информационно-деловой

ВЕСТНИК ОАО ЦНПО «КАСКАД»

Качество - достойное Державы!

www.kaskad.ru vestnik@kaskad.ru Ежемесячное издание Август 2007 № 8 (31)

Сегодня и завтра Ярославского филиала

Проблемы и перспективы

Филиал

В.В. Титов принял участие в заседании президиума Совета главных конструкторов информатизации регионов Российской Федерации

Новости

Командно-технологическая двусторонняя радиотелефонная связь для ТЭЦ «Луч»

Технологии

Можно ли обмануть сканер?

Продолжение обзора систем биометрии экспертом Объединения

Рынок

Филиал

Сегодня и завтра Ярославского филиала

Сегодня в СМИ все чаще звучат такие географические названия, как Лехтуси, Армавир, Габала; к этим небольшим населенным пунктам приковано внимание руководителей государств, дипломатов, журналистов. Работы на объектах, находящихся в центре внимания общественности, выполняли и выполняют сотрудники Ярославского филиала ОАО ЦНПО «Каскад»

Филиал возродился в новом качестве 23 мая 2002 года. Предшественником его было монтажно-технологическое управление «Омега», ранее входившее в Объединение — ЦНПО «Каскад».

Выполняя государственный заказ

Сегодня это — крепко стоящее на ногах предприятие с большими объемами работ, в том числе по восстановлению систем связи и аппаратуры передачи данных на территории России, а также в странах ближнего зарубежья: Украине, Таджикистане, Азербайджане, Республике Беларусь.Филиал участвовал в ремонте и модернизации телеметрической аппаратуры, обеспечивающей съем информации со спутников и ее передачу в систему управления. Одним из направлений работы филиала является оперативное сервисное и техническое обслуживание изделий, которые уже долгое время находятся в эксплуатации. Организовано телефонное консультирование заказчика.

«Наши специалисты, — говорит директор филиала Евгений Колесников, — принимают участие в работах завершающей стадии монтажа новой РЛС высокой заводской готовности на северо-западе России, в населенном пункте Лехтуси под Санкт-Петербургом, и на аналогичной РЛС в Армавире. (Подробнее см. «Вестник» № 5, 2007. — Прим. ред.) Специалисты филиала активно участвуют на всех стадиях работ в рамках выполнения государственного заказа. Эти работы выполняются в тесной кооперации с Белгородским, Мирнинским и Знаменским филиалами».

Одной из стратегических задач, стоящих перед филиалом, стало расширение присутствия на гражданском рынке, хотя конкуренция в регионе в сфере услуг, предлагаемых предприятием, очень высокая. Однако и на этом направлении умелый менеджмент руководства филиала позволяет оставаться в лидерах. Так, конкурентными преимуществами филиала являются разумная ценовая политика и высокий профессиональный уровень специалистов. То есть оптимальное соотношение «цена – качество». Известно, что технические решения, используемые на военных объектах, отличает высокая надежность и относительная простота в обслуживании. Гражданские заказчики эти факторы ценят. В настоящее время активно ведутся переговоры о заказе на выполнение проектно-монтажных работ на объектах города и области. О ходе этих работ «Вестник» проинформирует своих читателей в одном из ближайших номеров.

Молодое пополнение

Одной из важнейших задач, стоящих сегодня перед филиалом, стала задача обеспечения молодыми кадрами. Объекты, на которых работают специалисты филиала, расположены на всей территории России и стран СНГ. Это обуславливает специфику производства работ: постоянные разъезды, проживание на военных объектах, полевые условия. Не каждый может выдержать такие жесткие, спартанские условия работы и жизни. Но вместе с тем немного найдется предприятий, где молодому специалисту предоставляется

продолжение на стр. 2

Новости

Президент РФ посетил РЛС в Лехтуси

11 августа Владимир Путин осуществил рабочую поездку в Ленинградскую область и осмотрел новейшую радиолокационную станцию «Воронеж» в поселке Лехтуси

РЛС в Лехтуси была открыта 22 декабря прошлого года. Ряд работ на объекте осуществлялся специалистами ОАО ЦНПО «Каскад». Новая станция может использоваться не только как элемент системы предупреждения о ракетном нападении, но и как система противоракетной и противовоздушной обороны. «Воронеж» сейчас функционирует в режиме опытно-боевого дежурства. В соответствии с планами строительства Космических войск подобная РЛС создается также в районе города Армавир в Краснодарском крае. Подробнее о работах проводимых ОАО ЦНПО «Каскад» на этом объекте см. «Вестник» № 5, 2007 г.

