ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ СВЯЗИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПЕРСПЕКТИВНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Воронеж
2022

ББК 32.973
Т-38
УДК 002.001;002:001.8

Авторы: Н. С. Хохлов, С. С. Никулин, Л. А. Лекарь, С. В. Канавин, И. В. Гилев

Рецензенты:
Е.С. Поликарпов, начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД Российской Федерации имени В.Я. Кикотя, кандидат технических наук, подполковник полиции;
В.С. Дунин, заместитель начальника кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России, кандидат технических наук, подполковник полиции.

Повышение эффективности функционирования сетей связи органов внутренних дел на основе перспективных информационных технологий : учебное пособие / Н. С. Хохлов [и др.]. – Воронеж : Воронежский институт МВД России, 2022. – 142 с.

Т38

В учебном пособии рассматриваются вопросы повышения эффективности функционирования сетей связи органов внутренних дел на основе перспективных информационных технологий, проведены эксперименты по организации и применению системы радиосвязи в органах внутренних дел с использованием элементов цифровых информационных технологий. Отдельное внимание уделено вопросам оценки эффективности функционирования сетей связи МВД России с учетом использования ресурсов ИМТС для обеспечения функционирования базовой инфраструктуры ведомственной системы радиосвязи, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи МВД России с учетом информационных архитектур сетей нового поколения.

Учебное пособие предназначено для специалистов по эксплуатации аналоговых и цифровых систем радиосвязи специального назначения, курсантов, слушателей образовательных организаций МВД России по направлениям подготовки 11.05.04 – Инфокоммуникационные технологии и системы специальной связи, 10.05.02 – Информационная безопасность телекоммуникационных систем.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В учебном пособии применяют следующие обозначения и сокращения:

АПК – аппаратно-программный комплекс
АРМ – автоматизированное рабочее место
БС – базовая станция
ГИС – геоинформационная система
ДНА – диаграмм направленности антенн
ДМВ – деструктивное электромагнитное воздействие
ИМТС – интегрированная мультисервисная телекоммуникационная система
МШПД – мобильный широкополоснный доступ
ОВД – органы внутренних дел
ПУС – подвижный узел связи
РЭС – радиоэлектронные средства
РТР – ретранслятор
СР – средства радиосвязи
СУС – система управления и связи
СС СН – система связи специального назначенич
УКВ – ультракороткие волны
ЦКМ – цифровые карты местности
ЧТП – частотно-территориальное планирование
DMR – Digital Mobile Radio

Введение

В настоящее время система управления и связи органов внутренних дел (СУС ОВД) претерпевает значительные изменения. Происходит переход на использование цифровых радиосистем связи, интеграция последних с информационными системами передачи данных. Такая система должна быть помехозащищенной и конфликтно - устойчивой.

Главной целью построения системы связи является приведение ее в состояние, позволяющее обеспечить потребности управления деятельностью ОВД в современных условиях. Наличие и достоверность информации о развитии процессов в обществе в значительной степени определяют возможности правоохранительных органов в выработке и реализации эффективных управленческих решений, оперативном управлении деятельностью подразделений органов внутренних дел. Эффективное использование информационно-телекоммуникационных технологий обеспечивает подразделениям системы МВД России возможность выхода на качественно новый уровень взаимодействия с гражданами и обществом [1].

Активное развитие информационных и телекоммуникационных технологий предполагает реализацию универсальной гетерогенной транспортной среды, с вынесением функции услуг в оконечные сетевые узлы, и интеграцию с традиционными сетями связи. При этом ставится задача выбора и обоснования путей повышения эффективности сетей, методов оптимизации перспективных систем, внедрения на их основе новых технологий управления деятельностью ОВД. Применительно к цифровым радиосетям ОВД такие исследования не проводились.

Это определяет актуальность рассматриваемой проблемы повышения эффективности функционирования, внедрения перспективных систем управления ОВД на базе цифровых сетей связи и новых инфокоммуникационных технологий.

В рамках данной работы реализованы предложения по разработке и проверке на практике процедур, алгоритмов и программных средств выполнения отдельных этапов задачи оптимизации, связанных с оценкой эффективности системы связи ОВД.

Актуальность работы заключается в необходимости развития существующих ресурсов МВД России для сокращения времени реагирования и управления при функционировании базовой инфраструктуры ведомственной системы связи с учетом беспроводных решений и архитектуры широкополосных сетей, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи МВД России.

1. ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ СВЯЗИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПЕРСПЕКТИВНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Анализ особенностей построения сетей связи ОВД и определения повышения эффективности их функционирования

Научно-технический прогресс в области системы связи МВД России проявляется в развитии инфокоммуникационной инфраструктуры, замене устаревших технических средств новыми. Основой развития системы связи являются достижения фундаментальных наук, открывающие новые физические принципы и способы функционирования устройств и систем. В современной системе радиосвязи МВД России можно выделить следующие важные направления: интеллектуализация систем радиосвязи на основе компьютерных средств и технологий; освоение в практике ОВД новых диапазонов частот; повышение роли устройств обработки информации. Усложнение функций, связанных с передачей, накоплением и обработкой информации, решается за счет устройств цифровой техники. Так, важное место в оперативной деятельности ОВД играют дежурные части. Именно в их компетенции находится получение требуемой информации о совершенных преступлениях, наличии рядом сил и средств полиции, привлекаемых для участия в расследовании.

Для передачи оперативной информации от вышестоящей дежурной части к подчиненным частям в системе МВД России создана система громкоговорящего оповещения дежурных частей на базе аппаратно-программного комплекса «Мегафон-Р» с возможностью принятия информации в автоматическом режиме и дальнейшим подтверждением на интерфейсе АРМ оперативного дежурного. Оповещение реализуется через телекоммуникационные каналы МВД России. Один из важнейших этапов развития системы радиосвязи – организация устойчивых каналов передачи данных и доступа к информационным ресурсам и ведомственным информационным системам. Это возможно, например, за счет внедрения новых диапазонов частот, в частности, при использовании спутниковых каналов передачи. Пример: в МВД Республики Татарстан реализован авторизованный доступ участковых из отдаленных сельских поселений к ресурсам ИМТС МВД России. Это обеспечено использованием спутниковых терминалов модемом SkyEdge 2.

Спутниковые технологии связи существенно продвинули развитие инфраструктуры связи во многих подразделениях ОВД страны. Развитие навигационной спутниковой системы ГЛОНАСС позволило внедрить в деятельность ОВД во всех регионах новые технологии, в частности автоматизировать процесс управления силами и средствами подразделений ОВД, упростить контроль за несением службы и нахождением нарядов на

постах и маршрутах патрулирования. В дежурных частях появились АРМ системы управления мобильными нарядами и автотранспортными средствами. С их помощью возможно определять состав наряда, скорость, направление движения, осуществлять контроль за ходом дежурства, архивировать историю дежурства. Для обеспечения большой площади радиопокрытия и повышения надежности передачи данных в состав системы включена цифровая радиосеть, формирующая ретрансляцию данных от мобильных, пеших нарядов к диспетчерским центрам системы. Каждый ретранслятор принимает данные на навигационных частотах и передает их на частоте радиосети. Радиосеть синхронизируется по принципу передачи маркера. В случае, когда каждое устройство радиосвязи помимо функций приема и передачи может выполнять функции ретранслятора, появляется возможность реализации интеллектуальной самоорганизующейся радиосети. Такая сеть представляет собой структуру из многих абонентов и нескольких точек доступа к внешним сетям. Структура такой сети обладает возможностью самостоятельного конфигурирования в зависимости от нахождения радиосредств в зоне взаимной видимости. Информационный пакет проходит через все устройства на пути прохождения информации по маршруту. Таким образом, за счет ресурсов каждого абонента увеличивается радиус действия сети, надежность и оперативность связи. Пример: комплекс средств цифровой радиосвязи «Гранит Р–86АЦ». В основе комплекса протокол «Волновая сеть» на основе множественного случайного доступа к каналу передачи данных с контролем несущей. Радиосредства самоорганизующейся сети работают в широкополосном канале и позволяют передавать информацию и речь [3, 4].

Большинство радиосетей ОВД представляет собой конвенциональные системы радиосвязи, общим недостатком которых является неэффективное использование радиочастот. В настоящее время основные производители оборудования радиосвязи предлагают новые цифровые решения для конвенциональных радиосетей. Это, прежде всего, система MOTOTRBO (европейский открытый стандарт DMR) от компании Motorola, оборудование этого же стандарта от компании Hytera, а также системы IDAS (производства Icom) и NEXEDGE (производства Kenwood). Важным отличием систем связи стандарта DMR (Motorola, Hytera) от протоколов от компаний Icom и Kenwood является принцип разделения каналов – 2-слотовый TDMA с шириной канала 12,5 кГц в стандарте DMR и FDMA с шириной канала 6,25 кГц для IDAS/NEXEDGE. Эти системы, несмотря на разный подход к реализации, предусматривают возможность системной интеграции посредством среды TCP/IP, взаимодействуют с системой спутниковой навигации и обеспечивают повышенную функциональность, не достижимую для аналоговых систем радиосвязи.

Активно внедряемые в практику ОВД системы транкинговой связи предназначены для построения локальных и многозоновых сетей, предоставляющих различные виды услуг при высоком качестве связи. В частности, поддерживаются речевая связь между абонентами и группами абонентов, доступ к ведомственным телефонным сетям, телефонным сетям общего пользования и сетям передачи данных (телеметрия, аварийная сигнализация, цифровые данные). Для построения системы цифро-аналоговой радиосвязи с передачей данных и голоса между абонентами по связанным зонам радиосети и диспетчеризации требуется наличие транспортной сети широкополосной передачи данных (ШПД), организованной по беспроводной, оптической или проводной технологии. Для организации внутрисистемных линий связи (межсайтовые соединения, удалённые объекты связи и прочее) в сетях УКВ-радиосвязи цифровых стандартов радиосвязи (APCO 25, DMR, IDAS) используются общепринятые, широко применяемые в органах внутренних дел, интерфейсы (E1 G703, IP). Наиболее часто используются цифровые каналы, образованные с помощью волоконно-оптических линий связи (ВОЛС) или радиорелейных линий (РРЛ), реже – медные линии связи. IP-соединение ретрансляторов также может применяться для увеличения географической зоны покрытия радиосвязью.

Для подключения по IP также могут быть использованы ретрансляторы разных диапазонов. Преимуществом IP-соединения является возможность использования глобальной сети Интернет. При этом рекомендуется использовать роутеры или другие устройства, способные обеспечить функцию VPN. IP-сети находят применение не только для соединения компонентов цифровых сетей радиосвязи, но и для их интеграции с аналоговыми сетями. Например, система «Радиокупол» представляет собой специализированную RoIP-систему, разворачиваемую на базе RoIP-шлюзов, подключаемых к имеющемуся телекоммуникационному оборудованию и обеспечивающих коммутацию и диспетчеризацию аналоговой и цифровой радиосвязи [1, 4–7]. Для объединения зон действия разных ретрансляторов в общую зону радиопокрытия и подключения станций удалённого доступа используется опорная IP-сеть. Инфраструктура МВД России предоставляет IP-каналы связи ИМТС (интегрированные мультисервисные телекоммуникационные системы) ОВД, построенные на базе Ethernet-сетей с использованием протоколов TCP/IP, для передачи абонентского трафика и служебной информации между базовыми станциями, АРМ диспетчера, администратора и центра управления и коммутации в любом цифровом режиме.

Системы связи RoIP – это новый сегмент радиосвязи, разрабатываемый в России. RoIP является универсальной коммуникационной системой, которая преобразовывает радиосигнал в цифровые данные, подходящие для передачи по IP-сети, и наоборот. Эта

система предназначена для передачи речи по локальной сети в реальном времени между компьютером и удаленными радиостанциями. Система состоит из рабочего места диспетчера и удаленных радиостанций. Радиостанция подключается к IP-сети посредством шлюза RoIP. Основное назначение системы – обеспечение устойчивой радиосвязью объектов со сложной инфраструктурой и топологией, объединение в одну сеть несколько групп пользователей, использующих различный частотный ресурс; обеспечение возможности перехода на цифровые системы передачи голоса без замены и модернизации абонентского парка радиостанций. Устройство RoIP-шлюзов строится с учетом последних тенденций по созданию комплексных систем радиосвязи на основе IP-сетей для управления и информационного обеспечения различных служб общественной безопасности Использование в системах радиосвязи ПК дает возможность без применения специальных пультов программно изменять настройки ретрансляторов и базовых станций и осуществлять по IP-сети прямой контроль над состоянием систем связи. Система RoIP связи позволяет создать единый диспетчерский центр управления подразделениями (нарядами) различных служб (с возможностью организации конференцсвязи между диспетчерами), реализовывать удаленное управление и настройку базовых станций многозоновых радиосетей. С помощью данной схемы пользователи радиостанций получают доступ к тем сервисным возможностям, которые традиционно могли использовать только абоненты сотовых сетей связи или телефонных сетей общего пользования, включая прямой вызов телефонных номеров, переадресацию вызовов, конференцсвязь, а также запись переговоров в эфире [12–15].

Сложность создания сетей связи нового поколения заключается в том, что сети фиксированной, мобильной связи построены по разным стандартам и используют разное программное обеспечение. В этих условиях важно, чтобы программное обеспечение предоставления сервисов не зависело от архитектуры сети и технологии доставки информации. Для построения мультисервисной сети необходимы транспортные каналы и протоколы, способные поддерживать доставку информации различного вида (речь, данные, видео) [19]. Это реализуется объединением сетей мобильной связи, IP-сетей, сетей общего пользования в единую сеть, которая интегрирует различные технологии. Для передачи данных, в том числе фото и видеотрафика, в интересах ОВД используются системы технологии широкополосного радиодоступа. Такие технологии позволяют реализовать требования системы управления ОВД и значительно увеличить ёмкость сетей за счёт использования спектрально-эффективных методов передачи данных.

В настоящее время сети МШПД в системе связи органов внутренних дел Российской Федерации предназначены для формирования гибкой

транспортной инфраструктуры, позволяющей подключить как фиксированных, так и мобильных пользователей и передавать данные, телефонию, видеоинформацию в недоступных для организации проводных каналов местах, организовать подключение к ведомственным информационным ресурсам пользователей структурных подразделений МВД России (районные отделы полиции, подразделения полиции на транспорте, патрульные наряды ДПС). Указанные технологии полностью реализованы в оборудовании радиодоступа, базирующемся на мобильных технологиях IEEE 802.16–2005 («мобильный» WiMAX) и LTE [4–5].

Система радиосвязи специального назначения, являясь составной частью системы связи в целом, обеспечивает перенос информации между источниками и получателями информации. В то же время современная система радиосвязи начинает включать в себя информационные устройства для поиска, хранения и сжатия, преобразования и организации доступа к источникам информации, в том числе сетевые узлы – серверы, шлюзы, терминалы. Учитывая, что источники и получатели информации также являются элементами системы радиосвязи, можно сделать вывод о конвергенции сетей радиосвязи и информационных сетей, а также взаимном влиянии технологий, то есть возникновении и реализации инфокоммуникационных систем.

Развитие инфокоммуникационных сервисов осуществляется в рамках IP-сетей с одновременным расширением функциональности самих сетей связи. Важнейшими из них представляются: мультисервисность, предоставление услуг независимо от транспортных технологий; широкополосность, для гибкого изменения скорости передачи информации; мультимедийность, для передачи многокомпонентной информации. Такие требования предполагают наличие некоторой интеллектуальной надстройки, управляющей вызовами и предоставлением услуг, то есть системы радиосвязи становятся интеллектуальными.

Подобная интеллектуальность реализуется в общей инфраструктуре программными средствами для управления радиосредствами. Это позволяет характеризовать перспективные радиосредства как программно-определяемое радио, характеристики радиосистем в этом случае не только обусловлены программным обеспечением (ПО), но и используют инфраструктуру, обычно присущую только сетям. В программно-определяемом радио программное обеспечение определяет службы и интерфейсы, которые согласуют сигнальные приложения с аппаратными средствами. Структура такого радио определяется программным обеспечением цифровой обработки сигналов. ПО характеризует функции системы и интерфейсы управления, конфигурирование приложений, формирование сигнала и его обработки. Концепция программно-определяемого радио основана на использовании объектно-ориентированных языков (C++, Java и др.). Программно-реализуемая

архитектура имеет ряд преимуществ по сравнению с традиционными радиосредствами. Их применение, с учетом возможностей современных цифровых сигнальных процессоров, позволяет обеспечивать надежную связь и высокий уровень совместимости радиосистем. Расширяются возможности перенастройки системы, совместимость с разными аппаратными платформами. Концепция программно-определяемого радио базируется на разработке инфраструктуры операционной среды. Такая среда применяется для управления, настройки и регулирования радиосистем, используемых в них приложений. Это позволяет модернизировать системы, то есть внедрять новые технологии и улучшать характеристики.

Стремительный прогресс в области телекоммуникационных и информационных технологий привел к возможности конвергенции разнородных сетей в единую мультисервисную сеть. Данная сеть позволит предоставлять пользователям разнородные телекоммуникационные услуги – передачу голоса, мультимедийные услуги, передачу данных и многое другое. Мультисервисные сети связи могут быть созданы непосредственно на основе как существующих цифровых, так и виртуальных сетей.

Ядром мультисервисных сетей связи (NGN, Next Generation Networks – сетей следующего/нового поколения) являются опорные IP-сети, поддерживающие полную или частичную интеграцию услуг передачи речи, данных и мультимедиа. NGN реализует принцип конвергенции услуг электросвязи.

Пакетная коммутация, основанная на IP-технологии, реализуется в так называемых сетях следующего поколения NGN (Next Generation Network), которые предназначены для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS.

Основу сетей NGN, изначально сложившихся как NGN IPCC (International Packet Communication Consortium), составляют гибкие коммутаторы Soft switch и IP-АТС. NGN представляет собой модернизированную TDM-сеть с возможностью передачи IP-трафика, а также с дополнительными возможностями предоставления услуг для конечного пользователя. В настоящий момент в NGN на смену архитектуре IPCC приходит TISPAN, ключевым элементом которой является IMS (IP Multimedia Subsystem). Основное отличие NGN TISPAN (IMS) от NGN IPCC заключается в гибкости и масштабируемости таких сетей. В них функции управления сеансами и маршрутизацией выполняет CSCF (Call Session Control Function), пришедший на смену Soft switch. С одной стороны, сети NGN IPCC/TISPAN (IMS) предоставляют широкий набор дополнительных услуг (т. н. ДВО – дополнительные виды обслуживания), которые предоставляют возможности более эффективного управления сетью по сравнению с TDM-архитектурой. С другой стороны, такой спектр

функциональных возможностей увеличивает число уязвимостей и порождает источники угроз информационной безопасности.

Сложность создания сетей нового поколения заключается в том, что сети фиксированной, мобильной связи построены в соответствии с разными стандартами и используют разное программное обеспечение.

В этих условиях важно, чтобы программное обеспечение предоставления сервисов не зависело от архитектуры сети и технологии доставки информации.

Для построения мультисервисной сети необходимы транспортные каналы и протоколы, способные поддерживать доставку информации различного вида (речь, данные, видео). Это реализуется объединением сетей мобильной связи, IP-сетей, сетей общего пользования в единую сеть, которая интегрирует различные технологии. Функциональная модель такой сети может быть представлена транспортным уровнем, уровнем управления коммутацией и передачей информации, а также управления услугами.

Собственная мультисервисная сеть связи позволит:

– создать высокопроизводительную и помехоустойчивую технологическую основу для внедрения новых приложений, направленных на повышение уровня общественной безопасности;

– расширить возможности существующих ведомственных систем связи за счет добавления функций мобильности и мультимедийности;

– обеспечить дистанционное управление экипажами ведомственных автомобилей и двухсторонний мультимедийный цифровой радиообмен;

– организовать постоянное видеонаблюдение на территории города, в том числе с использованием мобильных объектов;

– обеспечить доступ мобильных и стационарных пользователей к информационным ресурсам и ведомственным базам данных;

– осуществить передачу телеметрической информации с мобильных и стационарных объектов;

– существенно снизить накладные расходы на аренду внешних каналов связи и телефонии.

Мультисервисная сеть связи – основа современной информационной системы связи специального назначения.

В учебном пособии изложены практические аспекты проектирования и расчета необходимого сетевого ресурса и оборудования для построения фрагмента сети NGN/IMS.

Такие широкие функциональные возможности NGN в сравнении с традиционными сетями, как открытость архитектуры; конвергентность услуг (голос, данные, видео) и сетей (ТфОП, Интернет, мобильной связи); мультистандартный доступ к услугам (xDSL, Wi-Fi, WiMAX, 3G/4G/5G); создают новые угрозы информационной безопасности или открывают более широкие возможности реализации известных угроз. Данные факторы требуют комплексного решения проблемы на основе разработки

соответствующих политик безопасности и методов защиты информации, а также построения системы обеспечения информационной безопасности.

Общая архитектура информационной безопасности NGN, согласно рекомендациям МСЭ X.805, Y.2701, определяется понятиями «слой» и «плоскость». Слои безопасности связаны с выполнением требований к сетевым элементам, образующим сквозную сеть [8, 9]. При распределении требований по слоям применяется иерархический подход для достижения межконцевой безопасности за счет обеспечения безопасности каждого слоя. Архитектура информационной безопасности в этом случае включает 3 слоя (рис. 1.1):

– слой инфраструктуры – совокупность сетевых элементов (шлюзы, гибкие коммутаторы, маршрутизаторы, серверы и др.) и каналов передачи информации;

– слой услуг – совокупность сетевых услуг (услуги IP-транспорта, услуги VPN, VoIP, QoS, услуги определения местонахождения и др.);

– слой приложений – совокупность основных приложений пользователей.

Рис. 1.1. Архитектура информационной безопасности NGN

Одним из преимуществ данного подхода является возможность его многократного применения для обеспечения межконцевой безопасности различных приложений. Степень уязвимости каждого слоя различна и, следовательно, меры противодействия определяются из задач, выполняемых каждым слоем.

Плоскости безопасности связаны с безопасностью деятельности в сетевой среде. В рамках архитектуры безопасности, по аналогии с архитектурой NGN, определяются три плоскости:

– плоскость административного управления (менеджмента) – совокупность функций эксплуатации, администрирования, технического обслуживания;

– плоскость оперативного управления – совокупность функций сигнализации для установления/разъединения соединений в сети независимо от среды передачи и телекоммуникационных технологий;

– плоскость конечного пользователя – совокупность функций доступа и использования ресурсов сети пользователями.

В соответствии с представленной архитектурой для каждого слоя и плоскости вводятся:

– функции безопасности: контроль доступа, аутентификация, конфиденциальность данных, целостность данных, неотказуемость, приватность (защищенность частной информации);

– механизмы безопасности: шифрование, цифровая подпись, управление доступом, контроль целостности данных, аутентификация, защита трафика, управление маршрутизацией, арбитраж, реализуемые соответствующими средствами информационной безопасности.

Важным требованием к архитектуре информационной безопасности NGN является соблюдение логического и физического (определяемого маршрутизацией) разделения трафика пользователей, сигнализации, управления, а также обеспечения безопасности во всех плоскостях [4].

1.2. Проведение экспериментов по организации и применению системы радиосвязи в органах внутренних дел с использованием элементов цифровых информационных технологий

Описание оборудования, используемого в серии экспериментальных исследований. В ходе подготовки научно-исследовательской работы проводилась серия лабораторных экспериментальных исследований на оборудовании, которые можно характеризовать небольшим числом измерительных и управляющих каналов, малыми энергетическими затратами на экспериментальной установке и менее требовательными условиями к самой установке. В качестве исследуемых систем связи были выбраны системы, использующие в своей работе широкополосные сигналы, описание таких сигналов произведено в работе [6, 9–11].

В качестве источников, воспроизводящих деструктивное электромагнитное воздействие, будем использовать: блокиратор мобильных сетей типа Alligator-40, генератор сигналов высокочастотный Г4-83 и радиосредство, работающее в одном частотном диапазоне с исследуемой системой радиосвязи.

Излучающие антенные системы: штыревые антенны, рассчитанные на соответствующие частотные диапазоны, а также рупорно-линзовая антенна П6-23 [13, 20–23].

В качестве измерительного оборудования, анализирующего спектр деструктивного воздействия, будем использовать портативный анализатор спектра, например, Rohde & Schwarz FSH8. Такое средство измерения обеспечивает наиболее важные функции высокочастотного анализа. Анализатор спектра может использоваться как для технического обслуживания или настройки передающих систем, проверки кабелей и антенн, так и оценки качества сигналов в радиовещании, радиосвязи и обслуживании, измерения напряженности электрического поля. Некоторые характеристики спектроанализатора приведены в таблице 1.1.

Таблица 1.1. Характеристики спектроанализатора

Характеристика	R&S FSH8
Диапазон частот	от 100 кГц до 8 ГГц
Полоса обзора частот	0 Гц, от 10 кГц до 3 ГГц
Ширина полосы пропускания	1, 3, 10, 30,100, 200, 300 кГц, 1 МГц
Собственные помехи	<–80 дБмВт
Отображаемые единицы Логарифмические	дБмВт, дБмкВ, дБмВ с преобразователем также дБмкВ/м дБмкА/м
Линейные	мкВ, мВ, В, нВт, мкВт, мВт, Вт с преобразователем также В/м, мВ/м, мкВ/м и Вт/м
ВЧ-вход	гнездо N-типа
Входной импеданс	50 Ом

Немаловажными преимуществами используемого анализатора спектра являются малые массогабаритные размеры, наличие аккумуляторной батареи и возможность интеграции с программным обеспечением, что позволяет использовать его в полевых условиях.

Захват и регистрация спектров помехового воздействия с дисплея анализатора спектра будем осуществлять при помощи программного обеспечения (ПО) R&S Instrument View. Многофункциональное программное обеспечение R&S FSH8View позволяет удаленно управлять анализатором, документировать результаты измерений, создавать граничные линии, таблицы каналов и т. п. Соединение с ПК возможно как с помощью LAN, так и USB. В комплексе проводимых экспериментов подключение осуществлялось по сети LAN. Проведена серия экспериментальных исследований, результаты которых будут рассмотрены далее.

Первый эксперимент по воспроизведению ДЭМВ. Экспериментальное исследование заключается в воспроизведении деструктивных электромагнитных воздействий, оказывающих влияние на мобильный терминал стандарта 3G. В качестве источника ДЭМВ авторами использован блокиратор сигналов мобильной связи типа «Alligator-40» [9]. В большинстве случаев блокиратор представляет собой генератор широкополосных радиопомех, создающий заградительную помеху по частоте во всем диапазоне работы системы мобильной связи. Генератор шума приспособлен для решения задачи временного блокирования мобильных устройств. Процесс блокирования сводится к постановке шумовых или маскирующих радиопомех по основному каналу работы приемника мобильного терминала с помощью генератора шума простой конструкции. Максимальная дальность действия данных блокираторов составляет десятки метров, хотя в условиях помещений из-за ослабления радиоволн при прохождении через стены и препятствия реальная дальность их действия значительно меньше [9], что согласуется с результатами работы [1–15].

В качестве антенн блокираторов чаще всего используют штыревые антенны, отдельную для каждого диапазона радиочастот. Выбранный блокиратор относится к генераторам шума в полосе функционирования системы мобильной связи 3G. Средством связи, на которое оказывается воздействие, выбран мобильный терминал стандарта 3G. Фото экспериментальной установки приведено на рис. 1.2.

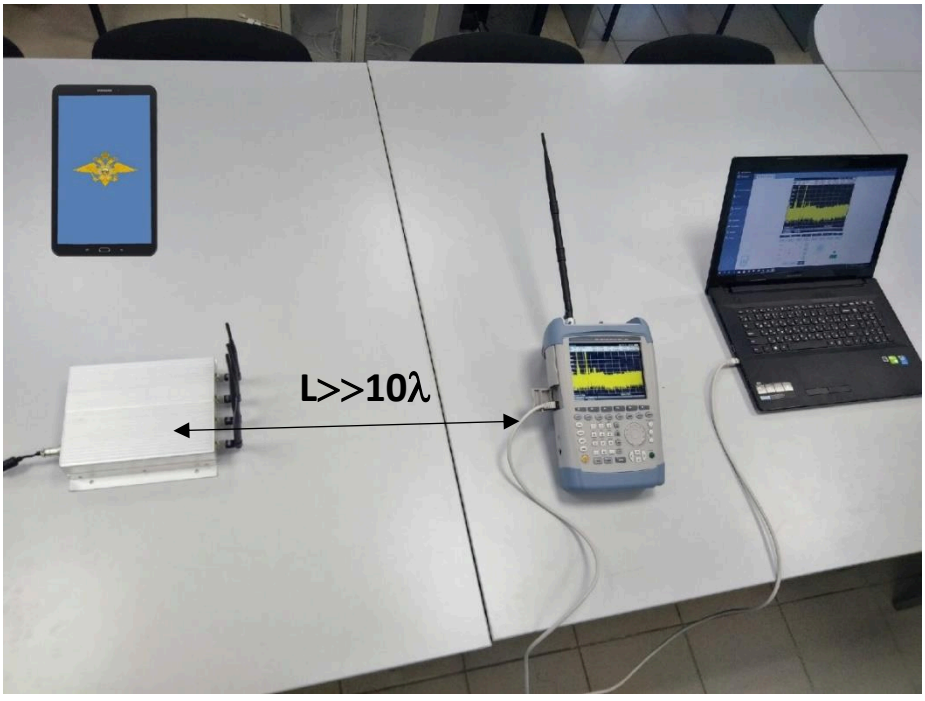


Рис. 1.2. Фото экспериментальной установки. В качестве источника ДЭМВ используется «Alligator-40»

Осуществляем настройку анализатора спектра, выставляя следующие параметры:

1. Центральная частота 2 ГГц.
2. Ширина полосы частот 500 МГц.
3. Предусилитель выключен.
4. Сопротивление антенны 50 Ом.
5. SWT 20 ms.

В рамках первой части эксперимента произведем захват спектра 3G терминала. Располагаем терминал на расстоянии 3–5 метров от спектроанализатора, настроенного на указанные параметры сигнала и с помощью ПО делаем скриншот указанного спектра (рис. 1.3).

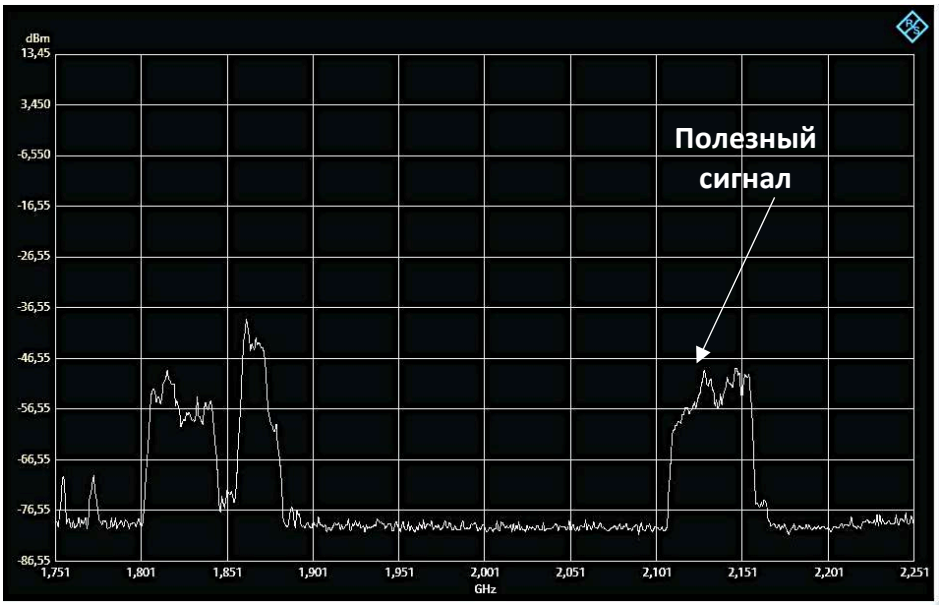


Рис. 1.3. Спектр полезного сигнала 3G терминала без воздействия ДЭМВ

Из полученного спектра видно, что мощность информационного сигнала составляет – 51 Дбм, а ширина полосы 50 МГц.

Второй частью эксперимента является добавление в указанную в первой части схемы блокиратор сигналов мобильных сетей. Фиксируем результаты воздействия подавителя на спектре рис. 1.4.

Из рисунка 1.4 видно, что мощность спектра помехи превосходит спектр мощности полезного сигнала более чем на 15 Дбм, а ширина – на 35 МГц, что позволяет сделать вывод, что передаваемый полезный сигнал становится подавленный помехой и принять и демодулировать его с заданной степенью достоверности на приемном терминале не представляется возможным. Аналогичные результаты можно получить и для систем связи 4-го поколения.

Второй эксперимент по воспроизведению ДЭМВ. В ходе второго экспериментального исследования с помощью генератора Г4-83, характеристики которого приведены в табл. 1.2, и рупорно-линзовой антенны П6-23, характеристики приведены в табл. 1.3, было осуществлено моделирование широкополосной деструктивной помехи.

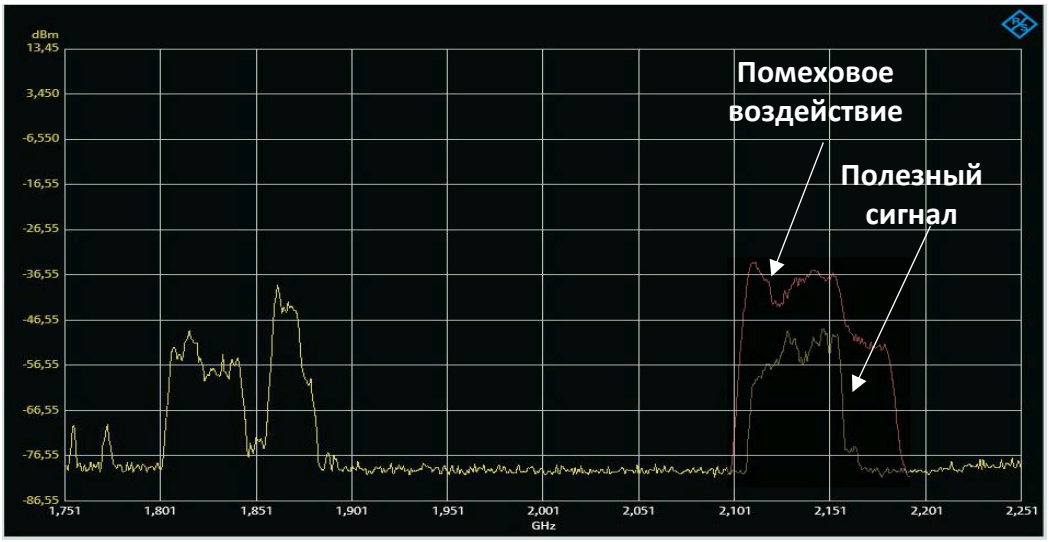


Рис. 1.4. Спектр полезного сигнала 3G терминала и воздействующего ДЭМВ

Генераторы сигналов высокой частоты Г4-83 служит для воспроизведения электромагнитного синусоидального сигнала. Сферой применения генератора Г4-83 является настройка различных радиоприемных устройств. Он предназначен для регулировки и проверки радиоэлектронной аппаратуры сантиметрового диапазона. Генератор Г4-83 находит широкое применение при разработке, производстве, эксплуатации и ремонте различных радиотехнических систем сантиметрового диапазона. В комплект генератора входит необходимый набор коаксиальных и волноводных переходов.

Широкополосная измерительная антенна П6-23М представляет собой рупорно-линзовую антенну со стандартным коаксиальным соединителем. Данный тип антенны выбран, поскольку она создает в дальней зоне плоский фронт электромагнитной волны, что наилучшим образом воспроизводит ДЭМВ, оказываемое аппаратурой правонарушителей. Антенна предназначена как для измерения плотности потока энергии, создания электромагнитного поля с заданной плотностью, так и для измерения параметров антенн различных типов, параметров электромагнитной совместимости радиоэлектронных средств, мониторинга электромагнитной обстановки и пеленгации источников электромагнитного излучения совместно с приёмными устройствами.

Таблица 1.2. Технические характеристики генератора

Диапазон частот	7,5–10,5 ГГц
Пределы допускаемой основной погрешности установки частоты	±0,5 %
Нестабильность частоты за 15 минут работы	5*10–5f
Уровень выходного сигнала	10–3–10–5 Вт (калиброванный выход), 3*10–3–3*10–8 Вт (некалиброванный выход).
Пределы допускаемой основной погрешности установки опорного уровня выходной мощности	±10–4 Вт: не более 1,2 дБ
Нестабильность выходной мощности за 15 минут работы	0,1 дБ
Параметры внешней ИМ	частота повторения: 0,01–20кГц, амплитуда: 20–40 В, длительность: 0,2–200 мкс, длительность фронта и среза: 0,25 и 0,5 мкс соответственно
Потребляемая мощность	150 В*А
Габариты	480х120х475 мм
Масса	20 кг

Таблица 1.3. Технические характеристики антенны

Диапазон частот, ГГц	1–12
Пределы допускаемой основной погрешности установки частоты	±0,5 %
Уровень выходного сигнала, Вт:	10–3–10–5
Погрешность эффективной площади	– 20%
КСВ	– 1,5.
Уровень: боковых лепестков	не более 10 дБ
Сопротивление входа	50 Ом

В ходе проведения лабораторных исследований антенна П6-23М комплектуется треногой (опорно-поворотным устройством), обеспечивающей ориентацию по азимуту, углу места, поляризации и высоте.

Настроим частоту генератора и центральную частоту спектроанализатора на 8 ГГц. На генераторе выберем прямоугольный повторяющийся импульс.

Зададим параметры спектроанализатора:

1. Опорный уровень –33,4 ДБм.
2. Время свипирования 20 мс.
3. Ширина полосы пропускания 23 МГц.
4. Полоса 120 ДБм.

Фото экспериментальной установки приведено на рис. 1.5.

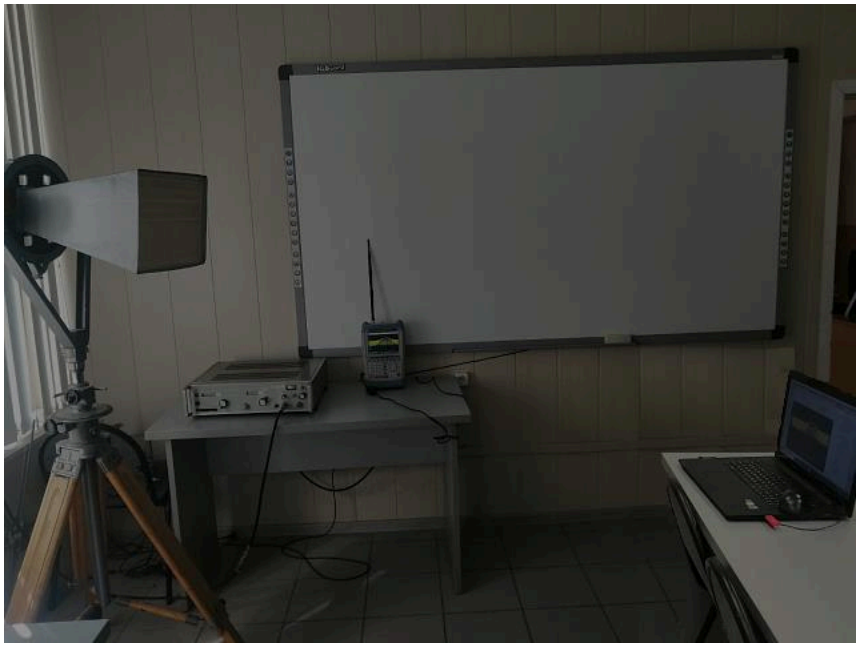


Рис. 1.5. Фото экспериментальной установки по воспроизведению ДЭМВ. В качестве источника ДЭМВ используется Г4-83

Полученный спектр ДЭМВ приведен на рис. 1.6.

Из спектра видно, что ширина помехового воздействия составляет 7 МГц, а мощность – 52Дбм, что, согласно данным о минимальном уровне сигнала приемной станции WIMAX (–116Дбм), не позволит распознать полезный сигнал. Подобная экспериментальная установка позволяет тестировать перспективное оборудование связи 5 поколения.

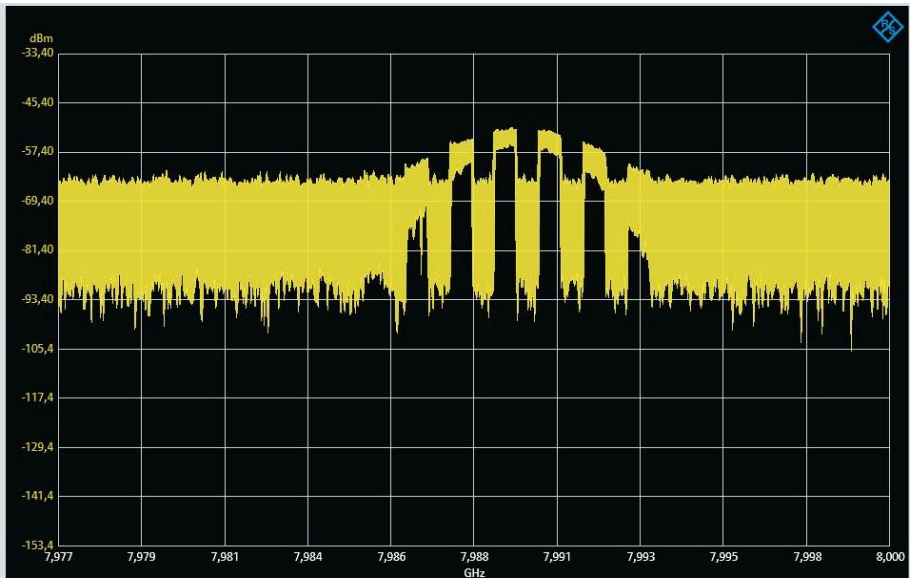


Рис. 1.6. Спектр воздействующего ДЭМВ

Третий эксперимент по воспроизведению ДЭМВ. Для проведения экспериментального исследования выберем мобильную цифровую систему передачи видео и звука, предназначенную для передачи высококачественной оперативной видео- и аудиоинформации по UHF/VHF радиоканалу от одного или нескольких носимых комплектов передачи данных (НКПД) на центральный пункт управления (ЦПУ). Приемо-передающее оборудование комплекса использует в своей работе цифровую модуляцию COFDM и технологии сжатия MPEG2/MPEG4. Для подобных комплексов передачи видео и звука, функционирующих, как правило, в условиях городской застройки и сложных условиях для организации связи, характерна передача данных с помощью портативного оборудования на расстояние от нескольких сотен метров до километра и более. Подробные характеристики и описание системы передачи видео и звука приведены в [12, 20].

