Умные устройства
Умные устройства, возможно, должны иметь этикетки, показывающие, насколько они безопасны, и рассматривать предложения, направленные на то, чтобы помочь потребителям определить, какие продукты более безопасны, а какие менее. Умные телевизоры и другие подключенные к интернету бытовые устройства будут сделаны для того, чтобы содержать этикетки, указывающие, насколько они безопасны, в соответствии с предложениями, выдвигаемыми правительством. Министры хотят, чтобы эти ярлыки сначала вводились на добровольной основе, но предлагают, чтобы в конечном итоге они стали обязательными. Эти этикетки помогут потребителям определить, какие продукты более безопасны, а какие менее безопасны. В соответствии с планами, объявленными цифровым министром Марго Джеймс в среду, розничные торговцы смогут продавать только те продукты, которые несут этикетку, которая будет указывать потребителям, соответствует ли устройство трем основным стандартам безопасности, установленным правительством в более длинном кодексе практики в феврале. Этот шаг призван решить проблемы, связанные с небезопасными подключенными бытовыми устройствами, такими как телевизоры, термостаты, дверные звонки и замки, которые могут быть захвачены злоумышленниками. Были также предупреждения о том, что правительства могут использовать их для слежки за людьми в своих домах. Джеймс сказал: "многие потребительские товары, подключенные к интернету, часто оказываются небезопасными, что ставит под угрозу конфиденциальность и безопасность потребителей. Наш Кодекс практики был первым шагом к тому, чтобы убедиться, что продукты имеют функции безопасности, встроенные на стадии проектирования, а не закрепленные болтами в качестве запоздалой мысли." Эти новые предложения помогут повысить безопасность подключенных к интернету устройств и станут еще одной вехой в нашем стремлении стать мировым лидером в области онлайн - безопасности.” Профессор Алан Вуд ворд, эксперт по кибер безопасности из Университета Суррея, сказал, что эти предложения представляют собой хорошее начало, но добавил: “Проблема в том, что происходит с теми, кто не следует рекомендациям. Или, что еще более важно, кто будет проверять, что устройство действительно следует всем возможным рекомендациям.” Он сравнил этот план с существующей маркой CE, сказав: "Конечно, люди могут подделать их. Это происходит в данный момент, и поэтому торговые стандарты должны преследовать тех, кто, по сути, делает ложные заявления.”Вуд ворд сказал, что правительство должно будет “поставить некоторые зубы за те стандарты, которые они устанавливают”, предложил наблюдатель по линии Управления Комиссара информации. Эта схема станет частью более широких правительственных консультаций по вопросам улучшения общей кибер безопасности в Великобритании с тремя ключевыми требованиями в Кодексе практики для производителей устройств. Эти требования включают в себя обеспечение того, чтобы пароли на устройствах internet of things не были сброшены на универсальную заводскую настройку, а также обеспечение того, чтобы они обеспечивали общедоступный контакт в рамках политики раскрытия любых обнаруженных уязвимостей. Он также призывает производителей устройств явно указать минимальный период времени, в течение которого устройство будет получать обновления безопасности. Доктор Ян Леви, технический директор Национального центра кибер безопасности, сказал, что последний шаг по нацеливанию подключенных устройств имеет решающее значение для сокращения сбоев в отрасли. "Серьезные проблемы безопасности в потребительских устройствах Интернета вещей, такие как предустановленные неизменяемые пароли, продолжают обнаруживаться, и недопустимо, чтобы они не были исправлены производителями.” Министры также выдвинули альтернативные предложения о том, чтобы сделать продажу любого устройства, которое не соответствует трем стандартам, незаконной, без необходимости в системе маркировки.