МЕЖДУНАРОДНЫЕ ПОТРЕБИТЕЛИ ОБЪЕДИНЯЮТСЯ РАДИ ПЕРЕМЕН

ВСЕМИРНЫЙ ДЕНЬ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ2019 БРИФИНГ:

НАДЕЖНЫЕ СМАРТ УСТРОЙСТВА

ЧТО ТАКОЕ СМАРТ УСТРОЙСТВО?

Смарт устройство может подключаться, совмещаться и взаимодействовать со своим пользователем и другими устройствами. Смарт устройства связаны друг с другом и с сетью Интернет посредством различных коммуникативных связей.[1] Наиболее популярные потребительские смарт устройства – это смартфоны, игровые приставки, смарт телевизоры, приборы слежения за состоянием здоровья (трекеры), термостаты, игрушки и подключенные автомобили. Эти устройства способны осуществлять сбор и анализ данных пользователя и их передачу другому подсоединенному устройству по сети. Эта глобальная сеть смарт устройств также известна как технология "Интернет вещей" (IoT).

Смарт устройства предлагают потребителям гарантированный комфорт, результативность и персонализированный сервис. Смартфоны – одни из самых популярных смарт устройств, так как они позволяют переписываться и осуществлять звонки, могут мониторить (отслеживать) действия пользователя, локацию (местоположение) и даже пульс. Кроме того, они могут выступать в качестве основного центра коммуникации, соединяющего пользователя с другими смарт устройствами, такими как принтеры, динамики, домашние системы безопасности или трекеры здоровья.

Что еще более важно – потребители в развивающихся странах, где доступ к сети Интернет через фиксированную широкополосную связь внутри дома ограничен[2], с большей вероятностью будут использовать смартфоны для выполнения таких важных задач, как осуществление платежей, отправка и получение денежных переводов, связь, доступ к заработной плате, кредиты и т. д. Это означает, что обеспечение доступности, безопасности и защищенности телефонов, подключенных к сети Интернет, особенно важно для потребителей, которые полагаются на их безопасность и надежность в предоставлении этих основных услуг.

Помимо смартфонов, также популярны другие подключенные устройства, включая смарт домашние системы безопасности и смарт мониторы слежения за состоянием здоровья. Например, фитнес-трекеры отслеживают уровень физической активности, характер сна и качество состояния здоровья, помогая пользователям достичь лучшего понимания информации о состоянии их здоровья. В доме смарт системы безопасности оснащены беспроводными веб-камерами, замками и датчиками движения. Если эти устройства зафиксируют необычную активность, то они могут посылать сигнал тревоги владельцу дома на его смартфон.

Так же существует и увеличивается количество смарт устройств, которые предлагают индивидуальные решения для людей с ограниченными возможностями. Например, смарт часы для людей с проблемами зрения, которые вибрируют при получении письма на электронную почту, затем переводят его содержание в шрифт Брайля на экран часов.[3] Смарт лампочки, подключенные к дверному звонку или телефону, предупреждают людей с проблемами слуха, когда звонит телефон или кто-либо находится у дверей.[4]

[1] Например: Bluetooth, 3G, 4G and Wi-Fi

[2] В наименее развитых странах (НРС) только 15 % подключений к сети Интернет осуществляются через фиксированную широкополосную связь. Только 18 % домохозяйств имеют доступ к Интернет дома в Африке. Фиксированная широкополосная связь определяется как доступ к общедоступному Интернету через проводные соединения. Она включает в себя кабельный модем, DSL, оптоволокно для дома /здания, другие фиксированные (проводные) широкополосные подписки, спутниковую широкополосную и наземную фиксированную беспроводную широкополосную связь. МСЭ, *Факты и цифры МСЭ 2017*, 2017

[3] Вебсайт: https://dotincorp.com/

[4] 'Сообщество глухих предоставляет возможность подключения домашнего освещения от Philips Hue', *Philips,* 29/09/2014

Быстрые темпы освоения смарт устройств

За последнее десятилетие освоение потребителем смарт устройств неуклонно возрастает, и прогноз показывает, что этот процесс будет продолжаться. Опросы показывают, что в настоящее время в мире установлено 23,1 миллиарда подключенных устройств, и ожидается, что к 2025 году эта цифра вырастет втрое[5]. Аналогичным образом, по прогнозам, во всех регионах практически удвоятся глобальные потребительские расходы на интеллектуальные устройства для дома в период между 2017 и 2022 гг.[6]

В частности, всемирное распространение смартфонов быстро возросло за последние три года. Сегодня в мире насчитывается около 4 миллиардов подключений к смартфонам, что почти вдвое больше, чем три года назад.

