Кто должен позаботиться о безопасности Интернета вещей?

Петрова Елена, КБ “Экономикс-Банк”

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CoNews FORUM 2017
2007-2017 10 лет

Добро пожаловать в сказочное сегодня!

- Устройства сами знают, что делать
- Присутствие рядом больше не нужно
- Расстояния - не преграда для управления

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CoNews FORUM 2017
2007-2017 10 лет

Чего ждет потребитель?

Производитель устройства уже позаботился о возможных рисках

За все последствия отвечает производитель

А что предоставляет разработчик?

Красивая реклама умных устройств с удаленным управлением

И практически ничего про риски и ограничения в инструкциях к устройствам

Почему молчит производитель?

- Разработчики не акцентируют внимание на возможных рисках
- Нет стандартов и массовых инцидентов
- Не хотят пугать потребителя и проигрывать в конкурентной борьбе

Кто должен обеспечить безопасность Интернета вещей?

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CoNews FORUM 2017
2007-2017 10 лет

Идея первая. Производитель

- Проектирует безопасное устройство
- Проводит испытания
- Формирует инструкции, простые и понятные
- Устанавливает ограничения

Идея вторая. Разработчики среды

- Создание адаптированных сред автоматизации. Нет лишних состояний и функций. Сообщения об ошибках однозначно описаны. Документация детализирована.
- И никаких "недокументированных возможностей"!
- Обязательное наличие и обязательное использование функции индикации ошибочного состояния!
- А в идеале - программа распознавания "нетипичного использования" и прекращения удаленного управления в связи с этим

Идея третья. Ритейл

При продаже устройств Интернета вещей необходимо объяснять про функции удаленного управления

Должен разъяснять про ограничения

Необходимо указывать на необходимость соблюдения требований безопасности

Идея четвертая. Разработчики стандартов

Разработать обязательный к применению стандарт, устанавливающий требования к проектировке бытовых и промышленных устройств, имеющих функции удаленного управления и использующие “умные сценарии”

Стандарт должен требовать защиту от совмещенных рисков технической, программной составляющей и удаленного доступа

Идея пятая. Контролирующие организации

Органы государственного контроля прав потребителей должны уже сегодня обратить внимание, с чем они могут столкнуться завтра применительно к использованию потребителем устройств Интернета вещей

А значит заранее создавать квалифицированные подразделения контроля распространения среди потребителей таких устройств

Идея шестая. Тоже помощники

Немалый вклад в безопасность могут внести поставщики услуг связи и облачного хранения

Если организуют системы выявления и предотвращения атак на устройства Интернета вещей

Безопасность - это общее дело!

- Проблема безопасности Интернета вещей только зарождается
- Острую актуальность эта проблема приобретет уже скоро
- В решении этой проблемы будут принимать участие многие
- Предстоит “набить немало шишек” в процессе эволюции устройств

Спасибо за внимание!

Петрова Елена, КБ “Экономикс-Банк”

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА