DOI: 10.25728/avtprom.2021.09.09

Комплексная система управления и обеспечения безопасности предприятия на базе беспроводных технологий Private LTE и Wi-Fi 6

Е.В. Трифонов, А.Н. Шмурьев (Компания Триалинк)

Обоснована важность и актуальность создания единой коммуникационной среды предприятия, состоящей из опорной сети, системы беспроводной связи, универсальных абонентских устройств и специального программного обеспечения. Проанализированы функциональные возможности беспроводных протоколов передачи данных Private LTE и Wi-Fi 6. Рассмотрены возможности и состав программно-аппаратного комплекса «МАРС Мониторинг», на базе которого предлагается разворачивать единую коммуникационную среду предприятия.

Ключевые слова: единая коммуникационная среда предприятия, беспроводные протоколы передачи данных, абонентские терминалы, PoC системы, резервирование, информационная безопасность, Private LTE, Wi-Fi 6, критически важная инфраструктура.

Введение. Цифровая трансформация и Industry 4.0

Программы цифровой трансформации и перехода на решения уровня Industry 4.0 приняты как на Федеральном уровне, так и в большинстве компаний и организаций самого различного профиля. В рамках Industry 4.0 используются технологии обработки больших данных, облачные решения, Internet вещей, цифровые двойники, приложения на базе искусственного интеллекта и др.

Процесс внедрения элементов Industry 4.0 достаточно сложный и дорогой. Кроме того, предприятия имеют различную степень готовности к цифровой трансформации. В связи с этим реальным представляется постепенный, поэтапный переход на решения уровня Industry 4.0. Такой эволюционный переход может занять несколько лет и потребует планирования не только капитальных вложений, но и решения технических вопросов. Современная ИТ-сфера – это наиболее динамично развивающаяся область. Новые технологии появляются ежегодно. Срок работы старых технологий в области ИТ сокращается, поэтому очень важно с самого начала правильно выбрать технические средства и решения, которые бы позволяли обеспечить интеграцию с другими системами и решениями сегодня и имели возможность модернизации и развития в будущем.

Единая информационная среда предприятия

Важной задачей современного предприятия является создание единой коммуникационной среды, состоящей из опорной сети, системы беспроводной связи, универсальных абонентских устройств и специального программного обеспечения. Единая коммуникационная среда дает возможность внедрения и интеграции в единый контур управления различных систем управления, применяемых на уровне технологических процессов, производства и предприятия в целом, а также систем управления, связанных с организацией охраны и безопасности промышленного объекта. К единой среде подключаются стационарные и мобильные объекты различных типов: видеокамеры, датчики, универсальные средства коммуникации, средства хранения данных, контроллеры различных подсистем управления, средства обеспечения безопасности, средства оповещения и визуализации.

Сформулируем основные требования, предъявляемые к единой коммуникационной среде предприятия:

- наличие единого центра управления;
- открытая архитектура;
- возможность масштабирования и модернизации;
- обеспечение информационной безопасности и защиты информации;
- надежность работы, в том числе в случае кризисных ситуаций;
- простота развертывания и сопровождения;
- интеграция с имеющимися подсистемами управления и безопасности или их элементами;
- подключение стационарных и мобильных объектов;
- резервирование системы электропитания и всех основных элементов ИТ-инфраструктуры;
- возможность использования протоколов пакетной передачи данных IEEE 802.3 (Ethernet);
- обеспечение необходимой пропускной способности при передаче данных (в том числе поддержка передачи видео в высоком качестве с необходимого числа видеокамер);
- поддержку необходимого числа объектов и абонентов (с учетом будущего развития);
- необходимый охват территории предприятия системой беспроводного доступа (с учетом требования к резервированию);
- интерфейсы для выхода во внешние сети (Internet, телефонная сеть и др.);

- интерфейсы для подключения облачных сервисов и стыковки с внешними ЦОДами;
- экономическая эффективность.

