

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОСТОЧНО-СИБИРСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Д. С. Джурук, А. А. Курмазов, А. В. Никитин

**ТЕХНИЧЕСКИЕ СРЕДСТВА
ОБЕСПЕЧЕНИЯ ОХРАНЫ ОБЪЕКТОВ**

ИРКУТСК

Федеральное государственное казенное образовательное учреждение
высшего образования
«Восточно-Сибирский институт
Министерства внутренних дел Российской Федерации»

Д. С. Джурук, А. А. Курмазов, А. В. Никитин

**ТЕХНИЧЕСКИЕ СРЕДСТВА
ОБЕСПЕЧЕНИЯ ОХРАНЫ ОБЪЕКТОВ**

Учебное пособие

Иркутск
Восточно-Сибирский институт МВД России
2019

УДК 351.75
ББК 67.621.163

Печатается по решению редакционно-издательского совета
ФГКОУ ВО «Восточно-Сибирский институт МВД России»

Рецензенты:

Д. В. Токарский, заместитель начальника
Управления вневедомственной охраны войск национальной гвардии
Российской Федерации по Иркутской области, полковник полиции;
Д. Ф. Флоря, начальник каф. оперативно-разыскной деятельности ОВД
Орловского юридического института МВД России им. В. В. Лукьянова

Технические средства обеспечения охраны объектов: учебное пособие /
авт.-сост. Д. С. Джурук, А. А. Курмазов, А. В. Никитин. — Иркутск:
ФГКОУ ВО ВСИ МВД России, 2019. — 64 с.

Содержание и методическая структура настоящего учебного пособия
предусматривает выполнение основной цели программы обучения по пред-
мету «Специальная техника ОВД»: обучить будущих специалистов право-
применительной деятельности основам технической организации охраны
имущества граждан.

Предназначено для курсантов и слушателей 4 курса специальности
40.05.01 «Правовое обеспечение национальной безопасности» и 40.05.02
«Правоохранительная деятельность»

УДК 351.75
ББК 67.621.163

ОГЛАВЛЕНИЕ

Введение	4
1. Понятие и общая характеристика интегрированных систем безопасности	5
2. История создания интегрированной системы охранно-пожарной сигнализации «Приток-А»	10
3. Структура, назначение и возможности интегрированной системы охранно-пожарной сигнализации «Приток-А»	14
4. Подсистема мониторинга и охраны подвижных объектов «Приток-МПО»	34
5. Основные направления и перспективы развития технических средств безопасности ОВД	49
Заключение	59
Список рекомендуемой литературы	62

ВВЕДЕНИЕ

Мировой и отечественный опыт обеспечения имущественной безопасности показывает высокую эффективность технических средств охраны. Сегодня наблюдается достаточно устойчивая тенденция возрастания роли технических средств, их применение в охране имущества различных форм собственности позволяет минимизировать или исключить влияние человеческого фактора (ошибки, усталость и др.). Охрана объектов при помощи технических средств многократно надежнее физической охраны.

На российском рынке широко представлены технические средства охраны как зарубежных, так и отечественных производителей, которые уделяют большое внимание разработке и созданию эффективных средств безопасности с учетом последних достижений науки, в области коммутационных, информационных и других технологий. Однако не все средства охраны по своим техническим показателям соответствуют предъявляемым требованиям, которые представлены в «Единых технических требованиях к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единых технических требованиях к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны». Исходя из этого Главное управление вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации и ФКУ НИЦ «Охрана» Росгвардии отбирают лучшие образцы и внедряют их в деятельность подразделений вневедомственной охраны.

Изложенные положения определили актуальность проблемы совершенствования средств охранно-пожарной сигнализации и предопределили выбор темы работы, определили её цели и постановку задач, научную, методическую и практическую значимость исследований.

1. Понятие и общая характеристика интегрированных систем безопасности

Вопросы разработки и создания интегрированных систем безопасности¹ достаточно часто поднимаются на страницах специализированных изданий, но в силу своей сложности и глубины являются поистине неисчерпаемыми. В связи с непрерывным развитием отдельных подсистем безопасности и специализированного программного обеспечения, для управления ИСБ она остаётся актуальной с момента своего возникновения и по настоящее время. Компании, которые занимаются данными системами, пришли к их созданию различными путями, но вместе с тем общие принципы построения и функционирования остаются схожими [1]. Рассмотрим некоторые вопросы, связанные с составом, принципами построения, ролью отдельных подсистем и требованиями к программному обеспечению для ИСБ.

Интегрированные системы безопасности представляют собой совокупность технических средств охраны и обеспечения безопасности объекта, объединённых на основе единого программного комплекса в общую информационную среду с единой базой данных. Вопрос «Из чего состоит интегрированная система безопасности?» лежит на поверхности, но на самом деле на него не так просто ответить, поскольку её (системы безопасности) состав может меняться в зависимости от большого числа факторов. «Базовый» набор подсистем, входящих в интегрированную систему безопасности, можно представить следующим образом:

- система контроля и управления доступом — СКУД;
- система охранной сигнализации — ОС;
- система видеонаблюдения — CCTV;
- система пожарной сигнализации — ПС.

Есть также определённый круг задач, обычно относящийся к классу Building automation (управление лифтами, вентиляция, кондиционирование и пр.), но они могут быть неразрывно связаны с безопасностью. Например, управление доступом на определённые этажи — это не только управление лифтами, но и вопрос, связанный с системой контроля и управления доступом (СКУД). Правами физического доступа клиентов в отдельные помещения и зоны управляет именно эта система, а каждый этаж может рассматриваться как отдельная зона доступа. Это простой пример того, что граница между отдельными подсистемами стирается, и возникает задача,

¹ Далее — ИСБ.

которую необходимо решить потребителю (и ему не важно, как называется система, решающая эту задачу) [2].

Состав каждой конкретной интегрированной системы безопасности может изменяться, дополняться какими-то новыми подсистемами, или, наоборот, исключать их из общего списка. Это зависит от конкретных задач, определённых на этапе проектирования ИСБ на «живом» объекте. Общий вывод прост: ИСБ — не застывшая неизменяемая конструкция, а фактически сложный «живой организм» [4].

Объединение различных подсистем в рамках единой ИСБ позволяет решать вопросы комплексного обеспечения безопасности объекта максимально эффективно именно за счёт их взаимодействия и обмена информацией. Можно сказать по-другому: отдельные подсистемы как бы дополняют друг друга, помогая в конечном итоге решить общую задачу — обеспечение безопасности [3]. В то же время при эксплуатации подсистем различного назначения возникает необходимость эффективного управления, а такая задача может быть решена только за счёт централизации данной функции.

Централизация управления всем комплексом систем безопасности, возможность дистанционного мониторинга и управления подсистемами, входящими в ИСБ, позволяют оператору составить максимально полную картину функционирования объекта и состояния его подсистем. Это даёт возможность принять правильное решение с учётом всех полученных данных вне зависимости от их источника [4].

Пример: сработала система охранной сигнализации. На управляющем мониторе выводится план объекта с указанием конкретного охранного датчика, который выдал сигнал. Оператор (на том же мониторе) выводит изображение от ближайшей камеры теленаблюдения и визуально контролирует ситуацию. В случае ложного срабатывания тревога отменяется. Получаем адекватную реакцию на конкретную тревожную ситуацию. Необходимо будет провести диагностику датчика и, в случае его неисправности, заменить [4].

Программирование логических связей между подсистемами позволяет существенно повысить эффективность работы и надёжность интегрированной системы. В современных ИСБ можно запрограммировать логику работы системы с учётом сложных комбинаций сигналов от различных подсистем. За счёт этого можно добиться существенного сокращения времени реакции на события, предоставив право решения в конкретных случаях электронике, а также снижения влияния «человеческого фактора» за счёт автоматизации действий и реакций [5].

Пример: сработала система пожарной сигнализации. На управляющий монитор автоматически выводится план объекта с указанием рабо-

тавшего пожарного датчика. Одновременно подаётся звуковой сигнал тревоги и команда на запись изображения с ближайшей камеры с одновременным выводом данного изображения на монитор. В случае отсутствия команды со стороны оператора в течение нескольких секунд (заснул, отошёл и т. д.) интегрированная система безопасности автоматически выдаёт команду подсистеме СКУД на разблокирование всех дверей по пути эвакуации из указанного помещения.

Регистрация и документирование всех действий оператора и работы отдельных подсистем позволяют совершенствовать работу интегрированной системы безопасности, а также обеспечивают необходимым рабочим материалом должностных лиц, ответственных за безопасность объекта. На основе анализа данных материалов можно реально оценить правильность работы персонала, установить факты противоправных действий, зарегистрировать тревоги и факты несанкционированного доступа [4].

Пример: подсистема СКУД зарегистрировала факт нарушения сотрудником Ивановым времени прохода в помещение бухгалтерии, после которого обнаружилась пропажа важных документов. Факт несанкционированного прохода был также задокументирован системой видеонаблюдения, получившей сигнал от СКУД. Подтверждение разрешения на проход поступило от дежурного оператора интегрированной системы безопасности. В итоге на рабочем месте Иванова были обнаружены пропавшие документы, и его задержали. Дежурный оператор службы безопасности получил строгий выговор с понижением полномочий в управлении системой.

ИСБ позволяют также обеспечить снижение эксплуатационных расходов за счёт максимальной эффективности использования существующих ресурсов. Помимо решения непосредственных вопросов безопасности, в ИСБ можно обеспечить связь с инженерными системами объекта, что принесёт дополнительные выгоды его владельцу.

Пример: можно задать специальные режимы функционирования систем кондиционирования и отопления помещений, которые ночью переводятся в экономичный режим работы, что позволяет экономить немалые средства.

В упомянутый в самом начале «базовый» набор подсистем ИСБ обычно входит СКУД и ОС. Логика работы данных подсистем очень сильно взаимосвязана. Действительно, предоставить кому-либо доступ в определённое помещение, не сняв его перед этим с охраны, было бы довольно странно. В то же время «будет не лишним» иметь возможность автоматической постановки на охрану помещения в случае выхода из него последнего человека. Приведённый пример подразумевает тесное взаимодействие подсистем СКУД и ОС. Следует отметить, что многие производители СКУД имеют в составе линеек производимого оборудования обычно и ОС,

способную взаимодействовать со СКУД на уровне протокола обмена (самом глубоком аппаратном уровне). Обычно в этой «связке» панели охранной сигнализации подключаются к управляющим контроллерам СКУД, или сами контроллеры СКУД уже имеют встроенные функции ОС. Такая тесная интеграция обеспечивает возможность программирования сложных алгоритмов взаимодействия данных подсистем без участия компьютера (на аппаратном уровне).

Сказанное выше не означает невозможность интеграции СКУД и ОС разных производителей, но в таком случае она обычно выполняется программными средствами. Собственно говоря, именно за счёт программных средств в большинстве случаев обеспечивается интеграция в ИСБ и других подсистем — ССТV и ПС (систем видеонаблюдения и пожарной сигнализации).

Говоря о роли отдельных подсистем в ИСБ, невозможно обойти вопрос главенства. Обычно главной является та система, которая имеет наиболее развитую внутреннюю логику и возможность программирования сложных сценариев управления уже на аппаратном уровне. Такой системой в большинстве случаев является СКУД. Программирование действий и реакций на уровне контроллера СКУД обеспечивает ИСБ возможность функционирования даже при неработающих управляющих компьютерах, а следовательно, — гарантирует выполнение довольно сложного набора необходимых действий в критической ситуации [3].

Схема ИСБ для объекта с распределенной филиальной структурой

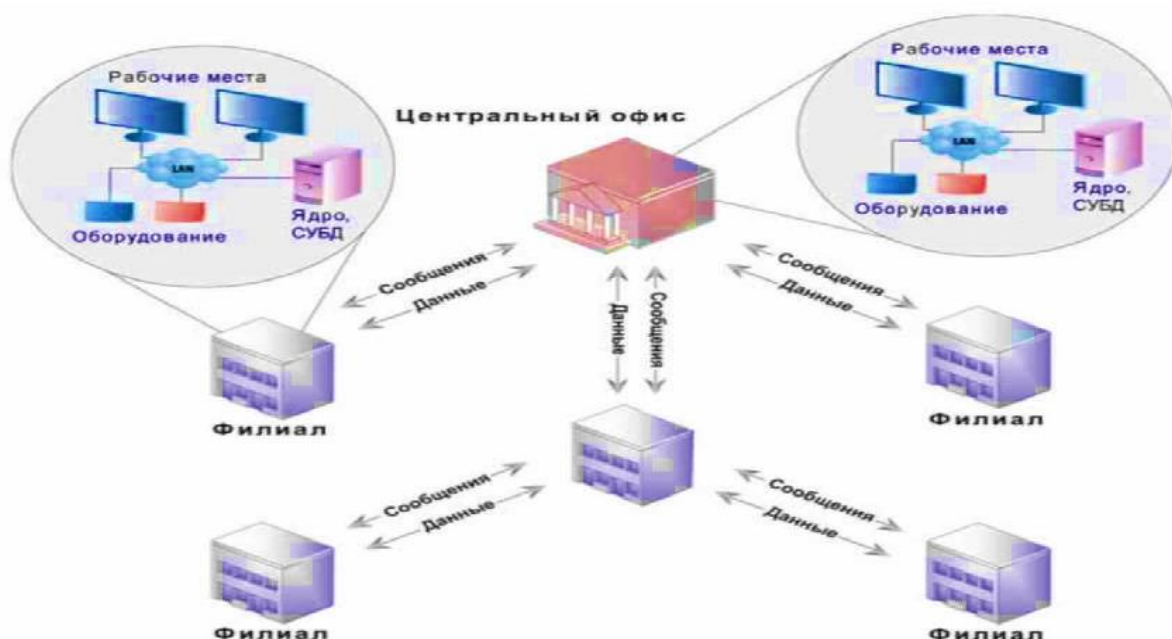


Рисунок 1

Программное обеспечение (ПО) для управления ИСБ имеет огромное значение, особенно когда идёт речь о предприятиях и объектах среднего и крупного масштаба, а также о предприятиях с распределённой филиальной структурой.

Это отдельная большая тема, поэтому в рамках данной работы можно дать лишь общие рекомендации. Организация сложного взаимодействия и объединение различных подсистем в рамках ИСБ, особенно в том случае, когда мы говорим об оборудовании не только разного назначения, но и различных производителей, возможны только на программном уровне. Это особенно актуально, когда объекты территориально разнесены на значительные расстояния (см. рис. 1).

Программное обеспечение для ИСБ должно иметь удобный и настраиваемый графический интерфейс. Каждый оператор, в зависимости от поставленной задачи, должен иметь возможность гибкой настройки — вывода только той информации, которая требуется ему для принятия решения в рамках предоставленных полномочий. Если он отвечает только за ПС, то остальная информация может оказаться избыточной. В то же время возможность вывода на компьютер изображения с камеры ССТV может, например, помочь ему удалённо оценить реальность угрозы при поступлении сигнала о возгорании от ПС. В конечном счёте именно несколько независимых источников получения информации могут реально помочь оператору принять правильное решение.

Важнейшим аспектом является надёжность работы ПО для ИСБ. Желательно, чтобы ПО для ИСБ имело такие функции, как «горячее» резервирование центрального сервера и «горячее» резервирование драйверов оборудования. Первая функция предоставляет возможность организации резервного сервера БД, который при выходе из строя основного сервера автоматически возьмёт на себя его работу. Вторая гарантирует, что при выходе из строя какого-либо из серверов, обслуживающих подсоединённое к нему оборудование, автоматически осуществляется переход этого оборудования на обслуживание функционирующими серверами системы. Данные механизмы повышения надёжности комплекса наиболее распространены на особо важных объектах и промышленных предприятиях, где действуют особенно жёсткие требования.

С точки зрения архитектуры построения ПО для ИСБ, желательно отделить пользовательский интерфейс от драйверов оборудования и других модулей системы. При этом управляющая консоль, драйверы оборудования, функциональные модули и ядро системы представляют собой отдельные, независимые друг от друга приложения. Благодаря этому существует возможность установления на рабочие станции только управляющей консоли, а подключение оборудования производить к другим компьюте-

рам системы. Оператор может повлиять на работу оборудования исключительно путём выдачи команд через управляющую консоль. Даже выключив свой компьютер, оператор не сможет прервать процесс работы системы с оборудованием. При этом в ПО должна быть развитая система контроля прав пользователей, позволяющая операторам исполнять только те команды, на которые они имеют право. Таким образом, достигается полная независимость работы всей системы от действий пользователей (операторов) [7].

Другой аспект надёжности — независимость работоспособности всей системы от работоспособности отдельных её модулей. При выходе из строя или выключении рабочих станций или серверов оборудования оставшаяся часть системы продолжает функционировать, а ранее выполняемые этими серверами функции автоматически переносятся на любые другие узлы сети, где установлены такие же модули. После восстановления работоспособности отключившихся узлов нагрузка переносится на них автоматически. Кроме устойчивости от сбоев эта особенность делает возможным распределение нагрузки между компьютерами в сети, а также даёт возможность производить добавление, обновление и удаление отдельных модулей, не останавливая работу всей системы [8].

В заключение можно сказать, что при выборе ИСБ необходимо чётко сформулировать перечень задач, которые она будет решать. Чем полнее и продуманнее будет данный перечень, тем лучше будет результат. Ну и, конечно же, необходимо обратиться к опытным профессионалам, которые имеют реальные внедрённые системы в России.

2. История создания интегрированной системы охранно-пожарной сигнализации «Приток-А»

Безопасность занимает в нашей жизни далеко не последнее место. Поэтому деятельность в области разработки и производства технических средств обеспечения безопасности является востребованной. Одним из ведущих производителей таких средств в России является ООО «Охранное Бюро «Сократ».

