Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет геодезии и картографии»
(МИИГАиК)

На правах рукописи

Лыгин Алексей Николаевич

Разработка и исследование методики сбора геоданных на основе технологий радиочастотной идентификации при их оперативном обновлении в ГИС

25.00.35 - Геоинформатика

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, профессор
И.Г. Журкин

Москва - 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность работы связана с возросшей необходимостью быстрого обновления и актуализации данных географических информационных систем (далее ГИС), например, инвентаризация, события на онлайн-карте). В условиях быстрого изменения местности (застройка, снос, вырубка деревьев и т.п.) необходимость оперативного обновления картографических материалов очевидна. Объекты в ГИС обладают пространственными и семантическими атрибутами, составляющими геодезическую основу. Для оперативного изменения геодезической основы возникает задача быстрой привязки изображений местности в ГИС, что осуществляется с помощью естественных и искусственных опознавательных знаков. Существующие методики обновления геоданных являются трудозатратными из-за проведения наземных работ, поэтому требуются новые средства и способы обновления геоданных.

Актуальность также обусловлена следующими предпосылками:

1) возросла необходимость снижения стоимости обновления геоданных;
2) требуется улучшить доступность информации в ГИС для пользователей;
3) необходимость повышения достоверности и надежности информации;
4) широкие перспективы развития и использования методики оперативного обновления ГИС.

Степень научной разработанности исследуемых проблем. В российской научной литературе не встречается методик оперативного обновления ГИС, особенно с использованием радиометок. Все существующие методики обновления сводятся к данным ДЗЗ, лазерному сканированию, геодезическим съемкам. Но эти методики сбора геоданных не предусматривают сбор метаданных, который должен быть достаточно оперативным и является замедляющим фактором при создании ГИС.

В зарубежной литературе встречаются самые разнообразные методики применения RFID в ГИС:

- В строительстве, внутри сооружений для создания трехмерной ГИС [1].
- В транспортной логистике для учета паломников и отображения в онлайновой ГИС [2].
- В логистике твердых бытовых отходов [3].
- В подземном транспорте [4].
- В управлении в условиях ЧС [5].
- Беспроводной мониторинг бытового электросчетчика с помощью технологий RFID и ZigBee [6].

Цель и задачи. **Целью** работы являлась разработка и исследование методики сбора геоданных на основе RFID-технологий для оперативного обновления ГИС. Применение новых радиотехнологий в ГИС. Для этого были решены следующие **задачи**:

- Исследовать возможности радиотехнологий (RFID, NFC, Bluetooth, ZigBee, Wi-Fi, WRAN, WiMAX, beacons) для применения их в оперативном обновлении ГИС.
- Разработать требования к радиоинфраструктуре.
- Разработать количественные критерии для выбора радиометки.
- Разработать методику сбора данных для ГИС с помощью RFID-технологий.
- Провести исследование разработанной методики сбора данных по разработанным критериям.

Объект исследования – процесс сбора геоданных для оперативного обновления ГИС.

Предмет исследования – методика сбора и оперативного обновления данных в ГИС с помощью RFID-технологий.

Методы исследования. Для решения задач использовались теоретические методы: абстрагирование, анализ и синтез, индукция и дедукция, геомоделирование, моделирование, системный подход, цифровой обработки изображений. А также эмпирические: сравнение, измерение, эксперимент.

Научная новизна, в отличие от существующих методик сбора данных, заключается в новом комбинировании существующих технологий, их применении в ГИС-технологиях (геодезии, ДЗЗ), где они ранее не использовались в России, и обобщении этих технологий в разработанной методике сбора геоданных для оперативного обновления геоданных в ГИС. В рамках методики разработаны требования к радиоинфраструктуре для её применения в обновлении геоданных в ГИС, разработаны условные количественные критерии для выбора оборудования радиоинфраструктуры. Это является новым знанием об организации устройств и способов технической системы (ГИС-инфраструктура), следовательно, является научным результатом из технической отрасли науки.

Теоретическая значимость. Состоит в технологическом развитии существующих способов и технологий сбора геоданных для ГИС, позволяющем улучшить эффективность (объём и точность) сбора геоданных для оперативного обновления ГИС, путем внедрения новых радиотехнологий передачи данных в цикл работы ГИС.

Практическая значимость. Полученные в исследовании результаты можно использовать в предприятиях отрасли для решения различных практических задач, например:

1. для создания более информативных съемочных сетей при строительстве;
2. мониторинга различных движущихся объектов и их отображения в ГИС;
3. инвентаризации объектов народного хозяйства и помещения данных о них в ГИС;
4. быстрого поиска объекта на местности и сбора геоданных с помощью БПЛА.

Выносимые на защиту положения и результаты.

1. Исследованы возможности современных радиотехнологий передачи данных для применения их в оперативном обновлении ГИС. Это дает возможность оценить пригодность исследованных радиотехнологий для нужд геоинформатики и смежных отраслей.

2. Предложено дополнение в аппаратный инструментарий полевых съемок для сбора данных в ГИС радиометками и считывателями радиометок, что позволяет работать с новыми радиотехнологиями хранения и передачи данных для ГИС.

3. Разработаны базовые требования к радиоинфраструктуре: к количеству доступной для записи памяти метки, к безопасности данных, к сроку службы и расстоянию считывания метки, к считывателю данных. Это конкретизирует минимальные требования к оборудованию для работы с радиотехнологиями сбора геоданных в ГИС.

4. Разработаны количественные критерии для выбора радиометки, что позволяет оценить степень эффективности радиометки для практического использования.

5. Разработана методика сбора данных для ГИС с помощью RFID-технологий, впервые дающая возможность внедрить современные радиотехнологии передачи и хранения данных в отрасль геоинформатики, объединив их с существующими способами.

6. Исследована разработанная методика сбора данных по обоснованно выбранным критериям и практически доказана целесообразность её внедрения. Методика должна улучшить доступность, полноту и качество геоданных и метаданных, увеличить надежность их передачи и хранения сразу в цифровом виде, что ускорит сбор геоданных по сравнению с традиционными ручными способами.

Достоверность и апробация научных и практических результатов работы подтверждается применением апробированного научно-методического аппарата, анализом большого количества отечественных и зарубежных литературных источников, существующего рынка радиооборудования, а также согласованностью выдвинутой гипотезы полученным собственным практическим результатам. Положения работы были опубликованы в материалах нескольких научных конференций и статьях автора в журнале перечня ВАК.

Диссертация состоит из введения, трёх разделов, заключения, библиографического списка, списка терминов и определений. Общий объём 104 страниц, включая 39 рисунков и 10 таблиц. Библиографический список состоит из 66 наименований, из них 32 на английском языке.

1. ОБЗОР RFID-ТЕХНОЛОГИЙ И АНАЛИЗ ИХ ВОЗМОЖНОСТЕЙ

1.1. RFID-технологии и стандарты

1.1.1. Определение и классификация RFID-технологий

Современные технологии позволяют создавать электронные устройства миниатюрных размеров для записи и считывания различного рода информации. Одной из таких технологий являются RFID-технологии (от англ. Radio Frequency IDentification, радиочастотная идентификация). RFID-технологии — это способ автоматической идентификации объектов через радиосигналы, в которых информация хранится в RFID-метках (транспондерах, радиометках, RFID-тегах), далее - метка или радиометка [7].

Радиометки состоят из интегральной схемы, где производится обработка и хранение информации, модулирование и демодулирование радиочастотного сигнала и приёмо-передающей антенны (рис. 1.1).

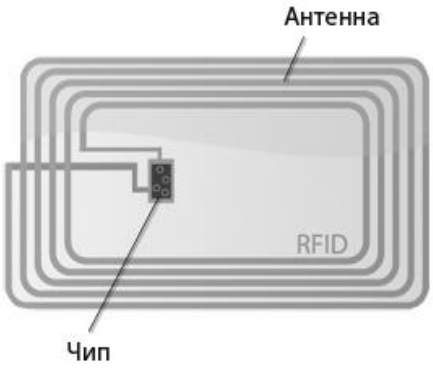


Рис. 1.1. RFID-метка.

RFID-система состоит из считывающего устройства (считыватель, ридер, интеррогатор) и RFID-метки (транспондера, RFID-тега) (рис. 1.2).

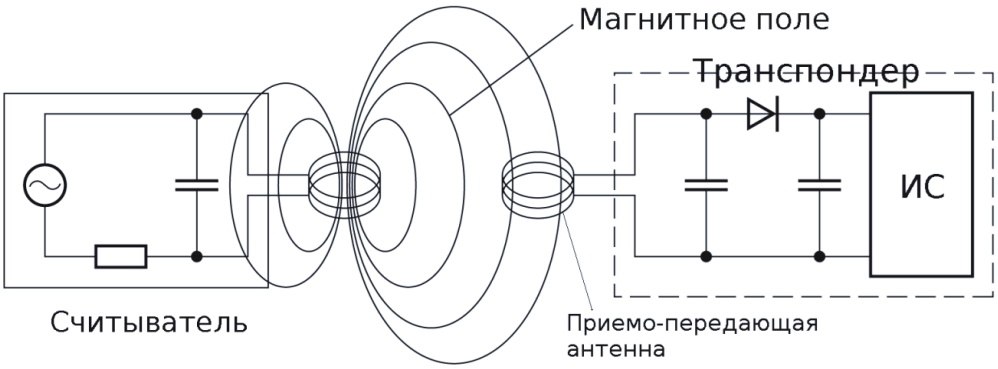


Рис. 1.2. Принципиальная схема RFID-технологии с активной меткой.

В памяти любой метки есть место под уникальный идентификатор (tag ID), который обычно занимает 128 бит данных и представляет собой уникальный номер данной метки в пределах, установленных данным производителем метки. Этот идентификатор закладывается на производстве и не подлежит изменению. Есть модификации, где к уникальному идентификатору прилагается необязательный пользовательский номер, который может изменяться по желанию пользователя метки.

RFID-метки классифицируют [8],[9]:

— по типу памяти (RO, WORM, RW);

— по источнику питания (активные, пассивные, полупассивные/полуактивные);

— по рабочей частоте (LF, HF, UHF, NF UHF, SAW RFID);

— по исполнению (форм-фактор зависит от целей использования).

По типу используемой памяти RFID-метки делятся на [9]:

— RO (англ. Read Only) — данные записываются только один раз, сразу при изготовлении. Такие метки пригодны только для идентификации. Никакую новую информацию в них записать нельзя и их практически невозможно подделать.

— WORM (англ. Write Once Read Many) — кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти, которую в дальнейшем можно многократно читать.

— RW (англ. Read and Write) — такие метки содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны многократно.

Активные RFID-метки обладают собственным источником питания и не зависят от мощности считывателя, поэтому они читаются на большем расстоянии, имеют бóльшие размеры и могут быть оснащены дополнительной электроникой. Но такие метки наиболее дороги, а у батарей ограничено время работы (до 10 лет в зависимости от времени активности).

Так же активные метки в большинстве случаев более надёжны и обеспечивают самую высокую дальность и точность считывания [10]. Активные метки, обладая собственным источником питания (срок работы до 10 лет), также могут генерировать выходной сигнал большей мощности, чем пассивные, позволяя применять их в более агрессивных для радиочастотного

сигнала средах: жидкостях и металлах. Некоторые RFID-метки имеют различные встроенные в чип сенсоры, например, для мониторинга температуры, влажности, толчков/вибрации, света, радиации, газов в атмосфере и др.

Пассивные RFID-метки не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования, размещённого в метке, чипа низкого потребления и передачи ответного сигнала.

Полупассивные (полуактивные) RFID-метки по принципу работы похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип питанием только после получения сигнала от считывателя, что значительно увеличивает срок работы метки. При этом дальность действия этих меток зависит только от чувствительности приёмника считывателя. Таким образом, такие метки могут считываться на таких же расстояниях, что и активные.

Активность или пассивность метки может быть заложена при изготовлении, либо являться программной функцией универсальной метки, которая меняет режим работы метки в зависимости от настроек пользователя.

В таблице 1.1. перечислены свойства RFID-меток в зависимости от наличия источника питания в них.

Таблица 1.1. Свойства RFID-меток.

Тип RFID-метки	Максимальное теоретическое расстояние считывания	Свойства
Активная	До 100м	Требует источник питания, чей срок службы до 10 лет, могут быть оснащены дополнительной электроникой (датчики)
Пассивная	2 см – 10 м	Не требует источника питания (питается от считывателя), неограниченный срок эксплуатации
Полупассивная	До 100 м	Требует источник питания, но его срок службы гораздо дольше, чем в активной метке.

Размер и форма RFID-меток зависит от размеров внешней антенны, которая во много раз превосходит чип, и цели применения метки. В свою очередь, размер антенны напрямую влияет на дальность считывания метки. Сегодня применяются метки, располагающиеся в корпусах

различных размеров - от корпуса в виде гвоздя до бруска в 30х5 см. На практике максимальная дальность считывания пассивных меток варьируется от 10 см (согласно стандарту ISO 14443) до нескольких метров (стандарты EPC и ISO 18000-6), в зависимости от выбранной частоты и размеров антенны.

Классификация по частоте включает в себя LF, HF, UHF, NF UHF, UHF RTLS [11].

1.1.2. Метки диапазона LF (Low Frequency) 125—134 кГц

Метка данного диапазона содержит в качестве антенны проводную многовитковую катушку, подсоединенную к чипу. Катушка вместе с конденсатором входной цепи чипа образует резонансный контур магнитного поля, работающий на частоте 125 кГц для обычных меток и 135 кГц для меток чипирования животных. Катушка может быть плоской спиральной для меток-карточек, брелков, «шайб» и наклеек, или компактной цилиндрической, на ферритовом центральном сердечнике (метки-капсулы, метки-гвозди). См. рис. 1.3, 1.4.

Рис.1.3. LF-метка в виде стеклянной колбы для пометки животных.

Рис.1.4. Круглые LF-метки в виде наклейки.

Катушки меток в данном диапазоне содержат десятки витков провода и не могут быть выполнены «печатным» способом (в отличие от меток HF и UHF) – для этого используются специальные станки, которые наматывают катушку, скрепляют ее клеящим составом, а концы провода подсоединяют к чипу. Затем эта конструкция уже помещается в пластиковую карточку, брелок и т. д. Из-за такой сложной технологии изготовления LF метки не имеют перспектив удешевления.

LF-метки получили наибольшее распространение в системах контроля доступа на чипах и с протоколом обмена Marin SA, совместимыми с семейством EM4100 швейцарской компании EM Microelectronic. Вторыми по распространенности являются чипы и считыватели семейства Hitag (1, 2, S) нидерландской компании NXP Semiconductors. Такие метки используются для чипирования животных в соответствии со стандартами ISO-11784, ISO-11785, ISO-14223.

LF-метки почти все не поддерживают механизмы антиколлизии, т.е. одновременно в зоне считывания может быть только одна метка. В противном случае результаты будут непредсказуемы.

Чипы Hitag S поддерживают механизм антиколлизий. Но т.к. полоса пропускания частот в этом диапазоне мала, то при низкой скорости обмена данными с меткой (около 9600 бит), одновременно можно считать максимум 10 меток.

В СКУД считывание меток используется на расстоянии до нескольких сантиметров (proximity). Такие считыватели распространены и недороги, но они должны поддерживать определенный тип чипа метки и могут быть в разных исполнениях – настольные, настенные,

мобильные, поддерживают разные интерфейсы связи – USB, RS232 (последовательный порт ПК), RS485 (для витой пары), Wiegand (проводной интерфейс связи считывателя с СКУД контроллером, образованный от считывателя карточек с магнитной полосой).

Существуют LF-считыватели на большие для этого диапазона расстояния - до 1 м. Расстояние считывания любой метки определяется следующими факторами:

— Мощность считывателя (ограничена разрешенными нормами);

— Параметры чувствительности считывателя;

— Параметры чувствительности чипа метки;

— Размер антенны метки – чем больше, тем больше расстояние её регистрации;

— Размер антенны считывателя – чем больше, тем больше расстояние;

— Взаимная ориентации плоскости антенны метки и антенны считывателя – максимальная чувствительность при параллельных плоскостях, минимальная при перпендикулярных.

— Среда, через которую передаются радиоволны.

Для диапазона LF при размерах витка катушки около стандартной пластиковой карты, максимальное расстояние регистрации метки при лучшей взаимной ориентации равна ~0,7 м при размере антенны считывателя около 0,7 м. При уменьшении антенны считывателя пропорционально уменьшается максимальное расстояние регистрации метки.

1.1.3. Метки диапазона HF (High Frequency) 13,56 МГц

Высокочастотная метка (HF - high frequency) связывается со считывателем через магнитную составляющую радиосигнала, как и LF-метка. Антенна HF метки состоит из катушки в несколько витков, подключенной к чипу. Т.к. количество витков обычно не более 10, то катушка выполняется методом печати, что удешевляет метку и позволяет производить её в больших количествах. Для соединения катушки с чипом необходим переходной изолированный элемент, что усложняет изготовление HF-меток, в отличие от UHF меток, где в этом нет необходимости). HF-метки работают на частоте 13,56 МГц.

HF метки производятся в виде тонких наклеек, карточек, брелков, браслетов (рис.1.5).

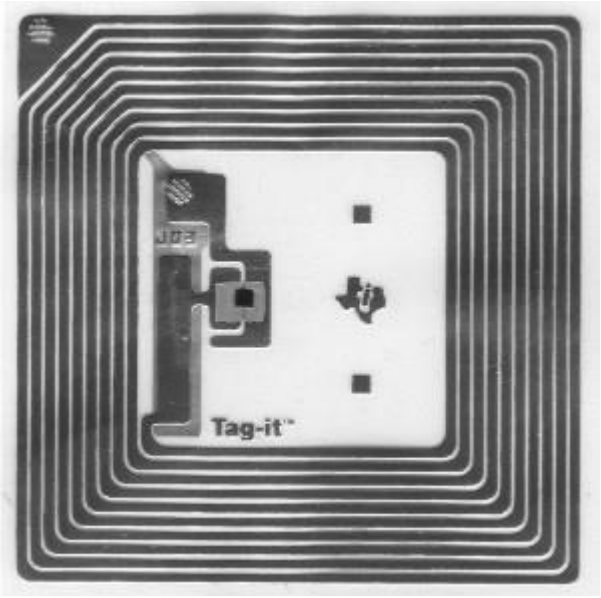


Рис.1.5. HF-метка в виде наклейки.

Для HF-меток действуют стандарты. В частности, в ISO/IEC 18000-3 определены основные параметры радиоинтерфейса. В ISO14443 и ISO 15693 подробно оговорены параметры HF систем, для малой (proximity, до нескольких сантиметров) и большой (vicinity, до 1 метра) дальности.

В HF метках поддержка механизма антиколлизий стандартизирована, но предназначен он только для чтения меток на относительно большом расстоянии и для считывания только основного идентификатора метки. Любые операции шифрованного обмена данными могут производиться только с одной меткой и с небольшого расстояния для предотвращения перехвата данных.

При антиколлизионном чтении меток в большой зоне возможно одновременное считывание до нескольких десятков меток за счет большей полосы пропускания и скорости обмена данных до 64 кбит/с.

Как и в LF, существует взаимное экранирование меток при их плотном прилегании друг к другу. Обычные HF-метки экранируются металлическими поверхностями, поэтому не работают или регистрируются только на близком расстоянии при расположении вблизи от них (1-5 мм). Однако есть специальные метки HF, рассчитанные на крепление на металлической поверхности. Как и любые метки, не работают в воде.

Считыватели для HF-меток, как и в LF, должны учитывать конкретный тип чипа метки, недороги и бывают в тех же исполнениях.

HF системы и считыватели на большие расстояния, до 1 метра, распространены гораздо меньше, хотя есть области их использования - в библиотечных системах автоматизации каталогизации и в качестве предотвращения кражи книг. Считыватели поменьше используются в библиотеках для считывания всех меток в стопке книг (5 – 7 шт. одновременно).

На практике для HF меток формата карточки максимальная дистанция регистрации метки в оптимальной взаимной ориентации антенн около 1 м при величине антенны считывателя 0,7 м. При уменьшении антенны считывателя пропорционально уменьшается максимальное расстояние считывания. HF-считыватели для 1 м расстояния существенно дороже обычных.

HF RFID метки используются в:

— системах контроля доступа персонала, посетителей, пациентов;

— транспортные и смарт-карты;

— библиотечные и архивные системы;

— перевозка багажа;

— прачечные;

— NFC-системы в смартфонах и связанной с ними умной электронике.

1.1.4. Метки диапазона UHF и NF UHF 860—960 МГц

За счет высокой частоты радиоволн обмен между считывателем и меткой происходит через полное электромагнитное поле, поэтому расстояния считывания достигают нескольких десятков метров для пассивных меток и до 100 м для активных.

Иногда используется магнитная составляющая поля на расстоянии до 20 см для регистрации метки в сложном окружении жидкостями или металлами (**NF UHF**, Near Field UHF) с частотами около 900 МГц. Полоса пропускания сигналов широкая, поэтому скорость обмена данными с меткой высокая.

Разрешенные частоты UHF разные для разных регионов мира и стран.

Основные региональные диапазоны [12]:

— Европа (ETSI): 865,6 ~ 867,6 МГц, включая более узкий диапазон РФ 866,6 ~ 867,4 МГц (без лицензии в режиме Listen Before Talk, до 921 Мгц требуется лицензия).;

— США (FCC): 902 ~ 928 МГц;

— Япония: 952 ~ 956,4 МГц (до 2018 года, а сейчас и в дальнейшем действует второй диапазон 916,7 ~ 920,9 МГц);

— Китай: 920,5 ~ 924,5 МГц.

В РФ широко распространены пассивные метки UHF стандарта EPC Class 1 Generation 2 (ISO/IEC 18000-63), кратко Gen2. Характеристики UHF меток стандарта Gen2 [13]:

— дальность считывания до 10 м (зависит от считывателя, антенны и конструкции самой метки);

— одновременное считывание до нескольких десятков уникальных меток в секунду;

— считывание одиночных меток при их перемещении через зону регистрации на скорости до 250 км/ч;

— очень низкая цена метки.

Метки данного стандарта просты и дешевы в производстве. Однако UHF-считыватели по-прежнему очень дороги, хотя обладают большей функциональностью по сравнению с RFID-системами других стандартов.

Обычно метка Gen2 имеет вид тонкой этикетки на бумажной или пластиковой основе. Внутри слой антенны и электронный чип, приклеенный к контактным зонам антенны. Производятся такие метки в виде рулонов, от которых отрезаются или отклеиваются отдельные метки для использования (рис.1.6.). Метки без корпуса называются инлей (inlay).

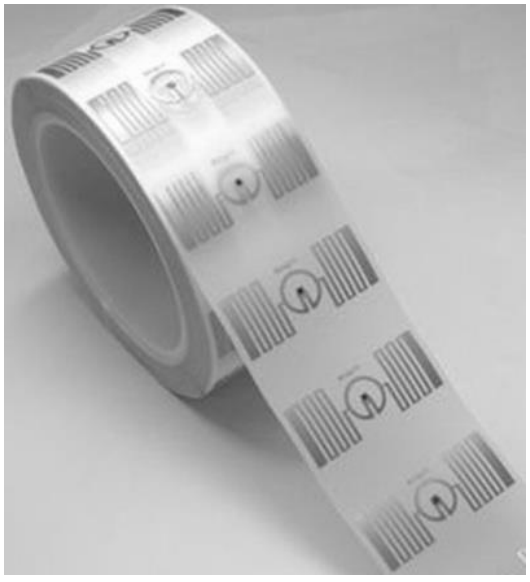


Рис.1.6. UHF-метки в рулоне.

Метки-инлеи встраиваются внутрь других корпусов в виде пластиковых карточек, брелков, специальных защищенных меток для сложных условий.

Отдельный тип меток – для закрепления на металле. Обычная метка-наклейка на металлической поверхности экранируется полностью, потому что не выступает над металлом. Но если поместить диэлектрическую прокладку в несколько миллиметров между металлом и самой меткой, то она уже будет работать, хотя и с большой потерей расстояния считывания по сравнению с меткой, расположенной далеко от металла. Метки на металл конструируются так, что их расположение не снижает расстояние считывания, или даже увеличивает, если метка расположена в нескольких сантиметрах от металлической поверхности. Необходимо учитывать, что такие метки имеют только одну рабочую сторону, которая не должна загораживаться металлом.

Считыватели для систем Gen2 производят любых видов – настольные, стационарные, мобильные, RFID-принтеры (печатают метки, считывают, записывают).

Свойства зон регистрации Gen2 очень зависят от типа и конструкции антенн считывателей, их поляризации, в отличие от витковых антенн LF и HF. Антенны с линейной поляризацией применяют в случаях стабильной ориентации меток в одном направлении. Но это редкость, чаще метки расположены произвольно. При произвольной ориентации необходимо использовать антенны с круговой поляризацией, которые хоть и менее чувствительны, но значительно стабильнее в считывании меток.

1.1.5. Метки UHF 2,4 ГГц для RTLS.

Диапазон 2,4 ГГц широко используются для активных меток (ISO 10374 RFID-идентификация грузовых контейнеров и железнодорожного транспорта), хотя стандартизирована и работа пассивных (ISO/IEC 18000-6C). Эти два стандарта мало распространены, и большинство реализаций закрыты от пользователя разработчиками и не совместимы друг с другом.

RTLS (Real-time Locating Systems — система позиционирования в режиме реального времени) — автоматизированная система, обеспечивающая идентификацию, определение координат, отображение на плане местонахождения контролируемых объектов в пределах территории, охваченной необходимой инфраструктурой. RTLS накапливает, обрабатывает и хранит информацию о местонахождении и перемещениях людей, предметов, мобильных механизмов и транспортных средств с целью мониторинга технологических и бизнес-процессов, сигнализации об отклонениях от регламентов, а также с целью ретроспективного анализа тех или иных процессов и ситуаций [10].

Активные метки UHF для RTLS 2,4 ГГц имеют собственный источник питания. Эти метки излучают радиосигнал, в отличие от пассивных и полупассивных меток, что позволяет использовать более эффективные схемы с большей чувствительностью, лучшим качеством приема и передачи сигнала.

Почти все активные метки построены на основе микроконтроллеров с дополнительными цифровыми и аналоговыми портами ввода-вывода (подключение датчиков, линий управления, кнопок) и часами, встроенным или внешним приемопередатчиком. Обычный срок службы батарей питания 1 - 5 лет и зависит от способа работы метки и емкости батареи.

Для многих современных активных меток в качестве протокола обмена используется стандарт IEEE 802.15.4 (ZigBee).

Системы определения места нахождения в реальном времени (RTLS) строятся на основе разных технологий:

— ультразвуковые,
— инфракрасные,
— ГНСС GPS и ГЛОНАСС,
— на основе сотовых сетей общего пользования,
— на основе беспроводных сетей Wi-Fi (IEEE 802.11),
— системы ближнего поля ~900 МГц (Near Field UHF),
— пассивные поверхностно-акустические метки (SAW RFID, ПАВ RFID).

Также часто под определением местонахождения понимается присутствие метки в определенной зоне. Если в помещении установлен один или несколько считывателей, то фактом перемещения объекта-метки будет являться только её регистрация другим считывателем.