Производим настройку спектроанализатора, указывая следующие параметры:

- ширина полосы частот 30 МГц;
- верхняя частота 440 МГц;
- нижняя частота 470 МГц;
- ширина полосы пропускания 100 КГц.

Схема экспериментального исследования приведена на рис. 1.7.

Первым этапом эксперимента является изучение спектра 3 НКПД и стороннего аналогового радиосредства, работающего в том же частотном диапазоне. Спектрограмма приведена на рис. 1.8.

Рис. 1.7. Схема экспериментального исследования

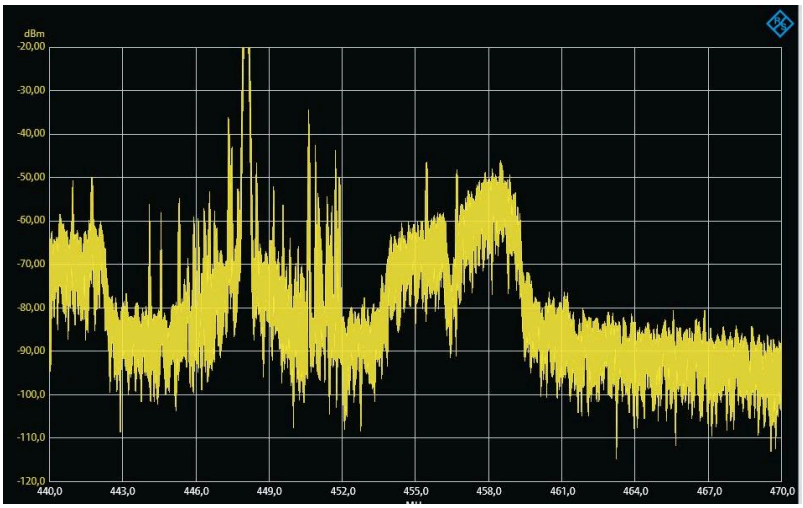


Рис. 1.8. Спектрограмма сигнала трех НКПД и стороннего аналогового радиосредства, настроенного на тот же частотный диапазон

Из спектрограммы видно, что спектр канала, на частоту работы которого настроено стороннее радиосредство, кардинально изменился. В нем появились интермодуляционные составляющие, оказывающие негативное влияние на передаваемый видеосигнал. На ЦПУ наблюдаются искажения видеосигнала и передаваемой речи, которые происходят, пока не прекратится работа стороннего аналогового радиосредства.

Вторым этапом эксперимента является изучение спектра 3 НКПД и стороннего цифрового радиосредства, настроенного на тот же частотный диапазон работы. Спектрограмма приведена на рис. 1.9.

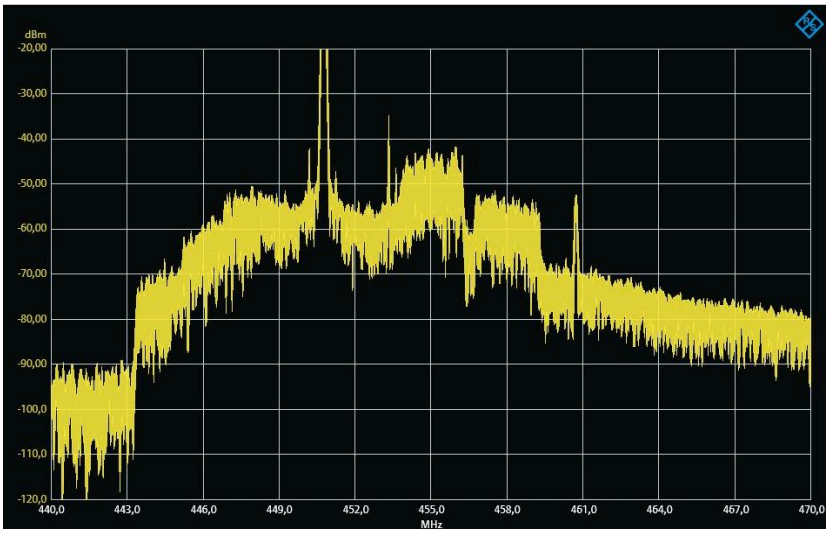


Рис. 1.9. Спектрограмма сигнала трех НКПД и стороннего цифрового радиосредства, настроенного на тот же частотный диапазон

Как видно из спектрограммы, спектр сигнала также очень сильно искажается и происходят интермодуляционные эффекты, но, однако, на ЦПУ не происходит замираний видеосигнала, а спектр периодически принимает нормальную форму. Это объясняется тем, что в цифровой связи используется пакетная передача данных, а между передачей двух пакетов существует определенная пауза. Особенности спектра сигнала связаны с технологией временного разделения TDMA.

На основании проведенного комплекса экспериментальных исследований авторами отработана типовая схема проведения комплекса экспериментальных исследований по воспроизведению деструктивных электромагнитных воздействий доступными лабораторными средствами, которая будет рассмотрена далее.

Типовая схема проведения экспериментальных исследований по воспроизведению деструктивных электромагнитных воздействий на СС СН доступными лабораторными средствами. На основании проведенных экспериментальных исследований по воспроизведению деструктивных электромагнитных воздействий авторами были сделаны некоторые обобщения, в результате которых можно предложить типовую схему экспериментальных исследований при помощи лабораторных средств, состоящую из совокупности функциональных блоков (рис. 1.10).

Средством воспроизведения ДЭМВ является лабораторная экспериментальная установка. В типовую схему экспериментальных исследований входит измерительная система (аппаратура), в нашем случае анализатор спектра, а также адаптеры, интерфейсы, соединительные кабели и элементы антенно-фидерных устройств. В качестве главного интерфейса выступает соединение между анализатором спектра и персональным компьютером. На персональном компьютере содержится база данных

помеховых воздействий [11, 21], а также специализированное программное обеспечение для обработки и фиксации помеховых воздействий.

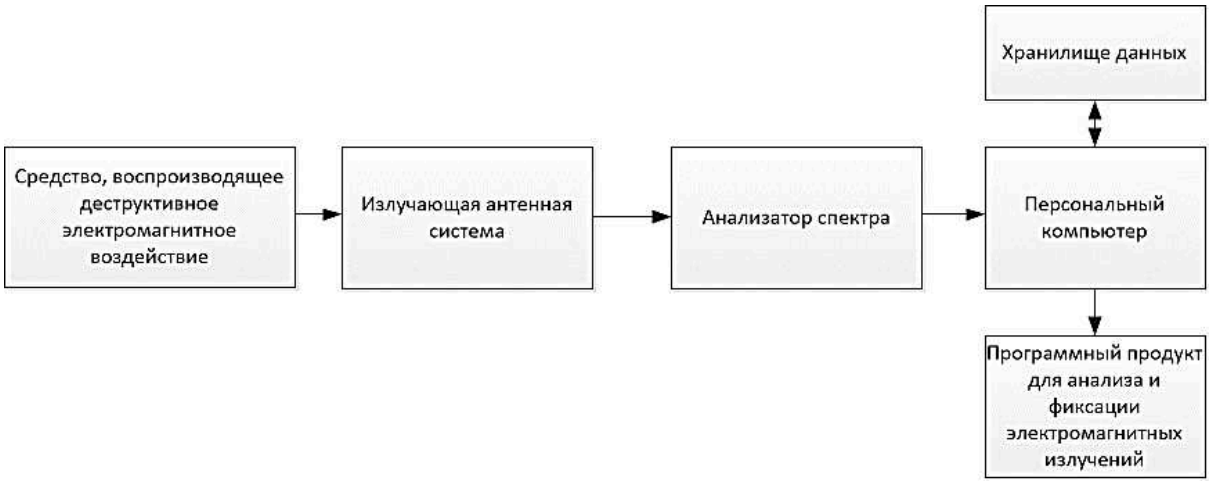


Рис. 1.10. Типовая схема проведения экспериментальных исследований при помощи лабораторных средств

В методических рекомендациях приведена схема проведения экспериментальных лабораторных исследований по воспроизведению электромагнитных воздействий доступными лабораторными средствами. На примере результатов выполненных экспериментальных исследований предложены возможные варианты реализации ДЭМВ, на основе которых получены данные электромагнитных воздействий на аппаратуру СС СН. В качестве средства измерений в проводимом комплексе экспериментальных исследований был использован анализатор спектра FSH 8. Применение подобного рода измерительной техники позволяет произвести детальный анализ и оценить степень воздействия деструктивных электромагнитных воздействий на типовые и перспективные СС СН. Данная схема будет использована авторами в дальнейших исследованиях с целью совершенствования способов противодействия ДЭМВ в СС СН.

1.3. Особенности эксплуатации подвижного узла связи органов внутренних дел при проведении мероприятий по охране общественного порядка и обеспечению общественной безопасности

Подвижные узлы связи предназначены для оперативно-тактического и стратегического звеньев управления и оборудуются в кузове-фургоне автомобиля типа КАМАЗ 43118 или размещаются в контейнере ККЗА.06, который транспортируется всеми видами транспорта [34].

Подвижные узлы связи, кроме приемных аппаратных, комплектуются двухканальными передающими аппаратными. Все аппаратные имеют

системы УКВ радиосвязи, радиостанции радиорелейной связи и могут оснащаться системами спутниковой связи.

Особенностями мобильных узлов связи являются:

– высокая степень автоматизации формирования трактов приема или передачи и автоматическое ведение связи за счет широкого применения средств вычислительной техники;

– значительное, более чем в три раза, сокращение обслуживающего персонала;

– автоматическая маршрутизация принятой информации.

Основными требованиями, предъявляемыми к современным узлам связи, являются:

– использование приемных антенных решеток с цифровым формированием диаграмм направленностей, применение технологий MIMO (Multiple Input Multiple Output) и AAS (Adaptive Antenna Systems);

– широкое внедрение цифровой обработки сигнала – цифровой прием, цифровая обработка принимаемого сигнала, цифровое формирование сигналов манипуляции, использование цифровых линий связи;

– магистрально-модульное построение как аппаратных средств, так и программного обеспечения, которое должно стать основой аппаратной и программной унификации;

– конвергенция различных систем связи.

Достижения в создании цифрового радиооборудования по технологии SDR открывают возможность построения полностью цифровых стандартов связи [43].

Внутриузловая связь в подвижном узле связи реализована на основе цифровых потоков Е1 и n×Е1. Это приводит к смене поколений аппаратуры уплотнения, аппаратуры радиорелейной связи, переходу от проводных линий связи к оптоволоконным.

Многофункциональные подвижные узлы предназначены для оперативно-тактического управления ОВД при проведении оперативных мероприятий.

Назначение подвижного узла связи (ПУС):

– организация связи во время спортивно-массовых мероприятий.

– организация связи при чрезвычайных происшествиях и техногенных катастрофах.

ПУС обеспечивает:

– доставку сотрудников, средств связи и специального оборудования к местам проведения мероприятий по дорогам на дальность до 500 км (без дозаправки);

– автономную работу и отдых персонала (6 человек + водитель) на время проведения работ, в том числе в районах с холодным климатом (до минус 40 °С);

– комфортные бытовые условия за счет наличия систем кондиционирования и отопления;

– организацию в УКВ диапазоне конвенциональной радиосвязи.

– организацию связи в стандарте APCO 25 и DMR;

– организацию спутниковой связи на базе оборудования с российской орбитальной группировкой «Ямал»;

– организацию сотовой связи при помощи СБМ-репитера;

– организацию офисных функций, документального обмена и видеоконференцсвязи (телефон, АРМ оператора в защищенном исполнении, принтер, сканер, ПО ВКС);

– сопряжение средств связи изделия с узлами опорной транспортной сети различных операторов посредством спутникового или проводного канала связи (на основе стандартных стыков);

– электропитание от сети или бесперебойное питание от автономного источника электроэнергии (электростанция или аккумуляторы);

– освещение мест проведения оперативных или аварийно-восстановительных работ;

– звуковое оповещение через рупорные громкоговорители.

Рис. 1.11. Подвижный узел связи

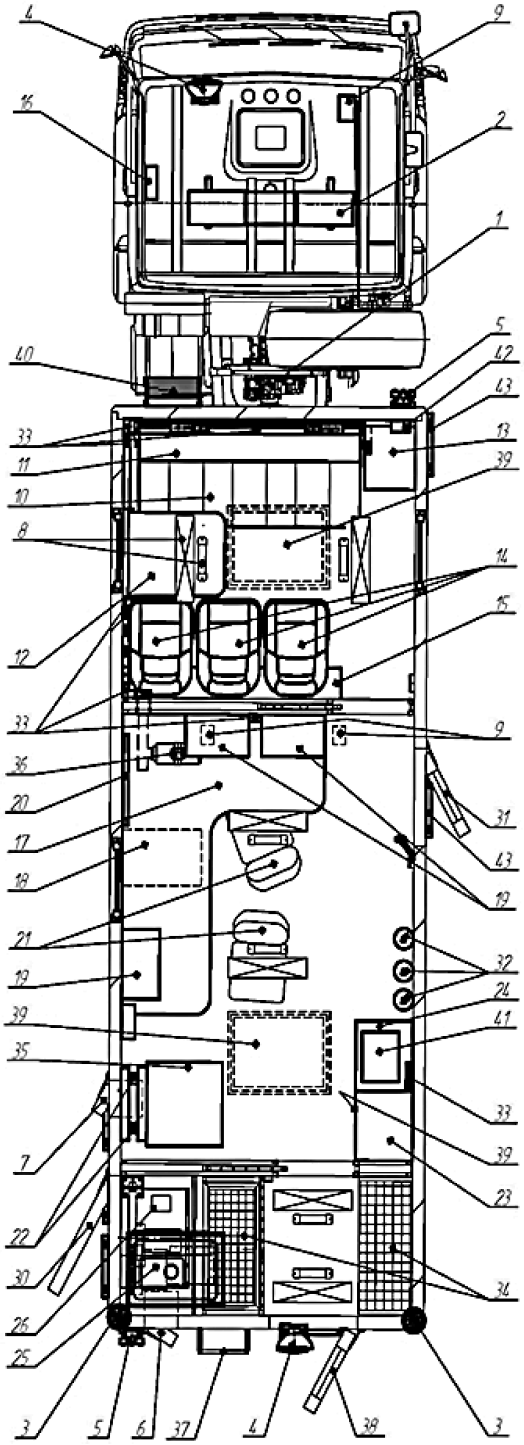
Подвижные узлы связи (ПУС) модели 5027 разработаны для органов внутренних дел Российской Федерации, входят в состав системы связи МВД России и предназначены для организации связи при работе как на стоянке, так и в движении, а также для оперативного взаимодействия в чрезвычайных ситуациях, при обеспечении охраны общественного порядка

и безопасности в рамках проведения массовых и международно-значимых мероприятий [34].

Таблица 1.4. Основные характеристики ПУС

Характеристика	Значение
Шасси	КАМАЗ-43118 (3 х-осный)
Колесная формула	6х6
Экипаж	до 6 человек
Тип мачты	Телескопическая, безоттяжечная
Высота мачты	более 12 м
Способ развертывания мачты	Автоматизированный (электропривод)
Кузов-фургон	Изотермический, с 3 отсеками: отсек связи; оперативный отсек; хозяйственный отсек
Поддерживаемые виды связи	Конвенциональная радиосвязь в диапазонах ОВЧ и УВЧ Связь в стандарте APCO 25 Связь в стандарте DMR Связь в стандарте DECT Спутниковая связь в ССС «Ямал» Связь GSM Связь по кабельным линиям (оптические и медные) Система широкополосного доступа Wi-Fi
Система видеонаблюдения	4 выносных автономных поста видеонаблюдения и видеосервер
Специальное имущество	Противогазы, респираторы, защитные костюмы, дозиметры, экспресс-лаборатория, газоанализатор, бинокль, фонарь, конусы ограждения, сигнальная лента, вехи, шанцевый инструмент и пр.
Коммутационное ядро	Маршрутизатор с интерфейсами Ethernet, E&M, FXS, E1
Размещение основного оборудования связи и электропитания	2 телекоммуникационных шкафа стандарта 19”
Хозяйственно-бытовые средства	Бак с водой, мойка, проточный водонагреватель, холодильник, СВЧ-печь, электроплита, хоз. шкафы, телевизор
Температура окружающей среды	-40...+50 °С

Подвижный узел связи модели 5027А1 на базе автомобиля с колесной формулой 6х6 (далее – базовое транспортное средство) ТУ 6530-001-17985721-2013 принят на снабжение органов внутренних дел Российской Федерации в соответствии с приказом МВД России от 15.07.2016 № 394дсп. Технические характеристики ПУС модели 5027А1 должны соответствовать требованиям ТУ 6530-001-17985721-2013 и комплекта конструкторской документации, имеющей литеру «01» [34].



Поз.	Наименование	Кол.
1	Базовое шасси КАМАЗ 43118	1
2	СГУ	1
3	Фонарь проблесковый	2
4	Фара-искатель	2
5	Мачта телескопическая	2
6	Люк вводной линий связи и подключений АФУ	1
7	Люк бортового ввода	1
8	Освещение рабочее, аварийное	6
9	Устройства подъема антены	3
10	Стол-трансформер	1
11	Полка спальная откидная	1
12	Стол выдвижной	1
13	Шкаф с дверцей "жалюзи"	1
14	Сидения на сдвижном механизме	3
15	Ящик под антены	1
16	Переговорное устройство кабины	Компл.
17	Рабочий стол Г-образный	1
18	Тумба трехсекционная	1
19	Полка	3
20	Телевизор на кронштейне	1
21	Кресло рабочее	2
22	Кронштейны-амортизаторы приборов КРТК	Компл.
23	Шкаф для одежды с антресолью	1
24	Тумба	1
25	Электроагрегат дизельный	1
26	Кондиционер автомобильный	1
30	Дверь агрегатного отсека	1
31	Дверь рабочего отсека	1
32	Огнетушитель	3
33	Кабель-каналы	компл.
34	Полка грузового отсека	компл.
35	Прибор КРТК	1
36	Отопитель автономный	1
37	Лестница техническая	1
38	Дверь грузового отсека	1
39	Люк эвакуационный	2
40	Лестница съёмная	1
41	МФУ	1
42	Переговорное устройство опер. отсека	1
43	Кронштейн фиксации лестниц съемных	6

Рис. 1.12. Компоновка ПУС 5027А1

Перечень принятых сокращений

АЗОУ – автоматическое защитное отключающее устройство
АКБ – аккумуляторная батарея
АРМ – автоматизированное рабочее место
АТС – автоматическая телефонная станция
АФУ – антенно-фидерное устройство

ВП – военная приемка
ГСМ – горюче-смазочные материалы
ДЧ УВД – дежурная часть управления внутренних дел
ЗИП – запасные части, инструменты и принадлежности
ЗУ – заземляющее устройство
ИМТС – интегрированная мультисервисная телекоммуникационная система
ИБП – источник бесперебойного питания
ИЭЭ – источник электрической энергии
КД – конструкторская документация
ЛЭП – линия электропередач
МБ – местная батарея
МВД – министерство внутренних дел
МО – министерство обороны
МФУ – многофункциональное устройство
ОВД – орган внутренних дел
ОВЧ – очень высокие частоты
ОТУ – общие технические условия
ПД – передача данных
ПЗ – представительство заказчика
ПКИ – постоянный контроль изоляции
ЭППС – экструдированный пенополистирол
ПУС – подвижный узел связи
ПЭВМ – персональная электронно-вычислительная машина
РС – радиостанция
РЭ – руководство по эксплуатации
СГУ – сигнально-громкоговорящая установка
СОЭ – система обеспечения электробезопасности
СЭС – система электроснабжения
СХОСС – схема организации спутниковой связи
ТЗ – техническое задание
ТЛФ – телефонный (ая)
ТО – техническое обслуживание
ЕТО – ежедневное техническое обслуживание
ТО-1(2) – первое (второе) техническое обслуживание
ТУ – технические условия
ТД – техническая документация
УВЧ – ультравысокие частоты
ЩР0 – щиток переносной распределительный
ЭМС – электромагнитная совместимость
ЭД – эксплуатационная документация

ПУС модели 5027А1 должен быть рассчитанным на эксплуатацию, сохранять работоспособность и свои технические характеристики в районах с умеренным и холодным климатом по ГОСТ 15150 при следующих условиях:

– температура окружающей среды в диапазоне от минус 40 до плюс 40°С включительно;

– атмосферное давление в диапазоне от 60 до 107 кПа включительно;

– относительная влажность 98%, при температуре плюс 25°С.

На стоянке ПУС мод. 5027 обеспечивает:

– организацию сетей оперативной радиосвязи (13 каналов связи) в ОВЧ, УВЧ диапазонах с обеспечением режима ретрансляции в используемых в МВД России и других ведомствах и структурах как аналоговых, так и цифровых стандартах DMR, APCO 25, iDAS с возможностью выхода в данные радиосети с рабочих мест ПУС, включая рабочее место старшего машины в кабине водителя;

– организацию взаимодействия радиообмена как отдельных групп, так и всех абонентов в единой радиосети, включая водителя и старшего машины;

– организацию коммутации на АРМ «Диспетчер» групп и абонентов, работающих в ОВЧ, УВЧ диапазонах аналоговых и цифровых стандартов DMR, APCO 25, iDAS, посредством модуля «Коммутация» АРМ «Диспетчер» и радиошлюзов;

Рис. 1.13. Организация радиосвязи при ЧС на базе АРМ «Диспетчер»

– организацию записи переговоров посредством АРМ «Диспетчер»;

– организацию спутникового направления связи с возможностью обеспечения одного голосового или одного канала передачи данных;

– коммутацию сформированных каналов связи на терминальные оконечные устройства, размещённые непосредственно в изделии;

– возможность обмена информацией с оконечных устройств рабочего места старшего машины в кабине водителя;

– оперативное документирование, обработку и передачу информации;

– определение местоположения на местности с помощью средств навигации;

– подключение кабельной линии для приема внешних каналов связи и взаимодействия с ИМТС ОВД МВД России;

– передачу данных, формируемых с использованием переносной персональной электронно-вычислительной машины (ноутбука) по каналам, образованным средствами связи из состава изделия.

Рис. 1.14. Межведомственная связь

При возникновении чрезвычайной ситуации задачи решают обычно несколько разных ведомств. Каждая группа (МЧС, ФСБ, полиция, «скорая помощь» и т.п.) использует свое радиооборудование, которое часто несовместимо с оборудованием других групп.

Координацию действий разных групп на месте ЧС возможно осуществлять, используя командно-штабную машину (КШМ), оборудованную системой «Радиокупол» [34].

Организация, имеющая КШМ, оборудованную системой «Радиокупол», играет важную роль при ликвидации ЧС. При этом производится запись всех радиопереговоров и после ликвидации ЧС возможно провести ее разбор и анализ, опираясь в том числе на записи радиопереговоров.

Рис. 1.15. Схема межведомственной организации радиосвязи при организации движения в колонне

В движении ПУС мод. 5027 одновременно или выборочно обеспечивает:

– образование радиоканалов в УВЧ и ОВЧ диапазонах в цифровых стандартах радиосвязи DMR, APCO 25, iDAS и аналогах с коммутацией образованных каналов связи на оконечные терминальные устройства, размещённые непосредственно в изделии, а также спутникового направления связи с возможностью обеспечения одного голосового или одного канала передачи данных;

– обмен информацией с оконечных устройств рабочих мест в режимах симплексной УВЧ и ОВЧ цифровой и аналоговой радиосвязи с возможностью выбора стандарта посредством диспетчерской консоли;

– организацию записи переговоров посредством АРМ «Диспетчер»;

– циркулярную коммутацию на АРМ «Диспетчер» необходимых групп и абонентов, работающих в ОВЧ, УВЧ диапазонах аналоговых и цифровых стандартов DMR, APCO 25, iDAS, посредством модуля «Коммутация» АРМ «Диспетчер» и радиошлюзов;

– определение местоположения на местности с помощью средств навигации.

Специальное транспортное средство ПУС мод. 5027 производится на базе автомобиля фургонной компоновки типа ГАЗель NEXT A32R32 (мод. 5027G) или FORD SOLLERS SB-LF (4x4) российской сборки, а также может изготавливаться и дооборудоваться кузов-фургон с установкой на шасси КАМАЗ 43502 (4x4) или КАМАЗ 43118 (6x6) мод. 5027А1.

Подсистема связи, телекоммуникации, управления, документирования и отображения информации ПУС мод. 5027 включает:

1. Интегрированный модуль оперативного управления (ИМОУ) в составе:

− радиостанции возимые ОВЧ диапазона (аналоговая, DMR, iDAS) – 3 шт. и УВЧ диапазона (аналоговая, DMR, iDAS, APCO 25) – 4 шт.;

− радиостанции-ретрансляторы стационарно-перевозимые ЦРР-25 УВЧ-диапазона (APCO 25) и ЦРР-25 УВЧ-диапазона (DMR);

− дуплексер УВЧ диапазона – 2 шт.;

− радиошлюз (2 шт.) для подключения до 70 IP-каналов;

− цифровой декодер голоса – 3 шт.;

− универсальный телекоммуникационный маршрутизатор 24-портовый;

− пульт удаленного управления по IP-сети (консоль диспетчерская).

Рис. 1.16. Рабочее место оператора ПУС

2. Комплекс аппаратуры ретрансляции и телекоммуникации блочно-модульного исполнения (КАРТК) в составе:

− радиостанции-ретрансляторы ОВЧ и УВЧ-диапазона (iDAS);

− дуплексеры ОВЧ и УВЧ-диапазона;

− радиошлюз для подключения до 20 IP-каналов;

− универсальный беспроводный маршрутизатор 8-портовый;

− многофункциональный автономный преобразователь напряжения (МАП);

− источник бесперебойного питания;

− блоки: преобразования напряжения (инвертор), ввода резерва, распределения переменного тока и постоянного тока;

− модуль вентиляторный.

Рис. 1.17. Комплекс аппаратуры ретрансляции и телекоммуникации блочно-модульного исполнения (КАРТК)

3. АРМ «Диспетчер» с модулями «Коммутация» и «Запись переговоров», программаторы цифровых базовых и абонентских радиостанций IDAS, носимых, возимых радиостанций аналоговых и стандарта DMR системы «Радиокупол», возимых радиостанций аналоговых и стандарта DMR типа «ЭРИКА», возимых радиостанций стандарта APCO 25.

4. Пульт удаленного управления по IP-сети (консоль диспетчерская) настольного исполнения – 2 шт., радиостанции носимые: УВЧ-диапазона (аналог/DMR) – 1 шт., ОВЧ-диапазона (iDAS) – 10 шт., УВЧ-диапазона (iDAS) – 10 шт. в кассетах оперативного отсека и зарядное устройство шестиместное для радиостанций ОВЧ и УВЧ диапазона (iDAS) в отсеке оператора связи.

5. Радиостанцию возимая ОВЧ диапазона (стандарта iDAS) и носимую ОВЧ-диапазона (стандарта аналог/DMR) в кабине водителя.

6. Антенны возимые, автомобильные ОВЧ и УВЧ диапазона на врезном основании, установленные на приводах крепления и подъема антенн – 5 шт., типа «Шайба-2» – 3 шт.

7. Антенны базовые РАДИАЛ D1 – 3 шт. и комплекса «Спрут» АБ – 1 шт. с комплектом ВЧ-кабелей для установки на телескопические мачты.

8. Телескопические мачты с пневмоприводом от компрессора – 2 шт.

9. Спутниковый телефон носимый и стационарный терминал спутниковой связи Iridium.

10. Усилитель сигнала и телефон сотовой связи (на 2 SIM-карты).

11. Многофункциональное устройство XEROX WorkCentre.

12. Телевизионный приемник (диагональ экрана 22"), ПЭВМ (ноутбук HP), диагональ экрана 15,6", телефонный аппарат Panasonic KX-TS в оперативном отсеке, катушку с телефонным кабелем (500 м) в грузовом отсеке.

Подсистема электроснабжения ПУС мод. 5027 обеспечивает подключение:

– от внешнего однофазного источника (электрической сети общего назначения напряжением 220 В) через переносной щиток распределительный (ЩР0);

– от штатного автономного выносного дизельного электроагрегата (220 В, 6 кВт) с комплектом силовых кабелей (на катушках 25 м – 2 шт., 3 м – 3 шт.);

– от дополнительных аккумуляторных батарей (12 В, 115 А/ч);

– 2 шт.; от бортовой сети базового автомобиля.

Подвижный узел связи (ПУС) модели 5027G (рис. 1.18) на базе автомобиля «Газель NEXT» разработан для органов внутренних дел Российской Федерации, входит в состав системы связи МВД России и предназначен для организации связи при работе как на стоянке, так и в движении, а также оперативного взаимодействия в чрезвычайных ситуациях, при обеспечении охраны общественного порядка и безопасности в рамках проведения массовых и международно-значимых мероприятий.

Рис. 1.18. Подвижный узел связи (ПУС) модели 5027G

ПУС соответствует требованиям технических условий ТУ 6530-001-17985721-2013, согласованным с ДИТСиЗИ МВД России, и комплекта конструкторской документации ЯИЖН.465225.006 литеры О1.

Подвижный узел связи МОД. 5027G ПУС построен на базе транспортного средства «Газель NEXT» мод. А32R32 с характеристиками: колесная формула 4х2; ведущие колеса – задние; цельнометаллический фургон утепленный; размеры грузового отсека кузова фургона, мм: длина – 3630; ширина – 1860; высота – 1930; двигатель дизельный, мощность, кВт – 110; максимальная скорость, км/ч – 110.

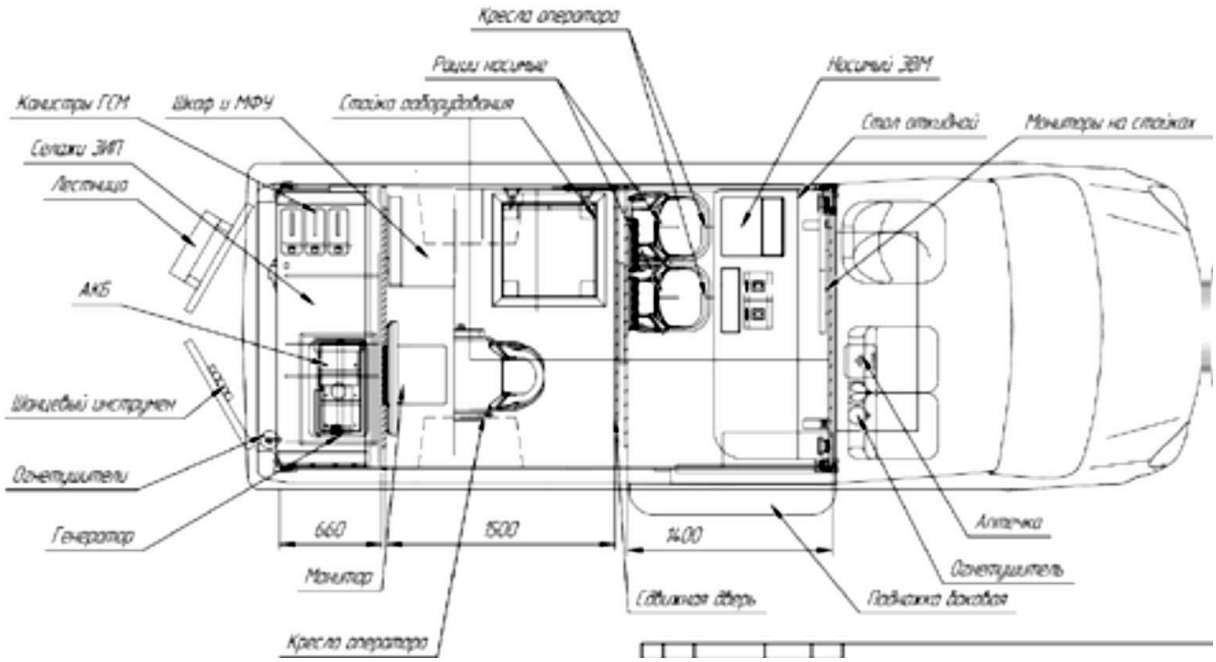


Рис. 1.19. Компоновка ПУС 5027G

Конструктивно ПУС состоит из кабины водителя и трех отсеков: оперативного отсека, рабочего отсека оператора связи и агрегатного отсека, разделенных перегородками и предназначенных под монтаж и перевозку оборудования, организацию рабочих мест для обеспечения обмена данными, телефонной, текстовой и видеоинформацией по каналам связи, образованным штатными средствами связи.

ПУС оснащен выдвижными аутригерами для фиксации кузова фургона на местности. На крышевой платформе кузова фургона размещены антенно-мачтовые системы с фиксацией телескопических мачт растяжками к аутригерам кузова.

Появляются новые требования – нормируется время развертывания и свертывания радиоузла, определяемое в настоящее время временем развертывания и свертывания антенн. Использование приемной и передающей антенных решеток для мобильного радиоузла еще более актуально, так как снижается время развертывания и свертывания. Использование цифровых радиоприемных устройств и цифрового

фазирования антенн позволяет не только повысить параметры приемных трактов, но и снизить вес аппаратуры.

1.4. Анализ некоторых уязвимостей информационной безопасности системы беспроводной связи стандарта DMR

В настоящее время для обеспечения двусторонней защищенной радиосвязи широко применяются системы цифровой беспроводной связи, которые активно сменяют более старые – аналоговые. К распространенным стандартам для построения цифровой беспроводной связи относятся DMR, TETRA, APCO-25 и др. Данные стандарты профессиональной беспроводной связи обладают большим количеством предоставляемых абонентам сервисов, обеспечивают более качественную голосовую связь, а также используют помехоустойчивое кодирование. Трафик голоса и данных при этом должен быть защищен от несанкционированных воздействий. В то же время в реализации таких систем имеется ряд слабых мест, которые могут как способствовать утечке информации в сторону пассивного наблюдателя-перехватчика, так и позволят нарушителям проводить эффективные активные атаки.

Подробнее рассмотрим стандарт DMR. Стандарт цифровой профессиональной беспроводной связи Digital Mobile Radio (DMR) позволяет осуществлять плавный переход от аналоговых систем беспроводной передачи к цифровым, поддерживая смешанный режим функционирования. В состав оборудования системы беспроводной связи стандарта DMR входят носимые, стационарные и мобильные средства радиосвязи, а также ретрансляционное оборудование, объединенное в единую сеть (рис. 1.20).

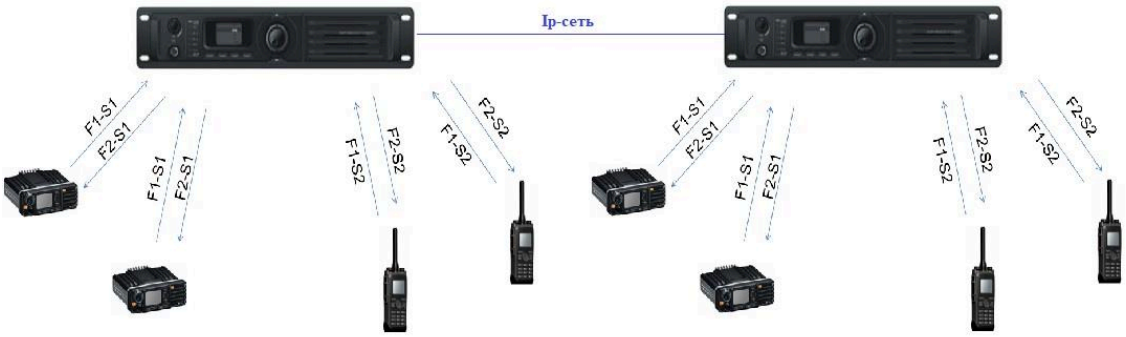


Рис. 1.20. Состав оборудования, входящего в систему беспроводной связи стандарта DMR

Оборудование стандарта DMR работает в типовых частотных диапазонах, таких как VHF и UHF. Стандарт DMR представляет собой структуру таймслотов с длительностью 30 миллисекунд. В этом промежутке

времени 27,5 мс предназначаются непосредственно для полезной информации, кодируемой 216-ю битами, а остальное время – 48 битов служебной информации [38, 40, 43, 44]. Стандарт предоставляет абонентом большое количество сервисов, среди которых возможность удаленного контроля, блокировка утерянных радиосредств, возможность одновременной передачи речи и данных, отправка коротких сообщений, осуществление вызовов на стационарные средства телефонии, шифрование данных и др. Однако, стандарт не лишен потенциальных уязвимостей передаваемой информации, которыми могут воспользоваться нарушители, тем самым нанеся ущерб информационной безопасности трафика, например, кодированных сообщений. Так же требуется отметить, что существенная доля «кодированного» трафика, на самом деле может передаваться операторами в открытом виде, несмотря на то что их пользователи были уверены в кодировании сообщений, что также может приводить к утечке важной информации.

Рассмотрению возможных уязвимостей стандарта DMR посвящена данная статья.

Уязвимость, заключающаяся в нарушении целостности и доступности передаваемой информации посредством деструктивного воздействия. В соответствии с [36] одним из факторов воздействующим на передаваемую информацию и вызывающим ее искажение или блокирование является деструктивное воздействие. Злоумышленник может осуществить генерацию деструктивного воздействия при помощи специально изготовленных средств генерации. При этом уровни деструктивных воздействий определяются в соответствии ГОСТ Р 52863-2007 [1].

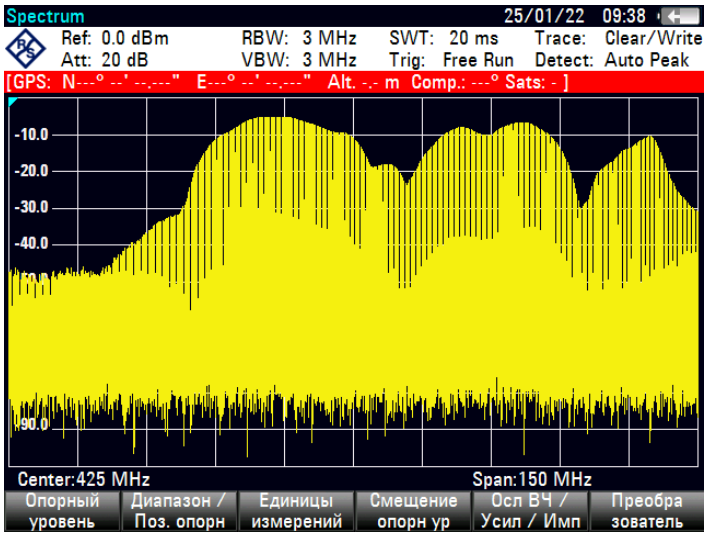


Рис. 1.21. Спектр возможного деструктивного воздействия, оказываемого на систему беспроводной связи стандарта DMR

С целью проверки данной уязвимости вторами в работах [41, 42] произведено воспроизведение подобного деструктивного воздействия. Один из примеров экспериментального спектра приведен на рис. 1.21. Как видно из рис.2 спектр деструктивного воздействия распределен от 380 до 485 МГц, что соответствует частотному диапазону функционирования системы связи стандарта DMR. Подобное воздействие может вызывать разрушение, искажение или блокирование передаваемой информации, если будет превышено значение показателя BER, рассмотренного в [37]. Следует также отметить, что средства генерации подобных воздействий могут управляться правонарушителями дистанционно, за счет чего может существенно осложнится поиск как самих устройств, так и лиц их использующих.

Уязвимость, заключающаяся в перехвате (прослушивании) передаваемых голосовых сообщений. Осуществление перехвата (прослушивания) нешифрованных передаваемых голосовых сообщений возможно осуществить достаточно простыми и доступными средствами, чем могут воспользоваться нарушители. Для этого ими может быть использован программно-определяемы приемник Software Defined Radio (SDR) и свободно распространяемое программное обеспечение. Под SDR будем понимать радиопередатчик и/или радиоприёмник, использующий технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, используемых в ходе обычной предварительно определённой работы с предварительными установками радиоустройства, согласно той или иной спецификации или системы [46]. Существую различные варианты реализации таких приемников, например, HackRF, RTL SDR, Lime SDR и др. Типовыми частотами приема и передачи являются 24-2000 МГц. Схема подключения для осуществления перехвата (прослушивания) переговоров нарушителями приведена на рис. 1.22.