При создании коммуникационной платформы предприятие имеет возможность:

1) использовать полностью или частично сеть и инфраструктуру оператора связи, предоставляющего услуги на данной территории (например, одного из сотовых операторов);

2) строить и развивать собственную систему связи в составе опорной проводной или оптоволоконной сети и систему беспроводного доступа.

В первом случае расходы на создание системы связи будут ниже. Операторы связи предлагают корпоративным заказчикам не только дешевые тарифы на телефонную связь и мобильный Internet, но и дополнительные услуги, такие как PTT-связь[1] для технологической голосовой связи или решения NB-IoT для подключения датчиков различных типов через сотовую инфраструктуру. Однако надежность работы операторской системы связи, особенно в случае кризисной ситуации, когда это особенно важно, невысокая. Ни один коммерческий оператор не может гарантировать немедленного предоставления необходимого сервиса (и голосовых вызовов и мобильного Internet) в 100% случаях. При работе через оператора также нужно предусмотреть регулярные платежи оператору связи за получаемый сервис.

Во втором случае расходы на создание собственной инфраструктуры будут выше, но при этом можно построит систему связи с заданным уровнем надежности, в том числе систему, удовлетворяющую требованиям, предъявляемым к критически-важной инфраструктуре (Mission critical). Можно заранее предусмотреть 100% надежную работу всех абонентов и подключенных устройств как в обычном режиме работы, так и в случае кризисной ситуации (природные или техногенные катастрофы, террористические атаки и т.д.). Такая модель коммуникационной среды предпочтительна для предприятий и организаций имеющих критически важную инфраструктуру.

Выбор коммуникационной модели зависит от специфики работы конкретной организации. Авторы рекомендуют строить и использовать собственную систему связи, что обеспечит более высокий уровень управления и безопасности.

Выбор беспроводной системы связи для использования в коммуникационной среде предприятия

На данный момент существует несколько протоколов (стандартов) беспроводной связи, использование которых позволит создать собственную беспроводную сеть с широкими возможностями, такими как передача живого видео в высоком качестве, высокая скорость передачи данных, поддержка подсистемы технологической голосовой связи и разнообразных ИТ-приложений. В качестве подходящих отметим стандарт LTE при условии строительства собственной частной сети - Private LTE [1], а также новый вариант сетей Wi-Fi – стандарт Wi-Fi 6 [2, 3]. Кроме того, протокол LoRa[2] [4] имеет ряд преимуществ при использовании в подсистемах мониторинга технологических процессов с подключением различных датчиков.

Отметим, что для работы сети LTE требуется разрешение на использование необходимых частотных диапазонов. Частотные диапазоны сетей LTE определены самим стандартом. В России сети LTE в основном строятся на диапазонах, принятых для Европы – 2100, 2300, 2600, 1800, 1900, 900 и 800 МГц. В ряде стран регулирующие организации предусмотрели наличие свободного частотного диапазона для развития сетей LTE, обслуживающих организации охраны общественной безопасности. В России пока таких «зарезервированных» для частных сетей LTE диапазонов нет. Имеющийся частотный ресурс распределен между крупными операторами.

Однако это не означает что строительство частных сетей LTE в России невозможно. Все крупные российские сотовые операторы предлагают заказчикам возможность построить частную LTE-сеть. При этом оператор предлагает подписать соглашение о работе сети на частотах, согласованных регулятором для работы данного оператора. Речь, правда, идет о развертывании частных LTE сетей в качестве сетей технологической связи в удаленных регионах, за пределами крупных городов – там, где у оператора нет своей коммерческой LTE сети, и частотный диапазон не используется.

Сеть LTE состоит из ядра системы (Core) и базовых станций. В отдельных случаях сотовые операторы предлагают заказчику купить собственные базовые станции LTE и подключить их к ядру системы, находящемуся у оператора. Такую систему нельзя на 100% считать частной, поскольку ее работа зависит от ядра, находящегося у оператора. В полностью независимой сети LTE и ядро сети, организующее слаженную работу всей системы и отвечающее за непрерывную и качественную связь, и базовые станции принадлежат заказчику и полностью им контролируются. Но учитывая высокую стоимость ядра затраты на такую сеть будут достаточно высокими.