Внутренние системы RTLS предполагают определение положения объекта-метки внутри заданной зоны ~10-200 м. По углам или сторонам зоны располагают три или больше ридера и/или маяки (beacon). Их положение фиксируется на плане относительно друг друга. Положение метки определяется методом трилатерации - вычисления расстояния от метки до ридера/маяка (при трех приемниках/маяках) или мультилатерации (при большем числе приемников или маяков для повышенной точности).

Если требуется небольшая точность, то для определения расстояния используется его вычисление по силе принимаемого радиосигнала (RSSI – Received Signal Strength Indication). Этот метод дает очень большую погрешность точности и сильно зависит от алгоритмов и техниче-

ских решений для устранения переотражений сигнала, помех и других факторов. Примерная точность 1-10 м в комнате 20 м^2.

Системы UHF RTLS диапазона 2,4 ГГц строятся на основе измерения расстояния по времени распространения сигнала (методика CSS - Chirp Spread Spectrum) – использование коротких линейно-частотно модулированных импульсов (стандарты ISO/IEC 24730) или SDS-TWR (Symmetrical Double-Sided Two Way Ranging) – симметричное двухстороннее двунаправленное определение расстояния (стандарт IEEE 802.15.4 ZigBee).

Точность определения местонахождения в UHF RTLS зависит от:

— на системы на основе RSSI влияет ориентация и направление излучения/приёма антенн;

— присутствие крупных экранирующих предметов в прямой видимости между меткой и приемником;

— большие поверхности, отражающие радиоизлучение, сбоку или сзади метки – за счет многолучевости (методика CSS уменьшает это влияние).

Реальная лучшая точность определения местоположения с использованием UHF RTLS систем порядка 1-3 м при размерах зоны контроля до 100x100 м [11].

1.2. Технология NFC

1.2.1. Стандарты и описание технологии NFC

NFC (Near Field Communication) – это беспроводная технология, которая позволяет передавать данные между двумя устройствами (смартфонами, планшетами или другими устройствами), поддерживающими технологию NFC [14].

Так же, как и в стандарте ISO 14443 (стандарт бесконтактных пассивных карт RFID ближнего радиуса действия (до 10 см) на магнитосвязанных индуктивностях.), в NFC связь поддерживается посредством индукции магнитного поля, где две рамочные антенны располагаются в пределах ближнего поля друг друга, образуя трансформатор с воздушным сердечником.

Технология подчиняется стандартам ISO/IEC 18092 / ECMA-340: Near Field Communication Interface and Protocol-1 (NFCIP-1) [15],

ISO/IEC 21481/ ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2) [16].

Наряду с ISO, существует некоммерческая ассоциация NFC Forum, основанная компаниями NXP Semiconductors, Sony и Nokia, для продвижения и использования технологии. NFC Forum

содействует реализации и стандартизации технологии NFC для гарантии взаимодействия устройств NFC.

NFC технология действует только на близких расстояниях порядка 2-10 см на той же частоте, что и HF RFID – 13,56 Мгц. Фактор близости делает технологию NFC относительно безопасной для использования на близких расстояниях, так как другое устройство не сможет считать с метки информацию или использовать вашу метку для нежелательного действия или отслеживания. Стандарты NFC не гарантируют безопасность соединения и предлагают защиты против подслушивания. Для безопасной связи нужно использовать шифрование поверх NFC. В любом случае, возможно подслушать данные только с расстояния в несколько метров [17].

NFC-устройство может проявлять себя, в зависимости от конструкции или задачи:

— Как обычная пассивная HF-метка. При этом она называется NFC-tag. Как минимум, должна передать свой уникальный идентификационный номер считывателю. Пример современного применения, бесконтактная карта для проезда в метро – смартфон подносится местом расположения NFC-антенны к считывателю карт турникета. При этом имеется возможность узнать число оставшихся поездок с помощью специальной программы на смартфоне;

— Как считыватель, который может использоваться для чтения HF-меток или других NFC-устройств, находящихся в режиме пассивной метки. В NFC-метках может быть записана самая разнообразная короткая информация — веб-ссылка, адрес электронной почты, телефон для связи и т.д. При этом в считывателе может быть заложен алгоритм программных действий на обнаружение определенного идентификатора (метки);

— Как средство связи двух активных NFC-устройств для двухстороннего обмена данными при расположении их близко друг к другу. Устройства NFC могут одновременно получать и передавать данные. Так они могут обнаруживать противоречия, если полученный сигнал не соответствует переданному.

Для использования технологии NFC, кроме модуля связи, необходима специальная программа в смартфоне, которых существует множество.

Технология NFC также используется как посредник для установления быстрого и бесконтактного начального соединения по технологии Bluetooth или безопасной разблокировки мобильного устройства. Связь между устройствами устанавливается мгновенно (около 0,1 с), в отличие от технологии Bluetooth (6 с).

Максимальная скорость передачи данных NFC 424 кбит/с, что на порядок меньше, чем Bluetooth (24 Мбит/с). В отличие от Bluetooth, NFC совместима с существующими RFID-структурами, потому что объединяет ранее существовавшие стандарты ISO 14443 (ближний RFID), ISO 15693 (дальний RFID) в стандарт ISO/IEC 18000-3. Тип сети в технологии NFC точка-точка, т.е. связь возможна только между двумя устройствами.

1.2.2. Классификация и технические характеристики чипов NFC

Для обеспечения совместимости NFC устройств устанавливаются специальные стандарты на международном NFC форуме. Эти стандарты обеспечивают совместимость чипов таких типов: Ultralight, Ultralight C, Standard (Classic) 1K, Desfire 4k, NTAG203 со всеми действующими и новыми устройствами. Однако, чип типа Classic 1K редко соответствует стандартам NFC Форума. Прогнозируется увеличение количества устройств, несовместимых с Classic 1к.

Память NFC устройств имеет объём порядка от сотни байт до десятков килобайт. Каждый байт равен примерно одному символу открытого текста. Однако для записи на устройство всегда используются дополнительный объём скрытой от пользователя служебной информации.

Чипы NFC устройств разделяют на следующие типы, в зависимости от производителя и используемого стандарта, основные их них приведены в Табл. 1.2. [18], [19].

Таблица 1.2. Характеристики и типы некоторых чипов NFC

Характеристика / тип чипа	**NXP Ultralight**	**NXP Ultralight C**	**Standard (Classic)1K**	**NXP NTAG216**
Объём памяти	64 байта	192 байта	1024 байта	924 байта
Объём памяти, доступной пользователю	46 байт	137 байт	716 байт	**888 байт**
Максимальная длина URL без http://www	41 символов	132 символов	256 символов	168 символов
Длина открытого текста	39 символов	130 символов	709 символов	881 символ
Совместимость с мобильным телефоном	Да	Да	Нет	Да
Использование	Экономичность,	Для приложе-	Общее приме-	Любое при-

Характеристика / тип чипа	**NXP Ultralight**	**NXP Ultralight C**	**Standard (Classic)1K**	**NXP NTAG216**
	короткие ссылки, смарт-постер и общее NFC применение	ний с обязательным шифрованием	нение и при высоких нагрузках	менение
Соответствие спецификации совместимости стандарту NFC Forum Type 2	Да	Да	Нет	Да
Уникальный идентификационный номер	Да	Да	Да	Да, 7 бит
Шифрование	Нет	3DES	Crypto-1	32 бит пароль
Средний диапазон сканирования. Показатель относительного расстояния диапазона сканирования чипа.	7	4	6	16

NDEF - это стандарт форматирования и обмена данных, разработанный NFC Forum. Все типы NDEF-сообщений могут быть записаны во все типы NFC чипов. В зависимости от размера доступной пользовательской памяти чипа, необходимо учитывать тип данных, которые будут на него записаны. Каждая NDEF запись содержит две части:

— Тип записи (record type) - указывает тип данных в записи

— Данные записи (payload).

В этих частях содержится описание простого действия для NFC устройства при контакте с NFC меткой. Более сложные действия могут быть произведены с помощью специального ПО на NFC устройстве.

В таблице 1.3. приведены некоторые сравнительные параметры NFC чипов известных производителей [18], [19].

Таблица 1.3. Сравнительные параметры чипов NFC

NFC чип	**Пользовательская память**	**Сравнительная скорость чтения**	**Блокировка записи**	**Условная относительная стоимость**	**Поддержка NDEF формата**	**Совместимость NFC Forum**
NXP NTAG210	48 байт	Очень высокая (106 кбит/с)	Да	$	Да	Да
NXP NTAG212	128 байт	Очень высокая (106 кбит/с)	Да	$	Да	Да
NXP NTAG213	144 байта	Очень высокая (106 кбит/с)	Да	$	Да	Да
NXP NTAG 413 DNA	160 байт	Очень высокая (424 кбит/с)	Да	$$$	Да	Да
NXP NTAG 215	504 байта	Очень высокая (106 кбит/с)	Да	$$	Да	Да
NXP NTAG216	888 байт	Очень высокая (106 кбит/с)	Да	$$	Да	Да
NXP Ultralight	46 байт	Средняя	Да	$	Нет	Да
NXP UltralightC	142 байта	Средняя	Да	$$	Нет	Да
Kovio 2Kb	230 байт	Высокая	Нет перезаписи	$$	Иногда	Да
Innovision Topaz (120b)	90 байт	Средняя	Да	$$$	Нет	Да

NFC чип	**Пользовательская память**	**Сравнительная скорость чтения**	**Блокировка записи**	**Условная относительная стоимость**	**Поддержка NDEF формата**	**Совместимость NFC Forum**
Innovision Topaz (512b)	454 байта	Средняя	Да	$$	Нет	Да
NXP DESFire EV1 (2K)	2046 байт	Средняя	Да	$$$	Нет	Да
NXP DESFire EV1 (4K)	4094 байта	Средняя	Да	$$$	Нет	Да
NXP DESFire EV1 (8K)	**7678 байт**	Медленная	Да	$$$$	Нет	Да
NXP Mifare (1K)	716 байт	Медленная	Симуляция	$$	Нет	Нет
NXP Mifare (4K)	3356 байт	Очень медленная	Симуляция	$$$	Нет	Нет
NXP Mifare Mini	190 байт	Средняя	Симуляция	$$	Нет	Нет
NXP ICODE SLI	106 байт	Высокая	Да	$$	Нет	Да
NXP ICODE SLI-X	106 байт	Высокая	Да	$$	Нет	Да

Почти все современные метки NFC имеют возможность шифрования 128-битным паролем, защиту от коллизий, возможность задания уникального пользовательского идентификатора и могут хранить данные 10-50 лет.

1.3. Технологии Bluetooth

В настоящее время существует три широко распространенных стандарта на беспроводные сети: Bluethooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4) и Wi-Fi (IEEE 802.11). Оборудование для этих сетей не требует получения лицензии, хотя и требует регистрации [20].

Bluetooth — производственная спецификация беспроводных персональных сетей (Wireless personal area network, WPAN). Bluetooth обеспечивает обмен информацией между компьютерами, мобильными телефонами, периферийными устройствами, гарнитурами на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи в радиусе около 50 м (зависит от преград и помех) [21].

Стандарт Bluetooth относят к физическому уровню модели OSI. Он организован в виде "пикосетей" (piconet), в которых одно ведущее устройство осуществляет взаимодействие не более чем с семью ведомыми (классический вариант, для Bluetooth LE больше). Ведомые устройства могут взаимодействовать друг с другом только через ведущее. Каждое устройство может быть членом четырех пикосетей одновременно, но главным может быть только в одной из них. Такое устройство выполняет роль моста между пикосетями. Несколько взаимодействующих пикосетей образуют так называемую scatternet ("разбросанную сеть") [22].

В Bluetooth переход с одной частоты на другую меняется 1600 раз в секунду и выполняется по случайному закону, который устанавливается для каждого соединения индивидуально, что значительно повышает защиту информации. Скорость передачи базового уровня стандарта около 435 Кбит/с, однако последняя расширенная версия допускает теоретическую скорость около 24 Мбит/с (Wi-Fi составляющая).

Стандартом Bluetooth разрешен следующий ряд излучаемых мощностей, делящий все устройства bluetooth на три класса (Таблица 1.4):

Таблица 1.4. Стандартизированные классы мощности Bluetooth

Класс	**Максимальная мощность, мВт**	**Максимальная мощность, дБм**	**Радиус действия, м (прямая радиовидимость)**
1	100	20	100
2	2,5	4	16
3	1	0	1

Принцип действия Bluetooth основан на радиопередаче. Связь происходит в свободном от лицензирования диапазоне 2,4-2,4835 ГГц ISM (Industry, Science and Medicine), который ис-

пользуется в различных бытовых приборах и беспроводных сетях. Протокол поддерживает соединения типа «точка-точка» и «точка-многоточка» [23].

Bluetooth имеет многоуровневую архитектуру, состоящую из основного протокола, протоколов замены кабеля, протоколов управления телефонией и заимствованных протоколов.

В настоящее время существует множество версий стандарта, последняя из которых Bluetooth 5.0 от 2016 г., которая включает в себя и поддерживает предыдущие версии стандарта.

Начиная с Bluetooth 4.0 стандарт включает в себя три стека протоколов радиосвязи (2,402 ГГц - 2,48 ГГц):

- Классический bluetooth (3 Мбит/с с низким энергопотреблением);
- Высокоскоростной Bluetooth (основан на протоколах Wi-Fi);
- Bluetooth LE (Low Energy) – с низким энергопотреблением (0,01-0,5 Вт).

Для взаимодействия двух устройств через Bluetooth необходимо, чтобы они имели одинаковый профиль – набор функций и возможностей, стандартизированных группой разработчиков Bluetooth SIG (Special Interest Group). Например, Basic Imaging Profile (BIP) — для пересылки изображений между устройствами и включает возможность изменения размера изображения и конвертирование в поддерживаемый формат принимающего устройства.

Соединение двух устройств происходит в три этапа:

1. Генерируется начальный ключ, для чего устройства требуют ввести пин-код, одинаковый для обоих устройств.
2. Генерируется ключ связи в процессе, называемом pairing (сопряжение).
3. Взаимная аутентификация (mutual authentication)

Защищенность технологии имеет недостатки. Уязвим сам процесс сопряжения, во время которого возможен взлом пин-кода и вмешательство в работу устройств. При потере сигнала, устройство должно быть переподключено, т.е. в тот момент связь будет уязвима для взлома, и чем больше радиус действия передатчика, тем более уязвимы устройства. Современные компьютерные мощности могут подобрать пин-код стандартной длины до 8 символов за такое же количество секунд во время процесса сопряжения, однако без пин-кода расшифровать трафик нереально в разумные сроки [24].

Технология Bluetooth имеет достоинства: небольшие размеры оборудования, простота использования, безопасность передачи информации благодаря аутентификации и кодированию, стандартизация.

Недостатки, которые сейчас активно устраняются, это относительно большое потребление энергии и невозможность построения сетей сложной конфигурации. Последнее связано с тем, что Bluetooth создан для беспроводной замены кабелей периферийных устройств компьютера, а не для создания беспроводной локальной сети.

1.4. Технология ZigBee

Технология ZigBee - это набор протоколов и расширений к международному стандарту IEEE 802.15.4, реализация которых обеспечивает информационную совместимость устройств различных производителей выполняющих низкоскоростной обмен данными по радиоканалу на небольшие расстояния [25].

Разработкой стандарта ZigBee занимается ZigBee Alliance с 2004 г. Стандарт описывает правила передачи информации на расстояние нескольких десятков метров с максимальной скоростью 250 кбит/с. Стандартом ZigBee предусмотрено три частотных диапазона – 2,4 ГГц (более 16 каналов во всем мире), 915 МГц (30 каналов, США) и 868 МГц (1 канал, Европа). Максимальная скорость передачи данных для этих эфирных диапазонов составляет 250 кбит/с, 40 кбит/с и 20 кбит/с соответственно.

Стандарт создавался для малой дальности действия, низкой стоимости, низкого энергопотребления, малой скорости передачи данных, небольших размеров и простоты устройств. Устройства ZigBee используются там, где применение Bluetooth экономически невыгодно, и где не требуется высокая скорость передачи данных. В стандарт закладывалась основная область применения ZigBee - передача информации от движущихся частей заводских механизмов, промышленные системы управления и мониторинга, беспроводные сети датчиков, отслеживание маршрутов движения и местоположения имущества и инвентаря, "интеллектуальное" сельское хозяйство, системы охраны [22].

ZigBee Alliance разработал профили приложений для проектов «умный дом», рационального использования энергии (ZigBee Smart Energy 1.0/2.0), телекоммуникационных приложений, различных видов ухода, игрушек, автоматизации строительства.

Между тем, стандарт ZigBee не ограничивает мощность передатчика, - она регулируется государственными нормативными документами в области радиосвязи. Поэтому на рынке присутствуют решения, позволяющие обеспечить связь дальностью 80 м в помещении и до 1 км в прямой видимости, за счет мощного передатчика (10 мВт) и специальной антенны. Стандарт обеспечивает описание важнейших функций устройств ZigBee:

- работа в режиме реального времени;
- предотвращение коллизий;
- комплексная поддержка защиты сетей;
- управление расходом энергии.

При начале работы устройство сначала проверяет доступность частоты, и только после этого начинает передачу. Поддерживается 128 битное шифрование передаваемых данных по протоколу AES. На рынке представлены чипы ZigBee, представляющие собой микроконтроллер с радиопередатчиком с размером Flash-памяти от 60 Кб до 128Кб. Возможно использовать отдельно радиомодуль с любым процессором и микроконтроллером.

ZigBee определяет три роли устройств [26]:

— координатор (ZC) - формирует топологию сети и может устанавливать мосты с другими сетями. В каждой сети определен только один координатор, который хранит информацию о сети и ключи доступа к ней;

— маршрутизатор (ZR) – посредник, передает данные от других устройств по заданному маршруту;

— конечное устройство (ZED) - передает данные только координатору или маршрутизатору, при этом не может связываться с другими конечными устройствами. Поэтому конечное устройство большую часть времени пребывает в режиме сна, что позволяет экономить энергоресурс. В производстве значительно дешевле координатора и маршрутизатора.

Стандарт ZigBee соответствует уровням модели OSI: физическому, канальному, сетевому, приложений. Более подробно соответствие уровней представлено в таблице 1.5 [22].

Таблица 1.5. Уровни модели OSI для стандарта ZigBee.

Номер уровня	**Название уровня OSI**	**Название уровня ZigBee**	**Функции**
7	**Прикладной**	APL (APS, ZDO и Application Objects) ZigBee	Передача сообщений, обнаружение устройств, определение роли устройств
6	**Уровень представления**	-	-
5	**Сеансовый**	-	-
4	**Транспортный**	-	-
3	**Сетевой**	NWK ZigBee	Безопасность, маршрутизация
2	**Канальный (передачи данных)**	LLC IEEE 802.15.4	CSMA/CA*, передача маячков, синхронизация
		SSCS IEEE 802.15.4	
		MAC IEEE 802.15.4	
1	**Физический**	PHY IEEE 802.15.4	Радиоканал 2,4 ГГц

*CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) —сетевой протокол канального уровня модели OSI, по нему проверяется чистота канала передачи данных и распознаются и избегаются коллизии.

Координатор на сетевом уровне организует новую сеть и назначает адреса новым устройствам сети. Без него сеть невозможна.

Топология Zigbee-сети может быть в виде точка-точка, звезды, дерева и самовосстанавливающейся ячеистой (mesh) сети (рис.1.7). А также иерархической или одноранговой. Ячеистая сеть всегда одноранговая, т.е. в ячеистой сети все устройства равноправны и могут передавать данные между собой. Сети можно объединять друг с другом, если они находятся в радиовидимости друг друга, при этом меняются роли связующих устройств.

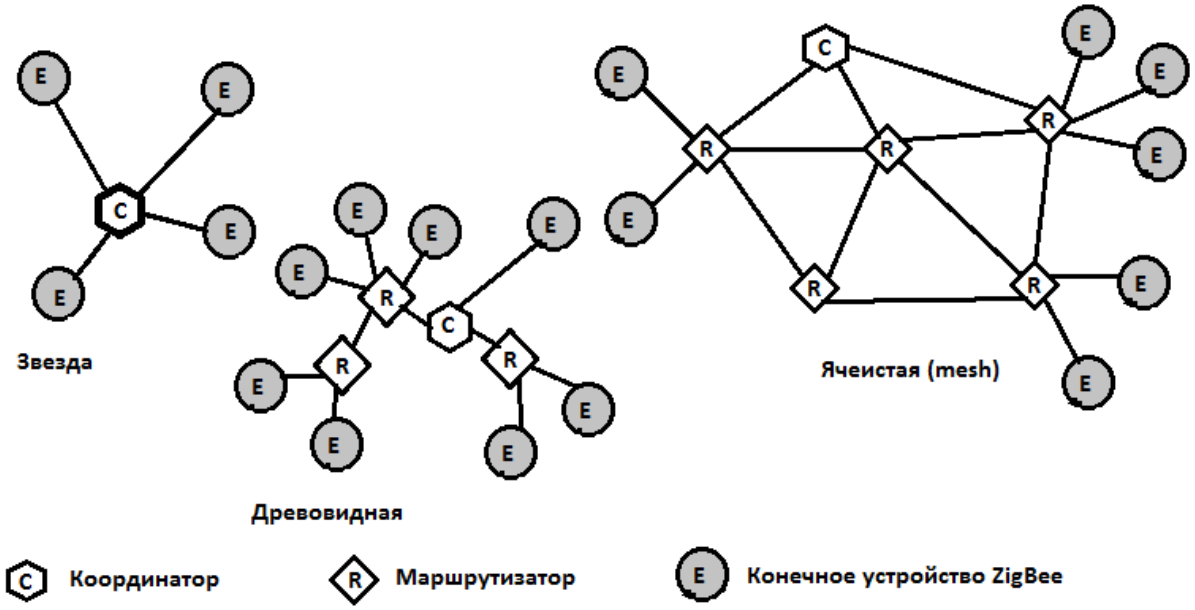


Рис.1.7. Виды топологии сети ZigBee.

В топологии звезды любое устройство может общаться только с координатором, который инициализирует и обслуживает сетевые и конечные устройства.

В древовидной и ячеистой сетях помимо координатора и конечных устройств, присутствуют маршрутизаторы, расширяющие сеть.

Стандарт предусматривает возможность выбора алгоритма маршрутизации данных. В сети с древовидной топологией используется иерархическая и маячковая маршрутизация. Сеть ZigBee может быть двух видов: с включенными и отключенными маячками.

Безмаячковая сеть ZigBee использует механизм доступа к каналам, т.е. маршрутизаторы организуют каналы между устройствами для передачи данных. Это энергозатратный вариант сети.

Маячковая сеть ZigBee осуществляет периодическую рассылку широковещательных сообщений - маячков для связи с другими устройствами и для подтверждения присутствия устройства в сети. Т.е. в таких сетях узлы должны быть активны только при передаче маячкового сообщения.

Процесс передачи данных в таких сетях представлен на рис.1.8 [22].

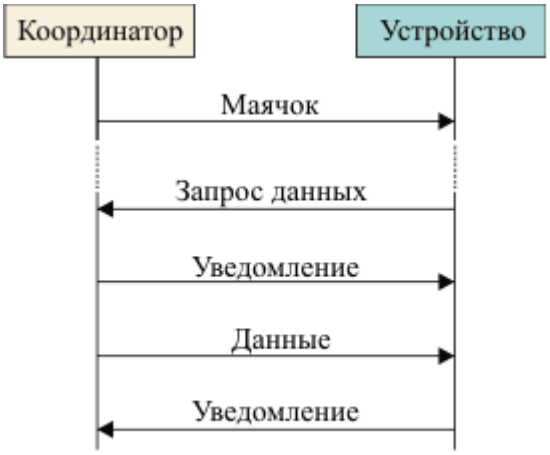


Рис.1.8. Схема процесса передачи данных в маячковой сети ZigBee.

Для передачи данных координатор помещает в маячок информацию о своей готовности передавать другому устройству (рис. 1.8). Каждое устройство периодически анализирует содержание маячка на наличие сообщения о готовности к передаче.

Энергоэффективность является ключевой проблемой технологии ZigBee. Для её решения применяются два подхода: уменьшение количества узлов, участвующих в переадресации и маршрутизации (маршрутизаторов), т.е. программный контроль топологии сети, что уменьшит энергопотребление в два раза [27].

Второй подход – использование схем планового пробуждения через протоколы канального уровня (по требованию, по графику, случайное) [28].

На сегодняшний день организация ZigBee Alliance разработала для интернета вещей (IoT) стандарт ZigBee PRO 2017, который обладает улучшенными характеристиками [29]:

— устанавливает обратную совместимость с предыдущими версиями стандарта для новых устройств.

— Энергоэффективность, по заявлением разработчиков, достигла уровня, когда солнечная батарея размером с кончик пальца может обеспечить отправку радиосообщения каждую минуту.

— Устройствам ZigBee требуется около 32 Кб для хранения программного кода и около 1 Кб для хранения данных.

— Устройства защищены от распространенного в интернете типа атак отказа в доступе (DDoS), потому что сеть ZigBee не подключена напрямую к интернету.

Представленные возможности стандарта ZigBee PRO 2017 превосходят по энергоэффективности и нетребовательности к объему памяти схожие технологии Bluetooth, Wi-Fi, NFC и др.

1.5. Технология Wi-Fi

Wi-Fi — семейство стандартов передачи данных по радиоканалам, основанное на стандарте IEEE 802.11, а также торговая марка ассоциации Wi-Fi Alliance для беспроводных компьютерных сетей. По сути, является беспроводным расширением сетей стандарта Ethernet и используется там, где неудобно или невозможно использовать проводные сети в силу разных причин.

Принцип работы технологии Wi-Fi состоит в следующем. Схема сети Wi-Fi может содержать минимум одну точку доступа и одного клиента. Предусмотрено подключение двух клиентов друг к другу напрямую.

Точка доступа Wi-Fi транслирует свой неуникальный идентификатор сети (SSID) в виде набора символов на скорости 0,1 Мбит/с каждые 100 мс, что является минимальной скоростью передачи данных для стандартов Wi-Fi. Зная SSID сети, клиент проверяет возможность подключения к этой точке доступа. При приёме нескольких точек доступа с одинаковыми SSID приёмник выбирает точку с наилучшим уровнем сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта [30].

Стандарт оставляет производителю свободу выбора многих аспектов построения беспроводных Wi-Fi-сетей.

В состав стандарта 802.11 входят несколько протоколов, различающихся скоростью передачи данных и частотой: 2,4 ГГц, 2,5 ГГц и 5 ГГц. На сегодняшний день максимальная теоретическая скорость Wi-Fi соединения по стандарту 802.11ac составляет 6,77 Гбит/с [31].

Технологию Wi-Fi относят к физическому и канальному уровням модели OSI.

