15 марта в мире отмечается Всемирный день прав потребителей.
В 2019 году Всемирный день прав потребителей пройдет под девизом: «*Trusted Smart Products*" – «За 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. Наиболее популярные потребительские смарт устройства – это смартфоны, игровые приставки, смарт телевизоры, приборы слежения за состоянием здоровья (трекеры), термостаты, игрушки и подключенные автомобили. 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. Помимо смартфонов, также популярны другие подключенные устройства, включая смарт домашние системы безопасности и смарт мониторы слежения за состоянием здоровья. За последнее десятилетие освоение потребителем смарт устройств неуклонно возрастает, и прогноз показывает, что этот процесс будет продолжаться.

ПРОБЛЕМЫ, СВЯЗАННЫЕ СО СМАРТФОНАМИ И СМАРТ УСТРОЙСТВАМИ

Доступность: Хотя несколько государств ввели такие меры, как снижение импортных пошлин, чтобы сделать смарт устройства и телефоны более дешевыми для потребителей, стоимость базы данных по-прежнему препятствует доступу в Интернет.

.**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. 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. 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. **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. **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.