Новости

ИАС ПИК проходит испытания на прочность вместе с «Булавой»

По результатам проведенного в конце июня успешного испытания новейшей российской баллистической ракеты «Булава-М» принято решение о начале ее серийного производства, о чем недавно сообщил прессе главком ВМФ адмирал флота Владимир Масорин

Полностью испытания планируется завершить в 2008 году, на текущий год запланировано еще 2 испытательных пуска. Во всех испытаниях ракет класса «Булава» принимала непосредственное участие ИАС ПИК ВМФ РФ (ОКР «Палтус»), разработанная специалистами ОАО ЦНПО «Каскад». С ее помощью производились измерения и передавалась телеметрическая информация. Таким образом, испытательные пуски «Булавы» стали серьезным испытанием и для продукции Объединения. И этот экзамен выдержан. По отзывам военных, оборудование работало отлично. Подробнее о системе см № 6 и10 за 2005 г. и № 7, 2007 г.

Филиал

Сегодня и завтра Ярославского филиала

начало на стр. 1

возможность для столь стремительного карьерного роста, как в Ярославском филиале ОАО ЦНПО «Каскад». Одним из гражданских объектов филиала стало ПТУ № 7, где готовят монтажников. В настоящее время подписан договор на оборудование учебных рабочих мест необходимой аппаратурой и контрольно-измерительными приборами. Руководство филиала полно оптимизма и уверенности, что перспективы на будущие работы весьма обнадеживающие. Дело в том, что ОАО ЦНПО «Каскад» вновь подтвердило свой статус предприятия, пользующегося высоким доверием заказчика. Объединением выиграны конкурсы на проведение работ в интересах Космических войск Российской Федерации. Подписаны контракты на выполнение ремонтно-восстановительных работ и монтажно-наладочных работ стартовых и технических комплексов космодрома Плесецк. Опыт и мощности филиала востребованы не только структурами Минобороны. Обустройство границы, таможенных пунктов, различные гражданские объекты — это лишь часть работ Ярославского филиала ОАО ЦНПО «Каскад». Филиал приложит все усилия для выполнения обозначенных работ в намеченные сроки и с неизменным качеством, которому привыкли доверять заказчики на протяжении многих лет.

Специалисты ОАО ЦНПО «Каскад» ведут монтаж оборудования на объекте

РЛС типа «Воронеж», на которой ведутся работы силами филиала

Бригада сотрудников ОАО ЦНПО «Каскад», осуществлявшая работы на объекте заказчика

Новости

В.В. Титов принял участие в заседании президиума Совета главных конструкторов информатизации регионов Российской Федерации

25–27 июля 2007 г. в соответствии с планом работы Совета главных конструкторов информатизации регионов Российской Федерации (СГК) и по приглашению администрации Иркутской области в г. Иркутске состоялось заседание президиума Совета главных конструкторов информатизации регионов Российской Федерации

Всего в заседании приняли участие 72 человека, а также более 20 представителей СМИ. Были рассмотрены вопросы формирования инфраструктуры для дистанционного оказания государственных услуг, принципы организации информационного взаимодействия федеральных органов исполнительной власти, органов власти регионов Российской Федерации и органов местного самоуправления в целях оказания государственных услуг в регионах.

В заседании президиума Совета главных конструкторов приняли участие представители Минэкономразвития России, Росинформтехнологии, администрации Иркутской области, исполнительного секретариата Конгресса муниципальных образований Российской Федерации, межрегиональных ассоциаций «Сибирское соглашение» и «Центрально-Черноземная», Гильдии отечественных специалистов по государственному и муниципальному заказам, ряда субъектов Российской Федерации, а также представители организаций и предприятий, работающих в сфере разработки и применения информационных технологий. Генеральный директор ОАО ЦНПО «Каскад» Валентин Васильевич Титов принял участие в заседании как руководитель предприятия — крупного системного интегратора, имеющего опыт по созданию и эксплуатации систем управления. На заседании большое внимание было уделено вопросам создания и эксплуатации удостоверяющих центров для предоставления государственных услуг на основе сервисоориентированной доверенной третьей стороны.

Напомним, что конкурс на выполнение работ по созданию автоматизированной системы «Корпоративная информационно-вычислительная сеть администрации Иркутской области» (КИВС) ОАО ЦНПО «Каскад» выиграло еще в прошлом году. Это еще раз доказало стабильную конкурентоспособность Объединения на гражданском рынке информационных технологий.

Автоматизированная система КИВС предназначена для создания интегрированной телекоммуникационной среды администрации Иркутской области на основе волоконно-оптических, проводных и беспроводных каналов связи. Она создается для повышения скорости и качества принятия управленческих решений и контроля их исполнения; формирования и защиты корпоративных информационных ресурсов от несанкционированного доступа; объединения локальных вычислительных сетей (ЛВС) подразделений администрации губернатора Иркутской области, органов исполнительной власти Иркутской области в единую корпоративную информационно-вычислительную систему. Кроме того, создание системы позволит обеспечить подразделения администрации губернатора и органов исполнительной власти доступом в Интернет и высококачественной телефонной связью.