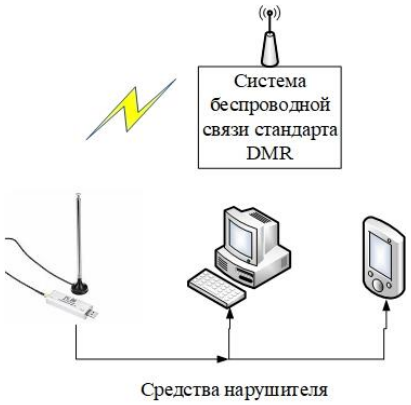


Рис. 1.22. Схема возможного перехвата (прослушивания) переговоров беспроводной связи стандарта DMR

Нарушитель, используя SDR-приемник и программное обеспечение, установленное на персональный компьютер или смартфон имеет возможность перехвата (прослушивания) нешифрованной передаваемой информации, что может привести к разглашению различного рода сведений, которые становятся доступными. Помимо перехвата (прослушивания) информации, нарушитель может получать другие сведения о системе беспроводной связи, приведенные на рисунке 1.23.

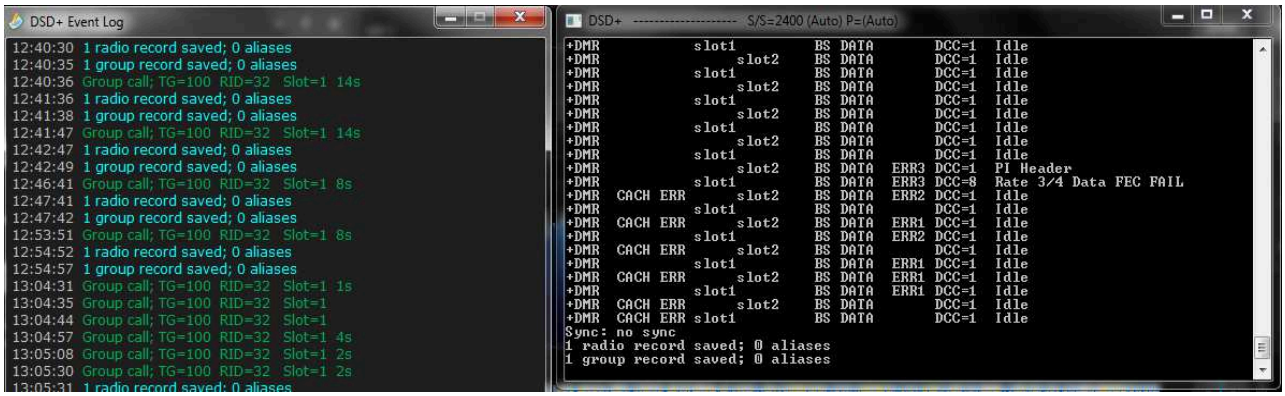


Рис. 1.23. Сведения, получаемые во время прослушивания переговоров беспроводной связи стандарта DMR

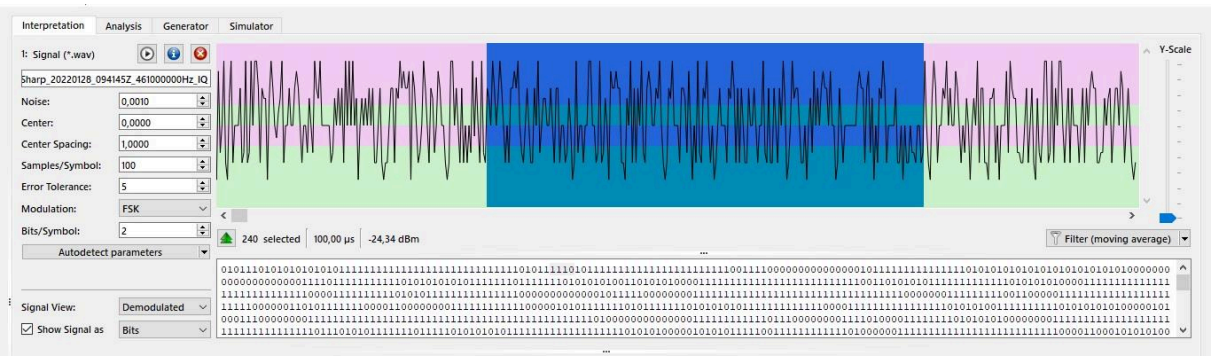
Как видно из рисунка 1.23. нарушитель получает полную информацию о сети беспроводной связи, а именно: какая информация передается (голос, данные), идентификаторы передающих радиосредств, время совершения вызова, тип совершения вызова (групповой, индивидуальный), параметры FEC, информацию о структуре сети и др. Обладая подобной информацией нарушитель сможет клонировать радиосредство и использовать его в качестве легального пользователя в сетях беспроводной передачи данных стандарта DMR, тем самым приведя к дезорганизации работы всей сети.

Уязвимость, заключающаяся во внедрении ложных голосовых сообщений.

Нарушитель, используя арсенал средств, описанных выше может также осуществить запись и анализ передаваемых в сети беспроводной связи стандарта DMR информационных пакетов рис. 1.24.

В результате возможно выполнение неправильных действий пользователями сети беспроводной передачи данных, а также постоянное внедрение данного информационного сообщения может привести к искажению или блокированию информационного обмена между пользователями сети.

На основании записанного информационного обмена возможно произвести оценку передаваемых битов данных, выделить



пакеты, передаваемые информацию и излучать данное информационное сообщение.

Рис. 1.24. Анализ передаваемых пакетов беспроводной связи стандарта DMR

Методы устранения уязвимостей, возникающих в процессе функционирования системы беспроводной связи стандарта DMR.

В качестве устранения первой уязвимости предлагается предусмотреть возможность перехода радиооборудования на другой диапазон если используется UHF то предусмотреть резервный канал в VHF и наоборот. Кроме этого радиостанция DMR может быть дополнена возможностью работы в стандартах 4G и WiFi (Motorola Ion – Multi-Mode Radio: Analog/DMR/LTE/Wi-Fi). В связи с этим, радиостанция комплектуется дополнительными модулями связи, а также в ее состав могут входить программные средства шифрования.

Для устранения второй и третьей уязвимостей предлагается использовать шифрование. В зависимости от требований конфиденциальности предъявляемых к передаваемой информации механизмы шифрования могут быть двух типов – базовое и полное.

Функция базового шифрования в стандарте DMR позволяет защитить передаваемые голосовые сообщения и данные от несанкционированного прослушивания и передачи сообщений. Тип шифрования может выбираться пользователем радиооборудования в зависимости от предъявляемых требований конфиденциальности передаваемой информации. Значение ключа шифрования свободно настраивается. При повышенных требованиях к информационной безопасности предусмотрены следующие виды криптозащиты: с 16 битным, 40 битным, 128 битным и 256 битным ключами шифрования. Базовое шифрование – это метод шифрования, который выполняет простые математические манипуляции ключом шифрования применительно к полезной передаваемой информации (голосовые и текстовые сообщения). Стоит учитывать, что базовое шифрование не использует сложные математические алгоритмы, такие как AES или потоковый шифр ARC4 для защиты информации. Шифрование ключами до 256 бит за счет большого количества комбинаций ключей позволяет обеспечить приемлемый уровень защищенности канала связи и

предотвратить прослушивание. Ключ шифрования устанавливается в радиоустройстве при его программировании и его не требуется передавать по радиоканалу [5, 11]. С учетом этого система шифрует и дешифрует передаваемые голосовые сообщения, не затрачивая на это дополнительное время. Ключ играет важную роль в шифровании. Рекомендуется настраивать уникальный ключ, который после преобразования в двоичное значение имеет не менее пяти битов отличных от других ключей. На рисунке 1.25 приведен базовый рабочий процесс шифрования в стандарте DMR.

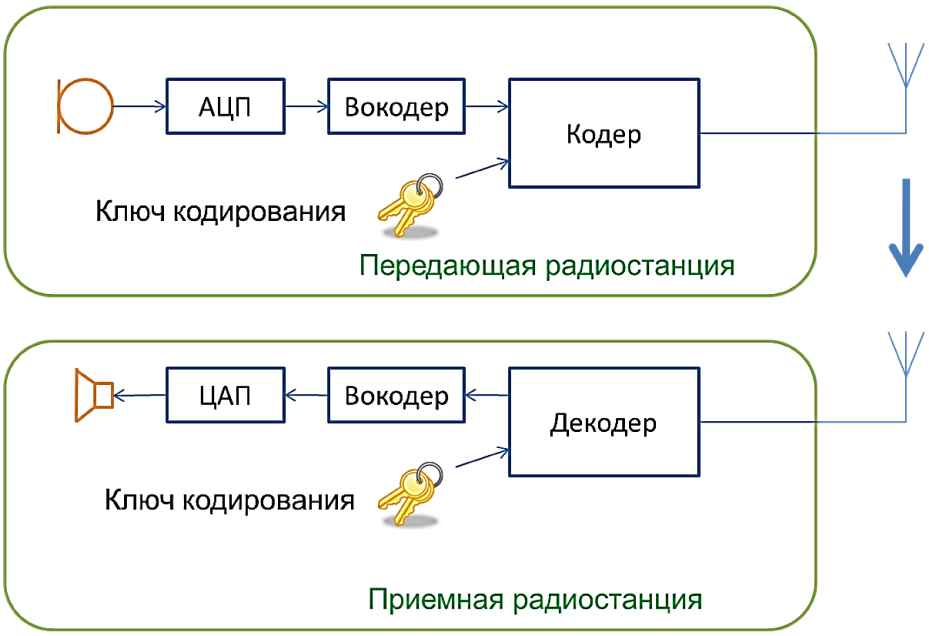


Рис. 1.25. Базовый рабочий процесс шифрования в стандарте DMR

Функция полного шифрования может обеспечить усиленную защиту при передаче голоса и данных. Обеспечение конфиденциальности реализуется на основе алгоритмов шифрования AES и ARC4. Этот механизм заключается в выборе типа ключа (40 бит, 128 бит и 256 бит) и значения ключа. 40-битный ключ использует ARC4 для генерации ключевого потока для преобразования голоса или данных, в то время как 128-битный или 256-битный ключ использует AES для преобразования голоса или данных. Такие ключи генерируют различные ключевые потоки для каждого голосового суперкадра или пакета данных, что предотвращает дешифровку сообщений злоумышленником путем захвата голоса или пакетов данных в радиоэфире.

Во время генерации ключа эти две технологии будут генерировать разные ключи. В этом механизме для отправки параметров шифрования требуется дополнительный заголовок, и это увеличивает время доступа к системе примерно на 60 мс. Время передачи также может быть увеличено из-за информации, связанной с шифрованием, встроенной в голосовой суперкадр.

Эти два механизма шифруют только голос и данные и не используются при дополнительных функциях системы связи стандарта DMR (радио включение/радио выключение, удаленный мониторинг, оповещение и т. д.).

В настоящее время доступно три режима передачи зашифрованных данных.

1) Прямой режим. В этом режиме терминалы связываются друг с другом напрямую по воздуху. Вы можете воспроизводить полученный зашифрованный голос через динамик и передавать зашифрованный голос.

2) Режим ретранслятора. При передаче данных радиостанции по воздуху ретранслятор может контролировать данные, даже если они зашифрованы. Кроме того, ретранслятор может передавать зашифрованные голосовые сигналы.

3) Режим многосайтового IP-подключения. В этом режиме зашифрованные данные могут передаваться через ретранслятор, IP-сеть или по воздуху. Поддерживается только сквозное шифрование/дешифрование данных. В режиме IP Multi-site Connect ретранслятор и IP-сеть предназначены для передачи данных. Радиостанции, и ретранслятор могут расшифровывать полученные данные и передавать зашифрованные данные. рис. 1.26.

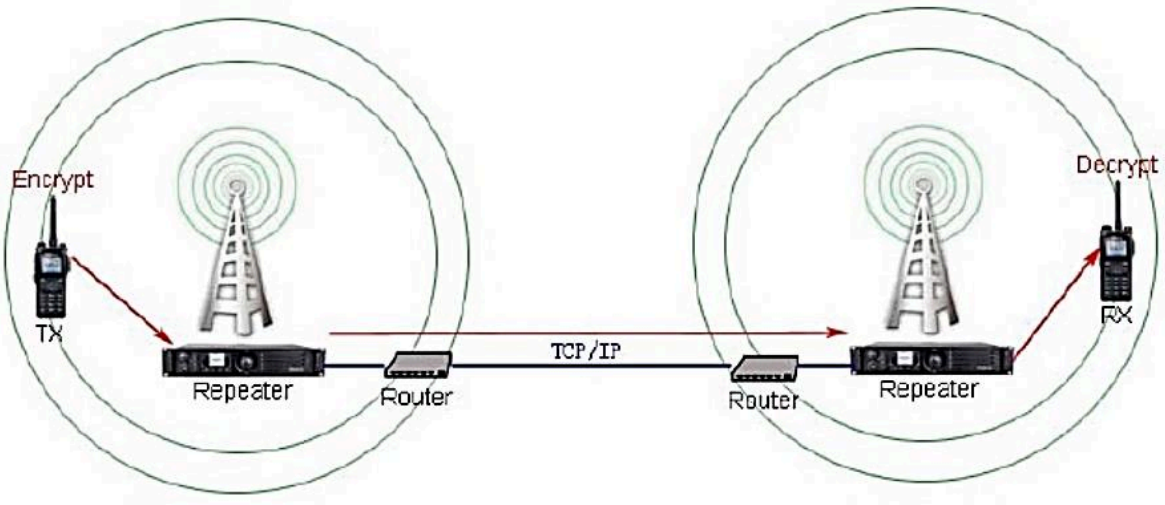


Рис. 1.26. Зашифрованная передача данных в режиме многосайтового IP-подключения

При практическом использовании системы беспроводной связи стандарта DMR имеющиеся базовые механизмы шифрования могут быть дополнены отчуждаемым модулем криптографической защиты информации, поскольку базовое шифрование непарностью обеспечивает защиту передаваемых данных и сведений о сети беспроводной связи. Данный модуль может быть выполнен в качестве micro SIM или micro SD-карты. В настоящее время разработаны специальные SIM-карты и

специализированные изделия в форм-факторах SD – карт серийного производства. Эти микросхемы могут эффективно заменить маскираторы, применяемые в средствах УКВ радиосвязи.

Таким образом, были исследованы некоторые уязвимости системы беспроводной передачи данных стандарта DMR, которые могут быть реализованы нарушителем. На практике операторы системы беспроводной передачи данных не всегда используют шифрование, однако не следует забывать об этой важной организационно-технической функции. В связи с этим, предложены возможные направления для дальнейшего устранения данных уязвимостей.

1.5. К вопросу об уязвимостях систем управления и передачи данных беспилотных летательных аппаратов

Мировой опыт развития беспилотных летательных аппаратов (БПЛА), показывает эффективность их применения и существенные перспективы развития во многих областях человеческой жизнедеятельности. Сегодня БПЛА могут быть использованы для решения достаточно широкого круга задач, вот лишь некоторые из них: наблюдение, картографирование, переброска грузов, оповещение, целеуказание, ретрансляционное оборудование, а также средств радиоподавления и др. К преимуществам БПЛА могут быть отнесены: дистанционный режим управления, возможность транспортировки полезной нагрузки, высокая мобильность и скрытность. Вместе с тем, они не лишены недостатков в виде: низкой скрытности каналов управления, ограниченность полезной нагрузки, сравнительно небольшая дельность при отсутствии средств ретрансляции и др [47, 48, 52, 64].

В территориальных подразделениях МВД России БПЛА используются с целью фиксации правонарушений, проведении следственных и оперативно-розыскных действий, поиска пропавших людей и скрывающихся преступников и др.

Таким образом, использование БПЛА является важным фактором для повышения оперативности реагирования и как следствие наиболее эффективного функционирования органов правопорядка.

Стоит отметить, что в настоящее время вопросы борьбы с БПЛА правонарушителей, а также информационная безопасность ведомственных БПЛА носят особенное значение, поскольку существуют средства, при помощи которых нарушители могут подавить каналы управления и передачи данных ведомственных БПЛА [53, 54]. Теме обеспечения информационной безопасности беспилотных летательных аппаратов МВД России будет посвящена эта статья.

Беспилотные летательные аппараты на службе МВД России. В МВД России в настоящее время ни один тип беспилотных летательных аппаратов не принят на снабжение, так как основным эксплуатантом беспилотных летательных аппаратов определена Федеральная служба войск национальной гвардии Российской Федерации. Однако, прописанные в положение о центрах информационных технологий, связи и защиты информации МВД России обязанности должностных лиц в скором времени будут дополнены с учетом необходимости применения ведомственных БПЛА, а также противодействию БПЛА правонарушителей.

Так, например, в ГИБДД БПЛА применяются для:

– фиксации нарушений правил дорожного движения;

– поиска угнанных транспортных средств;

– поиска транспортных средств, скрывшихся с места дорожно-транспортного происшествия и др [51].

Согласно Российской классификации, в МВД России применяются легкие БПЛА малого и среднего радиуса действия. Некоторые модели таких БПЛА приведены на рисунке 1.27. К ним можно отнести:

1. DJI Inspire 2;
2. ZALA 421;
3. Dji phantom 4 pro [10-14].

а) б) в)

Рис. 1.27. БПЛА а) DJI Inspire 2, б) ZALA 421, в) Dji phantom 4 pro.

Выявление возможных уязвимостей каналов управления и передачи данных беспилотных летательных аппаратов МВД России. Стоит отметить, что БПЛА также могут быть использованы нарушителями с целью дестабилизации функционирования органов государственной власти, наблюдения за периметром охраняемых объектов, транспортировки запрещенных веществ, грузов, оружия, организации террористических актов, препятствовать воздушному движению в аэропортах и др.

Немаловажной проблемой является возможное воздействие со стороны нарушителей на ведомственные БПЛА. С целью анализа и выявления возможных деструктивных воздействий на ведомственные

БПЛА необходимо рассмотреть один из самых уязвимых к воздействиям компонент – систему управления и передачи данных. В общем случае система управления имеет вид, представленный на рисунке 1.28. В систему управления БПЛА входят наземный и бортовой комплексы управления. Наземный комплекс управления состоит из пульта дистанционного управления, а также устройства трансляции видеоизображения с БПЛА. К бортовой системе управления можно отнести приемник сигналов управления, бортовые датчики, а также полетный контроллер [50, 52].

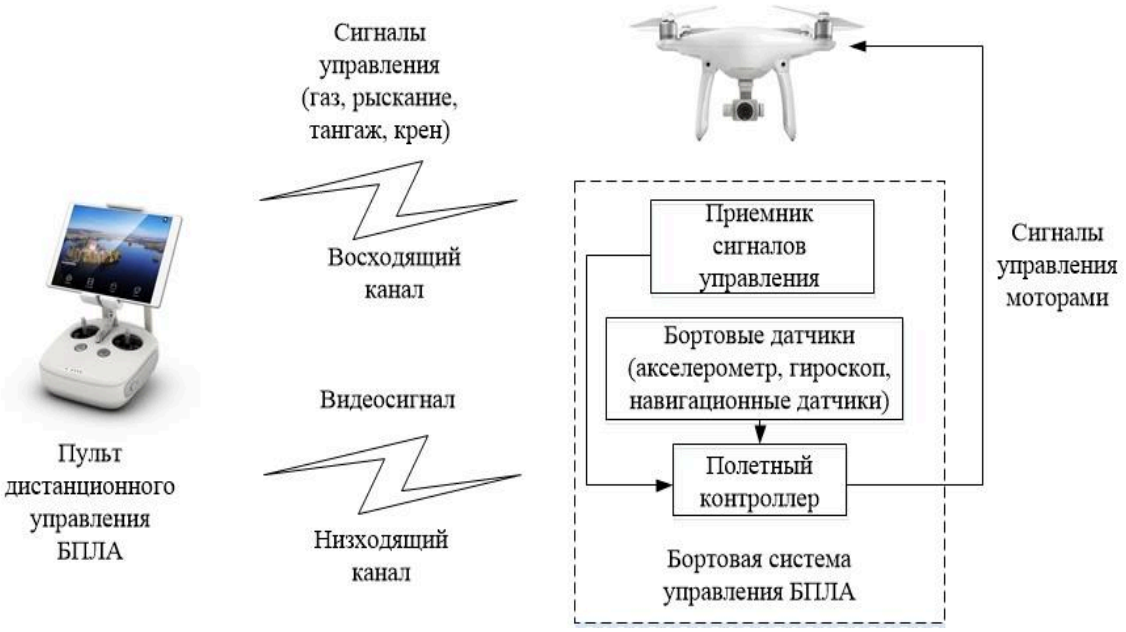


Рис. 1.28. Общий вид системы управления БПЛА

В качестве исследуемого объекта был выбран БПЛА, осуществляющий передачу видеоданных на смартфон, управляемый при помощи пульта управления, работающем на частотах 2.2-2.5 ГГЦ, систем глобального позиционирования данная модель БПЛА не содержит. Для анализа спектральных составляющих был использован анализатор спектра R&H FSH 8, подробные характеристики которого рассмотрены в работе [55].

Далее рассмотрим спектры каналов управления, а также передачи видеоданных с борта БПЛА, с целью выявления их уязвимостей. При исследовании БПЛА находился на удалении 15 метров от оператора. Полученный спектр передаваемого видеосигнала приведен на рисунке 3.

Из рисунка видно, что мощность передаваемого видеосигнала БПЛА составляет – 49 Дбм, а ширина полосы сигнала равна 21 МГц.

Далее перейдем к анализу спектра сигналов управления БПЛА, приведенных на рис. 1.29.

На рисунке 1.30. представлены спектры сигналов управления, отвечающие за газ и крен БПЛА, мощность которых составляет – 39 Дбм.

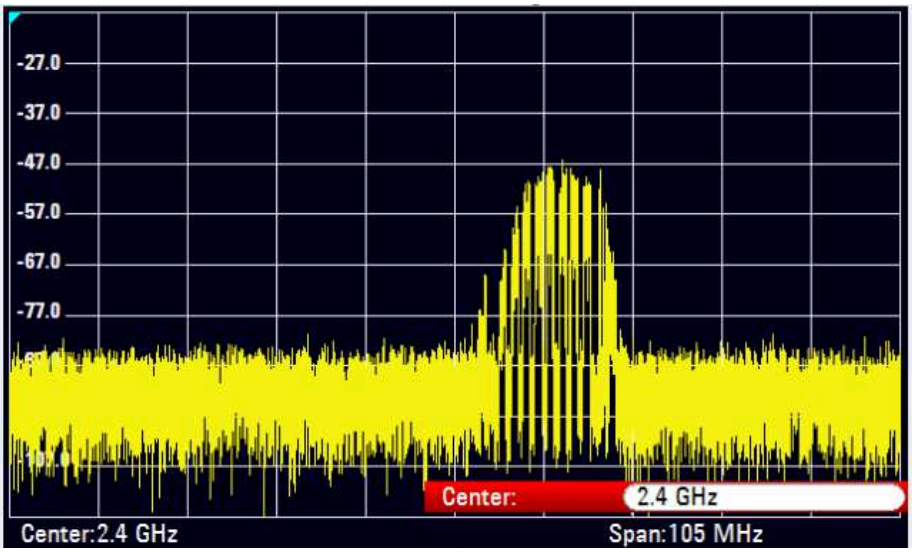


Рис. 1.29. Спектр принимаемого видеосигнала БПЛА.

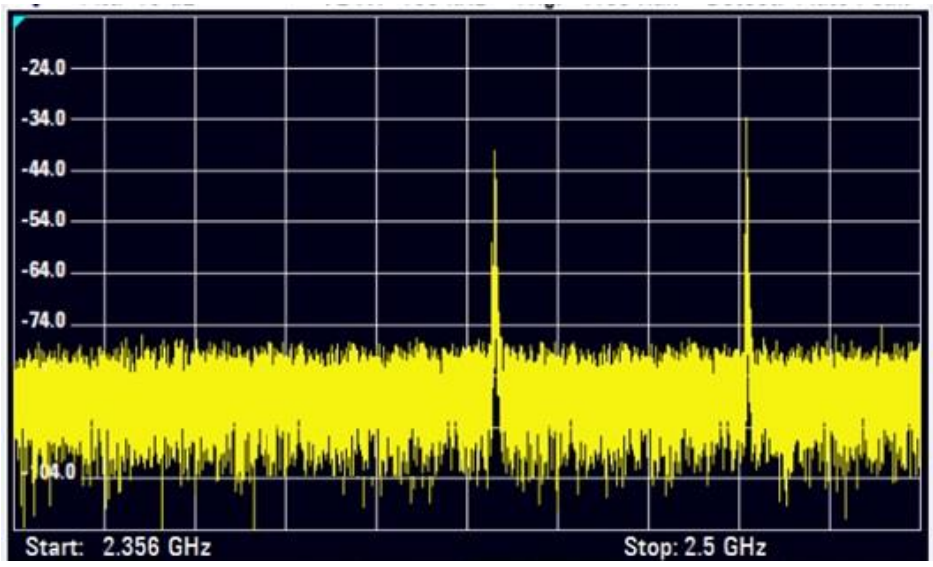


Рис. 1.30. Спектр принимаемых сигналов управления БПЛА

Анализ видеосигнала и сигналов управления БПЛА позволил выявить следующие уязвимости систем управления БПЛА [61]:

1. Подавление каналов управления БПЛА. Злоумышленник при знании частотного диапазона каналов управления может оказать деструктивное электромагнитное воздействие на каналы, который должен как минимум превосходить мощность каналов управления на 10 ДБм. При подавлении каналов управления БПЛА он может зависнуть на одном месте, сесть в месте текущего расположения или вернуться на точку взлета.

Аналогичные воздействия возможно оказать на каналы управления глобальными навигационными системами (ГЛОНАСС, GPS).

2. Подмена сигналов управления. Злоумышленник может перехватить и сгенерировать ложные сигналы управления и глобальных навигационных систем, тем самым уведя БПЛА в другое местоположение и захватить его и имеющиеся на нем информационные источники. Также БПЛА может быть использован для атаки оператора или других объектов, с целью повреждения и причинения иного экономического вреда. Следует отметить, что навязывание ложных координат систем глобального позиционирования происходит в 2 шага. На первом шаге деструктивное электромагнитное воздействие нарушителя блокирует сигналы, поступающие от легальных источников глобального позиционирования, тем самым переводя БПЛА в режим обнаружения и поиска сигналов навигации. На втором этапе генерируется деструктивное электромагнитное воздействие большой мощности, тем самым привязывая БПЛА к ложным сигналам позиционирования и последующем переходом в ложный режим определения координат.

3. Подавление каналов передачи видеоизображения. Злоумышленник может оказать деструктивное электромагнитное воздействие на канал передачи видеоданных, тем самым блокировав передачу потокового видео с борта БПЛА на пульт оператора. Тем самым порализовывается одна из основных функций БПЛА, такие как наблюдение и поиск. Помимо этого, нарушитель может передавать ложный поток видео, тем самым дезорганизовать работу оператора БПЛА.

С целью противодействия деструктивным электромагнитным воздействиям, оказываемым нарушителями, авторами была предложена система выбора методов противодействия, [63] работа которой основана на использовании в составе программной реализацией нейронной сети. Такая система анализирует мощности полезного сигнала и деструктивного воздействия, затем осуществляет их сравнение, на основании которого выбираются те или иные методы противодействия.

Авторами предлагается использовать аналогичную программную реализацию нейронной сети в составе бортового оборудования БПЛА. При этом в базу знаний вносятся правила действия БПЛА при оказании деструктивного электромагнитного определённой мощности. Нейронная сеть может иметь многоуровневую структуру, элементы которой будут взаимодействовать между собой. Вычислитель миссии внутри летательного аппарата анализирует мощности полезного сигнала и деструктивного воздействия, затем осуществляет их сравнение, на основании которого

выбираются те или иные методы противодействия. В качестве одного из возможных методов противодействия предлагается использовать рой БПЛА. Механизм осуществления выбора метода противодействия деструктивному электромагнитному воздействию представлен на рисунке 1.31.

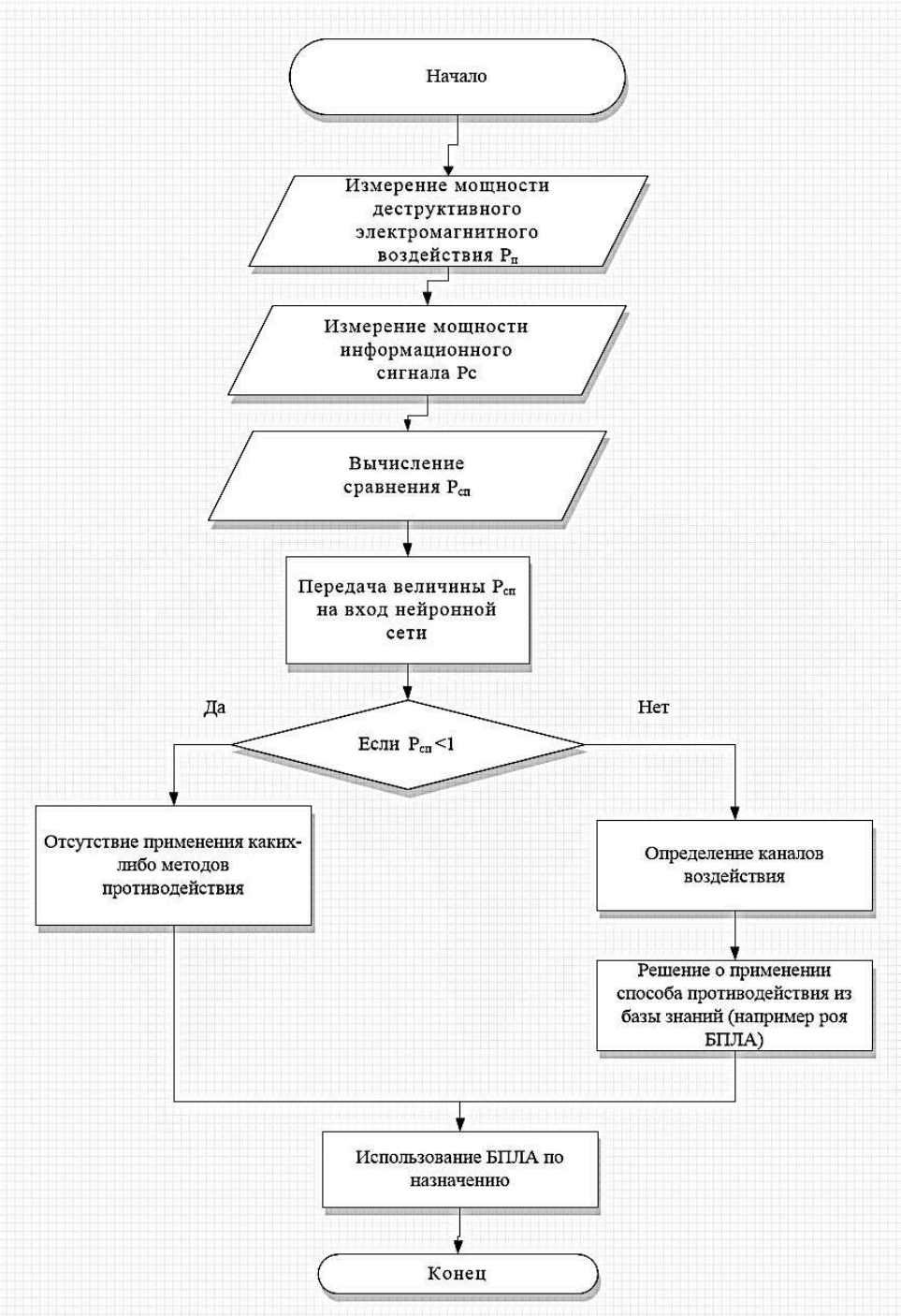


Рис. 1.31. – Алгоритм выбора метода противодействия для БПЛА

Один из возможных примеров применения роя будет рассмотрена далее.

Применение роя беспилотных летательных аппаратов в интересах МВД России. Пусть необходимо произвести разведку местности, где может скрываться лицо, подозреваемое в совершении преступления. Подозреваемый, полагая, что его поиски будут производиться с применением ведомственных БПЛА, с целью нарушения поисковой операции, испозьзует в районе своего местоположения БПЛА со средствами, генерирующими деструктивное электромагнитное воздействие.

Известно, что необходимо осуществить поиски в квадрате 10х10км. Для эффективного поиска необходимо N=17 БПЛА, сдвигающихся со скоростью 43,3 км\ч или 12м\с. Время полета составляет t=20 минут на высоте 300 м [62].

Пусть в арсенал злоумышленника входят B=4 БПЛА со средствами деструктивного электромагнитного воздействия. Пусть интенсивность вывода из стоя ведомственных БПЛА λ=5 мин$^{-1}$.

Время существования группировки БПЛА вычисляется в соответствии с выражением [49]:

$$\mathrm{T} = \frac{N^2}{2\lambda} = 29\text{мин}. \quad (1)$$

Как следует из выражения 1, через 10 минут вся группировка БПЛА будет выведена из строя, и не весь район будет исследован, как следствие правонарушитель может скрыться, в связи с чем, необходимо рассчитать численность роя БПЛА для осуществления поисковой операции в условиях воздействия БПЛА правонарушителя. Требуемое количество БПЛА вычислим согласно выражению 2 [49]:

$$N_0 = \sqrt{N^2 + 2\lambda \mathrm{t}} = 24\text{ед}. \quad (2)$$

В соответствии с выражением 2 для успешного поиска правонарушителя, оказывающего деструктивное электромагнитное воздействие на ведомственные БПЛА, в заданном квадрате, необходимо использовать рой численностью 24 единицы.

Рассмотрены возможные уязвимости каналов управления и передачи данных беспилотных летательных аппаратов. Приведены возможные ситуации применения БПЛА в интересах органов внутренних дел, а также представлены некоторые модели БПЛА, применяемые в органах правопорядка.

Произведен анализ радиосистем, применяемых в БПЛА, измерены приведены спектры сигналов управления и передачи видеоданных БПЛА. На основании спектрального анализа управляющих сигналов осуществлено формирование перечня возможных угроз на системы управления и передачи данных БПЛА со стороны правонарушителя. С целью минимизации деструктивного электромагнитного воздействия, оказываемого на

ведомственные БПЛА, было предложено использовать в составе бортовой системы БПЛА программную реализацию многоуровневой нейронной сети элементы которой будут взаимодействовать между собой. Вычислитель миссии входящий в состав летательного аппарата будет производить анализ мощности полезного сигнала и деструктивного воздействия, затем осуществлять их сравнение, на основании которого будет производиться выбор методов противодействия исходя из перечня сформированной базы знаний. В качестве одного из возможных методов противодействия рассмотрено использование роя БПЛА. Приведен пример конкретной ситуации применения роя БПЛА при проведении поисковой операции, рассчитана оптимальная численность БПЛА для проведения поиска правонарушителя, в условиях деструктивных электромагнитных воздействий на БПЛА, блокирующих каналы управления и передачи данных.

1.6. Разработка предложений по совершенствованию сетей радиосвязи ОВД на основе цифровых информационных технологий

Концепция развития цифровой радиосвязи органов внутренних дел Российской Федерации до 2024 года определяет основные направления развития и задачи по совершенствованию радиосвязи органов внутренних дел Российской Федерации с учетом современных требований системы управления МВД России, направленных на повышение эффективности правоохранительной деятельности [2].

Применение цифровой радиосвязи в системе связи МВД России является одним из основных инструментов, позволяющих повысить эффективность организации управления и взаимодействия подразделениями органов внутренних дел Российской Федерации.

Реализация положений Концепции создаст основу для перевода существующей цифровой радиосвязи на качественно новую техническую платформу на базе перспективных телекоммуникационных технологий, предлагающих инновационные решения, для оснащения подразделений органов внутренних дел Российской Федерации современными средствами радиосвязи.

Основными направлениями развития цифровой радиосвязи как системы обеспечения управления подразделениями органов внутренних дел Российской Федерации до 2024 года являются:

- Создание и внедрение:

– цифровых решений, обеспечивающих полноценное взаимодействие абонентов цифровых сетей радиосвязи стандартов APCO 25 и DMR и защиту передаваемой служебной информации ограниченного распространения;

– технических решений, обеспечивающих ведомственный защищенный мобильный широкополосный радиодоступ к сервисам ИСОД МВД России;

– комбинированных устройств, включающих в себя системы цифровой радиосвязи и устройства защищенного мобильного широкополосного радиодоступа к сервисам ИСОД МВД России.

- Подготовка образовательными организациями МВД России, реализующими соответствующие образовательные программы, квалифицированных специалистов в сфере управления и эксплуатации цифровой радиосвязи для подразделений органов внутренних дел Российской Федерации с учетом развития современных средств цифровой радиосвязи.
- Оснащение сотрудников органов внутренних дел Российской Федерации однотипными универсальными средствами цифровой радиосвязи, обеспечивающими взаимодействие абонентов цифровых сетей радиосвязи МВД России на всей территории Российской Федерации.
- Сокращение номенклатуры приобретаемых в рамках государственного оборонного заказа технических средств связи путем оптимизации ведомственных требований при принятии цифровых средств радиосвязи на снабжение МВД России.
- Соответствие состава и мест размещения элементов цифровой радиосвязи структуре подразделений органов внутренних дел Российской Федерации.

Основные задачи, посредством выполнения которых осуществляется совершенствование существующей цифровой радиосвязи подразделений органов внутренних дел Российской Федерации:

- Развитие цифровых сетей радиосвязи стандартов APCO 25 и DMR, в том числе двухстандартных (совмещенных APCO 25 / DMR), на базе оборудования и программного обеспечения отечественного производства.
- Внедрение отечественных абонентских радиостанций, использующих технологию, позволяющую программировать абонентское устройство радиосвязи для работы в цифровых сетях радиосвязи стандартов APCO 25 и DMR.
- Расширение радиопокрытия и увеличение канальной емкости систем цифровой радиосвязи (как в повседневной деятельности, так и при изменении оперативной обстановки), которые должны осуществляться путем применения подвижных узлов связи.
- Разработка и внедрение:

– ведомственных требований для оборудования стандарта DMR в части обеспечения совместимости оборудования различных производителей;

– ведомственного протокола взаимодействия цифровых сетей радиосвязи стандартов APCO 25 и DMR;

– средств криптографической защиты служебной информации ограниченного распространения для средств, использующих цифровые сети радиосвязи стандартов APCO 25 и DMR;

– защищенной ведомственной системы мобильного широкополосного беспроводного радиодоступа, которая должна функционировать как виртуальная частная сеть (VPN) по отношению к сетям связи общего пользования;

– планшетного компьютера, обеспечивающего мобильный широкополосный радиодоступ к сервисам ИСОД МВД России с использованием защищенной ведомственной системы мобильного широкополосного беспроводного радиодоступа.

- Актуализация образовательных программ, реализуемых образовательными организациями МВД России.
- Подготовка образовательными организациями МВД России квалифицированных специалистов в области управления и эксплуатации цифровой радиосвязи для подразделений органов внутренних дел Российской Федерации по образовательным программам высшего образования, основным программам профессионального обучения и дополнительным профессиональным программам.
- Оснащение образовательных организаций МВД России современными средствами цифровой радиосвязи в целях обеспечения эффективной подготовки специалистов для подразделений органов внутренних дел Российской Федерации.

2. ОПТИМИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ И СВЯЗИ ОВД

2.1. Задача оптимизации системы управления и связи ОВД

В настоящее время актуальной является задача структурной и параметрической оптимизации СУС МВД России, в результате чего должны быть обеспечены снижение эксплуатационных расходов, расширение возможностей и повышение качества функционирования. При этом, существенную роль имеют различия между субъектами Российской Федерации, что обуславливает разные требования к региональным системам управления и связи ввиду своеобразности рельефа, климатических особенностей и т. д. Это обуславливает различие в структуре, оснащении, организации эксплуатации и многом другом. В связи с этим возникает острая необходимость оптимизации уже существующих систем управления и связи посредством их модернизации и выбора соответствующих рабочих параметров, а также оптимального синтеза вновь проектируемых.

Требуется разработать методы, математические модели и алгоритмы оптимального выбора необходимых технических средств (ТС) и их объединения в единую систему, простые и понятные для рядового пользователя. Это обеспечивается нахождением легко определяемого критерия выбора технических средств и критерия оптимальности всей системы. Кроме того, как показывает практика, эффективность функционирования систем управления и связи определяется не только их технической составляющей, но и вопросами организации, кадрового обеспечения и многими другими.

Решение описанной выше задачи может проводиться на основе интеграции как уже находящихся в эксплуатации элементов СУС (подсистем, технических и программных средств, организационных структур и т. д.), так и новых. Так как система управления и связи будет развиваться постоянно, то ее оптимизация как на структурном, так и параметрическом уровне будет зависеть от времени, а ее параметры будут меняться в зависимости от появления новых требований к системе и изменения условий ее функционирования. Таким образом, речь идет о задаче оптимальной интеграции, которая является многокритериальной, дискретной, неэкстремальной, имеет высокую степень неопределенности в исходных данных и требованиях к конечному результату (критерию оптимальности) и большое количество трудноформализуемых и неформализуемых подзадач. Решить такую сложную задачу можно только поэтапно, осуществив ее грамотную декомпозицию, и широко применяя методы искусственного интеллекта, современные информационные и сетевые технологии, программные средства различного назначения [21].

Сложность и многоплановость сформулированной задачи делает необходимой разработку подхода, позволяющего сформировать минимальное множество универсальных методик, методов и алгоритмов, позволяющих решать весь спектр обозначенных проблем.

В настоящее время в структуре МВД России отсутствуют автоматизированные экспертные системы, направленные на выполнение задач оптимизации связи. Этот фактор является ограничивающим при осуществлении комплексной оптимизации. Применение таких систем позволит сотрудникам, задействованным в сфере обеспечения связи, принимать рациональные решения, основанные на опыте множества экспертов.

