СПЕЦИАЛИЗИРОВАННЫЙ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ
О ПРОБЛЕМАХ БЕЗОПАСНОСТИ

СОКРАТ

№ 01 (06) 2016 Иркутск

Централизованная охрана в современных условиях

Защита локальных вычислительных сетей

ОВЭ. На стыке двух миров

3.7.1 – новая версия ИС ОПС Приток-А

25 ЛЕТ РАЗРАБОТКИ И ПРОИЗВОДСТВА СИСТЕМ БЕЗОПАСНОСТИ

Интегрированная система охранно-пожарной сигнализации Приток-А

СТРУКТУРА

Приток-Автоприбытие	Регистрация и воспроизведение аудиоинформации Приток-РТП	Приток-Охрана-WEB
Резервный канал связи Приток-РКС (GSM)	ОПС Приток-А по телефонным каналам	Радиоохрана Приток-А
Видеонаблюдение Приток-Видео	Охрана и мониторинг Приток-Интернет	Охрана и мониторинг Приток-GSM
Контроль и управление доступом Приток-СКУД	Микрорадиоохрана Приток-МКР	Мониторинг и охрана Приток-МПО-ГЛОНАСС/GPS

Подсистема телекоммуникационных связей

Приток-TCP/IP

ПУЛЬТ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ

Совокупность программно-аппаратных средств ИС Приток-А, работающих под управлением единого программного ядра, позволяет формировать различные подсистемы, которые могут работать как автономно, так и в сочетании с другими подсистемами, образуя интегрированную систему безопасности

СОКРАТ

2016 № 1(6)

Издатель:
ООО Рекламно-издательская фирма «Гвоздь плюс»

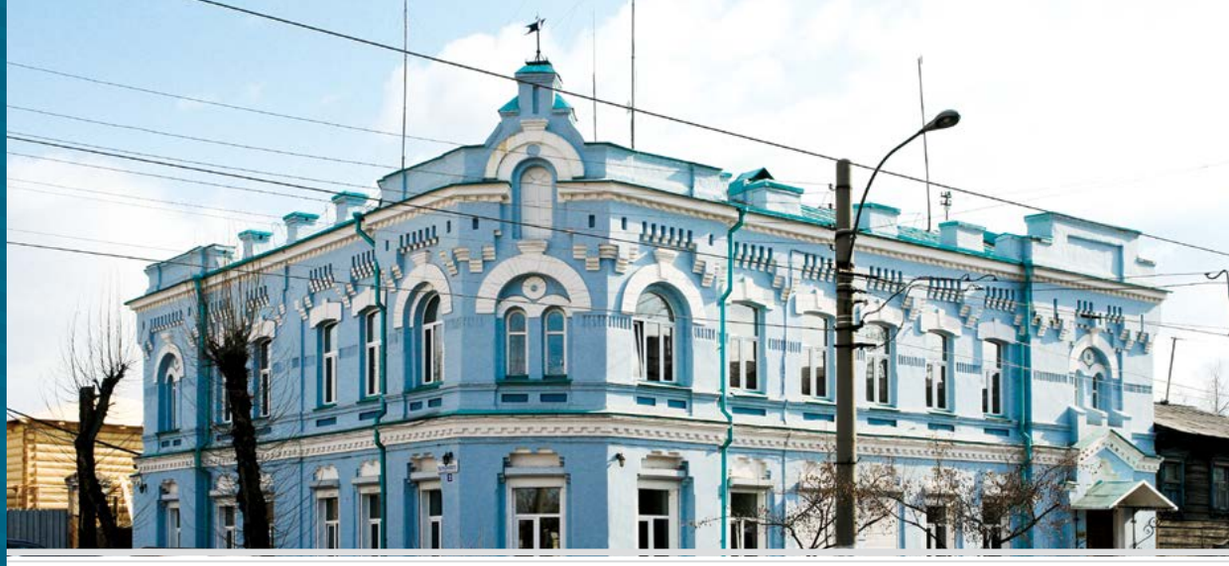
664025,
Иркутск, ул. Марата, 29
Тел.: (3952) 22-33-22,
34-20-79, 33-45-24
E-mail: gvozd@irmail.ru
www.kapitalpress.ru