В 1989 г. иркутские инженеры-электронщики и программисты из научного внедренческого общества «Приток» (ныне «Сократ») при участии сотрудников управления вневедомственной охраны при УВД Иркутской области создали комплекс технических средств охраны «Интегрированная система охранно-пожарной сигнализации Приток» (ИС ОПС «Приток»).

Это первая российская система централизованной охраны на основе ПЭВМ. ИС ОПС «Приток» предназначена для организации автоматизированной централизованной охраны объектов и квартир с использованием телефонных линий связи и радиоканалов. Система обеспечивает работу с аппаратурой ОПС, разработанной специально для неё, с аппаратурой более ранних сроков разработки и с вновь разрабатываемыми охранными приборами. В состав системы входит аппаратура, устанавливаемая в пункте централизованной охраны (ПЦО), телефонной станции и охраняемых объектах. Аппаратура на ПЦО — это автоматизированные места, оснащённые ПЭВМ; аппаратура на телефонной станции — это специально разработанные системы передачи извещений. Для организации полностью автоматизированной охраны разработаны специальные приборы приёмно-контрольные (ППК) [9].

Все изменения состояния параметров, охраняемых объектов и квартир (взятие, снятие, тревога, авария и т. д.) фиксируются на ПЭВМ. В системе предусмотрено свыше двадцати форм выходной информации (карточка объекта, формирование суточного наряда и рапорта, регистрация радио- и телефонных переговоров). ППК обеспечивает автоматизированную тактику и одновременную идентификацию ответственных лиц при сдаче под охрану и снятии с неё объектов и квартир с помощью электронных кодовых ключей.

Одним из главных преимуществ системы иркутского производства, по отношению к другим аналогичным разработкам, стала идея, заложенная ещё на стадии проектирования. «Приток» должен интегрировать в себя всё то, что эксплуатировалось в подразделениях вневедомственной охраны и других подобных структурах, и развиваться независимо от того, какие технологии передачи информации в данный момент используются.

Благодаря своей универсальности и уникальной возможности оперативно адаптироваться к самым свежим разработкам мировой научной мысли, «Приток» опередил всех. Когда это потребовалось, то телефонную линию — традиционный в то время канал связи с милицейским пультом — дополнили радиоканалом и каналом сотовой связи. Сейчас пришло время интернет-протоколов, систем спутниковой навигации ГЛОНАСС/GPS [9].

Ещё одна важная особенность системы «Приток», также заложенная изначально, — это возможность интегрироваться со всевозможными устройствами охраны, наблюдения и контроля доступа — видеокамерами, электронными замками, турникетами и т. п. и безгранично «размножаться».

Ограничений по количеству объектов или охраняемой площади у системы нет. Например, периметр иркутского авиазавода, за которым следит «Приток», имеет длину около 50 км.

Система может охранять целый город и даже группу городов. В частности, такие проекты с помощью ОБ «СОКРАТ» реализованы во вневедомственной охране на юге России. Под охраной системы «Приток» находится сразу несколько городов: Пятигорск, Ессентуки, Минеральные Воды, Георгиевск и Кисловодск, с единым пультом централизованного наблюдения в Пятигорске. Также едиными «пультами» охраняются города Ставрополь и Краснодар. С учётом того, что сегодня Главное управление вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации ставит задачу перед техническими специалистами вневедомственной охраны производить объединение (укрупнение) ПЦО, система «Приток» становится наиболее востребованной при решении этой задачи.

За два последних десятилетия охранные технологии прошли сразу несколько ступеней эволюции. Если раньше основным средством, чтобы сообщить о происшествии, был телефон 02, а группы быстрого реагирования отправлялись по вызовам едва ли не на перекладных, то теперь ситуация иная в корне. Степень оснащённости выросла в разы. Полицейские экипажи оборудованы спутниковой навигацией. Дежурный офицер, который руководит действиями, на электронной карте видит перемещение групп задержания и может принять обоснованное решение по направлению на тревогу ближайшей. А компьютер ему просто подскажет, как действовать лучше [9].

Но, наверное, неправильно было бы представлять, что проект талантливых иркутских электронщиков вдруг в одночасье изменил принципы работы российской вневедомственной охраны. Силловые ведомства — не те структуры, чтобы сразу и единым порывом принимать новшества. Пришлось действовать настойчиво, убеждая и доказывая преимущества их системы. Сложности и некоторое непонимание наших возможностей были поначалу со стороны научно-исследовательского центра «Охрана». Их московский центр — серьёзная организация, где работают высококвалифицированные специалисты. Испытания нашей системы проводились в Балашихе. И мы убедили тогда столичных экспертов, что и в Иркутске возможны разработка и производство аппаратуры достойного уровня, причём превосходящего отдельные образцы той техники, которая разрабатывалась аналогичными предприятиями России.

Это был первый, но далеко не единственный случай, когда приходилось доказывать специалистам МВД своевременность и перспективность своих разработок. В 1998—1999 гг., мягко говоря, непониманием встретили в столице предложение «СОКРАТА» использовать в охране спутниковые технологии, Интернет, вести мониторинг автотранспорта. В 2001—2002 гг. точно так же отнеслись к предложению применять сотовую связь.

В конце концов, соответствующие решения, конечно, принимали. К тому моменту уже были созданы модернизированные системы и проводились их эксплуатационные, комплексные испытания. Делалось всё для того, чтобы эта аппаратура сразу пошла в подразделения [10].

В конце 90-х годов специалисты «СОКРАТА» уже апробировали свой новый комплекс, построенный на базе «Притока» с использованием технологий GPS — автомобильную спутниковую охранно-поисковую систему, теперь этот комплекс модернизирован и получил название «Приток-МПО ГЛОНАСС/GPS». Первыми приборами оснастили несколько автомобилей вневедомственной охраны.

Когда патрульные машины появились на экранах мониторов в дежурной части, иркутские милиционеры поначалу удивлялись, как всё это работает. Потом поняли, что это удобно — ежесекундно контролировать действия экипажей и, главное, в случае тревоги эффективно распределять силы.

Теперь уже полицейские хвастаются тем, что в работе они используют сеть спутников ГЛОНАСС, зависших на околоземной орбите.

В те годы милиция и серьёзная электроника, вычислительные машины были вещами абсолютно несовместимыми. Но тот день, когда в «СОКРАТЕ» убедились, что их разработка нужна, отмечается как день рождения предприятия. 25 декабря 1989 г. был подписан первый договор на разработку новой охранной системы для Иркутского управления вневедомственной охраны [10].

Было понятно, что руководство управления вневедомственной охраны Иркутской области рисковало. Но практически за год сотрудники НВО «Приток» смогли разработать то, что им требовалось. А уже после Иркутска был Якутск, Крым — Евпатория, Краснодар и др.

Информация об иркутской разработке попала в Воронежский институт МВД, где действовали курсы по повышению квалификации сотрудников милиции вневедомственной охраны. Их интерес оказался неподдельным. В «СОКРАТ» начали приезжать специалисты из других регионов — смотреть, изучать. Тогда же начались первые поставки нового оборудования по стране.

Основной потребитель охранно-пожарной системы — подразделения вневедомственной охраны Главное управление вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации. Их сейчас более 500.

Охранный комплекс «Приток» присутствует в Бюллетене технических средств безопасности, рекомендованных к использованию вневедомственной охраной. Этот бюллетень на сегодняшний день утверждается ГУВО ФСВНГ РФ.

3. Структура, назначение и возможности интегрированной системы охранно-пожарной сигнализации «Приток-А»

Интегрированная система охранно-пожарной сигнализации Приток-А (ИС ОПС Приток-А, в дальнейшем просто — система Приток), созданная иркутскими специалистами, в настоящее время успешно функционирует в более чем 50 регионах России, а также в Казахстане и Узбекистане.

Система «Приток» обеспечивает:

- охрану стационарных и мобильных объектов; при этом количество объектов, транспортных средств и территория их расположения практически неограничены;
- предупреждение о возникновении пожаров и других чрезвычайных ситуаций;
- мониторинг критически важных объектов и потенциально опасных грузов;
- контроль и предупреждение правонарушений (в рамках программ «Безопасный город»);
- охрану людей в рамках программы защиты свидетелей;
- охрану и управление доступом в различных учреждениях, и многие другие функции, необходимые при создании комплексных систем безопасности.

ИС «Приток-А» может быть основой системы поддержки принятия решений (СППР), т. к. уровень её надёжности и защищённости обеспечивает передачу на ПЦН достоверной информации. Другими словами, система обеспечивает гарантированную доставку извещений с объекта на ПЦН. Это в конечном итоге позволяет принимать правильное решение о направлении на объект средств реагирования (полицейской группы, пожарного расчёта, техники по обслуживанию и т. д.) и только на реально произошедшие события.

С пультов централизованного наблюдения (ПЦН) системы «Приток» производится не только контроль состояния объектов, но также контроль исправности элементов охранной, пожарной сигнализации и других технических средств обеспечения безопасности, в том числе и каналов передачи данных. Всё это позволяет своевременно обнаружить возникшую неисправность, принять меры по восстановлению работоспособности элементов системы. Для надёжности работы в системе предусмотрено применение резервных и дублирующих элементов, в том числе и каналов передачи данных.

Для передачи извещений с объекта на ПЦН, а также для передачи команд управления с ПЦН на объект в системе применяются практически все существующие каналы передачи данных:

- физические двухпроводные, выделенные или занятые телефонные линии;
- УКВ-радиоканалы лицензионных диапазонов;
- УКВ-радиоканалы безлицензионных диапазонов;
- высокоскоростные цифровые каналы передачи данных, работающие с применением протоколов TCP/IP и UDP, в том числе и оптоволоконные линии связи;
- каналы сотовой связи стандарта GSM, 3G и 4G;
- каналы открытого Интернета [11].

ИС «Приток-А» соответствует «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны», разработанным и утверждённым ГУВО МВД России.

Интегрированная система ОПС «Приток-А» состоит из многообразия программных и аппаратных средств:

1. Программное обеспечение (ПО) ИС «Приток-А».

ПО позволяет строить как локальные, так и распределённые, высокопроизводительные системы охранно-пожарной сигнализации, контроля и управления доступом, мониторинга подвижных объектов, видеонаблюдения, объединённые в локальную (или VPN-сеть, через глобальную сеть «Интернет») сеть ПЦН и работающие под управлением единого программного ядра. ПО ИС «Приток-А» работает под управлением ОС Windows. Количество серверов и рабочих станций, и других узлов системы безопасности в составе ИС «Приток-А» не ограничено. Система может начинаться строиться на базе одного ПК и развиваться до сотен используемых рабочих мест, обеспечивая универсальную и масштабируемую структуру ПЦН [10].

ПО ИС «Приток-А» обеспечивает:

- надёжную интеграцию различных подсистем через универсальные протоколы TCP/IP и UDP;
- широкие возможности разграничения прав доступа к функциям управления системой и к информации, хранящейся в системе (сведения об объектах охраны, об ответственных лицах, о собственниках, о тактике охраны и действий групп реагирования и т. д.);
- конфигурирование отдельных подсистем и системы в целом, а также создание и ведение баз данных;
- настройку системы на заданные алгоритмы работы и обработку оперативной информации в соответствии с заданными алгоритмами;

— настройку пользовательского интерфейса системы для повышения его удобства и эргономичности, что в итоге сокращает время обработки всех сообщений, в том числе и тревожных;

— работу с объектами, контролируемыми (охраняемыми) различными подсистемами, через единый пользовательский интерфейс;

— управление системой при помощи мнемосхем и планов охраняемых и находящихся под контролем объектов;

— регистрацию и архивирование всех событий, происходящих в системе, и протоколов действий дежурного персонала ПЦН, хранение копий оперативной БД и создание архивных копий событий системы, что позволяет в кратчайшие сроки проводить разбор как штатных, так и нештатных ситуаций за любой период — от текущего дня до нескольких лет в прошлом;

— формирование, просмотр и печать различных таймерных и оперативных отчётов, что позволяет в любой момент времени иметь исчерпывающую и достоверную информацию в удобном для пользователей виде;

— организацию высокопродуктивного взаимодействия различных служб предприятия- пользователя системы:

а) дежурной части;

б) инженерной службы (службы технической поддержки);

в) подразделений договорных отношений;

г) отдела кадров;

д) бухгалтерии и других служб и подразделений, участвующих в эксплуатации системы.

2. Оборудование и программное обеспечение каналов передачи данных

Каналообразующие программно-аппаратные средства ИС «Приток-А» (подсистема телекоммуникационных связей «Приток-TCP/IP») работают с применением протоколов TCP/IP и UDP. Эти протоколы являются современными технологическими средствами для построения распределённых (WAN) и (или) глобальных (типа VPN) сетей [10].

Подсистема телекоммуникационных связей «Приток-TCP/IP» позволяет реализовать взаимодействие локальной вычислительной сети АРМ пользователей системы с техническими средствами безопасности, включёнными в состав ИС «Приток-А» (элементами системы), расположенными в любой точке распределённых сетей предприятий (WAN) и (или) глобальных сетей (типа VPN), независимо от физической среды передачи данных.

Каналы связи между АРМ ПЦН и элементами ИС «Приток-А» могут представлять собой:

2.1. Локальные сети стандарта Ethernet 10/100.

2.2. Сети Radio Ethernet.

2.3. Телефонные каналы с использованием xDSL-модемов.

2.4. Корпоративные сети передачи данных, так называемые VPN-сети, создаваемые на основе существующих высокоскоростных цифровых каналов передачи данных, работающих, в том числе, и по волоконно-оптическим линиям связи (ВОЛС).

2.5. Сети Ethernet, работающие по каналам сотовой связи стандарта GSM, 3G и 4G.

2.6. Сети открытого Интернета и любые другие каналы связи (и в любом сочетании), поддерживающие протоколы TCP/IP и UDP и имеющие интерфейс стандарта Ethernet.

Примером программно-аппаратной реализации подсистемы может служить Коммуникатор Приток-TCP/IP. Универсальность и многофункциональность данного оборудования проявляется в том, что на базе одного изделия мы получаем возможность реализации множества подсистем. И для этого нужно только поменять прошивку коммуникатора и провести его настройку. Иными словами, единственный экземпляр коммуникатора при заливке соответствующего ПО работает с различными типами ретрансляторов, ППКОП и с оборудованием других производителей, обеспечивая обработку и передачу данных в общем протоколе в сеть ПЦО.

Подсистема Приток-TCP/IP позволяет строить комплексные системы безопасности, не ограниченные ни в количественном составе элементов, ни в пространстве, т. е. предназначенные как для охраны отдельно взятой квартиры, автомобиля, так и для охраны (мониторинга) крупных предприятий, городов, районов.

Использование любого оборудования, в том числе широкого спектра современных средств связи любых производителей, для создания сети ИС «Приток-А» обеспечивает гибкость и надёжность всей системы в целом.

3. Оборудование и программное обеспечение для сопряжения со старыми системами охраны, а также с системами охраны других производителей

Эти программно-аппаратные средства предназначены для интеграции в состав ИС «Приток-А» отдельных элементов (ретрансляторов, оконечных устройств и т. д.) или целых подсистем охраны и безопасности, т. е. технических средств охраны (ТСО) других производителей. Интегрированные ТСО будут работать в составе ИС «Приток-А» с применением каналов передачи данных, для которых они были созданы, и по протоколам, которые в них были заложены, но под управлением единого программного ядра и единой базой данных ИС «Приток-А» [10].

Аппаратура сопряжения с техническими средствами охраны других производителей позволяет внедрять ИС «Приток-А» там, где охранно-пожарная сигнализация и другие элементы систем безопасности уже эксплуатиру-

ются. Это обеспечивает плавный переход на современные технические средства охраны, оставляя на некоторое время в работе существующее оборудование. Примером такого оборудования может послужить комплект модернизации ретрансляторов СПИ «Фобос-3» — «Приток-АФ-02.3», которое позволяет заменить устаревшие ретрансляторы Фобос на оборудование, отвечающее современным стандартам, но с сохранением поддержки существующих УО на объектах.

4. Оборудование для автоматизированной централизованной охраны с использованием линий связи телефонных сетей или физических линий

Для организации автоматизированной централизованной охраны стационарных объектов с использованием линий связи телефонной сети или физических линий выпускаются ретрансляторы серии «Приток-А» на различное количество подключаемых направлений (от 20 до 240). Ретрансляторы могут объединяться в сеть ПЦН, используя любые, в том числе оптоволоконные каналы передачи данных, с применением протокола ТСР/ІР. Количество подключаемых ретрансляторов в системе не ограничено [10].

Ретрансляторы серии «Приток-А» работают с применением двустороннего, имитостойкого, помехозащищенного протокола передачи данных, обеспечивающего защиту от подмены ППКОП, а также защиту от подключения эквивалента ППКОП на линию связи канала РТР — объект. Наличие автоматической подстройки чувствительности приемника ретранслятора под индивидуальные параметры линии связи практически исключает ложные срабатывания в системе охраны.

В связи с тем что ретрансляторы серии «Приток-А» обеспечивают работу не только с ППКОП серии «Приток», но и с УО, работающими по протоколу ретрансляторов серии «Фобос», следовательно, они могут устанавливаться на место отработавших свой срок и снимаемых с производства ретрансляторов «Фобос-3» и «Фобос-ТР». Поскольку УО, работающие в протоколе Сигнал-ВК4 (УО-1А, УО-3к и пр.), являются устаревшими и не соответствуют техническим требованиям к ТСО. Установка ретрансляторов серии «Приток» (в том числе использование комплекта модернизации «Приток-АФ-02.3») позволяет проводить постепенное плановое переоборудование на объектах.