Достижение сформулированной выше цели осуществляется путем решения следующих задач: 1) формулировка задачи оптимизации системы управления и связи МВД России и осуществление ее декомпозиции; 2) разработка методики формирования критерия оптимальности системы управления и связи МВД России; 3) разработка методов, математических моделей и алгоритмов, неообходимых для определения значения показателя эффективности конкретного объекта оптимизации и сформированного на основе данного показателя критерия оптимальности; 4) разработка программных средств (ПС) для автоматизированного решения поставленной задачи с использованием ресурсов ИМТС МВД России. Так как структура системы управления и связи МВД России имеет иерарахический вид, то иерархический подход должен быть положен в основу решения всех этих задач.

Предлагается рассматривать систему управления и связи МВД России как совокупность технического, программного, кадрового, информационного, нормативного, организационного обеспечения, решающую задачу передачи информации между подразделениями МВД России разных уровней в интересах выполнения задач, стоящих перед полицией, в оптимальном для текущего момента времени и региона режиме.

Техническое обеспечение (ТО) – это всё используемое для осуществления связи и управления этим процессом оборудование, его параметры, каналы передачи информации, типовые схемы построения сетей, иерархия элементов сети, их физическое расположение, методы передачи.

Программное обеспечение (ПО) представляет собой набор ПС, на базе которых основана работа технических средств связи, специализированные и вспомогательные программы для работы с оборудованием, системы автоматизированного проектирования, а также базы данных, являющиеся точкой сбора, обработки, хранения и выдачи информации и статистических данных, необходимых проектировщику и лицу, принимающему решение (ЛПР).

Организационное обеспечение (ОО) включает собой структуру подразделения, его штат, возложенные задачи, методы взаимодействия с другими подразделениями, обучение и подготовку специалистов, взаимодействие с поставщиками оборудования, ведение служебной документации и т. д.

Нормативное обеспечение (НО) – это правовые основы деятельности подразделений МВД, а также правила и предписания, регламентирующие построение, эксплуатацию и обслуживание систем связи, использование частотного ресурса, требования к оборудованию, его сертификация, соблюдение санитарных норм.

Информационное обеспечение (ИО) – это процессы сбора, обработки, хранения и передачи информации, полученной в результате функционирования сети связи и необходимой для принятия обоснованных управленческих, в том числе и оперативных, решений. Это и сама информация на различных носителях, и возможность использования её всеми уполномоченными на то сотрудниками.

Кадровое обеспечение (КО) – это комплекс действий, направленных на поиск, оценку и установление заранее предусмотренных отношений с сотрудниками как в самом подразделении, так и вне его пределов для найма новых сотрудников. Кадровое обеспечение включает в себя обучение специалистов, повышение их квалификации, учитывает не только индивидуальные способности и личные качества сотрудников, но и качество работы всего подразделения в целом.

Математическое обеспечение (МО) – включает в себя совокупность математических методов, моделей и алгоритмов предназначенных для решения задач передачи разнородной информации, управления данным процессом, а также проектирования оптимальных систем управления и связи.

Так как система связи МВД России – это совокупность неразрывно связанных и взаимодействующих между собой видов обеспечения, то решить задачу оптимизации этой системы сложно. Поэтому необходимо произвести декомпозицию задачи, то есть представить рассматриваемый объект как сложную систему, состоящую из подсистем более низкого уровня, которые в свою очередь делятся на системы еще более низких уровней.

Таким образом, задача оптимизации системы связи переходит в задачу оптимизации каждой из этих подсистем по отдельности, что в конечном счете приведет к желаемому результату.

Исходя из вышесказанного, предлагается разбить задачу оптимизации системы связи МВД России на следующие частные задачи:

1) оптимизация технического обеспечения;

2) оптимизация программного обеспечения;

3) оптимизация организационного обеспечения;

4) оптимизация нормативного обеспечения;
5) оптимизация информационного обеспечения;
6) оптимизация кадрового обеспечения;
7) оптимизация математического обеспечения.

Таким образом, получается многоуровневая иерархия компонентов системы (рис. 2.1), оптимизация в этом случае осуществляется с самого нижнего уровня и последовательно переходит на следующие.

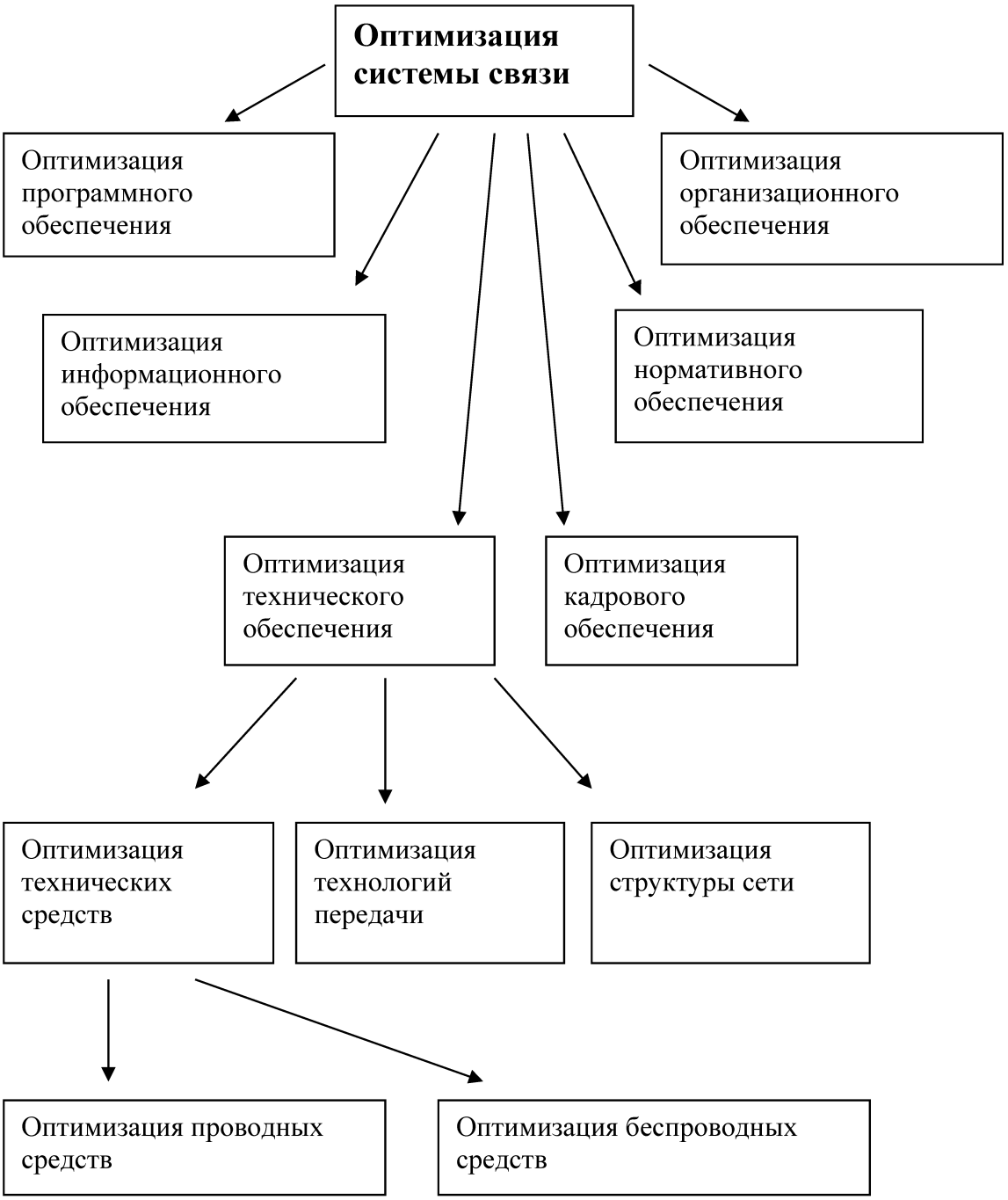


Рис. 2.1. Структура задачи оптимизации системы управления и связи

Оптимизация каждого из видов обеспечения требует дальнейшего разложения обеспечений на компоненты и их элементы, в результате чего решение комплексной задачи преобразуется в множество простых.

2.2. Формирование критерия оптимальности системы управления и связи ОВД на основе показателей качества ее функционирования

Как отмечалось ранее, одним из важнейших и сложнейших вопросов при оптимизации системы связи ОВД является выбор критерия оптимальности, так как жестко стоит проблема сбора исходной информации. Кажется естественным использование критерия «стоимость/эффективность», который необходимо минимизировать, однако его не всегда можно определить, так как на его значение влияют множество факторов как объективного, так и субъективного характера.

Часть исходной информации не количественная, а качественная и существует в виде суждений специалистов на основе их опыта. Другая часть – это количественные характеристики, которые необходимо пересчитывать, чтобы была возможность сравнения технических средств и систем в одинаковых условиях. Третью часть характеристик можно определить только путем эксперимента – физического или математического моделирования. Также возникает вопрос о том, по каким характеристикам необходимо производить сравнение различных вариантов построения систем связи и ее элементов, какие из этих характеристик имеют большую значимость по сравнению с другими.

Таким образом, задача оптимизации системы связи ОВД является многокритериальной. Причем вся система связи ОВД, виды ее обеспечения и их элементы являются композицией уже имеющихся решений (ТС, ПО, нормативных документов, штатных единиц и т. д.). Следовательно, необходимо решить задачу дискретной оптимизации, которая является неэкстремальной. Видно, что обобщенный критерий оптимальности при решении этой задачи должен формироваться на основе локальных критериев оптимальности решения частных задач.

Предлагается формировать критерий оптимальности на основе показателя качества функционирования системы управления и связи ОВД России, который является линейной сверткой нормированных показателей качества перечисленных выше видов обеспечения системы связи ОВД, полученных на основе их весовых коэффициентов.

Эти показатели качества обеспечений получаются аналогичным образом на основе локальных показателей каждого из обеспечений и т. д. Получается показатель эффективности, имеющий древовидную многоуровневую иерархическую структуру, отличающуюся большой гибкостью, так как к ней легко добавить как новые показатели эффективности функционирования, так и новые уровни иерархии.

Таким образом, обобщенный показатель эффективности функционирования системы или сети связи, находящийся на самом высоком (нулевом) уровне иерархии, имеет вид

$$K_0 = \sum_{j=1}^{J} b_{1j} K_{1j}, \qquad (2.1)$$

где *j=1, 2,…,J* – номер локального показателя эффективности на следующем уровне иерархии, K_{1j} – нормированное значение *j*-го локального показателя эффективности на 1-м иерархическом уровне обобщенного показателя эффективности, b_{1j} – его весовой коэффициент.

Для всех последующих *i*-х уровней иерархии локальные показатели эффективности имеют вид:

$$K_0 = \sum_{j=1}^{J} b_{i+1,j} K_{i+1,j}\,. \qquad (2.2)$$

На самом низком уровне иерархии значения показателя эффективности формируются на основе характеристик по правилу:

$$K_{ij} = (p_j - p_{j\min}\ )/(p_{j\,max} - p_{j\min}\ )\,, \qquad (2.3)$$

где: i – номер уровня иерархии локального показателя эффективности; j – номер характеристики на данном уровне; p_j – значение данной характеристики; $p_{j\max}$ – максимально возможное наилучшее значение данной характеристики, $p_{j\min}$ – минимально возможное наихудшее значение данной характеристики (в зависимости от условия задачи может иметь и нулевой и любое другое значение).

Значения показателей эффективности K_{ij} могут быть получены следующими способами:

1) рассчитаны на основе имеющихся характеристик;
2) методом экспертного оценивания;
3) с помощью физического или математического моделирования.

Значения весовых коэффициентов b_{ij} с высокой степенью достоверности в настоящее время можно определить только методом экспертного оценивания.

Использование при этом методов экспертного оценивания позволит:

1) получать значения весовых коэффициентов локальных критериев;
2) сводить качественные критерии к количественным;
3) определять новые значимые критерии (в том числе и новые виды обеспечений);

4) определять состав экспертных групп и весовые коэффициенты их оценок. Регулярные повторные экспертные опросы позволят своевременно реагировать на изменение требований к объекту оптимизации, его составным частям и условиям их функционирования.

Пример иерархичной структуры показателя эффективности функционирования сети связи ОВД представлен на рис. 2.2.

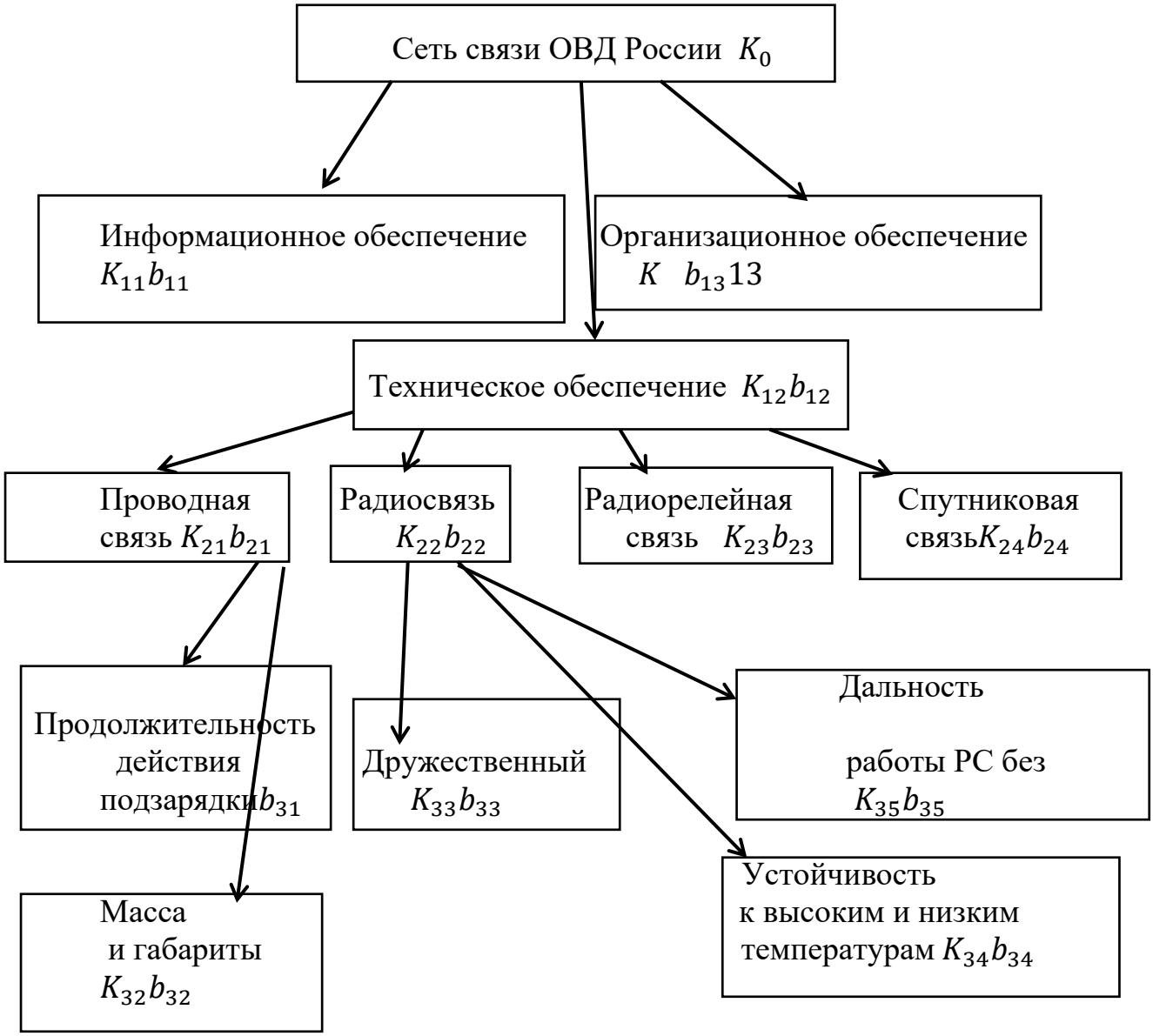


Рис. 2.2. Иерархичная структура показателя эффективности функционирования сети связи ОВД

На основе предложенного показателя качества функционирования сети связи ОВД можно сформировать критерий ее оптимальности. При этом возможно в зависимости от специфики решаемой задачи использовать два

подхода. Первый основан на использовании отношения стоимость/эффективность:

$$C = S/K_0 = \min, \quad (2.4)$$

где S – стоимость сети связи.

Второй подход основан на максимизации показателя эффективности при наложении ограничения на стоимость:

$$K_0 = \max, \qquad S \le max\,. \quad (2.5)$$

При этом возможно введение ограничений как на значения отдельных локальных показателей эффективности, так и на стоимость мероприятий по обеспечению данных значений:

$$S_{i,j} \le max, \;\; K_{i,j} \ge min. \quad (2.6)$$

Таким образом, получается многоуровневая иерархия компонентов системы, которая строится «сверху-вниз». Соответствующим образом формулируются и требования к элементам системы. Оптимизация же осуществляется в обратном направлении – «снизу-вверх», с самого нижнего уровня она последовательно переходит на последующие. Оптимизация производится на основе соответствующих критериев, имеющих аналогичную многоуровневую иерархическую структуру [3].

Предложенный подход позволяет как в масштабах всей системы управления и связи ОВД, так и на уровне отдельных подразделений: 1) осуществлять декомпозицию задачи оптимизации и соответствующего критерия; 2) разрабатывать единые процедуры и алгоритмы формирования критериев оптимальности; 3) составлять с помощью методов экспертного оценивания и кластерного анализа перечень значимых характеристик отдельных классов обеспечений и технических средств. Его реализация в виде соответствующих программных средств автоматизации позволит существенно повысить эффективность системы управления и связи ОВД.

2.3. Формирование критерия оптимальности системы управления сетями связи ОВД

Основными элементами задачи оптимизации управления сетями связи ОВД являются: 1) оптимизация принятия управленческих решений; 2) оптимизация системы связи в интересах решения задачи управления. При этом в интересах оптимального управления силами и средствами ОВД ведомственная система связи должна решать следующие задачи:

– доведение с заданными вероятностно-временными характеристиками приказов и сигналов централизованного управления от центральных пунктов управления до подчиненных пунктов;

– качественное и своевременное предоставление должностным лицам органов управления ОВД информационно-телекоммуникационных услуг;

– выполнение требований устойчивого, непрерывного, оперативного и скрытного управления силами и средствами;

– создание условий для обеспечения безопасности, достоверности и целостности информации, циркулирующей в системе управления ОВД, на этапах сбора, обработки, передачи, хранения, распределения и предоставления пользователям.

Эффективное решение этих задач достигается путем: 1) оптимизации структуры сети связи ОВД, используемой в управления силами и средствами; 2) оптимизации процедур управления системой связи ОВД. Второй пункт включает в себя и принятие оптимальных управленческих решений на уровне сети связи ОВД, однако по предметной области, характеру решаемых задач, требованиям к лицу, принимающему решение, он существенно отличается от принятия оптимальных управленческих решений на уровне сил и средств, напрямую подчиненных главной системе. Однако при этом многие фундаментальные проблемы, а соответственно, и методы их преодоления и там и там будут одинаковыми.

Предлагается использовать подход к формированию критерия оптимальности, аналогичный предложенному в параграфе 2.2.

Выделим следующие уровни иерархии задачи оптимизации системы управления сетями связи ОВД и, соответственно, критериев оптимальности (рис. 2.3).

Первый уровень: система управления и связи ОВД.

Второй уровень: 1) система принятия решений; 2) система связи ОВД, работающая в интересах управления.

Третий уровень (для системы связи ОВД): 1) структура системы связи ОВД; 2) управление системой связи ОВД.

Четвертый уровень (для структуры системы связи ОВД):
1) техническое обеспечение;
2) программное обеспечение;
3) организационное обеспечение;
4) нормативно-правовое обеспечение;
5) информационное обеспечение;
6) кадровое обеспечение;
7) математическое обеспечение.

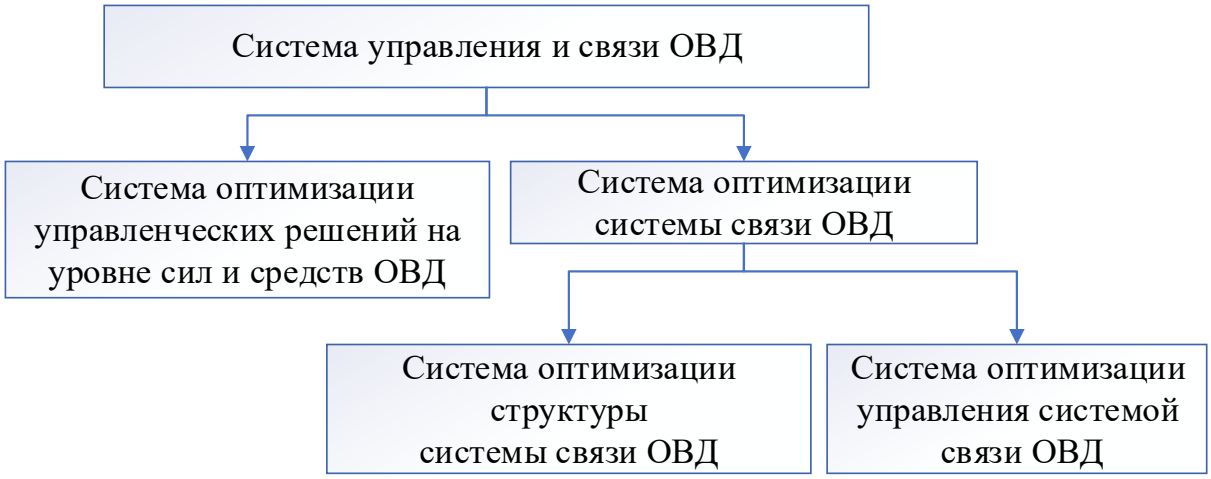


Рис. 2.3. Первые три уровня иерархической структуры системы управления и связи ОВД

Оптимизация каждого из указанных элементов требует дальнейшего их разбиения на компоненты и их элементы, в результате чего решение комплексной задачи преобразуется в множество простых. Таким образом, на основе данной структуры производится иерархическая декомпозиция задачи оптимизации системы управления и связи ОВД, а также формулируется критерий оптимальности [1, 3].

2.4. Математическое моделирование эффективности функционирования системы управления и связи ОВД

Значения многих показателей эффективности функционирования СУС как на уровне сетей связи, так и на уровне системы управления сетями связи можно получить только способом физического или математического моделирования. Математическое моделирование является более предпочтительным с точки зрения гибкости, финансовых и временных затрат, однако требует разработки соответствующих математических моделей. В данном параграфе предложены некоторые из них.

При решении задачи оптимизации системы связи МВД России часто возникает задача определения степени соответствия какого-либо объекта или субъекта поставленным перед ним задачам. Например, при выборе состава экспертной группы в первую очередь необходимо определить круг наиболее компетентных специалистов. Для этого необходимо: 1) осуществить классификацию (разбиение на классы) всех объектов предшествующих экспертиз; 2) произвести классификацию всех задействованных ранее экспертов; 3) определить степень компетентности каждого класса экспертов в области каждого класса задач; 4) произвести классификацию нового объекта экспертизы, то есть определить, к какому классу объектов он относится или к какому классу он ближе всего (если

новый объект образует новый класс); 5) выбрать класс экспертов, наиболее соответствующий классу объекта экспертизы; 6) если экспертов окажется очень много, то путем их экспертного опроса можно выявить наиболее компетентных в данной конкретной задаче и попутно определить весовые коэффициенты их суждений.

Аналогичная задача возникает при модернизации уже существующей системы связи. При этом необходимо: 1) классифицировать уже существующую систему связи; 2) классифицировать комплекс задач, которые она должна решать после модернизации; 3) определить по классу задач класс систем связи, в который наша система должна перейти после модернизации; 4) путем сравнительного анализа параметров системы до и после модернизации определить комплекс мер по ее переходу из одного класса в другой. Решение всех этих задач основывается на методах кластерного анализа. Рассмотрим данный подход на примере последней описанной задачи.

Оптимизацию систем и сетей можно производить на основе модели функционального соответствия системы связи стоящим перед ней задачам. Данная модель представлена на рисунке 2.4 и является композицией двух элементов (моделей): множества классов систем (сетей) связи и множества классов функциональных возможностей сети. Каждая из них в свою очередь состоит из множества других классов (моделей), отражающих различные (зачастую слабо формализуемые или не формализуемые) аспекты построения системы связи и функциональных возможностей сети.

Разбиение на классы систем связи и классы функциональных возможностей сетей связи производится на основе исходного множества информационных объектов, подлежащих классификации $A = \bigcup_{i=1}^{I} a_i$, где I – количество сетей в множестве, i – индекс сети. Пусть каждая сеть a_i представлена множеством значений параметров $P = \bigcup_{j=1}^{J} p_j$, J – количество параметров. На рис. 2.4 с индексами «о» и «с» даны обозначения, относящиеся к системе связи и функциональным возможностям соответственно. Значения параметров нормируются по формуле $p'_{ij} = p_{ij} / \sum_{i=1}^{I} p_{ij}$. Исходной информацией для проведения классификации является матрица D евклидовых расстояний между сетями в признаковом пространстве. Так, для любой пары объектов a_{i1} и a_{i2} расстояние между ними $d_{i1\ i2} = (\sum_{j=1}^{J} (p'_{i1\ j} - p'_{i2\ j})^2)^{1/2}$.

Между каждой сетью связи a_{oi} и каждой функциональной возможностью сети связи a_{cj} существует взаимосвязь, описываемая вероятностью соответствия j-й функциональной возможности a_{cj} конкретному i-му варианту построения сети (системы) связи a_{oi}. Эта

вероятность является условной вероятностью $q_{1ij}=P(a_{cj}|a_{oi})$. Кроме того, вектор соответствия варианта построения (класса) сети связи ее функциональным возможностям имеет параметры, описывающие среднюю стоимость экономического эффекта от использования j-й функциональной возможности a_{cj} при конкретном i-м варианте построения сети и другие параметры, обусловленные особенностями решаемой задачи, и образует множество параметров $Q = \bigcup_{m=1}^{M} q_m$, где M – количество параметров.

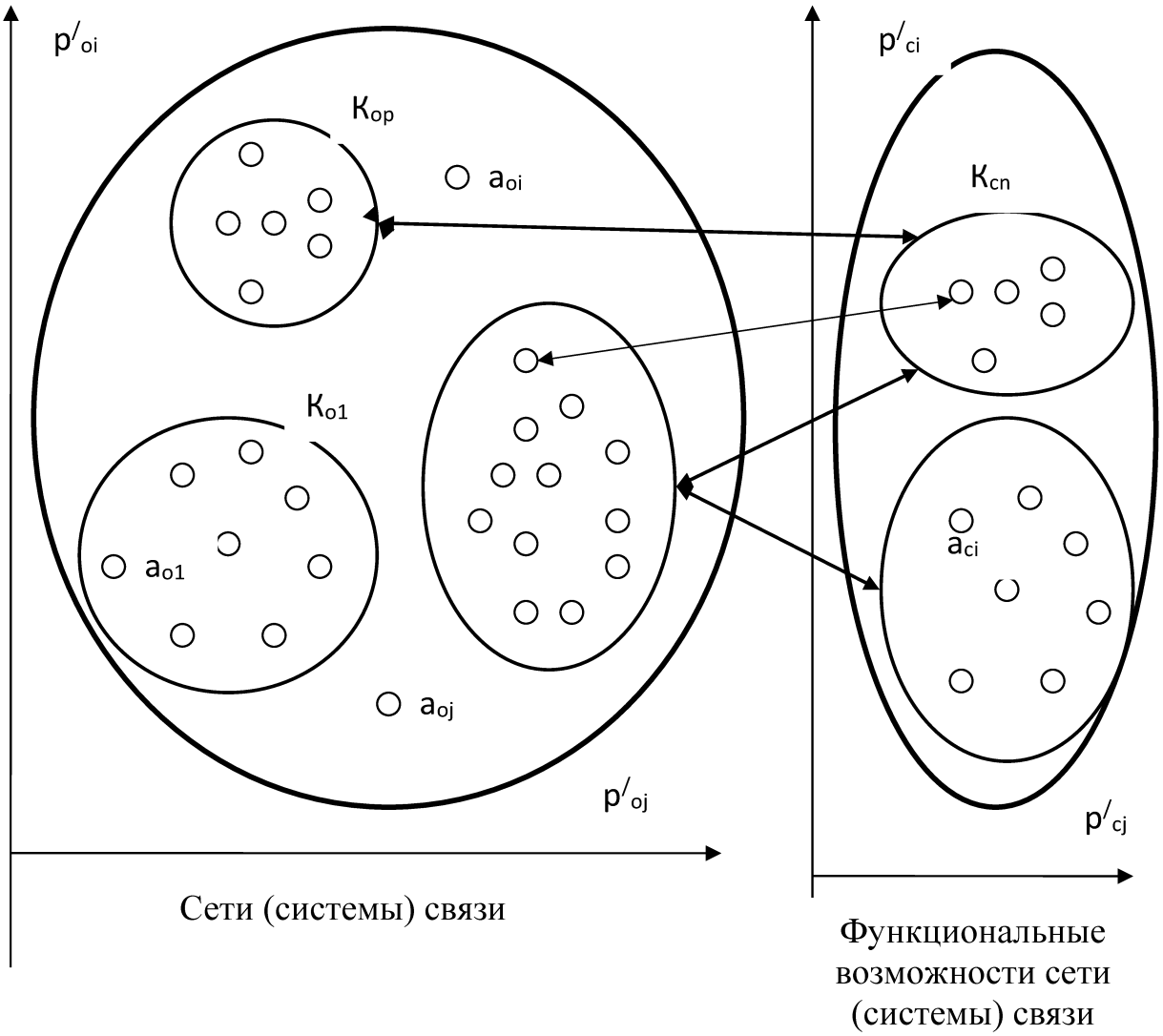


Рис. 2.4. Модель функционального соответствия сети (системы) связи

2.5. Построение защищенной системы мобильного широкополосного доступа, которая функционирует как виртуальная частная сеть

Концепция виртуальной частной сети (Virtual Private Network – VPN) появилась как альтернатива защищенной коммуникационной сети, функционирующей поверх сети связи общего пользования, и стала технологией, ориентированной на обеспечение целостности, конфиденциальности и доступности передаваемой информации. Безопасность информационного взаимодействия локальных сетей и отдельных элементов сети типа Internet требует качественного решения не только для задачи защиты локальных сетей и отдельных элементов со стороны внешней среды, но и для задачи защиты информации в процессе передачи по открытым каналам связи [65]. Для решения второй из указанных задач наряду с описанными ранее мерами и средствами защиты сегодня применяются виртуальные частные сети. VPN, как любая распределенная система, является комплексом взаимодополняющих средств и систем защиты [74, 75].

Технологии VPN обеспечивают гарантированный уровень транспортного обслуживания (качества сервиса) для корпоративного трафика, направляемого через публичные сети. VPN – любая сеть, построенная на основе публично предоставляемой сетевой инфраструктуры, логически разделенная для использования отдельными клиентами, данные по которой передаются безопасным способом [68, 69, 70, 72]. Защита информации в VPN в процессе ее передачи основана на построении защищенных виртуальных каналов связи, называемых криптозащищенными VPN тунелями. Для защиты от повтора, удаления и задержек пакетов сообщений используются встроенные возможности стека протоколов TCP/IP. Пример классификации частных виртуальных сетей приведен на рисунке 2.5.

В зависимости от шифрования технологии VPN можно реализовать на следующих видах протоколов: PPTP – туннелирование по TCP/IP сетям, SKIP, IPSec, TLS, SOCKS, SSL, GRE, L2F – туннелирование по X.25, ATM, Frame Relay, L2TP – туннелирование в разных сетях и других. Одним из основных требований, предъявляемых к аппаратным – и программным платформам реализации VPN, является наличие действующих сертификатов соответствия ФСБ России и ФСТЭК России. Сертификат ФСБ России на соответствие требованиям к шифровальным (криптографическим) средствам выдается только в том случае, если оборудование реализовано с использованием отечественных алгоритмов шифрования по ГОСТ 28147-89, а также соответствует Положению о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

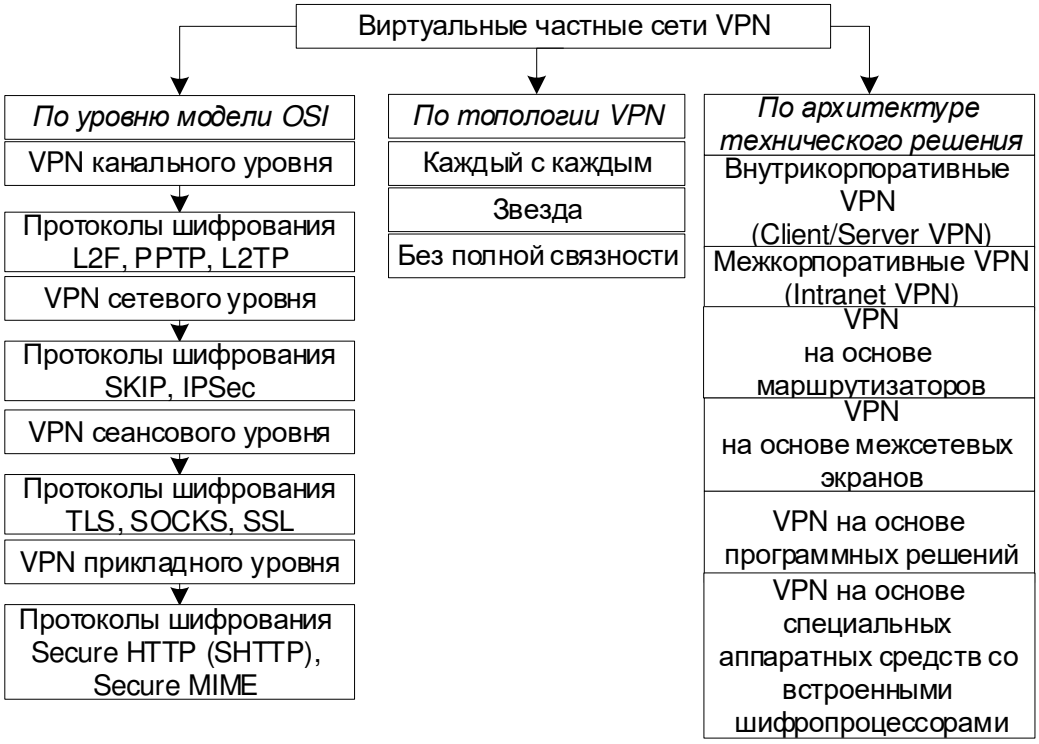


Рис. 2.5. Классификация частных виртуальных сетей

Криптографическим шлюзом принято считать аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам IPsec AH и/или IPsec ESP при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации и обеспечивающий базовую функциональность современного VPN-устройства [78]. В России основными потребителями криптошлюзов являются государственные учреждения, а также организации, являющиеся операторами персональных данных.

Зарубежные производители крайне редко поддерживают шифрование по ГОСТ и получают такие сертификаты соответствия на свои решения, чем активно пользуются российские компании-вендоры средств криптографической защиты информации. Отдельно необходимо отметить тренд, связанный с кибербезопасностью автоматизированных систем управления технологическими процессами (АСУ ТП). Сегодня некоторые производители СКЗИ предлагают рынку криптошлюзы в защищенном исполнении, отвечающие требованиям по пылевлагозащищенности и специальным температурным диапазонам. Появились и нормативные акты, формирующие требования к защите информации в подобных системах: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на

критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды» [67].

Проблемы безопасности инфокоммуникационных систем затрагивают множество составляющих – от защиты локальных сетей, в том числе беспроводных, до внедрения методов и средств защиты мобильных устройств.

Транспортная сеть защищенной ведомственной системы мобильного широкополосного беспроводного радиодоступа, которая должна функционировать как виртуальная частная сеть (VPN)

Основой построения транспортных сетей являются первичные сети. Первичной сетью называется совокупность типовых физических цепей, типовых каналов передачи и сетевых трактов системы электросвязи, образованная на базе сетевых узлов, сетевых станций, оконечных устройств первичной сети и соединяющих их линий передачи системы электросвязи [65].

Предоставление услуги виртуальной частной сети в представлении исполнителя (оператора связи) – возможность абонента объединить локальные сети удаленных офисов в единую корпоративную сеть на основе технологии VPN с применением шифрования. VPN может выступать как один из элементов комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения [76]. Стоит отметить, что шифрование может влиять на скорость соединения. Выбор технологии VPN и методов шифрования должен производиться в каждом конкретном случае, в зависимости от того, какие данные будут передаваться [67]. Процесс внедрения криптошлюзов может быть непростым, и это требует от организации наличия в штате квалифицированных специалистов. По данным статистического портала Statista.com, устройства для построения VPN станут год от года всё более востребованными [73].

В соответствии со статьей 13 Федерального закона от 07.07.2003 № 126-ФЗ (ред. от 30.04.2021) «О связи», сеть связи общего пользования предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации и включает в себя сети электросвязи, определяемые географически в пределах обслуживаемой территории и ресурса нумерации и не определяемые географически в пределах территории Российской Федерации и ресурса нумерации, а также сети связи, определяемые по технологии реализации оказания услуг связи. Она представляет собой комплекс взаимодействующих сетей электросвязи, в том числе сети связи для трансляции телеканалов и (или) радиоканалов.

Транспортная сеть (transport network) – часть сети связи, охватывающая магистральные узлы, междугородние станции, а также соединяющие их каналы и узлы (национальные, междугородные). В табл. 2.1 показаны структуры моделей транспортных сетей, имеющих функциональные уровни: физических трактов и каналов [67].

Главным требованием, предъявляемым к транспортным сетям, является выполнение сетью ее целевой функции – обеспечения пользователям возможности доступа ко всем разделяемым ресурсам сети.

Для построения виртуальных частных сетей оператор может использовать разные технологии: выделенные каналы, протокол ретрансляции кадров Frame Relay, шифрование туннелей в сети Интернет, многопротокольную коммутацию по меткам (MPLS), беспроводные технологии и другие.

По топологии виртуальной частной сети она может быть построена по типу «каждый с каждым», «звезда», «без полной связности». Качество услуги «Предоставление виртуальной частной сети» и показатели качества регламентирует ГОСТ Р 53729 – 2009.

Таблица 2.1. Структуры многоуровневых моделей транспортных сетей

<table>
<tr><td colspan="2">SDH</td><td colspan="2">ATM</td><td colspan="3">Оптическая сеть</td></tr>
<tr><td>Уровень каналов</td><td>Цифровые каналы E1, E3, E4</td><td rowspan="2">Уровни ATM</td><td>Виртуальные каналы</td><td colspan="3">Уровень каналов</td></tr>
<tr><td rowspan="2">Уровни трактов</td><td>Тракты виртуальных контейнеров VC-12</td><td>Виртуальные тракты</td><td rowspan="2">Уровни трактов</td><td>Другие электри-ческие тракты</td><td>Тракты SDH</td></tr>
<tr><td>Тракты виртуальных контейнеров VC-3, VC-4</td><td rowspan="3">Физичес-кий уровень</td><td>Цифровая секция (тракт)</td><td colspan="2">Оптические транспортные системы</td></tr>
<tr><td>Физичес-кий уровень</td><td>Секции мультиплексиро-вания и регенерации</td><td>Секции мультиплексирования и регенерации</td><td>Уровни оптичес-кой сети</td><td colspan="2">Секции оптического мультиплексиро-вания</td></tr>
<tr><td></td><td>Физическая среда</td><td>Физическая среда</td><td colspan="2">Оптическая ретрансляция Оптоволоконная линия</td></tr>
</table>

В качестве транспортной среды могут выступать:

– сеть радиосвязи;

– локальная сеть Ethernet;

– сеть связи сотовых операторов 3G/4G.

В качестве транспортной инфраструктуры также может быть использована инфраструктура радиорелейных и спутниковых каналов связи.

Интерфейс канала может быть как проводным (витая пара, оптоволокно), так и беспроводным (GPRS, HSPA, LTE, Wi-Fi, WiMAX).

Оператор связи обязан обеспечить предоставление доступа к сети VPN, а также возможности передачи данных различных видов голос, видео и другие. Показателями качества функционирования виртуальной частной сети для протокола IP будут выступать: процент потерянных пакетов, средние сетевые задержки пакетов, средние колебания сетевых задержек пакетов. Для протокола FR показателями качества функционирования виртуальной частной сети будут выступать: время переноса кадра, коэффициент потери кадров [67].

Необходимо учитывать, что транспортная среда может быть как реализована на собственной телекоммуникационной инфраструктуре организации, так и арендована у оператора телекоммуникационных услуг.

Обеспечение информационной безопасности мобильных устройств

Под категорию мобильных устройств подпадает любое переносное/носимое вычислительное устройство: ноутбук, нетбук, планшетный компьютер, интернет-планшет, карманный персональный компьютер, смартфон, устройства цифровой радиосвязи и мобильного широкополосного беспроводного доступа (МШБД) независимо от производителей оборудования радиосетей и применяемых стандартов цифровой радиосвязи. Мобильные устройства постоянно совершенствуются и изменяются, их характеристики разнообразны, а количество операционных систем для них с каждым днем становится все больше и больше. Исходя из вышесказанного, под термином «мобильные устройства» будет пониматься лишь часть устройств, которые обладают специализированной мобильной операционной системой (ОС) и системой управления. В настоящее время количество мобильных ОС достаточно велико и так же велико количество версий каждой ОС. Все они имеют много уязвимостей, и зачастую разных. Отечественная сертифицированная мобильная операционная система «Аврора» и программное обеспечение отечественной разработки в условиях импортозамещения позволит минимизировать существующие угрозы информационной безопасности.

