CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

ВСЕМИРНЫЙ ДЕНЬ ПРАВ ПОТРЕБИТЕЛЕЙ 2019

ЦИФРОВОЙ МИР: НАДЕЖНЫЕ СМАРТ-УСТРОЙСТВА

Издание на русском языке подготовлено
Международной конфедерацией обществ потребителей (КонфОП), членом Consumers International

КонфОП
Международная конфедерация обществ потребителей

ЧТО ТАКОЕ СМАРТ-УСТРОЙСТВО?

Смарт-устройство (также «умное», «интеллектуальное» устройство) способно подключаться к другим устройствам, обмениваться с ними данными, взаимодействовать с ними и со своим пользователем. Смарт-устройства могут подключаться друг к другу и к Интернету с помощью широкого спектра коммуникационных соединений[1]. Самые популярные среди потребителей смарт-устройства – это смартфоны, игровые приставки, смарт-телевизоры, портативные трекеры состояния здоровья (например, фитнес-трекеры), термостаты, детские игрушки и оборудованные доступом в Интернет автомобили. Все эти продукты способны собирать и анализировать пользовательские данные и передавать их на другие подключенные к сети устройства. Сети, состоящие из подключенных друг к другу смарт-устройств, называются Интернетом вещей (IoT).

От умных устройств потребители ожидают нового уровня удобства и эффективности, персонализации услуг. Неудивительно, что смартфоны – один из самых популярных видов интеллектуальных устройств, так как помимо текстовых сообщений и звонков они способны выполнять множество других функций: шагомера, геолокатора и даже измерителя пульса. Кроме того, смартфон можно сделать центральным хабом, который обеспечивает взаимодействие пользователя с другими интеллектуальными устройствами, такими как принтеры, акустические системы, домашние системы безопасности или фитнес-трекеры.

Смартфоны играют особую роль для потребителей из развивающихся стран, где доступ к Интернету через стационарное широкополосное подключение из дома весьма ограничен[2]. Потребители в этих странах используют смартфоны для осуществления платежей, отправки и получения денежных переводов, связи, доступа к заработной плате, кредитам т. п. – то есть для выполнения важнейших функций. Это означает, что обеспечение доступности, безопасности и защищенности подключенных к Интернету телефонов особенно важно для потребителей, использующих свои смартфоны для получения основных услуг.

Помимо смартфонов другими наиболее популярными смарт-устройствами являются системы безопасности умных домов и интеллектуальные устройства мониторинга состояния здоровья. Так, фитнес-трекеры следят за уровнем активности пользователя, характером его сна и частотой сердечного ритма, помогая анализировать текущее состояние здоровья. Системы безопасности умных домов включают в себя беспроводные камеры, замки и датчики движения. Если эти устройства регистрируют в доме необычную активность, они направляют на смартфон владельца соответствующее оповещение.

Расчет также количество умных продуктов, предлагающих индивидуальные решения людям с ограниченными возможностями. Например, это умные часы для людей с потерей зрения. Такие устройства вибрируют при получении входящих электронных сообщений и переводят их в шрифт Брайля на лицевой панели часов.[3] Умные лампочки, подключенные к дверному звонку или телефону, облегчают жизнь людям с потерей слуха.[4]

[1] Таких как, например, 3G, 4G и Wi-Fi

[2] В наименее развитых странах (least developed countries) доступ в Интернет через широкополосное подключение осуществляется в менее чем в 15% случаев. В Африке доступ в Интернет из дома имеют лишь 18% домохозяйств. Стационарное широкополосное подключение определяется как доступ к Интернету через проводное подключение. К проводным подключениям относятся в частности кабельные модемы, цифровые абонентские линии (DSL), подведенное к жилищу/зданию оптоволокно, прочие стационарные (проводные) широкополосные технологии подключения по подписке, спутниковые широкополосные и эфирные беспроводные подключения. ITU, *ITU Facts and Figures 2017,* 2017

