Умным устройствам, возможно, придется носить метки, показывающие, насколько они безопасны.

Министры рассматривают предложения, направленные на то, чтобы помочь потребителям определить, какие продукты более, а какие менее безопасны.

Кевин Роулинсон

Смарт-телевизоры и другие бытовые устройства, подключенные к интернету, будут иметь метки, указывающие, насколько они безопасны, согласно предложениям, выдвигаемым правительством.
Министры хотят, чтобы метки сначала были введены на добровольной основе, но предлагают сделать их обязательными. Метки помогут потребителям определить, какие продукты более, а какие менее безопасны.
Согласно планам, объявленным в среду цифровым министром Марго Джеймсом, ритейлеры смогут продавать только продукты, на которых нанесена метка, что будет указывать потребителям, соответствует ли устройство трем основным стандартам безопасности, установленным правительством в более длительном кодексе практики в феврале.
Этот шаг предназначен для решения проблем, связанных с небезопасными подключенными бытовыми устройствами, такими как телевизоры, термостаты, дверные звонки и замки, которые могут быть взломаны злоумышленниками. Также были предупреждения о том, что правительства могут использовать их для слежки за людьми в их домах.
Джеймс сказал: «Многие потребительские продукты, подключенные к интернету, часто оказываются небезопасными, что ставит под угрозу конфиденциальность и безопасность потребителей. Наш кодекс практики стал первым шагом к тому, чтобы убедиться, что продукты имеют функции безопасности, встроенные на этапе проектирования и не закрепленные как раздумье.
«Эти новые предложения помогут повысить безопасность устройств, подключенных к интернету, и являются еще одним этапом в нашем стремлении стать мировым лидером в области безопасности в интернете».
Профессор Алан Вудворд, эксперт по кибербезопасности в Университете Суррея, сказал, что предложения представляют собой хорошее начало, но добавил: «Проблема в том, что происходит с теми, кто не следует методическим рекомендациям. Или, что более важно, кто будет проверять, что устройство действительно следует возможным методическим рекомендациям, какими они ни были.».
Он сравнил план с существующим знаком СЕ, сказав: «Конечно, люди могут подделать их. Это происходит в данный момент, и поэтому торговые стандарты должны преследовать тех, кто фактически делает ложные заявления».
Вудворд сказал, что правительству необходимо «подставить зубы за те стандарты, которые они устанавливают», предложив сторожевого пса в духе Управления комиссара по информации.
Схема станет частью более широкой правительственной консультации по улучшению общей кибербезопасности в Великобритании, с тремя ключевыми требованиями в кодексе практики для устройства
производители.
Требования включают в себя обеспечение того, чтобы пароли в интернет-устройствах не сбрасывались до универсальных заводских настроек, а также обеспечение общедоступной точки контакта в рамках политики раскрытия любых обнаруженных уязвимостей.
Он также призывает производителей устройств явно указывать минимальный период времени, в течение которого устройство будет получать обновления безопасности
Доктор Ян Леви, технический директор Национального центра кибербезопасности, сказал, что последний шаг к нацеливанию подключенных устройств имеет решающее значение для уменьшения сбоев в отрасли. «Серьезные проблемы безопасности в потребительских устройствах IoT, таких как предустановленные неизменяемые пароли, продолжают обнаруживаться, и недопустимо, чтобы они не фиксировались производителями ».
Министры также выдвинули альтернативные предложения о том, чтобы продажа любого устройства, не соответствующего трем стандартам, была незаконной без необходимости использования системы маркировки.