Реализация виртуальных частных сетей на SIM-картах с российским шифрованием

SIM-карты могут быть оснащены российской криптографией. В этом случае оператор связи может использовать на своей сети аппаратный модуль безопасности, позволяющий внедрить отечественную

криптографию в телекоммуникационное оборудование. При этом виртуальный мобильный оператор компании будет соответствовать необходимому классу безопасности [66].

Разработчик сервисов идентификации IDX отвечает за разработку сервисов на базе доверенных SIM-карт. В базовый комплект входят квалифицированная электронная подпись, автозаполнение, которое хранится в защищенной области, генерация одноразовых паролей, возможность использовать SIM-карту как токен для платежных приложений по аналогии с ApplePay. Последняя опция предназначена для российских платежных приложений типа SberPay, TinkoffPay и других [66]. SIM-карты и модули безопасности с российским шифрованием разработал Институт точной механики и вычислительной техники им. С. А. Лебедева РАН.

С декабря 2019 года вступили в силу требования Минцифры по аутентификации и идентификации абонентов с использованием криптографии, одобренной ФСБ. Поставщики телекоммуникационного оборудования для сетей сотовой связи должны либо сертифицировать некоторые элементы собственной инфраструктуры как средство криптографической защиты информации, либо устанавливать внешние модули безопасности [66]. Эксперты называют минусами таких SIM-карт то, что их нельзя будет свободно продавать в салонах связи, вывозить за рубеж, а криптографические ключи необходимо перевыпускать каждые 15 месяцев.

Возможность защищенной передачи речи и данных на базе VPN

Оптимальной является сертификация микросхем по требованиям безопасности, например по уровню «конфиденциально». При этом доверенная среда на базе микросхемы является отчуждаемым элементом, а средства связи сертифицируются только на корректность встраивания. В эксплуатируемых и разрабатываемых устройствах в настоящее время используются алгоритмы шифрования, реализованные на американских сигнальных процессорах и, соответственно, средствами защиты не являющиеся и требованиям безопасности не отвечающие (являются маскираторами).

Маскираторы также широко используются в составе средств связи и представляют собой узлы, выполненные на компонентной элементной базе иностранного производства общего назначения в конечном счете также не являющиеся средством защиты информации.

В первом и во втором случае маскираторы уступают по массо-габаритным характеристикам, потребляемой мощности, надежности, устойчивости серийных поставок сертифицированным средствам защиты информации в микроэлектронном исполнении. В настоящее время разработаны и находятся в серийном освоении специальные SIM-карты и специализированные изделия в форм-факторах SD-карт серийного

производства. Эти микросхемы могут эффективно заменить маскираторы, применяемые в средствах УКВ радиосвязи, а также могут быть встроены в сотовые телефоны для создания защищенной служебной сотовой связи (рис. 2.6.) [68, 69, 70, 77].

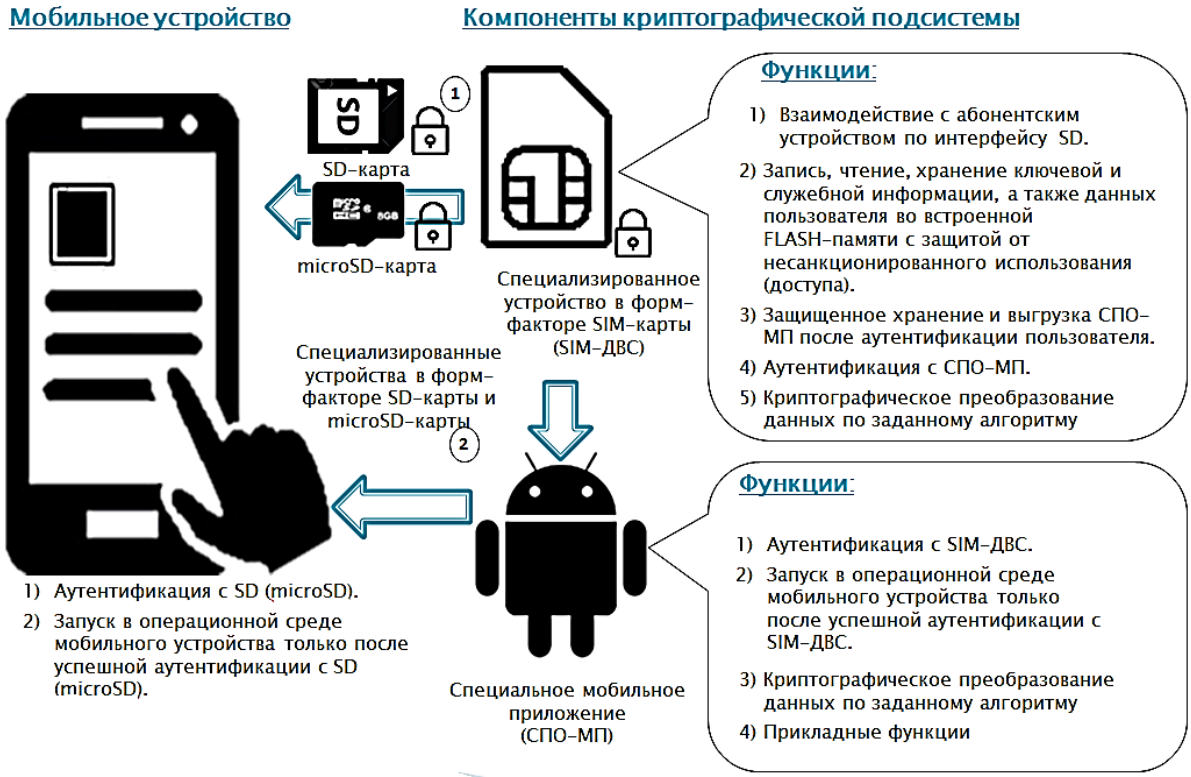


Рис. 2.6. Принцип встраивания криптографической подсистемы в мобильное устройство

Рассмотрим дополнительные функции, которые могут быть реализованы по отношению к функциям SIM-карт операторов сотовой связи, которые в настоящее время используются в служебной сотовой связи:

– защищенное от несанкционированного доступа хранение, а также запись/чтение ключевой криптографической и служебной информации во встроенной flash-памяти;

– защищенное хранение и запуск специального программного обеспечения, выполняющего в среде базового устройства (смартфон, планшет и т. п.) специальные функции;

– аутентификация пользователя и авторизация его полномочий только в случае успешного результата авторизации;

– выполнение с аппаратной поддержкой в доверенной изолированной среде SIM-карты функций криптографической защиты информации на основе российских криптографических алгоритмов: шифрования, имитозащиты, вычисления хэш-функции, цифровой подписи.

При этом существенным является тот факт, что ключи и прочая служебная информация, необходимая для работы криптографических

алгоритмов, никогда не будет выводиться за пределы доверенной и защищенной среды SIM-карты и, следовательно, не может быть явно скомпрометирована.

Требования к защищенной ведомственной системе мобильного широкополосного беспроводного радиодоступа, которая должна функционировать как виртуальная частная сеть (VPN) по отношению к сетям связи общего пользования

С учетом указанных выше положений можно сделать вывод, что защищенная система мобильного широкополосного беспроводного доступа, которая должна функционировать как виртуальная частная сеть (VPN) по отношению к сетям связи общего пользования, может быть использована в качестве транспортной инфраструктуры для организации цифровой защищенной интегрированной радиосвязи (ЦЗИР). Пример организации ЦЗИР приведен на рисунке 2.7.

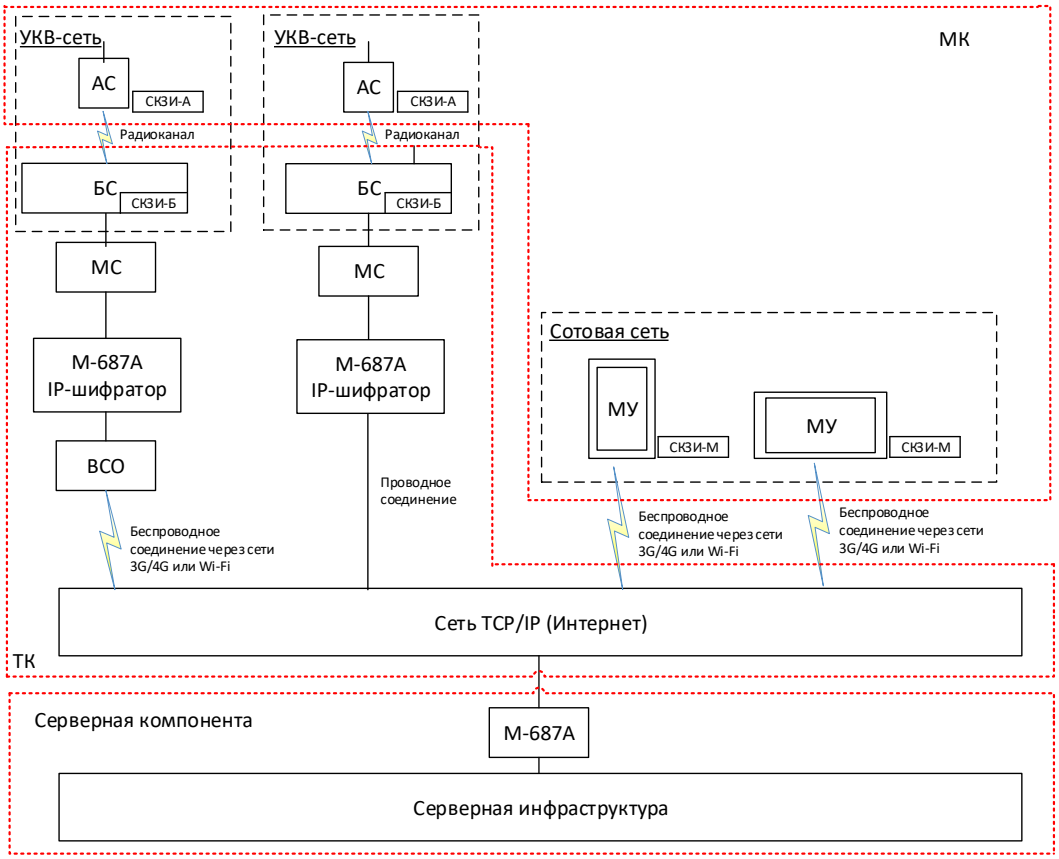


Рис. 2.7. Цифровая защищенная интегрированная радиосвязь (ЦЗИР):
АС – абонентская УКВ-станция;
БС – базовая УКВ-станция;
МС – модуль (устройство) сопряжения;

ВСО – вспомогательное сетевое оборудование (обеспечивает возможность подключения к сети Интернет беспроводным способом через сети 3G/4G или Wi-Fi) (маршрутизатор);

МК – мобильная компонента;

ТК – транспортная компонента;

МУ – мобильное устройство (смартфон или планшет)

В качестве оборудования криптографической защиты информации может быть использовано изделие М-687А, разработанное акционерным обществом «Пензенский научно-исследовательский электротехнический институт» [70, 72]. Внешний вид изделия М-687А показан на рисунке 2.8.

Рис. 2.8. Внешний вид изделия М-687А

Данный модуль предназначен для работы в мультисервисных сетях. Изделие обеспечивает:

– криптографическую защиту IP-пакетов методом полной инкапсуляции;

прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования – ГОСТ 28147-89;

– контроль целостности пакетов данных – имитозащиту по ГОСТ 28147 89;

– аутентификацию источника данных;

– поддержку фрагментации пакетов;

– пропускную способность 94 Мбит/с при длине передаваемых пакетов 1400 байт;

– гибкую полнофункциональную настройку изделия (с ПЭВМ);

– межсетевое экранирование информационных потоков с выполнением. следующих требований: возможность дистанционного мониторинга и управления ключевой информации от аппаратуры децентрализованного изготовления ключа (М-684), защиту от НСД при вскрытии корпуса, круглосуточную необслуживаемую работу.

Изделие подключается к локальной сети (или отдельной станции), а также к оборудованию транспортной сети по интерфейсам Ethernet (10BASE-T, 100BASE-TX, RJ-45 на скоростях 10 и 100 Мбит/с) и поддерживает протокол Ethernet 802.3 на портах, не внося ограничений в работу протоколов верхних уровней [72].

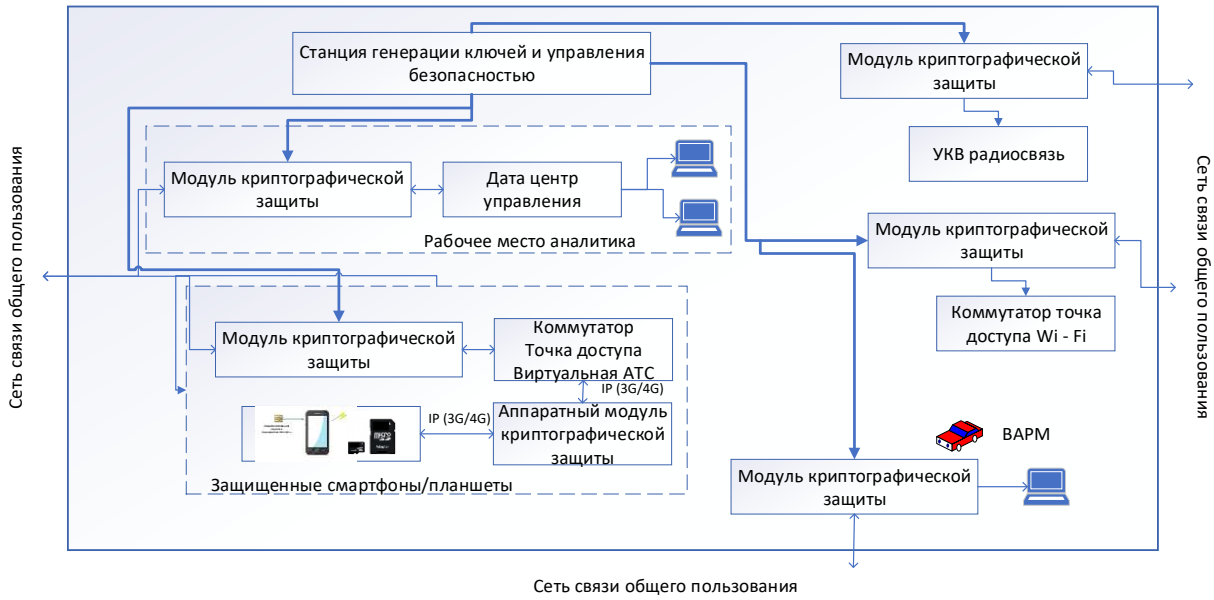


Рис. 2.9. Структурная схема фрагмента криптографически защищенной среды информационного взаимодействия разнородных сетей, организованной на действующей инфраструктуре сотовых операторов и интернет-провайдеров

ЦЗИР предназначена для организации системы территориально-распределенной цифровой радиосвязи (стандарт APCO 25, DMR, LTE), функционирующей как виртуальная частная сеть (VPN), по отношению к сетям общего пользования [77].

ЦЗИР должна обеспечивать:

– защиту информационного взаимодействия всех существующих сетей цифровой радиосвязи, переводимых на новую технологическую платформу, перспективных (вновь создаваемых) сетей цифровой радиосвязи и системы мобильного широкополосного беспроводного радиодоступа (МШПД) независимо от производителей оборудования радиосетей и применяемых стандартов цифровой радиосвязи;

– защищенное информационное взаимодействие существующих и перспективных цифровых радиосетей, а также перспективной МШПД со специализированными ведомственными сервисами;

– комплексное применение средств и сетей различных видов связи в правоохранительной деятельности;

– создание ведомственной системы МШПД, которая должна функционировать как виртуальная частная сеть по отношению к сетям общего пользования;

– взаимодействие ЦЗИР с АТС и защищенное информационное взаимодействие абонентов цифровых радиосетей через сети общего пользования;

– криптографическую защиту информации, циркулирующей в перспективных цифровых радиосетях и в сетях МШПД, на базе

портативных сертифицированных отечественных средств криптографической защиты.

ЦЗИР должна функционировать как виртуальная частная сеть по отношению к сетям общего пользования на основе протоколов TCP IP.

ЦЗИР должна быть организована на базе перспективных телекоммуникационных технологий, в том числе на основе сервис-ориентированной архитектуры, и должна представлять собой интегрированную среду информационного взаимодействия различных разнородных комплексов и систем связи.

ЦЗИР должна иметь собственную ведомственную серверную компоненту (ВСК), к которой предъявляются следующие требования:

– на основе ВСК должны осуществляться плановое и оперативное конфигурирование (реконфигурирование) системы, а также контроль ее функционирования.

– на основе ВСК должна быть организована система служб и сервисов информационного обмена и управления ЦЗИР. Требования к ВСК, включая требования к составу системных служб и сервисов, уточняются в ТТЗ на ОКР.

ВСК должна быть организована таким образом, чтобы была обеспечена ее полная функциональная достаточность и автономность работы, чтобы была исключена зависимость от каких-либо сторонних контролирующих и управляющих ресурсов.

ЦЗИР должна иметь транспортную компоненту (ТК), к которой предъявляются следующие требования:

- ТК должна функционировать как виртуальная частная сеть по отношению к стационарным и беспроводным мобильным сетям общего пользования на основе протоколов TCP IP.
- ТК должна обеспечивать интеграцию и информационное взаимодействие:

– существующих цифровых радиосетей (ТК для существующих цифровых радиосетей должна служить новой технологической платформой);

– перспективных (вновь создаваемых) цифровых радиосетей;

– сетей МШПД;

– мобильной компоненты ЦЗИР;

– единой мультисервисной системы;

– локальных вычислительных сетей и отдельных рабочих мест.

- ТК должна обеспечивать возможность комплексного применения средств и сетей различных видов связи на одном информационном направлении комбинированных линий и каналов связи.
- ТК должна обеспечивать взаимодействие абонентов разнородных цифровых радиосетей и расширение радиопокрытия систем цифровой

радиосвязи вне зависимости от физической удаленности между абонентами и отдельными радиосетями на всей территории Российской Федерации.

- В составе ТК должно быть использовано шлюзовое оборудование, обеспечивающее подключение к ЦЗИР разнородных цифровых радиосетей различных поколений вне зависимости от производителей оборудования и используемых стандартов цифровой радиосвязи.
- Подсистема криптографической защиты ТК должна быть организована на основе шифровальной аппаратуры, предназначенной для обработки конфиденциальной информации, не содержащей сведений государственной тайны с классом защиты не ниже КА согласно требованиям ФСБ Росси и модели нарушителя.

ЦЗИР должна иметь мобильную компоненту (МК), к которой предъявляются следующие требования:

- МК должна функционировать как виртуальная частная сеть по отношению к беспроводным (мобильным) сетям общего пользования на основе протоколов TCP IP.
- Сопряжение МК и ТК должно осуществляться по широкополосным каналам беспроводного доступа 3G, 4G, (LTE), Wi-Fi.
- Абонентское оборудование широкополосного доступа МК должно быть создано на основе:

– отечественных смартфонов, функционирующих под управлением отечественной сертифицированной мобильной операционной системы «Аврора» и программного обеспечения отечественной разработки;

– отечественных планшетных компьютеров, функционирующих под управлением отечественной сертифицированной мобильной операционной системы «Аврора» и программного обеспечения отечественной разработки.

- Смартфоны и планшетные компьютеры в составе ВМК должны обеспечивать функции комбинированных широкополосных устройств, обеспечивающих:

– доступ во все радиосети, сопрягаемые с ТК, инвариантно по отношению к их оборудованию и применяемым стандартам цифровой радиосвязи;

– доступ к службам и сервисам ВСК ЦЗИР;

– доступ к сервисам единой мультисервисной системы.

- В абонентском оборудовании перспективных (вновь создаваемых) цифровых радиосетей и МК в составе ЦЗИР должны быть использованы единые (однотипные) отечественные высокотехнологичные портативные средства криптографической защиты информации (СКЗИ).

СКЗИ в составе абонентского оборудования МК (цифровых радиосетей и МШПД) должны представлять собой автономные, легко отчуждаемые (легко заменяемые) устройства, сертифицируемые по классу защиты КС2 (КС3) согласно требованиям ФСБ России и модели нарушителя, и выполненные в стандартном форм-факторе micro SD-карт.

ЦЗИР должна обеспечивать возможность масштабирования как по вертикали, так и по горизонтали (по субъектам Российской Федерации, вплоть до отдельных удаленных рабочих мест и подвижных абонентов).

Встраиваемая криптографическая подсистема позволит обеспечить безопасность информационного взаимодействия разнородных сетей, организованного на действующей инфраструктуре сотовых операторов и интернет-провайдеров. На основе анализа предложены решения по реализации системы связи на базе технологии VPN.

2.6. Моделирование защищенного канала спутниковой связи органов внутренних дел с использованием аппаратуры оптимизации трафика

Оперативное развертывание сети спутниковой связи Министерства внутренних дел Российской Федерации в масштабе всей страны эффективно реализовано с применением технологии VSAT. Уникальность геостационарной орбиты в основном определяется глобальной зоной покрытия спутника, достигаемой благодаря значительной высоте – 36 000 км над землей [79, 80]. Сеть спутниковой связи органов внутренних дел Российской Федерации является составной частью интегрированной мультисервисной телекоммуникационной системы (ИМТС), построена на базе геостационарных спутников-ретрансляторов, состоит из центральной земной станции спутниковой связи (ЦЗССС) и спутниковых терминалов (малых земных станций спутниковой связи (МЗССС)), установленных по месту дислокации органов внутренних дел Российской Федерации [81]. Зона потенциального обслуживания ЦЗССС определяется зоной покрытия используемого космического аппарата. В настоящий момент для связи применяется спутник «Ямал-402», обеспечивающий покрытие европейской территории Российской Федерации и Сибири.

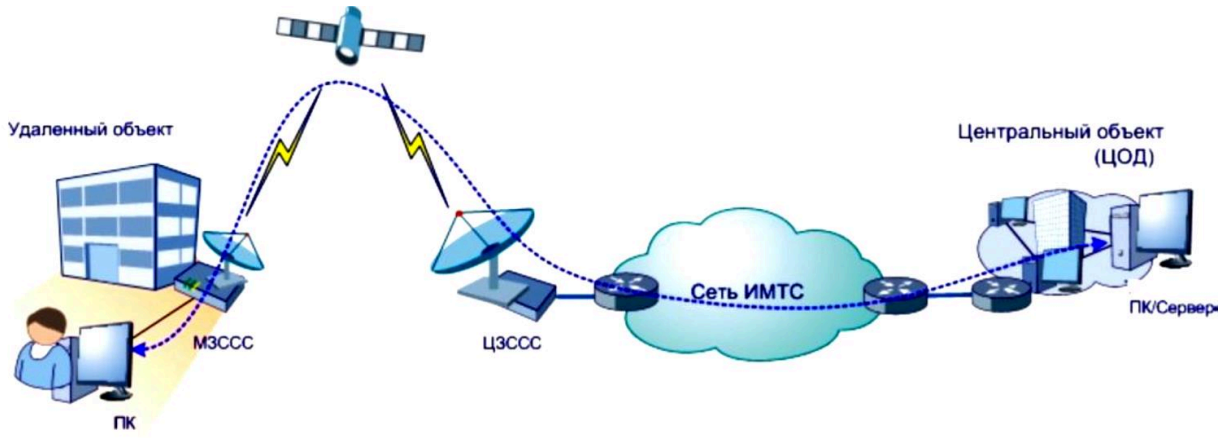


Рис. 2.10. Схема подключения к ресурсам ИСОД с использованием спутниковых каналов связи

В ряде случаев канал связи реализуется до региональных баз данных. При этом трафик от VSAT терминала на удаленном объекте передается на ЦЗССС через космический аппарат, разворачивается на пограничном маршрутизаторе ЦЗССС обратно в спутниковый сегмент сети и передается снова через космический аппарат на VSAT станцию, подключенную к региональным базам данных. Таким образом, трафик передается в два спутниковых скачка, что увеличивает задержку в передаче данных в два раза.

В настоящее время в МВД России активно используется спутниковый канал связи. Данный вид связи позволяет организовать канал связи между малыми земными станциями, расположенными на больших расстояниях, и делает возможным обслуживание абонентов в труднодоступных и удаленных местах дислокации. В рамках развития сети связи специального назначения МВД России спутниковые решения могут обеспечить реализацию задач по организации связи в интересах:

– подразделений и объектов МВД России на всей территории РФ;

– ситуационных центров, центров обработки данных (ЦОД);

– мобильных центров управления;

– подразделений МВД России в местах возникновения ЧС и проведения антитеррористических операций;

– необслуживаемых контрольных пунктов;

– постов ГИБДД;

– мобильных групп.

Стационарный объект представляет собой антенную систему с диаметром зеркала 1,2, 1,8 метра с приёмником LNB PLL, передатчиком 4 В. На узлах связи, в непосредственной близости от антенного поста, устанавливается модем SkyEdge II, а оконечное оборудование выполнено на базе 4-портового IP-маршрутизатора. Все объекты обеспеченны системой резервного питания (ИБП) с дополнительными аккумуляторными батареями, которые справляются с задачей по поддержанию работоспособности станции спутниковой связи в случае отключения основной питающей электрической сети до момента запуска резервных генераторов на объекте. Скорость спутникового канала связи единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России составляет 2 Мб/с. Такой скорости достаточно для работы сотрудника полиции с сервисами ИСОД МВД России.

Основными способами обеспечения безопасности передачи информации в спутниковом канале от абонента к абоненту являются: ограничение физического доступа к каналу связи; применение аппаратно-программных средств защиты информации [82, 83, 84]. Для полноценной работы пользователей в сервисах ИСОД МВД России и возможности использования спутникового канала связи необходимо применение шифрования передаваемой информации после приема трафика

спутниковым модемом. С учетом применения криптографических преобразований передаваемой информации скорость передачи значительно уменьшается, что затрудняет работу сотрудника полиции в сервисах ИСОД. Данную проблему можно решить, применяя аппаратуру оптимизации сетевого трафика.

Оптимизаторы wide area network (WAN) соединений наряду с выполнением кэширования и сжатия сетевого трафика оптимизируют протоколы от сетевого до прикладного уровня, что позволяет гораздо эффективнее использовать пропускную способность WAN каналов и добиться многократного ускорения работы распределенных приложений. В России наиболее известны аппаратно-программные комплексы оптимизации сетевого трафика от компаний производителей Riverbed, Cisco, Juniper, BlueCoat. К основным методам WAN оптимизации относятся: сжатие данных; дедупликация; кэширование файлов; Forward Error Correction; оптимизация работы протоколов TCP/IP; оптимизация сетевого взаимодействия приложений; управление загрузкой канала связи [85].

Проведем тестирование аппаратуры оптимизации трафика с целью увеличения скорости передачи информации после шифрования. В качестве примера рассмотрим методы оптимизации трафика с использованием средств защиты информации в компьютерной системе, предложенные в работе [86]. Для определения влияния средств криптографической защиты информации на параметры сетевого трафика, проходящего по спутниковым каналам связи, необходимо провести моделирование принципиально различных схем подключения к защищаемым ресурсам.

Методика проведения моделирования защищенного канала спутниковой связи органов внутренних дел с использованием аппаратуры оптимизации трафика

Моделирование нужно проводить с учетом нормальных погодных условий, не влияющих на характеристики спутниковых каналов связи. Логика моделирования строится на переключении одного и того же автоматизированного рабочего места пользователя между несколькими различными каналами связи: незащищенный, защищенный, защищенный оптимизированный.

Целью моделирования является оценка влияния используемых средств криптографической защиты информации (СКЗИ) на пропускную способность спутниковых каналов связи с учетом предложений разработчиков соответствующего программного обеспечения и программно-аппаратных комплексов, а также с учетом внедрения сетевых оптимизаторов трафика. В качестве оптимизатора трафика при моделировании будем использовать решение Riverbed Technology, сервер серии Steelhead. Принцип действия предлагаемых устройств основывается

на системе Riverbed Optimization System (RiOS), ядром которой являются алгоритмы блочной оптимизации Transaction Predicition (предсказание пересылки) и Scalable Data Referencing (SDR) для оптимизации TCP трафика, что обеспечивает значительное увеличение скорости обмена информации между узлами сети [87]. ПАК ViPNet Coordinator HW 100 и ПАК ViPNet Coordinator HW 2000 в схеме моделирования будут осуществлять функции СКЗИ.

Специализированный стенд для проведения моделирования защищенного канала спутниковой связи органов внутренних дел условно состоит из трех подключаемых зон ответственности:

– зона пользователя, подключаемая к спутниковому модему удаленной точки доступа;

– зона информационной системы, включающая в себя ресурсы ИСОД МВД России, подключаемые к центральной земной станции спутниковой связи «ИМТС Космос»;

– зона спутникового канала связи.

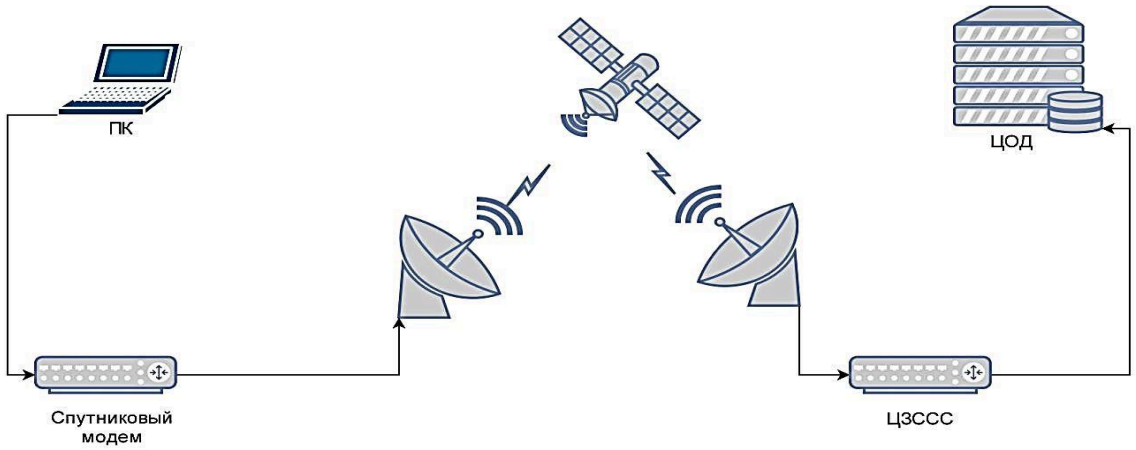


Рис. 2.11. Подключение АРМ к сервисам ИСОД МВД России без использования СКЗИ

Во всех трех зонах для выявления причин падения и повышения пропускной способности канала связи необходимо установить и использовать программу-анализатор сетевого трафика Wireshark, а также встроенные анализаторы апробируемых СКЗИ. Для сравнения результатов подключения к сервисам ИСОД можно использовать структурные схемы реализации трех типов.

На рисунке 2.12 показана схема установки СКЗИ ПАК ViPNet Coordinator в зонах пользователя и в зоне информационной системы.

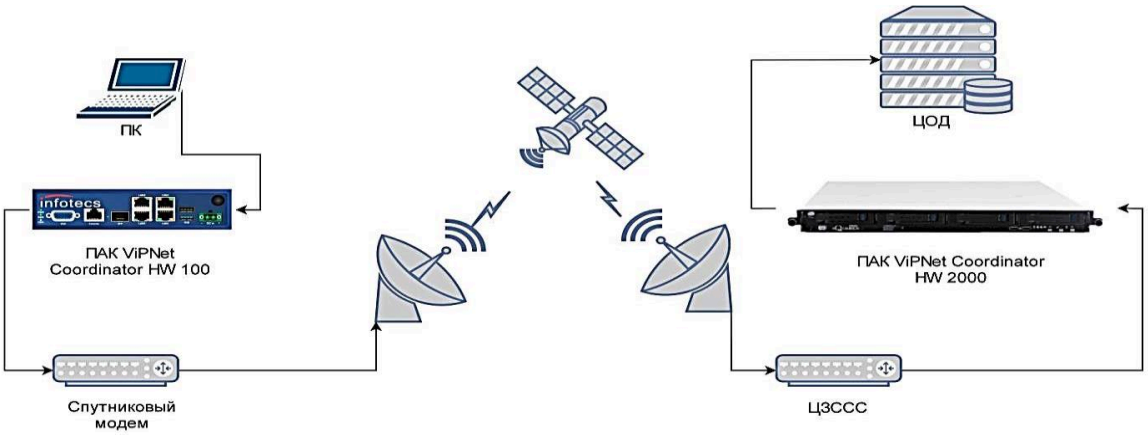


Рис. 2.12. Подключение АРМ к сервисам ИСОД МВД России
с использованием СКЗИ

Схема на рисунке 2.13 учитывает установку дополнительного оборудования – сетевых оптимизаторов трафика.

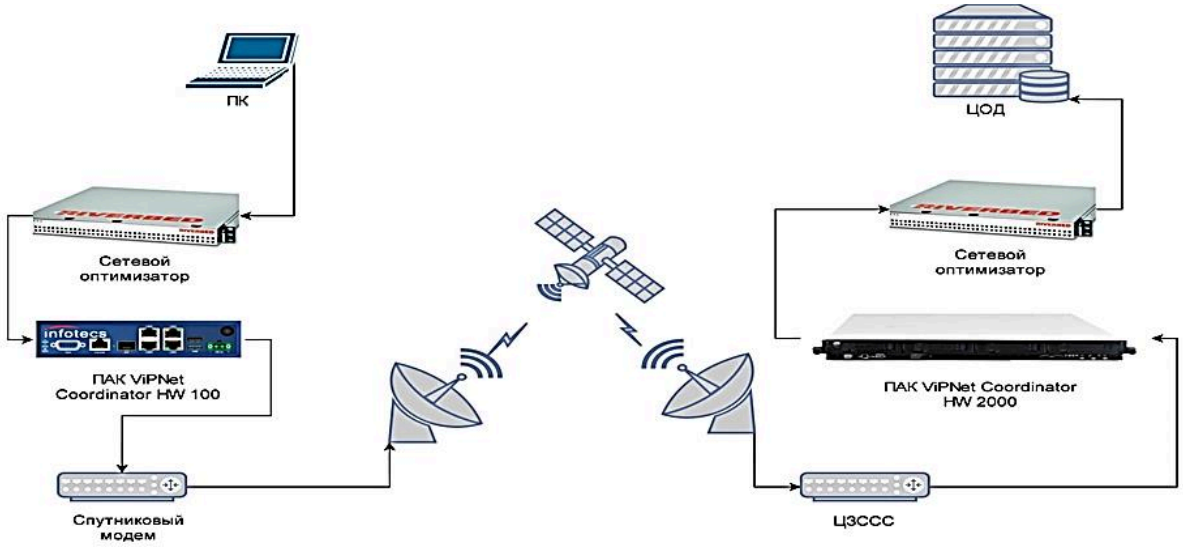


Рис. 2.13. Подключение АРМ к ресурсам ИСОД МВД России
с использованием СКЗИ и оптимизацией трафика

В зоне пользователя установлен ПАК ViPNet Coordinator HW 100, а в зоне информационной системы – ПАК ViPNet Coordinator HW 2000.

Установка может осуществляться «вразрез» трафика по пути следования оптимизированного потока данных с учетом всех требований информационной безопасности к типовому автоматизированному рабочему месту (АРМ) ИСОД МВД России. Для первичного анализа полученных замеров достаточно сравнить tcpdump с точек, указанных на рисунке 2.14. Точки захвата сетевого трафика – это сетевая карта типового АРМ ИСОД МВД России и точка обработки трафика на ЦЗССС.

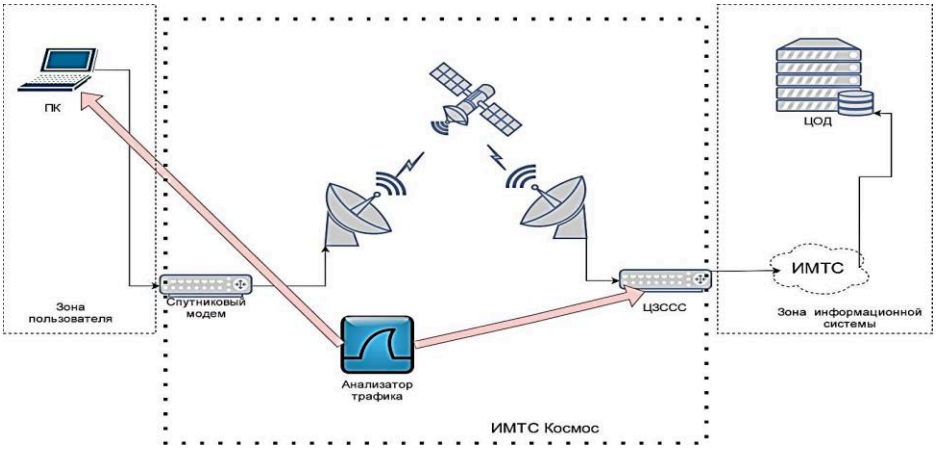


Рис. 2.14. Места установки анализатора трафика

Таблица 2.2. Сравнительный анализ методов моделирования

№ п/п.	Метод моделирования	Спутниковый канал связи	Защищенный СКС	Защищенный оптимизированный СКС
1	ftp-сервер (загрузка файла с ПК на серверы ИСОД)	11 МБ (≈0,24 МБ/с)	11 МБ (≈0,129 МБ/с)	11 МБ (≈0,647 МБ/с)
2	СВКС-М (встроенный тест скорости)	Ограничение: ADSL-1 вх: 3435 кб исх: 1742 кб	Ограничение: ADSL-1 вх: 1447 кб исх: 1386 кб	Ограничение: ADSL-1 вх: 15972 кб исх: 7374 кб
3	СЭД (встроенный тест скорости)	вх: 1,7 мб/с исх: 8,38 мб/с	вх: 0,23 мб/с исх: 8,37 мб/с	вх: 14,45 мб/с исх: 8,63 мб/с
4	Настройка типового рабочего места (встроенный тест скорости)	вх: 2,36 МБ/с исх:0,76 МБ/с	вх: 0,29 МБ/с исх:0,22 МБ/с	вх: 0,10 МБ/с исх: 0,03 МБ/с
5	СЭП (загрузка файла с ПК на серверы ИСОД)	11 МБ (≈0,22 МБ/с)	11 МБ (≈0,134 МБ/с)	11 МБ (≈2,75 МБ/с)
6	СЭП (загрузка файла с сервера ИСОД на ПК)	11 МБ (≈0,73 МБ/с)	11 МБ (≈0,189 МБ/с)	11 МБ (≈1,46 МБ/с)
7	СВКС-М (тестовый сеанс связи)	распознается видео и аудио, задержки в 0,5–1 секунду	распознается видео и аудио, задержки в 515 секунд	распознается видео и аудио, задержки в 3–5 секунд

Учитывая рекомендации разработчиков АО «Инфотекс», СКЗИ будет обновлено до версии 4.3.2.-3404 (HW2000) и 4.3.2-3446 (HW100), данное программное обеспечение сертифицировано по линии ФСБ России, но в МВД России в настоящее время только ожидается его поступление [87]. Для регулировки передачи зашифрованных данных за одну итерацию возьмем изменение максимального размера полезного блока данных одного пакета (MTU) на СКЗИ до значения 1400 байт.

Проверка работы сервисов ИСОД может осуществляться на пользовательском уровне посредством использования стандартных сервисов ИСОД МВД России: ВИСП, СЭД, СЭП, СВКС-М, дополнительного FTP-сервера и SFTP-сервера и инструментов замера трафика, встроенных в описанные сервисы. Некоторые графики зависимости динамического изменения скорости от времени представлены на рисунках 2.15–2.20 (по оси ординат – скорость загрузки данных в битах в секунду, по оси абсцисс – время в секундах). Выдержки соответствующих результатов из обширной экспериментальной базы моделирования представлены в таблице 2.2.

При выполнении моделирования п. 5, п. 6 наблюдается резкое изменение скорости, если загрузка файла осуществляется второй и более итерацией (скорость достигала 15 МБ/с). По информации от производителей аппаратуры оптимизации трафика, данный эффект дает само оборудование, сохраняя ранее переданные файлы в памяти устройства. В случае моделирования «защищенный оптимизированный СКС» п. 2, п. 3 показатели скорости выше пропускной способности канала, что может демонстрировать неэффективность встроенного инструмента замера скорости.

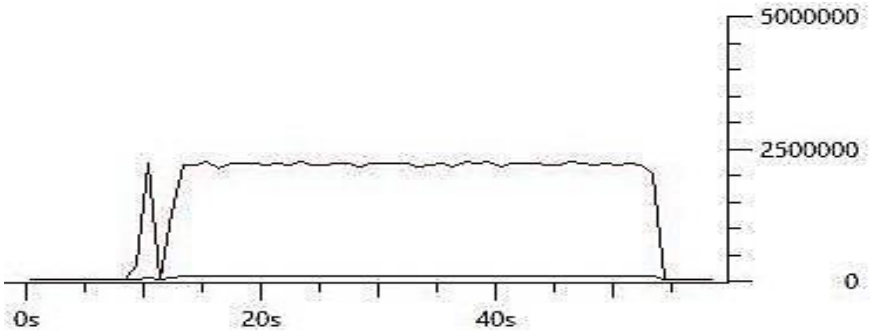


Рис. 2.15. График зависимости динамического изменения скорости от времени (незащищенный спутниковый канал связи, загрузка файла с ПК на сервер ИСОД МВД России)

Для выявления эффектов оптимизации в результатах моделирования из таблицы используются файлы, отличающиеся друг от друга типами и размерами.