Технологии

Командно-технологическая двусторонняя радиотелефонная связь для ТЭЦ «Луч»

В современных условиях на крупных промышленных объектах, где требуется координация действий сотрудников на больших площадях, невозможно обойтись без командно-технологической двустороней радиотелефонной связи, предназначеной для оперативного, технологического и административного персонала. Одна из таких систем создана специалистами ОАО ЦНПО «Каскад» для объекта РАО «ЕЭС России» — ГТУ-ТЭЦ «Луч» (г. Белгород)

Выбор для командно-технологической двусторонней радиотелефонной связи аппаратуры, использующей принципы связи стандарта DECT, для белгородской ТЭЦ «Луч» был обусловлен такими преимуществами систем DECT, как:

- высокое качество связи,
- возможность создания широкого круга систем — от домашних беспроводных телефонов до многоступенчатых микросотовых корпоративных сетей,
- совместимость оборудования разных производителей (DECT GAP),
- устойчивость к радиопомехам,
- конфиденциальность связи,
- безопасность для здоровья.

Состав системы:

- DECT-контроллер,
- комплект базовых станций,
- комплект антенн,
- комплект радиотрубок носимых,
- устройства резервного питания.

DECT является стандартом высококачественного цифрового радиодоступа в существующие телекоммуникационные сети. При этом обеспечивается органическое взаимодействие с уже существующими сетями связи и поддерживается большое разнообразие приложений и услуг. Технологию DECT называют микросотовой системой связи. Как и многие сотовые системы связи, DECT содержит базовые станции и мобильные терминалы. В зависимости от приложений, количество базовых станций меняется от одной до нескольких сотен. В отличие от традиционных сотовых систем, в DECT размер соты ограничен сотнями метров. Это объясняется тем, что излучаемая мощность в DECT-системе составляет только 10 мВт на канал. Такая микросотовая архитектура системы с эффективным механизмом повторного использования частот позволяет поддерживать огромный трафик на единицу площади. Из-за малой излучаемой мощности система DECT является единственной системой связи, разрешенной Европейской комиссией для применения на предприятиях, где влияние электромагнитных помех на оборудование может привести к непредвиденным последствиям.

Для работы оборудования в стандарте DECT в Европе и в России выделен диапазон частот 1880–1900 МГц. Этот частотный диапазон шириной 20 МГц разделен на 10 частотных полос с центральными частотами несущих Fn = 1897,344 МГц - n·1728 кГц. На каждой частоте организованы временные циклы длительностью 10 мс. Каждый цикл содержит 24 временных интервала, предназначенных для передачи информации от/к базовой станции со скоростью полезной информации 32 кбит/с, например речи с кодированием ADPCM по стандарту G.726. Первые 12 временных интервала используются для передачи от базовой станции (downlink), а следующие 12 временных интервала — для передачи к базовой станции (uplink).

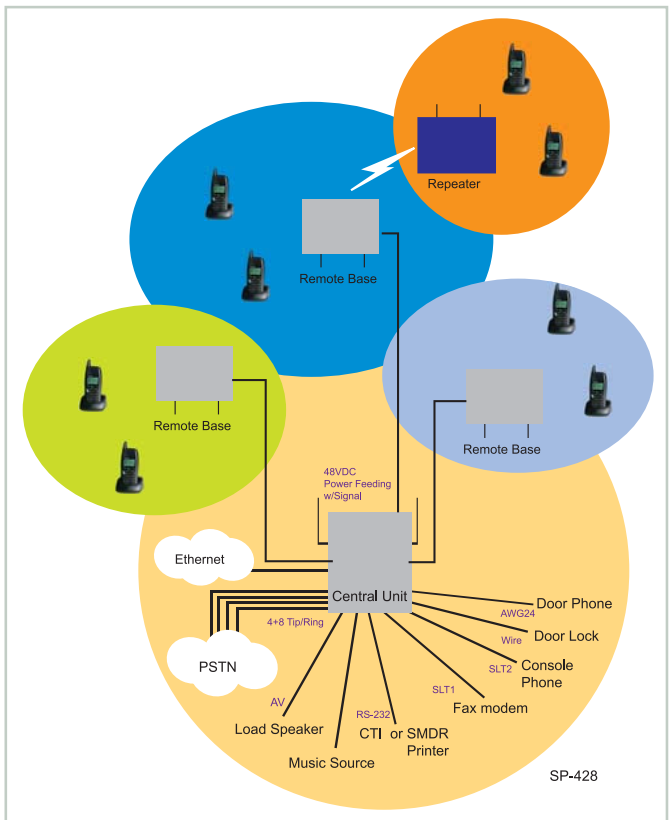
Структура радиоинтерфейса DECT

В терминологии DECT базовая станция называется RFP — Radio

Технологии

Командно-технологическая двусторонняя радиотелефонная связь для ТЭЦ «Луч»

начало на стр. 2



Приципиальная схема системы DECT-связи

Fixed Part. Каждая базовая станция в каждый момент времени может излучать только на одной частоте. Таким образом, базовая станция одновременно поддерживает не более 12 дуплексных каналов. При необходимости организации большего количества одновременных каналов несколько базовых станций (вплоть до 10 для организации до 120 одновременных каналов) могут объединяться в кластеры базовых станций. Иногда кластер называют базовой DECT-станцией (DECT Base Station — DBS). Для борьбы с замираниями используется механизм разнесенного приема. Суть этого метода заключается в том, что на каждой базовой станции имеется 2 антенны, разнесенные в пространстве, причем при работе с каждым каналом используется только одна из них. При возникновении замирания, т. е. резкого ухудшения качества приема из-за интерференции отраженных волн, происходит переключение антенн на базовой станции для этого канала. Управление переключением антенн, как и выбор рабочего канала, происходит под управлением мобильного терминала.

