременно автоматизацией, но и конечной целью автоматизированной системы.

AI может значительно улучшить производительность; и дать возможности использовать AI в качестве ключевого инструмента для выявления и реагирования на угрозы кибербезопасности.

C. Взаимодействие человека с компьютером

Даже с автоматизацией и дополненной реальностью будет необходимость принятия решений для людей через взаимодействие с машинами или взаимодействие человека и компьютера. Визуальные интерфейсы пользователя являются повсеместными, на настольных компьютерах, ноутбуках, планшетах и мобильных телефонах, а также других электронных устройствах. Распознавание речи становится более распространенным в качестве альтернативы или дополнения к графическим интерфейсам. А также интеграция представления данных с реальными миром, так называемая дополненная реальность, уже присутствует в ограниченном числе приложений (в основном картографирование и игры). Эта технология все больше и больше будет использоваться для людей, так как они быстрее понимают и взаимодействуют с их окружением.

Эти технологии будут иметь широкие последствия и будет влиять на целый ряд областей политики. Для кибербезопасности они представляют риски, которые должны быть решены: через человеческие уязвимости хакеры будут все чаще внедряться в цифровые сети, и надежная аутентификация будет иметь решающее значение.

D. Организационные формы в Великобритании и в США

В Великобритании 14 февраля 2017 года Национальный центр кибербезопасности (NCSC) был официально открыт Ее Величеством Королевой. Этот центр не был создан на пустом месте. Способность

государственных ведомств надежно и безопасно общаться друг другом в цифровом виде открылась в 1997 году с введением правительственной безопасности Интранет (GSi). Это открыло сотрудникам министерств и их агентствам возможность обмена информацией в электронном виде, сокращая традиционные ограничения, которые ранее замедляли работу государства.

Эта способность для правительства безопасно и надежно общаться по вопросам критических инфраструктур увеличилась в 1999 году после создания Координационного центра национальной безопасности инфраструктур (NISCC). Основной целью его создания было свести к минимуму любую угрозу для критических национальных инфраструктур путем предоставления консультаций и информации о том, как сохранить максимальную безопасных компьютерных сетей от растущих угроз электронных атак. NISCC в конечном итоге был объединен с Центром по защите национальных инфраструктур (CPNI) в 2007 году, который и по сей день предлагает советы по организации инфраструктур, от которых зависит нация.

В ответ на растущую потребность в защите национальной безопасности и защиты общественности онлайн, в 2011 году была создана стратегия кибербезопасности Великобритании. И положительные, и отрицательные последствия внедрения цифровых технологий продолжали расти почти десятилетие, и в 2016 произошло создание Национального правительственного центра кибербезопасности (NCSC) с видением, которое поможет сделать Великобританию самым безопасным местом для жизни и ведения бизнеса в Интернете. NCSC был создан как мост между промышленностью и правительством, предоставляя единый источник советов, рекомендаций и поддержки по кибербезопасность, в том числе управлению киберинцидентами по безопасности.

Национальный центр кибербезопасности (NCSC) является частью GCHQ и является авторизованным органом Великобритании по кибербезопасности. NCSC объединяет и заменяет три существующие организации по кибербезопасности - Центр кибер-оценки (CCA), Компьютерную группу реагирования на чрезвычайные ситуации в Великобритании (CERT UK) и CESG (подразделение информационной безопасности GCHQ) – и включает обязанности, связанные с Центром защиты национальной инфраструктуры (CPNI). Необходимо сказать, что NCSC (The National Cyber Security Centre) вслед за другими министерствами и ведомствами сам «уходит в киберпространство», происходит отказ от форматов «электронной бумаги» (PDF) и публикации в электронной форме происходят все чаще в формате HTML, поэтому многое из изложенного собрано с сайта NCSC https://www.ncsc.gov.uk/, на который мы и отсылаем нашего читателя.

