Умные телевизоры и другие подключенные к интернету бытовые устройства будут сделаны для ношения наклеек. выясните, насколько они безопасны, в соответствии с предложениями, выдвигаемыми правительством.

Министры сначала хотят, чтобы эти ярлыки вводились на добровольной основе, но предлагают, чтобы они были в конце концов это стало обязательным. Эти этикетки помогут потребителям определить, какие продукты являются более эффективными и которые менее безопасны.

В соответствии с планами, объявленными цифровым министром Марго Джеймс в среду, ритейлеры будут только тогда можно будет продавать продукцию, которая несла бы этикетку, которая указывала бы потребителям, стоит ли это 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, например, 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 небезопасно, ставя под угрозу конфиденциальность и безопасность потребителей. Наш Кодекс практики был первым шагом к тому, чтобы убедиться, что продукты имеют функции безопасности, встроенные с этапа проектирования, а не прикрутил ее как запоздалую мысль.

"Эти новые предложения помогут повысить безопасность подключенных к интернету устройств и ИС еще одна веха в нашем стремлении стать мировым лидером в области онлайн-безопасности.”

Профессор Алан Вудворд, эксперт по кибербезопасности из Университета Суррея, сказал, что эти предложения представлял собой хорошее начало, но добавил: "проблема заключается в том, что происходит с теми, кто не следует правилам. методические рекомендации. Или, что еще более важно, кто будет проверять, что устройство действительно следует за любым

возможные руководящие принципы таковы.”

Он сравнил этот план с существующей маркой CE, сказав: "Конечно, люди могут подделать их. Оно

происходит в данный момент, и поэтому торговые стандарты должны преследовать тех, кто, по сути, является, делать ложные заявления.”

Вудворд сказал, что правительству нужно будет “поставить некоторые зубы за любые стандарты, которые они используют". отправляйся", - предложил сторожевой пес по линии Управления Комиссара информации.

Эта схема станет частью более широких правительственных консультаций по вопросам улучшения общего положения кибербезопасность в Великобритании, с тремя ключевыми требованиями в Кодексе практики для устройств производители.

Эти требования включают в себя обеспечение того, чтобы пароли на устройствах internet of things не были сброшены на универсальные заводские настройки и обеспечение того, чтобы они обеспечивали общественный контакт в рамках политики за раскрытие любых обнаруженных уязвимостей.

Он также призывает производителей устройств явно указать минимальный промежуток времени, в течение которого устройство будет работать.получайте обновления для системы безопасности.

Д-р Ян Леви, технический директор Национального центра кибербезопасности, сказал, что последний шаг к тому, чтобы целевые подключенные устройства имеют решающее значение для снижения отказов в отрасли. "Серьезные проблемы с безопасностью в потребительских устройствах Интернета вещей, таких как предустановленные неизменяемые пароли, продолжают обнаруживаться иэто неприемлемо, что они не фиксируются производителями.”

Министры также изложили альтернативные предложения по внесению в продажу любого устройства, которое не соответствует требованиям до трех стандартов нелегально, без необходимости в системе этикеток.

**Summary “Smart devices”**

The text under consideration is entitled “Smart devices”. Text devoted to cybersecurity of smart devices such as TVs, thermostats and doorbells and locks. The author touches upon problems of the possibility of hacking devices with intruders. The text divided into the following parts: the beginning, where it comes to special tags on devices, and conclusion, it comes to building requirements for equipment manufacturers