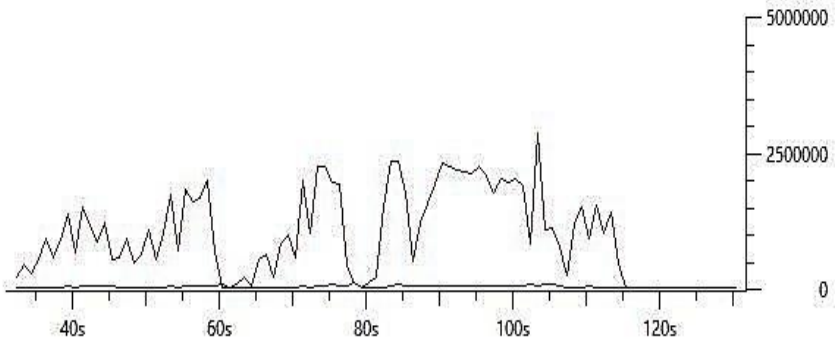


Рис. 2.16. График зависимости динамического изменения скорости от времени (спутниковый канал связи с использованием СКЗИ, загрузка файла с ПК на сервер ИСОД МВД России)

Использование СКЗИ демонстрирует частые потери скорости на СКС (рис. 2.16), но при этом наличие сетевого оптимизатора благоприятно сказывается на передаче данных, но не доводит показатели скорости до первоначальных значений (рис. 2.17).

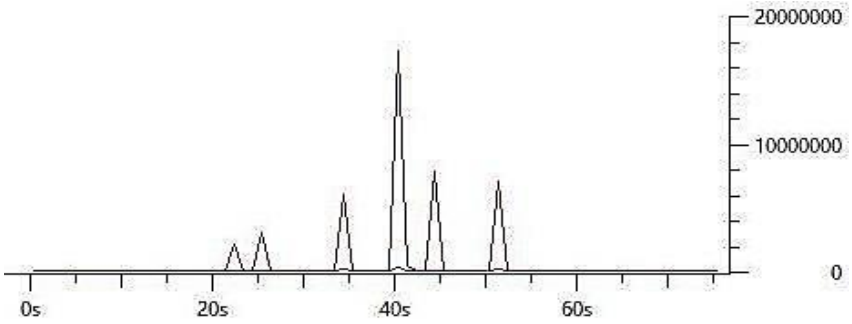


Рис. 2.17. График зависимости динамического изменения скорости от времени (спутниковый канал связи с использованием СКЗИ и оптимизацией трафика, загрузка файла с ПК на сервер ИСОД МВД России)

В случае со скачиванием файла с соответствующих ресурсов картина похожая, но значения скоростей гораздо меньше, чем при загрузке файла на сервер (рис. 2.17-2.20), из чего можно сделать вывод, что для устранения возможных причин асимметрии загрузки данных рекомендуется учитывать требования по настройке и конфигурированию сетевых оптимизаторов трафика.

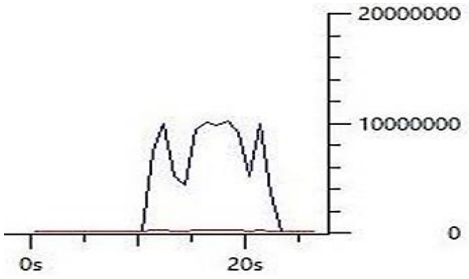


Рис. 2.18. График зависимости динамического изменения скорости от времени (не защищенный спутниковый канал связи при осуществлении загрузки файла с сервера ИСОД МВД России на ПК)

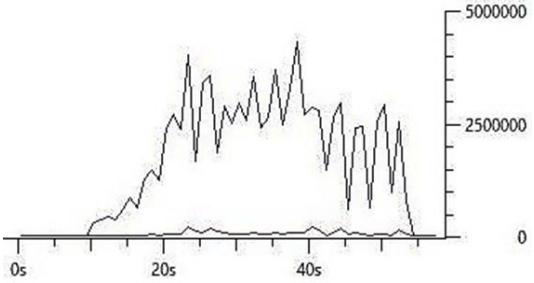


Рис. 2.19. График зависимости динамического изменения скорости от времени (спутниковый канал связи с использованием СКЗИ при осуществлении загрузки файла с сервера ИСОД МВД России на ПК)

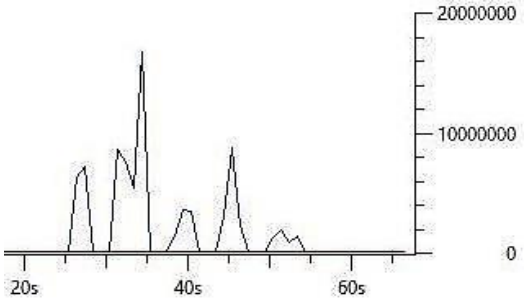


Рис. 2.20. График зависимости динамического изменения скорости от времени (спутниковый канал связи с использованием СКЗИ и оптимизацией трафика СКЗИ при загрузке файла с сервера ИСОД МВД России на ПК)

Применение данного оборудования целесообразно в распределенных ведомственных сетях для передачи данных по спутниковым каналам между удаленными подразделениями органов внутренних дел. В этом случае объем передаваемого трафика снижается в 3-5 раз, а пиковая скорость передачи данных возрастает.

Результаты моделирования защищенного канала спутниковой связи органов внутренних дел с использованием аппаратуры оптимизации трафика позволяют сделать вывод о том, что аппаратура оптимизации работает и позволяет улучшить параметры пропускной способности

защищенного канала спутниковой связи. Использование защищенного канала спутниковой связи для доступа к сервисам ИСОД МВД России в совокупности с сетевой оптимизацией трафика позволяет повысить эффективность передачи данных. В настоящий момент оптимизация защищенного канала спутниковой связи со стороны СКЗИ не требует модернизации оборудования, а лишь показывает эффективность включения в состав защищенного спутникового канала связи аппаратуры оптимизации сетевого трафика.

2.7. Радио-, радиотехнического контроль как инструмент оптимизации системы управления и связи ОВД

Современное развитие инфокоммуникационных технологий, средств информатизации, автоматизации связи и их широкое внедрение в практику деятельности подразделений органов внутренних дел (ОВД) приводят к актуализации вопросов, связанных с организацией радио-, радиотехнического контроля (РРТК).

Организация радио-, радиотехнического контроля подразделениями информационных технологий, связи и защиты информации территориальных органов внутренних дел Российской Федерации является одной из основных функций и полномочий указанных подразделений на основании приказа МВД России от 02.07.2012 № 660 «Об утверждении Типового положения о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации».

В области государственной и общественной безопасности увеличивается количество атак на объекты критической информационной инфраструктуры в связи с увеличением разведывательной деятельности иностранных государств в отношении Российской Федерации [1]. В соответствии с приказом МВД России от 21.12.2020 № 878 «Об утверждении Регламента по использованию комплексов (средств) радио-, радиотехнического контроля при проведении мероприятий по охране общественной безопасности» по организации РРТК [1] регламент определяет порядок использования комплексов (средств) радио-, радиотехнического контроля при проведении мероприятий по охране общественного порядка и обеспечению общественной безопасности.

Территориальный орган МВД России на региональном уровне включает комплекс (средство) РРТК в соответствующий раздел плана использования сил и средств по обеспечению правопорядка на улицах в иных общественных местах и плана обеспечения безопасности граждан и общественного порядка при проведении публичных и массовых мероприятий.

Сотрудник подразделения информационных технологий, связи и защиты информации территориального органа МВД России на региональном уровне, использующий комплекс средств РРТК, при выявлении фактов нарушения дисциплины связи осуществляет незамедлительный доклад руководителю, ответственному за организацию связи при проведении мероприятия по охране общественного порядка и обеспечению общественной безопасности.

При обнаружении источников радиоизлучений, создающих помехи радиоэлектронным средствам МВД России, сотрудник подразделения ИТСиЗИ МВД России производит их пеленгование и определения местоположения.

При выявлении и локализации источников радиоизлучений, создающих помехи РЭС МВД России, сотрудник подразделения ИТСиЗИ составляет и регистрирует в установленном порядке рапорт, в котором фиксирует сведения, содержащие данные о признаках административного правонарушения, предусмотренного статьей 13.4 Кодекса Российской Федерации об административных правонарушениях.

Мероприятия РРТК в системе органов внутренних дел Российской Федерации – это наблюдение за установленным порядком работы РЭС МВД России в целях проверки выполнения требований электромагнитной совместимости и соблюдения режимов работы, норм технической эксплуатации и правил работы, поиска и обнаружения легальных (зарегистрированных) и нелегальных (незарегистрированных) радиопередатчиков и источников других радиоизлучений, опознавания и определению местоположения их источников, создающих радиопомехи РЭС МВД России, выявления противоправного использования радиопередающих систем. Мероприятия проводятся гласно и не ограничивают конституционных прав граждан.

Мероприятия РРТК проводятся с целью защиты радиоэлектронных средств МВД России от вредного помехового воздействия различных РЭС, работающих в полосах радиочастот, назначенных МВД России. Мероприятия по РРТК в полосах радиочастот категории преимущественного пользования РЭС, используемыми для нужд МВД России, осуществляются в порядке, согласуемом, соответственно, с Минобороны России.

Мероприятия РРТК осуществляются в целях:

– выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения;

– выявления источников радиопомех;

– обеспечения электромагнитной совместимости РЭС МВД России.

При осуществлении РРТК проводятся:

– эфирные измерения параметров излучений РЭС МВД России и высокочастотных устройств (напряженности электромагнитного поля, отклонений несущей частоты от номинала, уровня внеполосных излучений, излучаемой мощности, формы диаграммы направленности передающей антенны, иное), влияющих на ЭМС с другими РЭС МВД России;

– радиопеленгация и локализация исследуемых источников излучений с выдачей рекомендаций для поиска соответствующим локальным сетям, на территории которых находятся пеленгуемые передатчики и другие источники радиопомех;

– звуковой контроль (прослушивание служебной связи, позывных сигналов радиостанций, иное) с целью подтверждения требуемого качества звучания, нелинейных искажений, разборчивости и влияния помех;

– определение зон уверенного приема сигналов РЭС МВД России;

– оценка степени занятости (загрузки) РЧС сигналами РЭС МВД России;

– проверка выполнения временных запретов (ограничений) на использование РЭС МВД России пользователями РЧС;

– оценка условий обеспечения ЭМС РЭС МВД России и высокочастотных устройств;

– предоставление в органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций сведений о выявленных нарушениях в использовании радиочастот или радиочастотных каналов РЭС МВД России высокочастотными устройствами и иными техническими средствами.

РРТК осуществляется с использованием предназначенного для этого оборудования, соответствующего действующим в Российской Федерации ГОСТам, техническим регламентам и санитарным нормам. Измерения при проведении РРТК выполняются с применением средств измерений утвержденного типа, прошедших поверку.

Запрещается проведение мероприятий РРТК в полосах радиочастот не назначенных МВД России, за исключением случаев участия в совместных мероприятиях согласно Регламенту взаимодействия в ходе осуществления радио-, радиотехнического контроля и мониторинга радиочастотного спектра на территории Российской Федерации, утвержденному совместным приказом Минобороны России, МВД России, Минкомсвязи России, ФСБ России, ФСО России, ФСТЭК России и ФТС России от 30 июня 2010 г. № 669дсп/472дсп/88дсп/321дсп/295дсп/372дсп/1260дсп.

Техническое обеспечение радио-, радиотехнического контроля подразделениями ИТСиЗИ МВД России

По своему эксплуатационному назначению комплексы (средства) РРТК подразделяются на стационарные, мобильные, носимые и дополнительное оборудование (измерительные средства).

Стационарные комплексы (средства) РРТК предназначены для автоматизированного и автоматического поиска, пеленгования и определения местоположения источников радиоизлучения, измерения параметров радиосигналов, высокие тактико-технические характеристики которых достигаются за счет конструкций антенно-мачтовых устройств и высоты подъема приемных антенн. Стационарные комплексы (средства) РРТК управляются дистанционно, что позволяет использовать их в автоматизированной системе РРТК.

Мобильные комплексы (средства) РРТК предназначены для поиска, пеленгования и определения местоположения источников радиоизлучения во время движения к источнику радиоизлучения. Электропитание оборудования осуществляется от источников, размещенных на борту транспортного средства. Мобильные средства РРТК по своим конструктивным особенностям уступают стационарным постам в функциональности, так как антенная система монтируется на автотранспортном средстве, что приводит к уменьшению рабочей зоны наблюдения за радиосредствами.

Носимые комплексы (средства) РРТК предназначены для поиска, пеленгования и определения местоположения источников радиоизлучения на временных постах РРТК и в труднодоступных местах и районах, а также для уточнения места источника радиоизлучения после определения стационарными и носимыми комплексами (средствами) РРТК. К ним применяются требования по габаритам, массе и электропитанию.

Дополнительное оборудование (измерительные средства) предназначено для измерения параметров сигналов, применяется для обнаружения сигналов, технического анализа и используется в стационарных, мобильных и носимых комплексах (средствах) РРТК.

В настоящее время используются различные средства радиомониторинга, включающие в себя антенны, приемные устройства, анализаторы и измерители параметров сигналов, программное обеспечение, а также автоматизированные комплексы различного назначения [4, 5].

Комплекс «Барс-МПИ2», в частности, обеспечивает: определение занятости полос радиочастот, а также радиочастот и радиочастотных каналов, построение панорамы спектра в координатах «частота-время» с отображением уровней сигнала в цвете, измерение частоты радиоизлучений, измерение уровня радиоизлучений, прослушивание и/или запись сигналов (слуховой контроль) с формированием временных меток, определение направления (пеленгование) на источник излучения (в том числе помех) с отображением информации на картографическом фоне, определение координат источников радиоизлучений при работе радиопеленгаторов в составе пеленгаторной группы, определение координат и курса в движении.

Так, в органах внутренних дел применяется комплекс «Барс-МПИ2»,

который предназначен для поиска, обнаружения, экспресс-анализа радиоизлучений в диапазоне 20…3000 МГц и пеленгования их источников (рис. 2.21).

Данный комплекс был эффективно использован в интересах ОВД для обеспечения технической поддержки массовых мероприятий, проводимых в городе Казани в 2013 году и в городе Сочи в 2014 году и для проведения ряда других специальных технических мероприятий в регионах Российской Федерации [6, 7].

Мобильный комплекс радиомониторинга «Барс-МПИ2» дополнительно укомплектовывается носимым комплексом поиска, обнаружения и пеленгования источников радиоизлучений «Барс-Н» (рис. 2.22).

Рис. 2.21. Комплекс пеленгования источников радиоизлучений «Барс-МПИ2» на базе автомобиля УАЗ Патриот, развернутый в Воронежском институте МВД России на кафедре инфокоммуникационных систем и технологий

Рис. 2.22. Носимый комплекс поиска, обнаружения и пеленгования источников радиоизлучений «Барс-Н»

Использование сотрудниками ОВД для решения практических задач комплексов радиотехнического контроля позволяет успешно контролировать радиочастотный спектр и обнаруживать незарегистрированные радиоизлучения, опознавать и определять местоположение их источников, выявлять незаконное или преступное использование радиопередающих систем.

Для качественного контроля радиообстановки необходимо использовать систему разнесенных комплексов РРТК. Центральный комплекс мониторинга осуществляет обнаружение и прием радиоизлучений, а мобильные комплексы РРТК осуществляют пеленгование и вычисление местоположения источника радиоизлучения. Мобильные комплексы РРТК дополнительно укомплектовываются носимым оборудованием для поиска источников радиоизлучений на местности, где прием мобильными комплексами затруднен.

Порядок организации и осуществления радио-, радиотехнического контроля подразделениями ИТСиЗИ МВД России

В повседневной деятельности РРТК проводится с целью мониторинга радиоэлектронной обстановки на территории оперативного обслуживания органа внутренних дел Российской Федерации и выявления источников преднамеренных и непреднамеренных радиопомех. При этом выполняются следующие мероприятия:

– поиск и определение местоположения источников преднамеренных и непреднамеренных помех РЭС МВД России и пресечение их работы в пределах полномочий органов внутренних дел;

– мониторинг радиоэлектронной обстановки в заданных территориальных районах.

– инструментальная оценка параметров электромагнитных полей излучений радиоэлектронных средств и (или) высокочастотных устройств;

– проверка соблюдения установленных правил радиообмена;

– проверка выполнения пользователями радиоэлектронных средств временных запретов (ограничений) на использование полос радиочастот или радиочастотных каналов, вводимых при проведении специальных мероприятий и в чрезвычайных ситуациях;

– локализация РЭС МВД России, использующих не по назначению радиочастоты или радиочастотные каналы.

При организации РРТК в качестве подготовительных мероприятий осуществляются:

– обучение сотрудников подразделений ИТСиЗИ МВД России для работы на комплексе (средстве) РРТК (в том числе допускается самостоятельное обучение) с последующим принятием зачетов на допуск к самостоятельной работе на указанном комплексе (средстве);

– проверка исправности комплекса (средства) РРТК, осуществление его ремонта и проведения технического обслуживания при необходимости;

– оборудование навигационно-мониторинговой системой мобильных средств в целях осуществления контроля за маршрутами их перемещения;

– разработка инструкции радио-, радиотехнического контроля и мониторинга радиочастотного спектра территориального подразделения ИТСиЗИ МВД России, в которой предусмотрены действия должностных лиц при выявлении источника радиопомех;

– разработка и утверждение ежеквартальных графиков осуществления мероприятий РРТК и мониторинга РЧС;

– оформление журнала учета работы комплекса (средства) РРТК;

– оформление журнала регистрации выявленных источников радиопомех радиоэлектронным средствам МВД России, нарушения порядка и правил использования РЧС.

Непосредственно перед каждым мероприятием РРТК разрабатывается и утверждается задание на проведение мероприятий РРТК и мониторинга РЧС.

К работе на комплексе (средстве) РРТК допускаются сотрудники подразделения ИТСиЗИ МВД России, обладающие соответствующими знаниями и навыками и сдавшие зачеты на допуск к самостоятельной работе.

В соответствии с разработанным заданием на проведение мероприятий РРТК и мониторинга РЧС сотрудниками подразделения ИТСиЗИ МВД России проводятся:

– сканирование полос радиочастот, выделенных для работы РЭС МВД России;

– мониторинг радиоэлектронной обстановки в заданных территориальных районах;

– поиск и определение местоположения источников преднамеренных и непреднамеренных помех РЭС МВД России и пресечение их работы в пределах компетенции;

– проверка соблюдения установленных правил радиообмена сотрудниками органов внутренних дел Российской Федерации, использующих в служебной деятельности средства радиосвязи;

– осуществление при необходимости записи переговоров служебной радиосвязи МВД России.

По результатам проведенной работы оформляется акт мероприятия РРТК.

Мероприятия РРТК проводятся при проведении общественных массовых мероприятий (ОММ). При этом в местах проведения указанных мероприятий выполняется мониторинг радиоэлектронной обстановки. Особое внимание уделяется работе каналов радиосвязи, по которым ведутся служебные переговоры руководящего и личного состава подразделений

полиции, обеспечивающих проведение ОММ. Комплексы (средства) РРТК должны учитываться в планах связи на проведение ОММ.

Выезды в случае осложнения оперативной обстановки для выполнения мероприятий РРТК осуществляются незамедлительно.

При обнаружении источников радиоизлучений, создающих помехи РЭС МВД России, производится его пеленгование и определение его местоположения.

При локализации источников радиоизлучений, создающих помехи РЭС МВД России, сотрудником, выполняющим мероприятия РРТК, составляется рапорт, в котором содержатся сведения, указывающие на наличие события административного правонарушения в соответствии с Инструкцией о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, утвержденной приказом МВД России от 29 августа 2014 г. № 736, и осуществляется вызов уполномоченного сотрудника полиции для выполнения мероприятий по компетенции.

Одновременно с рапортом предоставляется акт мероприятия радио-, радиотехнического контроля.

При поступлении информации о возникновении помех на радиочастотах, которые используются РЭС МВД России, мероприятия по их локализации и фиксированию осуществляются незамедлительно.

Организация взаимодействия с подразделениями Роскомнадзора, территориальных ФГУП «ГРЧЦ» и Минобороны России

В целях повышения эффективности проведения мероприятий РРТК органами внутренних дел организуется взаимодействие с:

- территориальными органами Роскомнадзора в части, касающейся принятия решения государственным инспектором Роскомнадзора при нарушении требований к использованию радиочастотного спектра, правил радиообмена или использования радиочастот, несоблюдения норм или параметров радиоизлучения, а также в рамках Соглашения о взаимодействии Министерства внутренних дел Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 23 августа 2017 года;
- филиалами ФГУП «ГРЧЦ» в рамках выполнения совместных мероприятий РРТК, оформления документов, обучения сотрудников, а также в случае отсутствия в подразделениях ИТСиЗИ МВД России необходимого оборудования для их проведения;
- подразделениями Минобороны России, осуществляющими функции РРТК, в рамках:

– контроля выполнения мероприятий Плана обеспечения ЭМС радиоэлектронных средств системы государственного и военного

управления федерального уровня на мирное и военное время (центральный план);

– проверки выполнения пользователями радиочастотного спектра временных запретов (ограничений) на работу радиоэлектронных средств – потенциальных источников радиопомех в условиях чрезвычайного положения, чрезвычайных ситуаций, при выполнении особо важных работ и проведении специальных мероприятий;

– выявления источников преднамеренных и непреднамеренных помех радиоэлектронным средствам военного и специального назначения и пресечения их работы в пределах компетенции.

– мониторинга радиоэлектронной обстановки в заданных территориальных районах.

– оперативного предоставления информации заинтересованной стороне при возникновении чрезвычайных ситуаций.

Наиболее оптимальным вариантом снабжения подразделений МВД России комплексами РТК видится закупка оборудования типа «Барс», которое положительно себя зарекомендовало при проведении совместных тренировок по ведению радио и радиотехнического контроля с участием Минобороны России, ФСО России, ФСБ России, ФСТЭК России и Роскомнадзора, а также при обеспечении охраны общественного порядка во время проведения общественно-массовых и спортивных мероприятий.

Указанные мобильные и носимые комплексы РРТК также широко применяются филиалами ФГУП «ГРЧЦ» в субъектах Российской Федерации и территориальными подразделениями Роскомнадзора.

Необходимо отметить, что комплексы РРТК не входят в перечень специальной техники и специальных средств, принимаемых на вооружение (снабжение, в эксплуатацию) органов внутренних дел Российской Федерации.

Учитывая изложенное, закупку комплексов РРТК для нужд подразделений МВД России предлагается осуществлять в соответствии с Федеральным законом от 05.04.2013 № 44-ФЗ как оборудование гражданского и двойного назначения.

К основным задачам обеспечения информационной безопасности ОВД относятся: совершенствование правовых, научно-практических, нормативно-технических, организационно-методических и иных основ информационной безопасности ОВД; реализация комплекса организационных (режимных) и технических мероприятий, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем ОВД от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования; создание и развитие систем информационной безопасности ОВД с учетом реализации «облачной инфраструктуры»; создание и развитие системы мониторинга

информационной безопасности ОВД; организация и совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности ОВД.

Приоритетным направлением в деятельности ОВД является качественное информационно-телекоммуникационное обеспечение их оперативных служб в различных условиях оперативной обстановки [3, 4]. При проведении массовых мероприятий, охране особо важных объектов, проведении контртеррористических операций и оперативно-служебных мероприятий особое внимание уделяется мониторингу обстановки, сбору и обработке оперативной информации.

Под мониторингом понимается определение параметров объектов и процессов во времени и пространстве. В настоящее время мы все чаще встречаемся с термином радиомониторинг, определяемым как вид деятельности по изучению и контролю радиообстановки, поиску и обнаружению легальных и нелегальных источников радиоизлучений [3]. Для органов внутренних дел это понятие трактуется гораздо шире. Специальный радиомониторинг – это получение различного рода информации с использованием технических средств на участке ее прохождения по радиоканалам. Включает в себя деятельность по изучению радиообстановки, измерению параметров радиосигналов, аудиту, поиску и контролю различных каналов радиосвязи, мобильного широкополосного доступа и других источников радиоизлучений в интересах органов внутренних дел.

Системы радиомониторинга (СРМ), сбора и обработки информации ОВД используется как инструмент решения задач от контроля радиообстановки при проведении контртеррористических операций до задач управления использованием радиочастотного спектра [3]. Такой мониторинг является технической основой как для получения оперативной информации, так и осуществления противодействия несанкционированным информационно-техническим воздействиям со стороны противоборствующей стороны.

Для обеспечения функционирования базовой инфраструктуры ведомственной системы радиосвязи, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи ОВД МВД России наиболее предпочтительным вариантом является использование существующих ресурсов ИМТС, которая предоставляет сквозную транспортную среду для сигналов управления и информационных сигналов (речь, данные) на базе стека протоколов TCP/IP (Transmission Control Protocol/Internet Protocol – Протокол управления передачей/Протокол Internet), в том числе по потоку E1, для передачи абонентского трафика и служебной информации между базовыми

станциями, АРМ диспетчера, администратора и центра управления и коммутации,

Отличительной особенностью систем сбора и обработки информации СРМ ОВД, являются: постоянно увеличивающееся или меняющееся число объектов, обслуживаемых системой, характер объектов (объекты могут часто менять свое местоположение, или быть мобильными), малые задержки системы на сигналы сигнализации, управления, разнообразие типов терминальных (исполнительных) устройств и протоколов обмена данными, сложность и большая стоимость прокладки проводных линий связи. Зачастую создание таких систем возможно только с использованием радиоканала. Система радиомониторинга должна отвечать требованиям по достоверности, надежности, задержкам в каналах связи, по обеспечению оперативного контроля состояния радиоканала, созданию гибких структур организации связи, информационной безопасности.

Перечень задач, решаемых с помощью средств радиомониторинга, включает выявление и анализ радиоизлучений для идентификации сигналов и помех, измерение параметров сигналов и помех, оценку их опасности или ценности для пользователя, измерение напряженности электромагнитного поля, определение положения источников радиоизлучений (ИРИ) и радиопомех на местности. Основными функциями радиомониторинга являются наблюдение за эфиром в широком диапазоне частот, оперативное обнаружение, анализ и локация потенциальных или специально организованных каналов противоправного информационно-технического воздействия. Аппаратура радиомониторинга должна оценивать эффективность мер противодействия таким воздействиям и в ряде случаев нейтрализовать их.

Обслуживаемые объекты и их инженерные сооружения, информация о состоянии которых обрабатывается СРМ, могут располагаться в различных районах города и определяются в соответствии с программой профилактики правонарушений, борьбы с преступностью и обеспечения безопасности граждан.

Как один из примеров радиомониторинга удаленного радиооборудования рассмотрим программное обеспечение «ТАКТ ПРО». Это программное обеспечение позволяет в системах радиосвязи, построенных на цифровых радиостанциях ТАКТ, организовать функции диспетчеризации и реализовать дополнительные услуги, расширяющие сервисные возможности таких систем. Программа имеет клиент-серверную архитектуру с возможностью разграничения доступа и определения прав для различных категорий пользователей [8].

Программа реализует: функции диспетчеризации и маршрутизации радиосвязи, взаимодействие диспетчеров, радиоабонентов и телефонных абонентов, геопозиционирование радиоабонентов на карте, ведение журнала событий, статистики и отчетов.

Программа обеспечивает: передачу, коммутацию и запись переговоров диспетчеров, радио и телефонных абонентов, передачу и запись текстовых сообщений, отображение и запись местоположения радиоабонентов, хранение и авторизованный доступ к записанным данным по переговорам, сообщениям, истории перемещений, удаленное блокирование/разблокирование радиостанций.

Программа поддерживает: цифровую телефонию VoIP по протоколу SIP, оборудование радиосвязи цифрового стандарта DMR, возможно подключение аналоговых радиостанций через аналоговый радиошлюз с ограничениями функциональности системы.

Функциональные возможности программного обеспечения подобного типа весьма обширны и обеспечивают: возможность ведения голосовых переговоров и отправку текстовых сообщений с диспетчерского места, администрирование и контроль за доступом различных категорий диспетчеров, определение прав доступа к радиоканалам, отслеживание местоположения, отображение местоположения радиоабонента на различных типах карт, отображение истории перемещений радиоабонентов, удаленное прослушивание радиоабонента (обстановки вокруг радиостанции), записи в базе данных, хранение в журнале информации обо всех происходящих событиях в системе.

Шлюз в телефонную сеть обеспечивает соединение телефонного абонента и радиоабонента автоматически или через диспетчера.

В условиях осложнения оперативной обстановки на первое место встает задача обеспечения безопасности при ведении переговоров в радиосистеме. Однако именно тот факт, что информация представляет некий оперативный интерес, может побудить потенциального нарушителя к противоправным действиям.

3. ПРОЦЕДУРЫ И АЛГОРИТМЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЦИФРОВЫХ СЕТЕЙ СВЯЗИ ОВД И ИХ СИСТЕМЫ УПРАВЛЕНИЯ

3.1. Разработка процедур экспертного оценивания и кластерного анализа для оценки эффективности функционирования сетей радиосвязи ОВД России

К процедурам оценки эффективности функционирования сетей и систем связи ОВД предъявляются следующие требования: 1) необходимость рассматривать систему связи как совокупность технического (программно-технического), программного, организационного, методического, информационного, математического, кадрового и нормативно-правового обеспечений (компонент); 2) возможность их применения в специализированной САПР (хранение всей информации в базах данных, применение для ее сбора и обработки распределенных вычислительных сетей и т. д.) [1]; 3) гибкая, легко адаптируемая под конкретную задачу, структура системы показателей качества и возможность формирования на их основе критерия оптимальности; 4) возможность их применения как для оценки качества всей сети или системы связи, так и ее отдельных элементов. Обеспечить выполнение данных требований можно путем использования экспертного оценивания и кластерного анализа.

Процедура экспертного оценивания применяется для решения следующих задач: 1) определение состава экспертных групп; 2) составление перечня задач, решаемых конкретной сетью или системой связи; 3) определение множества показателей качества (характеристик), на основе которого формируется критерий оптимальности; 4) определение весовых коэффициентов экспертов, показателей качества и задач, стоящих перед сетью связи; 4) определение степени соответствия класса сетей связи каждому классу решаемых ими задач; 5) сведение качественных характеристик к количественным.

Таким образом, объектами экспертизы являются: 1) специалисты, из которых формируются экспертные группы; 2) показатели качества функционирования сетей и систем связи; 3) решаемые сетями и системами связи задачи; 5) качественные характеристики отдельных элементов сетей и систем.

Процедура экспертного опроса для всех решаемых задач одинакова и имеет следующий вид:

1) путем анкетирования определяется перечень объектов экспертизы в данной предметной области. В него включаются все объекты хотя бы раз упомянутые при опросе;

2) методом парных сравнений или балльным методом определяются весовые коэффициенты данных объектов;

3) оптимизируется количество объектов путем исключения объектов с наименьшим весовым коэффициентом;

4) результаты заносятся в базу данных (БД).

Ранее подобная процедура экспертного оценивания была проверена при определении весовых коэффициентов различных видов обеспечения сетей связи, проведенном среди двух групп – специалистов по радиосвязи ОВД (г. Мурманска, и специалистов связи, обеспечивающих спортивные мероприятия в г. Сочи). Результаты во многом совпадают (техническое и организационное обеспечение, нулевой весовой коэффициент математического обеспечения), но есть и существенные различия (кадровое обеспечение), вытекающие из специфики решаемых задач. Сравнительный анализ результатов обоих опросов выявил целый ряд недостатков как при формировании группы экспертов, так и в процедуре их опроса. На основании этого были внесены существенные изменения во все процедуры экспертного опроса и разработаны соответствующие алгоритмы, проверенные на примере УМВД по г. Липецку.

Процедура кластерного анализа предназначена для разбиения на классы двух групп объектов классификации: 1) всего множества сетей и систем связи; 2) множества решаемых ими задач. На основе данного разбиения формируется математическая модель соответствия сети или системы связи стоящим перед нею задачам. Разбиение производится на основе геометрического расстояния между объектами в многомерном пространстве нормированных характеристик сетей и задач [2].

Процедура кластерного анализа, использующая описанную выше процедуру экспертного оценивания (в зависимости от стоящей задачи меняется объект экспертизы), имеет следующий вид:

1) в БД заносится исходная информация о существующих системах и сетях связи и решаемых ими задачах (их перечень и известные количественные значения характеристик из перечня, сформированного экспертами по уже описанной процедуре);

2) с помощью описанной выше процедуры экспертного оценивания определяется состав экспертной группы (если она необходима);

3) выбранные на предыдущем шаге эксперты с помощью все той же процедуры преобразуют качественные характеристики в количественные, от 1 до 1,0 и заносят в БД;

4) используя алгоритм кластерного анализа (описан далее) разбивают сети и системы связи на классы;

5) используя все тот же алгоритм кластерного анализа, разбивают на классы, решаемые сетями и системами связи задачи;

6) методом экспертного оценивания (по описанной выше процедуре) количественно определяют степень соответствия каждого класса систем и

сетей связи каждому классу решаемых задач нормируют их в диапазоне значений от 1 до 1, и заносят в БД;

7) для формирования требований к характеристикам проектируемой или модернизируемой сети или системы связи экспертным методом определяют количественные нормированные значения характеристик решаемых ими задач и заносят их в БД;

8) используя алгоритм кластерного анализа (описан далее), относят задачи, решаемые системой, к одному из классов задач, определенному на шаге 5;

9) определяют один или более классов систем или сетей связи, наиболее соответствующих определенному на предыдущем шаге классу задач новой системы или сети;

10) определяют диапазоны значений каждой из характеристик новой сети или системы связи, выбирая их минимальные и максимальные значения из наиболее соответствующих новой системе или сети классов (результат предыдущего шага), и заносят их БД.

Предложенный подход и процедуры позволяют обеспечить: 1) понятность и легкость интерпретации как процесса формирования системы показателей качества, так и полученных результатов; 2) иерархичность, т. е. возможность легко получить показателей качества сети связи или ее элемента (например, одного из указанных выше обеспечений) на основе локальных показатель качества, полученных при анализе составляющих ее частей; 3) гибкость, то есть возможность легко изменять систему показателей качества в соответствии с требованиями заказчика или новыми условиями решения задачи; 4) возможность формировать ее на основе как количественных, так и качественных характеристик; 5) использование при ее формировании мнения специалистов (экспертов), например, если значения каких-то характеристик или локальных критериев получить невозможно из-за того, что данная задача является неформализуемой или слабо формализуемой; 6) возможность ее использования при большой неопределенности исходной информации и значительных ее объемах; 7) возможность использования для получения значений отдельных показателей качества специальных программных средств: экспертных систем, систем автоматизации проектирования и т. д.

3.2. Разработка процедур экспертного оценивания и кластерного анализа для оценки эффективности управления сетями радиосвязи ОВД

К процедурам формирования показателей качества эффективности управления сетями и системами связи ОВД предъявляются требования,

аналогичные требованиям к процедурам формирования показателей качества эффективности функционирования сетей и систем связи ОВД.

Процедура кластерного анализа предназначена для разбиения на классы следующих групп объектов классификации: 1) всего множества сетей и систем связи; 2) множества сетей и систем связи, используемых в интересах задачи управления сетями связи; 3) множества решаемых задач управления.

На основе данного разбиения формируются две математические модели: 1) соответствия сети или системы типам сетей и систем связи, используемых в интересах задачи управления; 2) соответствия сети или системы связи, используемой в интересах задачи управления, стоящим перед нею задачам управления. Разбиение производится на основе геометрического расстояния между объектами в многомерном пространстве нормированных характеристик сетей и задач [24].

Процедура экспертного оценивания применяется для решения следующих задач: 1) определение состава экспертных групп; 2) составление перечня задач управления, решаемых конкретной сетью или системой связи; 3) определение множества показателей качества (характеристик), на основе которого формируется критерий оптимальности; 4) определение весовых коэффициентов экспертов, показателей качества и задач, стоящих перед сетью связи, используемой в интересах задачи управления сетями связи; 4) определение степени соответствия каждого класса сетей связи каждому классу решаемых ими задач управления; 5) сведение качественных характеристик к количественным.

Таким образом, объектами экспертизы являются: 1) специалисты, из которых формируются экспертные группы специалистов по управлению сетями связи; 2) показатели качества функционирования сетей и систем связи; 3) решаемые сетями и системами связи задачи; 4) качественные характеристики отдельных элементов сетей и систем управления.

Процедура экспертного опроса для всех решаемых задач одинакова и аналогична изложенной в параграфе 3.1. Отличие заключается в участии в формировании экспертных групп и специалистов управления и в сохранении результатов оценивания в другие разделы БД, относящиеся к подсистеме управления сетями связи. Кроме того, возможно формирование двух экспертных групп для решения задач: 1) оптимизации системы принятия управленческих решений (специалисты по управлению сетями связи); 2) оптимизации сетей связи, используемых в интересах управления.

Процедура кластерного анализа для оценки эффективности управления сетями связи, использующая описанную выше процедуру экспертного оценивания (в зависимости от стоящей задачи меняется объект экспертизы), имеет следующий вид:

1) в БД заносится исходная информация о существующих системах и сетях связи, системах и сетях связи, используемых в интересах решения

задач управления первой группой систем и сетей, а также решаемых задачах управления (их перечень и известные количественные значения характеристик из перечня, сформированного экспертами по уже описанной выше процедуре);

2) с помощью описанной выше процедуры экспертного оценивания определяется состав экспертной группы для решения задач, связанных с оценкой сетей связи (если она необходима);

3) если это необходимо, то аналогичным образом на основе другй группы специалистов определяется состав экспертной группы для решения задач, связанных с управлением сетями связи;

4) выбранные на втором шаге эксперты с помощью все той же процедуры преобразуют качественные характеристики сети связи в количестве от 1 до 1,0 (2.3) и заносят в БД;

5) аналогичным образом выбранные на третьем шаге эксперты преобразуют качественные характеристики системы управления в количестве от 1 до 1,0 (2.3) и заносят в БД;

6) используя алгоритм кластерного анализа (описан далее), разбивают сети и системы связи на классы;

7) с помощью того же алгоритма кластерного анализа, разбивают на классы сети и системы связи, решающие задачи управления сетями;

8) используя все тот же алгоритм кластерного анализа разбивают на классы задачи управления сетями;

9) методом экспертного оценивания (по описанной выше процедуре) количественно определяют степень соответствия каждого класса систем и сетей связи каждому классу задач управления, нормируют их в диапазоне значений от 1 до 1,0 (2.3.) и заносят в БД;

10) аналогичным образом количественно оценивается степень соответствия каждого класса систем управления сетями связи каждому классу задач управления и нормируют их в диапазоне значений от 1 до 1,0 (2.3) и заносят в БД;

11) для формирования требований к характеристикам проектируемой или модернизируемой системы управления сетями связи, зная класс объекта управления (получен на шаге 6), экспертным методом определяют количественные нормированные значения характеристик решаемых ими задач и заносят их в БД;

12) используя алгоритм кластерного анализа (описан далее) относят задачи, решаемые системой задач, к одному из классов задач, определенному на шаге 8;

13) определяют один или более классов систем управления, наиболее соответствующих определенному на предыдущем шаге классу задач новой системы управления сетью радиосвязи;

14) определяют диапазоны значений каждой из характеристик новой системы управления, выбирая их минимальные и максимальные значения

из наиболее соответствующих новой системе управления классов (результат предыдущего шага), и заносят их БД.

Предложенные процедуры оценки эффективности управления сетями радиосвязи ОВД России используют те же алгоритмы, что и описанные в параграфе 3.1 для оценки эффективности функционирования сетей радиосвязи. Это позволяет использовать при решении обеих задач одни и те же программные средства, реализующие эти алгоритмы.

3.3. Алгоритм кластерного анализа системы управления и связи ОВД

В основу алгоритма кластерного анализа, используемого для определения степени соответствия сети связи или системы управления сетями связи поставленным перед ней задачам, положен следующий метод, который разбивает исходное множество сетей связи на группы, объединенные по признаку сходства. Под сходством понимается расстояние между объектами в гиперпространстве признаков, представленном ортогональной системой координат, осями которой служат параметры объектов.

Признак (параметр) – описание одного из свойств объекта. Признаки могут быть как количественными, так и качественными. При кодировании свойств объектов значение каждого из признаков представляется в виде действительного числа. Признаковое пространство – геометрическая интерпретация всей совокупности признаков, участвующих в описании объектов. При этом каждому признаку соответствует одна из осей многомерного ортогонального пространства, размерность которого равна числу признаков. При решении задачи распознавания анализируются векторы гиперпространства, моделирующие объекты. Отдельные классы занимают определенные области многомерного пространства признаков, каждая точка такой области соответствует конкретной реализации объекта.

Условие ортогональности признакового пространства не является необходимым и реально выполняется только в том случае, если все признаки, образующие описание объектов, статистически независимы.

Пусть существует исходное множество информационных объектов, подлежащих классификации $A = \bigcup_{i=1}^{I} a_i$, где I – количество объектов в множестве, i – индекс объекта. Пусть каждый объект a_i представлен множеством значений параметров $P = \bigcup_{j=1}^{J} p_j$, J – количество параметров. Поскольку параметры могут быть описаны в различных единицах измерения, что приведет к невозможности их сопоставления, а также могут иметь различный диапазон значений, что вызовет предпочтительность некоторых из них перед остальными, необходимо проведение

нормирования параметров. После выполнения процедуры нормирования исчисление параметров производится в условных единицах, диапазоны их значений будут совпадать. Предлагается следующий способ нормирования

$$p'_{ij} = p_{ij} / \sum_{i=1}^{I} p_{ij} . \qquad (3.1)$$

Исходной информацией для проведения классификации является матрица D евклидовых расстояний между объектами в признаковом пространстве. Так, для любой пары объектов a_{i1} и a_{i2}:

$$d_{i1\ i2} = (\sum_{j=1}^{J} (p'_{i1\ j} - p'_{i2\ j})^2)^{1/2}. \qquad (3.2)$$

Для оценки взаиморасположения объектов в выборке, представим все элементы множества A в виде вершин сетевой структуры, дуги которой соединяют две наиболее близко расположенные вершины (рис. 3.1).