Таблица 1.6. Уровни модели OSI для Wi-Fi/IEEE 802.11 [16]

Номер уровня	**OSI модель**	**Сеть**	**Функции**
7	Прикладной	-	-
6	Уровень представления	-	-
5	Сеансовый	-	-
4	Транспортный	-	-
3	Сетевой	-	-
2	Канальный (передачи данных)	Подуровень LLC	-
		Подуровень MAC	
1	Физический	Подуровень PLCP	Беспроводная передача, оценка состояния эфира
		Подуровень PMD	

Предотвращение (но не обнаружение) коллизий является основным в беспроводных сетях, поскольку в них, в отличие от проводных сетей, передатчик заглушает принимаемый сигнал. Поэтому технология Wi-Fi использует метод доступа к сети CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance — сетевой протокол канального уровня модели OSI, по нему проверяется чистота канала передачи данных, распознаются и избегаются коллизии.), в котором использованы следующие принципы для снижения вероятности возникновения коллизий:

- Перед началом передачи точка сообщает время, которое она будет занимать канал связи.
- Следующая точка не может начать передачу, пока не истечет зарезервированное ранее время;
- Участники сети узнают факт принятия их сигналов, только получив подтверждение от принимающей точки.
- Две одновременно работающие точки смогут узнать об этом только когда не получат подтверждение о приеме;
- При неполучении подтверждения, участники сети ждут случайный промежуток времени до повторной передачи.

Дальность связи средствами Wi-Fi сильно зависит от условий распространения электромагнитных волн, типа антенны и мощности передатчика. Типовые значения, указываемые изготовителями Wi-Fi оборудования, составляют 100-200 м в помещении и до нескольких километров на открытой местности с применением внешней антенны и при мощности передатчика 50...100 мВт.

1.6. Технология IEEE 802.22 WRAN

Институт инженеров электротехники и электроники (IEEE) в 2011 г. выпустил стандарт беспроводных региональных сетей IEEE 802.22 WRAN (Wireless Regional Area Network) или White space. Устройства, поддерживающие этот стандарт, позволяют принимать данные на скорости до 22 Мбит/с на расстоянии до 100 км от ближайшего передатчика [32].

IEEE 802.22 WRAN — стандарт беспроводных сетей, соответствует физическому и канальному уровню модели OSI с типом соединения точка-многоточка (point-to-multipoint). Стандарт предназначен как для работы с профессиональными фиксированными базовыми станциями, так и с портативными пользовательскими модемами. Обмен данными происходит на свободных (white space) нелицензируемых частотах ОВЧ/УВЧ (54–862 МГц) телевизионного вещания. Радиус покрытия для фиксированного модема составляет 10-100 км, максимальная скорость до 22 Мбит/с при мощности передатчика 4Вт.

Стандарт описывает необходимость геопозиционирования (GPS или наземное) для работы системы. Это позволяет узнать регион размещения точки и по базе данных определить, какие каналы заняты в конкретной местности, а также осуществлять эффективную маршрутизацию данных. Для определения местоположения по GPS у каждого абонентского устройства будет расположено GPS-оборудование, либо положение определяется менее точно по информации сети. Данные о местоположении передается на базовую станцию по протоколу NMEA 0183 (текстовый протокол связи в GPS) [33].

Стандарт опирается на технологию когнитивной радиопередачи («умного» радио), которая обеспечивает подстройку параметров устройств сети так, чтобы передача данных велась на свободных нелицензируемых частотах. Это происходит следующим образом: постоянно анализируется спектр входящего радиосигнала, фоновые радиосигналы, поведение пользователей сети. Базовая станция, имея всю информацию о текущем частотном диапазоне и учитывая свое местоположение (по GPS или наземным каналам), определяет частоты для связи с пользователями сети. Когда связь установлена, базовая станция продолжает наблюдать за частотами, и при обнаружении новых сигналов, сразу же перестраивается на другие частоты.

Стандартом предполагается, что для покрытия зоны с радиусом в 30 км потребуется мощность излучения в 4 Вт [34].

На базовой станции размещается ненаправленная антенна для равномерного покрытия, либо секторная антенна, если в зоне абоненты распределены неравномерно или для связи с соседними базовыми станциями. На стороне клиента устанавливается ориентированная на бли-

жайшую станцию узконаправленная антенна. Кроме неё, в клиентском оборудовании размещена ненаправленная сканирующая антенна для работы «умного» радио и GPS-антенна (опционально).

В стандарте предусмотрено три вида схем модуляции радиосигнала. Схемы отличаются между собой объемом данных, который можно закодировать в одном символе. Схема модуляции выбирается оборудованием по условиям текущей передачи. Чем выше скорость, тем ниже надежность (выше вероятность возникновения ошибки). Таким образом, сеть постоянно подстраивается под каждого пользователя через балансировку между скоростью и помехоустойчивостью.

Для организации многопользовательского доступа используется техника частотно-временного разделения каналов (Orthogonal Frequency Division Multiple Access, OFDMA), основанная на технологии мультиплексирования сигнала с ортогональным частотно-временным разделением каналов (Orthogonal Frequency Division Multiplexing, OFDM). В OFDM доступные частоты делятся между пользователями сети. OFDMA и OFDM также используются в стандартах WiMAX и LTE.

OFDM может противостоять многолучевому отражению, которое возникает из-за препятствий между базовой станцией и абонентом. Для этого в OFDM применяют специальную вставку, так называемый циклический префикс. Для надежности передачи данных в 802.22 предусмотрено использование кодов ошибок (коды Галлагера), которые представляют пока лучший механизм корректировки ошибок при передаче по каналу связи с шумами в ограниченной полосе.

Для защиты лицензируемых частот для исключения помех необходимо выдерживать частотный интервал, чью ширину рекомендуют делать сопоставимой с шириной одного канала. Практически нужно иметь пробелы размером от трех каналов (один информационный и два защитных по бокам) и более [34].

Отличие стандарта IEEE 802.22 WRAN от смежных стандартов, в особенности от IEEE 802.16 WiMax, в том, что 802.22 ориентирован на сельскую местность, поэтому его зона покрытия в несколько раз больше, чем у WiMAX (100 км против 5 км).

Хорошую дальность действия сигнала удалось достичь благодаря уменьшению рабочих частот, обычно используемых в Wi-Fi, WiMax или LTE для передачи информации. Технология WRAN хорошо справляется со стенами и другими препятствиями. Недостаток - меньшие частоты (длинные волны) требуют больших антенн.

1.7. Технология IEEE 802.16 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) — жаргонное название телекоммуникационной технологии, разработанной WiMAX Forum с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств. Основана на стандарте IEEE 802.16, который также называют Wireless MAN [35].

Стандарт использует диапазоны частот 2-11 ГГц и 10-66 ГГц. Для первого диапазона (сантиметровый и миллиметровый диапазон) необходима прямая видимость, а для второго нет. Стандарт поддерживает сетевые топологии типа точка-мультиточка и ячеистую (mesh), технологии частотного (FDD) и временного разделения (TDD), технологию quality of service (QoS, вероятность того, что сеть связи соответствует заданному соглашению о трафике, или вероятность прохождения пакета между двумя точками сети). В узком техническом значении, этот термин означает набор методов для управления ресурсами пакетных сетей. Возможна передача звука и видео. Стандарт определяет пропускную способность 120 Мбит/с на каждый канал в 25 МГц.

Существует несколько версий стандарта (802.16d-2004 и 802.16e-2005), которые несовместимы между собой, т.к. разработчикам на тот момент не удалось достичь компромисса между целями применения технологии. Ведется разработка унифицированного стандарта WiMAX для фиксированных и мобильных пользователей.

Сеть WiMAX состоит из базовых станций, клиентского оборудования, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом. Минимум одна базовая станция соединяется с интернет-провайдером с помощью проводного соединения.

В WiMAX сетях используется алгоритм планирования, который гарантирует любому пользователю при подключении выделенный слот на точке доступа, в отличие от Wi-Fi сетей, где все пользователи, которые хотят передать информацию через точку доступа, сортируются по расстоянию (силе сигнала), приоритет для более доступных пользователей. Это чревато обрывом связи для более удалённых станций.

1.8. Технологии Bluetooth-маяков (beacons)

Bluetooth-маяки (биконы, beacons), далее маячки – класс автономных устройств, работающих по технологии Bluetooth Low Energy (BLE) на передачу (реже – приём) информации смартфону пользователя на расстоянии около 50 м (дальность вещания технологии BLE).

Маяки не являются отдельным классом радиовещательных технологий, но рассматриваются как отдельная технология доставки информации пользователю, в том числе и для определения его местоположения.

Существует несколько ведущих производителей и стандартов маяков, как и разработчиков приложений для разных областей их применения. В настоящее время технология маяков применяется для:

— как альтернатива QR-кодам – для интерактивных экскурсий по музею или по городу;

— бесконтактной регистрации на крупных мероприятиях;

— навигации внутри крупных помещений;

— бесконтактной оплаты счета (PayPal в США);

— контроля обслуживания в ресторане;

— создания карт посещаемости павильонов в торговом центре;

— контроля посещаемости в учебных заведениях;

— отслеживания пассажиропотоков в городе;

— поиска забытых вещей или багажа в аэропорту;

Радиомаячок излучает сигнал, устройство (компьютер, мобильное устройство) с соответствующим приложением и включенным Bluetooth получает его, определяет свое расстояние до радиомаячка (как правило, по силе сигнала) и совершает заданное приложением действие — например, выводит на экран push-уведомление о скидке в магазине.

Технология **push** («проталкивание») — способ распространения информации (контента – заголовка и текста), когда данные поступают от поставщика к пользователю по какой-либо сети на основе установленных параметров в виде уведомления. Пользователь решает принять или отвергнуть данные [36].

Через push-технологию можно получать не только уведомления, но и, например, синхронизировать данные.

Система радиомаяков обычно состоит из трёх компонентов: маячков, мобильного приложения, веб-сервиса.

Радиомаячок настраивается через приложение или веб-сервис разработчиком системы. Разработчик задает интервал вещания маячка, содержимое push-уведомления, иногда радиус оповещения. Дальше весь функционал зависит от приложения пользователя или от веб-сервиса, на котором разработчик может поместить карту, подсчитывать какую-либо статистику и размещать любой другой контент.

Обычно радиомаячок транслирует уведомление, содержащее ссылку на сайт, где размещен основной контент, который невозможно передать через медленное соединение маячка.

Отличительной особенностью технологии является низкое энергопотребление (в 1000 раз меньше, чем у Wi-Fi), поэтому вещательные устройства могут быть небольшими и автономными. Срок службы батареи зависит от режима вещания и может достигать трех-пяти лет. Средняя точность определения местоположения этой технологии порядка 1-2 м при использовании специализированных алгоритмов и дополнительного оборудования. Часто технологию маячков используют совместно с другими сетевыми технологиями для расширения зоны охвата сети (Wi-Fi).

Технология радиомаячков относится к популярной концепции **интернета вещей** (Internet of Things, IoT) - сеть сетей, состоящих из уникально идентифицируемых объектов (вещей), способных взаимодействовать друг с другом без вмешательства человека, через IP-подключение. Ключевым в этом определении является автономность устройств и их способность передавать данные самостоятельно, без участия человека (поэтому смартфоны и планшеты не включены в эту концепцию) [37].

Радиомаячки разных производителей отличаются поддерживаемыми стандартами, которые определяют размер, формат и содержимое сообщения. Наиболее распространены три стандарта: iBeacon от Apple, Altbeacon от Radius Networks, Eddystone от Google.

1.8.1. Стандарт iBeacon

Стандарт **iBeacon** определяет передачу только одного типа сообщения, которое состоит из следующих частей (рис.1.9) [38]:

— **UUID** — 16-байтный уникальный (в пределах производителя) идентификатор маячка.

— **Major** — 2-байтный беззнаковый номер (максимум 65536), идентифицирующий подмножество маячков в большой группе маячков.

— **Minor** — 2-байтный беззнаковый номер, идентифицирующий конкретный маячок в группе.

— **TX Power** — значение, основанное на уровне сигнала в 1 м от маячка. 8-битное знаковое целое — значение показателя уровня принимаемого сигнала (RSSI — Received Signal Strength Indicator), которое используется для определения близости маячка к приёмнику (мобильному устройству).

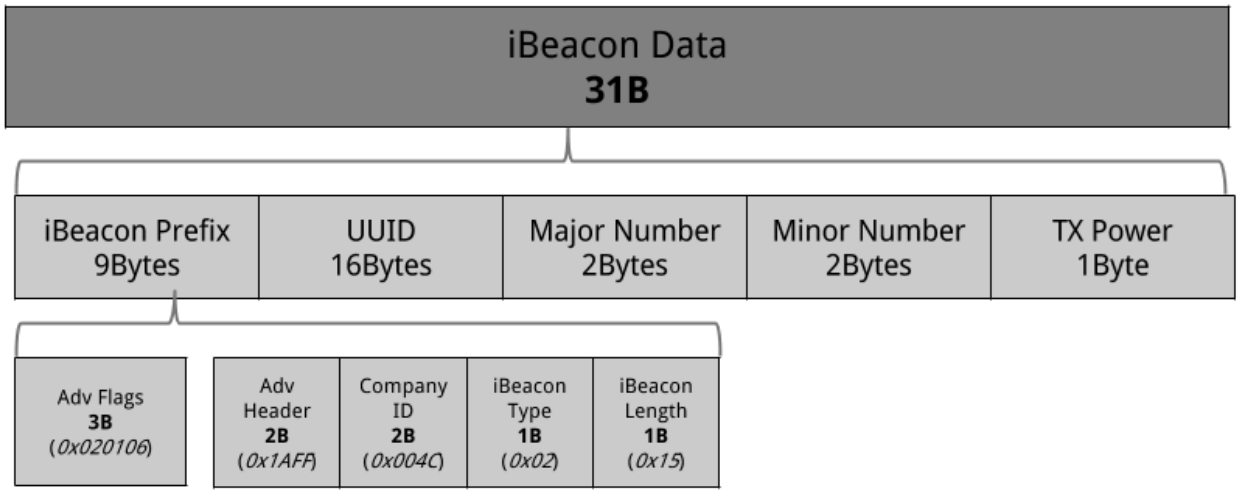


Рис.1.9. Структура сообщения стандарта iBeacon [38].

iBeacon Prefix содержит данные в шестнадцатеричной форме и подразделяется на:

— **Adv Flags** 3 байта (0x020106) определяет тип сообщения как обнаружимое и низкоскоростное (BLE General Discoverable и BR/EDR high-speed incompatible). Т.е. говорит об его широковещательной природе.

— **Adv Header** 2 байта (0x1AFF) обозначает, что сообщение будет размером 26 байт и в нем будет содержаться информация о производителе.

— **Company ID** 2 байта (0x004C) является особенностью стандарта сообщения от Apple и передает уникальный номер этой компании.

— **iBeacon Type** 1 байт (0x02) – вторичный идентификатор, который обозначает, что это маячок близости (proximity beacon), который используется во всех устройствах этого стандарта.

— **iBeacon Length** 1 байт (0x15) определяет оставшуюся длину сообщения в 21 байт. Таким образом, пользователю доступно всего 21 байт для редактирования.

Приложение на мобильном устройстве считывает **UUID**, **major number** и **minor number** и ищет совпадение в своей базе данных, где записаны данные об этом маячке. Сам маячок не может содержать такой объем информации и требует внешнего сетевого хранилища. Значение **TX power** должно быть предварительно настроено вместе с другим маячком для получения приемлемой точности определения расстояния от пользователя до маячка.

Недостатками стандарта iBeacon является его проприетарность, отсутствие встроенной поддержки платформой Android, ограничение одним типом сообщения, малый объем передаваемых данных.

1.8.2. Стандарт Altbeacon

Стандарт AltBeacon задумывался как открытый интероперабельный и обратно совместимый со стандартом iBeacon. Стандарт позволяет передать немного больше полезной информации (рис.1.10).

Рис.1.10. Структура сообщения стандарта AltBeacon [38].

Размер сообщения AltBeacon 28 байт, 26 байт доступны для изменения пользователем.

— **MFG ID** — Идентификатор производителя устройства, 2 байта.

— **Beacon Code** — Код сообщения (Advertisment packet), 2 байта.

— **Beacon ID** — Уникальный идентификатор радиомаячка, 20 байт. Может быть представлен как у iBeacon для совместимости с ним.

— **MFG RSVD** — зарезервированное поле 1 байт для служебной информации производителя.

Возможности стандарта:

— передача уникального номера маячка в пределах приложения, а не производителя;
— запись различных кодов маячка;
— передача служебной информации производителя.

Ввиду открытости стандарта, у него есть потенциал заменить закрытый стандарт iBeacon. Однако небольшая длина сообщения и необходимость установки специального приложения не позволит реализовать множество возможных решений.

1.8.3. Стандарт Eddystone

Стандарт **Eddystone** предложен Google в 2015 г., является открытым и использует опыт других стандартов, являясь гибким и ему не присущи недостатки стандартов iBeacon и AltBeacon. Находится в активной разработке и улучшении, сейчас отличается от iBeacon возможностью передавать гиперссылки, что делает его похожим на QR-код, только через Bluetooth. Пользователю доступно 28 байт.

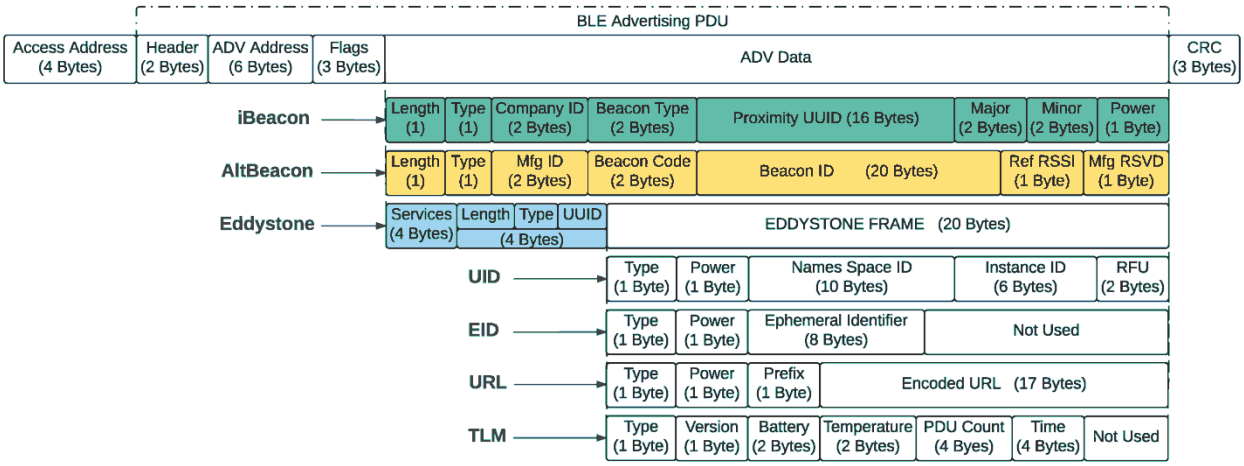


Рис. 1.11. Структура протоколов iBeacon, AltBeacon и Eddystone [38].

Поддерживает три типа сообщений (рис.1.11):

— **Eddystone-UID** — уникальный идентификатор устройства, 16 байт, состоящий из полей **namespaceId** (10 байт) **instanceId** (6 байт).

— **Eddystone-URL** — содержит URL в сжатом с помощью сервиса Google URL Shortener формате, 18 байт.

— **Eddystone-TLM** —телеметрия маячка (напряжение батареи, температура устройства, количество отправленных пакетов с момента включения и время работы).

— **Eddystone-EID** – эфемерный идентификатор с шифрованием.

Очевидным достоинством стандарта является возможность передавать веб-ссылки. При этом отпадает необходимость иметь специализированное приложение на устройстве-приёмнике – достаточно обычного веб-браузера.

Недостатком можно назвать привязанность технологии Eddystone к сервисам Google для задания параметров и сообщения маячка.

В 2016 г. Google представила расширение своего формата **Eddystone-EID**, с введением шифруемого 8 битным AES алгоритмом эфемерного идентификатора (**Ephemeral ID**), шифрованной телеметрией Eddystone-TLM и новый стандартный интерфейс для конфигурирования маячков — **Eddystone GATT service**.

По данным ABI Research, сейчас в мире работает 4 млн маячков, а к 2020 году их будет 400 млн.

Размер сообщения, помимо стандарта производителя, регулируется стандартом BLE, где полезный объем сообщения не может быть больше 37 байт без заголовка. Поэтому не стоит ожидать значительного объема передачи данных в одном сообщении от технологии маяков.

Достоинства технологии маячков:

— легкая беспроводная установка на стенах;

— низкая стоимость маячка 10-30$;

— длительный срок работы от батарейки (2-3 года при частом включении, до 10 лет с редким включением);

— относительно большой радиус покрытия вещания маячка;

— связь Bluetooth Low Energy потребляет очень мало энергии мобильного устройства пользователя при постоянной работе.

Недостатки:

— необходимость держать включенным приём Bluetooth на устройстве пользователя;

— требуется источник питания;

— для организации большой сети маячков нужно связывающее сетевое оборудование (Wi-Fi, WiMax), которое требует значительной энергии для работы (по сравнению с маячком).

1.9. Возможные области применения RFID-технологий в геоинформатике

Предлагается использовать RFID-метку в оперативном обновлении данных ГИС следующими способами: [39].

1. В теле марки (репера) с возможностями:

— возможность записи на одноразовую метку (марку) всех её параметров (номер, год изготовления, дата определения координат, сами координаты и другие метаданные;

— возможность по силе радиосигнала или вектору обнаружить примерное местоположение геодезической марки (пункта, репера) и считать с неё данные без визуального контакта с ней на расстоянии до 6 м (для пассивной метки) и порядка 100 м для активной и полуактивной меток (соблюдая условия радиовидимости);

— возможность избежать повторных измерений при повторном использовании записанных координат с метки;

— возможность шифрования данных с координатами для прочтения меток только специализированным оборудованием – для соблюдения требуемой секретности;

— измерять расстояние до метки, а также её координаты (при необходимости) соответствующим радиооборудованием, с точностью до 10 см, а с развитием технологий – точнее, что соответствует максимальной точности определения плановых, а тем более высотных координат с помощью GPS и ГЛОНАСС.

2. С помощью технологий позиционирования в реальном времени RTLS возможно определять местные координаты меток (до 1 см) или пользователя внутри зданий и сооружений, - в местах недоступных для прямого наблюдения с помощью спутниковой навигации.
3. Для оперативного обновления или отображения метаданных на кадастровой карте. Радиометка как приложение к паспорту участка в ЕГКН. Владельцу выдается метка с данными участка (владелец, площадь, год выдачи, номер участка), которая может быть прикреплена с внешней стороны забора (как почтовый ящик) и которую можно прочитать при необходимости.
4. Оперативное обновление данных в ГИС в реальном времени с помощью сетей активных меток (Eddystone, ZigBee, Wi-Fi, WiMAX и др.) в различных сочетаниях либо в постобработке, путём ручного сбора данных с пассивных меток, либо меток, не имеющих доступа в интернет.

Для более точных выводов о применении RFID-технологии в ГИС необходимы практические исследования с созданием опытных образцов меток.

Применение различных RFID-технологий с ГИС-технологиями выведет часть геодезической отрасли на новый технологический уровень, что позволит быстро собирать различные виды данных, в том числе пространственные, а также облегчит процесс принятия решений.

2. РАЗРАБОТКА МЕТОДИКИ СБОРА ГЕОДАННЫХ С ПОМОЩЬЮ RFID

2.1. Требования к RFID-инфраструктуре

2.1.1. Требования к количеству доступной для записи памяти

Как было описано в статье [40], технические требования к памяти метки, служащей в качестве репера/марки (источника данных для ГИС) следующие.

Память должна быть доступна для многократной записи и чтения – это обеспечивает метка существующего типа RW (read/write).

Геодезический репер может хранить следующие данные:

- номер марки – уникальный, задается при изготовлении;
- год изготовления;
- координаты различных типов;
- код (название) фирмы-изготовителя геодезического пункта;
- дополнительную информацию.

Эти же данные в полном объеме содержатся в каталогах вместе с описанием физико-географических условий района работ, годом производства работ, оценкой точности произведенных работ.

Поскольку объем памяти метки ограничен (обычно несколько сотен бит), не имеет практического смысла хранить подробную информацию.

Необходимо воспользоваться алгоритмом, отсекающим всю повторяющуюся информацию, учитывая определенную известность координат размещения меток и контрольной суммой (хэш-функция), позволяющей расшифровать сокращенную информацию.

Подсчитаем минимальное количество памяти для хранения данных на метке с учетом хэш-функции.

1) Номер собственно метки уникален (для одного изготовителя) и подсчёт памяти для его хранения не нужен, т.к. он заносится при изготовлении и не может быть изменён. Обычно 128 бит (16 символов).
2) Год изготовления репера – можно уточнить записью **полной даты**, на которую актуальны записанные координаты в формате ДД.ММ.ГГ, что потребует минимум 8 символов (**64 бита** памяти).

3) **Координаты репера**. Обычно требуется три координаты, но в разных сетях по-разному, поэтому возьмем как пример, систему GPS как самую распространенную. В этой системе нам нужны только три координаты:
   a) **Широта** в формате M.MMMMMM с дробной частью минут переменной длины (в программах навигаторов обычно 6 знаков после запятой), получается 7 символов (**56 бит)**.
   b) **Долгота** в формате M.MMMMMM с дробной частью минут переменной длины (берем 6), получается 7 символов (**56 бит)**.
   c) **Высота** в метрах в формате ±NNN.NNNN получается 9 символов (**72 бит**). В оригинальном протоколе NMEA 0183 нет высоты, но различные фирмы-производители навигаторов и ПО добавляют свои строки в протокол, содержащие данные о высоте [41],[42].
   d) **Идентификатор системы координат** можно представить как цифру (например, WGS-84 соответствует 1), возьмем с запасом 2 символа (**16 бит)**.
4) **Идентификатор организации-установщика**, возьмем 2 символа (**16 бит**). Вообще этот параметр необязателен и зависит от глобальности репера – сведения об организации будут привязаны к номеру метки и храниться в базе данных организации.

Таким образом, минимальное количество памяти, требуемое для хранения координат и их метаданных, составляет **280 бит** без шифрования и служебных символов.

Вопрос о юридической стороне вопроса широкой доступности таких данных остается вне рассмотрения данной работы.

Современные метки используют технологии EEPROM (Electrically Erasable Programmable Read-Only Memory) – энергонезависимая память малой ёмкости с возможностью записи, чтения и удаления данных. Это название используется теперь независимо от технологии изготовления используемой памяти (EEPROM, NOR flash) [43]. Все типы меток могут использовать механизм антиколлизий. Существующие решения, рассмотренные в первой главе, в основном, удовлетворяют требованиям о количестве памяти на метке, что представлено в таблице 2.1. согласно источникам [44], [45], [46].

Память меток в существующих решениях подразделяется, в том числе, на EPC (UII) и USER. Первая предназначена для хранения уникального идентификатора метки и имеет объемы 96, 128, реже 496 бит [47]. Пользовательская (USER) память предназначена для хранения произвольной информации, обычно в текстовом виде – метаданных, шифрованных данных, и имеет объём до нескольких килобайт и более.

Таблица 2.1. Максимальное количество памяти на потенциальной метке разных технологий и стандартов на 2017 г.