[3] Вебсайт, https://dotincorp.com/

[4] *'Deaf community empowered through connected home lighting from Philips Hue'*, *Philips,* 29/09/2014

СТРЕМИТЕЛЬНЫЙ РОСТ РАСПРОСТРАНЕНИЯ СМАРТ-УСТРОЙСТВ

В течение последних десяти лет объем потребления умных продуктов неуклонно рос. Прогнозы показывают, что этот рост продолжится. По данным исследований, в настоящее время в мире имеется 23,1 миллиарда подключенных устройств. При этом ожидается, что к 2025[5] году эта цифра увеличится втрое. Ожидается, что в период с 2017 по 2022 год общемировые расходы потребителей на интеллектуальные продукты для дома почти удвоятся. [6]

В частности, за несколько лет стремительно выросло количество смартфонов: сегодня в мире насчитывается около 4 миллиардов подключенных смартфонов, что почти вдвое больше, чем три года назад.

Прогнозируется, что к 2025 году 72% интернет-пользователей будут выходить в Интернет исключительно с мобильных телефонов. Около половины новых пользователей придется на Китай, Индию, Индонезию, Нигерию и Пакистан. [7]

Снова отметим, что в развивающихся странах[8] стационарное подключение к Интернету остается пока более дорогим способом доступа к сети. Поэтому именно благодаря развитию мобильного Интернета миллионы людей в этих странах впервые узнали об Интернете и его возможностях. [9]

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ДОСТУПА К СЕТИ

Однако в развивающихся странах темпы распространения всех типов смарт-устройств, включая смартфоны, отстают от развитых вследствие плохой инфраструктуры, малой ценовой доступности устройств и траффика, более медленного Интернета. Стоимость пакетов траффика в развивающихся странах остается самой высокой в мире, являясь существенным препятствием для дальнейшего распространения смарт-устройств. Так, для приобретения 1 ГБ траффика данных в Африке необходимо потратить 18% среднего месячного дохода одного человека. [10]

Но даже несмотря на такое отставание, аналитики прогнозируют, что распространение умных устройств в мире будет расти – в основном благодаря инвестициям в развитие инфраструктуры. По данным Ассоциации GSM (GSMA), к 2025 году две трети мобильных подключений по всему миру будут осуществляться через высокоскоростные сети, и 91% всех сетевых подключений – через 3G или 4G. Такие сети будут лучше поддерживать использование смарт-устройств и их взаимодействие с другими умными продуктами. [11]

ДОВЕРИЕ К СМАРТ-УСТРОЙСТВАМ С ПЕРВОГО ПРИМЕНЕНИЯ

Таким образом, по мере улучшения технических возможностей сетей во всех регионах мира и увеличения инвестиций в новые технологии, использование подключенных устройств и их сетей потенциально станет повсеместным. Без полного понимания того, что это означает с точки зрения как возможностей, так и рисков, потребители во всем мире могут остаться в уязвимом положении. Вовлечение в жизнь людей все большего количества умных устройств требует внимания к сопутствующим проблемам безопасности и конфиденциальности, ставит вопрос о необходимости разработки новых механизмов защиты потребителей для обеспечения их доверия к этим устройствам. [12]

---

[5] *'Internet of Things (IoT) connected devices installed based worldwide from 2015 to 2025 (in billions)'*, *Statista*
[6] *'Forecast consumer spending on smart home systems and services worldwide by region in 2017 and 2022 (in billion US dollars)'*, *Statista*,
[7] *'From 'mobile only' internet to content strategies: new GSMA study identifies the 'megatrends' shaping mobile industry'*, *GSMA*, 11/09/2018
[8] ITU Broadband Commission, *The State of Broadband: Broadband catalyzing sustainable development*, September 2017
[9] GSMA, *Accelerating affordable smartphone ownership in emerging markets*, Июль 2017
[10] A4AI, *2017 Affordability Report*, 2017
[11] GSMA, *The Mobile Economy*, 2018
[12] OECD, *The Internet of Things : Seizing the benefits and addressing the challenges. Background report for Ministerial Panel 2.2,* Май 2016