Особенности беспроводной сети на базе технологии Private LTE:

- выделенная сеть, принадлежащая заказчику;
- возможность построить сеть уровня критически важной инфраструктуры с требуемыми параметрами по надежности, пропускной способности и качеству сервиса (QoS);
- широкополосная технология, обеспечивающая высокую скорость передачи данных (возможность передавать живое видео в высоком качестве). Пропускная способность до 3 Гбит/с;

[1] PTT (англ. Push-to-talk, дословно — «Нажми, чтобы говорить») — полудуплексный стандарт голосовой связи с двусторонним радиоинтерфейсом и возможностью передачи сигнала одновременно только в одном направлении. Для переключения между режимами приема и передачи пользователю необходимо нажимать/отпускать соответствующую кнопку (тангенту) на радиоустройстве.

[2] LoRa – это технология беспроводной передачи данных, в которой используется метод радиомодуляции, который может осуществляться приемопередатчиками Semtech LoRa. Этот протокол модуляции обеспечивает передачу небольших данных на большие расстояния, высокую устойчивость к помехам при минимальном потреблении энергии.

- требуется разрешение на использование радиочастот. В России получить разрешения у регулятора крайне сложно. Можно использовать необходимые частоты по договору с одним из четырех сотовых операторов, но только за пределами крупных городов;

- требуется строительство инфраструктуры, состоящей из ядра, необходимого числа базовых станций и каналов связи между ними. Стоимость оборудования при этом достаточно высокая;

- в качестве абонентских терминалов могут использоваться смартфоны и планшеты (в том числе защищенные) и специальные терминалы голосовой PTT связи (PoC);

- оборудование для сетей Private LTE предлагается несколькими компаниями (в том числе и российскими). Но их выбор ограничен.

Внедрение частных сетей Private LTE позволяет развернуть различные ИТ-приложения, такие как системы оповещения, безопасности, мониторинга и голосовой технологической связи, Industrial Internet of Things (IIoT), а также обеспечить интеграцию со SCADA, MES, ERP системами. Таким образом частные сети LTE позволяют получить комплексное решение, соответствующее требованиям Industry 4.0.

Другим протоколом, позволяющим построить комплексное решение, является протокол Wi-Fi 6 (стандарт IEEE 802.11ax). Стандарт Wi-Fi существует много лет, но продолжает развиваться. Новый вариант стандарта – Wi-Fi 6 позволяет на тех же частотных диапазонах, открытых для использования в России (2,4 и 5 ГГц), значительно увеличить скорость передачи данных и число поддерживаемых абонентских устройств. На базе сети Wi-Fi 6 можно построить решения Internet вещей (IoT), системы видеонаблюдения, голосовой связи, оповещения, мониторинга и др. Протокол Wi-Fi 6 утвержден в России в качестве стандарта. Уже появилось оборудование для создания сетей Wi-Fi 6 отечественного производства. Для создания сети Wi-Fi не требуется получать разрешение на частоты. Стоимость точек доступа (Access Points) Wi-Fi 6 относительно невысокая.

Особенности беспроводной сети на базе технологии Wi-Fi 6 (IEEE 802.11 ax):

- собственная сеть, принадлежащая заказчику;

- позволяет построит сеть уровня критически важной инфраструктуры с требуемыми параметрами по надежности и качеству сервиса (QoS);

- широкополосная технология, обеспечивающая высокую скорость передачи данных (возможность передавать живое видео в высоком качестве). Пропускная способность до 9,6 Гбит/с;

- не требуется разрешение на использование радиочастот. Используются открытые для использования в России диапазоны 2,4 МГц и 5 МГц;

- инфраструктура сети Wi-Fi 6 состоит из точек доступа и каналов связи между ними;