Ожидается, что к 2025 году 72 % интернет-пользователей будут осуществлять подключение к сети Интернет исключительно через мобильные устройства. Около половины этих новых пользователей будут находиться в Китае, Индии, Индонезии, Нигерии и Пакистане[7].

Фиксированная интернет-связь остается более дорогим способом подключения потребителей в развивающихся странах[8], этим обусловлено возрастание и центральная роль использования мобильного интернета, что предоставляет многим людям возможности впервые ознакомиться с сетью Интернет и узнать о возможностях, которые он может предложить[9].

Расширяющийся доступ

Тем не менее, освоение всех смарт устройств, включая телефоны, происходит медленнее в развивающихся странах, в связи со слабой поддерживающей инфраструктурой, возможностями приобретения оборудования и данных, медленной скоростью интернета. С точки зрения использования смартфонов, стоимость пакетов данных в развивающихся странах остается самой высокой в мире и является препятствием для дальнейшего внедрения. Например, приобретение 1 ГБ данных в Африке стоит в среднем 18 % месячного дохода человека[10].

Несмотря на указанное отставание, аналитики прогнозируют, что распространение интеллектуальных (смарт) устройств в мире возрастет, в основном благодаря инвестициям в улучшенную инфраструктуру. По данным GSMA, к 2025 году две трети мобильных соединений по всему миру будут работать в высокоскоростных сетях, а 91 % всех сетевых подключений будут использовать 3G или 4G. Эти сети будут лучше оснащены для поддержки использования интеллектуальных (смарт) устройств и связи с другими интеллектуальными продуктами[11].

Обеспечение доверия к смарт устройствам с самого начала использования

По мере улучшения возможностей сети во всех регионах и увеличения инвестиций в новые технологии, подключенные технологии могут стать основным направлением. Без всестороннего понимания того, что это означает с точки зрения возможностей и рисков, потребители во всем мире могут остаться уязвимыми. Все большее внедрение смарт устройств в жизнь людей требует понимания проблем безопасности и конфиденциальности, и означает разработку механизмов защиты потребителей, способствующих укреплению их доверия к продукции[12].

ПРОБЛЕМЫ, СВЯЗАННЫЕ СО СМАРТФОНАМИ И СМАРТ УСТРОЙСТВАМИ

Доступность: Хотя несколько государств ввели такие меры, как снижение

В настоящее время только четыре африканские

[5] 'Технология «Интернет вещей» (IoT) связывает устройства, установленные по всему миру с 2015 по 2025 гг. (в миллиардах)', *Statista*

[6] 'Прогноз потребительских расходов на смарт домашние системы и услуги в регионах по всему миру в период 2017-2022 гг. (в миллиардах долларов США) ', *Statista*

[7] 'От «мобильного» интернета до контентных стратегий: новое исследование GSMA определяет «мегатенденции», формирующие мобильную индустрию', *GSMA,* 11/09/2018

[8] Комиссия МСЭ по широкополосной связи, *Положение широкополосной связи: широкополосная связь, катализирующая устойчивое развитие*, Сентябрь 2017 года

[9] GSMA, *Ускоряющийся доступ к владению смартфонами на развивающихся рынках*, Июль 2017 года

[10] A4AI, *Отчет о доступности 2017*, 2017

[11] GSMA, *Экономика мобильности*, 2018

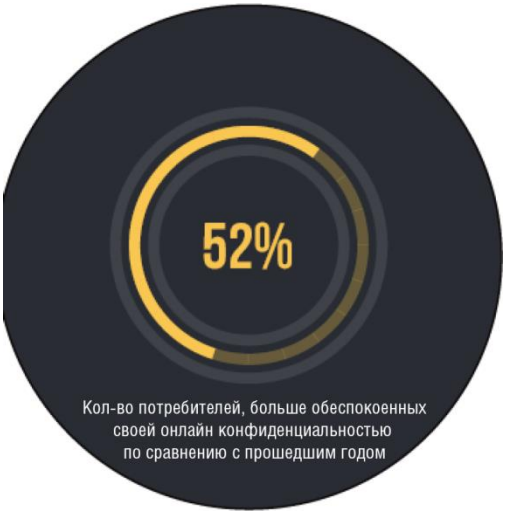
[12] OECD, *Технология «Интернет вещей»: Использование преимуществ и решение проблем. Справочный отчет для группы Министров № 2.2*, Май 2016 года