Технология	Максимальное количество памяти (USER)
RFID LF (125-134 кГц)	2 Кбит
RFID HF (13,56 МГц)	2 Кбит
RFID UHF (860-960 МГц)	3 Кбита
RFID UHF для RTLS (2,4 ГГц)	256 Мбит
NF UHF (~900 МГц)	32 бита
NFC	56 Кбит
Bluetooth маячки	224 бит (28 байт) из них 152 бита (19 байт) URL
ZigBee	480-1024 бита (60-128 кбайт)
Wi-Fi	Нет свободной пользовательской памяти, зависит от подключенного оборудования, потенциально безгранична.
WRAN	
WiMAX	

2.1.2. Требования к безопасности данных

Требования к безопасности данных рассмотрены в статье автора [48]. Если не рассматривать законодательную составляющую безопасности данных ввиду её изменчивости и неуниверсальности, то общие требования включают в себя:

— требования к защите данных от нелегального копирования с метки или во время передачи данных;
— требования к защите от нелегальной записи.

Для защиты от нелегального копирования данных с метки применяется шифрование данных при их передаче меткой. Из-за серьезных ограничений на вычислительную мощность пассивных RFID-меток невозможно использовать существующие мощные криптографические алгоритмы. Специальный раздел криптографии - LW-криптография или малоресурсная (легковесная) криптография занимается вопросами шифрования маломощных меток [49].

В настоящее время не существует оптимального решения, подходящего для использования в различных радиочастотных метках, бесконтактных смарт-картах и т.п. Таким образом, в каждом случае должен быть баланс между сложностью, размером и вычислительной мощностью RFID-системы и обеспечением безопасности данных.

Например, случай, когда координаты, записанные на репер, должны быть недоступны для прямого чтения неавторизованным лицом. И не должны быть изменены им без соответствующего разрешения. Самый простой метод защиты – установка пароля на чтение и запись таких данных. Но при этом методе есть нюансы: какой необходимой длины и сложности должен быть пароль, как он будет храниться и передаваться, как будут храниться и передаваться данные – будут ли они все шифроваться или будет шифроваться только пароль. Все эти вопросы решает легковесная криптография. Для каждого типа устройств есть свои методы защиты информации, однако они очень похожи и различаются только требованиями к балансу между безопасностью данных, производительностью микропроцессора и ценой реализации такой системы.

Учитывая эти категории требований, рассмотрим их в применении к различным технологиям, которые потенциально применимы в ГИС.

Безопасность данных в RFID

Типичными ограничениями, встречающимися в легковесной криптографии, являются:

- для аппаратной составляющей – размер чипа, потребляемая мощность, время выполнения программы;
- для программной составляющей – объём кода программы, количество оперативной памяти, время выполнения программы.
- ширина полосы рабочих частот канала связи или скорость передачи данных.

Многие требования, предъявляемые к алгоритмам, предназначенным к использованию в ограниченных условиях, представлены в международном стандарте ISO/ IEC FDIS 29192 – Information technology – Security techniques – Lightweight cryptography.

Технологии RFID отличаются относительно небольшим расстоянием взаимодействия считывателя и метки (до 10 м, кроме UHF 2,4 ГГц до 100 м), что влияет на требования к защите передаваемой информации. Т.е. вариант атаки «пользователь посередине» в данной технологии является маловероятным, поэтому не приоритетным. В данной работе не будут рассматриваться все возможные варианты вмешательства в безопасность данных.

Важнейшей характеристикой алгоритма шифрования является криптостойкость, т.е. как долго и с какими ресурсами алгоритм будет устойчив к расшифровке. Стойкость в легковесной криптографии ничем не отличается от таковой в обычной криптографии.

Криптографических алгоритмов существует очень много и их можно разделить на три больших группы:

- бесключевые, в которых не используются ключи для шифрования;

- с секретным ключом, когда стороны должны знать секретный ключ для расшифровки данных;

- с открытым ключом, когда стороны имеют два ключа (секретный и открытый) для расшифровки данных (рис.2.1).

Рис.2.1. Виды криптографических алгоритмов

Стандарты RFID технологий с точки зрения безопасности данных можно рассматривать как одно целое, потому что во всех видах протоколов RFID (LF, HF, UHF, NF UHF) и не только, как показывает анализ решений на рынке данных устройств, применяется один стандарт шифрования данных – AES 128 бит.

AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Этот алгоритм сейчас широко распространён, возникнув как стандарт в 2002 году [50]. На рисунке 2.2. представлена схема его работы.

Рис. 2.2. Блок-схема работы алгоритма AES

Открытый текст данных шифруется поэтапно. Генерируется секретный ключ в виде матрицы 4xNk, где Nk = 4, 6, 8 столбцов. Далее вычисляются все уникальные ключи итераций (128 бит) через секретный ключ. В начале шифрования входной блок данных (input) размером 128 бит копируется в массив 4x4 байт (state) по формуле:

$$state[r, c] = input [r + 4c], \quad 0 \leq r < 4 \text{ и } 0 \leq c < 4$$

После этого к массиву входных данных применяется процедура модульного сложения (XOR) с уникальным ключом итерации. Эта процедура называется итерация (раунд) и повторяется Nr число раз (10, 12, 14), в зависимости от длины секретного ключа (128, 192, 256 бит).

Далее происходит подстановка байтов через таблицу подстановок и циклический сдвиг массива байт на различные величины. В итоге, после завершения последней итерации, массив данных будет зашифрован. Расшифровка производится в обратном порядке.

Симметричное шифрование — способ шифрования, в котором для шифрования и дешифровки применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами, участвующими в шифрованном обмене данными. Алгоритм шифрования выбирается сторонами до начала обмена данными (рис.2.3).

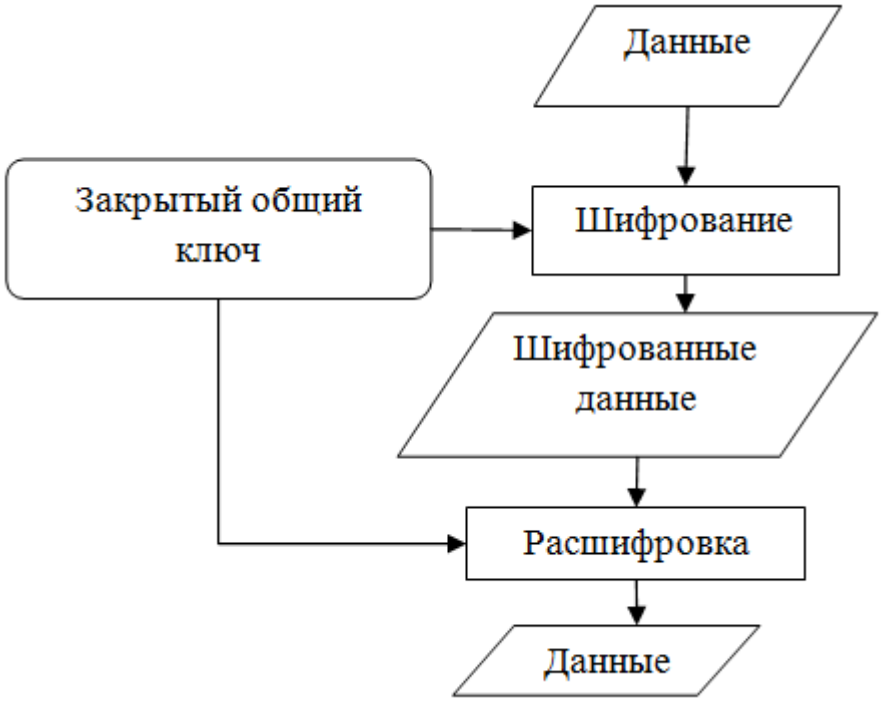


Рис. 2.3. Симметричное шифрование

В настоящее время симметричное шифрование бывает двух видов:

— блочное шифрование. Информация обрабатывается блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки (раунды). Результатом повторения раундов является нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных (рис.2.4).

— поточное шифрование, в котором шифрование проводится над каждым битом или байтом исходного (открытого) текста с использованием наложения на него последовательности, состоящей из случайных чисел (рис. 2.5). Поточный шифр может быть легко создан на основе блочного [51].

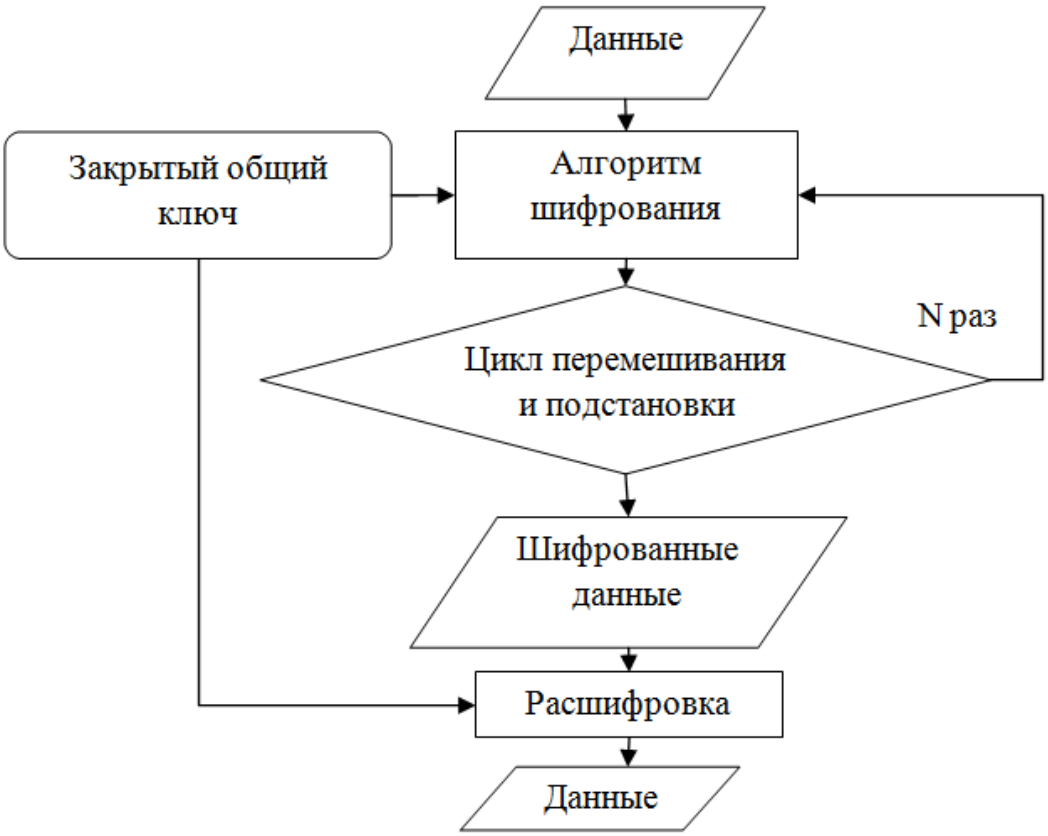


Рис. 2.4. Блочное шифрование

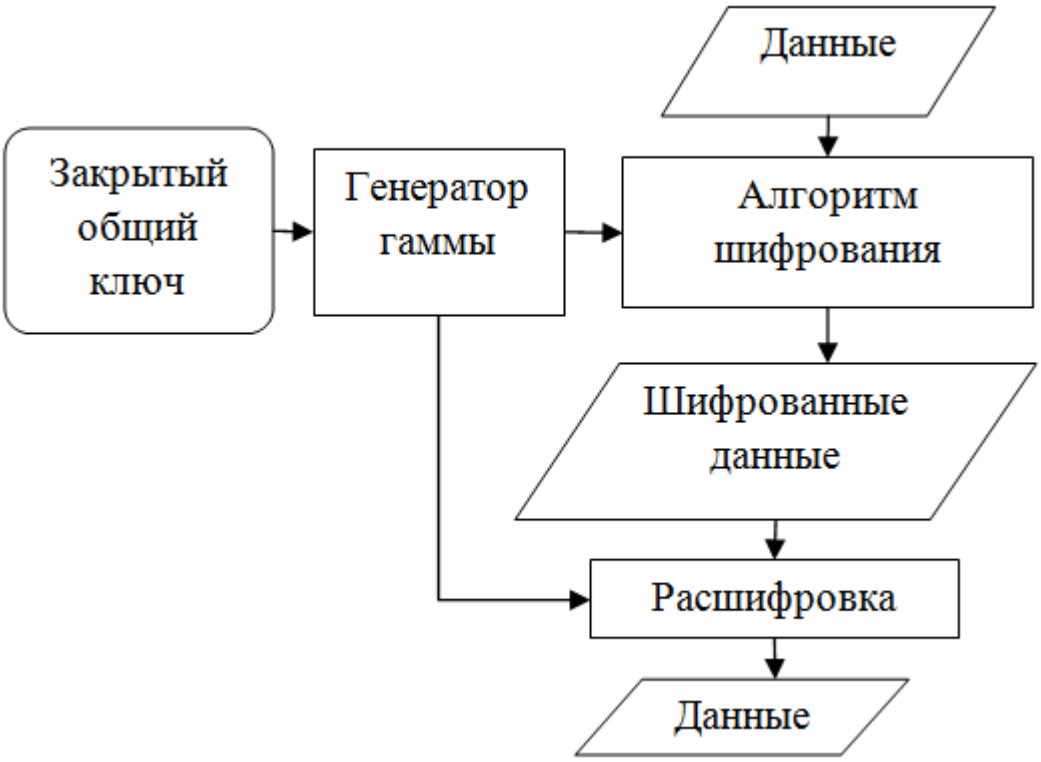


Рис. 2.5. Поточное шифрование

Симметричные алгоритмы с закрытым ключом используются для шифрования, аутентификации, проверки целостности данных в сообщении.

Асимметричные алгоритмы с открытым ключом используются для обеспечения неотказуемости, управления ключами и очень требовательны к объему вычислений и энергопотреблению по сравнению с симметричными (в 100-1000 раз медленнее, в 30 раз больше энергопотребление).

По анализу, проведённому в [52] получается, что в программной реализации для RFID подходят блочные шифры Piccolo, TWINE, XTEA и AES. Там же сравнение реализаций блочных и поточных шифров показало, что потоковые шифры не дают существенного преимущества в условиях ограниченных аппаратных или программных ресурсов.

Среди методов кодирования данных в 2012 г. хорошие конкурсные показатели имели хэш-функции, базирующиеся на легковесных блочных шифрах и семейства QUARK по сравнению с AES.

Асимметричное шифрование предполагает наличие двух ключей — открытого для шифрования и закрытого – для расшифровки. Отправитель перед отправкой создаёт у себя открытый

ключ и шифрует им сообщение, после чего данное сообщение можно расшифровать только закрытым ключом, который создается и хранится в секрете у принимающей стороны (рис. 2.6).

Ассиметричное шифрование для легковесной криптографии почти не применяется, в отличие от блочных симметричных шифров. В стандарт ISO/IEC 29192-4 (Mechanisms using asymmetric techniques) включены всего три алгоритма LWS: cryptoGPS, ALIKE (Authenticated Lightweight Key Exchange), IBS - механизм цифровой подписи.

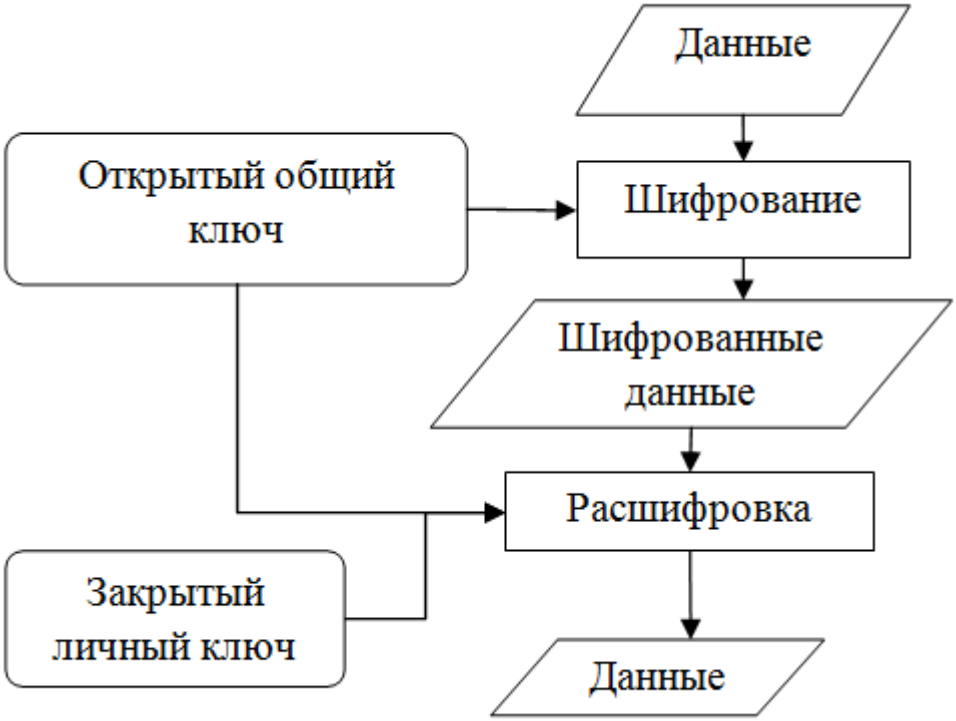


Рис. 2.6. Асимметричное шифрование

В настоящее время для RFID больше всего из асимметричных алгоритмов подходят работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography) и гиперэллиптическими кривыми (HECC – HyperElliptic Curves Cryptography). По сравнению с симметричным шифрованием, асимметричное с безопасной длиной ключа требует значительно больших аппаратных ресурсов. Такие выводы показывают причины широкого использования алгоритмов AES как симметричного блочного метода шифрования легковесной криптографии.

Также существует американский патент на шифрованную парольную защиту RFID-метки от 2007 г. Его суть в том, что постоянный идентификатор метки можно считывать с метки RFID, который может быть объединен с начальным случайным значением для создания комбинированного значения. Комбинированное значение может быть зашифровано и сохранено на

чипе RFID. Позже метка RFID может быть проверена на подлинность с использованием шифрованного значения [53].

Размеры микросхем принято измерять в условных логических элементах (Gate Equivalent, GE). За один условный логический элемент принимается площадь, занимаемая элементом NAND с двумя входами. При этом «ультралегкой» (ultra-lightweight) называется реализация, требующая менее 1000 GE, «низкостоимостной» (low-cost) – требующая не более 2000 GE и «легковесной» (lightweight) – не более 3000 GE [49].

В общем, предпочтительнее алгоритмы, требующие меньшего размера памяти вычислительного устройства (или меньшего числа логических элементов для их реализации). Например, блоки шифрования размером 4x4 бита предпочтительнее блоков 8x8, потому что последние требуют для своей реализации в среднем 1000 GE (минимум 120 GE). А 4x-битные могут быть реализованы со сложностью 21 – 39 GE, что возможно на микросхеме в десятки раз меньше.

В текущее время прослеживается тенденция использовать в легковесном алгоритме шифрования широко распространенные и хорошо исследованные элементарные преобразования (арифметические и логические операции), которые должны быть универсальны. Например, шифры, состоящие из трех видов преобразований: сложения по mod 2^n (Addition), побитового сложения (XOR) и циклического сдвига (Rotation). Самый распространенный пример такой реализации – алгоритмы AES.

Безопасность данных в NFC

Как показывает тот же анализ рынка устройств, в технологиях NFC применяются те же алгоритмы шифрования AES, т.к. он является современным эталоном криптографии. Однако сама технология NFC не обладает защитой данных, а всё шифрование является дополнением к ней.

Однако помимо алгоритмов шифрования, в данной технологии есть дополнительная естественная защита – расстояние считывания не более 10 см, что исключает вариант атаки «пользователь посередине». Примеры такой реализации известны всем – банковские карты, проездные в метро и пригородных поездах, электронные замки. Подобные реализации практически доказали свою надежность как безопасного носителя информации, и её передачи.

При использовании данной технологии в ГИС в качестве носителя координат (репера) вопрос безопасности данных будет иметь такой же вес, как в остальных рассматриваемых технологиях, а основное внимание будет уделяться практичности использования считывания данных на столь малом расстоянии.

Безопасность данных в маячках (beacons)

Маячки (beacons) работают по технологии связи Bluetooth, которая сама по себе стандартизирована с учетом безопасной передачи данных на расстояние около 1м и до 50 м в зависимости от версии стандарта.

Поскольку нас интересуют наиболее функциональные решения данной технологии, будет рассматриваться только стандарт от Google **Eddystone** как единственный открытый и легко исследуемый.

Последняя версия данного стандарта учитывает защиту данных и называется **Eddystone-EID** (Ephemeral Identifier, эфемерный идентификатор) [54].

Маячок Eddystone-EID меняет свой 128-битный шифрованный алгоритмом AES идентификатор псевдослучайным образом со средним периодом от 1 сек - 9 ч., задаваемым пользователем при настройке. Для генерации идентификатора используется эфемерный ключ (EIK) и таймер маячка. Ключ генерируется во время подготовки и настройки маячка и затем передаётся в облачную службу разрешения с использованием протокола согласования ключей на эллиптических кривых (Elliptic curve Diffie–Hellman). Этот протокол является достаточно надежным и позволяет получить общий секретный ключ, используя незащищённый от прослушивания канал связи, например во время подготовки и настройки маячка. Потом этот ключ может использоваться как таковой, либо для выработки ещё одного ключа на самом устройстве. Таким образом, доступ к ключу есть только у маячка и у облачной службы, в которой маячок зарегистрирован.

Служба Google Proximity Beacon API позволяет произвести регистрацию маячка двумя способами:

— обменом открытыми ключами с маячком, в полностью безопасной форме;
— передачей общего эфемерного ключа напрямую, что является менее безопасным, но позволяет зарегистрировать маячок в нескольких службах одновременно.

Некоторые зарубежные публикации предлагают свои протоколы шифрования для маячков, например, семейство протоколов **Lightweight Protocol for Sensors (LP4S),** рассмотренное в статье [38]. Их преимущества:

— могут быть использованы в маячках;
— могут использоваться как для отправки данных, собранных с датчиков маячка, так и для приема команд для исполнительных механизмов;

— гарантируют необходимый сервис качества передачи данных (QoS);
— не требовательны к энергопотреблению;
— могут находить и определять подключаемые устройства, используя технологии plug-and-play.

В этой же статье приводится формула расчета срока работы, шифрованного алгоритмом LP4S маячка, зависящая от батареи и интервала вещания и результаты эксперимента в таблице 6 [38]:

Срок_работы_батареи (мес) = ёмкость (мА*ч) / (0,001* средняя_потребляемая_сила_тока (μA) * 24 * 30.

Согласно этой таблице, наибольший срок службы батареи (5000 мА*ч) составляет 55 месяцев с интервалом вещания в 5 секунд.

Исследовав формат Eddystone на предмет применения к нему требований из [40], приходим к выводу о возможности применении данной технологии в ГИС для хранения всех данных на маячке. Самое безопасное применение, когда используется гиперссылка на защищенный облачный сервис, в котором уже применены все современные технологии защиты информации, например, базу данных координат пунктов.

Безопасность данных в сетях ZigBee

Устройства, работающие по протоколу беспроводной связи Zigbee (стандарт IEEE 802.15.4.) на частоте 900-928 МГц и 2.4 ГГц соединены в ячеистую сеть. Стандарт изначально был разработан для малоёмких устройств, например, датчиков на заводе, поэтому в среднем сети на основе Zigbee потребляют 1/4 мощности сетей Wi-Fi.

Протокол ZigBee широко использует методы симметричного шифрования AES для защиты данных на носителе и методы асимметричного шифрования на эллиптических кривых при передаче данных до 1 км [55].

При сроке работы от нескольких недель до месяцев, и при таких расстояниях может быть осуществлена атака «пользователь посередине», но применяемое шифрование надежно защищает сеть, т.к. для взлома нужно постоянное присутствие перехватывающего сообщения устройства в течение очень долгого времени, превышающего время передачи данных с любого из устройств. Поэтому при передаче данных с датчика ZigBee в ГИС, эти данные могут быть надежно защищены.

Таким образом, проанализировав возможные решения безопасности данных в различных технологиях (RFID, NFC, Eddystone, Zigbee), можно придти к выводам о том, что все они используют одни и те же алгоритмы шифрования данных – семейство симметричных методов AES и ассиметричное шифрование на эллиптических кривых, что вполне достаточно для защиты данных при любом возможном применении рассмотренных технологий в ГИС.

Потенциально применимы алгоритмы шифрования (для программной реализации), но не встречаются на рынке готовых устройств: симметричные блочные шифры ГОСТ 28147-89, KATAN, KTANTAN, Piccolo, PRINT, SIMON, SPECK, TWINE, XTEA; хеширование семейства QUARK, WH-16; асимметричные алгоритмы cryptoGPS, ALIKE, IBS (цифровая подпись); семейство LP4S.

Рассмотренные алгоритмы и методы шифрования применяются в том или ином виде во всех технологиях передачи и хранения данных, таких как Wi-Fi, WRAN, WiMAX, которые потенциально возможно применить в ГИС.

2.1.3. Требования к сроку службы и расстоянию считывания метки

Срок службы и расстояние считывания метки зависит от её типа: активная или пассивная, т.е. имеющей в своём составе источник питания или не имеющей. На рынке наиболее распространены пассивные метки, которые служат до 50 лет, но их главный недостаток – малое расстояние считывания (до 10 м в идеальных условиях). Такие метки подойдут для реперов в городе, где они сравнительно хорошо доступны. Кроме того, расстояние считывания зависит не только от метки, но и от считывателя – его мощности и размера антенны, а также от условий среды считывания.

Для реперов на пересеченной местности, лесах, где их гораздо тяжелее найти, пассивная метка не подходит. Активная метка всегда большего размера и требует источника питания, поэтому и обнаруживается на гораздо большем расстоянии (до 100 м). Срок службы такой метки зависит от типа батареи, интервала оповещения, условий работы и составляет около 2-10 лет.

Теоретически, чем больше антенна у метки, тем больше расстояние считывания с неё, поэтому если выполнить репер в виде металлической конструкции, присоединенной к метке, то дальность обнаружения сильно возрастёт, но это предположение требует практической проверки и технического анализа.

Крепление метки обычно зависит от места предполагаемого её применения и от среды, к которой она крепится. На рынке встречаются такие типы крепления метки (зависят от вида её исполнения): самоклеящиеся, на клей, резьбовое, магнитное, под сварку, под хомут/проволоку,

встраиваемые/для имплантации, забиваемые. Т.е. вид корпуса может быть любым в зависимости от цели использования. Все радиометки плохо работают в водной среде вплоть до полной невидимости так же, как в креплении на металлических поверхностях – нужно соблюдать соответствие типа метки и условий её прикрепления.

В таблице 2.2. Представлена сравнительная таблица с максимальными значениями параметров меток и устройств различных технологий. Дальность считывания зависит от мощности приёмника и передатчика, размера и параметров их антенн, среды распространения сигнала, среды прикрепления метки. Срок службы всех модулей EEPROM памяти одинаков – около 50 лет (теоретически), в таблице также указан срок работы с учётом элемента питания, память при этом останется работоспособной и не сбросится.