- в качестве абонентских терминалов могут использоваться смартфоны и планшеты (в том числе защищенные) и специальные терминалы голосовой PTT связи (PoC[3]);

- стандарт Wi-Fi 6 – IEEE 802.11 ax принят в России;

- использование протокола Wi-Fi 6 обеспечивает большую устойчивость к внешним помехам, подключение большого числа абонентов на ограниченной территории, высокие скорости передачи данных, «бесшовность» сети (переход мобильного абонента от одной точки доступа к другой без прерывания связи);

- обеспечивается обратная совместимость - возможность использовать устройства с более ранними версиями Wi-Fi (IEEE 802.11);

- поддержка разнообразных ИТ-приложений и голосовой связи VoIP (PoC);

- использование системы управления сетью (Network Management System – NMS) в сети Wi-Fi 6 позволит оптимизировать нагрузку на отдельные точки доступа, оптимально настроить их мощность и таким образом повысить надежность и пропускную способность сети в целом.

При оценке стоимости сети на базе решения Private LTE или протокола Wi-Fi 6 нужно учитывать стоимость создания опорной сети для подключения базовых станций или точек доступа. Необходимую скорость передачи данных в с системе Wi-Fi 6 можно получить, если абонент находится на расстоянии 200...400 м от точки доступа. Для покрытия значительной территории при использовании Wi-Fi 6 может потребоваться установить несколько десятков или даже сотен точек доступа, которые должны быть подключены к опорной сети (на базе оптического волокна или с помощью транспортных сетей (Backhaul) по радиоканалу). Стоимость создания такой опорной сети может значительно превосходит стоимость самих точек доступа и повлияет на общую стоимость системы.

Дальность связи в случае использования Private LTE зависит от используемого диапазона, рельефа, наличия препятствий, типа антенн, высоты их подвеса и других факторов. Наиболее выгодным с точки зрения дальности является диапазон 450 МГц (B31), однако возможности получения этого диапазона для сетей Private LTE очень ограничены. Более доступными для получения разрешений на развертывание Private LTE являются диапазоны B38 и B40 (2,3...2,4 ГГц), но дальность связи в этом случае будет значительно меньше. Даже в случае применения специальных направленных антенн с высотой подвеса 15...20 м дальность связи Private LTE B38 или B40 может быть не более 1,5...2 км. Но и такие параметры позволяют построить сеть с необходимым покрытием достаточно большой территории, используя три - четыре базовых станции Private LTE. При этом потребуется значительно меньше вложений в создание опорной сети для подключения базовых станций. Таким образом сложно сделать однозначный вывод относительно того, какая из предложенных технологий будет дешевле. Точные оценки стоимости обоих решений и их сравнение можно сделать, проведя расчеты радиопокрытия применительно к конкретному объекту и учитывая конкретные требования к беспроводной сети.

Выбор, какую из технологий использовать – Wi-Fi 6 или Private LTE, можно сделать исходя из требований

[1] PoC (Power over Coax) - новая система питания, которая может подавать энергию на аналоговые системы через коаксиальный кабель без какого-либо другого источника питания.

к конкретной системе и имеющихся ограничений (бюджет, возможность использовать лицензируемые частоты для сети Private LTE и др.). В определенных случаях возможно использование двух технологий – Private LTE и Wi-Fi 6 в одной сети.

Надежность работы системы связи зависит от надежной работы ее компонентов. В связи с этим рекомендуется предусмотреть резервирование всех основных элементов сети. Все элементы инфраструктуры рекомендуется обеспечить основным и резервным электропитанием. Расположение точек доступа Wi-Fi 6 или базовых станций Private LTE должно обеспечивать двойное резервирование по покрытию на всей территории предприятия.