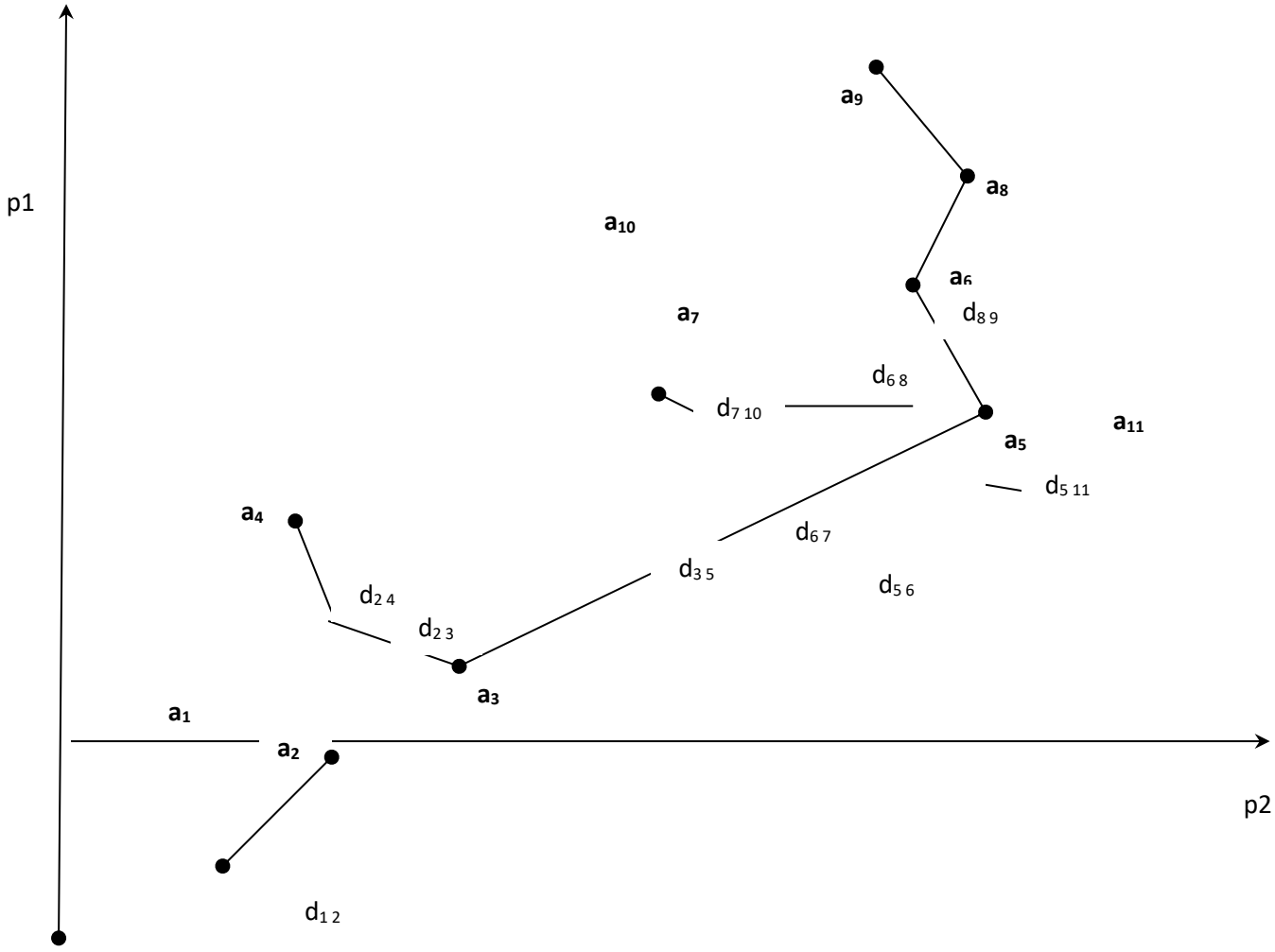


Рис. 3.1. Пример объединения объектов исходной выборки в сетевую структуру

Выбранный и модернизированный метод классификации заключается в постепенном объединении объектов в сеть R путем последовательного связывания дугами наиболее близко расположенных объектов. Далее получают *I*-1 вариант классификации путем разрезания дуг от самой длинной к самой короткой.

В качестве сравнительного критерия оптимальности варианта разбиения исходной группы на классы на шаге l относительно варианта на шаге $l + 1$ вводится коэффициент предпочтения варианта разбиения:

$$Q_l = (\bar{R}_{м\,l} - \bar{R}_{м\,l+1}) / (\bar{R}_{в\,l} - \bar{R}_{в\,l+1}),\ l = \overline{1, I-2}, \qquad (3.3)$$

где: l — индекс шага алгоритма, а среднее межклассовое расстояние $\bar{R}_{м\,l}$ формируется аналогично из разрезаемых дуг.

Последний шаг алгоритма разбиения будет иметь индекс $l = I - 1$. Наибольшее значение коэффициента Q_l указывает на то, что на шаге l алгоритма найдена длина дуги $D_{i1\ i2}$, соединяющей два объекта a_{i1} и a_{i2}, принадлежащих с большой степенью вероятности к одному классу, что вызвало более значительную разницу соседних значений среднего межклассового расстояния $\bar{R}_{м\ l}$ по сравнению с изменением значения среднего внутриклассового расстояния $\bar{R}_{в\ l}$, т.е. получено наиболее оптимальное разбиение выборки с образованием $K = l+1$ классов. Для реализации предложенного метода разработан алгоритм, приведенный в упрощенном виде на рис. 3.2.

Для реализации предложенного метода разработан алгоритм, приведенный в упрощенном виде на рис. 3.2.

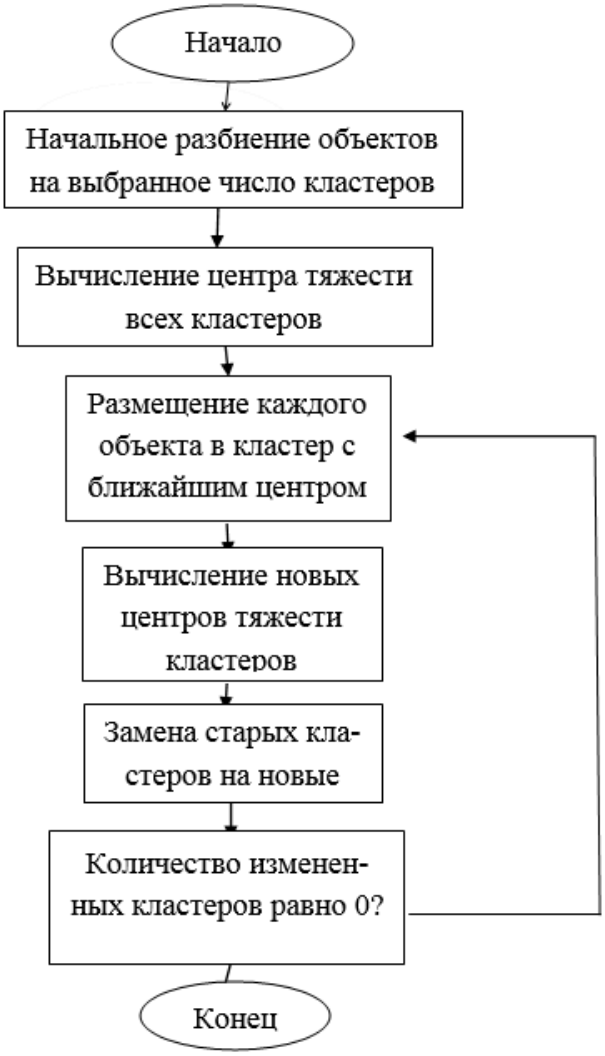
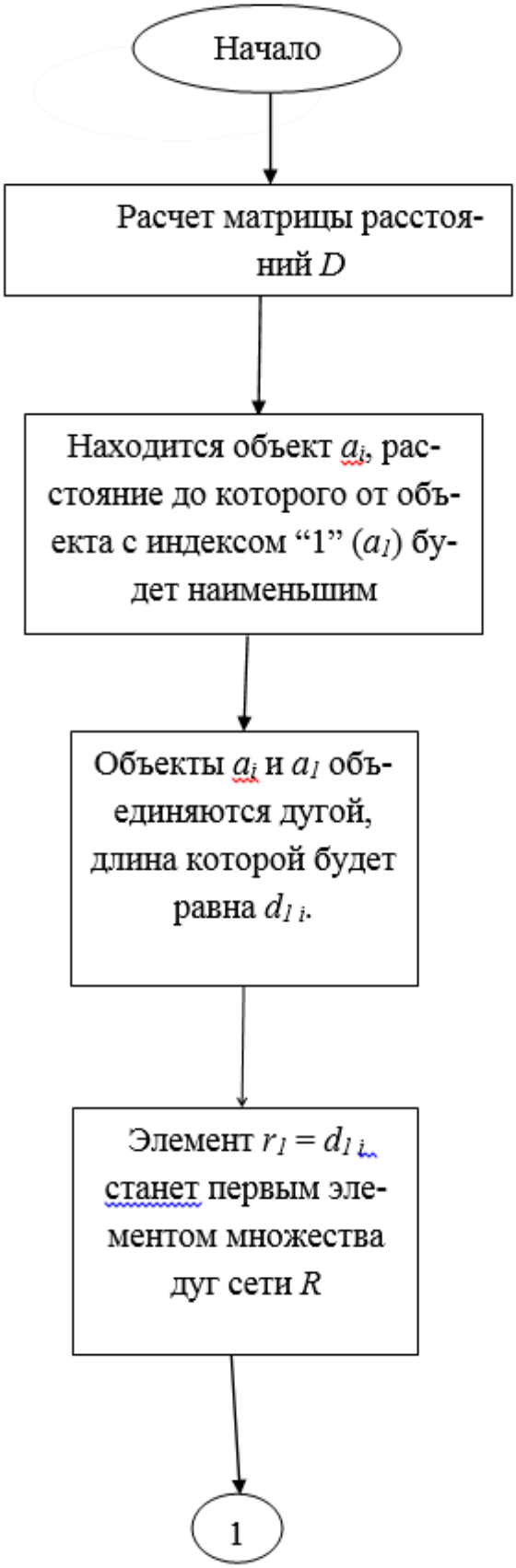


Рис 3.2. Алгоритм разбиения объектов на кластеры (классы) в упрощенном виде.

Разработанный для данного метода алгоритм классификации в полном виде описан на рис. 3.3.


Начало
Расчет матрицы расстояний D
Находится объект a_i, расстояние до которого от объекта с индексом "1" (a_1) будет наименьшим
Объекты a_i и a_1 объединяются дугой, длина которой будет равна $d_{1\,i}$.
Элемент $r_1 = d_{1\,i}$ станет первым элементом множества дуг сети R
1

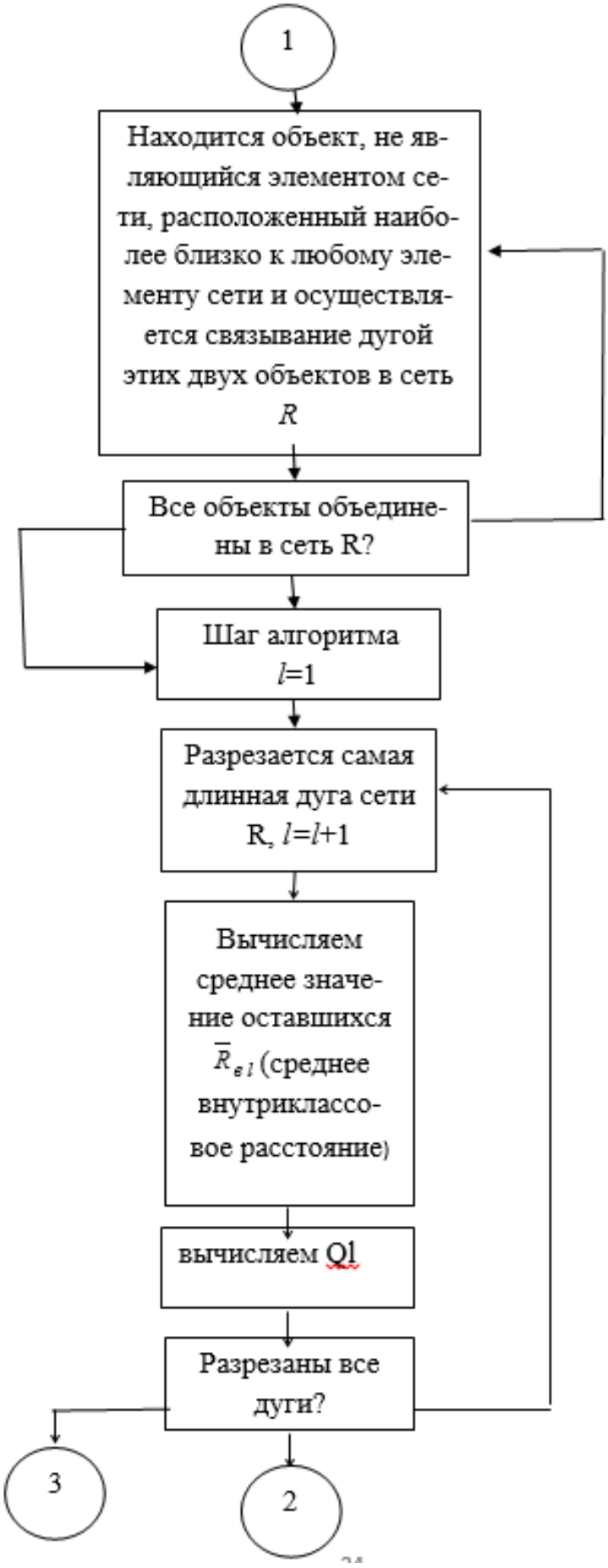

1
Находится объект, не являющийся элементом сети, расположенный наиболее близко к любому элементу сети и осуществляется связывание дугой этих двух объектов в сеть R
Все объекты объединены в сеть R?
Шаг алгоритма l=1
Разрезается самая длинная дуга сети R, l=l+1
Вычисляем среднее значение оставшихся $\overline{R}_{el}$ (среднее внутриклассовое расстояние)
вычисляем Ql
Разрезаны все дуги?
3
2

Рис. 3.3 Алгоритм построения сети в полном виде

3.4. Разработка алгоритмов экспертного оценивания эффективности функционирования системы управления и связи ОВД

Предлагается использовать экспертное оценивание для решения следующих задач:

1) Формирование множества параметров модели функционального соответствия и весовых коэффициентов, описывающих их значимость;
2) Формирование определения состава экспертной группы (по конкретным лицам или должностям) и весовых коэффициентов их мнений;
3) Определение состава технических средств для модели функционального соответствия.

Анализ метода экспертного оценивания показывает, что для решения первой задачи необходимо использовать метод парных сравнений, так как он позволяет получить весовые коэффициенты, а для выбора технических средств (ТС) необходимо использовать метод ранжирования, так как он позволяет сократить время, затрачиваемое на экспертный опрос. При этом для решения всех трех задач используется метод анкетирования экспертов. Количество экспертов определяется, исходя из их доступности, и может быть произвольным.

Для проведения экспертного оценивания специалистов (экспертов) и технических средств, которые можно применить, был использован метод парных сравнений. Разработанный алгоритм экспертного оценивания состоит из 2 частей: 1) алгоритм ввода исходных данных; 2) алгоритм расчётов нормированных весовых коэффициентов.

Алгоритм ввода исходных данных описывается следующей последовательностью шагов.

Шаг 1.

Заносим в таблицу значения оценок p = 1 эксперта по шкале «предпочтительнее» («важнее»), «одинаково», «менее предпочтительно» («менее важно»), сравнивается j = 1 обеспечение i = 2 обеспечением. Если эксперт считает, что j = 1 обеспечение «предпочтительнее», чем i=2обеспечение, то в строку i = 2, J = 1 столбца заносится «2» балла$_{21}$=2, а в i = 1 строку, j = 2 столбца заносится «0» баллов$_{12}$=0; Если эксперт выбирает «одинаково», то в строку i = 2, J = 1 столбца заносится «1» a_{21}=1 и a_{12}=1. Если эксперт выбирает «менее предпочтительно», то a_{21}=0 и a_{12}=2.

Шаг 2.

Повторяем действие шага 1, сравниваем j=1 обеспечение с i=3 обеспечением и аналогичным образом формируем элементы таблицы a_{ij}= a_{31} и a_{ij} = a_{13}.

Шаг 3.

Данное действие (шаг 1) повторяем до тех пор, пока не выполнится условие j = n, где n – количество видов обеспечения (характеристик).

Шаг 4.

Повторяем действие шага 1, сравниваем j = j+1 обеспечение с i = j+1 обеспечением и аналогичным образом формируем элементы таблицы

$a_{i;j+1} = a_{3;1+1}$ и $a_{i+1;j} = a_{1+1;j}$

Шаг 5.

Выполняем действие шага 4до тех пор, пока не выполнится условие j = n.

Шаг 6.

Возвращаемся на шаг 1 и повторяем действие шагов 1 – 3 для p = 2 эксперта. Заполняем вторую таблицу экспертных оценок.

Шаг 7.

Повторяем действие шага 4 до тех пор, пока не выполнится условие p=m, где m – количество экспертов.

Алгоритм расчёта нормированных весовых коэффициентов описывается следующей последовательностью шагов.

Шаг 1.

Высчитываем сумму полученных оценок, выставленных p = 1 экспертом для j – го обеспечения (j – го столбца) по формуле:

$$S_j = \sum_{i=1}^{n} a_{ij} \tag{3.5}$$

где j – номер столбца; i – номер строки.

Шаг 2.

Выполняем действие шага 1 для следующего j=2 обеспечения (столбца).

Шаг 3.

Повторяем действие шага 2, для всех остальных обеспечений, пока не выполнится условие j = n.

Шаг 4.

Выполняем действие шагов 1 - 3 для p = p+1 до тех пор, пока не выполнится условие p=m.

Шаг 5.

Высчитываем сумму балов оценки присвоенных всем обеспечениям по формуле:

$$S_{\sum} = \sum_{j=1}^{n} S_j, \tag{3.6}$$

Шаг 6.

Высчитываем значение нормированного весового коэффициента j=1 обеспечения для p = 1 эксперта по формуле:

$$b_j = \frac{S_j}{S_{\sum}} = b_{jp}. \tag{3.7}$$

Шаг 7.

Повторяем действие шага 5 для j = 2 обеспечения.

Шаг 8.

Повторяем действие шага 6 для следующих обеспечений, пока не выполнится условие j = n.

Шаг 9.

Высчитываем нормированные весовые коэффициенты b_j, j = 1, 2, …, n полученные p = 2 экспертом, повторяя действие шагов 1–8.

Шаг 10.

Высчитываем значение коэффициента b_j, полученного следующим экспертом до тех пор, пока не выполнится условие p = m.

Шаг 11.

Усредняем значение j = 1 весового коэффициента b_{jp} по всему множеству экспертов p = 1, 2, …, m по формуле:

$$b_{j\text{ср}} = \frac{1}{m}\sum_{p=1}^{m} b_{jp} \qquad (3.8)$$

Шаг 12.

Высчитываем среднее значение следующего j = 2 весового коэффициента, повторяя действие шага 11.

Шаг 13.

Высчитываем среднее значение всех весовых коэффициентов b_j, повторяя действие шага 12, пока не выполнится условие j = n.

ГЛАВА 4. РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ РАЗРАБОТАННЫХ АЛГОРИТМОВ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ И СВЯЗИ ОВД

4.1. Рекомендации по выбору состава экспертной группы для оценки эффективности функционирования цифровой сети связи ОВД на основе метода парных сравнений

Для того чтобы произвести качественный выбор технических средств, необходимо провести работу по выбору оптимального состава экспертной группы, которая будет осуществлять выбор ТС. Эксперты должны быть хорошо знакомы с предметом экспертизы, обладать достаточным опытом и быть способными выносить обоснованные объективные суждения.

В состав экспертной группы, решающей задачу выбора ТС систем связи для организации оптимальной сети связи, могут входить следующие специалисты: начальник отдела центра информационных технологий связи и защиты информации, заместитель начальника отдела, старший инженер и инженер группы организации связи, инженер группы обеспечения связи при проведении оперативных и массовых мероприятий, старший инженер и инженер группы технической защиты информации. Для определения оптимального состава экспертной группы применен метод парных сравнений. Этот метод является одной из самых распространенных экспертных процедур для определения весов сетей связи, сравниваемых по качественному признаку. Метод парных сравнений основан на поочередном сравнении всех сетей связи экспертизы друг с другом, и эксперту каждый раз необходимо определить, какая из предъявленных ему сетей связи предпочтительнее по рассматриваемому признаку. При этом порядок предъявления эксперту пар не имеет значения, так как не влияет на результаты парных сравнений. Далее полученную информацию используют для вычисления количественных оценок.

При групповой экспертизе определения относительных весов членов экспертной группы каждый эксперт предоставляет для групповой обработки свою матрицу парных сравнений. На основании индивидуальных матриц парных сравнений составляется групповая матрица. Опрос экспертов производился методом анкетирования.

На основании индивидуальных матриц парных сравнений экспертов строим групповую матрицу, элементы которой представляют собой оценку специалиста (табл. 4.1):

$\sum_{J} a_{ij}$ - сумма оценок каждого специалиста, q_i – относительный весовой коэффициент категории специалистов, который рассчитывается по формуле

Таблица 4.1. Матрица парных сравнений экспертов

Эксперты / Специалисты	1	2	3	4	5	$\sum_J a_{ij}$	q_i
Начальник ОЦИТС и ЗИ (Х1)	8	7	8	9	10	42	0,16
Заместитель начальника отдела (Х2)	10	9	10	8	10	47	0,17
Старший инженер группы организации связи (Х3)	7	5	6	7	8	32	0,12
Инженер группы организации связи (Х4)	8	10	8	7	8	41	0,15
Инженер группы обеспечения связи при проведении оперативных и массовых мероприятиях (Х5)	8	10	8	8	9	43	0,16
Старший инженер группы технической защиты информации (Х6)	5	7	9	8	6	35	0,13
Инженер группы технической защиты информации (Х7)	6	6	7	6	5	30	0,11

$$q_i = \frac{\sum_{j=1}^{n} a_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}}. \qquad (4.1)$$

Среднее значение относительного весового коэффициента (q_i) выбираем в качестве порогового

$$q_{cp} = \frac{\sum_i q_i}{m}, \qquad (4.2)$$

где m – количество категорий специалистов.

Подставляя в (4.2) $m = 7$ и значения q_i, получаем $q_{cp} = 0{,}14$.

При относительном весовом коэффициенте категории специалистов, превышающем пороговое значение, данная категория включается в состав экспертной группы.

Таким образом, получаем, что в состав экспертной группы следует включить следующие категории специалистов: начальник ОИТС и ЗИ, заместитель начальника отдела, старшего инженера группы организации связи, старшего инженера группы технической защиты информации.

Оценим эффективность полученных результатов на основе расчета дисперсий оценок для выделения категорий специалистов (табл. 4.2).

В табл. 4.2 характеристика δ_j^2 - дисперсия оценок *i*-ой категории специалистов, данных *j*-ым экспертом, которая рассчитывается по формуле:

$$\delta_j^2 = (a_{ij} - \overline{a_j})^2, \qquad (4.3)$$

Таблица 4.2. Дисперсия оценок категорий специалистов

Дисперсия / Специалист	δ_1^2	δ_2^2	δ_3^2	δ_4^2	δ_5^2	$\overline{\delta}_j^2$	$\overline{a_j}$
Начальник ОИТС и ЗИ	0,16	1,96	0,16	0,16	2,56	1,04	8,4
Заместитель начальника отдела	0,36	0,16	0,36	1,96	0,36	0,64	9,4
Старший инженер группы организации связи	0,04	3,24	0,04	0,04	0,64	0,8	8,2
Старший инженер группы технической защиты информации	0,36	1,96	0,36	0,36	0,16	0,64	8,6

где $\overline{a_j}$ – среднее значение оценок, данных *i*-й категории специалистов, $\overline{\delta}_j^2$ – общее значение дисперсии оценок для *i*-й категории специалистов, которое рассчитывается по формуле:

$$\overline{\delta}_j^2 = \frac{\sum_j \delta_{ij}^2}{m}, \tag{4.4}$$

где m – количество экспертов.

Так как общее значение дисперсии оценок для всех категорий невелико, ни одна из категорий не исключается из состава экспертной группы. Таким образом, в состав экспертной группы могут входить представители следующих категорий: начальник ОИТС и ЗИ, заместитель начальника отдела, старший инженер группы организации связи, старший инженер группы технической защиты информации.

4.2 Определение весовых коэффициентов обеспечения системы управления и связи ОВД

Разработанные процедуры и алгоритмы были проверены при решении двух задач: 1) определении значений весовых коэффициентов различных обеспечения системы связи ОВД (первая группа экспертов); 2) сравнительном анализе двух типов носимых радиостанций.

Экспертный опрос проводился в городе Липецк. Вторая группа экспертов формировалась с учетом результатов работы первой группы. Для решения первой задачи проводилось анкетирование экспертов, выбранных на предыдущем этапе. Экспертам предложено попарно между собой сравнить следующие виды обеспечений: 1) кадровое; 2) организационное; 3) информационное; 4) материально-техническое; 5) программное; 6)

морально-психологическое; 7) правовое. Интересно, что оценивать морально-психологическое обеспечение предложила группа экспертов из города Липецк при проверке процедуры определения значимых обеспечений и характеристик системы связи ОВД. Результаты опроса приведены в таблице 4.3.

Таблица 4.3. Результаты сравнения обеспечений

Параметр	Правовое	Кадровое	Организационное	Информационное	Материально-техническое	Программное	Морально-психологическое
Правовое	----	1;2;2; 2;1	1;1;1; 1;1	0;1;0; 0;0	2;2;2; 1;2	0;0;0; 1;0	1;0;1; 2;1
Кадровое	1;0; 0;0;1	----	0;1;1; 0;1	0;0;0; 1;0	1;2;1; 1;2	0;0;0; 0;0	1;1;0; 0;1
Организационное	1;1;1; 1;1	2;1;1; 2;1	----	0;0;0; 1;1	2;1;2; 2;1	0;0;1; 0;0	0;1;1; 1;0
Информационное	2;1;2; 2;2	2;2;2; 1;2	2;2;2; 1;1	----	2;1;2; 2;2	1;2;1; 0;1	2;1; 2;1;2
Материально-техническое	0;0;0; 1;0	1;0;1; 1;0	0;1;0; 0;1	0;1;0; 0;0	----	0;0;0; 0;0	0;0;0; 1;1
Программное	2;2;2; 1;2	2;2;2; 2;2	2;2;1; 2;2	1;0;1; 2;1	2;2;2; 2;2	----	2;2;1; 2;2
Морально-психологическое	1;2;1; 0;1	1;1;2; 2;2	2;1;1; 1;2	0;1;0; 1;0	2;2;2; 1;1	0;0;1; 0;0	----
Сумма оценок	7;6;6; 5;7	9;8;10; 10;7	7;8;6;5 ;8	1;3;1; 5;2	11;10; 11;9; 10	1;2;3;1 ;1	6;5;5; 7;7
Среднее значение	1;0,8; 0,8;0, 7;1	1,3;1,1 ;1,4;1, 4;1	1;1,1;0 ,8;0,7; 1,1	0,1;0,4 ;0,1;0, 7;0,2	1,5;1,4 ;1,5;1, 3;1,4	0,1;0,2 ;0,4;0, 1;0,1	0,8;0, 7;0,7; 1;1

В таблице 4.4 приведен конечный результат обработки полученной информации.

Таблица 4.4. Получение весовых коэффициентов видов обеспечения

Обеспечение	Правовое	Кадровое	Организационное	Информационное	Материально-техническое	Программное	Морально-психологическое
Эксперт 1	0,17	0,21	0,17	0,02	0,26	0,02	0,14
Эксперт 2	0,14	0,19	0,19	0,07	0,24	0,05	0,12
Эксперт 3	0,14	0,24	0,14	0,02	0,26	0,07	0,12
Эксперт 4	0,12	0,24	0,12	0,12	0,21	0,02	0,17
Эксперт 5	0,17	0,17	0,19	0,05	0,24	0,02	0,17
Обобщенный весовой коэффициент	0,15	0,21	0,16	0,06	0,24	0,04	0,14

Из данной таблицы видно, что приоритет при выборе обеспечения, отдаётся материально-техническому обеспечению.

В таблице 4.5 приведено сравнение весовых коэффициенты различных обеспечений сетей связи, полученные у трех экспертных групп специалистов по радиосвязи ОВД (г. Липецк, г. Мурманск, и специалисты связи, обеспечивающие спортивные мероприятия в г. Сочи).

Результаты во многом совпадают (техническое и организационное обеспечение, нулевой весовой коэффициент математического обеспечения), но есть и существенные различия (кадровое обеспечение), вытекающие из специфики решаемых задач.

Таблица 4.5. Весовые коэффициенты видов обеспечения сетей ОВД, полученные методом экспертного оценивания, различных групп специалистов

Вид обеспечения	Весовой коэффициент		
	г. Мурманск	г. Сочи	г. Липецк
Техническое	0,2791	0,31	0,24
Программное	0,1240	0,23	0,04
Кадровое	0,2392	0,07	0,21
Информационное	0,1116	0,21	0,06
Организационное	0,1763	0,15	0,16
Нормативно-правовое	0,0698	0,03	0,15
Морально-психологическое	0	0	0,14

4.3. Пример экспертной оценки предпочтительности использования возимых радиостанций в ОВД

С применением разработанных процедур и алгоритмов определялся перечень значимых характеристик носимых радиостанций, весовые коэффициенты характеристик, значения некоторых характеристик, которые можно было определить только методом экспертного оценивания, при сравнительном анализе двух типов носимых радиостанций – Icom F4162DT и Kenwood tk3160. Были определены значения критериев оптимальности для каждой из радиостанций (табл. 4.6). Причем дальность действия радиостанций в условиях прямой видимости определялась экспериментально. В ходе эксперимента было выявлено, что представленные радиостанции имеют приблизительно одинаковую дальность действия – около 15 км (при гарантированном качестве связи 65–70%).

Видно, что радиостанция фирмы Kenwood имеет наилучшую эффективность среди представленных. Теперь определим, насколько экономически рационально использовать эту радиостанцию с учетом стоимости (табл. 4.7).

Таблица 4.6. Весовые коэффициенты параметров радиостанций

Параметры радиостанций	Весовой коэффициент	Icom F4162DT		Kenwood tk3160	
Дальность действия, км	0,30	14,9	1	14,9	1
Время работы, ч	0,10	9	0	12	1
Эргономичность	0,08		1		1
Пыле-влагозащищенность	0,07	IP55 (1)	1	IP54	0
Прочность	0,05	IP55 (1)	1	IP54	0
Диапазон рабочих температур	0,05	-25..+55	0	-30..+60	1
Применение в цифровых и аналоговых сетях	0,05	+	1	-	0
Тип аккумулятора	0,05	Li-Ion	1	Li-Ion	1
Срок службы, г	0,04		1		1
Расширенный функционал	0,04	+	1	-	0
Ремонтопригодность	0,03		0		1
Количество каналов	0,03	512	1	16	0
Наличие дополнительных аксессуаров	0,03	+	1	+	1
Масса, г	0,025	340	0	282	1
Размеры, мм	0,025	53x136x 38.5	0	56x109.3 x34.5	1
Диапазон частот	0,02	400-470	1	440-470	0
	Показатель эффективности	0,71		0,73	

Таблица 4.7. Нормированная цена радиостанций

Модель	IC-4162DT	TK3160
Стоимость, р	34000	6500
Нормированная стоимость	0,84	0,16

Перемножив полученный показатель эффективности на нормированную цену, получим коэффициент оптимальности, учитывающий стоимость радиостанций (табл. 4.8).

Таблица 4.8. Коэффициент оптимальности с учетом стоимости

Модель	IC-4162DT	TK3160
Критерий оптимальности	0,85	4,55

Следовательно, по данному критерию наиболее эффективна радиостанция фирмы Kenwood. В этом случае стоимость является определяющим фактором в выборе радиостанции, так как их параметры приблизительно одинаковы.

4.4. Разработка методических рекомендаций по повышению эффективности функционирования сетей связи органов внутренних дел для использования в подразделениях ОВД

Широкое применение радиоэлектронных средств в самых разнообразных областях жизни современного общества привело к развитию электромагнитного терроризма. Под электромагнитным терроризмом понимают оказание деструктивного электромагнитного воздействия на радиоэлектронные средства с целью их разрушения или нарушения работы [2–5]. За последние годы появляются как новые проявления электромагнитного терроризма, как, например, ослепление лазерными лучами пилотов самолетов, так и воздействие на аппаратуру с помощью разнообразных генераторов помех (шума), что может привести к фатальным последствиям. Получило распространение воздействие на критическую инфраструктуру, в том числе на системы связи специального назначения, с помощью беспилотных летательных аппаратов (БПЛА) с установленными на них генераторами различного рода помех (импульсных, шумовых и др.). Такое оборудование, размещенное на БПЛА, управляемое дистанционно из удаленного от места совершения преступления места, воздействует с помощью электромагнитных излучений на оборудование систем связи специального назначения, например, систему, функционирующую в соответствии со стандартом IEEE 802.16d, воздействие на которую будет рассмотрена далее. Этот факт может привести к затруднению оперативного управления силами и средствами, в связи с чем приобретает особую актуальность разработка методов и средств противодействия подобному деструктивному электромагнитному воздействию, а также соответствующих моделей противодействия. Далее в работе будет рассмотрена модель противодействия деструктивному электромагнитному

воздействию, реализованная на основе аппарата нечетких экспертных систем.

Проведение экспертного опроса. Для определения параметров сигналов (мощностей) помех, при которых система может функционировать нормально, функционировать частично и не функционировать вовсе, воспользуемся методом экспертного опроса. Применительно к выбранным для рассмотрения системам связи характерным уровнем является минимальная паспортная мощность сигнала, воспринимаемая приемником системы связи 4-го поколения – 115 Дбм [6], при этом мощность помехи должна превосходить мощность полезного сигнала в 10 раз [7], т.е. мощность помехи, при которой система связи перестает выполнять свою целевую функцию – 105 Дбм. На основании данных условий респондентам было предложено определить уровни мощностей помех для каждого состояния системы связи. К опросу привлекались действующие сотрудники ОВД, работающие в профильных технических подразделениях более 10 лет. Было опрошено 10 экспертов. Опрос осуществлялся путем анкетирования, где было предложено выбрать уровни помех для трех состояний системы. Результаты экспертного опроса приведены в табл. 4.9 [9–10].

Оценку опроса экспертов будем производить в программном продукте STATISTICA.

Таблица 4.9. Экспертные оценки

	Плохо	Хорошо	Нормально
Эксперт 1	–105	–116	–110
Эксперт 2	–100	–115	–115
Эксперт 3	–105	–118	–112
Эксперт 4	–102	–116	–110
Эксперт 5	–100	–120	–111
Эксперт 6	–102	–115	–108
Эксперт 7	–100	–120	–107
Эксперт 8	–105	–119	–107
Эксперт 9	–103	–116	–109
Эксперт 10	–101	–117	–107

Произведем обработку оценок, выставленных экспертами, с целью выявления согласования в их оценках. Для этого обычно применяется мера согласованности экспертных мнений – дисперсионный коэффициент конкордации (коэффициент согласия), равный:

$$W = \frac{D}{D_{max}}, \tag{4.5}$$

где D – оценка дисперсии, D_{max} – максимальное значение оценки дисперсии. Коэффициент конкордации изменяется от 0 до 1, W = 0 в случае полного расхождения между выставленными экспертами оценок, если W = 1, то

мнения экспертов полностью совпадают. Для нашего случая значение коэффициента конкордации вычислялось программно (рис. 4.1).

Variable	Friedman ANOVA and Kendall Coeff. of Concordance (S ANOVA Chi Sqr. (N = 10, df = 2) = 19,53846 p = ,00006 Coeff. of Concordance = ,97692 Aver. rank r = ,97436			
	Average Rank	Sum of Ranks	Mean	Std.Dev.
Плохо	3,000000	30,00000	-102,300	2,110819
Хорошо	1,050000	10,50000	-117,200	1,932184
Норма	1,950000	19,50000	-109,600	2,590581

Рис. 4.1. Вычисление коэффициента конкордации и рангов модели

Вычисленный коэффициент конкордации W = 0,9, что позволяет сделать вывод о высокой согласованности выставленных экспертами оценок. Из предложенных респондентами значений определим среднее для каждого уровня воздействия, которые в дальнейшем будут положены в оценку результатов воздействующих на систему деструктивных помех при помощи аппарата нечеткой логики.

Далее будут рассмотрены основные функциональные состояния системы радиосвязи СН при деструктивных электромагнитных воздействиях и меры по противодействию данным воздействиям.

Лингвистическая модель определения основных состояний системы радиосвязи и методов противодействия разрушению информации в них, основанная на нечетких экспертных системах.

В качестве основного инструмента при прогнозировании состояния и мер противодействия при деструктивных электромагнитных воздействиях будем использовать нечеткие экспертные системы, поскольку задача прогнозирования состояния системы в условиях поражающих воздействий является сложной с математической точки зрения и требует учета всех возможных параметров системы и воздействий.

Для моделирования нечеткой экспертной системы будем использовать пакет Fuzzy Logic Toolboks программы Matlab. В качестве датчика, позволяющего оценить параметры воздействия, будем использовать физическое устройство типа анализатора спектра. Введем в рассмотрение значения лингвистических переменных для заполнения базы знаний

1. P – мощность помехи, P = {НОРМАЛЬНАЯ, СРЕДНЯЯ, КРИТИЧЕСКАЯ}, [–120,100], функции принадлежности термов имеют следующий вид (рис. 4.2):

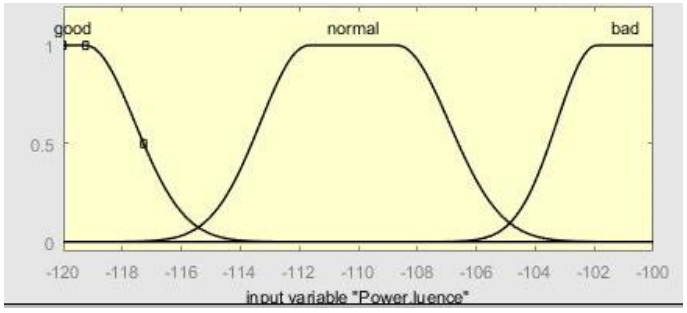


Рис. 4.2. Функции принадлежности термов переменной «Мощность помехи»

Значения данных параметров выбраны исходя из средних значений, полученных с помощью экспертного опроса.

2. F – функционирование системы, F = {НОРМАЛЬНО, ЧАСТИЧНО, НЕ ФУНКЦИОНИРУЕТ}, [0,1], функции принадлежности термов имеют следующий вид (рис. 4.3):

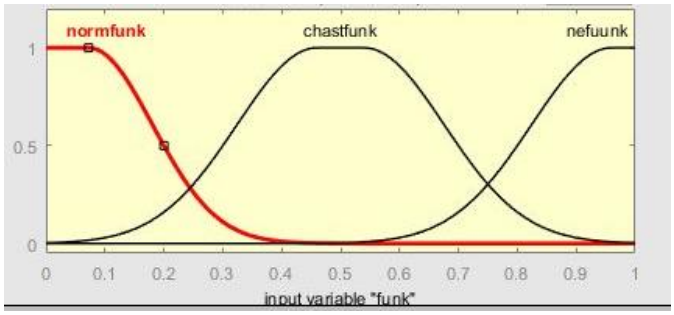


Рис. 4.3. Функции принадлежности термов переменной «Функционирование системы»

3. I – важность информации, I = {ПОВСЕДНЕВНАЯ, СРОЧНАЯ, ОПЕРАТИВНАЯ}, [0,1], функции принадлежности термов имеют следующий вид (рис. 4.4):

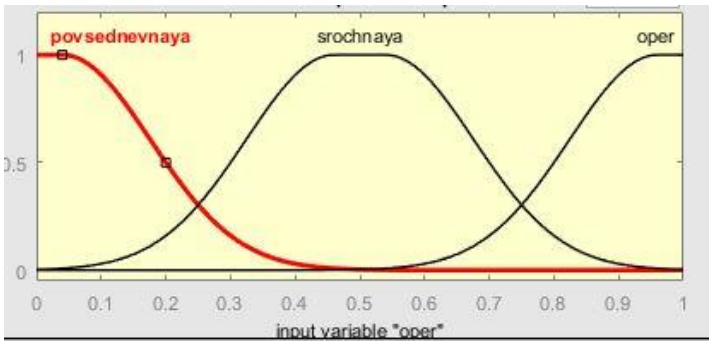


Рис. 4.4. Функции принадлежности термов переменной «Важность информации»

4. R – наличие информации рангом выше, R = {ОТСУТСТВУЕТ, ПРИСУТСТВУЕТ}, [0,1], функции принадлежности термов имеют следующий вид (рис. 4.5):

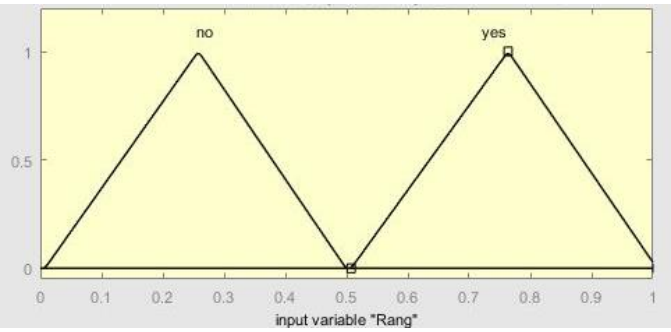


Рис. 4.5. Функции принадлежности термов переменной «Ранг информации»

Далее зададим множество возможных мер противодействия деструктивным электромагнитным воздействиям [8].