Таким образом, стандарт DECT обеспечивает до 120 одновременных дуплексных речевых каналов. Благодаря высокой помехоустойчивости от соседних базовых станций (отношение C/I = 10 дБ, где C — сигнал, I — интерференция) обеспечивается очень высокая емкость системы. Теоретические вычисления дают около 10 000 Эрл/км^2 (исходя из предположения, что базовые станции располагаются в узлах идеальной гексагональной решетки с радиусом 25 м). Все это достигается без необходимости частотного планирования. Отсутствие частотного планирования обеспечивается механизмом непрерывного динамического выбора и распределения каналов (CDCS/CDCA). Суть этого механизма заключается в том, что для установления каналы выбираются динамически из всего набора каналов по критерию отсутствия помех и качества прохождения сигнала. Причем канал не закрепляется за соединением на все время, а может меняться в активном соединении. Это происходит следующим образом. FP DECT непрерывно сканирует все 120 принимаемых каналов и измеряет силу принятого сигнала (RSSI — Received Signal Strength Indicator) для выбора канала с наименьшим уровнем (свободный канал без помех). В этом канале базовая станция излучает так называемый beacon-сигнал, который в числе прочих содержит информацию:

- для синхронизации PP,
- об идентификаторе системы,
- о возможностях системы,
- о свободных каналах,
- пейджинговую информацию.

Синхросигналы служат для синхронизации задающего генератора, цикловой и сверхцикловой синхронизации PP. Идентификатор системы позволяет PP определить «свою» FP из множества FP в эфире. Информация о возможностях системы предназначена для сообщения PP об услугах, которые поддерживаются данной системой. Информация о свободных каналах предназначена для сообщения PP о наличии свободных каналов в данной FP. В пейджинговой информации передаются сообщения о поступлении входящих вызовов. Анализируя информацию в beacon-канале, PP находит свою FP и «цепляется» к ней. При выходе из зоны действия текущей FP происходит поиск следующей. Таким образом, PP всегда «зацеплена» за ту или иную FP своей или дружественной системы.

После этого PP начинает непрерывно сканировать все свои 120 приемных канала и измеряет силу сигнала в каждом из них. Номера каналов с наименьшим RSSI заносятся в память. Одновременно в памяти находятся не менее двух таких каналов. При необходимости организации исходящей связи PP связывается с текущей FP и предлагает установить связь в одном из свободных (с точки зрения PP) каналов. Если этот канал отвергается FP, то PP предлагает следующий из списка свободных каналов. После согласия FP на установление соединения по одному из каналов, по этому каналу происходит обмен сигнализационной и другой служебной информацией, например запрос на установление исходящей связи и, после установления соединения, передачу речи.

Организация входящей связи происходит аналогичным образом. PP непрерывно анализирует пейджинговое сообщение на наличие входящих вызовов. После распознавания входящего вызова, PP посылает запрос на установление связи в одном из свободных каналов. Как видим, выбор канала для установления соединения происходит динамически и только по инициативе и под управлением PP. Этот механизм называется непрерывным динамическим выбором канала (CDCS). Активный канал, т. е. тот, в котором происходит разговор, не является постоянно выделенным на все время соединения. По тем или иным причинам, например при ухудшении качества сигнала в текущем канале, PP может сменить текущий канал на новый. При этом PP выбирает свободный канал из своего списка свободных каналов и предлагает FP перейти на него. При согласии FP происходит переход на этот новый канал. Переход на новый канал может происходить и по инициативе FP. При этом FP о своем желании перейти на новый канал сообщает PP, и далее все происходит, как описано выше, т. е. окончательный выбор нового канала осуществляется PP.

Если новый канал запрашивается у текущей FP, то такой переход называется intercell handover, а если у другой FP — то intracell handover. Этот механизм называется непрерывным динамическим распределением каналов (CDCA).

Хендовер в DECT-системе происходит «мягким» способом. Это значит, что во время хендовера между PP и системой одновременно существует два канала: текущий и новый. В какой-то момент времени информация между PP и системой передается одновременно по обоим каналам. Только после успешного перехода на новый канал происходит деактивация старого канала. Надо отметить, что хендовер начинается не только при ухудшении качества связи или при разрыве соединения, но и когда PP находит лучший с его точки зрения канал, т. е. для соединения всегда используется наилучший свободный канал. Механизм CDCS/CDCA существенно отличает DECT от сотовых систем связи, где управление каналами полностью осуществляется базовыми станциями под управлением контроллера. В технологии DECT центральный контроллер системы освобожден от работы, требующей большой вычислительной мощности, особенно в условиях высокого трафика.