Подсистемы голосовой технологической связи

Отдельно остановимся на системах голосовой технологической связи, которые существуют на многих промышленных предприятиях уже много лет и позволяют эффективно управлять персоналом и повышать уровень безопасности. В последние годы широкое распространение получили цифровые стандарты радиосвязи, такие как Tetra или DMR. Однако традиционные системы радиосвязи, даже построенные на цифровых протоколах, сложно интегрировать в общую ИТ-инфраструктуру предприятия. Появление новых решений в области голосовой связи, например технологии PoC (Push-To-Talk Over Cellular), с возможностью подключения абонентов через сети 3G/LTE или Wi-Fi дает возможность интеграции системы голосовой технологической связи в общую инфраструктуру предприятия.

Среди функций системы голосовой технологической связи на базе технологии PoC отметим:

- быстрый PTT-вызов – не нужно набирать номер и ждать когда абонент ответит на звонок;
- групповой, индивидуальный, экстренный вызовы – одним нажатием PTT вызываются все абоненты группы;
- возможность позиционирования абонентов как вне, так и внутри помещения;
- дополнительные функции, основанные на скоростной передаче данных, включая передачу фото и видео в высоком качестве, а также передачу файлов;
- функции диспетчерского приложения по работе с отдельными абонентами и с группами абонентов;
- возможность записи всех переговоров и других событий в системе;
- интеграция с традиционными системами радиосвязи и телефонными сетями с помощью специальных шлюзов.

Современные системы голосовой связи, построенные на технологии PoC, отличаются:

- простотой и высокой скоростью развертывания;
- наличием специальных функций безопасности и защиты от несанкционированного подключения;
- возможностью интеграции с другими ИТ-решениями и существующими системами радиосвязи;
- большим выбором абонентских терминалов и аксессуаров к ним;
- значительной зоной покрытия (в случае работы через операторские сети);
- возможностью построить систему класса mission critical при работе через сети Private LTE или Wi-Fi 6.

Абонентские терминалы в системах управления и обеспечения безопасности

Современные цифровые решения позволяют реализовывать программно-аппаратные решения уровня «мобильный сотрудник», предоставляющие возможность не только оперативно получать и передавать всю необходимую информацию сотруднику, но и сохранять при этом его мобильность. Создание таких решений стало возможным с развитием беспроводных систем связи и появлением различных абонентских устройств. Так современные смартфон или планшет являются универсальными средствами коммуникации, позволяющими кроме голосовых вызовов передавать фото или видео и работать с разнообразными ИТ-приложениями.

Для использования в системах управления и безопасности предприятия следует ориентироваться на использование специальных (промышленных) смартфонов и планшетов, которые имеют повышенные характеристики по защищенности, прочности и надежности, батареи повышенной емкости и специальную кнопку «PTT» для выполнения функций голосовой технологической связи – PoC (Push-To-Talk Over Cellular), аналогичных функциям традиционных систем профессиональной радиосвязи.

На рынке в настоящее время предлагается большое число абонентских терминалов PoC различных типов. Общим является возможность работы через сотовые сети 3G/LTE, что требует установки внутри терминала SIM-карты, или работа без SIM-карты при использовании сети Wi-Fi.

Большинство PoC терминалов имеют специальную кнопку PTT (Push-To-Talk), одним нажатием которой обеспечивается быстрый вызов другого абонента или сразу группы абонентов (групповой вызов). Иногда в качестве PoC терминала используют и обычный смартфон, не имеющий физической кнопки PTT. При этом используется «виртуальная кнопка», появляющаяся на экране смартфона. Такой способ PPT связи возможен, но не рекомендуется по причине того, что в этом случае невозможно обеспечить быстрый вызов одним нажатием. Для нажатия на «виртуальную кнопку» на экране требуется вывести смартфон из спящего состояния, разблокировать его (введя PIN-код), вывести на экран необходимое приложение (с «виртуальной кнопкой») и только после этого нажать на нее. Наличие физической кнопки PTT позволяет обеспечить вызов действительно одним нажатием, как это происходит в системах радиосвязи.