5. Оборудование для автоматизированной централизованной охраны по УКВ — радиоканалу лицензионных диапазонов [10].

Для организации автоматизированной централизованной охраны стационарных объектов, с использованием УКВ-радиоканала, в составе ИС «Приток-А» выпускаются так называемые базовые модули (БМ), радиоретрансляторы (РР), через которые с АРМ ПЦН через радиоэфир осуществляется постоянный контроль состояния охраняемых объектов, оборудован-

ных ППКОП с радиопередающими устройствами (РПДУ). Также через это оборудование производится приём, обработка и передача на АРМ ПЦН извещений, поступающих от ППКОП, и передача с АРМ ПЦН команд управления на ППКОП.

Поскольку и в БМ на ПЦН, и в РПДУ на объектах устанавливаются приёмопередатчики, то тем самым обеспечивается двусторонняя связь АРМ ПЦН — ППКОП, что позволяет вести постоянный контроль работоспособности канала передачи данных и производить автоматизированную постановку и снятие с охраны, получая извещение об этом на объекте.

6. Серия приборов приёмно-контрольных охранно-пожарных (ППКОП), коммуникаторов и концентраторов «Приток-А-4(8)» [10].

Приборы серии «Приток» выпускаются для контроля различного количества шлейфов, что позволяет оборудовать средствами охранной, пожарной и тревожной сигнализации объекты любой категории сложности.

Приборы выпускаются для работы по занятым телефонным линиям на частоте 18 кГц, для работы по УКВ-радиоканалу различных диапазонов частот, для работы по каналам сотовой связи стандарта GSM, для работы по каналам с использованием интерфейса RS485. Современные приборы выпускаются для работы по любым каналам передачи данных, использующим протоколы TCP/IP и UDR в том числе и для работы через Интернет.

ППКОП серии «Приток» работают с применением двустороннего имитостойкого протокола, защищённого 128-разрядным динамическим кодом.

ППКОП обеспечивают автоматизированную постановку под охрану и снятие с охраны при помощи идентификационных кодов (ИК), вводимых в ППКОП при помощи электронных идентификаторов Touch Memory и (или) клавиатуры. ИК заносятся в базу данных АРМ ПЦН по каждому шлейфу отдельно. ППКОП передаёт ИК в АРМ ПЦН для сравнения каждый раз при постановке под охрану и снятии с охраны.

Во всех современных ППКОП серии Приток реализован механизм дополнительной защиты ИК — применяется комбинация «код+ключ». В таком случае используется цифровой код, вводимый с клавиатуры ППКОП, известный только определённому ХО, и независимый ключ ТМ. Данный алгоритм значительно увеличивает защиту ИК от дублирования и попытки подбора кода.

Программирование тактики охраны и разграничения доступа производится с АРМ ПЦН или при помощи клавиатуры.

В ППКОП, работающих по занятым телефонным линиям, применяется адаптивная подстройка чувствительности приёмника ППКОП под индивидуальные параметры линии связи.

7. Оборудование для мониторинга подвижных объектов (МПО)

Выпускаются базовые модули (БМ) и бортовые комплекты (БК). БМ — это устройства, которые устанавливаются на ПЦН или в любом другом месте и обеспечивают приём информации с бортовых комплектов (БК) и передачу этих данных в АРМ ПЦН [10].

Бортовые комплекты (БК) — это оборудование, устанавливаемое на подвижном объекте, при помощи которого производится определение координат, скорости и направления движения этих объектов. Указанные параметры рассчитываются на основании сигналов, принимаемых со спутников Глобальной навигационной системы слежения (ГЛОНАСС) и (или) всемирной системы спутниковой навигации GPS (Global Positioning System), и в дальнейшем эти данные передаются в ИС Приток-А.

Передача информации с БК на БМ производится как по УКВ — радиоканалу, так и по каналам сотовой связи стандарта GSM, в режимах SMS-сообщений и GPRS.

Связь между БМ и АРМ ПЦН осуществляется по любым каналам с применением протокола TCP/IP или UDP, поэтому АРМ и БМ могут находиться друг от друга практически на любом расстоянии.

Подсистема «Приток-МПО» используется как для реализации мониторинга состояния ГЗ (групп задержания) или ведомственного транспорта, так и для охранных функций транспортных средств собственников. Также при использовании персональных трекеров организуется мониторинг и приём тревожных сообщений от физических лиц — инкассаторских служб или частных пользователей.

8. Оборудование и программное обеспечение для записи аудиоинформации на жёсткий диск компьютера [10].

Оборудование и программное обеспечение регистрации радио- и телефонных переговоров (подсистема «Приток-РТП») предназначены для регистрации и воспроизведения аудиоинформации, а также для организации автоматизированного оповещения. Используется там, где необходимо обеспечить запись и передачу аудиоинформации, поступающей и (или) передаваемой по телефонным или радиоканалам, а также присутствующей в помещении пульта централизованного наблюдения (запись с микрофона зала).

9. Программное обеспечение для интеграции в состав ИС Приток видеонаблюдения

Программное обеспечение позволяет работать с видеосерверами Domination, а также с различными IP-видеокамерами. Такая интеграция позволяет осуществлять визуальный контроль состояния объектов непосредственно с АРМ дежурного персонала ПЦН. Подсистема «Приток-Видеонаблюдение» позволяет получить картинку в АРМ ДПЦО автоматически (со-

гласно сценарию — возможно с нескольких различных камер) при тревожной ситуации на охраняемом объекте или по запросу пользователя.

10. Различное технологическое оборудование и тестовое программное обеспечение, применяемое для контроля работоспособности элементов ИС «Приток-А» как в процессе производства, так и в процессе эксплуатации.

Из всей совокупности программно-аппаратных средств ИС «Приток-А», работающих под управлением единого программного ядра, в зависимости от необходимости решения задач обеспечения безопасности могут формироваться различные подсистемы:

1. Подсистема телекоммуникационных связей («Приток-ТСР/IP») — для создания сети ПЦН. «Приток-ТСР/IP» обеспечивает передачу извещений и команд управления между элементами системы по цифровым, в том числе и оптоволоконным, каналам передачи данных.

2. Подсистема охранно-пожарной сигнализации (ОПС «Приток-А») — для централизованной охраны по телефонным каналам связи.

3. Подсистема радиоохраны («Приток-А-Р») — для централизованной охраны по лицензионному УКВ-радиоканалу.

4. Подсистема охраны и мониторинга по каналам сотовой связи («Приток-GSM») — для централизованной (в составе ИС «Приток-А») или автономной (как отдельная подсистема «Приток-МПО») охраны по каналам сотовой связи стандарта GSM, в режимах SMS-сообщений, GPRS или автодозвона, а также для создания подсистемы GSM-оповещения.

5. «Подсистема Микрорадиоохраны» («Приток-МКР») — для беспроводного наращивания (удлинения) подсистем ИС Приток-А и для создания автономных систем охраны с использованием трансиверов (приёмопередатчиков) мощностью не более 10 мВт, работающих в безлицензионных диапазонах частот.

6. Подсистема охраны и мониторинга через открытый Интернет («Приток-интернет») — для организации централизованной охраны через открытый Интернет. Для реализации резервных каналов связи могут использоваться другие подключения в сеть «Интернет» (через других провайдеров) и (или) каналы связи через сеть GSM в режиме GPRS.

7. Подсистема мониторинга и охраны подвижных объектов («Приток-МПО-ГЛОНАСС/GPS») — для контроля местоположения мобильных объектов на электронной карте и отображения на ней состояния объектов, в том числе находящихся в «тревоге».

8. Подсистема контроля и управления доступом («Приток-СКД») — для создания автономных и распределенных систем контроля и управления доступом с функцией централизованной охраны по цифровым каналам с применением протокола TCP/IP и интерфейса RS485.

9. Подсистема видеонаблюдения («Приток-Видео») — для получения видеоизображения с видеокамер, установленных на охраняемом объекте, подключаемых через видеосервер или с IP-видеокамер, и трансляции его на ПЦН по команде или по заданному событию.

10. Подсистема регистрации телефонных и радиопереговоров («Приток-РТП») — для записи аудиоинформации с различных каналов на жёсткий диск компьютера, поиска и воспроизведения её по заданным параметрам, организации системы оповещения.

Структура ИС «Приток-А» такова, что один ПЦН, созданный на её основе, может обеспечить охрану (мониторинг) небольшого учреждения, крупного предприятия, городского района, всего города и даже группу городов одновременно. Мониторинг может производиться с любого количества рабочих станций (автоматизированных рабочих мест — АРМ), устанавливаемых в сети ПЦН на любом расстоянии и в любом количестве.

Неоспоримым достоинством ИС «Приток-А» является то, что для передачи на ПЦН извещений о состоянии охраняемых объектов или подачи с ПЦН на объект управляющих команд имеется возможность одновременно использовать все вышеперечисленные каналы связи. Это позволяет создавать основные, резервные и дублирующие каналы передачи данных, что существенно повышает надёжность работы системы, способствует её дальнейшей модернизации и развитию.

Для описания всевозможных способов построения ИС «Приток-А» и её отдельных подсистем воспользуемся самым наглядным способом, т. е. изображением и рассмотрением структурных схем отдельных подсистем.

За 22 года, в течение которых ИС «Приток-А» эксплуатируется в подразделениях вневедомственной охраны МВД более чем 50 регионов России, на крупных промышленных предприятиях, в частных охранных структурах России, Казахстана и Узбекистана, количество созданных и запущенных в эксплуатацию систем достигло значительных величин. Составы этих систем, способы организации связи внутри систем, варианты подключения оборудования настолько многообразны, что изобразить обобщённую структурную схему системы «Приток-А» в полном объёме не представляется возможным. Для этого потребуется слишком много места и времени.

Попробуйте себе представить, как будет выглядеть структурная схема системы, если в одном из вариантов построения использовать не менее шести типов каналов (сред) передачи данных, не менее 35 видов объектового оборудования в различных комбинациях при нескольких десятках тысяч охраняемых объектов.

Что получится при перемножении приведённых данных? Учитывая то, что для каждого канала (каждой среды) применяются несколько вариантов различных ретрансляторов, коммуникаторов, базовых модулей или просто различное многообразие подключений в сетях VPN или в открытом Интерне-

те, общая схема достигнет невероятных размеров. Есть ли выход? Конечно, есть!

Обратимся к аналогии. Очевидно, что при строительстве великого разнообразия зданий и сооружений в крупном городе на самом деле использовалось всего несколько типов кирпичей (модулей). Но архитектор сначала рисует общий вид здания, а затем проектирует подробности его построения. Также и мы выпускаем большое многообразие электронных модулей (кирпичей), из которых в зависимости от задачи (общего вида) мы строим необходимую систему охраны (здание).

Итак, мы, поставили себе задачу построения различных ПЦН на основе элементов и подсистем ИС «Приток-А».

1. Начнём с самого необходимого: создадим основу, т. е. ПЦН для инсталляции программного обеспечения ПО ИС «Приток-А» без привязки к какой-либо конкретной подсистеме. А затем представим обобщённые структурные схемы ПЦН для всех подсистем ИС «Приток-А».

Как мы уже говорили, количество компьютеров в составе ПЦН не ограничено. Для достижения необходимой производительности и надёжности целесообразно использовать на ПЦН как минимум два компьютера с разделением функций серверов и рабочих станций. На рабочих станциях могут запускаться различные пользовательские АРМ.

Рекомендуемая (оптимальная) схема организации сети современного пульта централизованного наблюдения, позволяющего в дальнейшем использовать все возможности ИС «Приток-А», приведена на рис. 2.

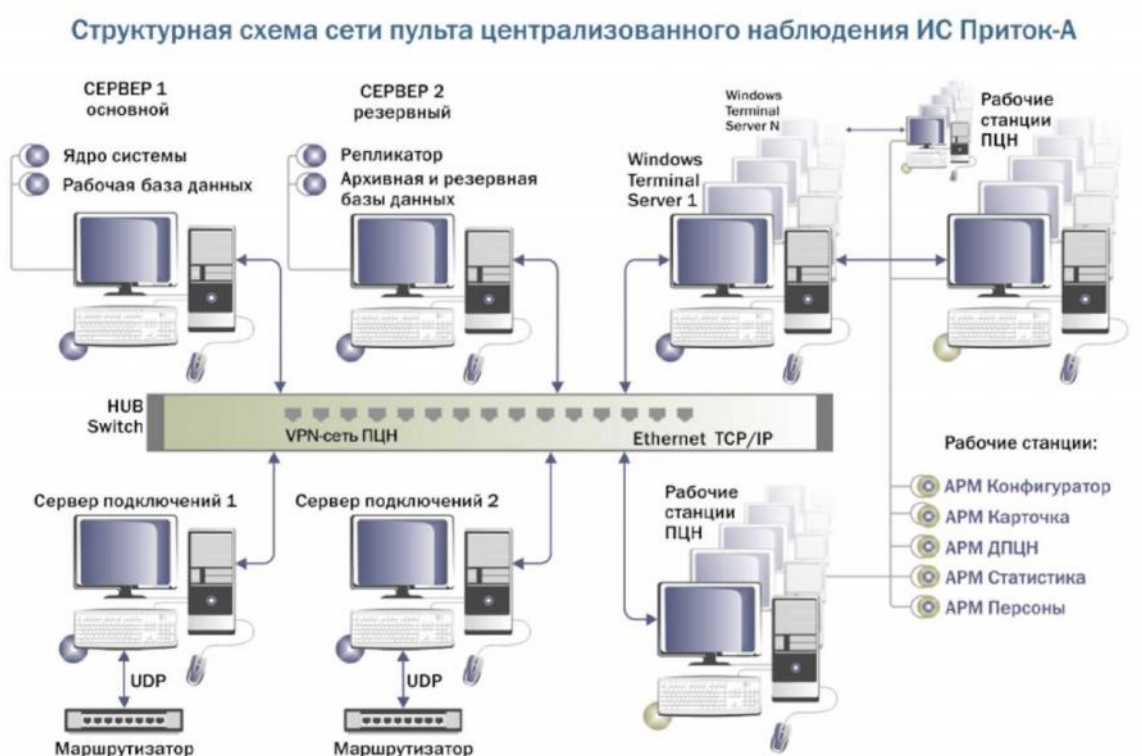


Рисунок 2

Хотя и сервер, и рабочую станцию можно запустить на одном компьютере, мы приводим максимальную структуру сети ПЦН. В конечном счёте, всё зависит от необходимого уровня надёжности и количества объектов, которые надо подключить к ПЦН для охраны.

Таким образом создана основа ИС «Приток-А — ПЦН» с установленным программным обеспечением. Далее, в зависимости от того, какую подсистему нам потребуется запускать в эксплуатацию, мы будем подключать необходимое для этого базовое оборудование и конфигурировать систему должным образом. Для простоты изображения структурных схем в дальнейшем мы не будем показывать дополнительные и резервные серверы и всевозможные варианты подключения рабочих станций (АРМ).

2. Для создания ПЦН, который обеспечивает охрану и мониторинг через VPN-сети типа GPON и (или) открытый Интернет («Приток-Интернет»), структурная схема ПЦН будет выглядеть, как указано на рис. 3.

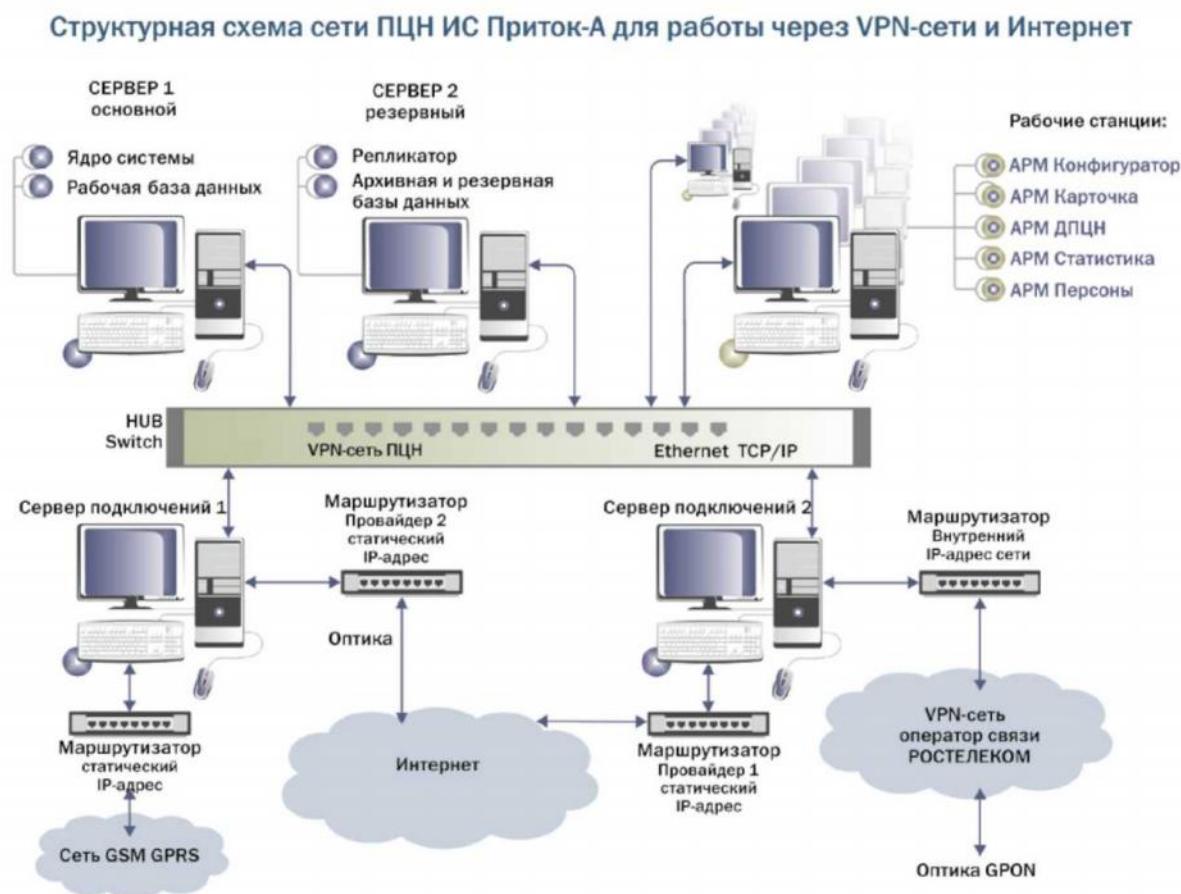


Рисунок 3

«Сервер подключений» подключается через маршрутизаторы в открытый Интернет. Для надёжности подключаемся не к одному, а к двум провайдерам. Каждый провайдер в этом случае выдаёт свой статический

IP-адрес. Подключение сети ПЦН может также быть сделано и через мобильный Интернет операторов сотовой связи. Для надёжности на ПЦН можно создать не один сервер подключений. Сеть ПЦН может строиться с применением разных технологий создания VPN-сетей (например, GPON оператора связи «Ростелеком»). В этом случае и на ПЦН, и на объектах будут закреплены IP-адреса внутренней VPN-сети такого оператора.