ПРОБЛЕМЫ СМАРТФОНОВ И ДРУГИХ СМАРТ-УСТРОЙСТВ

Ценовая доступность: Хотя некоторые страны ввели особые меры, например, снизили ввозные пошлины, чтобы удешевить смарт-устройства и телефоны[13], стоимость передачи данных все еще является барьером для доступа в Интернет.[14]

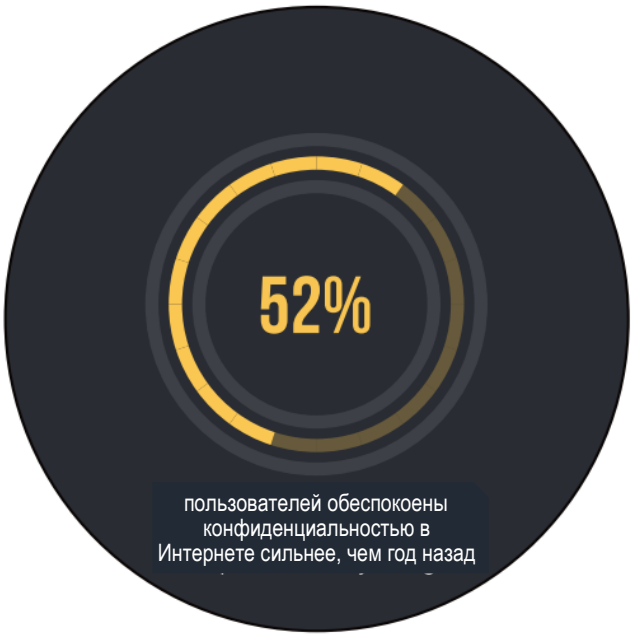
Сегодня только четыре африканские страны достигли целевого показателя Альянса за Доступный Интернет (A4AI) в 2% месячного дохода за 1 ГБ траффика данных

В Южной Африке высокая стоимость траффика привела к протестам и запуску в социальных сетях кампании под хэштегом #DataMustFall.[15] Стоимость передачи данных высока и в других регионах мира: так, за 1ГБ данных в Непале и Никарагуа придется отдать 4% и 9% среднего месячного дохода соответственно.[16]

Безопасность: Все интеллектуальные устройства являются частью более крупных подключенных систем и сетей, оттого уязвимость любой отдельно взятой части может поставить под угрозу всю систему. В последние годы мы узнали о множестве громких кибератак, запущенных хакерами, которые получили доступ к незащищенным потребительским устройствам. В 2016 году крупная кибератака нарушила работу Интернет-сервисов в Северной Америке и Европе, когда были атакованы незащищенные принтеры, домашние Wi-Fi роутеры и радио-няни. Это позволило вирусу стремительно распространиться и заразить в итоге почти 65 000 устройств менее чем за 24 часа. [17]

Помимо рисков нарушения работы сетей и сервисов, незащищенные смарт-устройства ставят под угрозу безопасность самих потребителей. Исследователи выявили, что устройства можно взламывать и управлять ими удаленно – в одном из случаев специалисты в области компьютерной безопасности смогли получить доступ к подключенному к сети автомобилю и управлять его рулевой системой, тормозной системой и дверными замками.

Защита личных данных: Проведенное в 2018 году глобальное потребительское исследование показало, что 52% пользователей за год стали сильнее беспокоиться о своей конфиденциальности в Интернете.[18] При этом 43% респондентов другого опроса заявили, что хотели бы узнать больше о данных, собранных о них с помощью подключенных устройств, а 47% респондентов были обеспокоены возможностью кражи личных данных.[19] Значительный риск с точки зрения сохранения конфиденциальности данных возникает из-за того, что устройства могут и конструктивно предназначены для обмена данными друг с другом, способны автономно передавать данные третьим сторонам. Объекты внутри подключенной системы могут собирать данные или информацию, которые сами по себе безвредны, но при сопоставлении и анализе вместе с другими данными способны раскрыть достаточно точные сведения о личности, что приводит к расширению возможностей по отслеживанию пользователей и их профилированию.