Как и в системах радиосвязи, в PoC системах могут работать носимые абонентские терминалы и мобильные терминалы (предназначенные для установки на транспортном средстве). Носимые терминалы PoC представлены в виде смартфонов или планшетов, имеющих специальную кнопку PTT и терминалов, внешне похожих на радиостанции систем профессиональной мобильной радиосвязи (ПМР). PoC терминалы «типа радиостанция» предназначены для работы сотрудников, которым не нужны никакие другие возможности кроме голосовых вызовов различных типов. Использование смартфонов и планшетов в качестве PoC терминалов позволяет абоненту работать не только в PoC системе

но и пользоваться смартфоном как обычным сотовым телефоном или использовать другие ИТ-приложения. Таким образом, смартфоны и планшеты могут быть универсальным средством коммуникации, имеющим возможности PoC и другие функции.

Для работы в сложных условиях эксплуатации требуются абонентские устройства с повышенными характеристиками по прочности и защищенности, в частности, имеющие повышенную защиту от пыли и влаги (индекс IP) и ударопрочные корпус и экран, соответствующие требованиям военного стандарта MIL810.

Надежность работы абонентских терминалов определяется не только прочностью корпуса. В профессиональных абонентских устройствах обычно используются аккумуляторы большей мощности, предусмотрена возможность замены батареи и зарядки в настольном зарядном устройстве (типа «стакан»), что не требует постоянного использования USB-C или Micro-USB разъема, а также использование с терминалом различных аксессуаров – наушников, гарнитур, выносных микрофонов (в том числе с кнопкой PTT). Большинство PoC терминалов типа «радиостанция» позволяют использовать соответствующие аксессуары от радиостанций ПМР.

Важной особенностью профессиональных абонентских устройств является громкость внешнего динамика. Большинство обычных смартфонов имеет внешний динамик, но громкость его работы значительно меньше, чем у радиостанций систем ПМР, и недостаточна для нормальной работы в PoC системах даже при невысоком уровне внешних шумов. Специальные смартфоны, имеющие кнопку PTT, комплектуются динамиком повышенной мощности.

Для работы на объектах с повышенным риском взрыва или пожара предлагаются специальные PoC смартфоны и планшеты, соответствующие требованиям стандарта ATEX (взрывозащита в пылевых или газовых средах).

Большинство из предлагаемых PoC терминалов работают под управлением распространенных операционных систем для мобильных устройств. Чаще всего это Android, но есть и PoC смартфоны и планшеты, работающие под управлением российской ОС для мобильных устройств – Аврора. Возможность использования смартфонов и планшетов отечественного производства с ОС Аврора (доверенная среда) особенно важно для государственных организаций и предприятий с высокими требованиями по информационной безопасности.

Некоторые PoC терминалы «типа радиостанция» работают под управлением ОС Linux. Использование Linux в PoC терминалах может дать преимущество по скорости соединения, поскольку в этом случае ОС не выполняет никаких других задач, кроме выполнения PoC вызовов. Однако разработка PoC- приложений для Linux может оказаться сложнее, чем аналогичная разработка для Android.

При выборе абонентского терминала кроме его функциональности и параметров надежности следует ориентироваться на использование более поздних версии Android и чип-сетов новых поколений.

Информационная безопасность и защита информации

Требования к информационной безопасности повышаются не только в организациях охраны общественной безопасности и государственных структурах, но и в коммерческих компаниях. Защита персональных данных и коммерческой информации становится все более важной задачей. С целью обеспечения информационной безопасности следует предусмотреть выполнение следующих принципов:

- использование собственной ИТ-инфраструктуры предприятия;
- использование собственных протоколов обмена данными;
- применение средства шифрования и криптографии (при необходимости);
- использование программного обеспечения и аппаратных средств отечественного производства;
- внедрение специальных средства идентификации абонентов для исключения возможности создания «двойников» и реализации несанкционированного подключения;
- наличие специальных средств работы администратора системы, например, приложения для мониторинга ИТ-инфраструктуры, обеспечивающие оперативный контроль над работой системы.

