О последствиях массового внедрения Интернета вещей

День добрый, уважаемые коллеги!

Хотел бы поблагодарить организаторов этой встречи за возможность выступить с небольшим комментарием.

Коллеги, мы услышали ряд интересных и содержательных выступлений по актуальным проблемам международной информационной безопасности. Я хотел бы сказать несколько слов о некоторых социально-гуманитарных последствиях массового внедрения Интернета вещей.

По определению компании Cisco *Интернет вещей - это любые устройства, способные подключаться к Интернету*[1]. Согласно компании Gartner в 2017 году количество таких устройств составит 8,4 миллиарда.[2] По прогнозам компании Cisco, к 2020 году будут функционировать до 50 миллиардов подключенных устройств, что означает достижение критической массы в процессе реализации потенциала Интернета вещей[3].

Применение технологии Интернета вещей обладает огромным потенциалом для развития экономики и повышения качества жизни. Но вместе с тем массовое внедрение этой технологии имеет и значительную негативную возможность для человека, общества и государства.

Ведущие государства мира и международные организации проявляют осознанное беспокойство по возможным негативным последствиям, новым вызовам и угрозам, которые могут принести технологии Интернета вещей.

Для Японии, страны с высоким индексом развития информационно-коммуникационных технологий (ИКТ) – 8, 43 балла (это 10-е место в мире, согласно Индексу Глобального развития ИКТ-2017, подготовленного Международным Союзом Электросвязи (ITU))[4], обеспечение

[1] Источник: https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/02-03b.html
[2] https://www.gartner.com/newsroom/id/3598917
[3] Источник: https://www.cisco.com/c/ru_ua/about/press/2017/05-30.html
[4] Источник: https://www.itu.int/net4/ITU-D/idi/2017/

кибербезопасности в условиях сверхбурного развития Интернета вещей, является стратегической задачей в сфере обеспечения национальной безопасности.

Так, Национальным Центром обеспечения готовности к инцидентам и стратегии кибербезопасности при Правительстве Японии (NISC)[5] в августе 2016 года подготовлен документ «Общие принципы обеспечения безопасности Интернета вещей» («General Framework for Secured IoT Systems»), содержащий основные элементы политики обеспечения безопасного функционирования Интернета вещей[6].

В ноябре 2016 г. Министерство внутренней безопасности США (U.S. Department of Homeland Security) подготовило документ «Стратегические принципы защиты Интернета вещей. Версия 1.0» (STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT) Version 1.0)[7], в котором содержатся конкретные рекомендации, подготовленные по итогам профессиональных обсуждений.

В Российской Федерации в соответствии с программой «Цифровая экономика», утвержденной Правительством РФ 28 июля 2017 года, проводятся работы по пересмотру некоторых стандартов и технических регламентов с позиций, в том числе, и необходимости обеспечения информационной безопасности Интернета вещей.

Уважаемые коллеги!

Зададимся вопросом: готов ли человек к тому, чтобы в его личном пространстве находились и действовали десятки технических устройств, которые имеют выход в глобальную сеть и самостоятельно работают с Интернетом? Готовы ли производители технологий и устройств, используемых в Интернете вещей, взять на себя социальную ответственность

[5] См.: National center of Incident readiness and Strategy for Cybersecurity // http://www.nisc.go.jp/eng/
[6] См. http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf
[7] Источник: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

за возможные социально-гуманитарные последствия? Ответа, по-видимому, пока нет!

Во-первых, все производители устройств заявляют: все на благо человека, но при этом не все заложенные в устройства функции нам известны.

Яркие примеры негативных социальных последствий – это случаи в США, Германии, Норвегии с так называемыми «умными» игрушками, имеющими незаявленные выходы в глобальную сеть и нарушающими права на неприкосновенность частной жизни, имевшими судебные последствия.

В США Федеральное бюро расследований (ФБР (FBI)) просит родителей проверять «умные» игрушки своих детей. По данным ФБР, эти игрушки с выходом в Интернет, оснащенные видеокамерами и микрофонами, которые записывают и распознают речь владельца, имитируя «живое» общение, могут представлять серьезную угрозу персональной безопасности.

В текущем году в Интернет попали записи разговоров 800 тысяч обладателей продукции американской компании «Spiral Toys», производящей «умные» мягкие игрушки.

В это же время в Германии Федеральное сетевое агентство (Bundesnetzagentur) запретило продажу «умных» кукол «Моя подруга Кайла» (My Friend Cayla), назвав игрушку шпионским устройством.[8]

Подобное использование «умных» устройств явно нарушают положения Резолюции Генеральной Ассамблеи ООН от 19 декабря 2016 года «Право на неприкосновенность частной жизни в цифровую эпоху» (A/RES/71/199).

Во-вторых, управление устройствами Интернета вещей может быть перехвачено извне и, с определенной долей вероятности, они будут работать не на благо отдельного потребителя, группы или общества, а во вред им.

[8]См.: https://club.esetnod32.ru/news/novosti_eset/igrushki-shpiony/

Как всем вам известно, мировое сообщество не может справиться с киберпреступностью. И эта масса преступников и преступных группировок, действующих в кибепространстве, с энтузиазмом ухватятся за новые технические возможности, которые могут дать миллионы устройств, объединенных технологиями Интернета вещей, что может, в свою очередь, вызвать серьезные социальные последствия.

