

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ИОТ УСТРОЙСТВ

И.С. Терех, Е.А. Криштопова

В современных IoT экосистемах огромное количество датчиков, машин и других объектов отправляют данные по беспроводной связи на облачные сервера. Несмотря на множество возможностей для бизнеса, использование IoT-инфраструктуры несет риски информационной безопасности для компании и для отдельных пользователей.

Опросы западных потребителей показывают, 90 % из них не уверены в безопасности устройств IoT.

Проблемы информационной безопасности использования IoT делятся на две группы:

- повышение устойчивости подключенных устройств к кибератакам;
- защита конфиденциальности передаваемых персональных данных.

Разнообразие типов данных, мощностей и типов устройств IoT не позволяет создать универсальное техническое решение для любой инфраструктуры IoT и делает особенно важным правовые и организационные методы обеспечения безопасности.

Анализ имеющейся литературы, рекомендаций и практических реализаций показывает, что для обеспечения минимального уровня безопасности инфраструктуры IoT и данных ее пользователей необходимы уникальные пароли для подключенных устройств, сетевой адрес производителя для сообщений об уязвимостях, минимально требуемый срок обновления безопасности при продаже и эксплуатации устройств.

В дальнейшем необходимо развернуть работы над национальными, региональными и глобальными системами сертификации устройств IoT.