импортных пошлин, чтобы сделать смарт устройства и телефоны более дешевыми для потребителей[13], стоимость базы данных по-прежнему препятствует доступу в Интернет[14].
В Южной Африке высокая стоимость базы данных привела к протестам и кампании в социальных сетях #DataMustFall[15]. Стоимость базы данных также высока в других регионах: цена за 1 ГБ колеблется от 4% до 9% от ежемесячного дохода в Непале и Никарагуа, соответственно.[16]

страны достигли цели Альянса по доступной сети Интернет (A4AI): стоимость 1 ГБ данных, составляющая 2 % ежемесячного дохода.

Защита и безопасность: Все смарт устройства являются частью более крупных подключенных систем и сетей, и уязвимость в любой части может поставить под угрозу всю систему. В последние годы мы наблюдали множество резонансных кибератак, которые инспирировались хакерами, получившими доступ к незащищенным потребительским устройствам. В 2016 году крупная кибератака разрушила интернет-сервисы в Северной Америке и Европе, атаковав небезопасные принтеры, домашние маршрутизаторы Wi-Fi и радионяни, позволяющие быстро распространять вирус, заразив почти 65000 устройств менее чем за 24 часа.[17]

Помимо нарушения работы сети и обслуживания, незащищенные смарт устройства также ставят под прямую угрозу безопасность потребителя. Исследователи показали, что они могут взламывать устройства и управлять ими удаленно: на одном примере исследователи безопасности смогли получить доступ к подключенному автомобилю и управлять рулем, тормозной системой и дверными замками.



Конфиденциальность и защита данных: глобальное исследование потребителей, проведенное в 2018 году, показало, что 52% пользователей более обеспокоены своей онлайн конфиденциальностью, чем год назад.[18] 43 % респондентов из другого опроса заявили, что хотели бы узнать больше о данных, собранных о них с помощью подключенных устройств, а 47 % беспокоятся о краже личных данных.[19] Значительный риск для конфиденциальности данных возникает из-за того, что устройства могут (и действительно для этого предназначены) обмениваться данными друг с другом и автономно передавать данные третьим сторонам. Объекты в подключенной системе могут собирать данные или информацию, которые безвредны сами по себе, но которые при сопоставлении и анализе с другой информацией могут выявить достаточно точные знания о человеке, что приводит к повышению отслеживаемости пользователей и профилирования.

Открытость: потребители могут понимать функциональность устройства, но то, каким образом их данные собираются и используются, а также как они связаны с бизнес-моделью компании, часто остается неясным. Исследование, проведенное 25 международными регуляторами конфиденциальности, показало, что 59 % устройств не смогли адекватно объяснить пользователям, как была собрана их личная информация, раскрыта и как использована. Деко Протесте, Член Потребительского Международного Союза в Португалии, осуществил тайные закупки Smart TV в магазинах. Было обнаружено, что покупателям не было доступно никакой информации о том, как устройства собирали и использовали их данные. Однако, при использовании телевизора необходимо согласиться с политикой сбора данных провайдера.

[13] 'Гана снизила тариф на импортные телефоны на 50%' *IT Web Africa,* 18/10/2016

[14] Мавритания, Нигерия, Тунис, Египет, от A4AI

[15] 'Иказа обдумывает регулирование цен на интернет-данные', *Eye Witness News,* 09/2018

[16] A4AI, *Стоимость базы мобильных данных Broadband*, 2017

[17] 'Как мошенничество Minecraft обрушило интернет', *Wired,* 13/12/17

[18] Центр по международным правительственным инновациям, *Глобальное исследование CIGI-Ipsos 2018 по вопросам безопасности и надежности в сети Интернет*, 2018

[19] '75% пользователей смартфонов изучают политику конфиденциальности, индустрия готова принять опытных потребителей', *Mobile Ecosystem Forum,* 29/06/2017

Возможность взаимодействия: для потребителя важно быть уверенным в том, что его собственные различные смарт устройства способны взаимодействовать друг с другом для максимально эффективного использования. Если Вы приобрели «домашний ассистент» и обнаружили, что он не способен взаимодействовать с другими устройствами в Вашем доме, то это будет ограничивать функциональность этих устройств. Если устройства эффективно работают лишь с устройствами одного производителя, потребитель может быть замкнут одной системой, а это ограничивает выбор и конкуренцию.

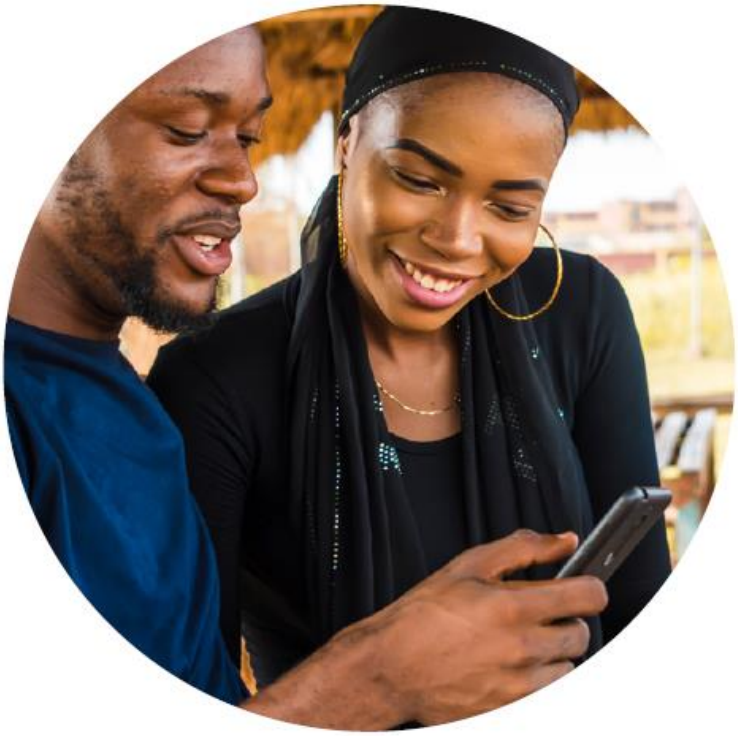
Обновления системы безопасности: общей проблемой подключенных устройств является отсутствие обновлений систем безопасности. Если обновления недоступны, устройства становятся уязвимыми для вирусов или кибератак. Однако компании не обязаны предоставлять обновления, и не договариваются о том, как долго они должны их предоставлять.

Наш американский участник Потребительского Отчета протестировал приложение ГЛОУ, которое записывает персональную информацию о женском здоровье и фертильности, и обнаружил ряд уязвимостей, которые позволяют кому-либо, обладающему основными хакерскими навыками, взломать эту чувствительную базу. Производитель быстро устранил эти уязвимости после их обнаружения.

ПРИМЕРЫ РАБОТ НАШИХ ЧЛЕНОВ

Компания IDEC против ограничения передачи данных в Бразилии: в 2016 году Интернет Сервис Провайдер (ИСП) в Бразилии приступил к введению использования широкополосного соединения. Поддержка радиотелефоном режима передачи данных - это предел использования данных, установленный провайдером (ИСП). Как только предел достигнут, Интернет-провайдер может замедлить обслуживание или даже отключить потребителя от сети Интернет. Член Международной ассоциации потребителей IDEC вместе с другими бразильскими группами по защите прав потребителей и цифровых прав провели кампанию по запрету ограничения данных.
Давление со стороны этих групп привело к тому, что регулятор ANATEL организовал общественные консультации по этому вопросу.

#WatchOut: Норвежский совет потребителей (NCC) и британская охранная фирма протестировали четыре экземпляра «смарт-часов» для детей.[20] Исследование показало, что устройства имеют серьезные недостатки безопасности: ненадежные функции безопасности и отсутствие защиты потребителей. У двух из этих устройств были уязвимости, которые позволяли потенциальному злоумышленнику контролировать приложения, таким образом получая доступ в реальном времени к расположению (геолокации) и аудиозаписям детей.



