АНАЛИЗ ВОЗМОЖНЫХ УГРОЗ СИСТЕМЫ «УМНЫЙ ГОРОД»

Качинская Н.В.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Логин В. М. – ст. преподаватель каф. ПИКС

Целью является выявление и обозначение рисков «умного» города.

Интеллектуальные технологии совершенствуются с поразительной скоростью, города улучшают свои услуги с точки зрения безопасности, здравоохранения, транспорта и общего благосостояния своих жителей. Для этого используют систему «умный город». В основе данной системы лежит концепция интеграции нескольких информационных и коммуникационных технологий. Проекты «Умный город» включают в себя:

-Видеонаблюдение и видеоаналитика
-ИТС – интеллектуальные транспортные системы
-Безопасность на общественном транспорте
-Профессиональная радиосвязь и широкополосный доступ (LTE, 5G)
-IoT – интернет вещей
-Беспилотные автомобили
-Биометрия
-Обработка неструктурированных данных
-Технологии поддержки принятия решений
-Распределенные базы данных
-Геоинформационные технологии и навигация
-Машинное обучение
-Облачные/туманные/граничные вычисления [1]

Особенность развития технологии в большом разнообразии направлений и путей развития, что влечет за собой необходимость разработки системы безопасности для каждого нового проекта и невозможности унификации.

Тема безопасности при создании «умных городов» становится все более актуальна во всем мире. Развитие данной системы идет главным образом в направлении уменьшения стоимости и увеличении охватываемых областей жизни человека, зачастую в ущерб безопасности.

Целью данного проекта является выделение основных уязвимостей данной системы как со стороны аппаратной части, так и информационной безопасности.

Выделим следующие виды угроз:

- Уязвимость перед кибератаками. В первую очередь это уязвимость перегрузки системы с помощью DDoS-атаки, блокировка систем с помощью вымогательского ПО, остановка автоматизированных систем управления и другие.

- Риск утечки данных. Электронные медицинские карточки, пропуски на предприятия, оплата покупок, проезда банковской картой и получение доступа к этим данным – предоставит практически полную информацию о жизни человека.

- Риск технической неисправности. Современные технические приборы все еще не совершенны и неисправность или сбой в их работе может привести к получению недостоверной информации или материальному ущербу.

- Риск создания ЧС. Ложная сработка или взлом системы оповещения приведет к панике что может привести к жертвам. Автоматизированные системы управления, СКУД и другие системы могут привести к трагедии в аналогичных ситуациях.

- Риск несанкционированного доступа и изменения данных. Изменение данных в медицинской карточке, показателей датчиков аварийных систем или интеллектуальной транспортной системе так же находится под угрозой.

- Риск зависимости от техники. Когда все направления жизни города находятся под контролем «умных» систем возможное их отключение уже является угрозой так как вызовет «паралич» большей части инфраструктуры города.

Список использованных источников:

1. Статья: Умные города, Smart cities [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Интеллектуальные_города_(Умные_города,_Smart_cities).

2. РИСКИ "УМНЫХ" ГОРОДОВ [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/riski-umnyh-gorodov.

3. Как работает искусственный интеллект «умного» города» [Электронный ресурс]. – Режим доступа: https://www.cnews.ru/articles/2019-08-22_kak_sdelat_gorod_umnee.