УДК 004.05

IoT – как угроза для современных организаций

Лысенкова Л. В., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: преподаватель Михасик Е. И.

Аннотация:
В статье рассматриваются угрозы, которые несут в себе IoT. Показана необходимость тщательного анализа использования интернет вещей в организациях.

IoT (Internet of things) – это аббревиатура, которая обозначает «интернет вещей» [3]. IoT базируется на сети передачи данных между физическими объектами, которые оснащены встроенными средствами и технологиями взаимодействия друг с другом или с внешней средой. Из чего можно сделать вывод, что IoT – это автоматизация, но более высокого уровня.

На рис. 1 отображается краткая история развития IoT. Исходя из того, что все началось еще в 1830-х годах с изобретения телеграфа, прогнозируется, что к 2030 году количество подключенных к сети устройств достигнет примерно 24 млрд [5].

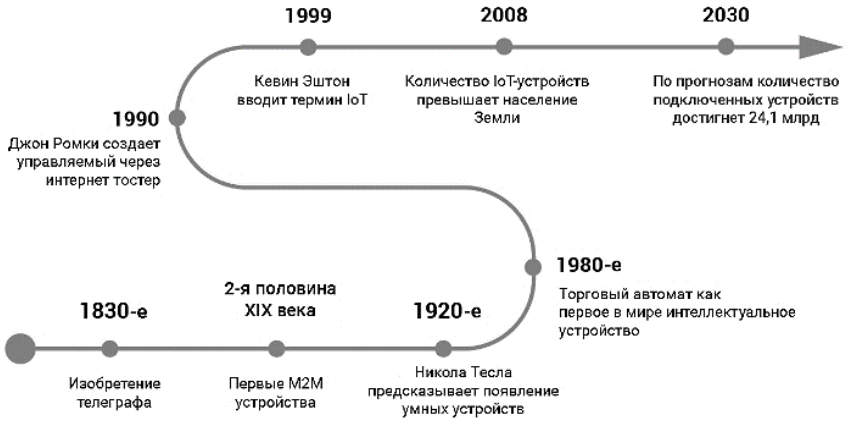

Рис. 1. История развития IoT

Концепция IoT была сформулирована в 1999 году Кевином Эштоном: «Интернет вещей – это метка идентификации, позволяющая идентифицировать объекты посредством радиосигналов, на которую можно занести определенную информацию, а позднее считать устройством» [5].

Концепция IoT состоит из следующих компонентов: IoT-устройства, IoT-сети, облачные формы, IoT-приложения и сервисы, люди и процессы [1]. Данные компоненты взаимодействуют друг с другом, обрабатывают данные и выполняют различные функции (обнаружить изменения в окружающей среде, включать и выключать устройства, подключаться к интернету и многое другое).

Рассматривая каждый компонент IoT отдельно, можно выделить, что:

1. IoT-устройства – все предметы, которые используются в деятельности и имеют выход в интернет.

2. IoT-сети – те сети, по которым IoT-устройства обмениваются данными с другими, обрабатывающими полученную информацию.

3. Облачные формы – технологии, которые позволяют хранить и обрабатывать информацию на удаленных серверах; в облаке хранится вся передаваемая туда информация.

4. IoT-приложения и сервисы – приложения и сервисы, позволяющие управлять IoT-устройствами дистанционно, забирая данные с их датчиков.

5. Люди и процессы – люди, которые ставят цели перед IoT-устройствами, но сами не участвуют непосредственно в управлении ими.

Системы IoT используют: TCP/IP-протоколы для обмена данными через каналы глобальной сети интернет, MQTT-протокол для обеспечения надежной передачи данных в сетях с низкой пропускной способностью и низкой надежностью [3].

Данный способ «общения» (посредством протоколов), позволяет объединить системы между собой и создать «сеть сетей». Но, несмотря на все преимущества, внедрение IoT может представлять серьезную угрозу для современных организаций.