В США Национальный центр кибербезопасности (NCCoE), входящий в состав Национального института стандартов и технологий (NIST), также имеет очень богатый сайт https://nccoe.nist.gov/about-the-center (в США переход на новые формы публикаций в интернете не так развит, как в Великобритании). Он является совместным центром, в котором отраслевые организации, государственные учреждения и академические учреждения работают вместе для решения наиболее острых проблем кибербезопасности бизнеса. Это государственно-частное партнерство позволяет создавать практические решения для кибербезопасности для конкретных отраслей промышленности, а также для широких межсекторальных технологических задач. Через консорциумы в рамках Соглашений о совместных разработках и разработках (CRADAs), включая партнеров по технологиям - от лидеров рынка Fortune 50 до небольших компаний, специализирующихся на обеспечении безопасности ИТ, NCCoE применяет стандарты и передовые методы для разработки модульных, легко адаптируемых примеров решений для кибербезопасности с использованием имеющейся в продаже технологии. NCCoE документирует эти примерные решения в серии NIST Special Publication 1800, которая отображает возможности в NIST Cyber Security Framework и детализирует шаги, необходимые для повторного создания примера решения для другого объекта. NCCoE была создана в 2012 году NIST в партнерстве со штатом Мэриленд и графством Монтгомери, штат Мэриленд. Библиотека разработанных документов центра и NIST находится по адресу https://nccoe.nist.gov/library?title=&field_library_type_value=All&field_project_reference_target_id=All откуда мы приведем наиболее заинтересовавшие нас сегодняшние решения.

E. Примеры

Принцип «безопасного по умолчанию « предполагает, что есть процедуры подготовки безопасных решений в сотрудничестве с теми компаниями, которые их создают. Поэтому спектр таких разработок необычайно широк и затрагивает практически все отрасли экономики. Приведем несколько примеров.

1) Цифровая медицина

Приведем пример из разработок по безопасности в цифровой медицине. Он касается инфузионных насосов [14]:

«Технологические достижения внесли свой вклад в феномен Интернета вещей (IoT) , где у физических устройств теперь есть технология, позволяющая им подключаться к Интернету и общаться с другими устройствами или системами. С подключением к Интернету миллиардов устройств, многие отрасли, в том числе здравоохранение, начинают использовать инструменты IoT для повышения операционной эффективности и улучшения инноваций.

Медицинские устройства, такие как инфузионные насосы, когда-то были автономными инструментами,

которые взаимодействовали только с пациентом или медицинским поставщиком. Благодаря технологическим усовершенствованиям, направленным на улучшение ухода за пациентами, эти устройства теперь беспроводным образом подключаются к различным системам, сетям, и другим инструментам в организации доставки медицинских услуг (HDO) - в конечном итоге способствуют развитию Интернета в медицине (IoMT) .

По мере роста IoMT риски кибербезопасности повысились. По данным Ассоциации Технического информационного отчета (AIRI) 57 (TIR57) «это создало новый источник риска для безопасной работы медицинских устройств». В частности, радиоиндустрия (насос, сеть и данные, хранящиеся в насосе и на нем) сталкиваются с рядом угроз, включая несанкционированный доступ к защищенной медицинской информации (PHI), изменения предписанных доз препарата и вмешательство в функцию насоса.

Помимо управления взаимосвязанными медицинскими устройствами, HDOs контролируют сложные, высоко технические среды, из бэк-офисных приложений для биллинговых и страховых услуг, управления цепочками поставок и инвентаря и планирования персонала в таких клинических системах, как радиологическая (radiological) и фармацевтическая поддержка. В этой сложной среде здравоохранения производители HDOs и медицинских устройств, которые разделяют ответственность и берут совместный, целостный подход к снижению рисков кибербезопасности для экосистемы инфузионного насоса, могут лучше защитить системы здравоохранения, пациента, PHI и корпоративную информацию.

Национальный центр кибербезопасности передового опыта (NCCoE) в Национальном институте стандартов и технологии (NIST) проанализировал факторы риска в экосистеме инфузионного насоса и вокруг него, используя оценку риска на основе анкетирования. По результатам этой оценки, NCCoE затем разработал пример реализации, который демонстрирует, как HDO могут использовать основанные на стандартах коммерчески доступные технологии кибербезопасности для лучшей защиты экосистемы инфузионного насоса, включая информацию о пациентах и пределы дозировки библиотеки лекарств".