Таблица 2.2. Параметры дальности и срока службы существующих радиометок в разных технологиях хранения и передачи данных.

Технология	**Макс. отн. дальность считывания**	**Срок службы**
RFID LF (125-134 кГц)	0,7 м при антенне 0,7 м	10-50 лет пассивные 1-5 лет активные
RFID HF (13,56 МГц)	1 м при антенне 0,7 м (до 2 м)	
RFID UHF (860-960 МГц)	10 м (пассивная) -100 м (активная)	
RFID UHF для RTLS (2,4 ГГц)	100 м	
NF UHF (~900 МГц)	0,3 м	
NFC	0,1 м	50 лет
Bluetooth маячки с Eddystone-EID	1-100 м или 50 м (BLE)	2-10 лет, память до 50 лет
ZigBee	80 м – 1 км	неск. недель – неск. месяцев*
Wi-Fi	100 м – 2 км	Требуют постоянного источника питания
WRAN	10 – 100 км	
WiMAX	5 – 80 км	

* - для конечных устройств. Координатор и маршрутизатор должны иметь постоянное питание для поддержания сети.

2.1.4. Требования к считывателю данных

Поскольку работа с реперами предполагает выезд на место расположения устройства с данными, то первое требование к считывателю данных – возможность работы с ним в полевых условиях, т.е. **мобильность**. Такому требованию удовлетворяют только настольные и мобильные считыватели. Оба этих типа считывателей можно взять с собой, и отличаются они друг от друга только степенью мобильности – если можно взять с собой ноутбук, то и настольный считыватель тоже.

Второе требование к считывателю – **поддержка криптографии**. Этой способностью обладает очень мало считывателей на рынке, и они весьма дороги.

Третье, главное, требование – **дальность считывания**. Во множестве применений она должна быть максимальной. Дальность считывания метки напрямую зависит, в основном, от размера антенн и мощности метки и считывателя, условий окружающей среды.

Четвертое требование – **система оценки близости считывателя к метке**. Оно может выполняться различными способами в зависимости от условий применения (пересеченная местность, лес, под землёй или в помещениях).

Пятое требование – **наличие встроенного в считыватель или связанного с ним спутникового навигационного приёмника геодезической точности**. Требуется в случаях, когда нужно записать координаты на метку, определяя их на месте её крепления. Не обязательно для выполнения, если в метку интегрирован такой приёмник.

2.2. Методика сбора данных для ГИС

С учетом предыдущих требований к инфраструктуре, предлагается следующая методика сбора геоданных для оперативного обновления ГИС, описанная в статье [40] на рисунке 2.1, но более детализированная. Похожая схема предлагалась в статье [56], но в ней описан частный случай, где в качестве источника координат служит GPS-приёмник без дополнительной надстройки для хранения данных и без конкретизации требований к системе.

Под **радиометкой (радиомаячок, маячок)** подразумевается радиотехническое устройство, обладающее памятью и возможностью считывания и записи на нём данных, в том числе и геоданных и передачи этих данных по радиоканалам вне зависимости от своего расположения и назначения. В настоящее время существует ряд технологий передачи данных по радиоканалам: RFID, NFC, Bluetooth LE маячки, ZigBee, Wi-Fi, WRAN, WiMAX и др. Имеется достаточно большое число методик и способов по использованию радиометок при сборе различного рода данных [1-6, 57-59]. Их анализ для решения отдельных геодезических задач приведен в работах [39,40]. На основе этого анализа предлагается обобщенная методика по сбору геопространственных данных на местности с применением радиометок, включающая следующие технологические этапы (рисунок 2.1):

1) **Запись геоданных**. В случае геодезического репера (марки), координаты которого известны и требуется привязка метки этому реперу. Координаты репера и его метаданные заранее непосредственно записываются на радиометку или после их определения в поле и установки радиометки на репер. Или координаты и метаданные хранятся в базе данных ГИС (или облачного сервиса), куда вносится уникальный номер радиометки, соответствующей заданным координатам (реперу). При необходимости, метка шифруется паролем, делается доступной только для чтения.

2) **Крепление радиометки**. К реперу или в заданное место крепится радиометка любым предусмотренным способом или устанавливается готовый репер с радиометкой с выполненным этапом 1.

3) **Чтение геоданных с радиометки**. При помещении считывателя в поле доступности радиометки (дальность считывания), номер метки и все данные с неё (вариант: координаты, метаданные, показания датчиков) передаются по радиоканалу на считыватель. Эта операция может требовать передачи пароля, установленного на метке. Передача закрытых данных должна осуществляться при зашифрованном соединении, а данные на метке должны быть защищены от несанкционированного чтения и изменения.

4) **Передача данных в ГИС**. Данные со считывателя (либо считыватель смартфон - и есть компьютер с ГИС) передаются по сети на компьютер любым удобным способом, и вносятся в базу данных ГИС или облачный сервис. В случае сети ZigBee или похожей, считывателем выступают промежуточные устройства – роутеры, координаторы, которые считывают данные с радиометок, находясь стационарно в определенных местах, и передают их через локальную или глобальную сеть в ГИС или геосервис.

В случае работы с радиометкой при её попадании в зону действия считывателя, номер метки определяется, локализуется её примерное местоположение по силе сигнала, считываются записанные на метку координаты и метаданные, что не требует специальных запросов в разные организации при наличии у пользователя соответствующего ключа к расшифровке данных.

Поиск объекта, идентифицированного радиометкой, значительно облегчается при использовании ГИС или ГИС-навигатора, в которые загружаются изображения идентифицируемого объекта вместе с картой участка местности, где расположен объект (компьютерный абрис). Это позволяет оператору рассматривать ЦММ под разными ракурсами.

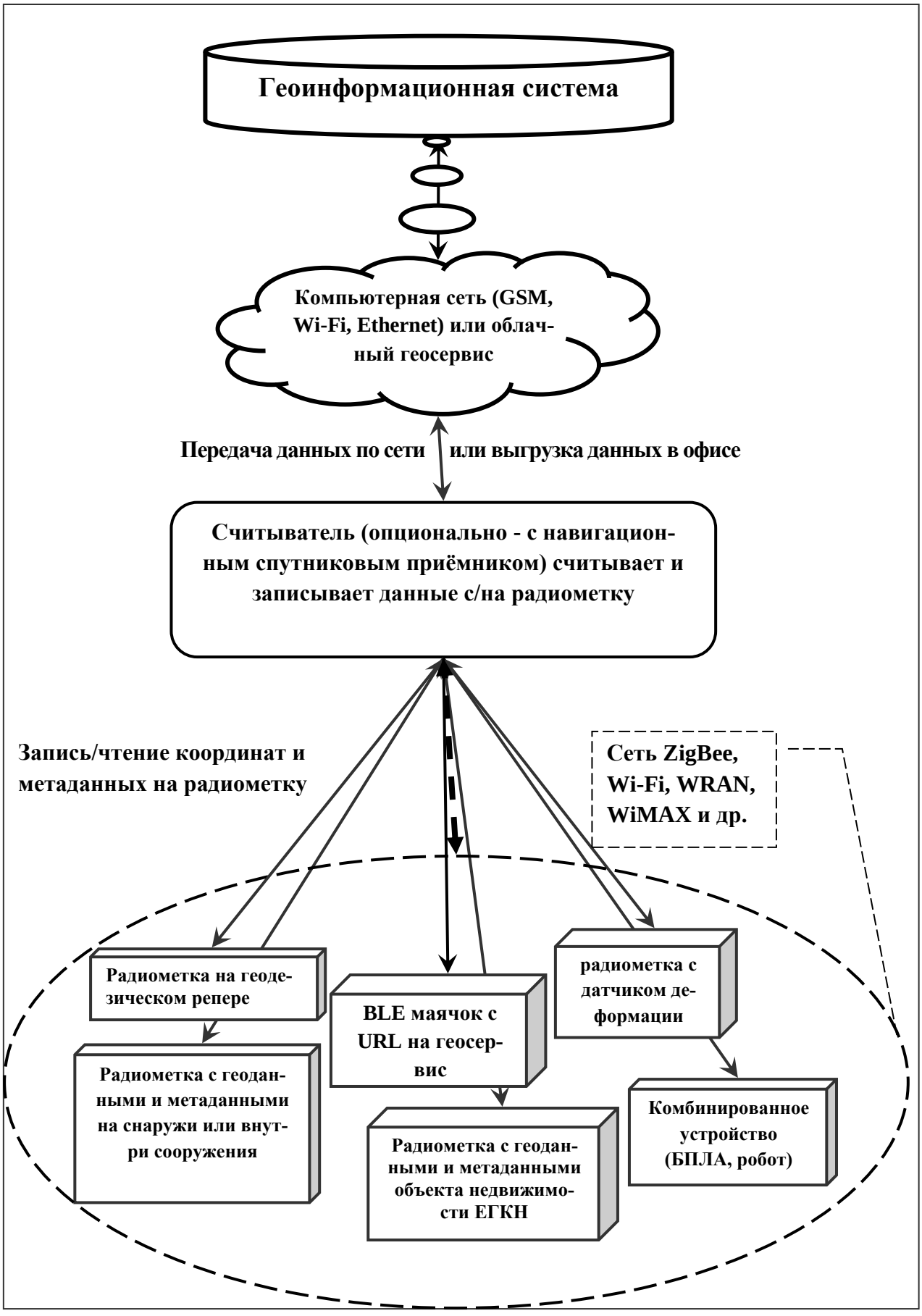


Рис. 2.1. Модель методики сбора данных «радиометка – ГИС».

2.3. Разработка количественных критериев для выбора радиометки

2.3.1. Обоснование и формулировка критериев радиометки

Исходя из требований к радиометке (см п.2.1), можно аналитически определить свойства и количественные критерии эффективности для выбора радиометки. Скорость передачи данных, количество участников сети, рабочая частота не являются критичными в общих требованиях к метке.

В качестве основных свойств эффективности радиометки примем следующие:

1. **объём памяти** для записи (бит, байт), – её должно быть достаточно для записи всех необходимых данных в зависимости от цели применения;
2. **возможность шифрования данных** (да/нет, 1/0)**.**
3. **дальность считывания**, (м) - расстояние, с которого можно уверенно получить данные с метки и записать их;
4. **срок работы** метки (недели, месяцы, годы) - приблизительное время работы метки (возможность считывать данные) до её замены или замены элемента питания. Срок работы связан с энергопотреблением устройства (Вт) и ёмкостью источника питания (А*ч);
5. **мобильность** - возможность автономной работы метки (да/нет), её размеры (мм);
6. **стоимость радиометки,** руб.

Перечисленные основные свойства являются сложными, составными из количественных и качественных характеристик самой метки и связанных устройств. Формулы некоторых критериев универсальны и основаны на [60].

Относительно простыми одноразмерными свойствами являются все свойства, кроме шифрования и мобильности. Поэтому они могут быть описаны с помощью безразмерного критерия:

$$\alpha_i = \frac{k_{\text{п}} - k_{\text{ф}}}{k_{\text{п}} + k_{\text{ф}}}, \quad (1)$$

где $k_{\text{п}}$ и $k_{\text{ф}}$ – пороговый и фактический параметры выбранного свойства соответственно, характеризующие рассматриваемое свойство таким образом, чтобы $k_{\text{п}} > k_{\text{ф}}$.

Критерий эффективности α_i может принимать любое значение от 0 до 1, и чем больше его значение, тем лучше соответствие заданному свойству.

Возможность шифрования выражается как 1 – данные и их передача шифруются, 0 – данные открыты. Обозначим этот критерий δ (0;1).

Свойство мобильности несёт в себе две размерности – одна логическая (возможность автономной работы – да/нет), вторая – линейная размерность или площадь, в мм, или мм^2. Поэтому для одной характеристики, - размера, можно применить критерий α_5 из (1), а второй критерий (автономность) обозначим γ (0 или 1). Таким образом, критерий оценки эффективности β будет складываться из двух критериев:

$$\beta = \alpha_5 \times \gamma, \tag{2}$$

где α_5 – критерий размера метки, γ - критерий автономности (0 или 1).

При невыполнении одного из них, эффективность нулевая. Например, при невозможности автономной работы, метка становится не мобильной, а стационарной, тогда её размеры уже не особо важны.

Исходя из введённых критериев эффективности отдельных свойств метки, можно определить общую эффективность метки в целом по интегральному критерию:

$$Q = \alpha_1^{P_1} \times {\delta_2}^{P_2} \times \alpha_3^{P_3} \times \alpha_4^{P_4} \times {\beta_5}^{P_5} \times \alpha_6^{P_6}, \tag{3}$$

где P_1-P_6 – весовые коэффициенты, характеризующие влияние соответствующих свойств в пределах (0,1). Они определяются как отношение веса каждого критерия к максимальному весу всех свойств метки.

После того, как определились коэффициенты эффективности выбора метки, рассмотрим составляющие свойств эффективности подробнее.

2.3.2. Дальность считывания

Дальность считывания метки имеет сложную зависимость от параметров:

- размера и конфигурации антенны метки;
- размера и конфигурации антенны считывателя;
- максимальной собственной мощности сигнала метки (зависит от питания, размера и конфигурации антенны метки);
- максимальной мощности сигнала считывателя;
- условий окружающей среды (препятствия, состав).

2.3.3. Мобильность

Складывается из технологии изготовления метки. В данном случае мобильность – когда возможна работа метки (передача данных) без стационарного (проводного) питания. Пассивные

метки питаются от считывателя при запросе данных, активные и полупассивные метки требуют внутренний заменяемый источник питания для работы. Например, если требуется батарейка, но есть возможность использовать преобразователь питания из внешней среды (солнечная батарея), то метка будет обладать большей мобильностью, чем просто с батареей. Чтобы не учитывать множество всех возможных технологий питания, ограничимся логическим условием наличия/отсутствия стационарного питания метки. Критерий косвенно влияет на срок работы метки.

2.3.4. Срок работы

Срок работы метки зависит от срока работы всей микросхемы в общем случае. Т.е. если всё устройство выйдет из строя из-за поломки конденсатора или резистора, то метка будет считаться нерабочей. Рассматривать параметры всех элементов, которые могут войти в состав радиометки, бессмысленно из-за их непредсказуемости и сложности, поэтому для простоты срок работы определяется меньшим из двух параметров:

- срок службы памяти до невозможности считать данные с неё;
- срок службы элемента питания до его замены:
  - энергопотребление метки
    - энергопотребление микросхемы;
    - температура окружающей среды;
    - режим работы (интервал вещания маяка).

Таким образом, слабым местом и основным параметром срока работы является срок службы элемента питания вне зависимости от его типа.

2.3.5. Количество памяти для пользователя

Памяти, доступной пользователю для записи, должно быть достаточно для хранения всех данных в зависимости от цели применения. Как было выявлено в п. 2.1.1., минимум необходимой для записи пользователем памяти составляет 280 бит. Как следует из таблицы 2.3, этому критерию удовлетворяет любая рассмотренная радиотехнология.

2.3.6. Стоимость

Стоимость метки является суммой параметров:

- себестоимость метки, включая интегрированное оборудование;
- затраты на установку;
- затраты на эксплуатацию;
- затраты на инфраструктуру (считыватель, ПО).

Эти параметры тоже составные и зависят от множества факторов, рассмотрение которых не относится к теме данной работы. Стоимость будет считаться в условных единицах от 1 до 5.

2.3.7. Возможность шифрования

Возможность шифрования данных задана как логический критерий (1 или 0), потому что на основе рассмотренных ранее средств защиты данных, был сделан вывод о достаточной защищенности данных любым протоколом шифрования, применяющимся во всех рассмотренных технологиях. Влияет на стоимость.

В таблице 2.3 приведены свойства и параметры меток рассмотренных технологий.

Таблица 2.3. Количественные критерии выбора радиометки в различных технологиях беспроводной радиосвязи

Технология	объём памяти (USER) нужно >280 бит	Шифрование данных на метке (пароль)	Макс. дальность считывания (прямой видимости), м	Срок службы	Мобильность	Стоимость метки (относительная)**
№ критерия	**1**	**2**	**3**	**4**	**5**	**6**
RFID LF (125-134 кГц)	2 Кбита	128 бит AES	0,7 м при антенне 0,7 м	10-50 лет пассивные	+	₽
RFID HF (13,56 МГц)	2 Кбита		1 м при антенне 0,7 м (до 2 м)		+	₽
RFID UHF (860-960 МГц)	3 Кбита		10 м (пассивная) -100 м (активная)		+	₽
RFID UHF для RTLS (2,4 ГГц)	256 Мбит		100 м	1-5 лет активные	+	₽
NF UHF (~900 МГц)	32 бита		0,3 м		+	₽
NFC (ISO/IEC 18000-3)	56 Кбит		0,1 м	50 лет	+	₽
Bluetooth (802.15.1) маячки стандарта Eddystone-EID	224 бит (28 байт) из них 152 бита (19 байт) URL		1-100 м или 50 м (BLE)	2-10 лет, память до 50 лет	+	₽₽
ZigBee 802.15.4*	480-1024 бита		80 м – 1 км	неск. недель – неск. месяцев	+	₽₽₽
Wi-Fi (802.11b,g,n,ac)	зависит от подключенного оборудования.	WPA2 AES	100 м – 2 км	Требуют постоянного источника питания	-	₽₽₽₽
WRAN 802.22			10 – 100 км		-	₽₽₽₽
WiMAX 802.16d			25 – 80 км		-	₽₽₽₽₽
802.16e (мобильный)			1 - 5 км		-	₽₽₽₽₽

* - для конечных устройств. Координатор и маршрутизатор должны иметь постоянное питание для поддержания сети.

** - стоимость метки условная, рассчитана по средней минимальной цене метки (устройства) на рынке.

3. ОПЕРАТИВНОЕ ОБНОВЛЕНИЕ ДАННЫХ В ГИС

3.1. Примеры интеграции радиотехнологий в ГИС

Проведем несколько экспериментальных примеров практического применения разработанной методики сбора данных.

3.1.1. Пример применения методики для интеграции данных с метки NFC в ГИС

Пример использования технологии NFC для хранения геоданных и их передачи в ГИС. Здесь и далее ГИС подразумевается в узком смысле как ПО и периферийное оборудование.

Пример состоит из демонстрации возможности записи и чтения данных метки NFC для последующей их передачи в ГИС и наоборот.

В данном примере использовались NFC метка компании NXP Semiconductors (Германия) типа NTAG 216 (рисунок 3.1), её параметры указаны в таблицах 1.2 и 1.3; программы NFC TagInfo, NXP TagWriter на смартфоне под управлением ОС Android 7.0.

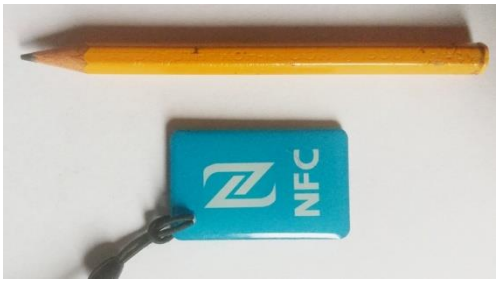


Рис.3.1. Метка NFC NTAG 216.

Технология NFC работает с близким радиусом действия и малым количеством памяти, поэтому примером может быть запись координат объекта, на который крепится NFC-метка и его ограниченные метаданные. Эти геоданные хранятся на самой метке и могут быть переданы в геоинформационную систему для дальнейшей обработки и отображения.

В качестве источника геоданных использовался тип веб-гис Портал открытых данных правительства Москвы https://data.mos.ru. Из него была взята одна строка данных реестра объектов, возводимых в рамках 214-ФЗ, т.е. один точечный объект строительства с его местоположением и метаданными (рис 3.2).

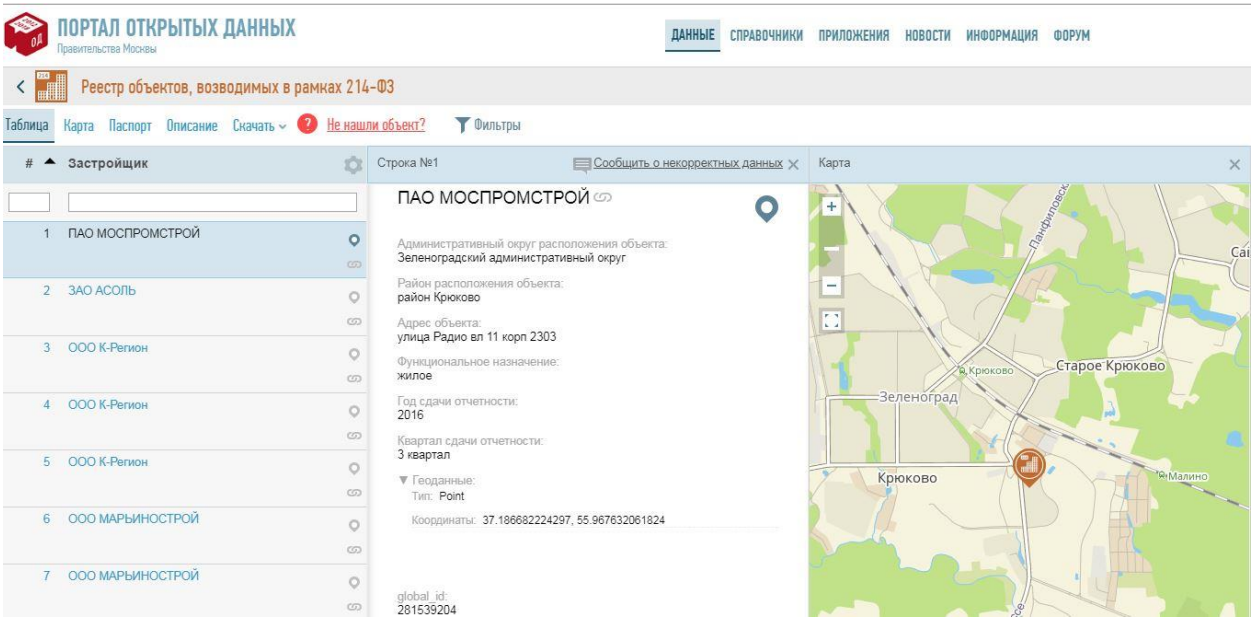


Рис.3.2. Данные для примера с Портала открытых данных (точечный объект).

Затем эти данные были экспортированы в формате .csv в QGIS (рис. 3.3, 3.4)

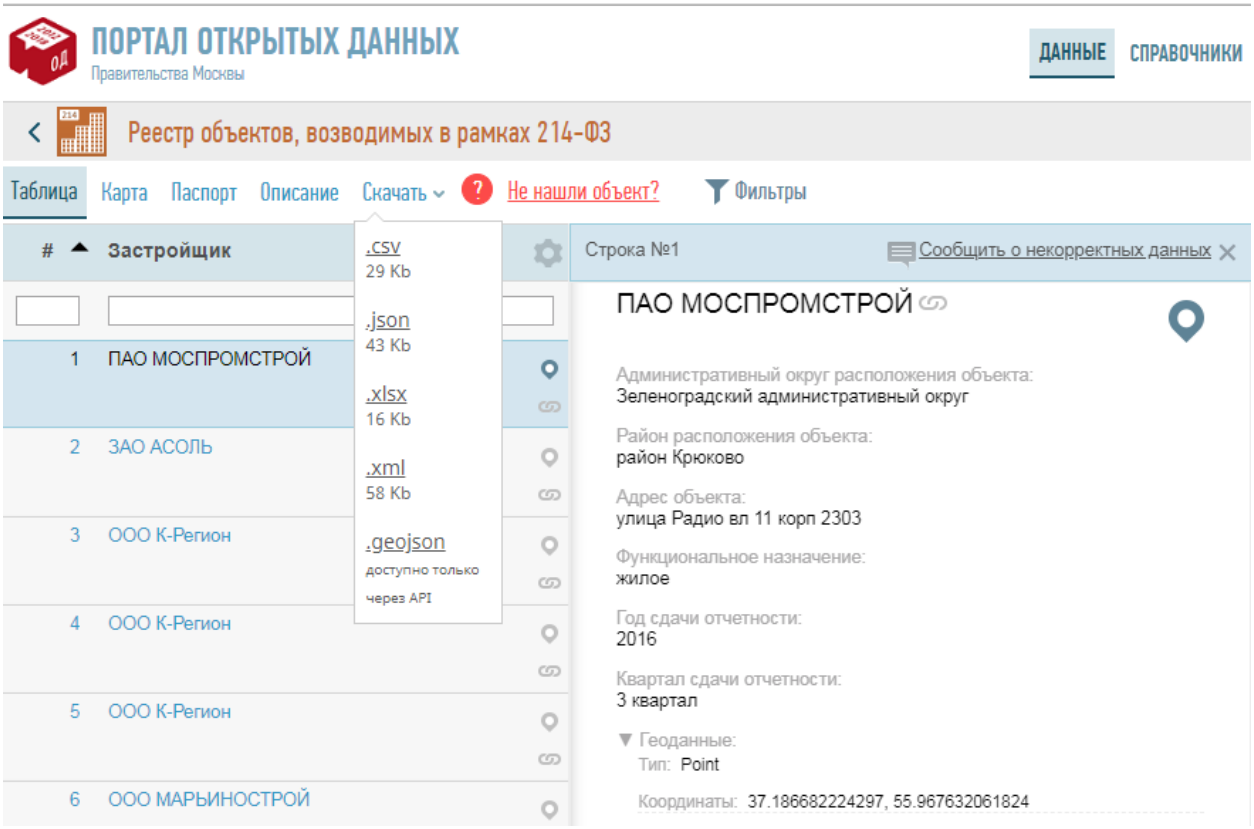


Рис.3.3. Экспорт данных с Портала открытых данных.

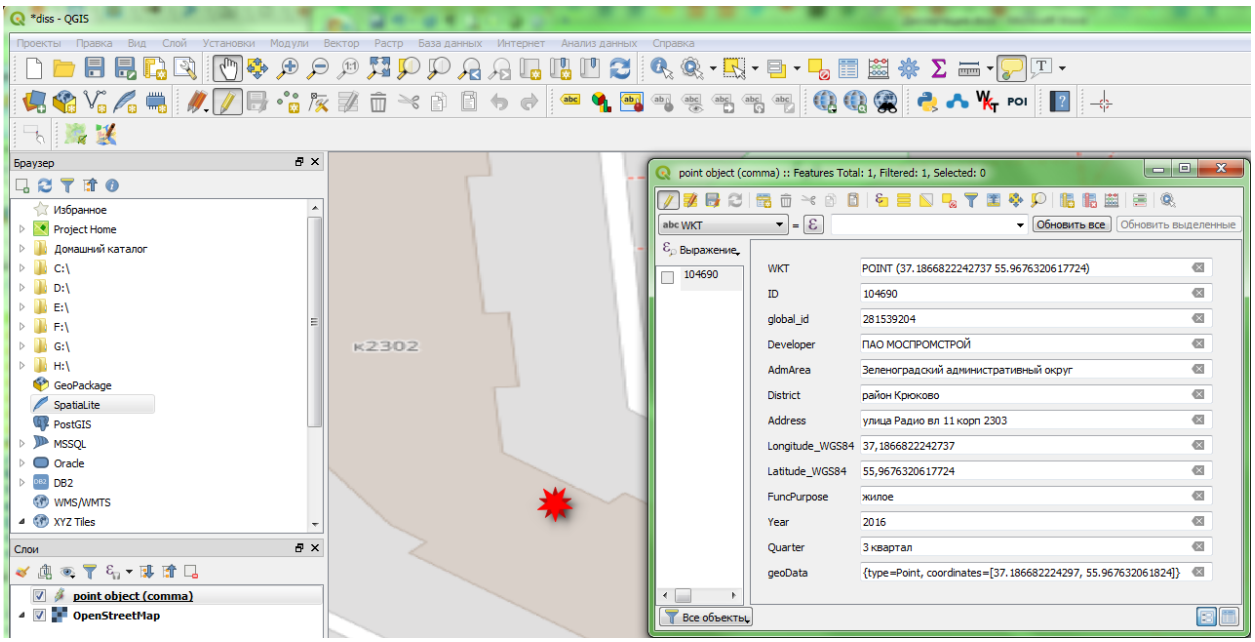


Рис.3.4. Данные с Портала открытых данных в QGIS

QGIS позволяет редактировать данные объекта формата CSV, а затем экспортировать их в нужном формате.