К примеру: *согласно данным японской прессы (Национального института информационно-коммуникационных технологий Японии), в 2016 году было зарегистрировано 128,1 млрд. кибератак против сетей в Японии, что более чем в два раза превышает аналогичные показатели 2015 года. При этом более 50 % атак, выявленных в прошлом году, были направлены на целевые камеры наблюдения, подключенные к Интернету, домашние беспроводные маршрутизаторы и другие устройства с выходом в Интернет; количество подобных атак увеличились примерно на 26 процентов по сравнению с 2015 годом*[9].

В-третьих, хотя эти технические устройства и не полноценные компьютерные устройства, они ограничены вычислительными мощностями, но, имея возможность выхода в Интернет, они могут быть использованы для проведения DDos-атак. Это явление получило название Ботнет вещей.

Самый известный пример: в октябре 2016 года при помоще ботнета Mirai мощной DDoS-атаке подверглась инфраструктура Managed DNS крупного DNS-провайдера Dyn: для атаки было задействовано около 100000 инфицированных IoT-устройств. Уже через месяц новый вариант вредоносной программы Mirai отключил доступ к Интернету порядка 900 тысячам клиентам немецкой телекоммуникационной компании Deutsche Telekom.

[9] Cyberattacks targeting Japan networks hit a record 128.1 billion in 2016. https://www.japantimes.co.jp/news/2017/02/08/national/crime-legal/cyberattacks-targeting-japan-networks-hit-record-128-1-billion-2016/#.Wgi6SrhR37k

Уважаемые коллеги,

Зададимся еще одним вопросом: а готово ли государство обеспечить информационную безопасность своих граждан в условиях массового внедрения Интернета вещей (IoT)? Задача сверхтрудная!

Здесь надо вспомнить о важности выполнения положений еще одной Резолюции Генеральной Ассамблеи ООН - «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», принятой 21 декабря 2009 года (A/RES/64/211).

Согласно исследованию компании Trustlook (сентябрь 2017 года)[10]*, уровень осведомленности пользователей об угрозах Интернета вещей сравнительно невысок на фоне растущего количества киберугроз в данной сфере.*

Исследование показало, что более трети (35%) владельцев устройств из сферы «Интернета вещей» не изменяют установленный по умолчанию пароль, что делает эти устройства уязвимыми к кибератакам. Помимо этого, 54% пользователей не устанавливают никакое стороннее программное обеспечение для защиты устройств от киберпреступников.

С ростом количества устройств увеличиваются и связанные с ними риски. По оценкам экспертов, к 2020 году доля кибератак на IoT-устройства составит 25%.

Как не печально, но уже можно говорить, что при помощи «умных» устройств можно оказать деструктивное воздействие на работоспособность любого элемента критически важной инфраструктуры не только в криминальных, но и в террористических и даже в военных целях.[11]

[10] http://www.securitylab.ru/news/488795.php / https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf
[11] О.В.Храмов. http://www.scrf.gov.ru/news/allnews/2164/

Уважаемые коллеги!

Одним из самых простых действий обезопасить себя от рисков - это соблюдение основных положений культуры информационной безопасности. Необходимость развития, внедрения, и обязательного применения культуры информационной безопасности во всех случаях взаимодействия с ИКТ-технологиями, включая и сферу Интернета вещей – задача крайне важная.

Наш симпозиум – результат многолетнего и успешного сотрудничества Московского университета и Университета Токай – 2-х авторитетных научно-образовательных университетов, одна из главных целей деятельности которых – разработка и обучение знаниям. И здесь хочу обратить ваше внимание на концептуальную статью ректора МГУ академика В.А.Садовничего «Как защитить человека от инфогенных рисков и угроз?», написанную в 2013 году (она также переведена и на японский язык), где подтверждается, что долг ***«научно-образовательной корпорации – разработать и внедрить систему знаний, навыков и норм глобальной культуры информационной безопасности».*** По мнению ректора Московского университета *для ликвидации безграмотности в области информационной безопасности необходимо объединение усилий науки, образования, средств массовой информации, бизнес-структур, сообществ Интернет-пользователей. И на первом месте здесь наука и образование, которые должны дать инструментарий для решения поставленных задач – научно-обоснованные рекомендации, широкий спектр специальных образовательных программ, методик преподавания, учебной и научно-популярной литературы.*

Благодарю за внимание!

どうしたら情報的リスク及び脅威から個人を守れる？

ヴィクトル・A・サドーヴニチィ

ロシア科学アカデミーの正会員
M.V.ロモノーソフ・モスクワ国立総合大学学長

教育機関は世界的な情報セキュリティの文化の知識、スキルや基準の仕組みを開発し、実装する義務がある。

情報セキュリティに関する非識字状態を改善するのは、急性的でグローバルな課題であるため、専門の政府機関にて解決策を開発し実施するしかないと思われる。科学、教育、メディア、企業、インターネットユーザーのコミュニティの総合的な協力が必要である。ただし、リーダーシップは科学と教育業界にあるべきである。エビデンスに基づいた勧告、特殊な教育プログラムや指導方法、教育と科学専門の大衆教材など、直面する課題を解決するために必要になる、広い範囲のツールを編み出される必要があるためだ。

2013年・モスクワ市・MGU