2) Бизнес гостеприимства или гостиничный бизнес

Бизнес гостеприимства или гостиничный бизнес относится к сектору экономики, который уже прошел значительную цифровую трансформацию. Приведем пример из [16]:

"Гостиничные организации полагаются на системы управления имуществом (PMS) для ежедневных задач, планирования и ведения записей. В качестве операционного концентратора PMS взаимодействует с несколькими службами и компонентами в ИТ-системе отеля, например, системами Point-of-Sale (POS), дверными замками, сетями Wi-Fi и другими приложениями для гостевых сервисов. Помимо сложностей соединений, компоненты и сервисы внешних бизнес-партнеров также обычно подключаются к PMS, например, на локальных курортах или ресторанах, онлайн-агентам путешествий и партнерам по управлению взаимоотношениями с клиентами или приложениям (локальные или облачные). Многочисленные подключения и пользователи PMS могли бы обеспечить более широкую область для атаки со стороны злоумышленников. Демонстрация методов повышения безопасности PMS может помочь защитить бизнес от сетевых вторжений, которые могут привести к нарушениям данных и мошенничеству.

Основываясь на отраслевых исследованиях и в сотрудничестве с заинтересованными сторонами индустрии гостеприимства, NCCoE начинает проект, целью которого является оказание помощи организациям гостеприимства в реализации более сильных мер безопасности внутри и вокруг PMS. При этом особое внимание уделяется системе POS, посредством сегментации сети, точка-точка шифрования, токенизации данных, многофакторной аутентификация (MFA) для удаленного и партнерского доступа, анализа поведения сети и пользователя и ограничения использования только для бизнеса.

В сотрудничестве с бизнес-сообществом гостеприимства и поставщиками технологий, которые внедряют стандарты, повышающие кибербезопасность, NCCoE будет изучать методы повышения безопасности PMS и ее соединений и разработает пример реализации, состоящий из компонентов с открытым исходным кодом и коммерчески доступных компонентов. Этот проект подготовит руководство по практике кибербезопасности NIST - свободно доступное описание решения и практические шаги, необходимые для эффективной защиты PMS и его многочисленных соединений в ИТ-системе отеля".

3) Геолокация

Геолокация уже составляет основу множества сервисов и услуг в цифровой экономике и, несомненно, будет развиваться в будущем. Приведем пример работ в этом направлении [15]:

«Организации часто должны использовать облачные серверы, физически расположенные в своих собственных странах или где их данные генерируются и обрабатываются. Определение приблизительного физического местоположения объекта, такого как сервер облачных вычислений, обычно называется геолокацией. Геолокация для облачных серверов может быть достигнута разными способами с 6-кратной степенью точности, но традиционные методы геолокации не обеспечены безопасностью, а она обеспечивается посредством управления и оперативного контроля, которые не могут быть автоматизированы и масштабированы. Традиционные методы геолокации зависят от людей и процессов, которым нельзя доверять, чтобы удовлетворить потребности облачной безопасности.

Мотивация этого строительного блока (Building Block) заключается в повышении безопасности облачных вычислений и ускорении внедрения технологий облачных вычислений путем создания автоматизированных корневых компонентов корневого метода доверия для обеспечения соблюдения и мониторинга ограничений геолокации для облачных серверов.

Ключ доверия к аппаратным средствам - это надежная комбинация аппаратного обеспечения и прошивки, которая поддерживает целостность геолокационной информации и платформы. Аппаратный корневой центр доверия помещается в организации, с уникальным идентификатором хоста и метаданными платформы, хранящимися в защищенном от несанкционированного доступа аппаратном обеспечении. Эта информация доступна с помощью средств управления и безопасности с помощью защищенных протоколов, чтобы подтвердить целостность платформы и подтвердить местоположение хоста.