Уникальная возможность технологии DECT по динамическому выбору и распределению каналов гарантирует, что всегда используется только наилучший канал. Эта способность DECT позволяет сосуществовать нескольким системам в одной и той же полосе частот, при этом обеспечивается высококачественная и безопасная связь. Кроме того, этот механизм существенно увеличивает емкость трафика в системе за счет минимизации каналов с несколькими путями распространения, в особенности это важно для офисных приложений, где существует большое количество переотражений.

Метод MC/TDMA/TDD совместно с механизмом CDCS/CDCA обеспечивают высокую емкость DECT-системам даже в условиях высокого трафика и агрессивной помеховой обстановки. При этом обеспечивается высокое качество услуг без необходимости частотного планирования.

Как было сказано выше, разработчики стандарта DECT использовали богатый опыт в разработке протоколов для сетей ISDN. Поэтому, аналогично сетям ISDN, DECT соответствует принципам взаимодействия открытых систем Международной организации стандартов (OSI ISO). Архитектура протоколов DECT включает:

- физический уровень (PHL Layer),
- уровень доступа к среде (MAC Layer),
- уровень управления звеном передачи данных (DLC layer),
- сетевой уровень (NWK layer),
- прикладные уровни (Alication profiles).

Прикладные уровни определяются специальными стандартами профилей DECT. Уровни доступа к среде и управления звеном передачи данных относятся ко второму уровню OSI. Уровни DLC и NWK подразделяются на две плоскости: плоскость управления (C-plane) и пользовательская плоскость (U-plane). Первый уровень, физический, обеспечивает среду для связи с RFP и определен в стандарте ETS 300 174-3. Этот стандарт определяет параметры радиотракта DECT. В частности, в стандарте определены диапазон частот, излучаемая мощность, метод модуляции, структура временного разделения TDMA и др. DECT является технологией общего радиодоступа, работающего в диапазоне частот 1880–1900 МГц. Для организации физических каналов используется механизм MC/TDMA/TDD, описанный выше. Механизмом MC (множества несущих) в этом диапазоне обеспечивает 10 несущих с центральными частотами Fn = 1897,344 МГц - n·1728 кГц. Модуляция несущей осуществляется со скоростью 1152 Мбит/с частотной манипуляцией с девиацией частоты 288 кГц. Для минимизации полосы частот используется гауссовский фильтр с параметром 0,5 (произведение ширины полосы и длительности). На каждой несущей путем временного разделения создается 24 канала. Комбинация «несущая частота + временной канал» называется физическим каналом. Всего существует 240 физических каналов. Из этих 240 каналов половина используется для передачи информации от RFP к PP, а другая половина — в обратном направлении. Таким образом, именно PHL-уровень отвечает за механизм MC/TDMA/TDD. Следовательно, DECT в состоянии поддерживать 120 одновременных дуплексных каналов.

Для обеспечения высокоскоростной передачи данных (до 2 Мбит/с) базовый стандарт ETS 300 175 был дополнен методом высокоскоростной передачи на основе фазовой модуляции. Используются две схемы модуляции: 4-уровневая (4-DQPSK) и 8-уровневая (8-D8PSK). Модуляция с высокой плотностью (4- и 8-уровневая) используется только для модуляции информационного канала (B+Z-fields), а для модуляции каналов синхронизации и управления (S+A-fields) используется частотная манипуляция. Таким образом, обеспечивается совместимость новых систем с высокой плотностью модуляции с существующими системами.

Каждый физический канал (временной интервал) содержит защитный интервал длительностью 25 мкс для обеспечения множественного доступа, 32 бита синхронизации (SYN), 64 бита управления (C) и биты данных (I) переменной длины. Биты синхронизации используются физическим каналом для целей синхронизации, и они присутствуют в каждом физическом канале. Таким образом, ресинхронизация может производиться перед каждым физическим каналом. Биты C и I образуют два логических канала соответственно, для целей управления и передачи пользовательских данных, как в ISDN.

Уровень доступа к среде является нижней частью второго уровня (уровень 2a) протокола DECT и отвечает за установление радиоканала между PP и RFP. Основными функциями этого уровня являются:

- установление соединений,
- обеспечение сигнализации,
- управление хендовером.

Именно MAC-уровень отвечает за «мягкий» хендовер и механизм CDCS/CDCA. Кроме того, MAC-уровень обеспечивает канал для передачи пейджинговой информации и сигнализации. Информация пользователя (плоскость U) передается прозрачно, без обработки.

Уровень управления звеном передачи данных является верхней частью второго уровня (уровень 2в) протокола DECT и отвечает за надежную передачу управляющей информации по физическому каналу. На этом уровне решаются задачи:

- по защите передаваемых данных от ошибок,
- по управлению качеством физического соединения,
- по управлению выбором канала физическим уровнем.