[20] #WatchOut, Анализ смарт-часов для детей, *Forbrukerradet*, Октябрь 2017 года

Обеспечение нашей надежности: Международная ассоциация потребителей вместе с ANEC, ICRT и BEUC опубликовали ряд принципов[21], подчеркивающих важность включения основных прав пользователей, конфиденциальности и безопасности в IoT сети и устройства. Принципы и рекомендации предназначены для разработчиков, производителей, высокопоставленных политиков и регуляторных органов, и выделяют основные риски, с которыми сталкиваются потребители при использовании продуктов IoT, и что можно сделать для их разрешения.

Призыв к лучшим обновлениям в смартфонах: Голландский член Международной ассоциации потребителей Consumentenbond обратился в суд с иском к компании Samsung за то, что она не предоставила достаточный период для обновлений безопасности своих смартфонов. Samsung утверждает, что их продукция более высокого класса, и получает обновления на более длительный период времени.[22]

Тестировщики взломали смарт (интеллектуальный) дом: работая с этичными хакерами в SureCloud, наш бельгийский участник Test-Achats протестировал 19 популярных продуктов для умного дома[23] и обнаружил, что почти половина протестированных продуктов имеет серьезные недостатки в области безопасности. Недостатки безопасности позволили хакерам удаленно управлять устройством и перехватывать данные, отправляемые в сети.

Стремление к честному (справедливому) использованию мобильного обслуживания в Руанде: поскольку все больше и больше потребителей в Руанде используют мобильные услуги для банковского доступа и доступа к основным государственным услугам, наш член ADECOR заявляет, что становится все более важным не только обеспечение защиты и безопасности данных потребителей, но и то, что мобильные телефоны хорошего качества и услуг должны реализовываться по доступным ценам. В сотрудничестве с потребителями, гражданским обществом, операторами мобильной связи и Интернет-провайдерами, ADECOR составил список рекомендаций по улучшению мобильных услуг. Это включает привлечение представителей потребителей к проверке телефонных операторов и обращение в Руандийское бюро стандартов (RSB) с целью помочь предотвращению импорта некачественных мобильных телефонов.

Какое исследование безопасности смарт игрушек: в период с 2016 по 2017 год, наряду с другими организациями потребителей и исследователями в области безопасности, были проведены исследования[24] безопасности подключенных игрушек. Их исследование показало, что несколько популярных детских игр имели серьезные недостатки в безопасности. Игрушки, оснащенные динамиками и микрофонами, вызывали особую озабоченность; без аутентификации Bluetooth на Toy-Fi Teddy хакеры смогли подключиться к игрушке, отправить голосовые сообщения ребенку и получить от него ответы.

Отчеты потребителей, касающиеся подключенных автомобилей: Анализ Consumer Report, американского члена Международной ассоциации потребителей, показывает, что подключенные автомобили собирают большие объемы данных о водителях и пассажирах. Исследования моделей автомобилей, начатые в 2018 году, показали, что 32 из 44 брендов предлагают беспроводное соединение для передачи данных. Однако, несмотря на увеличение объемов собираемых данных, юридические правила относительно того, кто владеет данными, не очень ясны.[25] Союз потребителей, отдел защиты интересов Consumer Reports, считает, что Конгресс США должен принять закон, предоставляющий потребителям в США надежные юридические права на неприкосновенность частной жизни.[26]

[21] ANEC, ICRT и BEUC, *Обеспечение доверия потребителей в технологии «Интернет вещей». Принципы и рекомендации*, 2017
[22] 'Голландское дело против Samsung из-за отсутствия обновлений в конце концов направлено в суд', *Android Police,* 26/03/2018
[23] Подключенный дом – дом в опасности!, *Test-Achats*, Май 2018 года
[24] Смарт игрушки – стоит ли покупать?, Какие?, 2017
[25] 'Кто владеет данными, которые собирает ваш автомобиль?', *Consumer Reports, 02/05/2018*
[26] 'Защита данных запланировано и по умолчанию', *ICO,* 2017

ПОЛИТИКА ОТКЛИКОВ НА ВОЗМОЖНОСТИ И ПРОБЛЕМЫ В СМАРТ УСТРОЙСТВАХ

Как выше отмечалось, уровни освоения смарт (интеллектуальных) устройств сильно различаются по всему миру. Отражая эту разницу, отклики правительств различных стран на проблемы и возможности, связанные с подключенными устройствами, также сильно различаются как внутри регионов, так и между ними.