На объектах устанавливается ППКОП с ТСП-модулями, коммуникаторы ТСП/ IP, приборы с РКС-03 или приборы серии «Приток-А-КОП». Для обеспечения доступа в сеть «Интернет» охранного оборудования и совместного использования одного канала связи на объекте, например, пользователями веб-ресурсов, устанавливается маршрутизатор «бытового» уровня — DlinkDIR-300 или подобный, соответствующий требованиям провайдера сети.

На ПЦН и на объекте могут организовываться резервные каналы передачи данных через другого (запасного) провайдера, в том числе обеспечивающего другой физический канал связи. Это полностью соответствует требованиям, изложенным в разделах 5 и 6 «Единых требований к СЦН, предназначенным для применения в подразделениях вневедомственной охраны».

3. Самым мобильным и быстро создаваемым является ПЦН на основе сотовой связи стандарта GSM (см. рис. 3). По всей вероятности, эта схема в комментариях не нуждается. Следует отметить, что в данном случае качество системы охраны определяется зоной покрытия и надёжностью мобильной связи, предоставляемой операторами. Количество контролируемых объектов не ограничено. Особенностью данной схемы является то, что извещения о состоянии охраняемого объекта могут передаваться как на ПЦН, так и (или) на мобильные телефоны собственника. Например, в службу безопасности, её руководителям и т. д.

Связь ПЦН с объектовыми приборами может производиться с применением различных режимов: автодозвона, SMS-сообщений и GPRS. Для работы в режиме GPRS на ПЦН потребуется соединение через сеть «Интернет» с сервером оператора сотовой связи. Для надёжности работы в ППКОП предусмотрено наличие двух sim-карт различных операторов, а на ПЦН — подключение к нескольким операторам сотовой связи. Возможно, использование подключений к серверам провайдера непосредственно через сеть GSM или через VPN-сеть без использования сетей общего доступа (Интернет).



Рисунок 4

4. На предприятиях, в учреждениях, в районах, где развиты высокотехнологичные средства связи по скоростным цифровым каналам, ПЦН можно строить с использованием подсистемы телекоммуникационных связей «Приток-TCP/IP» (см. рис. 5).



Рисунок 5

Такой ПЦН легко создавать там, где уже есть внутренняя, локальная вычислительная сеть или для предприятия (учреждения) оператором связи создана корпоративная VPN-сеть.

Основные приборы, которые будут работать в такой системе охраны, — современная серия ППКОП, имеющая встроенные коммуникаторы ТСР/IP. Для подключения к такому ПЦН могут применяться коммуникаторы Приток-ТСР/IP различных вариантов исполнения, коммуникаторы резервных каналов связи «Приток-РКС». Они смогут обеспечить подключение различных ППКОП, коммуникаторов, концентраторов серии «Приток», которые уже установлены на объектах.

Достоинством данной схемы построения ПЦН является возможность организовать охрану объектов независимо от их местоположения. Все зависит от того, какого масштаба будет создана VPN-сеть. Причём система охраны может быть построена путём интеграции в уже существующую инфраструктуру корпоративной сети предприятия, учреждения.

5. Для организации подсистемы автоматизированной централизованной охраны по телефонным каналам связи (ОПС «Приток-А») необходимо к созданному ПЦН подключить хотя бы один ретранслятор серии «Приток-А» (см. рис. 6). Эта схема наиболее распространённая среди сотен действующих в России ПЦН.



Рисунок 6

При подключении одного ретранслятора «Приток-А-01» такая схема обеспечивает организацию пульта централизованного наблюдения для охраны до 240 направлений, а при использовании концентраторов до 7200

объектов в учреждении или на предприятии при наличии внутренней системы телефонных или проводных коммуникаций. В условиях плотной городской застройки эта схема обеспечивает организацию охраны микрорайона. Добавляя ретрансляторы, количество которых в составе ИС «Приток-А» не ограничено, можем получить систему практически любого масштаба.

6. На основе применения приёмопередатчиков УКВ-диапазонов можно создать подсистему радиоохраны «Приток-А-Р». Говоря другими словами, к ПЦН подключаем базовый модуль «Приток-А-Р-БМ», в котором установлена радиостанция. Такая схема применяется там, где отсутствуют телефонные или иные проводные физические коммуникации (см. рис. 7). Базовый модуль, как правило, устанавливается там, где обеспечивается наибольшее покрытие связи по выделенному УКВ-каналу. БМ работает с сетью ПЦН по каналу, обеспечивающему работу протокола TCP/IP. Для увеличения зоны покрытия на одной частоте в системе могут применяться до трёх радиоретрансляторов.



Рисунок 7

На объектах устанавливаются ППКОП с объектовыми РПДУ. Как видим из структурной схемы, что на объектах могут устанавливаться как отдельные ППКОП, так и концентраторы.

При использовании одной частоты такая схема обеспечивает организацию пульта централизованного наблюдения с 250 объектовыми РПДУ, то есть для охраны до 7500 объектов при использовании концентраторов. При необходимости увеличения количества охраняемых объектов выделя-

ется дополнительная частота и система легко наращивается путём добавления базового модуля и ретрансляторов. Базовых модулей, работающих на разных частотах, в системе может быть неограниченное количество.

7. Для беспроводного наращивания (удлинения связи) выше рассмотренных схем ПЦН ИС «Приток-А» создадим подсистему микрорадиоохраны «Приток-МКР». Она создаётся путём использования аппаратуры на основе трансиверов (приёмопередатчиков) мощностью не более 10 мВт (см. рис. 8). Работа «Приток-МКР» основана на создании радиосети с динамической маршрутизацией, в которой каждый узел связи может являться ретранслятором. В качестве узлов радиосети используется модуль «Приток-РПДУ-03», будем называть его «узлом связи» радиосети «Приток-МКР» [11].

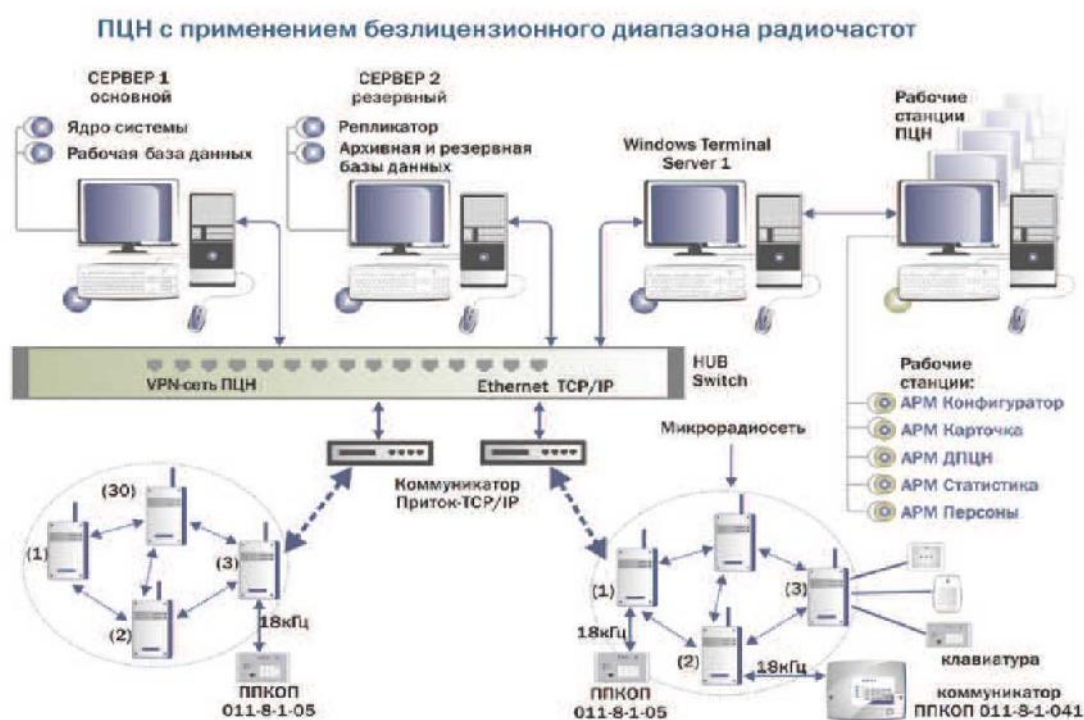


Рисунок 8

Для решения задачи наращивания подсистем с использованием Приток-МКР ПЦН менять не надо. Надо просто базовый узел из РПДУ-03 подключить к одному из концентраторов или коммуникаторов и произвести настройку новой конфигурации системы. Для использования Приток-МКР в качестве автономной системы охраны необходимо выбрать элемент, к которому будет подключён базовый «узел связи» РПДУ-03, а этот элемент подключить в сеть ПЦН, используя технологию TCP/IP. Такими коммуникаторами могут быть «Коммуникатор-TCP/IP», «Коммуникатор-GSM» или «Коммуникатор Приток-РКС».

8. Подсистема мониторинга и охраны подвижных объектов «Приток-МПО-ГЛОНАСС/ GPS» также создаётся на основе одного и того же ПЦН

и программного обеспечения. Для этого в состав ПЦН дополнительно устанавливается (генерируется) ещё один сервер — Сервер МПО-WEB, который включает в себя и Сервер карт. К сети ПЦН подключаются базовые модули (БМ-УКВ), обеспечивающие связь с бортовыми комплектами (БК) по УКВ-каналу и базовые модули (БМ-GSM), обеспечивающие связь с бортовыми комплектами (БК) и трекерами по каналам GSM (см. рис. 9).



Рисунок 9

В настоящее время выпускаются различные бортовые комплекты для работы как по УКВ-каналу, так и по каналам сотовой связи стандарта GSM, в режимах SMS и GPRS. Освоено серийное производство бортовых комплектов, которые удовлетворяют требованиям МВД, т. е. могут работать одновременно и по УКВ-каналам и по каналам GSM.

В сервер и рабочую станцию устанавливается соответствующее программное обеспечение АРМ «Приток-МПО» и необходимые электронные карты.

Рабочая станция позволяет:

- проконтролировать местоположение, скорость и направление движения транспортного средства (ТС), состояние БК (охраняется, не охраняется, тревога и т. д.), работоспособность БК, результаты ответов на поданные запросы и результаты выполнения поданных на БК команд управления;
- задать район нахождения, время и точку прибытия ТС, а также проконтролировать выполнение заданных параметров;
- рассчитать и отобразить, на основании оперативных или архивных данных, величину пробега, расход топлива, конфигурацию трасс движения ТС за указанный период.

Для контроля за перемещением и для охраны граждан система «Приток-МПО» обеспечивает работу с персональными GSM/SMS/GPRS/GPS трекерами. При работе с трекерами обеспечиваются функции отображения текущего местоположения, охраны трекера — обработка нажатия на тревожную кнопку SOS, привязки трекера к определённым зонам контроля, маршрутам движения и т. д.

9. ПЦН с элементами системы контроля и управления доступом («Приток-СКУД») строится для предприятий и организаций, где охрана производственных и других помещений совмещается с необходимостью иметь систему контроля и управление доступом, т. е. управлять дверями, турникетами, шлагбаумами и другими точками прохода/проезда (см. рис. 10) [11].

Общее количество охраняемых зон и точек прохода, подключаемых к одному коммуникатору, может быть 30. Количество коммуникаторов в системе не ограничено. Контроллеры «Приток-СКД» могут работать как в сети, так и автономно по заранее прописанному в них сценарию прохода.



Рисунок 10

10. Для обеспечения визуального наблюдения за охраняемыми объектами на основе ИС «Приток-А» можно создать систему видеонаблюдения. Для этого к ПЦН подключаем видеосервер, работающий с аналоговыми видеокамерами (см. рис. 10), или видеосервер, к которому через SWITCH подключаются IP-видеокамеры (см. рис. 11).

ПЦН Приток-Видео с применением аналоговых видеокамер

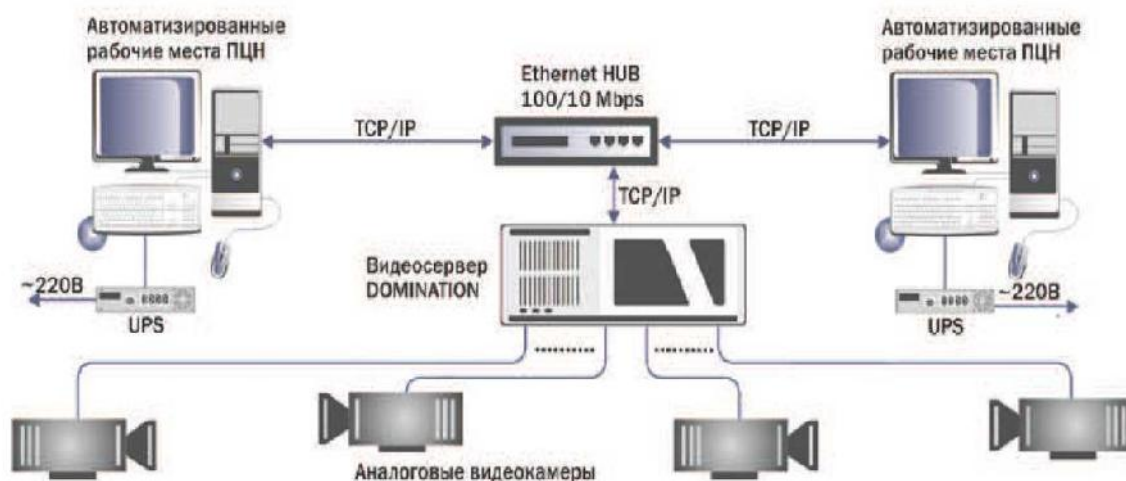


Рисунок 11

ПЦН Приток-Видео с применением IP-видеокамер

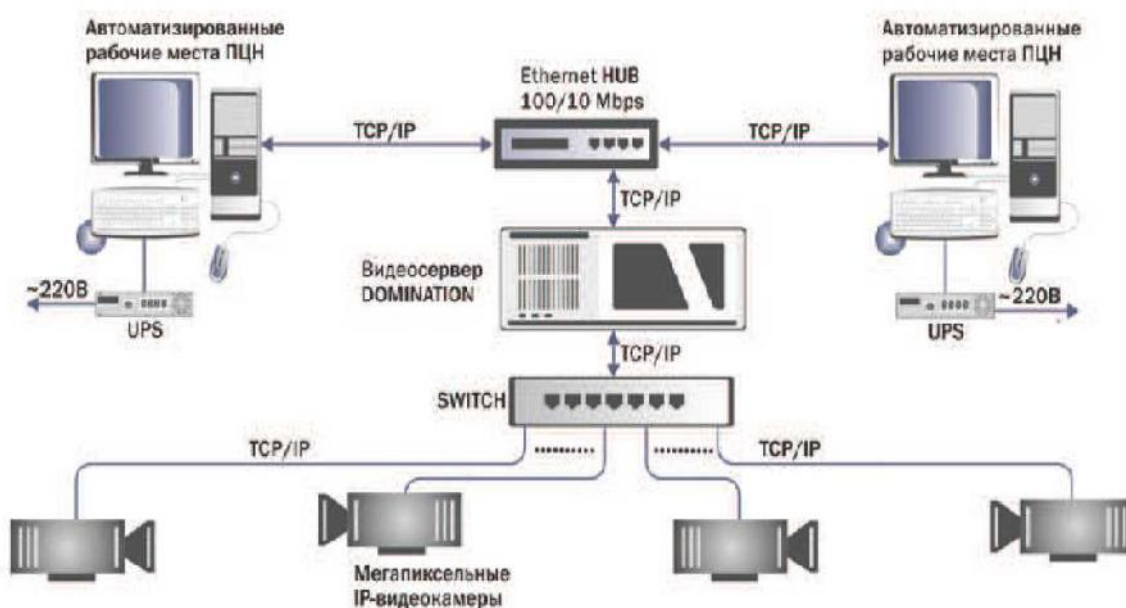


Рисунок 12

При описании конфигурации системы установленные видеокамеры привязываются к карточке наблюдаемого объекта. При вызове с АРМ ПЦН «Показать камеру» при работе с выбранным объектом будут активизированы все видеокамеры, привязанные к карточке данного объекта. Изображение будет выведено локально на АРМ, с которого была подана команда, или на специально выделенный ПК или монитор из нескольких доступных. Вы-

зов изображения с АРМ может быть подан дежурным пультом или автоматически по событию, указанному при настройке.