Комплексная система управления и безопасности от компании Триалинк

Рассмотрим комплексную систему управления и безопасности, построенную на базе цифровых решений от компании Триалинк. В качестве универсальной платформы, позволяющей интегрировать различные ИТ продукты используется программно-аппаратный комплекс «МАРС МОНИТОРИНГ». Система имеет открытую архитектуру, поддерживает большинство существующих интерфейсов и протоколов передачи данных и имеет возможности расширения списка поддерживаемых интерфейсов с помощью специальных плат расширения. Система позволяет подключать проводные и беспроводные датчики различного назначения, осуществлять сбор телеметрической информации с датчиков, выполнять фото- или видеофиксацию произошедших событий. Таким образом «МАРС МОНИТОРИНГ» позволяет создавать единую информационную среду предприятия и управлять ею.

Использование технологии LoRa для подключения беспроводных датчиков позволяет значительно сократить затраты на установку и обслуживание датчиков и повысить надежность их работы. Собственный протокол обмена данными с беспроводными датчиками повышает защищенность системы «МАРС МОНИТОРИНГ». Использование в составе системы «МАРС МОНИТОРИНГ» базовых станций MARS CASA, также разработанных компанией Триалинк, позволяет построить собственную LoRa сеть для сбора и обработки телеметрической и видеоинформации.

Открытая архитектура системы «МАРС МОНИТОРИНГ» позволяет интегрировать с ней системы видеонаблюдения, системы управления (ERP, SCADA) от других производителей, а также систему технологической голосовой связи RONET (технология PoC) и систему оповещения и громкоговорящей связи «МАРС АРСЕНАЛ» производства компании Триалинк.

