РИСКОГЕННЫЕ АСПЕКТЫ РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ

Екадумова Ирина Ивановна
Белорусский государственный университет, Минск

Информационно-коммуникационные технологии (ИКТ), призванные обеспечить комфорт повседневной жизни человека и эффективность его деятельности, выступают одним из факторов его уязвимости. Развитие ИКТ привело к возникновению новых инструментов воздействия на людей – устройств, участвующих в коммуникации по принципу m2m (*machine-to-machine*). В Рекомендациях Международного союза электросвязи МСЭ-Т Y.2060 интернет вещей (ИВ) определяется как «глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий» [5]. При этом под вещью понимается «физический объект (физическая вещь) или объект виртуального (информационного) мира (виртуальная вещь, например, мультимедийный контент или прикладная программа), которые могут быть идентифицированы и объединены через коммуникационные сети» [5].

Предпосылками развития ИВ стали снижение цен на передачу данных, рост числа устройств, подключаемых к глобальной сети, а также развитие больших данных и облачных вычислений. Сегодня половина населения Земли пользуется доступом к интернету при помощи миллиардов «умных» устройств, которые обрабатывают данные и обмениваются ими в глобальной сети. ИВ используется в сфере энергетики, здравоохранения, образования, управления производством и материальными ценностями, «умных городов», контроля за состоянием окружающей среды, а также в быту.

Использование технологий ИВ способствует экономическому росту и повышению качества жизни людей. Как отмечается в пресс-релизе Международного союза электросвязи (МСЭ), это происходит благодаря их доступности, приемлемости в ценовом отношении и масштабируемости. Доступность означает распространенность на рынках, дешевизну, легкую заменяемость при наличии инфраструктуры поддержки (Wi-Fi, интернет-кафе и т. д.) и приспособленность к работе в сложных условиях. Приемлемость по цене предполагает, что затраты на исследования и разработки в области ИВ покрываются за счет большого спроса на рынках, а их адаптация к условиям рынков развивающихся стран не слишком затратна. Масштабируемость состоит в особенности конструкции ИВ, которая обеспечивает возможность очень простого автоматического конфигурирования без участия опытных специалистов в установке и техническом обслуживании [1].

Любой пользователь «умного» устройства во многом непреднамеренно занимается сбором данных о себе, создавая тем самым риски, связанные с раскрытием собранной информации как сегодня, так и в будущем [3].

Использование «умных» устройств сопряжено с проблемой баланса удобства и информационной безопасности, что предопределяет особые требования к их устойчивости и надежности. Такие устройства должны быть защищены от взлома и выведения из строя. Между тем, для многих из них нет защитных решений, поскольку их производители редко выпускают обновления безопасности и новые прошивки [4]. При сегодняшнем уровне защиты интернет-устройств хакеры способны не только взламывать их, но и собирать из них мощные ботнеты. Для упреждения подобных проблем в будущем в Евросоюзе используется юридическое закрепление минимума требований к безопасности «умных» устройств и их сертификация. Для сотрудничества правительственных и коммерческих структур в этом направлении создан Альянс для инноваций в интернете вещей [10].

Угрозы интересам пользователей интернета вещей могут исходить не только от злоумышленников, но и от правительств. Примечателен в этом отношении опыт внедрения системы социального кредитования в Китае, где с 2014 года цифровые технологии используются для создания рейтинга граждан, на основе которого одни граждане будут поощряться льготами, а другие наказываться административным санкциям и ограничениями. Информация для рейтинга собирается усилиями государственных органов, частных организаций и самих граждан. Источниками информации (о покупках, доходах, посещаемых местах, интересах и круге общения, предпочитаемом контенте и т. п.) являются также мобильные устройства [2]. Хотя проект задумывается для предотвращения угрозы дезорганизации общества, страдающего от дефицита доверия, его внедрение сопряжено с серьезными рисками, по меньшей мере, по двум причинам. Во-первых, алгоритмы вычисления рейтингов не прозрачны, а основания поощрений и наказаний прописаны в законодательстве довольно смутно. Следовательно, граждане не застрахованы от ошибок и произвола в принятии важных для них решений. Во-вторых, система определения надежности граждан не распространяется на высшее руководство, что, по мнению южнокорейских экспертов, может превратить ее в инструмент тотального контроля правительства над обществом [9].

Риски, сопряженные с развитием ИВ, во многом обусловлены препятствиями на пути его развития – прежде всего, чрезмерным многообразием протоколов при отсутствии единых общепринятых стандартов, проблемами энергопитания подключенных устройств, психологической неготовностью людей использовать «умные» устройства. Их существование создает запрос на развитие страхования в сферах деятельности, связанных с использованием ИВ. Так, в России обсуждается страхование рисков в области защиты информации в рамках государственной программы «Цифровая экономика». Предполагается, что полисы информационной безопасности будут введены на обязательной основе с 2020 года для отдельных отраслей экономики, таких как банковская сфера, аэропорты, вокзалы и стратегические отрасли промышленности – металлургия, машиностроение, судостроение, авиапром и др. [7].