На втором уровне (уровни 2a и 2в) используются так называемые протокольные блоки данных, состоящие из:

- заголовка,
- поля данных MAC-уровня,
- поля данных DLC-уровня,
- циклического проверочного кода (CRC).

Заголовок сообщения определяет тип сообщения и тип DECT-системы (домашняя, офисная или общего пользования). Кроме того, передается идентификатор системы, информация о поддерживаемых функциях системы и пейджинговая информация.

Второй уровень протокола DECT очень похож на второй уровень протокола ISDN (LAP-D). Поэтому он способен поддерживать услуги и функциональность ISDN. При этом D-канал ISDN может отображаться в C-канал DECT, а B-канал — в I-канал.

Третий уровень протокола DECT — сетевой уровень — используется только в C- плоскости, т. к. на пользовательском (U) уровне он прозрачен. Этот уровень отвечает за сигнализацию и содержит функции для:

- управления вторым уровнем,
- управления вызовами,
- управления мобильностью,
- передачи информации с/без установления соединения,
- обеспечения ДВО.

Для обеспечения хендовера не требуются функции третьего уровня, т. к. за это отвечает только второй уровень. В этом заключается основное (принципиальное) отличие DECT от GSM.

Профиль GAP является основой для всех остальных профилей DECT. GAP является главным профилем доступа DECT, предназначенным для использования в системах, поддерживающих телефонные услуги, независимо от типа присоединенной сети. Он определяет минимум необходимых требований к PP и RFP для обеспечения их совместимости. В профиле GAP определены процедуры для установления и разрушения входящих и исходящих соединений, для поддержания мобильности, включая роуминг.

Хотя стандарт DECT определяет технологию радиодоступа, обеспечивающего мобильность, но не рассматривает сетевые аспекты системы. Поэтому технология DECT может быть использована для доступа в любые сети. Такие сети, построенные на основе DECT и GSM, обладают двумя качествами: высокая плотность обслуженного трафика для малоподвижных абонентов в местах наибольшего скопления абонентов за счет подсистемы базовых станций DECT и большая площадь радиопокрытия и высокая мобильность за счет подсистемы базовых станций GSM.

Павел Черкашин, главный инженер проекта (Белгородский филиал ОАО ЦНПО «Каскад»), демонстрирует смонтированную систему командно-технологической двусторонней связи ГТУ- ТЭЦ «Луч»

информационно–деловой
ВЕСТНИК *ОАО ЦНПО «КАСКАД»*

Рынок

Можно ли обмануть сканер?

Продолжение (начало в № 7, 2007)

Системы контроля удаленного доступа (СКУД) — одно из перспективных направлений применения последних достижений микроэлектроники. ОАО ЦНПО «Каскад» на протяжении ряда лет вело проектирование, разработку и внедрение подобных систем, накопив в этой сфере немалый опыт. Сегодня этим опытом с читателями «Вестника» продолжает делиться начальник отдела системной интеграции Объединения Г.С. Терентьев

Комбинированные системы

В прошлом номере нами были подробно рассмотрены ошибки ложного распознавания FAR, соответствующие случаям верификации, т. е. сравнения двух биометрических шаблонов между собой. Для большинства практических задач точность, достигаемая в этом случае, при любом из трех методов вполне достаточна.

В случае идентификации вероятность ложного распознавания FAR увеличивается пропорционально количеству человек в базе данных системы при той же чувствительности (FRR). Так, если при FRR равной 1,3 % лучший пальцевый сканер в режиме верификации обеспечивает значение FAR 0,001 % (один шанс из 100 000), то в режиме идентификации при той же FRR и базе данных в 10 000 человек FAR составляет 10 % (один шанс из 10), что уже недопустимо для большинства приложений.

Таким образом, в режиме идентификации при базах данных до 1000 или 2000 человек некоторые методы (распознавание по пальцам, 3D-фото, радужной оболочке) могут обеспечить приемлемую точность для систем контроля доступа. При базах данных объемом более 1000–2000 человек ни один из биометрических методов в чистом виде неприменим для большинства задач. Для увеличения точности в режиме идентификации целесообразно использовать несколько биометрических методов одновременно.

Одно из наиболее распространенных «мультимодальных» решений — распознавание по отпечаткам нескольких пальцев. Точность, достигаемая в случае пяти пальцев, пока недостижима для комбинаций других методов. Несмотря на это, практическое использование таких систем ограничено по ряду описанных выше критериев.

Международный подкомитет по стандартизации в области биометрии (ISO/IEC JTC1/SC37 Biometrics) разрабатывает единый формат данных для автоматического распознавания лиц, включающий двух- и трехмерные изображения. Некоторые производители уже начали интеграцию этих двух методов. Вероятнее всего, что вскоре распознавание лица с использованием обоих источников информации будет рассматриваться как один биометрический метод.