Угрозы от большого количества устройств и соединений в IoT-сетях можно поделить на несколько групп:

1. Возможность дистанционного взлома и кража данных.

2. Возможность дистанционного взлома и управления устройствами.

3. Возможность отказа или нарушения работы систем, включающих IoT.

Первой угрозой от большого количества устройств и соединений в IoT-сетях будет являться безопасность данных [4]. Устройства IoT часто используются для передачи и хранения конфиденциальной информации о клиентах или других важных данных. При попадании данной информации в руки злоумышленников, может произойти кража личной информации о клиентах или сотрудниках, т. е. нарушение конфиденциальности данных. Нарушение конфиденциальности данных может привести к серьезным санкциям. Следовательно, организация понесет большие потери.

Вторая угроза – возможность дистанционного взлома и управления устройствами. При получении злоумышленником доступа к нелицензированным устройствам IoT в организации, может произойти нарушение общественной безопасности, беспорядки в транспортных сетях и энергоснабжении и др.

Третья угроза – возможность отказа или нарушения работы систем, включающих IoT. В организациях генерируется огромный объем данных IoT-устройствами. Для обработки такого количества данных требуются мощные, сложные системы и надежные алгоритмы анализа. Отказ данных систем или ошибка в анализе могут привести к принятию неверных решений, ошибкам и значительным потерям.

Таким образом, IoT является эволюцией технологий, которая частично меняет способы взаимодействия людей с окружающим миром. IoT открывает широкие возможности для улучшения жизни и повышения эффективности в различных областях, но требует внимания к вопросам безопасности и конфиденциальности. Безопасность данных, возможность взлома и сложность управления большим объемом информации – все это проблемы, требующие постоянного контроля и развития соответствующих технологий и регулирования. Организации, чтобы минимизировать риски связанные с IoT, должны уделить должное внимание обеспечению безопасности. К этому относится: применение сильных методов шифрования данных, установка обновлений и патчей для всех устройств IoT, регулярное обновление паролей, установка многофакторной аутентификации, обучение сотрудников [2].

Список использованных источников

1. Понимание основ инфраструктуры IoT [Электронный ресурс] // Xinyetong. – Режим доступа: https://kurl.ru/gRuNh. – Дата доступа: 24.10.2023.
2. Сервер попал в неприятности [Электронный ресурс] // Дом – Dubaifood.ru. – Режим доступа: https://dubaifood.ru/server-popal-v-nepriyatnosti/. – Дата доступа: 23.10.2023.
3. Суомалайнен, А. Интернет вещей: видео, аудио, коммутация [Электронный ресурс] / А. Суомалайнен. – М. : ДМК Пресс, 2019. – Режим доступа: https://www.litres.ru/book/antti-suomalaynen/internet-veschey-video-audio-kommutaciya-44336615/. – Дата доступа: 23.10.2023.
4. Что такое соблюдение информационной безопасности [Электронный ресурс] // Городец870. – Режим доступа: http://textovod.com/unique/link?url=https%3A%2F%2Fxn--870-iddfg5dar7d.xn--p1ai%2Ffaq%2Fcto-takoe-soblyudenie-informacionnoi-bezopasnosti&key=88728fe78d4eda271eb6059a7e2a6072. – Дата доступа: 21.10.2023.
5. Что такое IoT и что о нем следует знать [Электронный ресурс] // Хабр. – Режим доступа: https://habr.com/ru/companies/otus/articles/549550/. – Дата доступа: 12.11.2023.

УДК 37.011.33

Кураторский час как форма воспитательного мероприятия в ВУЗе

Малиновская Д. А., магистрант
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: канд. пед. наук, доцент Евсеева О. П.

Аннотация:

В данной статье рассматриваются понятия воспитательное мероприятие, особенности и требования, предъявляемые к ним. Описывается, что такое кураторский час его виды и формы, а также методы воспитания, приводятся возможности использования электронного ресурса для проведения кураторского часа.