CSV – (Comma-Separated Values — значения, разделённые запятыми) — текстовый формат, предназначенный для представления табличных данных. Сегодняшняя ситуация такова, что CSV - набор значений, разделенных любыми разделителями, в любой кодировке с любыми окончаниями строк и различным экранированием спецсимволов. Это очень затрудняет обмен данными между программами.

Далее точечный объект был записан на NFC метку с помощью смартфона. В настоящее время существует два пути записи: запись вручную через соответствующую программу (использовалась TagWriter) и запись из файла в формате CSV, понятном для этой программы. Трудность в том, что экспортированный с Портала открытых данных файл CSV по структуре отличается как от экспортируемого из QGIS, так и читаемого программой TagWriter. Поэтому при небольшом объёме данных проще записать их вручную. Дополнительное удобство в том, что наглядно видно размер помещаемых данных.

TagWriter это бесплатная программа для Android смартфонов, позволяющая работать с метками NFC. Её основные функции представлены на рисунках 3.5, 3.6, 3.7.

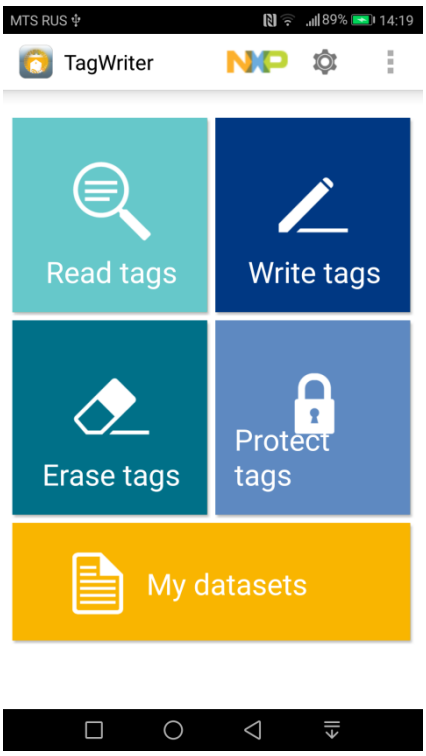


Рис.3.5. Основные возможности программы TagWriter (чтение, запись, очистка, защита меток NFC).

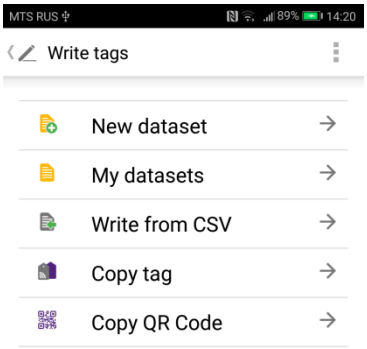


Рис.3.6. Возможности записи данных на метку NFC программы TagWriter

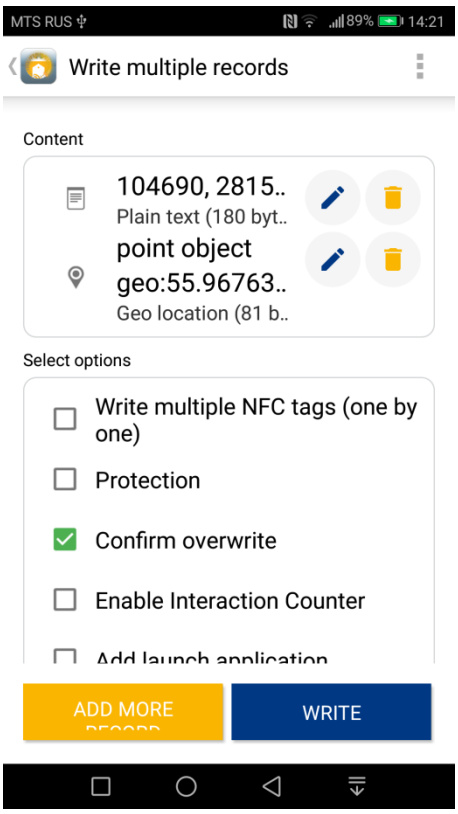


Рис.3.7. Процесс записи данных на NFC метку.

Программа позволяет установить счётчик обращений на метку, защитить данные на метке этого типа (NTAG) паролем 32 бит (4 символа), который не позволит удалить, перезаписать или форматировать данные на метке, но не защитит их от чтения (режим Password protection). Все опции защиты метки таковы (рис.3.8):

— Soft protection – защита «только чтение» для данных пользователя. Необратимое действие для NTAG метки. Однако можно очистить память и восстановить доступ к метке, данные будут потеряны.
— Lock tag – блокирует данные от изменения, необратимо.
— Lock prevention – не дает заблокировать данные, необратимо.

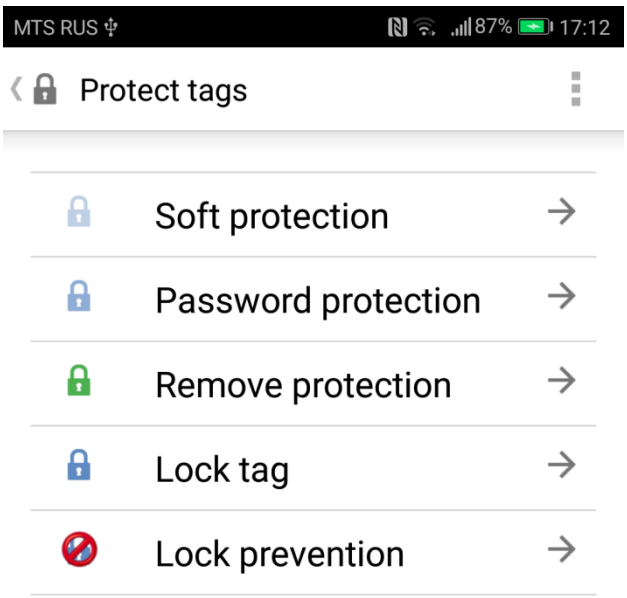


Рис.3.8. Способы защиты данных NFC метки в программе TagWriter.

После записи метка читается в этой же программе (рис.3.9). При нажатии на строчку с координатами загружается выбранная программа или сервис с картами, в которой показано местоположение по прочитанным координатам (рис. 3.10).

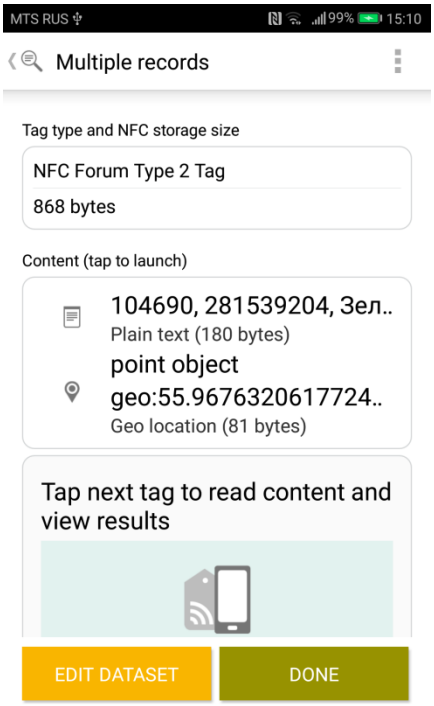


Рис.3.9. Окно программы TagWriter после чтения NFC метки.

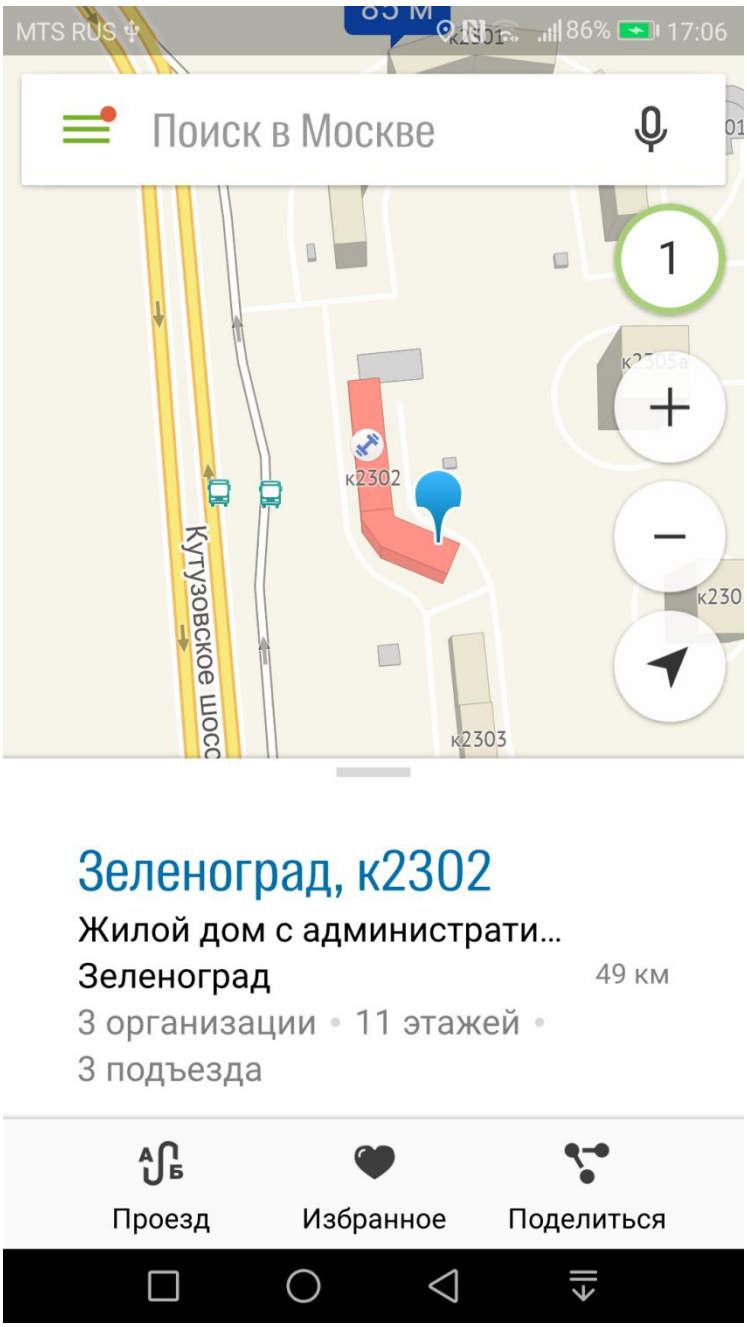


Рис.3.10. Объект в картографическом сервисе 2GIS после чтения координат метки.

Для чтения метаданных более удобна и информативна программа NFC TagInfo (рис.3.11).

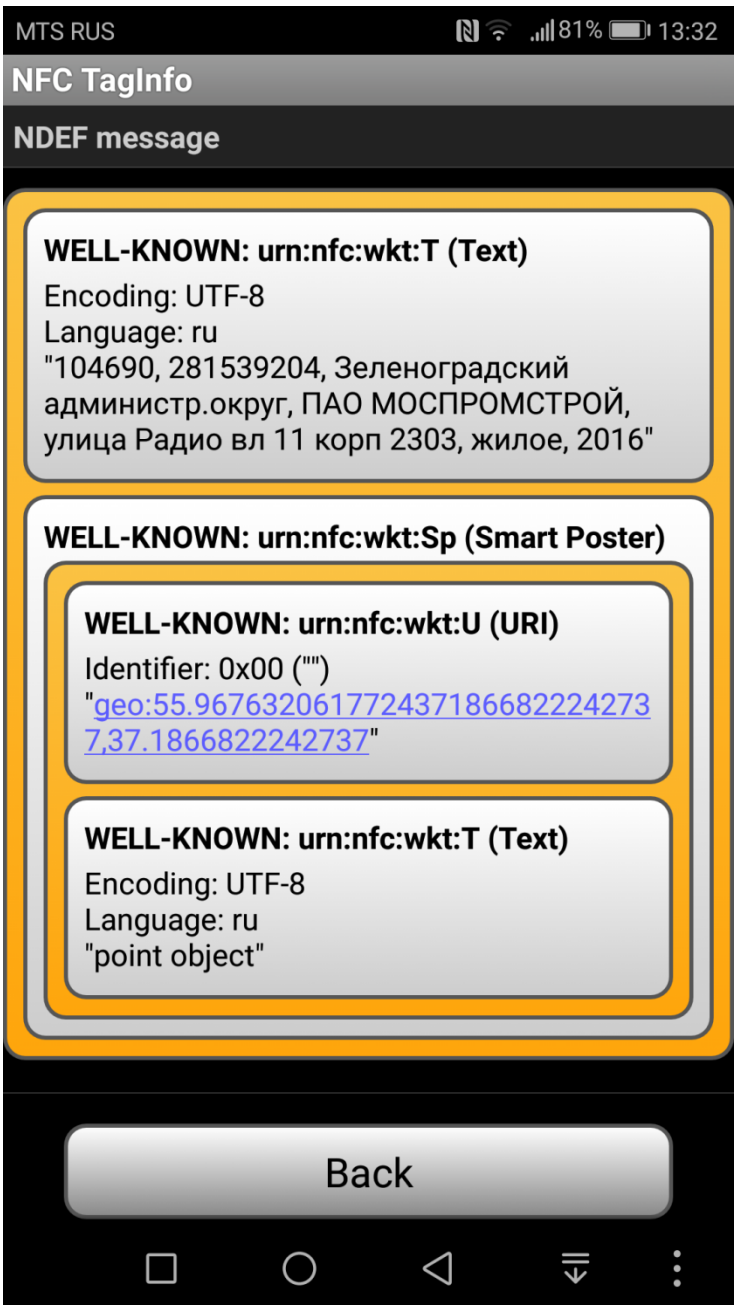


Рис. 3.11. Данные метки в программе NFC TagInfo.

Как видно из рисунка 3.11, на метку уместились все необходимые геоданные и метаданные точечного объекта. Задача записи геоданных и их метаданных на метку NFC выполнена.

Согласно [61], не существует стандартизированного формата записи координат на NFC метку. Есть три способа их записи:

— специальные схемы URI (например, Geo:, поддерживается Android);
— ссылки на облачный картографический сервис или клиент;
— сценарий (скрипт) переадресации, зависящий от операционной системы.

Ни один из распространенных форматов записи геоданных не позволяет внести на NFC метку высоту, полигональный или линейный объект, чтобы они таким же образом читались в картографических сервисах. Однако высоту можно записать отдельно в блок открытого текста, используя существующие программы. Вообще тэг *geo:* позволяет записывать необязательный параметр высота в метрах, как и все координаты, по умолчанию в непроецированной СК WGS-84.

Обратная задача – сбор данных с метки NFC и её передача в ГИС решается частично, не имея готового автоматизированного решения, кроме упомянутого мобильно-навигационного. Т.е. если считать ГИС картографический сервис, доступный со смартфона, то задача отображения местоположения объекта выполняется автоматически, но метаданные не переносятся, а берутся и зависят от картографического сервиса или программы.

В данном случае можно экспортировать из программ NXP TagWriter и NXP TagInfo наборы данных. Все данные, которые хранились на метке, записываются автоматически в эти наборы и хранятся на мобильном устройстве. Программа позволяет экспортировать наборы в двух форматах:

— формат *.twdb, читаемый только программами этого производителя (NXP), представляет собой файл базы данных SQLite, не распознаваемый как геоданные программами ГИС (QGIS).
— формат .xml (TagInfo), который легко можно прочитать текстовым редактором, но требуется специальная программа для интеграции в ГИС, т.к. тэги не унифицированы. Экспортируемый файл можно передать множеством способов (почта, сеть и др.), но он перегружен лишней информацией о метке.

Вычислим интегральный критерий эффективности радиометки Q для данного примера по формуле (3). Так как цель примера - демонстрация возможности записи и чтения данных метки NFC для последующей их передачи в ГИС, то будут востребованы все количественные критерии эффективности метки. Учитывая технические характеристики и общие условия применения NFC-метки, вычисляем интегральный критерий её эффективности с распределенными единичными весами, т.к. у нас не заданы конкретные условия:

$$Q_1 = 0{,}0114_1^1 \times 1_2{}^1 \times 0{,}3333_3^1 \times 0{,}6667_4^1 \times 1_5{}^1 \times 0{,}3333_6^1 = 0{,}00084$$

В данном случае были использованы все количественные критерии для выбора радиометки.

Таким образом, можно сделать вывод о потенциальной возможности интеграции данных с NFC меток в ГИС, для чего требуется дополнительная доработка программ, участвующих в интеграции.

Для записи данных на метку NFC также требуется доработка программ, если требуется записать большой объем данных, иначе можно обойтись ручным вводом и существующим ПО.

3.1.2. Пример применения методики для навигации внутри здания с помощью маячков в ГИС

Самый доступный способ определения расстояния до маячка – оценка его силы выходного сигнала RSSI Tx (дБм). Измеряется в децибел милливатт, где 0 дБм = 1 мВт.

RSSI (received signal strength indicator) - индикатор уровня принимаемого сигнала, полная электрическая мощность принимаемого приёмником сигнала.

Для стандартов Wi-Fi и Bluetooth 4.0, RSSI является единственным параметром, позволяющим измерить расстояние между приёмником и передатчиком с высокой точностью (по сравнению с оценкой по времени прохождения сигнала). Мощность выходного сигнала маячка вычисляется по формуле:

$$Tx = 10\lg\left(\frac{P(\text{Вт})}{1\ \text{мВт}}\right)\ (\text{дБм})\ \text{, где}$$

Tx (дБм) – мощность выходного сигнала маячка, дБм,

P (Вт) = абсолютная мощность, Вт.

В телекоммуникациях используется формула передачи Фрииса для вычисления мощности, получаемой одной антенной от другой антенны в идеальных условиях, находящейся на известном расстоянии и передающей известную мощность сигнала [62]:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2\text{, где}$$

G_t – коэффициент усиления антенны передатчика,

G_r – коэффициент усиления антенны приёмника,

P_t – мощность антенны передатчика без потерь, Вт,

P_r – мощность антенны приёмника без потерь, Вт,

R – расстояние между антеннами, м,

λ – длина волны передающегося сигнала, м.

Формула для вычисления уровня мощности (дБм) принимаемого сигнала (для вычисления расстояния) между приёмником и передатчиком, полученная из предыдущей формулы Фрииса:

$$P_d = P_0 - 10 \cdot n \cdot lg\left(\frac{d}{d_0}\right) \text{ , где}$$

d – расстояние от передатчика до приёмника, м;

d_0 – калибровочное расстояние (м) от приёмника до передатчика, на котором измерялась мощность сигнала P_0, обычно 1 м;

P_0 – мощность принимаемого сигнала на расстоянии d_0 от передатчика;

n – коэффициент потери мощности сигнала в среде его распространения (для воздуха n=2).

Таким образом, формула для вычисления расстояния выглядит следующим образом:

$$d = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_r}}$$

Однако эта формула применима только для открытых пространств и не учитывает переотражение сигнала, что даёт ошибку определения расстояния, сравнимую с самим расстоянием до передатчика.

Существуют другие способы определения расстояния и местоположения между приёмником и передатчиком радиосигнала, описываемые в [63], подробное рассмотрение которых не входит в данную работу.

Для демонстрации возможностей технологии BLE Beacons для сбора и отображения пространственных данных можно привести следующий простой пример, основанный на методе поиска ближайшей точки доступа [63].

Создаётся план сооружения или местности в формате SVG в местной системе координат. В данном случае это план этажа здания, в котором выделены помещения (рисунок 3.12). Заданным объектам карты присваивается MAC-адрес радиомаячка. В каждом помещении крепятся радиомаячки, транслирующие свой уникальный MAC-адрес. Координаты радиомаячков могут быть вычислены как для внутренней, так и для внешней систем координат.

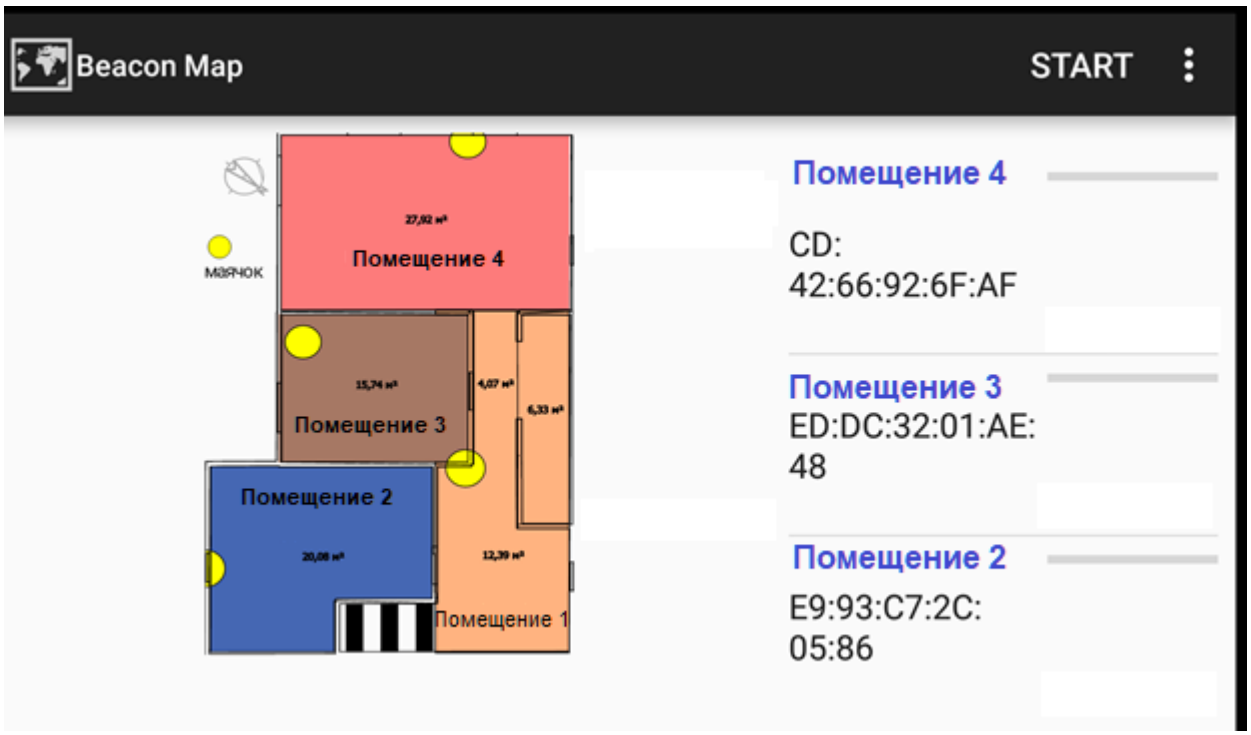
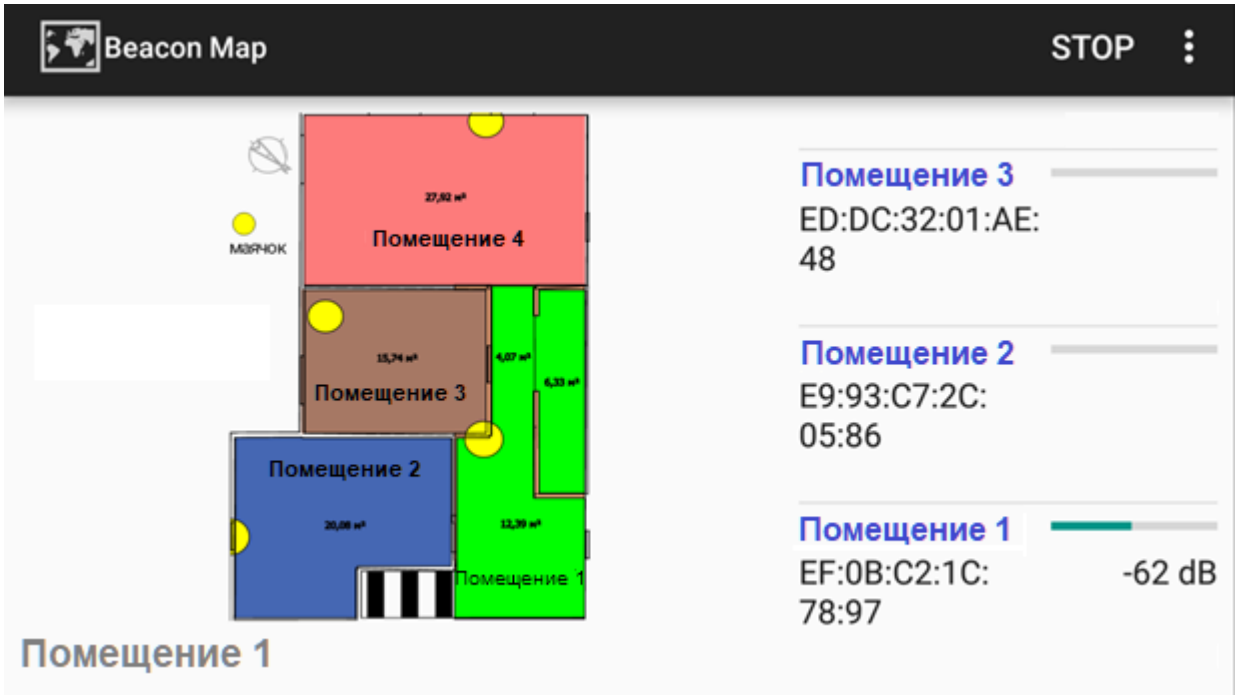


Рис. 3.12. План помещения с указанием размещения BLE маячков в формате SVG, загруженный в программу Beacon Mapper.

При приближении мобильного устройства к радиомаячку, программа (Beacon Mapper) рассчитывает силу сигнала RSSI и по ней на изображении выделяет зелёным цветом, в каком помещении находится приёмник сигнала (рисунок 3.13).