Объединение 2D- и 3D-методов распознавания лица позволяет объединить и преимущества этих способов. Так, комбинированный метод обеспечивает достаточную точность в режиме идентификации при базах данных размером до 10 000 лиц, а в перспективе — до 100 000.

Тем не менее даже эти показатели неприемлемы для задач государственного или межгосударственного масштаба, где требуется идентификация по базам данных в несколько сотен тысяч или несколько миллионов человек (это может быть, например, задача поиска человека с заданными биометрическими характеристиками в государственной базе данных выданных паспортов или виз). В таком случае возможны комбинированные системы: «много пальцев», или «палец + лицо», или «палец + радужная оболочка глаза», и т. д.

Сценарии использования биометрии

Угрозы безопасности на транспорте, которые вызваны преднамеренными действиями людей, можно разделить на две группы: связанные с персоналом и доступом в служебные помещения и связанные с потоком пассажиров.

Персонал

Современные транспортные терминалы обслуживают тысячи сотрудников. Все они имеют доступ в служебные помещения, многие из таких помещений критически важны с точки зрения безопасности. При этом часть персонала (например, члены экипажей) не являются постоянными сотрудниками транспортного узла (аэропорта), а появляются там только с некоторой периодичностью.

Применение биометрических технологий для контроля доступа в служебные помещения, выхода на летное поле и для предотвращения нежелательных действий сотрудников уже реализовано в нескольких аэропортах. В этой сфере рынок предлагает эффективные и надежные биометрические системы. Один из возможных и обоснованных сценариев работы в этом случае — режим верификации. Дополнение почти повсеместно используемых идентификационных карточек, электронных жетонов (токенов) и ключей биометрической верификацией позволяет исключить возможность обмена карточками между сотрудниками, минимизировать риски при потере или краже пропуска и существенно снизить влияние человеческого фактора.

Сочетание биометрической системы и идентификационных карточек (жетонов) позволяет на несколько порядков повысить надежность.

Режим идентификации для доступа персонала может быть надежным, если число сотрудников не превышает 1000–2000 человек или 10 000 человек в случае комбинированного использования двух- и трехмерных методов распознавания лиц. Режим идентификации имеет ряд преимуществ перед верификацией: он удобнее в использовании (не требуется постоянно иметь при себе пропуск) и характеризуется меньшим временем прохода. Если число сотрудников больше указанного значения, использование биометрических методов в режиме идентификации становится ненадежным.

Пассажиропоток

Пассажиры, в отличие от постоянного персонала, попадают в поле зрения службы безопасности лишь на короткий срок, о них практически ничего не известно и, наконец, это очень плотный поток — в аэропортах это десятки тысяч человек в день. Чем здесь могут помочь биометрические системы?

Посадочный талон. Биометрическая верификация/идентификация при посадке на рейс. Одна из задач службы безопасности аэропортов — исключить возможность обмена посадочными талонами после регистрации пассажира на рейс. Повторная сверка паспортов при посадке на каждый рейс не всегда возможна.

Одна из моделей использования биометрии, которую можно применять уже сегодня, такова: сверка документов и запись биометрического шаблона в базу данных в момент регистрации пассажира на рейс, биометрическая верификация посадочного талона в момент посадки. Посадочный талон может содержать штрихкод с номером пассажира или даже его биометрический шаблон.

Так как количество пассажиров на один рейс не превышает 1000 человек, вполне надежно будет отказаться от посадочного талона и использовать биометрическую идентификацию пассажиров при посадке на рейс.

Тем не менее, использование режима верификации позволяет определять личность и рейс любого пассажира в аэропорту в любой момент, а не только при посадке. Так как количество пассажиров в транспортном узле может превышать 2000, для такой задачи режим идентификации ненадежен и отказ от посадочных талонов нецелесообразен.

Программы для привилегированных пассажиров. Другая модель использования биометрических технологий в транспортных узлах, которая уже внедряется в некоторых аэропортах, — это ускоренная регистрация и проход для пассажиров, которые часто летают. При первичной регистрации пассажира в программе привилегированных клиентов его биометрические данные записываются в базу данных или на карточку участника программы, а последующие проверки документов становятся автоматическими и занимают несколько секунд. Службы безопасности могут провести глубокую проверку гражданина на благонадежность перед присвоением ему статуса привилегированного пассажира.

Высвободившиеся ресурсы службы безопасности можно сосредоточить на остальных пассажирах. Для этого сценария трехмерная фотография более приемлема, чем отпечатки пальцев, поскольку не вызывает психологического дискомфорта. Такое оборудование тестируется сейчас в европейских аэропортах.

Если карта участника программы привязана к предоплаченному или бонусному счету, возникает возможность оплаты различных услуг в аэропорту (телефония, доступ в Интернет, оплата стоянки и т. п.) просто при «предъявлении лица».