11. Подсистема регистрации телефонных и радиопереговоров Приток-РТП создаётся методом установки плат оцифровки и сжатия речи в одну из рабочих станций, в которую загружается ПО АРМ «Приток-РТП», (см. рис. 13). Это обеспечивает запись аудиоинформации, поступающей с различных каналов, подключаемых к данной плате, на жёсткий диск данной рабочей станции. ПО АРМ «Приток-РТП» позволяет по заданным параметрам производить поиск и воспроизведение ранее записанной аудиоинформации. Данная подсистема позволяет организовывать систему оповещения. Подсистема оповещения создаётся путём подготовки аудиосообщений, которые воспроизводятся абонентам по заранее подготовленному расписанию.



Рисунок 13

И в заключение. Приведённые схемы не дают полного представления об ИС «Приток-А». Варианты ПЦН для решения различных задач в области обеспечения безопасности могут быть построены на основе любой отдельной подсистемы с включением в неё элементов другой подсистемы. Это говорит о том, что после создания ПЦН одной подсистемы дальнейшее наращивание функциональных возможностей обеспечивается подключением к существующему ПЦН необходимого для этого оборудования и конфигурированием вновь созданной системы должным образом. Говоря другими словами, начав строительство ПЦН с элементарных модулей, мы сможем последовательно наращивать (увеличивать) масштабы системы и в конечном итоге получить

Интегрированную систему охранно-пожарной сигнализации «Приток-А» необходимой конфигурации.

На сегодняшний день в 50 регионах России ИС «Приток-А» эксплуатируется более чем в 500 подразделениях вневедомственной охраны. Система установлена в учреждениях власти, в том числе и в Государственной думе РФ. А кроме этого, на крупных промышленных предприятиях, таких как АК АЛРОСА, Ангарская нефтехимическая компании, Кузнецкий металлургический и Западносибирский металлургический комбинаты, Иркутское авиационное производственное объединение (сегодня — корпорация «Иркут»), каскад ГЭС (Иркутская, Братская, Усть-Илимская), Невинномысская ГРЭС и на многих других предприятиях, учреждениях здравоохранения и культуры и т. д.

ИС «Приток-А» принята за основу технической составляющей комплексных систем безопасности.

4. Подсистема мониторинга и охраны подвижных объектов «Приток-МПО»

Подсистема мониторинга и охраны подвижных объектов «Приток-МПО ГЛОНАСС/GPS» предназначена для мониторинга и охраны подвижных объектов (транспортных средств — ТС) и оценки оперативной обстановки по электронной карте контролируемого (охраняемого) района, города (местности), а также для контроля за перемещением и охраны граждан [12].

Одним из основных условий функционирования системы «Приток-МПО» является наличие установленной в АРМ ПЦН электронной карты местности.

Состав подсистемы «Приток-МПО»:

- программное обеспечение (ПО) ИС «Приток-А», устанавливаемое в АРМ (рабочие станции) пульта централизованного наблюдения (ПЦН) — диспетчерского центра (ДЦ), с электронной картой местности;
- базовый модуль «Приток-БМ-01(-02)»;
- базовый модуль «Приток-БМ-03(GSM)»;
- бортовой комплект «Приток-БК-01GPS (VHF)»;
- бортовой комплект «Приток-БК-011 ГЛОНАСС\GPS (VHF)»;
- бортовой комплект «Приток-БК-02GPS (UHF)»;
- бортовой комплект «Приток-БК-021 ГЛОНАСС\GPS (UHF)»;
- бортовой комплект «Приток-БК-03GPS (GSM)»;
- бортовой комплект «Приток-БК-031 ГЛОНАСС\GPS (GSM)»;
- бортовой комплект «Приток-БК-032 ГЛОНАСС\GPS (GSM/УКВ)»;

- бортовой комплект «Приток-БК-04GPS (GSM)»;
- бортовой комплект «Приток-БК-05 ГЛОНАСС\GPS (GSM)».

Базовый модуль (БМ) — устройство, которое обеспечивает приём информации с БК и передачу этих данных в диспетчерский центр (ДЦ) «Приток-МПО».

Бортовой комплект (БК) — устройство, которое устанавливается на ТС и обеспечивает приём со спутников Глобальной навигационной системы слежения (ГЛОНАСС) и (или) всемирной системы спутниковой навигации GPS (Global Positioning System) навигационных данных, расчёт своих координат, скорости и направления движения, контроль состояния датчиков охранной сигнализации и передачу этой информации в БМ.



Рисунок 14



Рисунок 15

Основные функции БК-03:

- дистанционная замена программного обеспечения БК-03 с АРМ ПЦН;

— дистанционная настройка режимов работы БК-03 с АРМ ПЦН и (или) с сотового телефона пользователя;

— возможность работы с семью пользователями (номерах сотовых телефонов), в том числе и БМ-03 ДЦ, которые записываются в БК-03 и наделяются правами доступа при настройке;

— определение координат с точностью до 10 м и скорости движения ТС с точностью до 2 км/ч;

— постановка под охрану, снятие с охраны с применением электронных идентификаторов (ЭИ) Touch Memory и (или) по команде от пользователя, подаваемой с помощью SMS-сообщения. В БК-03 может быть записано три ЭИ;

— контроль напряжения бортовой сети ТС, состояния охранных датчиков и передача сообщений пользователям, то есть на ДЦ;

— формирование и передача сигнала тревоги при буксировке автомобиля, находящегося под охраной;

— автоматическая блокировка двигателя, если не было произведено штатное снятие;

— выполнение команд пользователей по управлению центральным замком, запуском и блокировкой двигателя, дополнительной сиреной при поиске ТС.

Принцип действия «Приток-МПО» основан на определении координат, скорости и направления движения ТС на основании данных, принимаемых со спутников Глобальной навигационной системы слежения (ГЛОНАСС) и (или) всемирной системы спутниковой навигации GPS (Global Positioning System), передаче этих данных на ДЦ и отображении состояния контролируемого объекта и его местоположения на электронной карте местности.

Передача информации от БК в БМ обеспечивается как по УКВ-радиоканалу, так и по каналам сотовой связи стандарта GSM 900/1800, в режимах SMS-сообщений и (или) GPRS. При применении УКВ — радиоканала расстояние между БК и БМ может быть до 30 км, радиус действия GSM-канала определяется зоной покрытия сети операторов сотовой связи.

Обмен данными между БМ и рабочими станциями ДЦ (АРМ ПЦН) производится с применением протокола TCP/IP, поэтому расстояние от ДЦ до БМ определяется наличием канала передачи данных.

БМ и БК, предназначенные для работы по УКВ — радиоканалу имеют индексы — 01 и 02.

БМ для работы по каналу GSM имеют индексы — 03,04 (GSM).

БК, предназначенные для работы по каналу GSM, имеют индексы — 03,04,05.

БК, предназначенный для работы и по УКВ — радиоканалу и по каналу GSM, имеют индекс-032.

БК-01 и БК-02 предназначены только для мониторинга ТС, устанавливаются на ТС открыто. В герметичном металлическом корпусе БК установ-

лены приёмник сигналов спутниковой навигации, радиостанция и блок контроля. Сверху на корпусе установлены УКВ и спутниковая антенны. Питание БК производится от бортовой сети ТС +12В.

БК-01 и БК-02 обеспечивают прием навигационных сигналов со спутников, расчёт координат и скорости движения ТС, контроль состояния тревожной кнопки и передачу информации на ДЦ через БМ-01 или БМ-02 соответственно.

БК-03 предназначен для мониторинга и охраны, устанавливается на ТС скрытно, состоит из бортового контроллера со встроенным GSM-модулем и приемника спутниковой навигации. Питание БК-03 производится от бортовой сети ТС +12В и от резервной батареи.

В БК-03 могут устанавливаться SIM-карты любых операторов. Он может работать самостоятельно и совместно с любой другой сигнализацией, установленной в ТС. Имеет пять входов для подключения датчиков охранной и тревожной сигнализации и четыре выхода (ключа) управления, например управление работой двигателя и звуковым оповещением.

Бортовой комплект «Приток-БК-032» предназначен для определения координат подвижного объекта, скорости движения, его состояния, охраны, дистанционного управления функциями охраны и передачи/получения этой служебной информации в диспетчерские центры по УКВ — радиоканалу и по каналам сотовой связи стандарта GSM. БК устанавливается в транспортное средство (автомобиль).

Приток БК-032



Рисунок 16

Основные функциональные характеристики БК-032:

- вычисление навигационных параметров транспортного средства: координат, скорости движения, курса, высоты над уровнем моря в системах ГЛОНАСС/GPS;
- наличие двух каналов связи с базовыми модулями центра мониторинга: канал GSM в режимах SMS и GPRS и УКВ-радиоканал. Скорость передачи данных по УКВ-радиоканалу — не менее 2400 бод;
- наличие режима речевой связи с центром мониторинга;

— возможность накопления навигационной информации в собственной энергонезависимой памяти;

— возможность дистанционной передачи накопленных данных в центр мониторинга через каналы GSM (GPRS) или при подключении БК к рабочей станции через специальный разъем.

Бортовой комплект БК-032 соответствует требованиям ГОСТ Р 50789, ГОСТ Р 50842, ГОСТ 23216—78, ГОСТ 14254 (IP51), ГОСТ 12.1.004, ГОСТ 12.2.007, ГОСТ Р МЭК 60065.

Состав подсистемы «Приток-МПО»:

— блок управления, состоящий из контроллера, модуля ГЛОНАСС/GPS, модуля GSM, резервного источника питания с аккумуляторной батареей, устройства управления электрическими цепями транспортного средства, подключёнными к БК;

— антенны GSM, ГЛОНАСС/GPS;

— УКВ-радиостанция;

— автомобильная УКВ — антенна на магнитном основании;

— комплект кабелей для монтажа и кабели антенно-фидерных устройств (АФУ).

Бортовой комплект БК-032 имеет:

— восемь входов для подключения датчиков, с защитой от напряжения до 100В;

— вход для подключения тревожной кнопки;

— разъем для подключения пульта формализованных сообщений;

— специальный разъем для подключения мобильного компьютера.

БК-032 позволяет производить приём и выполнение команд диспетчерского центра:

— получение и изменение параметров БК (16 параметров);

— управление ключами на БК «вкл./откл.» (по пяти ключам);

— производить приём и отображение неформализованной информации (до 64 символов).

Диспетчерский центр — «Приток-МПО».

Диспетчерский центр «Приток МПО» обеспечивает обработку, отображение в реальном масштабе времени и архивирование всей информации, поступающей автоматически или по запросам, а также обработку и отображение архивной информации. Подсистема «Приток-МПО» работает автономно или в составе ИС «Приток-А».

Возможный состав диспетчерского центра «Приток-МПО».

Программное обеспечение рабочей станции (ПО АРМ «Приток-МПО ЛИПГ.425618.001 ПО»), которое обеспечивает работу оперативного персонала со всем объемом информации системы мониторинга «Приток-МПО», в том числе и с архивными данными. Устанавливается на ПК (сервер ДЦ «Приток-МПО») с ОС семейства Windows. Может использоваться совместно в составе ИС «Приток-А». Основные задачи — обработка, отоб-

ражение на карте местности, приём и отправка команд и сообщений при работе с БК, персональными трекерами и стационарными объектами.

Базовый модуль «Приток-А-Р-БМ-01» или «Приток-А-Р-БМ-02», предназначенный для мониторинга подвижных объектов по УКВ — радиоканалу, который обеспечивает:

- приём информации с БК и передачу команд управления на БК по УКВ — радиоканалу;

- связь с рабочими станциями системы через каналы, поддерживающие протокол TCP/IP.

Базовый модуль «Приток-А-БМ-03 (GSM)», предназначенный для мониторинга стационарных и подвижных объектов по каналам сотовой связи, который обеспечивает:

- связь с рабочими станциями системы через каналы, поддерживающие протокол TCP/IP;

- поддержку работы с бортовыми комплектами и персональными трекерами в режимах GPRS, SMS и дозвона.

Программное обеспечение сервера ДЦ «Приток-МПО».

Программное обеспечение сервера совместимо со средствами защиты информации по проводным и беспроводным каналам связи и межсетевого экранирования, сертифицированных ФСБ и ФСТЭК России.

Программное обеспечение сервера делает возможным подключение и обслуживание абонентского оборудования как по TCP/IP — совместимым транспортным сетям, так и по ведомственным сетям УКВ.

Контроль перемещения и охрана граждан.

Для контроля за перемещением и для охраны граждан система Приток-МПО обеспечивает работу с персональными GSM/SMS/GPRS/GPS-трекерами.

При работе с персональными трекерами «Приток-МПО» производит прием сообщений от трекеров по GSM-каналу в режимах SMS-сообщений и GPRS. На основании сообщений, полученных от трекеров, АРМ Приток-МПО производит:

- отображение текущего местоположения и состояния трекера (подвижного объекта: человека, животного и т. д.) на электронной карте местности;

- просмотр архива перемещения трекера;

- расчёт пробега и формирование различных аналитических отчётов с последующим выводом на печать;

- охрану трекера — обработку сообщения после нажатия на тревожную кнопку SOS;

- привязку трекера к определённым зонам контроля, маршрутам движения;

- контроль превышения скорости движения, отклонения от заданного маршрута движения, выход из зоны контроля.



Рисунок 17

Рабочие станции (АРМ ПЦН) «Приток-МПО» позволяют:

1. Проконтролировать местоположение, скорость и направление движения ТС, состояние БК (охраняется, не охраняется, тревога и т. д.), работоспособность БК по результатам диагностики, результаты ответов на поданные запросы и результаты выполнения поданных на БК команд управления.

2. Рассчитать и отобразить на основании оперативных или архивных данных величину пробега, расход топлива, конфигурацию трасс движения ТС за указанный период.

3. Задать район нахождения, время и точку прибытия ТС, а также проконтролировать выполнение заданных параметров.

4. Подать команды управления на БК: взять под охрану, заблокировать двигатель и т. д.

«Приток-МПО» поддерживает работу с различными типами треков. Например, с трекерами GlodalSat.

GlobalSatTR-203 — это персональное устройство контроля местоположения (тренинга) с функцией быстрого определения координат.

Среди прочих функций трекера можно также отметить голосовой мониторинг, функцию «Гео-зон», встроенный дата-логгер (запись пройденного пути). Односторонняя бесшумная связь позволяет узнать, что происходит вокруг. Функция «Гео-зон» (GeoFence) позволяет задавать разрешённые или запрещённые зоны. При пересечении границ этих зон прибор рассылает БМБ — уведомления.

Трекер легко настраивается дистанционно либо при помощи USB-соединения.

GlobalSatTR-206 — компактное устройство для удалённого позиционирования с встроенными модулями GPS и GSM. У трекера имеются LCD-

дисплей, телефонная книга на 20 номеров, функции быстрого набора на четыре клавиши, восемь мелодий вызова.

Текущие координаты передаются через SMS на мобильные телефоны либо на персональный компьютер по сети «Интернет» посредством GPRS.

Технология интеграции трекеров в состав Приток-МПО отработана, следовательно, подключение других трекеров для работы в составе Приток-МПО будет производиться в кратчайшие сроки.