Прозрачность:

Потребители могут понимать , в чем функциональность их устройств, но то, как именно собираются и используются их данные, и как они связаны с бизнес-моделями компаний, зачастую им неизвестно. Проведенное 25 международными регулирующими организациями исследование показало, что про 59% устройств невозможно было выяснить, как именно они собирают, используют и раскрывают личные данные пользователей. Deco Proteste, член Всемирной организации потребителей из Португалии, провел контрольные закупки с магазинах смарт-телевизоров. Выяснилось, что потребитель перед совершением покупки не имеет возможности получить информацию о том, как устройство будет собирать и использовать его личные данные. При этом для того, чтобы начать пользоваться смарт-телевизором, пользователю необходимо согласиться с политикой сбора данных.

[13] 'Ghana slashes tariff on imported phones by 50%' IT Web Africa, 18/10/2016
[14] Mauritius, Nigeria, Tunisia, Egypt, A4AI
[15] 'Icasa mulls regulating internet data prices', Eye Witness News, 09/2018
[16] A4AI, Mobile Broadband Data Costs, 2017
[17] 'How a dorm room Minecraft scam brought down the internet', Wired, 13/12/17
[18] Centre for International Governance Innovation, 2018 CIGI-Ipsos Global Survey on Internet Security and Trust, 2018
[19] 'Seventy-five per cent of smartphone users read privacy policies as industry gets ready to embrace savvy consumers', Mobile Ecosystem Forum, 29/06/2017

Функциональная совместимость: Обеспечение того, чтобы различные умные устройства, которыми владеют потребители, могли продуктивно обмениваться данными друг с другом, также очень важно для потребителей с точки зрения максимально эффективного использования приобретенных устройств. Если вы купили «домашний помощник» и обнаружили, что он не может подключиться к другим устройствам в вашем доме, это серьезно ограничит его функциональность. Если устройства могут эффективно работать только с другими гаджетами от той же компании, потребитель оказывается вынужденно привязанным к одной системе, а это ограничивает его выбор и конкуренцию на рынке.

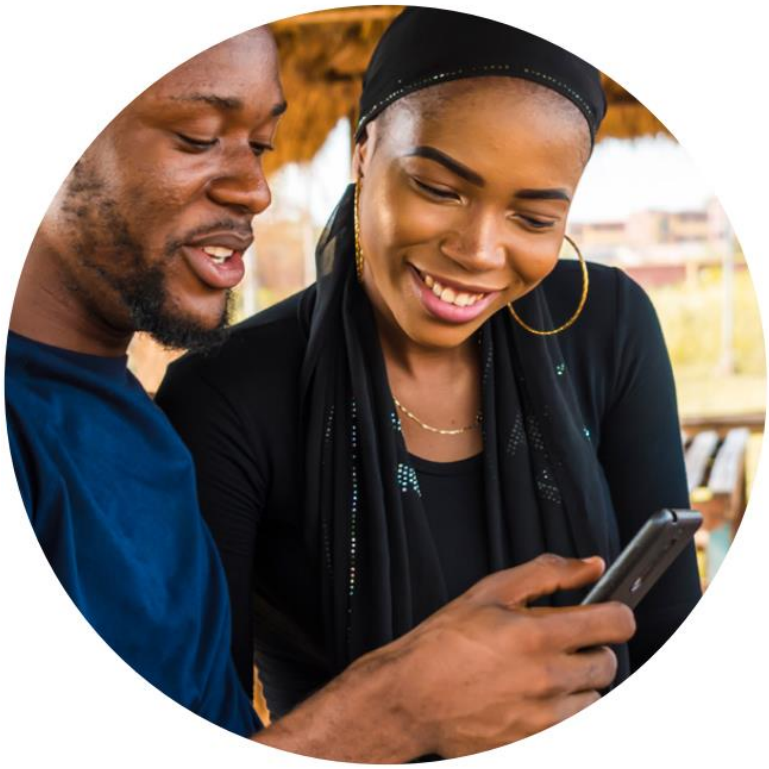
Обновления функций безопасности: Общая проблема с подключенными устройствами – это отсутствие обновлений функций безопасности. Если обновления недоступны, устройства могут стать уязвимыми для вирусов и кибератак. Тем не менее компании не обязаны предоставлять обновления, и кроме того, нигде не оговаривается, как долго они должны предоставлять такие обновления для устройств старых моделей.