После того, как облачная платформа была подтверждена, чтобы быть надежной и соответствовать определенной политике геолокации, тогда могут быть созданы другие свойства использования для поддержки дополнительных возможностей безопасности, которые построены на основе этого основополагающего корневого узла доверия. Одним из вариантов использования является возможность разрешить перенос рабочих нагрузок из локального центра данных в центр обработки данных провайдера, размещенный в Интернете, чтобы воспользоваться преимуществами общедоступных облачных ресурсов. Кроме того, в поддержку разных случаев использования могут быть применены различные наборы политик. Во-первых, возможности защиты данных могут быть реализованы так, что рабочие нагрузки дешифруются только после того, как платформы хостинга будут измерены и соответствуют политике геолокации. Во-вторых, сетевые потоки данных между компонентами рабочей нагрузки могут быть изолированы во время выполнения в поддержку организованной организацией политики сегментации в общих средах. Наконец, свойства обеспечения безопасности могут автоматически оцениваться и применяться для поддержки отраслевых инфраструктур управления рисками и связанных с ними средств контроля безопасности.

4) Предыстория

Общие технологии облачных вычислений разработаны с высокой гибкостью и удобством, прозрачно используя любые доступные ресурсы для обработки рабочих нагрузок для своих клиентов. Тем не менее, существуют проблемы безопасности и конфиденциальности, связанные с совместным использованием ресурсов и позволяющие неограниченную миграцию рабочей нагрузки. Всякий раз, когда несколько рабочих нагрузок присутствуют на одном облачном сервере, необходимо отделить эти рабочие нагрузки, чтобы они не мешали друг другу, не позволяли получать доступ к конфиденциальным данным друг друга. В противном случае можно скомпрометировать безопасность или конфиденциальность других рабочих нагрузок. В качестве примера рассмотрим две конкурирующие компании с рабочими нагрузками на облачной платформе с несколькими арендаторами; каждая компания хотела бы удостовериться, что серверу можно доверять, чтобы защитить свою информацию от других компаний. Аналогичным образом, одна организация может иметь несколько рабочих нагрузок, которые должны быть разделены на две части из-за различных требований безопасности и потребностей для каждой рабочей нагрузки, например, изолирования регулируемой рабочей нагрузки от рабочей нагрузки, ориентированной на общественность.

Еще одна проблема с общими облачными вычислениями заключается в том, что рабочие нагрузки могут перемещаться из облачных серверов, расположенных в одной стране, на серверы в другой стране. Каждая страна имеет свои законы для обеспечения безопасности данных, конфиденциальности и других аспектов информационных технологий (ИТ). Поскольку эти законы могут противоречить политике или мандатам организации (например, законам, нормам), организация может решить, что ей необходимо ограничить, какие облачные серверы используют в каждой стране".

F. Вызовы безопасности в недалеком будущем

Широкий спектр вопросов безопасности умных городов, а также быстрое развитие и освоение новых технологий ставит задачи изучения того, что, наиболее вероятно, затронет эту отрасль в будущем. Все более высокий стимул для кибератаки будет соответствовать растущему числу потенциальных нападающих. Разрыв между развитым и развивающимся миром, в котором во многом цифровые технологии все еще находятся в зачаточном состоянии, будет быстро уменьшаться из-за падения затрат, связанных с технологией. Использование доступного Интернета быстро растет в Азии, Африке и на Среднем Востоке, и некоторые аналитики прогнозируют, что глобальный уровень компьютерной грамотности достигнет 90% к 2025 году. Вероятно, кибер-безопасность будет испытывать феномен «качелей», технологическим развитием, дающим толчок верх то правонарушениям, то защите.

Быстро растущая зависимость от Интернета правительствами, предприятиями и отдельные лица шпионаж и наступательные кибер-способности становятся привлекательными для большего количества государств и организаций.

Приведем несколько таких главных вызовов почерпнутых из исследований NCSC и NCCoE .

1) Квантовые технологии

Спустя тридцать лет после того, как они были впервые предложены, квантовые компьютеры остаются

в значительной степени теоретическими. Но, учитывая прогресс, возможно, что квантовые компьютеры смогут выйти из лаборатории в следующем 10 лет.

Если это будет так, квантовая обработка могла бы дать возможность быстро взломать ключи открытого ключа технологии шифрования, что потребует нового подход к безопасности. Квантовая технология радикально отличается процессорами, которые могли бы работать в миллионы раз быстрее, чем то, что используются сегодня.