M – меры противодействия, M = {ОБЫЧНЫЙ РЕЖИМ, ОЖИДАНИЕ, ОЧЕРЕДЬ, ИСПОЛЬЗОВАНИЕ MIMO, РЕЗЕРВНЫЙ КАНАЛ}, [0,1], функции принадлежности термов имеют следующий вид (рис. 4.6):

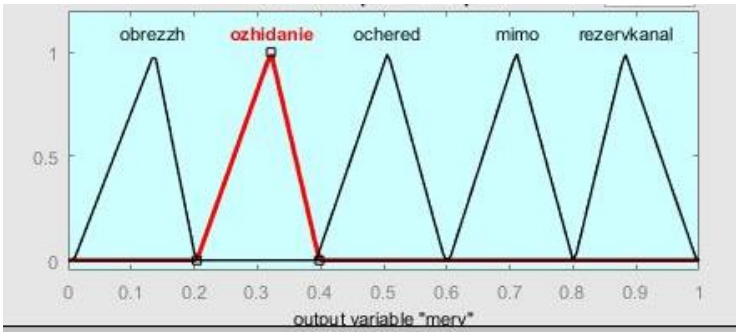


Рис. 4.6. Функции принадлежности термов переменной «Меры противодействия»

Следующим шагом является создание базы правил, на основании которых будут выбираться определенные меры противодействия. Она будет выглядеть следующим образом:

1. If P = НОРМАЛЬНАЯ & F = НОРМАЛЬНО & I = ПОВСЕДНЕВНАЯ, then M = ОБЫЧНЫЙ РЕЖИМ;
2. If P = НОРМАЛЬНАЯ & F = НОРМАЛЬНО & I = СРОЧНАЯ, then M = ОБЫЧНЫЙ РЕЖИМ;
3. If P = НОРМАЛЬНАЯ & F = НОРМАЛЬНО & I = ОПЕРАТИВНАЯ, then M = ОБЫЧНЫЙ РЕЖИМ;
4. If P = СРЕДНЯЯ & F = ЧАСТИЧНО & I = ПОВСЕДНЕВНАЯ & R = ОТСУТСТВУЕТ, then M = ОЖИДАНИЕ;

5. If P = СРЕДНЯЯ & F = ЧАСТИЧНО & I = ПОВСЕДНЕВНАЯ & R = ПРИСУТСТВУЕТ, then M = ОЧЕРЕДЬ;

6. If P = СРЕДНЯЯ & F = ЧАСТИЧНО & I = СРОЧНАЯ & R = ОТСУТСТВУЕТ, then M = ИСПОЛЬЗОВАНИЕ MIMO;

7. If P = СРЕДНЯЯ & F = ЧАСТИЧНО & I = СРОЧНАЯ & R = ПРИСУТСТВУЕТ, then M = ОЧЕРЕДЬ;

8. If P = СРЕДНЯЯ & F = ЧАСТИЧНО & I = ОПЕРАТИВНАЯ, then M = ИСПОЛЬЗОВАНИЕ MIMO;

9. If P = КРИТИЧЕСКАЯ & F = НЕ ФУНКЦИОНИРУЕТ& I = ПОВСЕДНЕВНАЯ & R = ОТСУТСТВУЕТ, then M = РЕЗЕРВНЫЙ КАНАЛ;

10. If P = КРИТИЧЕСКАЯ & F = НЕ ФУНКЦИОНИРУЕТ& I = ПОВСЕДНЕВНАЯ & R = ПРИСУТСТВУЕТ, then M = ОЧЕРЕДЬ;

11. If P = КРИТИЧЕСКАЯ & F = НЕ ФУНКЦИОНИРУЕТ & I = СРОЧНАЯ & R = ОТСУТСТВУЕТ, then M = РЕЗЕРВНЫЙ КАНАЛ;

12. If P = КРИТИЧЕСКАЯ & F = НЕ ФУНКЦИОНИРУЕТ & I = СРОЧНАЯ & R = ПРИСУТСТВУЕТ, then M = ОЧЕРЕДЬ;

13. If P = КРИТИЧЕСКАЯ & F = НЕ ФУНКЦИОНИРУЕТ & I = ОПЕРАТИВНАЯ, then M = РЕЗЕРВНЫЙ КАНАЛ;

Вычисления производились по алгоритму Мамдани [12, 15–17]:

1. Формирование базы правил.

2. Фазификация (нахождение соответствия между численным значением входной переменной и значением функции принадлежности соответствующего ей терма лингвистической переменной).

3. Агрегирование (определение степени истинности условий по каждому из правил):

$$T(\mu_A(x), \mu_B(x)) = \min(\mu_A(x), \mu_B(x)). \quad (4.6)$$

4. Активизация (определение весовых коэффициентов правил), по умолчанию взята =1.

5. Аккумуляция (нахождение функций принадлежности для каждой из выходных лингвистических переменных):

$$¥x\epsilon\ X\ \mu A\cup B(x) = \max\{\mu A(x);\ \mu B(x)\}. \quad (4.7)$$

6. Дефазификация (переход от функций принадлежности выходной лингвистической переменной к её четкому значению).

Полученные зависимости приведены на рис. 4.7. Они могут быть применены в алгоритме, предложенном в следующем разделе.

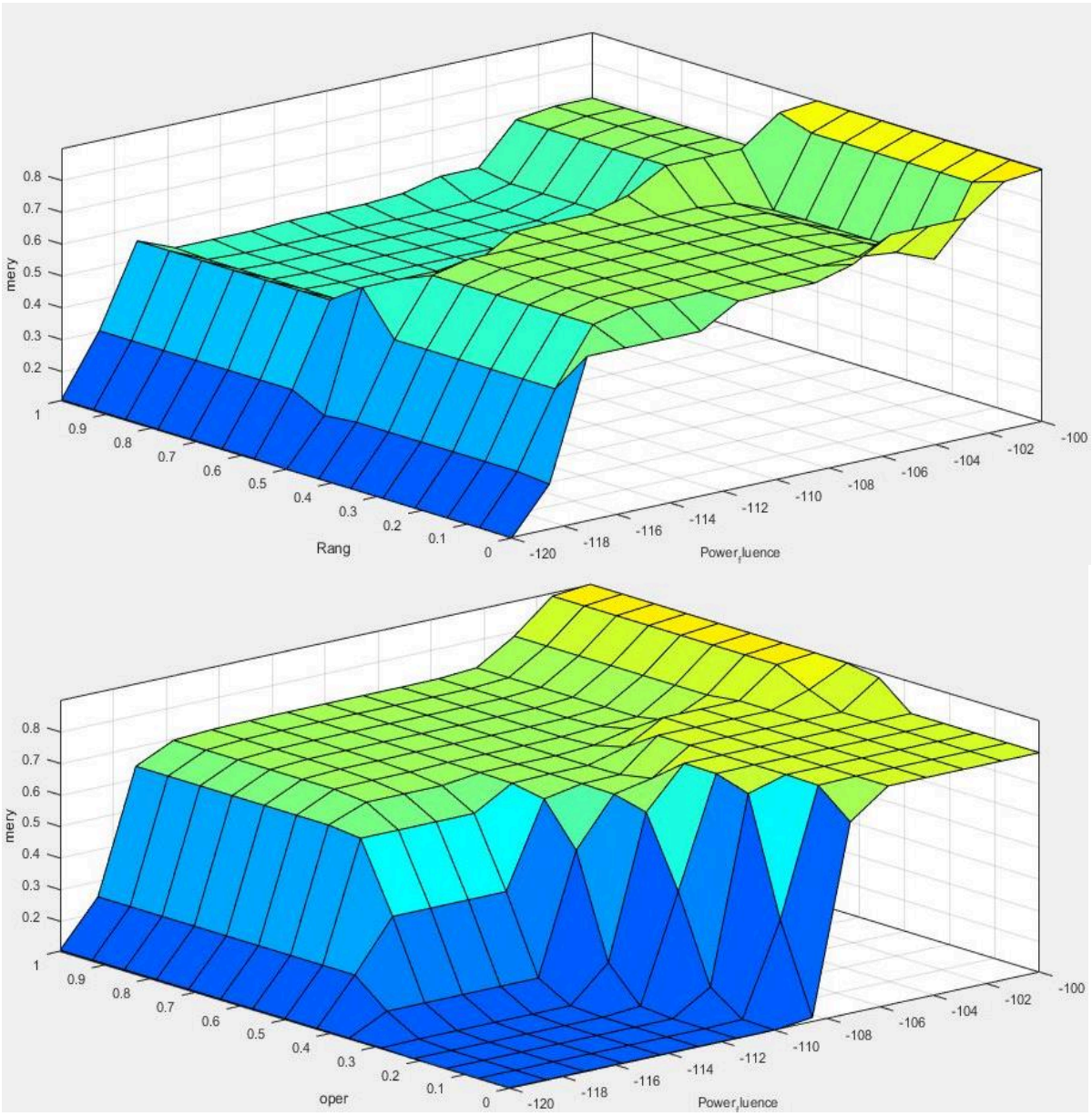


Рис. 4.7. Зависимости мер противодействия от входных переменных

Из данных зависимостей можно сделать вывод, что, например, при значении классификатора равном – 114 Дбм, значение лингвистической переменой «Мощность помехи» соответствует терму «СРЕДНЯЯ» и значении классификатора равном 0,7 значение лингвистической переменой «Оперативность информации» соответствует терму «ОПЕРАТИВНАЯ». По исходным заданным условиям активизируется правило 8, согласно которому результирующее значение выходной переменной «Меры» равной 0,7, что определяет значение лингвистической переменной «ИСПОЛЬЗОВАНИЕ MIMO»

Реализация нечеткой экспертной системы в виде алгоритма.

Предложенные нечеткие зависимости могут быть использованы в составе алгоритма, где принимаются решения в условиях неопределенности.

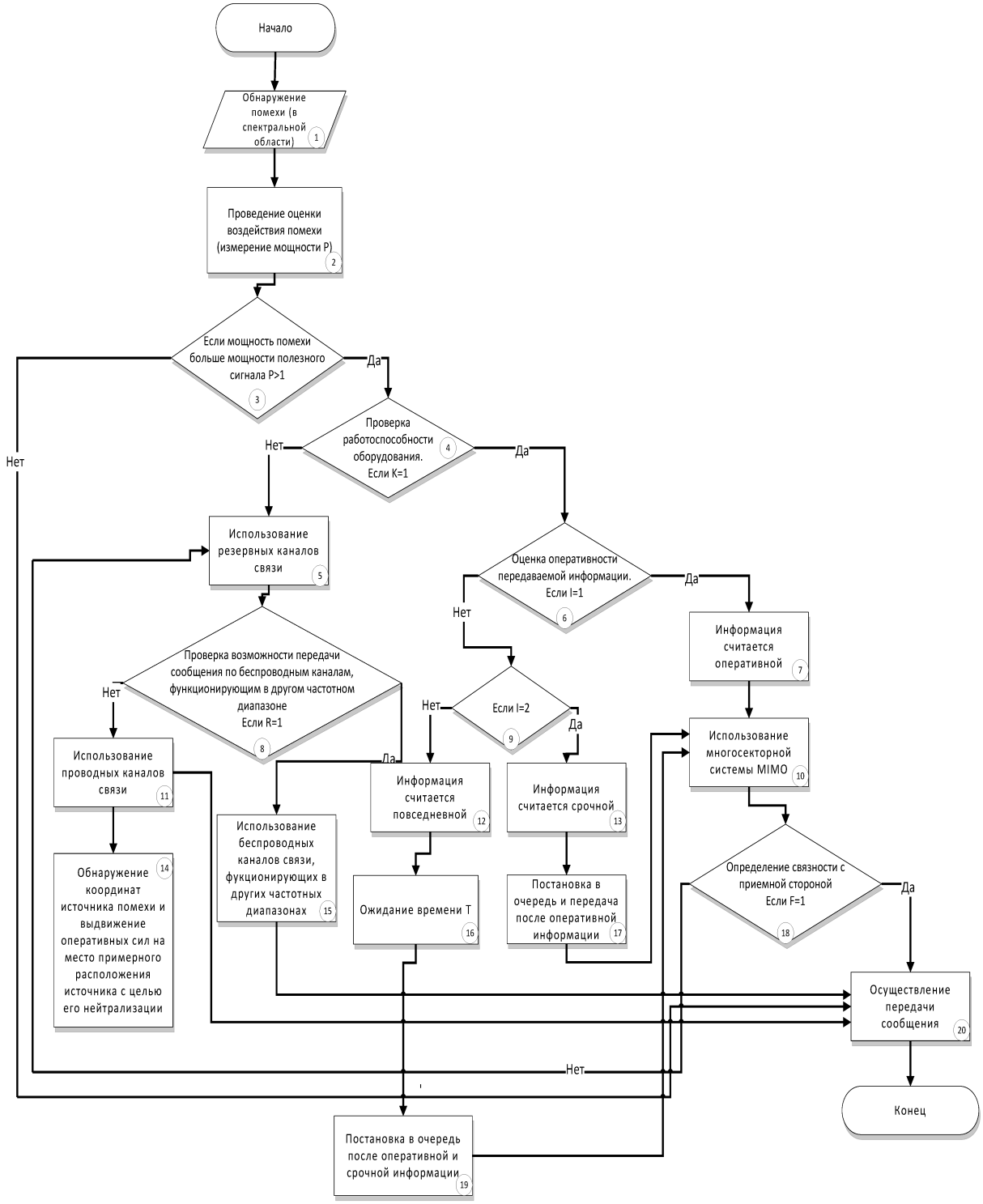


Рис. 4.8 Вариант реализации алгоритма

Пример алгоритма приведен на рис. 4.8. В данном алгоритме предполагается использование на этапах 3, 4, 6, 9 полученных ранее нечетких зависимостей, с помощью которых лицо, принимающее решение, сможет правильно классифицировать помеху и выбрать необходимые для этого меры противодействия.

Лицо, принимающее решение, задавая параметры переменных, может ориентироваться на предложенные зависимости и получить поддержку при принятии управленческих решений, данный алгоритм может быть реализован программно, благодаря чему можно добиться автоматизации процесса принятия решения.

Таким образом, в данном ученом пособии была рассмотрена тема противодействия деструктивным электромагнитным воздействиям при помощи нечетких экспертных систем. Выбранный метод является актуальным в данной ситуации, поскольку математический аппарат, описывающий системы, очень сложен и часто вне рассмотрения может оказаться некоторое количество важных показателей. Был проведен экспертный опрос, в ходе которого были определены уровни воздействия, при которых система связи специального назначений находится в каждом из трех состояний.

Полученные оценки были в дальнейшем использованы при построении модели противодействия на основе нечеткой логики. Модель позволяет определить меры противодействия деструктивным воздействиям при различных значениях входных параметров.

На основании данной модели предложен алгоритм, который может быть реализован в виде программного продукта и осуществлять поддержку при принятии решений по применению мер противодействия в условиях действующих деструктивных помех.

ЗАКЛЮЧЕНИЕ

Применение цифровой радиосвязи в системе связи МВД России является одним из основных инструментов, позволяющих повысить эффективность организации управления их подразделениями органов внутренних дел Российской Федерации.

В учебном пособии выявлена необходимость развития существующих ресурсов МВД России для сокращения времени реагирования и управления при функционировании базовой инфраструктуры ведомственной системы связи с учетом беспроводных решений и архитектуры широкополосных сетей, а также передачи речевого трафика и данных на мобильные объекты органов внутренних дел в перспективных сетях радиосвязи ОВД МВД России. Разработаны рекомендации по повышению эффективности функционирования сетей связи органов внутренних дел для использования в подразделениях МВД России.

Практическое решение задач, сформулированных в данной работе, в дальнейшем позволит создание системы интеллектуализированного автоматизированного проектирования и эксплуатации систем связи ОВД, что позволит существенно снизить затраты на модернизацию и эксплуатацию сетей радиосвязи при повышении качества их работы.

Современные системы подвижной радиосвязи, созданные на базе цифрового оборудования, позволяют обеспечить:

– возможность передачи в одном абонентском устройстве различных видов информации (речь, данные, сообщения), что соответствует концепции создания сети интегрального обслуживания;

– выравнивание качества речевого радиообмена по всей зоне обслуживания;

– высокую степень интеграции со стационарными сетями связи органов внутренних дел;

– повышение оперативности связи при реализации различных режимов связи, режим аварийных и приоритетных вызовов, уменьшение времени установления соединений, выделение частотных ресурсов для определенной группы абонентов, создание независимых подсистем в интересах отдельных групп абонентов;

– обеспечение радиосвязи не только между абонентами одной группы, но и между группами, возможность взаимодействия с сетями связи органов государственной власти, телефонными сетями общего пользования;

– устойчивое функционирование абонентских терминалов в условиях повышенного уровня внешних помех, возможность пользоваться радиосвязью с одновременным применением оружия, средств индивидуальной химической защиты;

– возможность дистанционного управления абонентскими терминалами;

– эффективное использование радиочастотного спектра, большее количество каналов в отведенной полосе.

Цифровые системы транкинговой радиосвязи более качественно реализуют режимы передачи данных, что все более востребовано на практике. При этом скорость передачи данных в цифровых системах значительно выше, чем в аналоговых. Цифровые системы радиосвязи имеют гибкую структуру адресации абонентов, что позволяет создавать различные виртуальные системы в пределах одной системы, а также организовать взаимодействие систем радиосвязи специального назначения различных ведомств.

Ряд подразделений органов внутренних дел нуждается в реализации дополнительных возможностей, таких как передача данных и навигация. Особые требования предъявляются к обеспечению защиты информации, передаваемой по радиоканалам. Защищенность специальных радиосистем является их важнейшим свойством.

В учебном пособии дается представление об основных принципах построения систем радиосвязи специального назначения, рассматривается взаимосвязь между радиотехническими и информационными процессами в каналах связи. Показано, что современные радиотехнологии базируются на основе сочетания традиционных возможностей радиосредств и IP-технологий.

На базе единого системного подхода изложены современные принципы построения систем радиосвязи специального назначения. Системы радиосвязи составляют транспортную основу современных информационных технологий, в которых сбор первичной информации, передача отображающих их сигналов по каналу связи на расстояние и прием этих сигналов обеспечиваются радиотехническими устройствами и системами, а обработка информации – средствами вычислительной техники.

Внедрение в информационные технологии средств вычислительной техники во многом изменило как привычные способы построения радиотехнических систем, так и способы передачи и обработки сигналов в них (концепция программно-определяемого радио). Знание архитектуры сетей, способов коммутации сигналов и сообщений становится необходимым для специалистов различных отраслей.

Представленный в работе материал позволит курсантам и слушателям, изучающим системы радиосвязи специального назначения, сотрудникам ОВД, получить представление о возможностях пповышения эффективности функционирования сетей связи органов внутренних дел на основе перспективных информационных технологий.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. О связи : федеральный закон от 07.07.2003 № 126–ФЗ // СПС «Консультант Плюс». URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284635&fld=134&dst=1000000001,0&rnd=0.051152897698079736#08312366978414549 (дата обращения: 09.03.2022). – текст: электронный.

2. Об утверждении концепции развития цифровой радиосвязи органов внутренних дел Российской Федерации до 2024 года приказ МВД России от 28 ноября 2019 г. № 892.

3. Канавин, С. В. Перспективы применения систем мобильного широкополосного доступа в сетях подвижной радиосвязи на основе стандартов MOBILE WIMAX и LTE / С. В. Канавин, А. С. Лукьянов – текст: непосредственный // Моделирование, оптимизация и информационные технологии. – Воронеж : Воронежский институт высоких технологий, 2016. – № 2. – С. 6–10.

4. Гилев, И. В Модель противодействия разрушению информации при деструктивных электромагнитных воздействиях в системах радиосвязи специального назначения на основе нечетких экспертных систем И. В. Гилев – текст: непосредственный // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 158–168.

5. Хохлов Н. С. К выбору критерия оценки эффективности функционирования инфокоммуникационных систем ОВД в условиях противодействия /О. И. Бокова, С. Н. Ляшенко, Н. С. Хохлов – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2016. № 1–3. С. 128–132.

6. Хохлов, Н. С. Экспериментальное исследование мобильной цифровой системы передачи видео и звука при совместном функционировании с радиоэлектронными средствами специального назначения в интересах органов внутренних дел / Н. С. Хохлов, С. В.Канавин, И. В. Гилев – текст: непосредственный. // Вестник Воронежского института МВД России. – 2019. – № 3. – С. 118–130.

7. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на показатели радиоэлектронной защиты / Н. С. Хохлов [и др.] – текст : непосредственный // Вестник Поволжского государственного технологического университета. Серия : Радиотехнические и инфокоммуникационные системы. – 2019. – № 1. – С. 22–30.

8. Хохлов Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел при электромагнитных воздействиях : монография. – Воронеж : Воронежский институт МВД России, 2005. – 181 с. – текст: непосредственный.

9. Базовая станция MicroMAXd: основные характеристики. – URL: http://winncom.ru/products/airspan–micromax (дата обращения: 09.03.2022). – текст: электронный.

10. Пименов, П. Н. Метод оценки помехоустойчивости средств широкополосного радиодоступа к воздействию сверхкоротких электромагнитных импульсов : диссертация кандидата технических наук. – Москва, 2015. – 133 с.

11. Хохлов, Н. С. Использование многосекторной антенной системы MIMO как элемента комплекса средств противодействия деструктивным электромагнитным воздействиям / Н. С. Хохлов, С. В. Канавин, И. В. Гилев – текст: непосредственный // Вестник Воронежского института МВД России. – 2019. – № 4. – С. 126-136.

12. Gilev, I. Modeling the Destructive Effect of Interference on Mobile Networks, Using the 3G Standard as an Example, Using a Noise Generator / I. Gilev, S. Kanavin – текст: непосредственный // Bulletin of the Lipetsk State Technical University. 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA). Lipetsk. 2019. p. 407-410. DOI: 10.1109/SUMMA48161.2019.8947533.

13. Gilev, I. Mathematical Modeling of Multicriteria Conflicts of Analytical Activity in Situation Centers of the Internal Affairs Authorities / I. Gilev, O. Piankov, A. Terentev – текст: непосредственный // Bulletin of Samara State Technical University. 2019. XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP). Samara. 2019. p. 795-798. DOI: 10.1109/CSCMP45713. 2019.8976766.

14. Хохлов, Н. С. Методический подход к оценке рисков нарушения информационной безопасности в самоорганизующихся мобильных сетях на основе аппарата нечеткой логики / Н. С. Хохлов, С. В. Канавин, А. Е. Рыбокитов – текст: непосредственный // Вестник Воронежского института МВД России. – 2018. – № 4. – С. 84–92.

15. Яхъяева, Г. Э. Нечеткие множества и нейронные сети : учебное пособие. / Г. Э. Яхъяева – текст: непосредственный //Москва : Лаборатория знаний, 2018. – 316 с. – текст: непосредственный.

16. Методы и технологии искусственного / Пер. с польск. И. Д. Рудинского. – Москва : Горячая линия – Телеком, 2010. – 520 с. – текст: непосредственный.

17. Жильцов, В. В. Практикум по нейросетевым технологиям: учебно–методическое пособие. / В. В. Жильцов, В. В. Чувикова – текст: непосредственный. // – Омск: СибАДИ, 2010. – 60 с

18. Гилев, И. В. Моделирование системы мобильного широкополосного доступа стандарта WIMAX в условиях многолучевого распространения сигнала / И. В. Гилев, С. В. Канавин – текст: непосредственный. // Вестник Воронежского института МВД России. – 2019. – № 2. – С. 181–191.

19. О методах обучения многослойных нейронных сетей прямого распространения. – URL // http://www.mechanoid.kiev.ua/neural–net–backprop3.html (дата обращения: 09.03.2022). – текст: электронный.

20. Задача византийских генералов – URL: // https://ru.wikipedia.org (дата обращения: 02.02.2022). – текст: электронный.

21. Andrew, N. G. Machine learning yearning. – URL: http: https://d2wvfoqc9gyqzf.cloudfront.net/content/uploads/2018/09/Ng–MLY01–13.pdf// (дата обращения: 09.03.2022). – текст: электронный.

22. Интеллектуальные навигационно-телекоммуникационные системы управления подвижными объектами с применением технологии облачных вычислений / Н. Г. Марков [и др.]. – текст: непосредственный. // – Москва : Горячая линия-Телеком, 2014. – 158 с.

23. Кикоть, В. Я. Социальное управление. Теория, методология, практика: монография / В. Я. Кикоть, Д. И. Грядовой. – текст: непосредственный. – Москва : ЮНИТИ-ДАНА, 2010. – 311 с.

24. Новосельцев В.И. Системный анализ: современные концепции. Воронеж: КВАРТА, 2003. – 360 с.

25. Организация радиосвязи в органах внутренних дел : учебное пособие : допущено МВД России в качестве учебного пособия для курсантов и слушателей образовательных организаций высшего образования системы МВД России / О. И. Бокова, Н. С. Хохлов, С. Н. Ляшенко, О. В. Пьянков, А. Н. Глушков. – текст: непосредственный. // – Воронеж: Воронежский институт МВД России, 2016. – 106 с.

26. Ляшенко, С.Н. Конвергенция сетей подвижной связи ОВД на основе IP протоколов и ROIP технологий / , С. Н. Ляшенко, О. И. Бокова, Н. С. Хохлов. – текст: непосредственный // Охрана, безопасность, связь. 2017. № 1-1. с. 187-191.

27. Рыжков, В.И. Информационные технологии в государственном и муниципальном управлении / В.И. Рыжков. – текст: непосредственный. – Хабаровск: Изд-во ДВАГС, 2004. – 220 с.

28. Новосельцев, В. И. Общая концепция модельного изучения конфликтов. Моделирование и анализ конфликтов в социально-экономических системах: монография / В. И. Новосельцев, С. А. Редкозубов. – текст: непосредственный. – Воронеж: ИПЦ «Научная книга». 2011. – С.25 – 34.

29. Ненадович, Д. М. Методологические аспекты экспертизы телекоммуникационных проектов / Д. М. Ненадович. – текст: непосредственный. – Москва : Горячая линия – Телеком, 2008. – 280 с.

30. Бокова, О. И. Анализ эффективности функционирования радиотехнических устройств ЕИТКС ОВД с помощью показателей качества, построенных на основе методов теории эффективности / О. И. Бокова, С. Е. Ефимов. – текст: непосредственный // Вестник Воронежского института России. – №1. – 2009. – С. 71-76.

31. Хохлов, Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел при электромагнитных воздействиях: Монография. // Н.С. Хохлов. – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2005. – 183 с.

32. О техническом регулировании : Федереральный закон от 27.12.2002 № 184-ФЗ. – URL : http://www.consultant.ru/ (дата обращения: 09.03.2022). – текст: электронный.

33. Об утверждении перечня средств связи, подлежащих обязательной сертификации : постановление Правительства Российской Федерации от 25.06.2009 № 532. – URL : http://www.consultant.ru/ (дата обращения 09.03.2022). – текст: электронный.

34. Техническое обеспечение защищенных систем связи: учебное пособие / О. И. Бокова [и др.] ; под редакцией доктора технических наук, профессора Н. С. Хохлова. – Воронеж : Воронежский институт МВД России, 2019. – 180 с. – текст: непосредственный.

35. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. – Введ. 2008-07-01. – Москва : Стандартинформ, 2008. – 34 с. – текст: непосредственный.

36. ГОСТ Р 52863-2007. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения – Введ. 2008-02-01. – Москва : Стандартинформ, 2007. – 10 с. – текст: непосредственный.

37. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 05.02.2010 N 26 «Об утверждении Правил применения базовых станций и ретрансляторов сетей подвижной радиосвязи. Часть IV. Правила применения оборудования подсистем базовых станций сетей подвижной радиосвязи стандарта DMR». – URL : https://digital.gov.ru/uploaded/files /26.05.02.2010_1.pdf (дата обращения: 15.02.2022). – текст: электронный.

38. ETSI TS 102 361-1 V1.4.5 (2007-12) Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol. — URL : https://www.etsi.org/deliver/etsi_ts/102300_102399/10236101/02.05.01_60/ts_10236101v020501p.pdf (дата обращения: 02.02.2022). – текст: электронный.

39. Secusmart – шифрование на microSD. – URL : https://venemus.com/other/933-secusmart-shifrovanie-na-microsd.html. (дата обращения: 02.02.2022). – текст: электронный.

40. Хохлов, Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел в условиях противодействия угрозам информационной

безопасности: монография / Н. С. Хохлов. – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2005. – 181 с.

41. Модели и методы формирования комплексов противодействия угрозам информационной безопасности в сетях связи специального назначения: монография / С. В. Канавин [и др.] ; под ред. Н. С. Хохлова. – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2020. – 175 с.

42. Гилев, И. В. Экспериментальное исследование по воспроизведению деструктивных электромагнитных воздействий, приводящих к разрушению и модификации информации в системах связи специального назначения / И. В. Гилев, С. В. Канавин, Н. С. Хохлов . – текст: непосредственный. // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 25–38.

43. Проектирование наземных радиосистем передачи информации с помощью специализированных программных комплексов / Канавин С. В., Хохлов Н. С., Бокова О. И. – текст: непосредственный. // Моделирование, оптимизация и информационные технологии. – Воронеж : Издательство Воронежского института высоких технологий. – 2016. – С. 1–6.

44. Бойко, А. А. Киберзащита автоматизированных систем воинских формирований: монография / А. А. Бойко. – текст: непосредственный. //. – Санкт-Петербург : Наукоемкие технологии, 2021. – 300 с.

45. Защищенные радиосистемы цифровой передачи информации / П. Н. Сердюков [и др.]. – текст: непосредственный. – Москва : АСТ. – 403 с.

46. Программно определяемая радиосистема. – URL : https://ru.wikipedia.org (дата обращения: 02.02.2022). – текст: электронный.

47. Отчет о НИР. Разработка нормативной правовой базы для применения робототехнических систем МВД России, в том числе с беспилотными летательными аппаратами, и комплекса технологических решений (искусственного интеллекта) по обработке больших данных в сфере внутренних дел : – Воронеж : Воронежский институт МВД России, 2020.

48. Исследование путей применения робототехнических комплексов (систем) в правоохранительной деятельности на базе перспективных информационно-коммуникационных технологий : отчет о НИР (заключительный) / А. Г. Конуров [и др.]. – текст: непосредственный. – Москва : ФКУ НПО «СТиС» МВД России, 2019.

49. Моисеев В. С. Групповое применение беспилотных летательных аппаратов: монография. / В. С. Моисеев. – текст: непосредственный. // – Казань: Редакционно-издательский центр «Школа», 2017. – 572 с.

50. Гололобов, В. Н. Беспилотники для любознательных. / В. Н. Гололобов, В. И. Ульянов. – текст: непосредственный. // – Санкт - Петербург : Наука и Техника, 2018. – 256 с.

51. На службу гаишникам пришли дроны [Электронный ресурс]. – URL : https://www.gazeta.ru/auto/2021/08/16_a_13883414.shtml?updated. (дата обращения: 07.10.2022). – текст: электронный.

52. Макаренко, С. И. Противодействие беспилотным летательным аппаратам: монография / С. И. Макаренко. – текст: непосредственный. – Санкт-Петербург: Наукоемкие технологии, 2020. – 204 с.

53. Хохлов, Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел в условиях противодействия угрозам информационной безопасности: монография / Н. С. Хохлов. – Воронеж : Воронежский институт МВД России, 2005. – 181 с. – текст: непосредственный.

54. Модели и методы формирования комплексов противодействия угрозам информационной безопасности в сетях связи специального назначения: монография / С. В. Канавин [и др.] ; под ред. Н. С. Хохлова. – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2020. – 175 с.

55. Гилев, И. В. Экспериментальное исследование по воспроизведению деструктивных электромагнитных воздействий, приводящих к разрушению и модификации информации в системах связи специального назначения / И. В. Гилев, С. В. Канавин, Н. С. Хохлов. – текст: непосредственный // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 25–38.

56. Самоцвет Н. А. Методы формирования и обработки сигналов и помех в аппаратуре испытаний РЭС на радиоэлектронную защиту импульсов : диссертация кандидата технических наук. – Воронеж., 2018. – 180 с. – текст: непосредственный.

57. Вооружение и специальные средства полиции за рубежом: Научно-технический информационный сборник. Вып. 2. – Москва.: ФКУ НПО «СТиС» МВД России, 2018. – 72 с. – текст: непосредственный.

58. Открытый обзор продукции российских производителей специальных средств и техники (для комплексного обеспечения правоохранительной деятельности): Научно-технический информационный сборник. Вып. 3. – Москва.: ФКУ НПО «СТиС» МВД России, 2018. – 113 с. . – текст: непосредственный.

59. Туманов, Е. А. Возможности применения беспилотных летательных аппаратов на службе госавтоинспекции / Е. А. Туманов, С. В. Назаров, Д. А. Тарасенков, В. Д. Головкин . – текст: непосредственный. // Дневник науки. 2019. – № 12. – С. 46.

60. Использование беспилотных летательных аппаратов в обеспечении безопасности дорожного движения. [Электронный ресурс]. – URL : https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-obespechenii-bezopasnosti-dorozhnogo-dvizheniya/viewer (дата обращения: 07.10.2022). – текст: электронный.

61. Леньшин А. В. Бортовые комплексы обороны самолетов и вертолетов / А. В. Леньшин. – текст: непосредственный. – Воронеж : Научная книга, 2018. – 312 с.

62. Сизов, О. С. Опыт применения беспилотных аэрофотосъемочных и батиметрических систем для реконструкции динамики уровня воды в андреевской озерной системе (тюменская область) / О. С. Сизов, Н. В. Приходько, В. М. Костомаров, В. А. Зах, А. В. Соромотин // Материалы Всероссийской научно-практической конференции (Иркутск, 22–23 мая 2018 г.). – текст: непосредственный. – Иркутск : Издательство Института географии им. В.Б. Сочавы СО РАН. – 2018. – С. 107–111.

63. Гилев, И. В. Система выбора и реализация способов противодействия деструктивному электромагнитному воздействию, оказываемого нарушителем / И. В. Гилев, С. В. Канавин, Н. С. Хохлов // патент на изобретение от 18.12.2020 № 2020142005. . – текст: непосредственный.

64. Особенности построения мобильных комплексов радиомониторинга на базе БПЛА / Канавин С.В., Кульбикаян Б.Х. – текст: непосредственный // Труды Международной научно-практической конференции. Перспективные телекоммуникационные и информационные системы и технологии. – Ростов-на-Дону: Издательство Ростовский государственный университет путей сообщения. – 2015. – С. 43-46.

65. Запечников, С. В. Основы построения виртуальных частных сетей. Учебное пособие для вузов / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. – текст: непосредственный. – Москва : Горячая линия – Телеком, 2012. – 248 с.

66. https://habr.com/ru/news/t/560122/ «Воентелеком» тестирует SIM карты с российским шифрованием. – текст: электронный.

67. Обзор криптографических шлюзов российских и зарубежных производителей. URL: https://www.antimalware.ru/analytics/Market_ Analysis/cryptographic-gateways-russian-and-foreign-manufacturers-2017 (дата обращения: 24.02.2022). – текст: электронный.

68. Кондрущенков, О. М. Актуальные решения по созданию защищенной ведомственной системы сотовой связи: Сборник МНПК Охрана, безопасность, связь 2018 / Кондрущенков О. М., Лекарь Л. А. – текст: непосредственный. – Воронеж : Воронежский институт МВД России, 2019. – Т. 1. – № 4. – С. 175 – 180.

69. 5. Кондрущенков, О. М. Построение защищенного ведомственного портала / О. М. Кондрущенков, Л. А. Лекарь. – текст: непосредственный. // Информационная безопасность социотехнических систем. – 2017. – № 3 (1). – С. 32–37.

70. Кондрущенков О. М. Защищенная территориальнораспределенная мультисервисная система связи для обеспечения управления в реальном масштабе времени / О. М.

Кондрущенков, Л. А. Лекарь. – текст: непосредственный. // Информационная безопасность социотехнических систем. – 2017. – № 1 (1). – С. 53–58.

71. Дурук, Е. В. Основы организации и управления VPN – сетями современных информационных систем специального назначения / Е. В. Друк, И. В. Левко. – текст: непосредственный. // T-Comm. – 2019. – Т. 13. – № 6 – С. 19–29.

72. М-687А, М-687В http://пниэи.рф/activity/production/m-687.htm (дата обращения: 24.02.2022). – текст: электронный.

73. Канавин, С. В. Построение защищенной ведомственной системы связи на базе технологии VPN: Сборник МНПК Общественная безопасность, законность и правопорядок в III тысячелетии 2021 / С. В. Канавин – Воронеж : Воронежский институт МВД России, 2021. – № 7-2. – С. 240 – 242.

74. К вопросу выбора стратегии защиты системы связи специального назначения при угрозах информационной безопасности. Моделирование, оптимизация и информационные технологии. / С. В. Канавин. – текст: непосредственный. – Воронеж: 2021. – Т. 9. – № 3 (34). – С. 21-22.

75. Оценка возможного ущерба и времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения. Моделирование, оптимизация и информационные технологии. / О. И. Бокова, С. В. Канавин, Н.С. Хохлов. – текст: непосредственный. – Воронеж: 2020. – Т. 8. – № 4. – С. 33-34.

76. Модель комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Моделирование, оптимизация и информационные технологии / О. И. Бокова, Д. А. Жайворонок, С. В. Канавин, Н. С. Хохлов. – текст: непосредственный. – Воронеж : Воронежский институт высоких технологий, 2020. – Т. 8. – № 2 (29). – С. 41-42.

77. Отчет о НИР Разработка требований к защищенной ведомственной системе мобильного широкополосного беспроводного радиодоступа, которая должна функционировать как VPN (виртуальная частная сеть) на системе связи общего пользования. – Воронеж : Воронежский институт МВД России, 2021. – № госрегистрации 07217594 – 74 с. – текст: непосредственный.

78. Ляшенко, С. Н. Использование спутниковых каналов связи в интересах МВД России / С.Н. Ляшенко, О.И. Бокова, С.В. Канавин// Общественная безопасность, законность и правопорядок в III тысячелетии. – 2016. – № 1. – С. 189–194.

79. Канавин, С. В. Организация мобильной видеоконференцсвязи с использованием аппаратуры VSAT. / С. В. Канавин, А. С. Лукьянов, А. Р. Дзогоев. – текст: непосредственный. // Проблемы обеспечения

безопасности при ликвидации последствий чрезвычайных ситуаций. – 2017. – Т. 1. – С. 472–476.

80. Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации : приказ МВД России от 23.09.2015 № 926 / СПС «КонсультантПлюс». – текст: электронный.

81. Гурлев, И. В. Методы и способы обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT / И. В. Гурлев. – текст: непосредственный. // Науковедение : интернет-журнал. – 2017. – Т. 9. – № 3. – С. 77.

82. Спутниковые системы связи : учебное пособие для вузов / под ред. А. М. Сомова. – Москва : Горячая линия – Телеком, 2015. – 244 с.

83. Канавин, С. В. потребителей аппаратуры ГЛОНАСС на основе аппаратно-программного моделирующего комплекса навигационно-мониторинговых систем для управления подвижными объектами / С. В. Канавин, О. И. Бокова, Н. С. Хохлов. – текст: непосредственный. // Моделирование, оптимизация и информационные технологии. – 2017. – №. 4. – С. 32.

84. Тавлинский, Д. А. состояния и перспективы развития методов WAN-оптимизации сетевого трафика / , Д. А. Тавлинский, Р. В. Чикин. – текст: непосредственный. // Научная мысль. – 2018. – Т. 4. – № 2. – С. 55–64.

85. Федорова, В. А. Анализ влияния средств защиты информации на пропускную способность сети / В. А. Федорова, Т. А. Моисеева, И. А. Колягина // Радиопромышленность. – 2018. – № 1. – С. 68–73.

86. Riverbed Technology [Электронный ресурс]. – URL: http://www.ctscorp.ru/riverbed-technology (дата обращения: 10.08.2021). – текст: электронный.

87. ViPNet Coordinator HW. – URL: https://infotecs.ru/product/setevye-komponenty/vipnet-coordinator-hw (дата обращения: 10.08.2022). – текст: электронный.

Учебное издание
Хохлов Николай Степанович,
доктор технических наук, профессор;
Никулин Сергей Сергеевич,
кандидат технических наук;
Людмила Антоновна Лекарь,
кандидат технических наук;
Канавин Сергей Владимирович,
кандидат технических наук;
Гилев Игорь Владимирович

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ СВЯЗИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПЕРСПЕКТИВНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

В авторской редакции

Подписано в печать __.__.____. Формат 60×84$^{1}/_{16}$.
Бумага офсетная. Гарнитура Таймс новая. Печать офсетная.
Усл.-печ. л. _____.
Тираж ___ экз. Заказ №___.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53