Consumer Reports, наш член из США, протестировал Glow – приложение, регистрирующее личную информацию о здоровье и фертильности женщин, и обнаружил ряд уязвимостей, которые позволили бы человеку с базовыми навыками взлома получить доступ к этим конфиденциальным данным; производитель устранил эти уязвимости после разоблачения

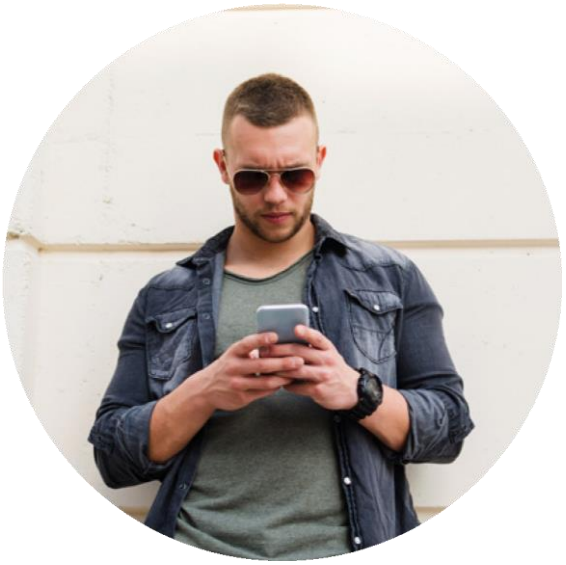
ПРИМЕРЫ ДЕЙСТВИЙ ЧЛЕНОВ CI

IDEC провела кампанию против ограничения траффика данных в Бразилии: в 2016 году Интернет-провайдеры в Бразилии начали вводить ограничения на траффик данных через широкополосные подключения. Ограничение траффика данных фактически означает установление провайдером предельного количества данных, которыми можно обменяться через соединение. По достижении пользователем установленного лимита Интернет-провайдер может снизить скорость передачи или вовсе отключить его от Интернета. Организация IDEC, член Всемирной организации потребителей, вместе с другими бразильскими организациями по защите прав потребителей и цифровых прав провела кампанию против таких ограничений. Давление со стороны этих групп привело к тому, что бразильский регулятор ANATEL организовал общественные консультации по вопросу ограничения траффика.

#WatchOut: Норвежский Совет Потребителей (NCC) и британская компания, занимающаяся безопасностью, протестировали четыре модели умных детских часов.[20] Тест показал, что устройства имеют серьезные недостатки, ненадежные с точки зрения безопасности функции, не обеспечивают защиты потребителей. У двух моделей были выявлены недостатки, позволяющие потенциальному злоумышленнику контролировать приложения и таким образом в режиме реального времени получать доступ к данным о местонахождении детей и к аудио данным.



[20] #WatchOut, Analysis of smartwatches for children, *Forbrukerradet*, Октябрь 2017



Завоевание доверия: Всемирная организация потребителей совместно с ANEC, ICRT и BEUC опубликовала ряд принципов[21], подчеркивающих необходимость приоритизации защиты прав потребителей, конфиденциальности и безопасности сетей и устройств в развитии Интернета Вещей. Эти принципы и рекомендации предназначены для разработчиков, производителей, политиков и регулирующих органов. В них учтены основные риски, с которыми сталкиваются потребители при использовании Интернета Вещей, даны рекомендации по решению существующих проблем.