2) 4 000 низкоорбитальных спутников

Сегодняшний спутниковый интернет дорог и имеет большую задержку (время между данными которые были отправлены и получены) из-за высоких орбит этих аппаратов. Это делает его плохим вариантом для многих приложений, таких как игры, видеоконференцсвязь, прямая трансляция и просмотр онлайн.

Но сегодня спутники разрабатываются для доставки Интернета по всему миру намного дешевле и быстрее (связь с землей осуществляют приемники с использованием радиочастотного спектра). В конечном итоге могут быть задействованы около 4000 спутников на низкой околоземной орбите. Оценки показывают, что латентность на этой высоте была бы сопоставимой с /или лучше существующего широкополосного решения, которые используют сеть оптических кабелей, проложенных на земле и на морском дне. Можно также посмотреть работу [17] о причинах этого.

3) Интернет Вещей (IoT) и Интернет "меня"

IoT относится к подключению всего в Интернет. Все, что связано с этим цифровая сети мобильных устройств, носимые, потребительская и бытовая электроника, автомобили, датчики окружающей среды и многое другое могут взаимодействовать с людьми, социальными сообществами, правительствами, систем управления и бизнесом. Информация выходит за рамки текстовых, аудио и видео форматов, и начинает включать сенсорную и контекстуальную информацию. Хотя это создает новые возможности, это также представит многие новые испытания для безопасности.

Местоположение - ключевая услуга, которая лежит в основе большинство услуг и приложений в Интернет Вещей. Носимые технологии, смартфоны и даже автомобили найдут новые пути использовать геолокацию как услугу. Стремление к сервисам, основанным на местоположении, таргетинг рекламы и сегментация рынка приведет к новым достижениям того, как география и наше путешествие повлияют на наш онлайн-опыт. Интернет всего будет скроен для каждого пользователя, с предпочтениями и привычками от ряда датчиков - от центрального отопление, социальных сетей до биофизических. Это будет создавать захватывающие новые способы обеспечения индивидуального, личный опыт для потребителей.

4) Облако контекста

Точно так же произойдет изменение от «больших данных», к «богатым данным», которые будут питаться контекстом и быть фокусными. Контекст, генерируемый аналитическими суждениями, справочные данные и историческое понимание, необходимы для обогащения новых данных и автоматического соединения их вместе.

Контекст предоставит новые способы для запросов и аналитики, которые будут построены на основе поведения, демографии, географии и социальной идентичности.

5) Виртуальные базы данных

Постоянная эволюция сетей будет вероятно, приведет к разработке «Семантической сети». Машины буду узнавать, выявлять, захватывать, манипулировать и интерпретировать данные с минимальным или даже отсутствующим человеческим вмешательством. Эта беспрецедентная скорость и уровень доступа может быть использован с помощью методов рассуждений и выводов для более сложных форм анализа на онтологическом и семантическом уровнях.

6) Автономные агенты

Автономные агенты автоматически проанализируют в реальном времени огромные объемы данных. Выполняя сканирование через разрозненные наборы данных, они будут обеспечить алгоритмы ранжирования и укладки продвигать и вычислять заранее ценное понимание.

Руководствуясь рекомендациями аналитиков и глубокими технологиями обучения, они будут меняться и адаптироваться по-новому, чтобы находить информацию, оценивать и прогнозировать будущие состояния.

7) Цифровые аборигены в связанной рабочей силе

Любой, у кого есть малыш и планшет, знает, что эта технология настолько встроена в следующее поколение, что использование ее придет естественно.

Интернет находится в центре подключенной рабочей силы. Сотрудники могут разрабатывать и учиться из всех тех же источников и платформ, доступных для потребителей, в безопасной и стабильной манере.

Работа и жизнь будут сбалансированы с возможностями общаться и использовать современные технологии и инструменты. Сотрудники будут таким образом «цифровыми аборигенами», осваивая технологии для любых целей, и имеющие способности использовать эти знания и опыт или дать рекомендации для любых потенциальных полезностей.

8) Получение соответствия через биометрию

Эта технология часто подвергалась критике за ее влияние на наше здоровье, но сегодня она вызывает большой оптимизм.