Помимо намеренных действий людей, опосредованных использованием «умных» устройств, актуальной проблемой является риск утраты контроля над ними. Эта проблема стала насущной в свете разработок военного назначения. Ведущие специалисты в области робототехники и искусственного интеллекта сегодня прилагают усилия по привлечению к этой проблеме внимания международной общественности. Так, в августе 2017 г. 26 представителей кампаний, занимающихся созданием искусственного интеллекта и робототехникой, написали открытое письмо в Организацию объединенных наций, в котором призвали запретить разработку и использование систем смертоносного автономного оружия. Авторы письма отмечают, что подобное оружие грозит стать новой революцией в военном деле и создает угрозу развития вооруженных конфликтов более масштабных, чем ранее, и слишком стремительных, чтобы люди успели их осмыслить [6].

Предупреждением опасных последствий развития ИВ на глобальном уровне занимается МСЭ, который рекомендует заинтересованным сторонам создавать динамичную экосистему путем поддержки стартапов и инкубаторов ИВ, содействовать инновациям, устраняя барьеры на их пути, развивать центры обработки данных, стандарты использования ИВ, создавать атмосферу доверия [8].

Таким образом, развитие ИВ оказывает существенное влияние на общественное развитие. В этой области внедряются передовые технологии, способствующие повышению эффективности широчайшего спектра направлений человеческой деятельности. Риски, производимые развитием ИВ, зависят в своих проявлениях от социально-экономического эффекта ИВ, а также от запросов и действий пользователей, производителей, правительств и заинтересованных международных инстанций. Управление рисками, порождаемыми развитием ИВ, требует соотнесения результатов технологического прогресса с интересами всех заинтересованных сторон, а также нахождения баланса между удобством и безопасностью пользователей «умных» устройств.

Список литературы

1. Интернет вещей может стать ключом к установлению недорогих соединений, которые преобразуют жизнь людей в развивающихся странах. Пресс-релиз [Электронный ресурс] // Международный союз электросвязи. – Режим доступа: http://www.itu.int/net/pressoffice/press_releases/2016/pdf/02-ru.pdf. – Дата доступа: 29.10.2017.
2. *Ковачич, Л.* Большой брат 2.0. Как Китай строит цифровую диктатуру / Л. Ковачич [Электронный ресурс] // Московский Центр Карнеги, 18.07.2017. – Режим доступа: http://carnegie.ru/commentary/71546. – Дата доступа: 10.09.2017.
3. *Куликова, А.* Интернет вещей: виртуальное благоденствие и реальные риски / А. Куликова [Электронный ресурс] // Индекс безопасности. – 2015. – Т. 21. – № 3 (114). – С. 95-112. – Режим доступа: http://www.pircenter.org/media/content/files/13/14482861000.pdf. – Дата доступа: 10.09.2017.
4. Ловушки «интернета вещей». Анализ данных, собранных на IoT-ловушках «Лаборатории Касперского» / В. Кусков [и др.] [Электронный ресурс] // АО «Лаборатория Касперского», июнь 19, 2017. – Режим доступа: https://securelist.ru/honeypots-and-the-internet-of-things/30874. – Дата доступа: 10.08.2017.

5. Обзор интернета вещей. Рекомендация МСЭ-Т Y.2060 [Электронный ресурс]. – С. 1. – Режим доступа: https://www.itu.int/rec/T-REC-Y.2060-201206-I. – Дата доступа: 29.10.2017.

6. Открытое письмо к Конвенции Организации Объединенных Наций об употреблении определённого вида оружия [Электронный ресурс] // Future of Life Institute // Future of Life Institute. – Режим доступа: https://futureoflife.org/open-letter-united-nations-convention-certain-conventional-weapons-russian. – Дата доступа: 29.10.2017.

7. Полис на всякий вирус [Электронный ресурс] // Коммерсантъ, 27.10.2017. – Режим доступа:https://www.kommersant.ru/doc/3450079. – Дата доступа: 29.10.2017.

8. Harnessing the Internet of Things for Global Development / International Telecommunication Union and Cisco [Электронный ресурс] // International Telecommunication Union. – Geneva, 2016. – Режим доступа: http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf. – Дата доступа: 29.10.2017.

9. *Jinwoo, K.* Orwell's Nightmare: China's Social Credit System / K. Jinwoo [Электронный ресурс] // The Asan Institute for Policy Studies, 28.02.2017. – Режим доступа: http://en.asaninst.org/contents/orwells-nightmare-chinas-social-credit-system. – Дата доступа: 10.08.2017.

10. *Stupp, C.* Ansip Plans New EU Cybersecurity Centre / C. Stupp [Электронный ресурс] // Euractiv.com, 20.07. 2017. – Режим доступа: https://www.euractiv.com/section/cybersecurity/news/ansip-plans-new-eu-cybersecurity-centre. – Дата доступа: 10.08.2017.