Призыв к улучшению качества обновлений смартфонов: Consumentenbond, член Всемирной организации потребителей из Нидерландов, подал в суд иск против Samsung за то, что компания не предоставляла обновления функций безопасности для своих смартфонов в течение достаточно продолжительного срока. Компания утверждала, что их более дорогие продукты получают обновления в течение более длительного периода времени.[22]

Test-Achats взломала умный дом: Действуя в кооперации с этичными хакерами из SureCloud, наш бельгийский член Test-Achats протестировал 19 популярных продуктов для умных домов[23] и выяснил, что почти половина из них имеет серьезные уязвимости, позволяющие хакерам контролировать устройства удаленно и перехватывать данные, передаваемые по сети.

Борьба за честные мобильные услуги в Руанде: Поскольку в Руанде все больше и больше потребителей используют мобильные услуги для проведения банковских операций и получения доступа к основным государственным услугам, наш член, организация ADECOR, заявляет о важности обеспечения поставщиками мобильных услуг защиты и безопасности данных потребителей, высокого качества мобильных телефонов и доступности услуг. В тесном сотрудничестве с потребителями, гражданским обществом, операторами мобильной связи и Интернет-провайдерами, ADECOR составила список рекомендаций по улучшению качества и доступности мобильных услуг, включая привлечение представителей потребительских организаций к проверкам компаний-операторов и обращение в Руандийское бюро стандартов (RSB) с целью предотвращения ввоза в страну некачественных мобильных телефонов.

Which? проверяла умные игрушки на безопасность: В 2016 и 2017 годах организация Which? совместно с другими организациями потребителей и специалистами в области безопасности провела исследование[24] подключаемых к компьютерным сетям игрушек. Исследование показало, что некоторые из популярных детских игрушек имеют серьезные проблемы с безопасностью. Особую озабоченность вызвали игрушки, оборудованные динамиками и микрофонами; при отсутствии аутентификации через Bluetooth хакерам удалось подключиться к интерактивному медвежонку Toy-Fi Teddy и передавать через него голосовые сообщения ребенку, получая ответы.

Consumer Reports исследовало автомобили с сетевыми функциями: Анализ, проведенный членом Всемирной организации потребителей из США Consumer Reports, показал, что подключаемые к сети автомобили собирают большое количество данных о своих водителях и пассажирах. Исследования, проведенные с автомобилями 2018 модельного года, показали, что 32 из 44 брендов предлагают тот или иной вид беспроводного подключения своих автомобилей для передачи данных. При этом, несмотря на рост количества собираемых данных, законодательные нормы, регулирующие владение и распоряжение такими данными, остаются нечеткими.[25] Consumers Union, адвокативное подразделение Consumer Reports, считает, что Конгресс должен принять закон, наделяющий потребителей в США серьезными и однозначными правами на свои данные.[26]

---

21 ANEC, ICRT and BEUC, *Securing consumer trust in the internet of things. Principles and Recommendations,* 2017
22 'Dutch case against Samsung for lack of updates finally heads to court', *Android Police,* 26/03/2018
23 Connected house, house in danger!, *Test-Achats*, May 2018
24 Smart toys - should you buy them?, Which?, 2017
25 'Who Owns the Data Your Car Collects?', *Consumer Reports, 02/05/2018*
26 'Data protection by design and default', *ICO,* 2017

ПОЛИТИЧЕСКИЕ ОТВЕТЫ НА ВЫЗОВЫ И ВОЗМОЖНОСТИ СМАРТ-УСТРОЙСТВ

Как уже отмечалось выше, уровни распространения смарт-устройств сильно различаются в зависимости от страны. Соответственно, реакция правительств на новые, связанные с подключенными устройствами вызовы и возможности также сильно разнится как внутри регионов, так и от региона к региону.