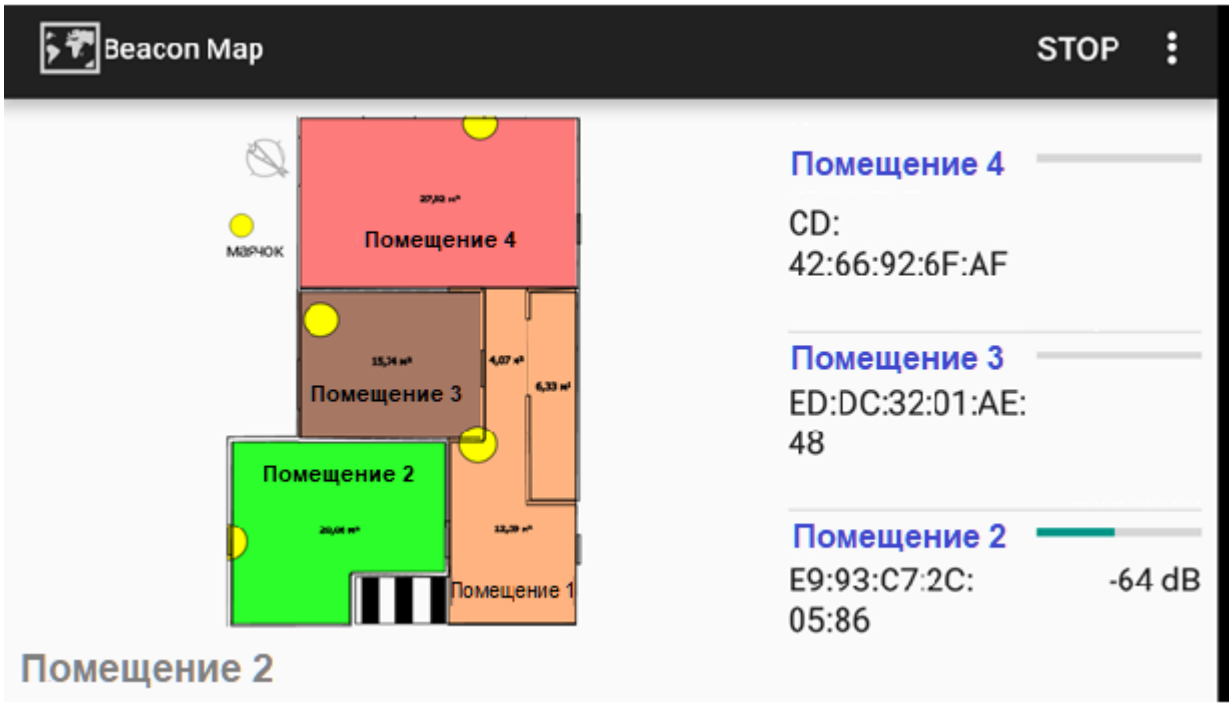


Рис. 3.13. Снимки экрана работы программы Beacon Mapper для определения местоположения приёмника по силе сигнала RSSI в помещении.

Вместо BLE маячков в этом методе определения местоположения по ближайшей точке доступа могут применяться любые излучающие радиоустройства из рассмотренных радиотехнологий (Wi-Fi, WiMAX и др.), соответственно изменится масштаб их применения. Однако достигнуть высокой точности и приемлемой надежности результатов в таком методе очень сложно из-за несовершенства математических моделей распространения радиоволн в разнородной среде. Для повышения точности определения местоположения предлагается комбинировать существующие алгоритмы определения расстояний по радиоволнам [64].

Существует мобильное ПО, способное определять как внутреннее, так и внешнее местоположение радиоустройств. Например, HERE indoor radiomapper позволяет загрузить план здания и совместить его с картой от Google, позволяя ориентироваться по маячкам, Wi-Fi, GPS и сотовым сетям (рисунок 3.14).

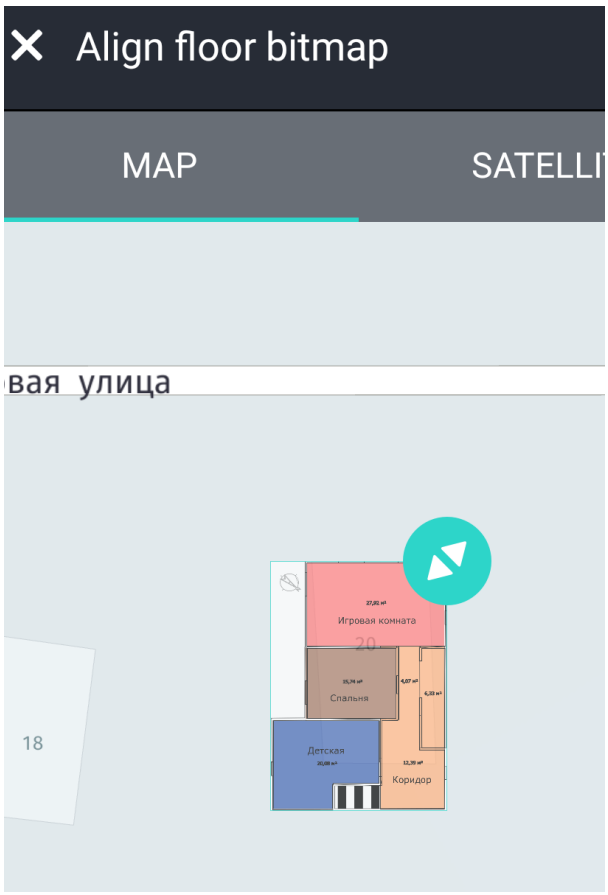


Рис.3.14. Привязанный план здания в программе HERE indoor radio mapper с использованием слоя Google maps.

Существующие доступные решения не обеспечивают достаточную точность определения местоположения маячка, ошибка может составлять сотни метров при переотражении сигнала. Однако в идеальных условиях можно довольно точно определить местонахождение радиомаячка с точностью 3-5 м без применения особых алгоритмов и технологий. Например, используя программу Beacon Locator, можно обнаружить радиомаячки, которые находились на расстоянии около 10 м друг от друга. На рисунке 3.15 информация о радиомаячках достоверно отсортирована по силе RSSI, хотя пересчет в метрах показывает неточные значения. Т.е. стоя рядом с радиомаячком с Minor ID: 22222, приложение правильно показывает, что он ближе.

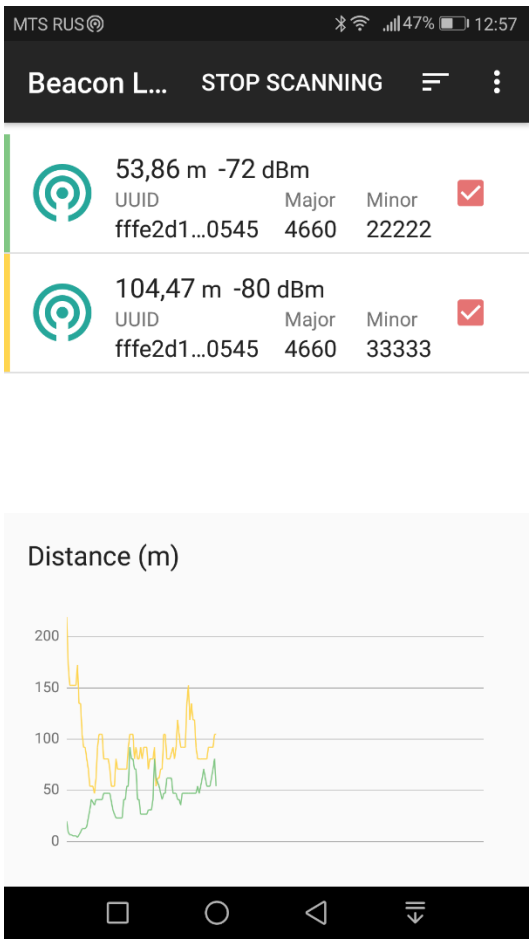


Рис. 3.15. Определение близости к определенному маячку в приложении Beacon Locator.

Вычислим интегральный критерий для маячка в этом примере.

$$Q_2 = 1_1^1 \times 1_2{}^1 \times 0{,}6667_3^1 \times 1_4^1 \times 1_5{}^1 \times 0{,}1539_6^1 = 0{,}10261$$

Объём памяти, шифрование, размеры метки в этом примере нас не интересовали (коэффициент и вес 1), фактический срок службы неизвестен, поэтому принимаем его максимальным для этого маячка (125 месяцев при интервале оповещения 1с). Стоимость маячка выше, чем у NFC-метки примерно вдвое (в 2,2 раза). В сравнении с предыдущим примером, интегральный критерий показывает в 122 раза лучший показатель. Это значит, что NFC-метка совершенно не подходит для навигации по сравнению с BLE-маячком.

3.1.3. Пример применения методики для идентификации опознака при привязке изображения в ГИС

При привязке изображений в ГИС часто возникает проблема поиска и уверенного распознавания естественных или искусственных опознаков на самом изображении. При **близком расположении однородных по текстуре объектов изображения** довольно трудно точно определить к какому из них относится опознак с известными координатами. Предлагается использо-

вать разработанную методику для увеличения надежности и быстродействия идентификации опознавательных знаков на изображении с помощью радиомаячков, помещаемых на или вблизи опознака для идентификации и определения приближенного местоположения опознака на изображении.

Координаты радиомаячка определяются с помощью считывателя (смартфон, БПЛА), обладающего возможностью точной собственной привязки. Точность должна быть не меньше, чем размер опознака и расстояние между ними. На этом же этапе происходит определение точных координат опознаков с помощью геодезических съемок.

При чтении радиометки считывается её уникальный идентификатор, вычисляются или считываются ее геодезические координаты, а также определяется положение в плоскости формируемого изображения в местной системе координат снимка. Указанные данные позволяют **вычислить зону поиска** для фотоизображения идентифицируемого объекта местности. Чем точнее данные о положении радиомаячка, тем значительнее сокращается зона поиска изображаемого объекта или опорной точки на снимке.

Применение методики даёт два преимущества:

1) Повышается надежность идентификации опознака на изображении для его последующей точной привязки. Считая, что все опознаки на изображении в заданной площади равновероятны, мы получаем увеличение надежности в N раз (для трансформированных снимков), где N – количество идентифицируемых опознаков, снабженных радиомаячками.

2) Повышается скорость опознавания опознавательных знаков на изображении при использовании корреляционной функции со сдвиговым алгоритмом, благодаря уменьшению области поиска опознака на снимке.

Коэффициент корреляции вычисляется по формуле:

$$r_{xy} = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \cdot \sum_{i=1}^{n} y_i}{\sqrt{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2} \cdot \sqrt{n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2}}$$

где r_{xy} — коэффициент парной корреляции от -1 до 1;

n — число возможных зон нахождения опознака размером b x b в пределах снимка;

x_i — i-ое значение координаты X в выбранной СК;

y_i — i-ое значение координаты Y;

Изображение местности S последовательно разбивается на произвольные одинаковые зоны размера b x b с перекрытием (рис.3.16), т.е. S = n (b x b). Далее вычисляется коэффициент корреляции координат радиомаячка для каждой такой зоны и при его максимальном значении делается вывод о наличии опознака в центре данной зоны.

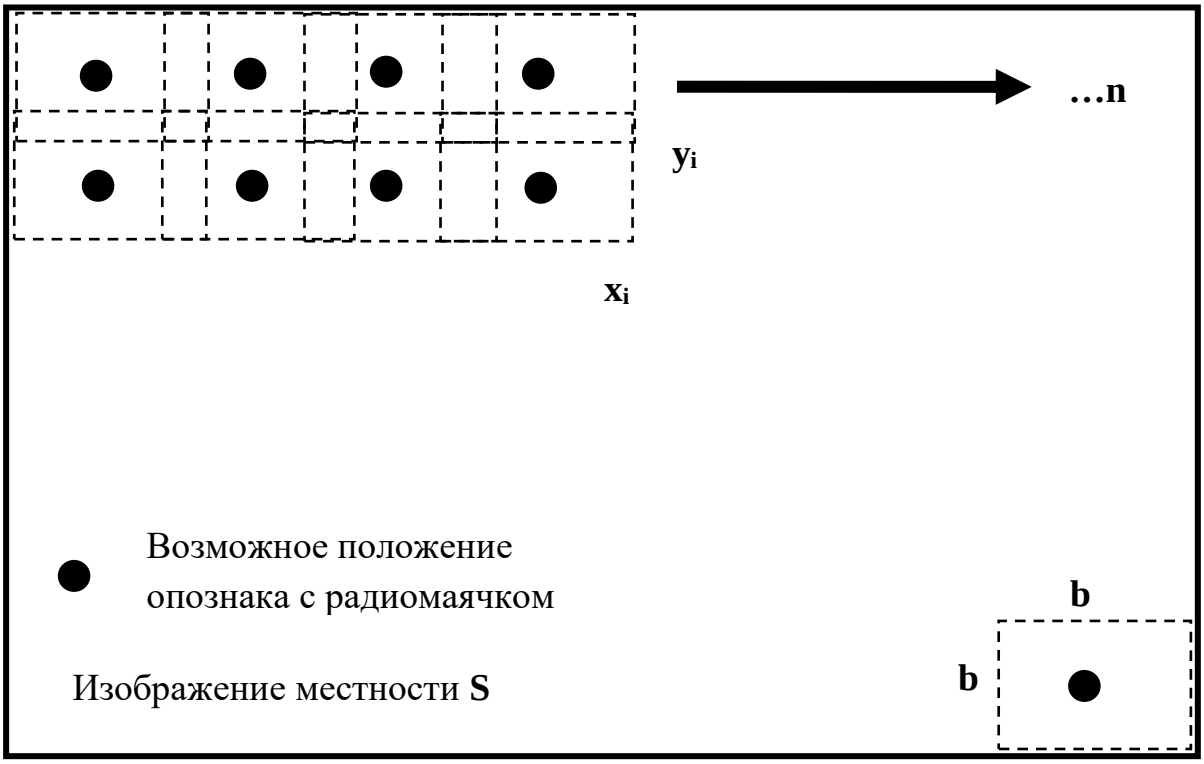


Рис.3.16. Схема алгоритма идентификации опознака на изображении с помощью функции парной корреляции.

Для проверки предложенного способа идентификации фотоизображений заданных объектов местности был проведен следующий эксперимент [65].

На местности в качестве опознаков были взяты три внутренних угла цветной рамки с регулярной изобразительной структурой (на рис.3.17 опознаки обозначены стрелками). Координаты двух углов рамки были измерены GPS-приёмником с точностью около 1 см (на рис.3.17 обозначены флажками). Фотосъемка местности производилась с БПЛА *DJI Mavic PRO* с высоты 30 метров, продольное/поперечное перекрытие = 85%. Радиомаячки были установлены вблизи опознаков в пределах 20 см. Координаты радиомаячков получены через смартфон с использованием программного обеспечения *Bluetooth LE Tool* ввиду отсутствия аналогичного ПО

для БПЛА. Изображения радиомаячков после предварительной ориентации снимков показаны как точки *1-3* на рисунке 3.17.

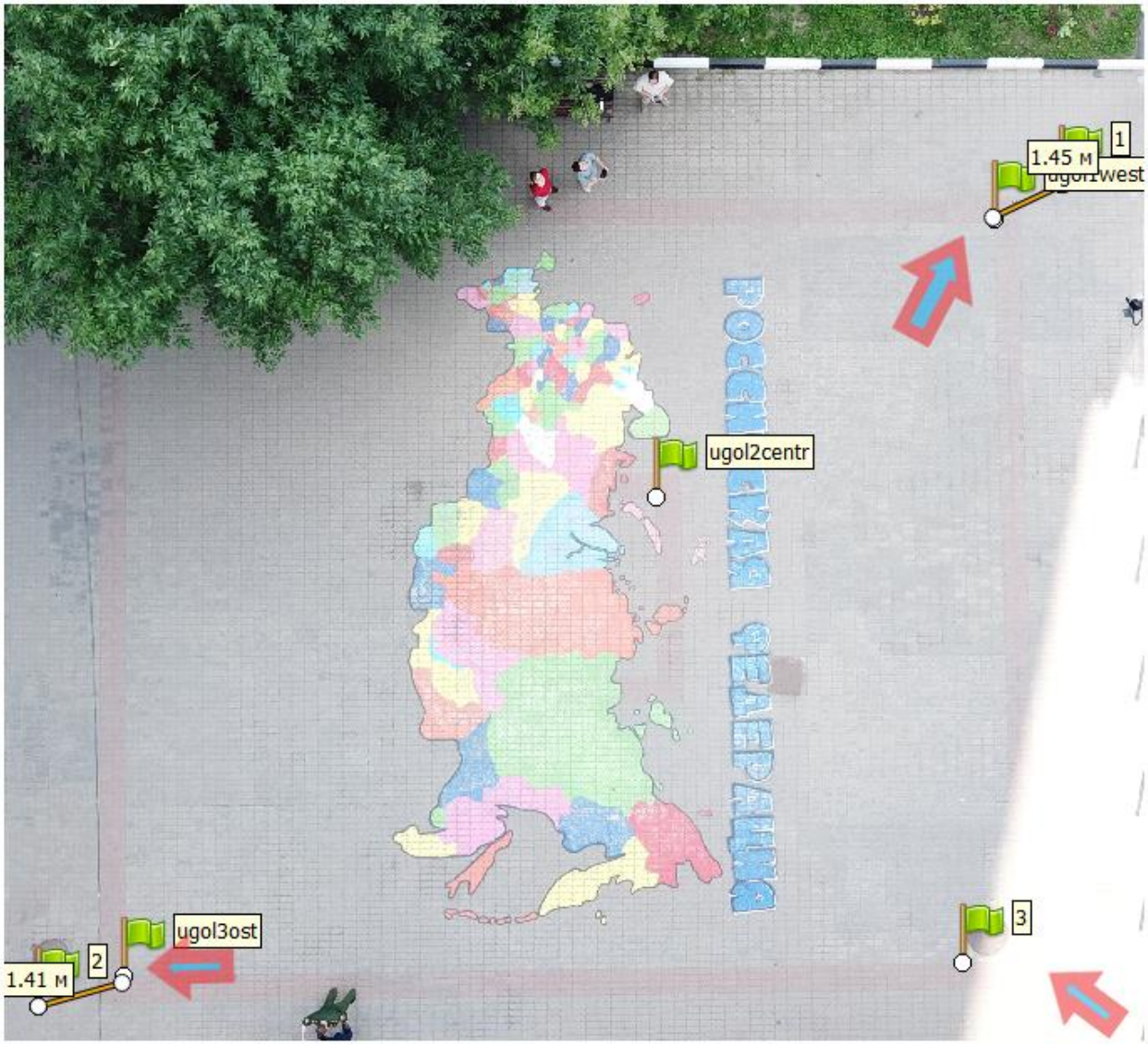


Рис.3.17. Снимок опознаков и положение радиомаячков.

Параметры съемки:

- Всего изображений: 26
- Высота полёта: 29.6 м
- Разрешение съёмки: 8.88 мм/пикс
- Площадь покрытия: 1080 м²
- Позиций съёмки: 24
- Модель камеры: FC220 (4.73mm)
- Разрешение: 4000 x 3000
- Фокусное расстояние: 4.73 мм

Съемочные материалы были загружены в программный пакет Agisoft Photoscan.

После завершения выравнивания в окне программы отображаются положения камер и разреженное облако точек (рисунок 3.18).

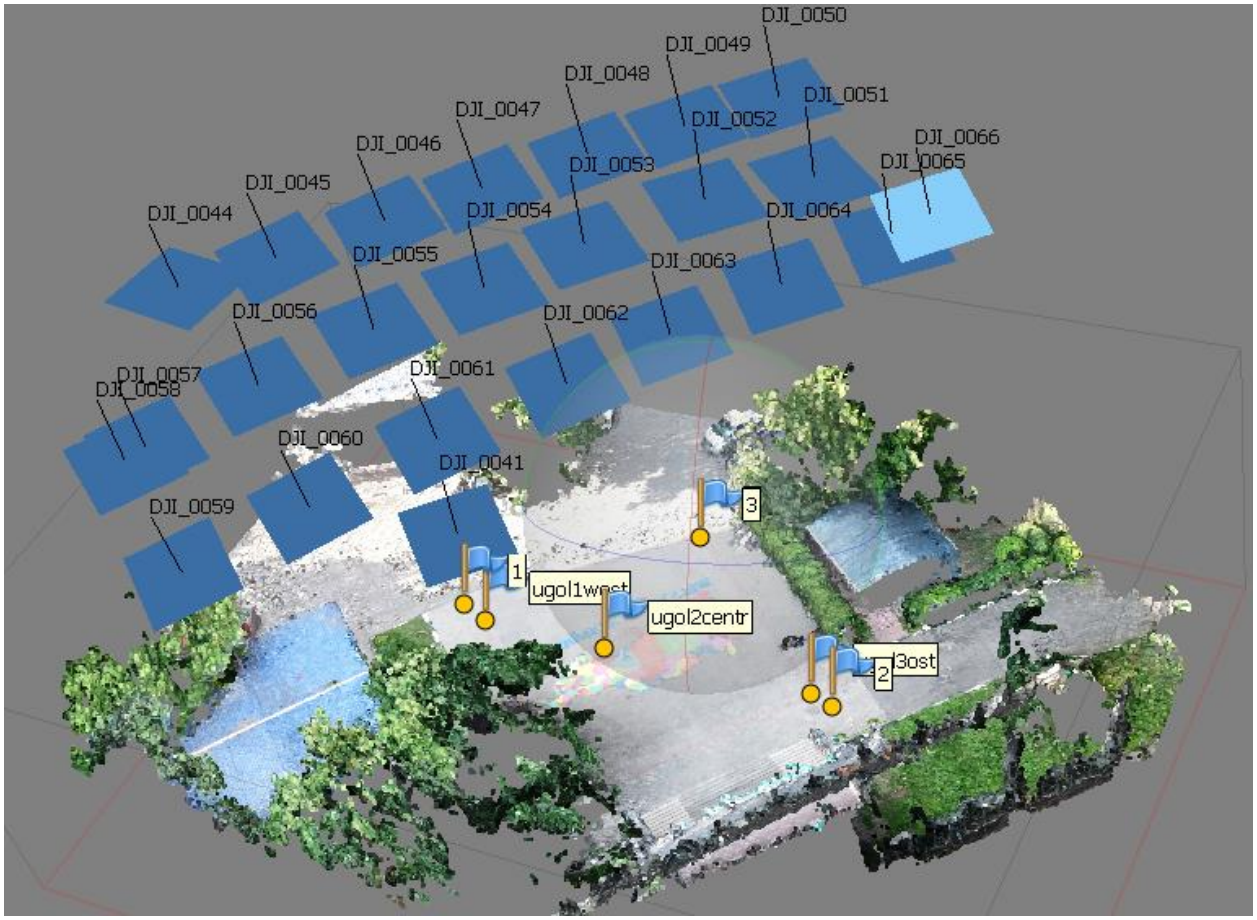


Рис.3.18. Разреженное облако точек съёмки в ПО Agisoft Photoscan.

После того, как ориентация и положение кадров определены, в проект поступает информация о координатах естественных опознаков, полученных посредством использования радиомаячка, которая показывает положение плоскости полученных снимков.

В результате эксперимента были получены следующие результаты. Среднее расхождение положения проекции естественного опознака и его координат, полученных посредством радиомаячка, составляет 1,43 метра. Ориентировочный расчёт показывает, что область поиска на снимке будет порядка 0,6 мм в диаметре в масштабе снимка (1:6343). При расстоянии между опознаками порядка десятков метров, точность определения зоны нахождения опознака вполне достаточна для его уверенной идентификации.

Эксперимент показал возможность применения разработанной методики оперативного обновления геоданных в ГИС и её практическую полезность на примере идентификации опознаков при точной привязке снимков.

3.2. Исследование методики сбора данных

Разработанная методика будет исследована по выбранным критериям для цели оперативного обновления ГИС по условной пятибалльной шкале:

1. критерий интеграции по местоположению;
2. критерий интеграции по времени;
3. критерий интеграции по тематике;
4. доступность геоданных для сбора;
5. наличие и полнота метаданных для поиска геоданных;
6. надежность хранения геоданных;
7. оперативность обновления данных в ГИС;
8. масштабируемость;
9. совместимость с существующей инфраструктурой геоданных.

Интеграцией называют восстановление и (или) повышение качественного уровня взаимосвязей между элементами системы, а также процесс создания из нескольких разнородных систем единой системы, с целью исключения (до технически необходимого минимума) функциональной и структурной избыточности и повышения общей эффективности функционирования [63].

Как показано в [64], среди критериев интеграции местоположения, времени и тематики, устойчивым критерием интеграции в ГИС как базе геоданных, является местоположение хранимого объекта. Т.е. методика учитывает все три критерия интеграции с ведущей ролью данных местоположения.

Доступность геоданных для сбора в сравнении с существующими методами повышается за счёт работы сразу с цифровыми данными, особенно при комбинировании разработанной методики с новыми технологиями и их развитием.

Критерий наличия и полноты метаданных для поиска геоданных означает, что разработанная методика позволяет увеличить качество и количество метаданных.

Надежность сбора, хранения, передачи данных увеличивается, т.к. происходит в цифровом виде с использованием современных техник защиты данных на цифровых носителях.

Оперативность обновления ГИС возрастает из-за скорости передачи данных и её надежности по сравнению с ручным вводом. Потенциально она зависит от уровня используемых технологий и может быть почти мгновенной в некоторых сценариях использования (например, сеть ZigBee с датчиками передает параметры в заданном интервале времени). Этот критерий является наиболее важным, т.к. текущая ситуация в мире имеет тенденцию к экспоненциальному увеличению количества данных, что требует увеличения скорости их сбора, обработки, передачи.

Масштабируемость означает, что данная методика может быть применима как к минимальным объемам данных (один объект), так и к глобальным, через сети охватывающим большие территории.

Совместимость с существующей инфраструктурой означает, что методика учитывает существующие методы сбора и хранения геоданных для нужд ГИС, являясь их комбинированием с новой технологической составляющей. Существующая инфраструктура телекоммуникаций достаточно развита для применения методики, не требуется изобретать новое оборудование – только использовать существующее с новым ПО.

Внедрение разработанной методики не требует существенных материальных и людских затрат. В основном, это вопрос разработки приложений и онлайн-сервисов, что уже происходит за рубежом и в небольшой степени в России.

Таблица 3.1. Соответствие методики сбора данных выбранным критериям

N	**Критерий**	**Степень соответствия критерию**
1	Критерий интеграции местоположения	5
2	Критерий интеграции времени	4
3	Критерий интеграции тематика	3
4	Доступность геоданных для сбора	4
5	Наличие и полнота метаданных для поиска	4
6	Надежность хранения данных	4
7	Оперативность обновления данных в ГИС	4
8	Масштабируемость	5
9	Совместимость с существующей инфраструктурой геоданных	4
10	Стоимость получения данных для ГИС	4
11	Стоимость инфраструктуры геоданных	4

3.3. Перспективы применения методики

В предыдущих примерах было видно, что точность определения местоположения мобильного устройства в технологии Bluetooth маячков совершенно недостаточна для задач навигации. Например, если передвигается не человек, а БПЛА или робот, то постоянно скачущая точность в 1-10 м внутри помещения не позволит ему передвигаться.