Биометрия - уже значительная область роста. В ожидании изменений того что, датчики биологической обратной связи станут проникать в соответствие личности и появится основанное на данных понимание биологии, тогда проблемы безопасности неизбежно

возникнут в этом фундаментальном интерфейсе между человеком и машиной.

IV Выводы

Развитие в России цифровой экономике определено решениями Президента РФ [1,2,3], и тема умных городов уже вошла в программы ее развития. Вместе с тем, авторам представляется, что в этом, безусловно, важном и нужном деле необходим всесторонний учет уже достигнутого в мире и быстрое освоение необходимого.

Как умные города, так и их безопасность - это фактически почти вся цифровая экономика в миниатюре. Для того, чтобы двигаться вперед, мы выбрали опыт Великобритании и США, хотя и ЕС с некоторым запозданием двигается в том же направлении.

Зачастую в таком движении проблемы безопасности просто игнорируются, а регламенты отстают. Проблемы цифрой экономики России - это общие проблемы всех нас, и их необходимо обсуждать и решать сообща.

Библиография

[1] Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации « от 1 декабря 2016 года № 642

[2] Указ Президента Российской Федерации «О стратегии развития информационного общества в Российской Федерации» от 9 мая 2017 года № 2013

[3] Указ Президента Российской Федерации «О стратегии экономической безопасности Российской Федерации на период до 2030 года» от 13 мая 2017 года № 208

[4] PAS 185:2017. Smart Cities – Specification for establishing and implementing a security-minded approach. BSI 2017 First published November 2017

[5] PAS 1192-5: 2015 Specification for security-minded building information modelling, digital built environments and smart asset management. BSI May 2015

[6] 2018 TAG Cyber Security Annual volumes 1 outlook for fifty cyber security control Copyright © 2018 TAG Cyber LLC.

[7] National Cyber Security Centre (NCSC). Digital service security – Guidance. October 2016. Available from: https://www.ncsc.gov.uk/guidance/digital-servicesecurity [viewed November 2017]

[8] Cabinet Office. Government Security Classifications. Available from: https://www.gov.uk/government/publications/government-securityclassifications [viewed November 2017]

[9] INTERIM CYBER SECURITY SCIENCE & TECHNOLOGY STRATEGY: FUTURE-PROOFING CYBER SECURITY. CABINET OFFCE 2017

[10] DoD Policy Recommendations for The Internet of Things (IoT). Chief Information Officer. U.S. Department of Defense. December 2016

[11] Fostering the advancement of the internet of things. The department of commerce. Internet policy task force & digital economy leadership team. January 2017.

[12] Strategic Principle for securing the internet of things (IoT). U.S. Departament of Homeland Security. Version 1.0, November 15, 2016

[13] National Cyber Security Centre Overview Crown copyright 2017

[14] NIST SPECIAL PUBLICATION 1800-8 Securing Wireless Infusion Pumps In Healthcare Delivery Organizations Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C) Gavin O'Brien National Cybersecurity Center of Excellence Information Technology Laboratory Sallie Edwards Kevin Littlefield Neil McNab Sue Wang Kangmin Zheng The MITRE Corporation McLean, VA DRAFT May 2017

[15] TRUSTED GEOLOCATION IN THE CLOUD Mike Bartock Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Murugiah Souppaya Computer Security Division Information Technology Laboratory National Institute of Standards and Technology DRAFT May 11, 2017

[16] SECURING PROPERTY MANAGEMENT SYSTEMS Cybersecurity for the Hospitality Sector William Newhouse National Cybersecurity Center of Excellence National Institute of Standards and Technology Michael Ekstrom Jeff Finke Sarah Weeks The MITRE Corporation. September 13, 2017.

[17] Куприяновский В. П. и др. ГИГАБИТНОЕ ОБЩЕСТВО И ИННОВАЦИИ В ЦИФРОВОЙ ЭКОНОМИКЕ //Современные информационные технологии и ИТ-образование. – 2017. – Т. 13. – №. 1. – С. 105-131.

[18] Kupriyanovsky V. et al. Web of Things and Internet of Things in the Digital Economy //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 5. – С. 38-45.

[19] Соколов И. А. и др. Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 7.