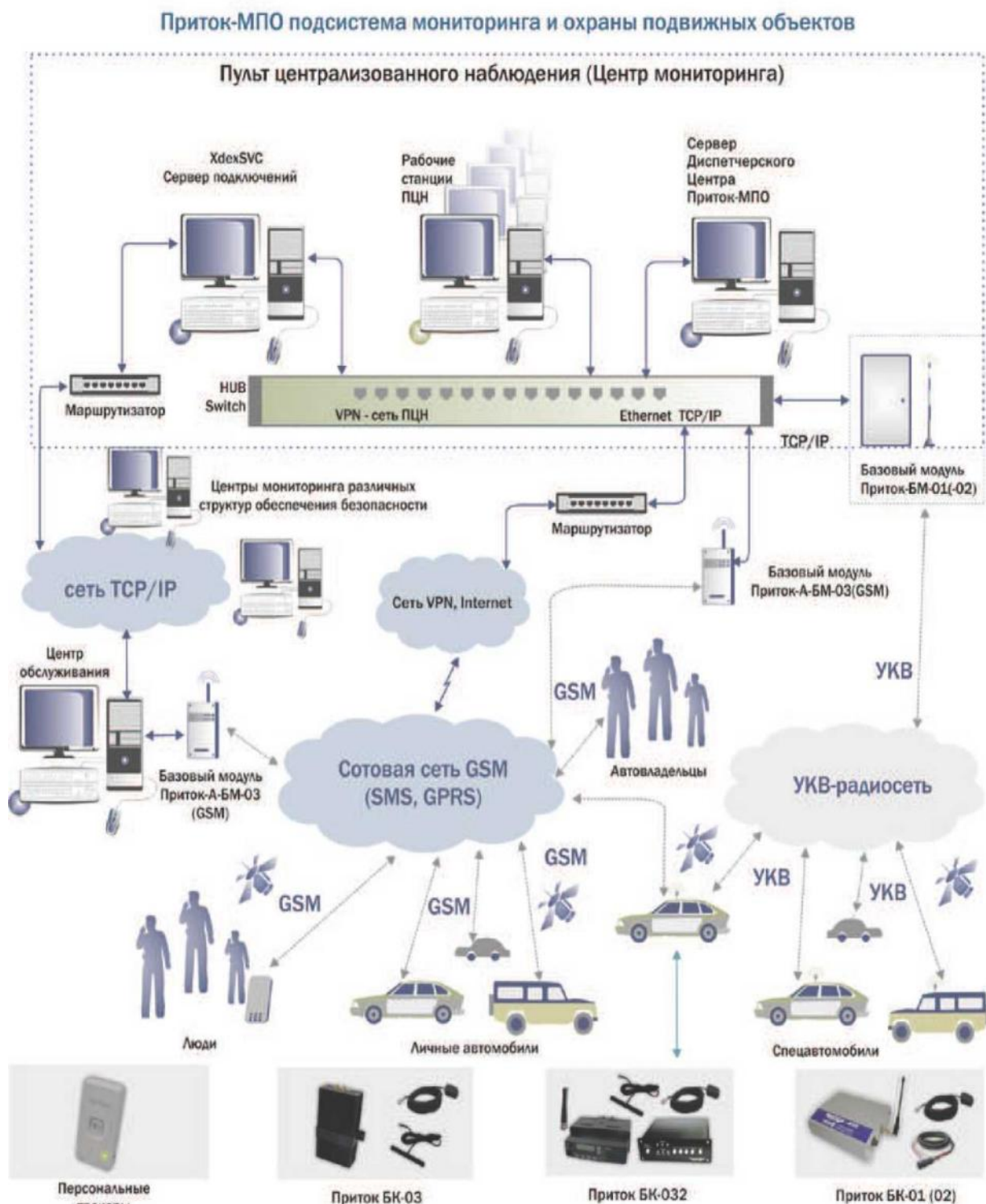


Рисунок 18

Работа «Приток-МПО» в составе ИС «Приток-А» позволяет организовывать несколько центров мониторинга, в том числе и работающих через web-узлы. АРМы ПЦН, входящие в состав одной системы, позволяют объединить работу различных подразделений МВД и МЧС, а также частных охранных предприятий. Возможность одновременного отображения на карте местности стационарных и подвижных объектов, находящихся в тревоге, местоположения людей, оперативной информации о состоянии контролируемых (охраняемых) объектов, а также местоположения экипажей (групп) реагирования, позволяет оптимизировать управление экипажами (группами) реагирования.

«Приток-Автоприбытие» существенное дополнение в «Приток-МПО».

В оперативной работе подразделений вневедомственной охраны может быть обозначена следующая проблема. Дежурный пульта централизованного наблюдения (ПЦН) держит связь с группами реагирования (в дальнейшем — с группами задержания) по радиоканалу в открытом эфире. В такой ситуации допускается вероятность того, что злоумышленник имеет возможность прослушать их диалог в эфире, используя радиостанцию. При этом злоумышленник может узнать секретные данные по охраняемому объекту, а также маршрут движения ГЗ.

Назначение, задача.

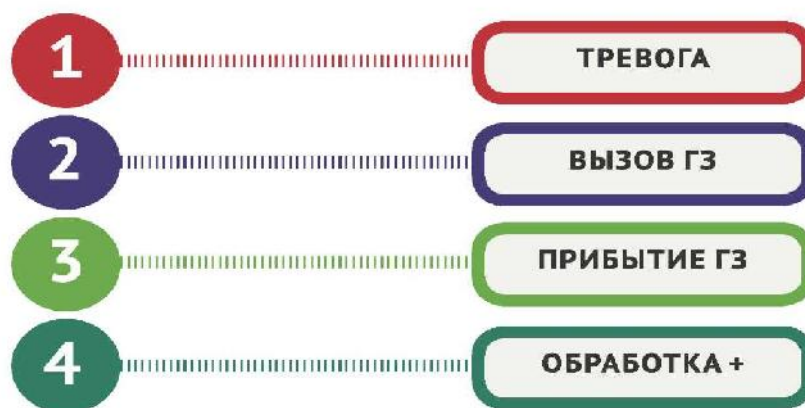


Рисунок 19

Итак, разобьём весь процесс действий дежурных пульта и экипажей ГЗ во время возникновения тревожной ситуации на четыре фазы:

Для каждой фазы дежурному и экипажу необходимо иметь информацию и решать свои основные задачи:

Для дежурного пульта:

Фаза 1. Определять ближайшую к месту тревоги либо менее занятую ГЗ в момент возникновения тревоги.

Фаза 2. Сообщить конкретной ГЗ сведения о тревоге и передать характеристики тревожного объекта, не используя открытый радиоэфир.

Фаза 3. Зафиксировать в автоматическом либо полуавтоматическом режиме фактическое прибытие ГЗ на место тревоги.

Фаза 4. Зафиксировать в полуавтоматическом либо ручном режиме факт тревоги, причину тревоги, состояние объекта и принимаемое решение.

Для экипажа ГЗ:

Фаза 1. Иметь оперативный список тревог, назначенных для обработки данной ГЗ.

Фаза 2. Иметь возможность подтвердить ДПЦН, что сведения для обработки новой тревоги получены.

Фаза 3. По карте видеть своё местоположение на местности и видеть маршрут движения до места тревоги.

Фаза 4. Дополнительно получать в автоматическом режиме данные по тревожному объекту.

Наряду с поставленными задачами необходимо:

1. ДПЦН необходимо в любой момент времени видеть все назначенные тревоги для каждой ГЗ и для всех ГЗ одновременно и знать общее количество тревог, находящихся в обработке.

2. ДПЦН должен иметь возможность видеть на карте местоположение ГЗ, место тревожного объекта, программный статус ГЗ. Статус ГЗ формируется из справочника одним кликом мыши: «обрабатывает особо важную тревогу, на обеде, ТО, сломался и т. д.».

И ДПЦН и экипажи ГЗ должны максимально использовать возможности программно-аппаратных средств, имеющихся в системе «Приток-А» на ПЦН и на борту ГЗ. При этом надо обязательно учесть, что на транспортных средствах, кроме Р/ст, может быть установлено или не установлено навигационное оборудование «Приток-МПО».

Таких вариантов может быть много:

1. ТС не оборудовано бортовым комплектом (БК) «Приток-МПО».

2. ТС не оборудовано БК «Приток-МПО», но у экипажа есть сотовый телефон.

3. ТС оборудовано БК «Приток-МПО».

4. ТС оборудовано БК, и у экипажа есть сотовый телефон.

5. ТС оборудовано БК, и установлен бортовой компьютер (наладонный коммуникатор, планшетный ПК).

6. В ТС установлен бортовой компьютер (наладонный коммуникатор, планшетный ПК с навигационной системой ГЛОНАСС/GPS).

Также имеются и варианты использования на ПЦН ПО:

1. Используется ПО только АРМ ДПЦН.
2. Используется ПО только АРМ «Приток-МПО».
3. Используется ПО и АРМ ДПЦО и АРМ «Приток-МПО».

Исходя из вышеперечисленных требований, специалистами ОБ «СОКРАТ», была произведена доработка программного обеспечения АРМ ДПЦН, АРМ «Приток-МПО», решена задача создания подсистемы «Приток-Автоприбытие».

Для этапа «Вызов ГЗ» в АРМ ДПЦО произведено следующее:

1. Изменена закладка «Действия».
2. Создано новое плавающее окно Группы задержания.
3. Создан новый справочник «Статус ГЗ». Вид новой закладки Действия и плавающего окна Группы задержания приведены ниже.
4. В новой закладке теперь стало видно расстояние до тревожного (активного) объекта и количество назначенных тревог.
5. После назначения ГЗ для обработки возникшей тревоги в окне будет указано текущее расстояние до каждого тревожного объекта.
6. Красным цветом в списке выделены тревоги, по которым от ГЗ пока еще не пришло подтверждение о получении задания.
7. Видно состояние пульта, который имеется у экипажа, и статус, который определил ДПЦН для данной ГЗ.
8. При выборе в этом окне строки с информацией о какой-то тревоге, в главном окне АРМ ДПЦН открывается карточка этого тревожного объекта.

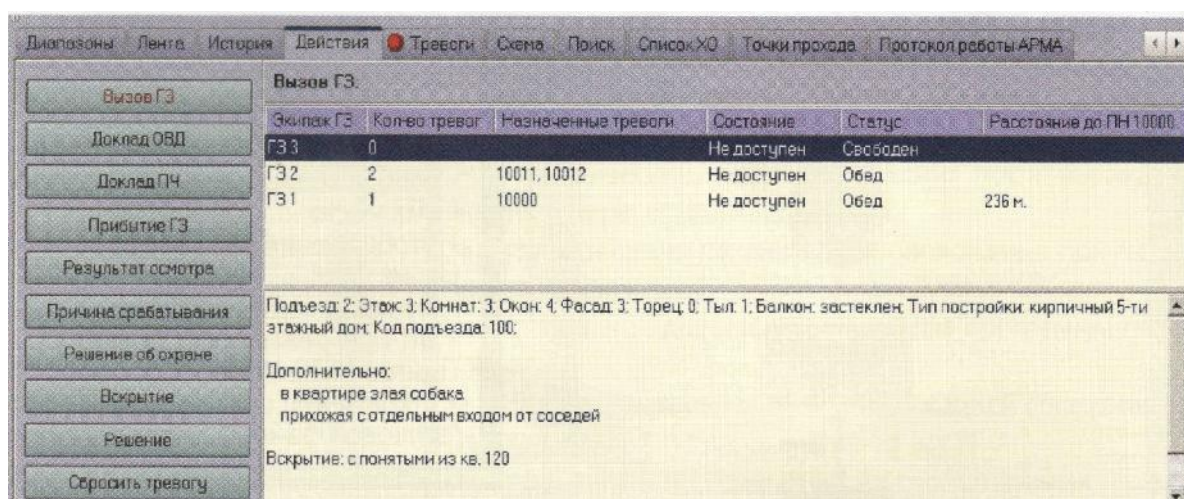


Рисунок 20

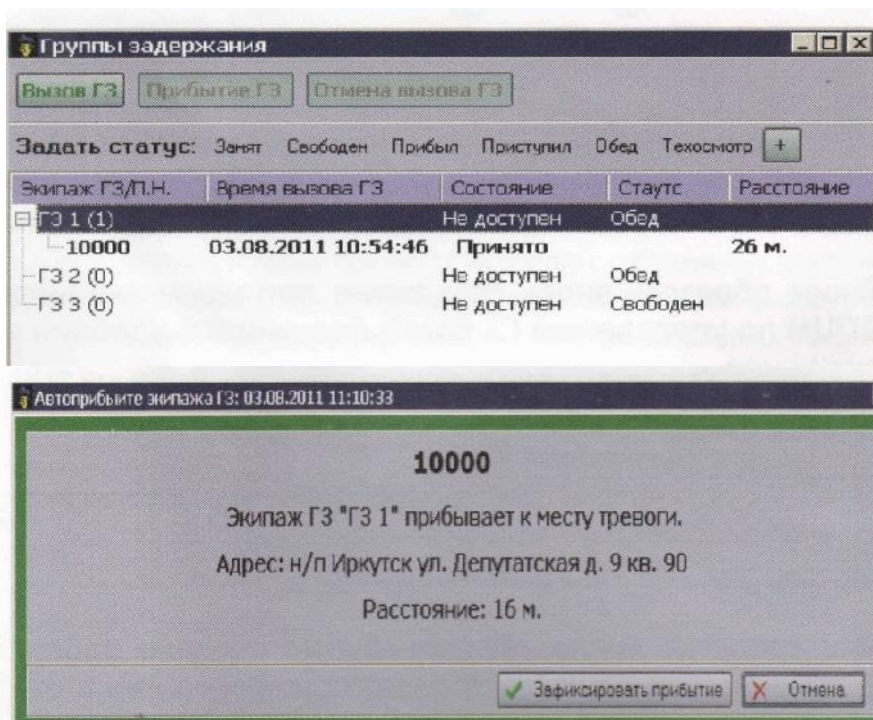


Рисунок 21

Программа «Экипаж».

«Экипаж» — приложение для ОС Android, которое входит в состав подсистемы «Приток-Автоприбытие». Программа устанавливается и выполняется на специализированном планшетном компьютере, используемом в группе задержания.

Программа «Экипаж» позволяет сотрудникам группы задержания оперативно получать, подтверждать и обрабатывать отправляемую дежурным ПЦН информацию, касающуюся тревожного объекта. При этом адрес, характеристика и другая информация не передаётся голосом в радиоэфире. Для передачи данных используются каналы связи GSM(GPRS)/3G.

Интерфейс программы позволяет:

1. Отображать на карте расположение тревожного объекта, получать информацию о возникновении тревоги (дата и время) и о тревожном объекте (адрес, характеристика, маршрут движения, схема проезда и т. д.).
2. Подтвердить факт получения тревожного сообщения, для этого оператору в ГЗ достаточно прикоснуться пальцем (или специальным стержнем) к транспаранту Тревоги.
3. Отображать на карте местоположение ГЗ относительно тревожного объекта.

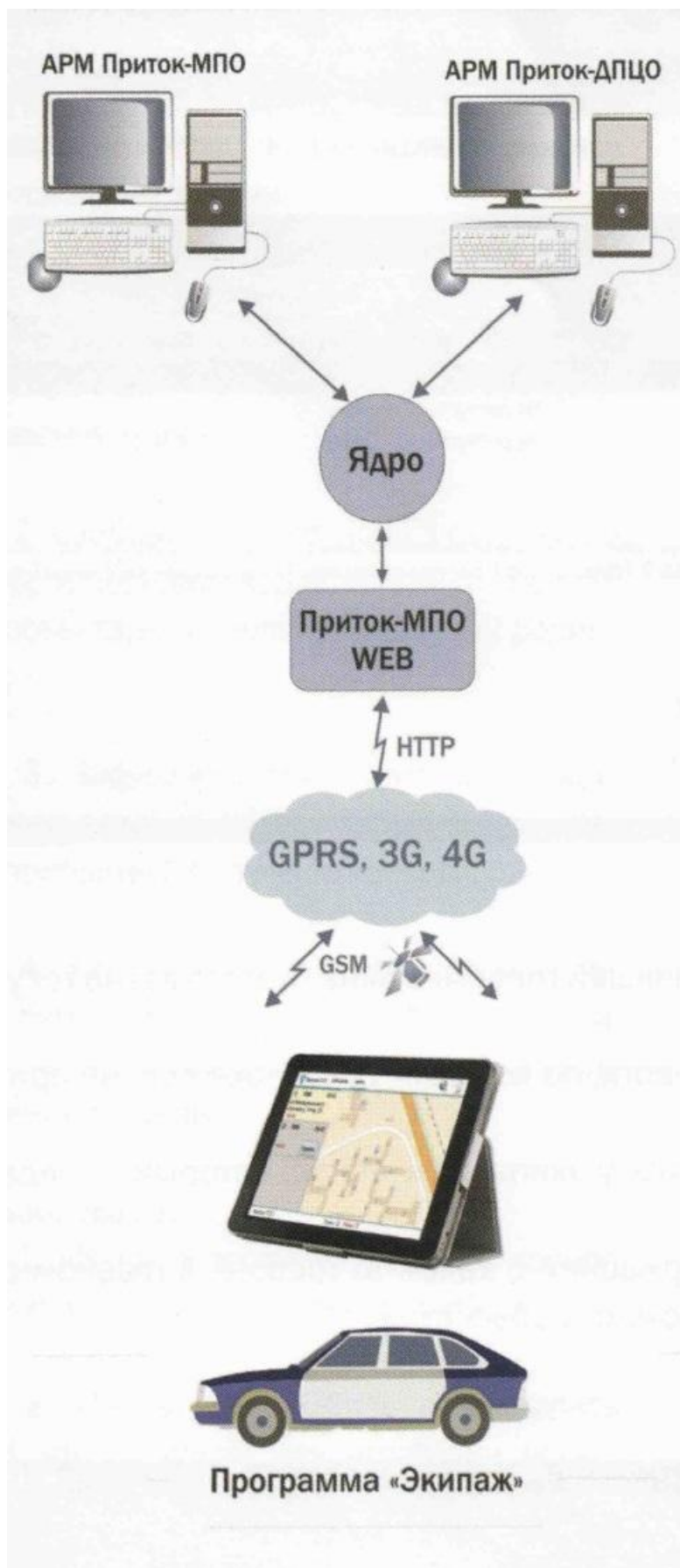


Рисунок 22

Основные функции программы:

- отображение списка назначенных для ГЗ тревог, их количества и количества новых;
- вибрация и проигрывание звука при получении новой тревоги и при отмене;
- отображение детальной информации по тревоге, выбранной в списке тревог;
- отображение таймера по каждой тревоге с момента вызова ГЗ до прибытия ГЗ на место;
- отображение истории работы по тревоге и истории работы ГЗ по всем тревогам;
- функция подтверждения факта получения новой тревоги;
- off-line режим работы с программой при разрыве соединения с сервером Приток-МПО-WEB;
- отключение спящего режима устройства при работе с программой «звуковой файл назначается пользователем программы «Экипаж».

Принцип работы.

После установления соединения с сервером «Приток-МПО-WEB» программа «Экипаж» автоматически запрашивает список тревог, назначенный дежурным ПЦН для данной ГЗ.

В ходе своей работы программа периодически опрашивает сервер на предмет обновления списка тревог, которые отображаются в главном окне программы.

После отображения новой тревоги на планшете сотрудник группы задержания должен подтвердить её получение. Факт подтверждения тревоги фиксируется в истории по тревоге в программе «Экипаж» и в истории по объекту в АРМ ДПЦО.

