Смарт-устройства могут иметь ярлыки

показывая, насколько они безопасны

Министры рассматривают предложения, направленные на то, чтобы помочь потребителям определить, какие продукты являются более

которые менее безопасны

Кевин Роулинсон

Предложения направлены на повышение безопасности подключенных к Интернету устройств. Фотография:

Alamy Стоковое Фото

Смарт-телевизоры и другие подключенные к интернету бытовые устройства будут сделаны для установки ярлыков

насколько они безопасны, по предложениям, выдвигаемым правительством.

Министры хотят, чтобы этикетки были введены на добровольной основе, но предлагают, чтобы они были

в итоге сделано обязательно. Этикетки помогут потребителям определить, какие продукты являются более

и которые менее безопасны.

В соответствии с планами, объявленными министром цифрового телевидения Марго Джеймсом в среду, ритейлеры

продавать только те товары, на которых нанесена этикетка, которая

устройство соответствует трем основным стандартам безопасности, установленным правительством в

более длинный кодекс практики в феврале.

Этот шаг предназначен для решения проблем, связанных с небезопасными подключенными бытовыми устройствами,

такие как телевизоры, термостаты, дверные звонки и замки, которые могут быть похищены злоумышленниками.

Также были предупреждения о том, что правительства могут использовать их для слежки за людьми в их домах.

Джеймс сказал: «Многие потребительские товары, которые подключены к Интернету, часто оказываются

небезопасно, ставя под угрозу конфиденциальность и безопасность потребителей. Наш кодекс практики был первым шагом

чтобы убедиться, что продукты имеют функции безопасности, встроенные на стадии проектирования, а не

заперты как запоздалая мысль.

«Эти новые предложения помогут повысить безопасность подключенных к Интернету устройств и

еще одна веха в нашем стремлении стать мировым лидером в области онлайн-безопасности ».

Профессор Алан Вудворд, эксперт по кибербезопасности в Университете Суррея, сказал, что предложения

было хорошим началом, но добавил: «Проблема в том, что происходит с теми, кто не следует

методические рекомендации. Или, что более важно, кто будет проверять, что устройство действительно следует

возможные руководящие принципы. »

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, по сути,

делать ложные заявления ».

Вудворд сказал, что правительству необходимо «поставить некоторые зубы за те стандарты, которые они

изложить », предлагая сторожевого пса в соответствии с канцелярией Уполномоченного по информации.

Схема станет частью более широкой правительственной консультации по улучшению общего положения.

кибербезопасность в Великобритании, с тремя ключевыми требованиями в кодексе практики для устройства

производители.

Требования включают обеспечение паролей в Интернете устройств, которые не могут быть сброшены до

универсальные заводские настройки и обеспечение их общедоступного контакта в рамках политики

за раскрытие любых обнаруженных уязвимостей.

Он также призывает производителей устройств явно указать минимальную продолжительность времени, в течение которого устройство будет

получать обновления безопасности.

Доктор Ян Леви, технический директор Национального центра кибербезопасности, сказал, что последний шаг к

целевые подключенные устройства имеют 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 устанавливались производителями ».

Министры также выдвинули альтернативные предложения о продаже любого устройства, которое не соответствует

по трем стандартам незаконно, без необходимости системы маркировки.