[20] Куприяновский В. П. и др. ЦИФРОВАЯ ЖЕЛЕЗНАЯ ДОРОГА–ERTMS, BIM, GIS, PLM И ЦИФРОВЫЕ ДВОЙНИКИ //Международный научный журнал «Современные информационные технологии и ИТ-образование». – 2017. – Т. 13. – №. 3. – С. 129-166.

[21] Kupriyanovsky V. et al. Digital Economy and the Internet of Things-negotiating data silo //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 8. – С. 36-42.

[22] [40] Kupriyanovsky V. et al. Digital Economy= data models+ big data+ architecture+ applications? //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 5. – С. 1-13.

[23] Куприяновский В. П. и др. Умная инфраструктура, физические и информационные активы, Smart Cities, BIM, GIS и IoT //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 10.

[24] Куприяновский В. П. и др. Семантика, метаданные и онтологии в приложениях для умного города-новые стандарты BSI //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.

[25] Kupriyanovsky V. et al. On Localization of British Standards for Smart Cities //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 7. – С. 13-21.

[26] Куприяновский В. П. и др. Стандарты для создания дорожных карт умных городов на примере BSI //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 8.

[27] Drozhzhinov V. et al. Smart Cities: models, tools, rankings, and standards //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 3. – С. 19-48.

[28] Куприяновский В. П., Намиот Д. Е., Куприяновский П. В. On standardization of Smart Cities, Internet of Things and Big Data. The considerations on the practical use in Russia //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2. – С. 34-40.

[29] Namiot D. et al. Smart Cities and education in digital economy //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 3. – С. 56-71.

[30] Куприяновский В. П. и др. Smart Cities as the" capitals" of the Digital Economy //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2. – С. 41-52.

[31] Namiot D., Sneps-Sneppe M. On the domestic standards for Smart Cities //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 7. – С. 32-37.

[32] Намиот Д. Е., Куприяновский В. П., Синягов С. А. Info-communication services in the Smart City //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 4. – С. 1-9.

[33] Добрынин А. П. и др. The Digital Economy-the various ways to the effective use of technology (BIM, PLM, CAD, IOT, Smart City, BIG DATA, and others) //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 1. – С. 4-11.

[34] Ярцев Д. И. и др. Экономика стандартизации в цифровую эпоху и информационно-коммуникационные технологии на примере Британского института стандартов //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 6.

[35] Куприяновский В. П., Намиот Д. Е., Куприяновский П. В. On standardization of Smart Cities, Internet of Things and Big Data. The considerations on the practical use in Russia //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2. – С. 34-40.

[36] Соколов И. А. и др Искусственный интеллект как стратегический инструмент экономического развития страны и совершенствования ее государственного управления. Часть 1. Опыт Великобритании и США //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 9.

[37] Соколов И. А. и др. Искусственный интеллект как стратегический инструмент экономического развития страны и совершенствования ее государственного управления. Часть 2. Перспективы применения искусственного интеллекта в России для государственного управления //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 9.

[38] Куприяновский В.П. и др. Интеллектуальная мобильность и мобильность как услуга в Умных Городах //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 12.

[39] Sokolov I. et al. On opportunities for the development of the digital railway as a base for a multimodal transport system of smart cities in the digital economy //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 12. – С. 60-76.

On digital security of smart cities

Igor Sokolov, Vasily Kupriyanovsky, Vyacheslav Alenkov, Oleg Pokusaev, Dmitry Yartsev, Andrey Akimov, Dmitry Namiot, Yulia Kupriyanovsky

***Abstract*— The article deals with issues related to digital security in the Smart City. The standards and implementations of Smart City models are geared towards the application of rapidly developing digital technologies and are aimed at economic, social, environmental and other positive effects when applying digital technologies in cities. The introduction of such innovations, in fact, not only transforms the urban lifestyle at an incredibly fast pace and gives huge advantages to the inhabitants of cities, but is also accompanied by completely new digital threats and dangers. The article discusses the standard BSI PAS 185 - a specification for creating and implementing a security-oriented approach. Thus, this standard is focused on the development process, rather than on final decisions. The work of the National Center for Cyber-security of Great Britain is also examined in detail.**

***Keywords*— security, Smart City, BSI, PAS-185.**