После подтверждения тревоги оператор программы «Экипаж» просматривает детальную информацию по тревожному объекту и осуществляет выезд по указанному адресу.

По факту прибытия ГЗ на место дежурный ПЦН фиксирует в АРМ ДПЦО событие «Прибытие ГЗ». ГЗ осматривает объект и докладывает о результате осмотра. Дежурный ПЦН фиксирует событие «Результат осмотра» и «Причина срабатывания». Все события фиксируются в истории по тревоге в программе «Экипаж».

Отработанная тревога заносится в историю тревог программы «Экипаж». История тревог может быть в любой момент просмотрена в отдельном окне программы.

Таким образом, вновь созданные программно-аппаратные средства «Приток-Автоприбытие» сделали работу ДПЦН по управлению ГЗ более надежной и удобной и исключили возможность перехвата информации в радиозфире.

Программа «Трекер Приток-А».

«Трекер Приток-А» — приложение для ОС Android со стандартными функциями программного GPS/ГЛОНАСС трекера.

Программа «Трекер Приток-А» позволяет контролировать передвижение сотрудников, клиентов, детей и близких, используя телефон (планшет) со встроенным GPS/ГЛОНАСС приёмником.

Работая в фоновом режиме, приложение передаёт данные с координатами на сервер центра мониторинга в постоянном либо периодическом режиме, используя любое доступное интернет-соединение (GPRS, 3G, 4G, WiFi).

Интерфейс программы позволяет:

1. Просматривать текущие координаты местоположения, полученные со встроенного GPS/ГЛОНАСС приёмника (даже в автономном режиме без отправки координат на сервер).
2. Гибко настраивать параметры отправки координат на сервер: по времени, по пройденному расстоянию, при изменении угла направления.
3. Нажать тревожную кнопку в случае возникновения нештатной ситуации, с передачей сигнала в мониторинговый центр.
4. Запускать приложение автоматически при старте телефона, планшетного компьютера.

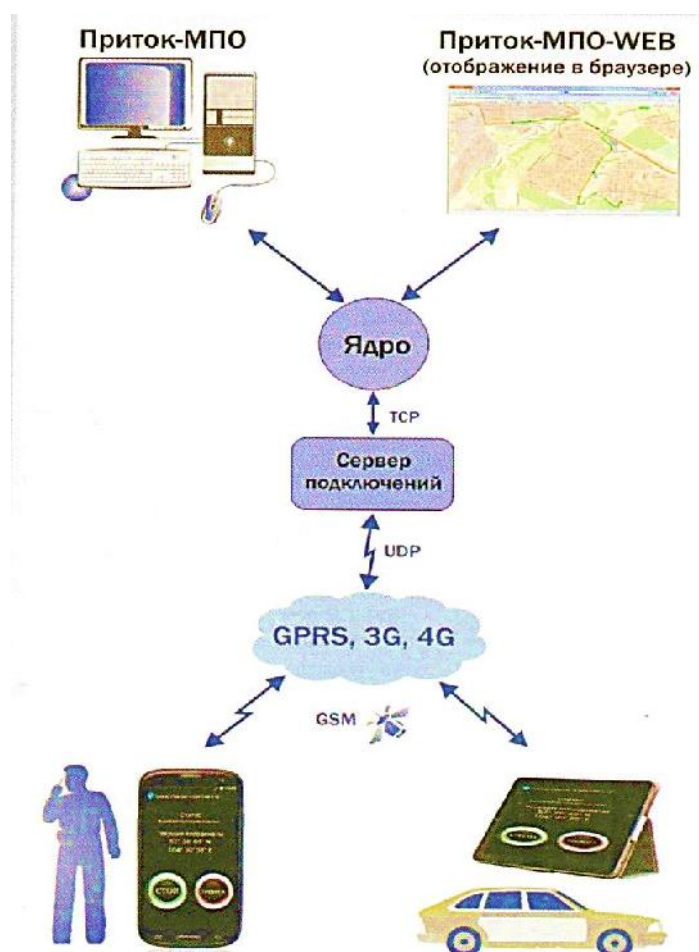


Рисунок 23

Основные возможности.

Основные функции трекера:

- отправка координат текущего местоположения, скорости движения и угла направления по сигналам встроенного GPS/ГЛОНАСС приёмника;
- настройка параметров отправки данных на сервер по времени, пройденному расстоянию, углу поворота;
- автоматический запуск приложения после выключения и перезагрузки телефона;
- автоматическая отправка местоположения при запуске приложения;
- ограничение доступа к настройкам программы по паролю;
- работа в фоновом режиме с индикацией состояния программы;
- шифрование передаваемых на сервер данных.

5. Основные направления и перспективы развития технических средств безопасности ОВД

Российский рынок представлен широким спектром отечественных и зарубежных технических средств охраны, позволяющих закрыть практически все ниши в сфере охранной деятельности. Однако постоянный мониторинг российского рынка, проводимый вневедомственной охраной, как крупнейшим поставщиком охранных услуг в России, показывает, что не все технические средства, в особенности импортные, действительно применимы у нас в стране и могут обеспечить высокую надёжность охраны объектов. Поэтому вневедомственная охрана на конкурсной основе отбирает для своих целей наилучшие по стоимостным и техническим показателям изделия с целью последующего их внедрения в практическую деятельность наших подразделений [13].

Претворение в жизнь единой технической политики, направленной на обеспечение безопасности и надёжной охраны объектов, НИЦ «Охрана» осуществляет по двум скоординированным и взаимосвязанным магистральным направлениям своей научно-исследовательской деятельности.

1. Создание и перевооружение службы вневедомственной охраны техническими средствами безопасности нового поколения.

2. Организационно-техническое и методологическое обеспечение подразделений вневедомственной охраны в работах по внедрению и эксплуатации технических средств.

Важнейшими, основополагающими документами, определяющими работу по первому направлению, являются «Единые технические требования к объектовым подсистемам технических средств охраны, предназначенным для применения в подразделениях вневедомственной охраны» и «Единые технические требования к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны». Представленные в них требования задают тот технический уровень, которому должны удовлетворять изделия для применения во вневедомственной охране [14].

Они обеспечивают надёжную защиту объектов и квартир, позволяют исключить возможность использования недоброкачественной техники и частично сократить затраты на охрану.

Эти требования не носят застывший характер, в них вносятся коррективы, диктуемые научно-техническим прогрессом и новыми задачами по обеспечению безопасности. Наряду с этим публичное издание данных документов позволяет избежать преференций в отношении того или иного производителя и ставит их всех в одинаковые условия.

Выходу в свет «Единых требований...» предшествовал переход НИЦ «Охрана» на принципиально новую позицию в создании охранной техники. Она заключается в проведении разработок ТСО совместно с ведущими отечественными производителями путём объединения их значительных возможностей в создании и производстве аппаратуры нового поколения с научным потенциалом и большим опытом работы НИЦ «Охрана».

Если прежде НИЦ «Охрана» осуществлял разработку приборов самостоятельно, без привлечения сторонних организаций, то с образованием и развитием новых коллективов, которые стали занимать ведущее положение на рынке технических средств безопасности, появилась реальная возможность интеграции усилий. Это позволило существенно расширить фронт работ по созданию аппаратуры, повысить технический уровень разработок, сократить время на подготовку их серийного производства, что в конечном итоге дало возможность ежегодно пополнять арсенал вневедомственной охраны 12—15 новыми изделиями, а не тремя-четырьмя, как было при прежнем подходе [15].

Сегодня тесное взаимодействие по созданию новых ТСО осуществляется более чем с 50 предприятиями-изготовителями Москвы, Санкт-Петербурга, Казани, Рязани, Иркутска и других промышленных центров страны, а также Московской и Челябинской областей. Ежегодный объём выпуска составляет более ста тысяч единиц продукции, что обеспечивает устойчивую производственную загрузку десяткам и сотням рабочих мест российских предприятий. Причём в этих творческих альянсах НИЦ «Охрана» выполняет

функции идеолога, головного разработчика, который определяет ключевые технические характеристики нового изделия, тактику применения и другие жизненно важные показатели [15].

Рассмотрим подробно задачи, решаемые НИЦ «Охрана» в рамках каждого из направлений своей деятельности.

Первой из таких задач является минимизация возможности «квалифицированного» обхода аппаратуры существующей охранной сигнализации.

На основе проведённого специалистами Центра системного анализа причин допущенных краж были выработаны технические решения и выполнены необходимые работы по усовершенствованию применяемых во вневедомственной охране систем централизованного наблюдения «Альтаир», «Атлас-20», «Ахтуба», «Заря», «Приток-А», «Юпитер» в части повышения их имитостойкости и крипто-защиты, которые обеспечивают устойчивость к несанкционированному доступу и исключают возможность «квалифицированного» обхода. Например, оборудование ИС «Приток-А» работает, используя алгоритм шифрования AES 128.

Вторая задача в направлении технического перевооружения подразделений — это повышение информативности СЦН, т. е. увеличение количества информации, поступающей с объекта. Её решение позволяет оптимизировать действия групп задержания за счёт постоянного мониторинга поведения преступника на объекте или развития других негативных ситуаций, что напрямую влияет на оперативность принятия обоснованных решений, грамотное распределение сил и средств.

Для повышения результативности несения службы нарядами групп задержаний проведены работы по введению полной автоматизации контроля прибытия нарядов полиции на объект по сигналу «Тревога». В настоящее время во все СЦН введена функция «Контроль наряда», а также внесены соответствующие дополнительные требования в «Единые требования к системам централизованного наблюдения...».

Важным аспектом является и защита передаваемой группам задержания информации об охраняемых объектах при обработке сигналов «Тревога». Актуальность скрытного целеуказания ГЗ подтверждена многократными случаями прослушивания частот полиции криминальными элементами, что затрудняет эффективное пресечение их противоправных действий.

Так, в составе системы «Приток-А» имеются подсистемы «Автоприбытие» и «Мониторинг подвижных объектов (МПО)», которые обеспечивают передачу информации (в цифровом зашифрованном виде) о тревожном объекте по каналам сотовой связи (GPRS/3G) на бортовой компьютер (смартфон, планшет) группы задержания и автоматическое фиксирование прибытия ГЗ к тревожному объекту.

Внедрение данной возможности позволяет отказаться от голосовой передачи информации в открытом радиоэфире и наиболее полно задействовать все возможности системы «Приток-А». Такая интеграция подсистем охраны, мониторинга служебного автотранспорта, охраны личных автомобилей позволяет на новом качественном уровне организовать работу по охране объектов.

Третья задача — это организация охраны объектов по альтернативным каналам передачи информации, а именно по цифровым каналам Ethernet (TCP/IP), каналам операторов сотовой связи (GSM-канал), а также информаторным каналам (автодозвон).

Эта задача связана прежде всего с монопольным положением на отечественном рынке предприятий связи, по линиям которых осуществляется в настоящее время охрана абсолютного большинства объектов, а также необходимостью обеспечения охраны объектов, не имеющих стационарных линий телефонной связи.

В настоящее время в крупных городах России операторами телефонной связи проводится переключение абонентов с медных телефонных линий на оптоволоконные цифровые каналы связи (так называемые PON-технологии). Это потребовало пересмотра технических решений в части организации централизованной охраны. А именно — все названные выше системы, находящиеся в эксплуатации, были доработаны в части создания принципиально нового объектового оборудования, передающего информацию с объектов и квартир непосредственно на ПЦО.

Например, «Приток-РКС» (резервный канал связи) применяется для подключения существующих объектов охраны (которые использовали стационарные телефонные линии связи или радиоканал) по новым альтернативным каналам связи — цифровым каналам TCP/IP и каналам связи сотовых операторов GPRS/GSM. «Приток-РКС» может использоваться как во вновь устанавливаемом оборудовании, так и для резервирования или обеспечения работоспособности приборов, которые уже были установлены на объектах охраны.

Такой подход предусматривает исключение ретрансляционного оборудования, которое устанавливалось на АТС, что, в свою очередь, должно привести к снижению затрат как на аппаратуру СЦН в целом, так и на услуги операторов связи.

Апробация ряда данных технических решений уже проведена в УВО Санкт-Петербурга, Ставропольского края, Иркутской и ряда других областей.

В столичном регионе, где массовое переключение абонентов запланировано на самое ближайшее время, организована пилотная зона для детальной проработки вариантов организации централизованной охраны с исполь-

зованием различных цифровых каналов передачи информации с объекта непосредственно на ПЦО с учётом обеспечения требуемого уровня надёжности охраны. А именно — использование в качестве каналов передачи данных:

- построенной для нужд охраны VPN-сети, арендуемой у поставщика услуг связи;

- собственной корпоративной VPN-сети, построенной за счёт средств охраны;

- открытых каналов сети «Интернет».

Каждый из указанных вариантов имеет свои преимущества и недостатки по затратам на осуществление охраны, по обеспечению необходимых надёжностных характеристик и т. п. Однако, учитывая, что в ближайшем будущем именно цифровые каналы передачи данных будут занимать доминирующее положение, детальная проработка и апробация всех вышеуказанных вариантов является для ОБ «СОКРАТ» весьма актуальной и приоритетной задачей.

Приборы «Приток-А-КОП» предназначены для работы через подобные сети. Вне зависимости от построения сети передачи данных VPN, открытый канал Internet или собственные корпоративные сети — «Приток-А-КОП» передаёт на ПЦО данные, используя несколько точек подключения, реализовав тем самым все возможные варианты.

Ещё одной важной задачей совершенствования деятельности ПЦО, сокращения задействованной численности личного состава, обеспечения сохранности охраняемого имущества и безопасности клиентов является объединение (укрупнение) ПЦО, действующих в пределах одного населённого пункта, создание на их базе многофункциональных мониторинговых центров.

Вместе с тем решение задачи укрупнения ПЦО невозможно без выработки дополнительных критериев, позволяющих оптимизировать временные, материальные и организационные затраты.

Важнейшим условием минимизации затрат на переоснащение подразделений является принцип преемственности и совместимости со старым оборудованием.

В противном случае на ПЦО в дополнение к имеющимся рабочим местам придётся разворачивать новые. А это приведёт к необходимости увеличивать численность персонала ПЦО, изыскивать дополнительные площади, расширять парк компьютерной техники и т. д. При этом этап перехода на новую технику будет растянут на несколько лет, в течение которых ни о каких экономических преимуществах говорить не придётся.

Отсюда следует, что вновь вводимые в эксплуатацию СПИ должны обеспечивать возможность плавного и поэтапного внедрения с обеспече-

нием поддержки как старого ретрансляционного оборудования (для СПИ, не выработавших установленных сроков службы «Фобос», «Фобос-А», «Фобос-ТР», «Фобос-З»), так и с обеспечением поддержки старого объектового оборудования со стороны новых ретрансляторов (поскольку замена объектового оборудования требует значительного времени, в том числе на работу с клиентами, которых необходимо будет убеждать на приобретение новой техники).

Для этих целей в ОБ «СОКРАТ» был внедрён в эксплуатацию комплект модернизации ретрансляторов «Фобос». Он позволяет модернизировать существующие ретрансляторы СПИ «Фобос-З», исключив расходы на демонтаж, монтаж нового оборудования, смену кабельных подключений и т. п. Обновлённый ретранслятор обеспечивает поддержку уже подключённых УО и позволяет подключать новые современные приборы охраны.

Следующим критерием оценки является возможность работы системы на участках АТС-АТС и АТС-ПЦО по цифровым каналам связи, поскольку в случае объединения далеко расположенных друг от друга ПЦО, прямые провода использовать не представляется возможным. Кроме того, современные технологии связи вообще не предполагают наличия медных выделенных линий на межстанционных соединениях.

Применяя Коммуникаторы ТСР ИС «Приток-А», мы можем через цифровые каналы связи передать извещения от широкого спектра поддерживаемого оборудования вне зависимости от расстояния. В «Коммуникаторе ТСР» для загрузки доступно более десятка различных программ — физически один коммуникатор может быть настроен на любой тип оборудования только перепрограммированием параметров.

И, наконец, необходима возможность управления любым охраняемым объектом с любого рабочего места (т. е. возможность динамически менять нагрузку на одного оператора) в масштабах данного ПЦО, поскольку это даёт возможность произвести сокращение оперативного персонала и равномерно распределить потоки информации пропорционально количеству работающих сотрудников. ПО ИС «Приток-А» позволяет гибко распределить права персонала по доступу к различным функциям системы, АРМам и распределить между операторами любое работающее оборудование.

Кроме того, желательно предусмотреть возможность в рамках одной системы передачи извещений на ПЦО дополнительно принимать сообщения от СПИ, работающих без использования станционного оборудования (автодозвон, радиоканал и т. д.).

На основе проведённого анализа с экономической и технической точек зрения наиболее эффективно решение задачи по объединению ПЦО возможно с использованием систем «Приток» и «Атлас-20».

Кроме того, дальнейшее решение данной задачи лежит в унификации внедряемых новых и эксплуатируемых аппаратных и программных средств.

В целях унификации программного обеспечения систем передачи извещений разработаны «Единые тактико-технические требования к программному обеспечению АРМ СПИ, применяемых в подразделениях вневедомственной охраны». Документ содержит перечень обязательных требований, которые необходимо будет учитывать при разработке, модернизации и серийном выпуске АРМ СПИ [14].

В продолжение данной темы в текущем году ведётся работа по созданию программно-аппаратной платформы ПЦО, позволяющей в едином формате отображать информацию о состоянии охраняемых объектов, а также поддерживать работу с объектовым и ретрансляционным оборудованием различных СПИ, использующихся в подразделениях вневедомственной охраны.