В ЕС и США мы наблюдаем становление нормативно-правовой базы, особенно в отношении безопасности и конфиденциальности смарт-устройств. В Азиатско-Тихоокеанском регионе в ответ на растущий потребительский спрос растет объем государственной поддержки и инвестиций в рассматриваемые технологии. Так, Япония, Южная Корея, Индия, Малайзия и Сингапур разработали национальные стратегии в отношении Интернета вещей. В то же время в Латинской Америке, Африке и на Ближнем Востоке рынки умных устройств все еще находятся на самой начальной стадии развития (за исключением таких стран, как Турция, ОАЭ и Бразилия), поэтому реакция правительств на подключаемые потребительские устройства в этих регионах весьма ограничена.

Ниже выделен ряд наиболее значительных наработок последних лет в области регулирования Интернета Вещей:

Особое выделение спектра частот: Радиочастотный спектр – это диапазон радиочастот, выделенных для нужд мобильной индустрии или других секторов, в которых применяются радиоволны. Для снижения стоимости беспроводных подключений нужный спектр должен быть доступен для соответствующих отраслей на конкурентной и недискриминационной основе.[27] В Бразилии национальный регулятор ANATEL разработал план распределения спектра, согласно которому частоты для оказания определенных услуг выделяются по мере роста спроса на эти услуги. При составлении плана учитывается и мнение общества.

GDPR и проектируемая конфиденциальность (Privacy by Design): Принцип проектируемой конфиденциальности теперь закреплен в Общем регламенте ЕС по защите данных (GDPR). Обеспечение конфиденциальности уже на этапе проектирования означает, что разработка механизмов обеспечения конфиденциальности и защиты данных являются неотъемлемой частью процесса проектирования и создания продукта, а не отдельной функцией, добавляемой в готовое устройство.

Директива ЕС о безопасности сетей и информационных систем: Директива вступила в силу в мае 2018 года. Она требует от провайдеров цифровых услуг (торговых онлайн площадок, поисковых систем и облачных сервисов) внедрения основанных на оценке рисков мер по обеспечению безопасности в отношении интегрированных в их сети устройств Интернета Вещей.[28]

Постановление ЕС ePrivacy: Постановление ЕС ePrivacy распространяется на обмен данными на уровне межмашинного взаимодействия (Интернет Вещей). Провайдеры Интернета вещей должны получать согласие конечных пользователей на доступ к информации, касающейся подключенных устройств[29].

Рекомендации по обеспечению безопасности Интернета вещей Федеральной Торговой Комиссии (FTC) США: FTC указала, что провайдеры Интернета вещей должны принимать меры для защиты устройств от несанкционированного доступа. Рекомендации FTC включают в себя требование к провайдерам о разработке спецификаций достаточно длинных и сложных паролей, об ограничении числа попыток входа и о надежности хранения деликатной информации.[30]

Стандарт проектируемой конфиденциальности (Privacy by Design): Международная организация по стандартизации (ISO) находится на ранних стадиях разработки нового стандарта по защите потребителей в Интернете вещей. Этот стандарт станет руководством по внедрению принципа проектируемой конфиденциальности в потребительские товары и услуги.

Если вам нужны дополнительные примеры действий в области Интернета вещей, ознакомьтесь с **Цифровым Индексом Всемирной организации потребителей**. Цифровой Индекс представляет собой онлайн-коллекцию действий и инициатив политических кругов, бизнеса и гражданского общества, направленных на защиту прав потребителей. Выполнив поиск по Индексу, вы найдете порядка 200 примеров действий, охватывающих 10 областей, включая доступ и инклюзию, защиту данных и конфиденциальность, безопасность и защиту, конкуренцию и выбор. Для ознакомления со всеми примерами в этой области, проведите поиск по теме «Интернет вещей (IoT)».

[27] *'2017 Affordability Report'*, *A4AI*, 2017
[28] 'Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity', *European Commission,* 19/07/2018
[29] 'The new EU ePrivacy Regulation: what you need to know', *i-scoop,* 2017
[30] FTC Consumer Product Safety Commission, *The Internet of Things and Consumer Product Hazards: Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection*. 2018