В ЕС и США мы начинаем наблюдать за развитием нормативно-правовой базы, особенно в отношении безопасности и конфиденциальности интеллектуальных продуктов. В Азиатско-Тихоокеанском регионе, отражая растущий потребительский спрос, мы наблюдаем сильную государственную поддержку и инвестиции в подключенные технологии. Например, Япония, Южная Корея, Индия, Малайзия и Сингапур разработали национальные стратегии IoT. В Латинской Америке, Африке и на Ближнем Востоке рынки смарт (интеллектуальных) устройств все еще находятся в зачаточном состоянии (за исключением таких стран, как Турция, ОАЭ и Бразилия), поэтому реакция правительства на подключенные потребительские товары в этих регионах ограничена.

Ниже мы выделяем ряд наиболее значительных недавних разработок в области управления и регулирования IoT:

Смарт (интеллектуальное) распределение диапазона частот: Спектр относится к диапазону радиочастот, выделенных отрасли мобильной связи или другим секторам для использования радиосвязи. Чтобы снизить стоимость беспроводных соединений, спектр должен быть доступен для отраслей на конкурентной и недискриминационной основе.[27] В Бразилии национальный регуляторный орган электросвязи ANATEL разработал план распределения частот, который назначает полосы для определенных услуг по мере роста спроса. Также принимается во внимание общественное мнение.

GDPR и конфиденциальность по плану: принцип конфиденциальности по плану является теперь обязательством Общего регламента ЕС по защите данных (GDPR). Соблюдение требований конфиденциальности при проектировании означает, что конфиденциальность и защита данных были включены в продукт с момента его создания, а не закреплены на нем по окончанию производства.

Директива ЕС о безопасности сетевых и информационных систем: Директива вступила в силу в мае 2018 года. Она требует от поставщиков цифровых услуг (онлайн-рынков, поисковых систем и услуг облачных вычислений) внедрять меры безопасности на основе рисков для устройств IoT, встроенных в их сети[28].

Регламент ЕС ePrivacy: Регламент ЕС ePrivacy применяется к межмашинным коммуникациям (IoT). Провайдеры IoT должны получать согласие конечного пользователя на доступ к информации, связанной с подключенным устройством.[29]

Рекомендации по безопасности IoT Федеральной торговой комиссии США (FTC): FTC заявляет, что поставщики IoT должны принять меры для защиты устройств IoT от несанкционированного доступа. Рекомендации FTC включают требование к провайдерам разрабатывать сложные и уникальные спецификации паролей, ограничивать количество попыток входа в систему и надежно хранить конфиденциальную информацию.[30]

Стандарт Privacy by Design (Конфиденциальность по плану): Международная организация по стандартизации (ISO) находится на ранних стадиях разработки нового стандарта защиты потребителей в «Интернете Вещей» (IoT). Стандарт обеспечит руководство по конфиденциальности при разработке структуры для потребительских товаров и услуг.

Если вы ищете дополнительные примеры политики IoT, ознакомьтесь с **Цифровым индексом Международной Организации Потребителей**. Цифровой индекс представляет собой онлайн-совокупность цифровых потребительских стратегий и инициатив от политиков, бизнесменов и гражданского общества. Выполняя поиск по индексу, вы найдете около 200 стратегий, охватывающих 10 областей, включая доступ и включение, защиту данных и конфиденциальность, безопасность и защиту, а также конкуренцию и выбор. Ищите в технологию «Интернет Вещей», чтобы обратиться ко всем стратегиям и вопросам на эту тему.

---

[27] *'Отчет о доступности 2017'*, *A4AI*, 2017

[28] 'Комиссия просит членов государств включить в национальные законы общеевропейское законодательство о кибербезопасности', *Европейская комиссия,* 19/07/2018

[29] 'Новый Регламент ЕС ePrivacy: что нужно знать', *i-scoop,* 2017

[30] Комиссия FTC по безопасности потребительских товаров, *«Интернет вещей» и опасности для потребительских товаров: комментарии сотрудников Бюро по защите прав потребителей Федеральной торговой комиссии*. 2018