Последние разработки в стандартах Bluetooth 5.1. позволяют теоретическую возможность навигации с точностью до сантиметра. [66]

Согласно спецификации Bluetooth CS 5.1., предусмотрены два метода определения направления на устройство [66]:

1. Угол прибытия (**A**ngle **o**f **A**rrival). Передатчик (LE Transmitter) посылает специальные пакеты с одной антенны. Приёмное устройство, содержащее переключатель частоты (RF Switch) и массив антенн, принимает пакеты, переключая антенны и по разнице фаз вычисляет угол прибытия сигнала (рис. 3.19).

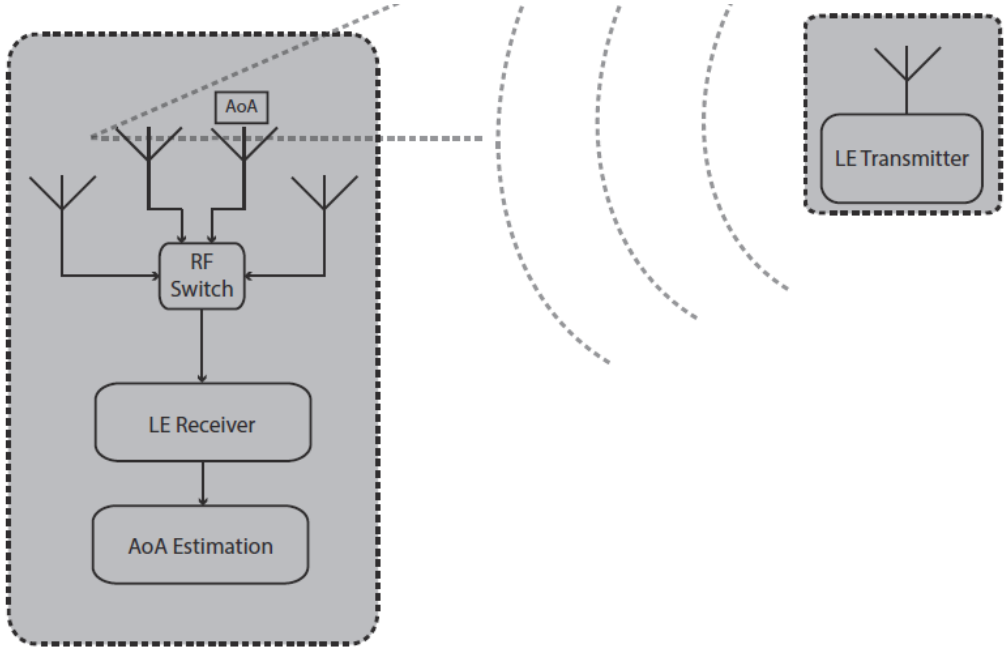


Рис. 3.19. Метод определения направления в BLE 5.1. по углу прибытия сигнала.

2. Угол передачи (**A**ngle **o**f **D**eparture). Устройство с вариатором частот и массивом антенн может создать свой угол передачи определяемым путем отправки специальных пакетов, переключая антенны во время передачи сигнала. Приемник с одной антенной получает эти пакеты и вычисляет угол передачи через задержку сигнала, зная расстояние между антеннами передатчика.

Оба метода используют одну формулу для вычисления угла:

$$\theta = arccos\left(\frac{(\psi\lambda)}{2\pi d}\right);$$

Где ψ – разность фаз сигналов, λ – длина волны, d – расстояние между антеннами массива.

Это новшество стандарта теоретически позволит навигацию, например, с помощью БПЛА в условиях городской застройки, когда автономные и стационарные устройства, работающие по технологии Bluetooth LE, расположенные на сооружениях, смогут как определять местоположение БПЛА с сантиметровой точностью, так и наоборот, позволят ему ориентироваться без применения оптики и GPS. А также при этом собирать или записывать данные на эти устройства, производить их поиск и обнаружение. Если навигация с БПЛА будет успешно реализована, это позволит значительно ускорить оперативное обновление данных ГИС и задействовать его автоматизацию.

ЗАКЛЮЧЕНИЕ

Итоги диссертационного исследования следующие.

- Исследованы возможности радиотехнологий хранения и передачи данных (RFID, NFC, Bluetooth, ZigBee, Wi-Fi, WRAN, WiMAX, BLE beacons) для применения их в оперативном обновлении ГИС.
- Разработаны требования к радиоинфраструктуре.
- Разработаны количественные критерии для выбора радиометки.
- Разработана и исследована методика сбора данных для ГИС с помощью современных радиотехнологий хранения и передачи данных, включая те, которые ранее в отрасли не применялись.

Экспериментально было доказано:

1. Эффективность и полезность методики сбора геоданных с помощью радиотехнологий в её применении для ускорения идентификации однородных опознаков на привязываемом снимке.
2. Применимость методики и радиотехнологий для целей внутренней и наружной навигации и обновления геоданных.
3. Применимость разработанной методики сбора и обновления геоданных с помощью радиотехнологий в ГИС на примере технологии NFC и QGIS.

Рекомендуется использовать радиометку в оперативном обновлении данных ГИС следующими способами:

1. В репере или марке с возможностями:

- записи на одноразовую радиометку (марку) параметров (номер, год изготовления, дата определения координат, координаты и метаданные;
- по силе радиосигнала (RSSI), времени прохождения сигнала, его вектору или комбинированными способами обнаружить примерное местоположение геодезического репера (марки, пункта, опознака) и считать с неё данные без визуального контакта с ней на расстоянии до 6 м (для пассивной метки) и порядка 100 м для активной и полуактивной меток (соблюдая условия радиовидимости);
- избежать повторных геодезических измерений при прямом переиспользовании записанных координат с метки;
- шифрования данных с координатами для прочтения меток только специализированным оборудованием в целях соблюдения требуемой секретности;

— измерять расстояние до метки, а также её координаты (при необходимости) соответствующим радиооборудованием, с точностью до 10 см, а с развитием технологий – точнее, что соответствует максимальной точности определения плановых, а тем более высотных координат с помощью GPS и ГЛОНАСС.

2. С помощью технологий позиционирования в реальном времени RTLS возможно определять местные координаты меток (до 1 см) или пользователя внутри зданий и сооружений, - в местах недоступных для прямого наблюдения с помощью спутниковой навигации.
3. Для оперативного обновления или отображения метаданных на кадастровой карте. Радиометка как приложение к паспорту участка в ЕГКН. Владельцу выдается метка с данными участка (владелец, площадь, год выдачи, номер участка), которая может быть прикреплена с внешней стороны забора (как почтовый ящик) и которую можно прочитать при необходимости.
4. Оперативное обновление данных в ГИС в реальном времени с помощью сетей активных меток (Eddystone, ZigBee, Wi-Fi, WiMAX и др.) в различных сочетаниях, либо в постобработке, путём ручного сбора данных с пассивных меток, либо меток, не имеющих доступа в интернет. Такие сети можно использовать для мониторинга схода лавин, оползней и других потенциально подвижных областей, где требуется постоянное обновление геоданных на некоторой небольшой площади.

Перспективы применения методики. Применение различных RFID-технологий с ГИС-технологиями выведет часть геодезической отрасли на новый технологический уровень, что позволит быстрее собирать различные виды данных, в том числе пространственные, а также облегчит процесс принятия решений, использующий такие данные.

Дальнейшая разработка темы диссертации имеет широкие **перспективы** в применении к различным отраслям народного хозяйства, где требуется оперативное обновление данных и геоданных точечно или на некоторой площади. При современном бурном развитии информационно-коммуникационных технологий видна возможность масштабирования применяемой методики и связанных с ней технологий, которое ограничено только технологиями связи. Также требуется расширение экспериментального апробирования и исследования применения методики в описанных ранее случаях её применения.

СЛОВАРЬ ТЕРМИНОВ

Асимметричное шифрование предполагает наличие двух ключей — открытого - для шифрования, и закрытого – для расшифровки. Отправитель перед отправкой создаёт у себя открытый ключ и шифрует им сообщение, после чего данное сообщение можно расшифровать только закрытым ключом, который создается и хранится в секрете у принимающей стороны.

Интернет вещей (Internet of Things, IoT) - сеть сетей, состоящих из уникально идентифицируемых объектов (вещей), способных взаимодействовать друг с другом без вмешательства человека, через IP-подключение. Ключевым в этом определении является автономность устройств и их способность передавать данные самостоятельно, без участия человека (поэтому смартфоны и планшеты не включены в эту концепцию).

Коллизия (collision — ошибка наложения, столкновения) — в терминологии компьютерных и сетевых технологий, наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени в среде передачи коллективного доступа.

Радиометка (метка) – в данной работе это любое устройство с памятью и возможностью чтения/записи геоданных и метаданных в/из неё и передачи этих данных посредством радиотехнологий по сети (RFID, NFC, Bluetooth LE маячков, ZigBee, Wi-Fi, WRAN, WiMAX и др.) вне зависимости от её расположения и назначения, источника питания. В зависимости от области применения, это может быть RFID-метка, NFC-метка, Bluetooth маячок, конечное устройство сети ZigBee, любое комбинированное устройство с памятью, датчиками, навигационным спутниковым приёмником, служащее в качестве носителя геоданных прямо или косвенно.

Симметричное шифрование — способ шифрования, в котором для шифрования и дешифровки применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами, участвующими в шифрованном обмене данными.

AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Этот алгоритм сейчас широко распространён, возникнув как стандарт в 2002 году.

Bluetooth — производственная спецификация беспроводных персональных сетей (Wireless personal area network, WPAN). Bluetooth обеспечивает обмен информацией между компьютерами, мобильными телефонами, периферийными устройствами, гарнитурами на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи в радиусе около 50 м (зависит от преград и помех).

Bluetooth-маяки (биконы, beacons), далее - радиомаячки, – класс автономных устройств, работающих по технологии Bluetooth Low Energy (BLE) на передачу (реже – приём) информации смартфону пользователя на расстоянии около 50 м (дальность вещания технологии BLE).

CSV – (Comma-Separated Values — значения, разделённые запятыми) — текстовый формат, предназначенный для представления табличных данных. Сегодняшняя ситуация такова, что CSV - набор значений, разделенных любыми разделителями, в любой кодировке с любыми окончаниями строк и различным экранированием спецсимволов. Это очень затрудняет обмен данными между программами.

EEPROM (Electrically Erasable Programmable Read-Only Memory) – энергонезависимая память малой ёмкости с возможностью записи, чтения и удаления данных. Это название используется теперь независимо от технологии изготовления используемой памяти (EEPROM, NOR flash).

NFC (Near field communication, «коммуникация ближнего поля», «ближняя бесконтактная связь») — технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров.

Push-технология («проталкивание») — способ распространения информации (контента), когда данные поступают от поставщика к пользователю по какой-либо сети на основе установленных параметров. Пользователь решает принять или отвергнуть данные.

RFID (Radio Frequency IDentification, радиочастотная идентификация) — метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

RSSI (received signal strength indicator) - индикатор уровня принимаемого сигнала, полная электрическая мощность принимаемого приёмником сигнала.

RTLS (Real-time Locating Systems — система позиционирования в режиме реального времени) — автоматизированная система, обеспечивающая идентификацию, определение координат, отображение на плане местонахождения контролируемых объектов в пределах территории, охваченной необходимой инфраструктурой. RTLS накапливает, обрабатывает и хранит информацию о местонахождении и перемещениях людей, предметов, мобильных механизмов и транспортных средств с целью мониторинга технологических и бизнес-процессов, сигнализации об отклонениях от регламентов, а также с целью ретроспективного анализа тех или иных процессов и ситуаций.

Wi-Fi IEEE 802.11 — семейство стандартов передачи данных по радиоканалам, а также торговая марка ассоциации Wi-Fi Alliance для беспроводных компьютерных сетей. Является беспроводным расширением сетей Ethernet и используется там, где неудобно или невозможно использовать проводные сети.

WiMAX IEEE 802.16 (Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная WiMAX Forum с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств. Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX - жаргонное название, т.к. это не технология, а название форума, на котором Wireless MAN и был согласован).

WRAN IEEE 802.22 — стандарт беспроводных сетей, соответствует физическому и канальному уровню модели OSI с типом соединения точка-многоточка (point-to-multipoint). Обмен данными происходит на свободных (white space) нелицензируемых частотах ОВЧ/УВЧ (54–862 МГц) телевизионного вещания. Радиус покрытия для фиксированного модема составляет 10-100 км, максимальная скорость до 22 Мбит/с при мощности передатчика 4Вт.

ZigBee - это набор протоколов и расширений к международному стандарту IEEE 802.15.4, реализация которых обеспечивает информационную совместимость устройств различных производителей выполняющих низкоскоростной обмен данными по радиоканалу на небольшие расстояния.

СПИСОК ЛИТЕРАТУРЫ

1. Chien-Ho Ko, 3D-Web-GIS RFID Location Sensing System for Construction Objects / Chien-Ho Ko // The Scientific World Journal. – 2013. – Vol. 2013. – Article ID 217972. DOI: 10.1155/2013/217972
2. Koshak N., Nour A. Center K.G.I.S.I. Integrating RFID and GIS to support urban transportation management and planning of hajj / N. Koshak, A. Nour // 13th International Conference on Computers in Urban Planning and Urban Management, Utrecht, The Netherlands. - 2013.
3. Arebey, Maher & Hannan, M.A. & Basri, Hassan & Abdullah, Huda. Solid waste monitoring and management using RFID, GIS and GSM / M.Arebey, M.A. Hannan, H.Basri, H. Abdullah // 2009 IEEE Student Conference on Research and Development (SCOReD). Serdang: IEEE. - 2009. - P. 37-40. DOI: 10.1109/SCORED.2009.5443382
4. Xiao, Ning-Cong & Li, Xunbo & Qin, Guangxu & Ma, Songqing & Zhang, Li. Localization system based on RFID and GIS for underground moving targets / Ning-Cong Xiao, Xunbo Li, Guangxu Qin, Songqing Ma, Li Zhang // 2008 IEEE International Conference on Mechatronics and Automation. Takamatsu: ICMA. - 2008. - P. 808-813. DOI: 10.1109/ICMA.2008.4798861
5. Ahmed, Ashir. Role of GIS, RFID and handheld computers in emergency management: an exploratory case study analysis / Ashir Ahmed // JISTEM - Journal of Information Systems and Technology Management (Online). – 2015. Vol.12 (1). - P.3-27. DOI:10.4301/s1807-17752015000100001
6. Boonsong, Wasana, & Ismail, Widad. Wireless Monitoring of Household Electrical Power Meter Using Embedded RFID with Wireless Sensor Network Platform / Wasana Boonsong, Widad Ismail // International Journal of Distributed Sensor Networks. - 2014. P.1-10. DOI:10.1155/2014/876914
7. RFID [Электронный ресурс] / Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/RFID (дата обращения 18.02.2018).
8. Финкенцеллер К. Справочник по RFID. Теоретические основы и практическое применение индуктивных радиоустройств, транспондеров и бесконтактных чип-карт. [Текст]: пер. с нем. / К. Финкенцеллер. М.: Додэка-XXI, 2008. 488 с. ISBN 978-5-94120-151-8
9. Сандип Лахири. RFID. Руководство по внедрению = The RFID Sourcebook / Дудников С. М.: Кудиц-Пресс, 2007. 312 с.
10. Маниш Бхуптани, Шахрам Морадпур. RFID-технологии на службе вашего бизнеса = RFID Field Guide: Deploying Radio Frequency Identification Systems / Троицкий Н. М.: Альпина Паблишер, 2007. 290 с.
11. Технологии позиционирования в реальном времени [Электронный ресурс] / rtlsnet.ru. – Режим доступа : http://www.rtlsnet.ru/technology/view/4 (дата обращения 23.09.2019).

12. Regulatory status for using RFID in the EPC Gen2 (860 to 960 MHz) band of the UHF spectrum [Электронный ресурс] / The Global Language of Business. – Режим доступа : https://www.gs1.org/sites/default/files/docs/epc/uhf_regulations.pdf (дата обращения 23.05.2018).

13. Что такое NFC [Электронный ресурс] / NFC UKRAINE. – Режим доступа : http://nfcukraine.com (дата обращения 24.05.2018).

14. Near Field Communication [Электронный ресурс] / Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/Near_Field_Communication (дата обращения 15.06.2018).

15. Standard ECMA-340, Near Field Communication Interface and Protocol (NFCIP-1) [Электронный ресурс] / Ecma International. – Режим доступа : http://www.ecma-international.org/publications/standards/Ecma-340.htm (дата обращения 15.06.2018)

16. Standard ECMA-352, Near Field Communication Interface and Protocol −2 (NFCIP-2) [Электронный ресурс] / Ecma International. – Режим доступа : http://www.ecma-international.org/publications/standards/Ecma-352.htm (дата обращения 15.06.2018).

17. Hancke, Gerhard P. Eavesdropping Attacks on High-Frequency RFID Tokens / Gerhard P. Hancke // Journal of Computer Security - 2010 Workshop on RFID Security (RFIDSec'10 Asia). - 2011.Vol.19 (2). - P. 259—288.

18. NFC чипы [Электронный ресурс] / База знаний NFCpoint. – Режим доступа : http://nfcpoint.ru/wiki/doku.php?id=nfc_chip_types (дата обращения 20.06.2018).

19. Сайт производителя NFC [Электронный ресурс] / nxp.com. – Режим доступа : http://www.nxp.com (дата обращения 20.06.2018).

20. Решение № 04-03-04-003 от 6 декабря 2004 года. - Государственная комиссия по радиочастотам (ГКРЧ). г. Москва, 2004. - 7 с.

21. Bluetooth [Электронный ресурс] / Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/Bluetooth (дата обращения 25.06.2018).

22. Энциклопедия АСУ ТП [Электронный ресурс]. - Режим доступа : http://www.bookasutp.ru (дата обращения 26.06.2018).

23. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с. ISBN: 5-94836-049-0.

24. Ellisys Bluetooth Security – Truths and Fictions [Электронный ресурс] / ellisys.ru. – Режим доступа : http://ellisys.ru/technology/een_bt06.pdf (дата обращения 27.06.2018).

25. Артюшенко В. М. Электротехнические системы жизнеобеспечения зданий на базе технологий BACNET [Текст] / Монография. М.: ГОУ ВПО «МГУС», 2006. 138 с.
26. ZigBee specification. Document 053474r13. - ZigBee Standards Organization, Dec. 1, 2006. [Электронный ресурс] / olmicrowaves.com. – Режим доступа : http://www.olmicrowaves.com/menucontents/designsupport/zigbee/1171625602_ZigBee-Specification-2006-r13.pdf (дата обращения 27.06.2018).
27. Szewczyk R., Woo A., Hollar S., Culler D. E., Pister K. System Architecture Directions for Networked Sensors / R. Szewczyk, A. Woo, S. Hollar // the 9th International Conference on Architectural Support for Programming Languages and Operating Systems. New York, 2000, P. 93-104.
28. Короткова Е.В., Вершинин Е.В. Проблемы энергоэффективности и защиты данных в беспроводных сенсорных сетях // Электронный журнал: наука, техника и образование. - 2016. № 2 (6). - С. 125-132.
29. ZigBee Alliance [Электронный ресурс]. – Режим доступа : http://www.zigbee.org (дата обращения 1.07.2018).
30. IEEE Standards Association [Электронный ресурс]. – Режим доступа : http://standards.ieee.org (дата обращения 1.07.2018).
31. Official IEEE 802.11 Working Group Project Timelines [Электронный ресурс] / grouper.ieee.org. – Режим доступа : http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm (дата обращения 2.07.2018).
32. IEEE 802.22TM-2011 Standard for Wireless Regional Area Networks in TV Whitespaces Completed [Электронный ресурс] / businesswire.com. – Режим доступа : http://www.businesswire.com/news/home/20110726007223/en/IEEE-802.22TM-2011-Standard-Wireless-Regional-Area-Networks (дата обращения 2.07.2018).
33. IEEE 802.22 Working Group on Wireless Regional Area Networks [Электронный ресурс] / ieee802.org. – Режим доступа : http://www.ieee802.org/22 (дата обращения 3.07.2018).
34. 802.22 White Space: новый стандарт беспроводной связи [Электронный ресурс] / Эл. журнал xakep.ru. – Режим доступа : https://xakep.ru/2011/11/17/57821 (дата обращения 3.07.2018).
35. WiMAX [Электронный ресурс] / Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/WiMAX (дата обращения 4.07.2018).
36. Push notifications explained [Электронный ресурс] / Urban Airship urbanairship.com. – Режим доступа : https://www.urbanairship.com/push-notifications-explained (дата обращения 5.07.2018).
37. Индустриальный интернет вещей [Электронный ресурс] / Сайт Ростелеком. – Режим доступа : https://www.rostelecom.ru/projects/IIoT/study_IDC.pdf (дата обращения 5.07.2018).

38. Dixys L. Hernández-Rojas, Tiago M. Fernández-Caramés, Paula Fraga-Lamas, Carlos J. Escudero. Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications [Электронный ресурс]. – Режим доступа : http://www.mdpi.com/1424-8220/18/1/57/htm // Sensors. 2018. № 18 (1), 57; doi:10.3390/s18010057 (дата обращения 7.07.2018).
39. Лыгин, А.Н. RFID-технологии и возможности их применения в геодезии / А.Н. Лыгин, И.И Лонский, В.В. Калугин, В. В. Шлапак // Известия высших учебных заведений. Геодезия и аэрофотосъемка. МИИГАиК, 2015. № 6. С.125-130.
40. Лыгин, А.Н. Применение RFID-технологии и ГИС в геодезии / А.Н. Лыгин // Известия высших учебных заведений. Геодезия и аэрофотосъемка. МИИГАиК, 2016. №6. С.105-110.
41. National Marine Electronic Association. [Электронный ресурс]. – Режим доступа : http://www.nmea.org (дата обращения 10.07.2018).
42. Технические спецификации протокола NMEA в фирме Garmin [Электронный ресурс]. – Режим доступа : http://www.garmin.com (дата обращения 10.07.2018).
43. Национальная библиотека им. Н.Э. Баумана [Электронный ресурс]. – Режим доступа : https://ru.bmstu.wiki/EEPROM_(Electrically_Erasable_Programmable_Read-Only_Memory) (дата обращения 10.07.2018).
44. Сайт компании HID Global [Электронный ресурс]. – Режим доступа : https://www.hidglobal.ru (дата обращения 11.07.2018).
45. Сайт RFID [Электронный ресурс]. – Режим доступа : http://www.rf-id.ru (дата обращения 11.07.2018).
46. ISBC Технологии RFID идентификации [Электронный ресурс]. – Режим доступа : http://www.isbc-rfid.ru (11.07.2018).
47. Traub, Ken. EPC Memory vs. User Memory. [Электронный ресурс] / Ken Traub // RFID journal. 2016. – Режим доступа : http://www.rfidjournal.com/articles/view?15156 (дата обращения 12.07.2018).
48. Лыгин, А.Н. Обзор проблем безопасности данных в технологиях RFID для геоинформационных систем / А.Н. Лыгин // Известия высших учебных заведений. Геодезия и аэрофотосъемка. МИИГАиК, 2018. Т. 62. №4. С.453 – 460.
49. Жуков, А.Е. Легковесная криптография. Часть 1 / А.Е. Жуков // Вопросы кибербезопасности. 2015. № 1 (9). С. 26-43. - [Электронный ресурс] / cyberrus.com. – Режим доступа : http://cyberrus.com/wp-content/uploads/2015/05/vkb_09_04.pdf (дата обращения 14.07.2018).
50. Biryukov A., Khovratovich D. Related-key Cryptanalysis of the Full AES-192 and AES-256 [Электронный ресурс] / A. Biryukov, D. Khovratovich // Advances in Cryptology. University of

Luxemburg, 2009. – Режим доступа : https://eprint.iacr.org/2009/317.pdf (дата обращения 14.07.2018). DOI: 10.1007/978-3-642-10366-7_1.

51. Симметричные криптосистемы [Электронный ресурс] / Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/Симметричные_криптосистемы (дата обращения 15.07.2018).
52. Жуков, А.Е. Легковесная криптография. Часть 2 / А.Е. Жуков // Вопросы кибербезопасности. 2015. № 2 (10). С. 2-10 [Электронный ресурс] / cyberrus.com. – Режим доступа : http://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (дата обращения 14.07.2018).
53. Robert R. Oberle. Rfid tag using encrypted password protection. [Электронный ресурс]. – Режим доступа : https://patentimages.storage.googleapis.com/23/db/29/3754d458bec49a/US20090096574A1.pdf (дата обращения 15.07.2018).
54. Блог разработчиков Google [Электронный ресурс]. – Режим доступа : https://developers.google.com/beacons/eddystone (дата обращения 15.07.2018).
55. Грязин, Д.С. Разработка угоноустойчивого комплекса автомобиля / Д.С. Грязин // Труды 56 научной конференции МФТИ.М.: МФТИ, 2013. С.171-172.
56. Кондауров, И.Н., Беляев, В.А. Использование ГИС-сервисов в системах с подвижными GPS-приемниками / И.Н. Кондауров, В.А. Беляев // Изв. вузов. Геодезия и аэрофотосъемка, 2012. №6. - С.72–76.
57. Дудяк, Е.И. Методы определения координат сотрудников и техники предприятия с использованием технологии WI-FI / Е.И. Дудяк // Техника радиосвязи. Омск.: Омский научно-исследовательский институт приборостроения, 2015. № 1 (24). С. 67-77.
58. Богуренко, П.А., Бурлаков, М.Е. Обзор методов локального позиционирования объектов в wi-fi-сетях /П.А. Богуренко, М.Е. Бурлаков // Вестник ПНИПУ, 2017. № 23. С. 146-158.
59. Kirkland, Wash. Bluetooth Enhances Support for Location Services with New Direction Finding Feature. 2019 [Электронный ресурс] / bluetooth.com. – Режим доступа : https://www.bluetooth.com/news/pressreleases/2019/01/bluetooth-enhances-support-for-location-services-with-new-direction-finding-feature (дата обращения 20.07.2019).
60. Журкин, И.Г., Шайтура, С.В. Геоинформационные системы. / И. Г. Журкин, С.В. Шайтура. – М.: Кудиц-пресс, 2009. - 272 с.
61. Сайт NFC Forum [Электронный ресурс]. – Режим доступа : https://nfc-forum.org (дата обращения 22.07.2018).
62. Рутледж Д. Энциклопедия практической электроники. - М.: ДМК Пресс, 2002. - 522 с.
63. Соловьёв, И.В. Применение модели информационной ситуации в геоинформатике / И.В. Соловьёв // Науки о Земле, 2012. №1. С. 54-58.

64. Кудж, С.А. Организация геоданных / С.А. Кудж // Перспективы науки и образования, 2014. №1. - С.61-65.

65. Журкин, И.Г., Лыгин, А.Н., Митрофанов, Е.М. Методика применения радиометок для оперативного обновления геоданных в ГИС средствами дистанционного зондирования / И.Г. Журкин, А.Н. Лыгин, Е. М. Митрофанов // Изв. вузов «Геодезия и аэрофотосъемка». - 2019. Т. 63. № 5. - С.584-590 DOI: 10.30533/0536-101X-2019-63-5-584-590

66. Bluetooth Core Specification 5.1 [Электронный ресурс]. – Режим доступа : https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457080&_ga=2.44860900.1982500905.1548831725-1150752798.1548831725 (дата обращения 23.08.2018).