Объектовые средства и подсистемы охраны включают в себя большой круг технических средств, устанавливаемых на охраняемом объекте. Это средства обнаружения проникновения, оповещатели, источники электропитания, приборы приёмно-контрольные, средства контроля доступа и телевизионного наблюдения.

При этом, учитывая, что одной из приоритетных задач, решаемых вневедомственной охраной, является защита критически важных объектов, основной упор в деятельности НИЦ сделан на решение проблем, связанных с организацией охраны объектов именно этой категории. Речь идёт прежде всего о протяжённых объектах топливно-энергетического комплекса, аэропортах со сложной конфигурацией периметра и тяжёлой помеховой обстановкой, объектах кредитно-финансовой системы, культурного наследия и ряда других, перечень которых определён распоряжением Правительства Российской Федерации от 2.11.2009 № 1629р.

Отечественная и зарубежная практика показывает, что наиболее перспективным и общепризнанным путём организации их защиты является применение интегрированных систем безопасности (ИСБ), которые, как правило, включают подсистемы:

- автоматизированной охранной сигнализации;
- автоматизированной пожарной сигнализации;
- контроля доступа;
- видеонаблюдения и охранного телевидения.

Оснащение критически важных объектов интегрированными системами позволяет существенно поднять уровень их безопасности и обеспечить защиту не только от несанкционированного проникновения (криминальные и террористические угрозы), пожарной опасности, но и расширить возможности по защите от других видов угроз (аварии оборудования, природные факторы и др.).

Кроме этого ИСБ позволяют оптимальным образом сократить людские и материальные ресурсы, а также финансовые затраты (в том числе бюджетные) на оборудование объектов, эксплуатацию аппаратуры и содержание охранников [11].

Некоторые системы охраны (например, «Приток») изначально развивались и реализовывались как интегрированные системы, включающие в себя весь комплекс подсистем охраны, мониторинга, контроля доступа, видеонаблюдения, радиолокационного обнаружения, регистрации переговоров и пр.

Ряд проводимых НИР направлены на совершенствование защиты объектов посредством систем охранного телевидения.

Так, в целях повышения эффективности существующих систем охранного телевидения организованы работы, направленные на изучение возможности применения современных алгоритмов анализа видеоизображений, а также получение объективной оценки представленных на российском рынке систем интеллектуальной видеоаналитики, которые позволяют обеспечить возможность автоматизированного выявления потенциальных угроз различного вида, в том числе в местах массового скопления людей. Результаты работы будут использованы при создании ведомственных нормативных документов по совершенствованию систем охранного телевидения, применяемых во вневедомственной охране [16].

Ещё одной назревшей проблемой является обеспечение комплексной защиты банковского оборудования от хищения денежных средств. По данным МВД России, ЦБ РФ и крупнейших банков страны, отмечен устойчивый рост краж денежных средств из банкоматов и терминалов, число которых достигает сотен тысяч. Для её решения Центром разработан новый извещатель «Шорох-3», позволяющий обнаруживать различные криминальные воздействия на банкоматы, а именно попытки взлома, перемещения и др.

В развитие данной темы проводятся работы по исследованию возможности создания комплекса технических средств для охраны банкоматов и платёжных терминалов от преступных посягательств. Создаваемый комплекс будет включать в себя необходимый набор охранных извещателей, системы передачи извещений по различным каналам связи, техниче-

ские средства и системы отслеживания текущего местоположения банкоматов с передачей информации на ПЦО и экипажам группы немедленного реагирования, средства активного противодействия преступным посягательствам на банкоматы.

Второе магистральное направление — организационно-техническое и методологическое обеспечение подразделений вневедомственной охраны в работах по внедрению и эксплуатации технических средств.

Многолетний опыт совместной работы НИЦ «Охрана» со службой вневедомственной охраны говорит о том, что недостаточно разработать совершенные по своим техническим характеристикам устройства. Для эффективной реализации всех возможностей приборов необходимо ещё надлежащим образом обеспечить полноценную поддержку для их правильного выбора при проведении монтажных работ и эксплуатационного обслуживания, что и реализуется в рамках данного направления.

В условиях сокращения в ходе реформирования МВД России инженерно-технического состава вневедомственной охраны, подразделения столкнулись с проблемой дефицита доходчивых и простых в применении методических и практических рекомендаций и пособий, которые, по существу, могли бы служить инструментом для достижения максимального результата меньшим числом сотрудников.

В связи с этим работа по данному направлению в последние годы значительно активизировалась. В частности, увеличено число работ по созданию нормативно-технических документов.

Качественно изменился и состав рассматриваемых вопросов, которые относятся не только к выбору и применению технических средств, как было прежде, но и в большой степени затрагивают различные каждодневные организационные стороны деятельности подразделений.

Говоря о направлении методологического обеспечения вневедомственной охраны, нельзя не остановиться на работе НИЦ «Охрана» в рамках Технического комитета по стандартизации ТК 234 «Системы тревожной сигнализации и противокриминальной защиты» Федерального агентства по техническому регулированию и метрологии.

Важность этой работы заключается в том, что она позволяет НИЦ «Охрана», как базовому органу ТК 234, определять в ГОСТах требования к техническим средствам безопасности с учётом специфики их применения, что препятствует наполнению российского рынка некачественной, порой морально устаревшей импортной и отечественной продукцией и способствует оснащению объектов, охраняемых ОВО, современными техническими средствами, полностью соответствующими специфике решаемых вневедомственной охраной задач.

Более того, данная работа приобрела ещё большую значимость при состоявшемся вступлении России во Всемирную торговую организацию. В условиях членства в ВТО складывается положение, при котором отсутствие своих национальных стандартов будет компенсировано действием международных стандартов, что представляет реальную угрозу широкого, ничем не сдерживаемого проникновения импортной продукции на наш рынок технических средств безопасности. А это касается не только технического уровня и качества изделий, но сохранения рабочих мест на российских предприятиях.

При этом, как показывает практика участия наших специалистов в заседаниях рабочих групп Международной электротехнической комиссии (МЭК ТК 79) по разработке международных стандартов, ряд государств весьма активно лоббируют исключительно свои интересы, занижая требования к продукции в разрабатываемых международных стандартах с целью удешевления своих товаров и, соответственно, более активному их продвижению на международный рынок.

Барьером может служить, с одной стороны, разработанная с учётом требований международных стандартов стройная система национальной стандартизации России в данной области, а с другой — активное участие наших специалистов в разработке международных стандартов с учётом их гармонизации с национальными.

Объективно оценивая такое положение дел, только за последние два года на основе Программы национальной стандартизации Российской Федерации НИЦ «Охрана» в рамках ТК 234 разработаны и утверждены Росстандартом пять национальных стандартов.

В заключение можно отметить, что успешной реализации указанных приоритетных направлений научно-исследовательской деятельности НИЦ «Охрана» способствуют, с одной стороны, тесное взаимодействие с ДГЗИ МВД России, как с основным заказчиком научно-технической продукции, а с другой — постоянная обратная связь с подразделениями на этапах испытаний и освоения новой техники, при подготовке нормативно-технических документов.

ЗАКЛЮЧЕНИЕ

Любой регион нашей страны имеет свои черты, особенности и преимущества, которые становятся его визитной карточкой.

В Иркутске создано и действует предприятие, которое вполне заслуженно может считаться гордостью региона. Два десятилетия назад иркутские инженеры-электронщики и программисты разработали систему, которой в течение ряда лет в России не было даже аналогов. Эта система, получившая название «Приток», сказала совершенно новое слово в охране имущества граждан. В 90-е годы она перевернула представление российских органов внутренних дел о том, как можно обеспечивать безопасность и управлять ею.

Сегодня система «Приток» эксплуатируется более чем в 350 городах России. Число квартир жителей разных регионов нашей страны, которые она охраняет, приближается сейчас к миллиону, среди них и квартиры тысяч иркутян. Под охраной «Притока» сотни российских предприятий, в нашем регионе это гидроэлектростанции и другие объекты «Иркутскэнерго», Иркутский алюминиевый завод, корпорация «Иркут» (Иркутский авиационный завод), Ангарская нефтехимическая компания и многие другие [10].

Систему используют более 500 подразделений вневедомственной охраны России. А подразделения вневедомственной охраны ГУВО ФСВНГ России являются основными потребителями иркутской охранно-пожарной системы. И неслучайно под присмотром «Притока» даже здание Государственной думы Российской Федерации.

Оборудование и программное обеспечение интегрированной системы охранно-пожарной сигнализации «Приток-А» включено в список технических средств охраны, соответствующий требованиям МВД РФ.

Благодаря своей универсальности и уникальной возможности оперативно адаптироваться к самым свежим разработкам мировой научной мысли, «Приток» опередил многие аналогичные проекты из других городов России.

Одним из главных преимуществ системы иркутского производства, по отношению к другим аналогичным разработкам, стала идея, заложенная ещё на стадии проектирования. «Приток» должен интегрировать в себя всё то, что эксплуатировалось в подразделениях вневедомственной охраны и других подобных структурах, и развиваться независимо от того, какие технологии передачи информации в данный момент используются.

Благодаря своей универсальности и уникальной возможности оперативно адаптироваться к самым свежим разработкам мировой научной мысли, «Приток» опередил всех. Когда это потребовалось, то телефонную линию — традиционный в то время канал связи с пультом — дополнили радиоканалом

и каналом сотовой связи. Сейчас настало время интернет-протоколов, систем спутниковой навигации ГЛОНАСС/GPS.

Ещё одной важной особенностью системы «Приток», также заложенной изначально, является возможность интегрироваться со всевозможными устройствами охраны, наблюдения и контроля доступа, видеокамерами, электронными замками, турникетами и т. п. и безгранично «размножаться».

Например, в небольшом офисе или квартире монтируется минимально необходимый набор охранно-пожарных приборов, который в режиме двухсторонней связи взаимодействует с пультом централизованного наблюдения. Но при необходимости система развивается, беря под своё крыло все офисы на этаже или же весь многоквартирный жилой дом, а затем и гаражи его жильцов, магазины и близстоящие объекты инфраструктуры.

Кроме того, система, используя сеть спутников на околоземной орбите, может мониторить передвижение автотранспорта по дорогам России — от Калининграда до Владивостока.

За два последних десятилетия охранные технологии прошли сразу несколько ступеней эволюции. Если раньше основным средством для сообщения о происшествии был телефон 02, а группы быстрого реагирования отправлялись по вызовам едва ли не на перекладных, то теперь ситуация в корне иная. Степень оснащённости выросла в разы. Полицейские экипажи оборудованы спутниковой навигацией. Офицер, который руководит действиями, по электронной карте видит перемещение групп и может принять обоснованное решение по направлению на тревогу ближайшей. А компьютер ему просто подскажет, как действовать лучше.

Стремясь оставаться современной, Интегрированная система (ИС) охранно-пожарной сигнализации (ОПС) «Приток-А» и в настоящее время успевает за бурным развитием средств связи и коммуникаций.

Например, цифровая технология GPON обеспечивает доступ к ресурсам сети «Интернет» на скорости до 1 Гб/с, что в двести раз выше, чем по медным линиям, и в десять раз выше, чем на данный момент могут предложить большинство из провайдеров.

Уже сегодня Охранное бюро «СОКРАТ» производит аппаратуру, которая позволяет отказаться от традиционных методов построения технических средств централизованной охраны, с использованием линий связи обычной телефонной сети, а именно:

1. Аппаратуру, работающую по волоконно-оптическим цифровым каналам передачи данных, с использованием технологий VPN-сетей и открытого Интернета. Технология VPN-сетей применяется для повышения надёжности и сопряжения ПЦН с уже установленной аппаратурой, работающей по старой классической схеме. Резервирование каналов связи как на ПЦН,

так и на объектах производится дополнительным (с другим провайдером) подключением к Интернету, или через каналы сотовой связи в режиме GPRS.

2. Аппаратуру, работающую по каналам сотовой связи стандартов GSM и 3G. Она позволяет организовать централизованную охрану, используя эти каналы в качестве основных. А для охранных приборов, работающих по другим различным каналам передачи данных, каналы сотовой связи могут применяться в качестве резервных. Для надёжности имеется возможность установки в прибор и в РКС двух sim-карт. Соответственно на ПЦН имеется два подключения к серверам операторов сотовой связи и два БМ-03 с различными sim-картами.

3. Аппаратуру, работающую по радиоканалам в безлицензионных диапазонах частот, Приток-МКР. Эта аппаратура предназначена для беспроводного удлинения связи подсистем ИС «Приток-А», а также для создания автономных систем централизованной охраны с использованием приёмопередатчиков мощностью не более 10 мВт. Принцип действия «Приток-МКР» основан на создании радиосети с динамической маршрутизацией, в которой каждый узел связи (их может быть 250) является ретранслятором. В качестве узлов связи используется серийно выпускаемый модуль РПДУ-03, который в том числе является и прибором, т. к. имеет четыре охранных шлейфа.

4. Аппаратуру, использующую технологии ГЛОНАСС GPS, в сочетании с GSM-связью в режиме GPRS, для мониторинга и охраны подвижных объектов. Приток-МПО-ГЛОНАСС/GPS обеспечивает мониторинг и охрану подвижных объектов (транспортных средств — ТС). Выпускаются различные бортовые комплекты для работы как по УКВ — каналу, так и по каналам сотовой связи стандарта GSM, в режиме GPRS. ПЦН остаётся прежним.

Всё перечисленное выше может быть включено в состав систем, которые уже эксплуатируются более чем в 50 регионах России. А основным отличием современной схемы от классической является отсутствие охранный аппаратуры на АТС.

В ближайшей перспективе качественные изменения, мы предполагаем, произойдут в части более широкого использования аппаратуры сотовой связи третьего и четвертого поколения — 3G, 4G.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ²

1. Интегрированные системы безопасности // Гипермаркет систем безопасности [Электронный ресурс]. — Режим доступа: https://www.aktivsb.ru/statii/integrirovannye_sistemy_bezopasnosti.html (дата обращения: 10.09.2018).
2. Гинце А. С. Интегрированные системы безопасности // Алгоритм безопасности. — 2014. — № 1. — С. 6—8.
3. Полоник Р. А., Фролов И. А. Интегрированные системы безопасности — новое перспективное направление развития технических средств обеспечения безопасности // Охрана, безопасность и связь. — 2014. — № 1—2. — С. 101—107.
4. Механические устройства определяют эффективность преграждающих устройств в СКУД [Электронный ресурс]. — Режим доступа: <http://www.cnews.ru/reviews/free/techsec2006/articles/lock.shtml?print> (дата обращения: 20.10.2018).
5. Альтерман А. Д., Лушников Н. Д. Интегральные системы безопасности и их основные функции // Аллея науки. — 2018. — № 3. — С. 894—896.
6. Козин А. А., Михайлов А. П., Михайлин А. С. Аппаратные и программные средства в сфере систем безопасности и охраны // Теория и практика современной науки. — 2018. — № 4. — С. 339—342.
7. ПК LyriX Назначение, архитектура, возможности [Электронный ресурс]. — Режим доступа: <http://docplayer.ru/36994706-pk-lyrix-naznachenie-arhitektura-vozmozhnosti.html> (дата обращения: 15.10.2018).
8. Гинце А. С. Интегрированные системы безопасности // Системы безопасности. — 2014. — № 2. — С. 129—134.
9. Интегрированная система охранно-пожарной сигнализации «Приток-А» // realsystem.ru [Электронный ресурс]. — Режим доступа: <http://www.realsystem.ru/new/taxonomy/term/10253%2C3814> (дата обращения: 19.10.2018).
10. Никитин А. В. Интегрированная система охранно-пожарной сигнализации «Приток» на службе правоохранительных органов // Вестник Восточно-Сибирского института МВД России. — 2015. — № 1. — С. 5—11.
11. Зыбин Д. Г., Ролдугин С. В., Коротких В. Е. Особенности использования интегрированной системы «Приток-А» для обеспечения безопасности объектов ФСИН России // Вестник Воронежского института ФСИН России. — 2013. — № 1. — С. 14—18.

² Данный список литературы оставлен с учётом затекстовых ссылок, указанных в пособии.

12. Грачёв А. Е., Соколов С. А. Охрана объектов различного назначения с использованием интегрированной системы безопасности «Приток-А» // Актуальные вопросы эксплуатации систем охраны и защищённых телекоммуникационных систем. — 2015. — № 1. — С. 68—69.

13. Зайцев А. Г. Направления развития технических средств и систем охраны в современных условиях // Алгоритм безопасности. — 2013. — № 3. — С. 6—10.

14. Всероссийское Совещание-семинар начальников управлений Вневедомственной охраны МВД России [Электронный ресурс]. — Режим доступа: https://vimvd.ru/upload/iblock/334/173_2013_4.pdf (дата обращения: 25.10.2018).

15. Матвеев Ю. В., Сафонов Ю. А., Зубова Н. В., Метелева Н. Г. Путь от научной идеи до внедрения технических средств охраны в производство // Технологии техносферной безопасности. — 2016. — № 5. — С. 278—282.

16. Зайцев А. Г. Направления развития технических средств и систем охраны в современных условиях // Алгоритм безопасности. — 2013. — № 3. — С. 1—5.

Учебное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА
ОБЕСПЕЧЕНИЯ ОХРАНЫ ОБЪЕКТОВ

Авторы-составители:
Джурук Дмитрий Сергеевич,
Курмазов Алексей Александрович,
Никитин Александр Викторович

Редактор
А. В. Андреев

Подписано в печать 8.07.2019

Усл. печ. л. 4,0

Тираж 30 экз.

Формат 60х84/16

Заказ № 38

НИиРИО ФГКОУ ВО «Восточно-Сибирский институт МВД России»,
ул. Лермонтова, 110