Паспортно-визовые документы. Системы безопасности национального масштаба

Первая задача, связанная с использованием паспортно-визовых документов на транспорте и при пересечении государственных границ, — это сверка подлинности документа и его соответствия владельцу. Сегодняшнее визуальное сравнение с фотографией в паспорте эффективно только тогда, когда оно применяется сотрудниками, прошедшими специальную подготовку. При этом утомляемость и снижение внимания сотрудника при плотном потоке очень велики. Кроме того, возможна коррупция или халатность сотрудников паспортного контроля.

Биометрические технологии призваны повысить надежность и эффективность сверки документов, а также обеспечить электронное документирование (логирование) всех сверок. Для решения этой задачи существуют два сценария — двойной или тройной верификации.

Двойная верификация подразумевает сверку биометрического шаблона, записанного в электронном паспорте или визе, с биометрическими характеристиками проверяемого пассажира.

Тройная верификация подразумевает дополнительную сверку двух указанных характеристик с шаблоном, хранящимся в общегосударственном регистре биометрических данных. При таком сценарии любая попытка подделки паспорта становится бессмысленной, поскольку тройная верификация выявит несоответствие с шаблоном в государственном регистре, записанным при выдаче паспорта. Тройная проверка включена в рекомендации ICAO по применению биометрических систем, но для этого варианта требуется создать сначала государственную инфраструктуру, поддерживающую запросы на верификацию личности по биометрическим данным.

Вторая задача, связанная в основном с моментом выдачи паспортно-визового документа, — это проверка того, не выдавался ли ранее аналогичный документ гражданину с теми же биометрическими данными, но под другим именем, а также сверка биометрических данных гражданина с базами данных оперативных и специальных служб. И в том и в другом случае решение задачи подразумевает использование биометрических методов в режиме идентификации, при этом размер баз данных может быть очень большим.

Для решения первой задачи — двойной и тройной верификации — по точности подойдет любой из трех основных методов. Для решения второй задачи — идентификации гражданина по большой базе данных —необходимо использовать комбинированные методы.

Наиболее обоснованное решение — это первичный сбор и занесение в единый государственный регистр, а также в электронные идентификационные документы как дактилоскопической информации с двух пальцев, так и изображений лица. В таком случае для решения задачи верификации, т. е. при сверке документов при пересечении границ, достаточно комбинированного (2D + 3D) метода распознавания лица. Метод бесконтактный, обеспечивает максимальную измеряемость биометрической характеристики (т. е. максимальную скорость верификации и прохода), а поэтому не замедлит и даже ускорит пассажиропоток через точки контроля. Точность 3D-метода, а тем более комбинированного метода, высока и отвечает всем требованиям в режиме верификации, а также в режиме идентификации с не очень большими (до 10 000) оперативными базами данных (такими, как список объявленных в розыск).

Использование дактилоскопической информации предлагается только в момент проверки личности до выдачи документа, а также при необходимости задержания гражданина и предъявлении обвинения. Такое использование дактилоскопической информации позволяет увеличить уровень защиты этих данных, открывая доступ к ним только сотрудникам правоохранительных служб.

В заключение хочу рассказать о новости от компании Aladdin Knowledge Systems, представляющей новый вид биометрической идентификации.

Вполне возможно, что уже очень скоро сверка отпечатков пальцев, радужной оболочки глаза и другие «архаичные» способы биометрического контроля потеряют свою актуальность. Сотрудники Aladdin Knowledge Systems уверены, что есть способ получше — они называют его «биодинамической подписью». Этот вид биометрического контроля, основанный на измерении показателей деятельности человеческого сердца и некоторых других физиологических показателей (в частности, электрических импульсов, генерируемых человеческим телом).

Устройство, осуществляющее измерение всех этих параметров жизнедеятельности организма, получило закономерное название BioDynamic Reader. Оно оснащено двумя сенсорами, к которым нужно прикасаться пальцами рук, — таким образом и происходит считывание и обработка показателей. Как утверждают разработчики, все эти показатели уникальны для каждого человека, а подделать их гораздо сложнее, чем, например, те же отпечатки пальцев.

Может, так оно и есть, но нельзя забывать о том, сколько раз перспективные в теории технологии на деле оказывались далеко не столь оправданными в использовании и надежными.

Г.С. Терентьев,
начальник отдела системной интеграции
integrator@kaskad.ru

Статья подготовлена по материалам интернет-изданий

Главный редактор М. Сарбучев
Редактор В. Лучко
Корректор М. Бучацкая

Ответственный за выпуск от ОАО ЦНПО «Каскад» З. Леквеишвили

Россия, 125047, Москва, 1-я Брестская ул., 35
Телефон: (499) 978-58-73, (495) 251-76-50
Факс: (499) 978- 57-36
e-mail: vestnik@kaskad.ru
http://www.kaskad.ru

Тираж 999 экз.

При участии:
Фишка
Изящные бизнес решения
www.fishca.ru
ЭВЕРС
ПУТЬ К ВЕРШИНЕ
evers – media@list.ru

Распространяется по уникальной базе ОАО ЦНПО «Каскад»