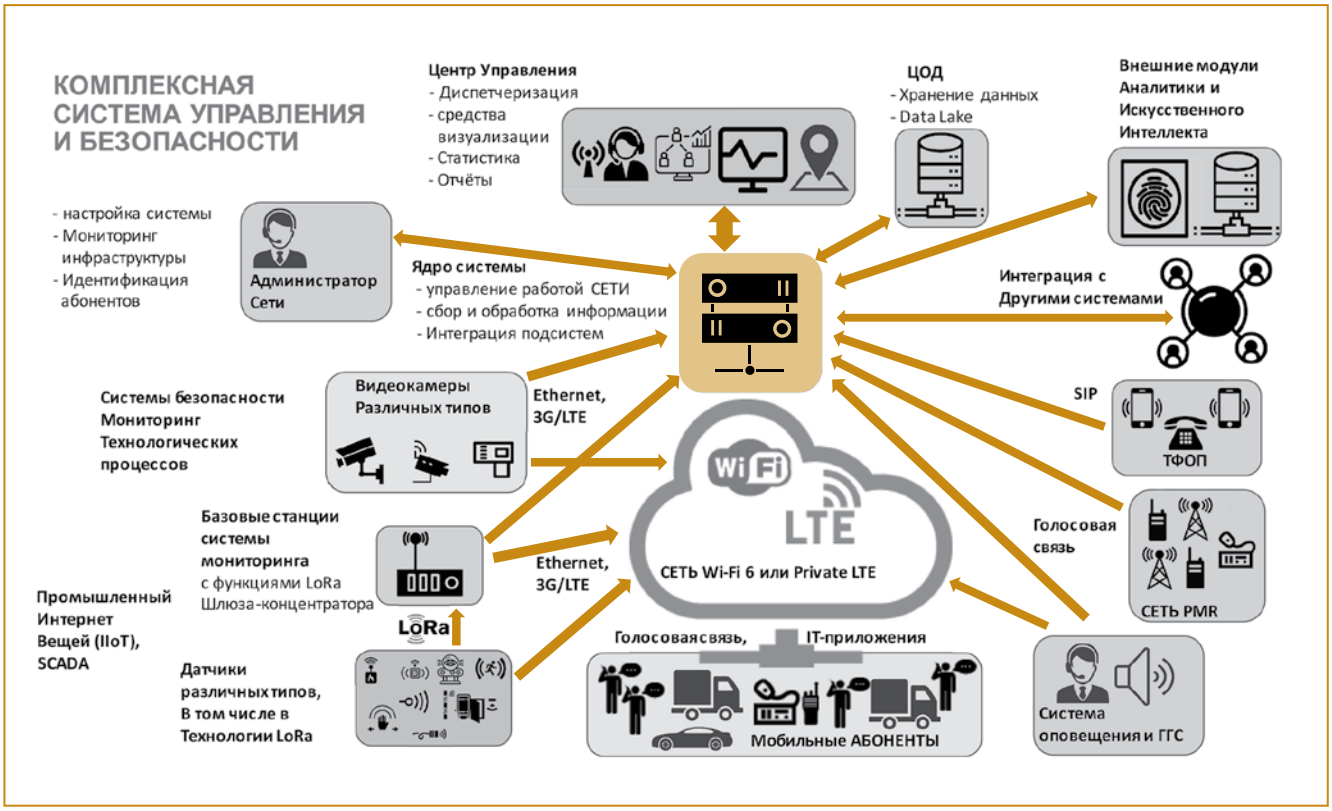

Схема комплексного решения для управления и безопасности на базе платформы «МАРС МОНИТОРИНГ»

В качестве коммуникационной сети для работы системы «МАРС МРНИТОРИНГ» предлагается использовать беспроводную сеть стандарта Wi-Fi 6 или частную сеть Private LTE. Выбор одного из указанных стандартов производится с учетом особенностей работы и потребностей конкретного заказчика.

Схема комплексного решения для управления и безопасности на базе платформы «МАРС МОНИТОРИНГ» показана на рисунке.

Система построена на оборудовании и ПО отечественного производства, включая абонентские терминалы, работающие под управлением ОС Аврора.

«МАРС МОНИТОРИНГ» может выполнять функции сбора информации различного типа и входить в комплексное решение более высокого уровня, такое как система «Умный город».

Выводы

Цифровая трансформация и переход на решения Industry 4.0 проходит успешно при условии правильного планирования и обоснованного выбора технических средств и современных решений. При этом для обеспечения высокого уровня надежности работы системы рекомендуется создание собственной беспроводной системы связи с использованием стандартных протоколов передачи данных Private LTE или Wi-Fi 6 (IEEE 802.11 ax) и технических решений отечественного производства. Такие системы могут удовлетворять требованиям, предъявляемым к критически важной инфраструктуре, при обеспечении необходимого резервирования основных элементов системы и планирования ее функций в условиях экстренной ситуации.

Компания Триалинк, имеющая многолетний опыт работы в области внедрения ИТ-решений, основанных на использовании протоколов пакетной передачи данных (IEEE 802.3 – Ethernet), интеграции ИТ-систем различных типов и сложности, а также опыт в разработке и поставе собственных ИТ-решений, предлагает систему «МАРС МОНИТОРИНГ» в качестве универсальной платформы для интеграции различных подсистем и решений предприятий в комплексную систему управления и безопасности, удовлетворяющую требованиям Industry 4.0.

Список литературы

1. Корпоративные сети Private LTE/5G-Ready в России: география и отраслевая принадлежность предприятий// COMNews.ru. 2021. май.
2. Пять причин перейти на Wi-Fi 6 // hi-tech.mail.ru. 2020. Декабрь.
3. *Gold J.* FAQ: What you need to know about 802.11ax, the next big Wi-Fi standard // Network World. 2016. March.
4. *Верхулевский К.* Технология LoRa в вопросах и ответах // Беспроводные технологии. 2016. №1.

Трифонов Евгений Валентинович *– директор по продажам,*
Шмурьев Алексей Наримановичч *– генеральный директор компании Триалинк.*
Контактный телефон 7(495)232-11-32.
E-Mail: info@trialink.ru, e.trifonov@trialink.ru