Подготовка статей:
Константин Куликов

Верстка, допечатная подготовка:
Роман Шкаликов

Иллюстрации:
Татьяна Бояркина

Журнал отпечатан в типографии «Репроцентр А1»



Содержание

Система централизованной охраны «Приток»

Тенденции развития

Начиная с 1989 года ОБ «СОКРАТ» работает над темой автоматизации пультов централизованного наблюдения (ПЦН). За 27 лет развития техника охраны проделала путь от ручных диспетчерских полукомплектов до полностью автоматизированных комплексов, основанных на интернет-технологиях.

Интернет, как среда передачи данных охранной сигнализации, имеет неоспоримые преимущества по универсальности, доступности и цене. Активное внедрение технологий доступа в Глобальную сеть для частных лиц и организаций предоставляет большие возможности и для оказания услуг охраны и мониторинга.

Системы охраны по занятым телефонным линиям, получившие широкое распространение, еще продолжают эксплуатироваться, но под натиском технологии GPON (сокращенно от Gigabit Passive Optical Network – гигабитная пассивная оптическая сеть) вынужденно демонтируются и выводятся из эксплуатации.

Различные РСПИ (радиосистемы передачи извещений), несмотря на очевидное преимущество, заключающееся в автономности работы, имеют и недостатки. Это ограниченный радиус действия, небольшая емкость в рамках одного узла системы и др. Интернет не имеет границ, и поэтому СПИ (системы передачи извещений), использующие IP-технологии, не привязаны к территориям, не ограничены по количеству и могут быть мобильны.

Рассмотрим подробнее систему пожарно-охранной сигнализации «Приток» образца 2016 года. В первую очередь, обратим внимание на программное обеспечение (ПО) системы – это «Приток» версии 3.7.1. Текущая версия «Приток» всегда представлена на сайте www.sokrat.ru и поддерживает все ранее выпущенные и на сегодня актуальные технологии охраны (занятые линии, РСПИ, интернет).

Все АРМы (автоматизированные рабочие места) ПО «Приток» сетевые, что позволяет легко масштабировать ПЦН от 100 до 100 000 и более пультовых номеров. Более того, вся охранная аппаратура подключена к ПО «Приток» также по IP-сети. Это дает возможность безболезненного переезда расположения ПЦН в пределах досягаемости аппаратуры по IP-сети.

Павел Воробьев,
начальник отдела
НИиОКР ОБ «СОКРАТ»

С помощью ПО «Приток» легко решаются вопросы объединения ПЦН. Использование ресурсов глобальных сетей (например, интернет) или сетей предприятий позволяет реализовать функциональное разделение по структурам ПЦН и подключение «удаленных» АРМов других подразделений – обслуживающих организаций, технических служб и пр. Возможность работать с любым объектом, подключенным к системе с любого АРМа, позволяет динамически перераспределять нагрузку между операторами.

В единую систему «Приток» подключен мониторинг подвижных объектов «Приток-МПО», который обеспечивает на электронной карте местности, используя систему ГЛОНАСС/GPS, визуальный контроль служебного автотранспорта, а также охрану частных автомобилей. Единая информационная база объектов охраны и подвижных объектов мониторинга в системе «Приток» позволяет предоставлять расширенный спектр услуг для населения и качественную работу оперативных служб охраны.

Используя систему «Приток-Экипаж», целеуказания о тревогах передаются в ГЗ также по каналам интернета. Эта возможность исключает перехват сообщений в открытом радиоэфире и повышает достоверность информации, а группа видит на карте своего планшета путь к тревожному объекту с учетом пробок.

К системе «Приток» подключен WEB-интерфейс, позволяющий обслуживающим организациям, используя интернет-каналы, с помощью WEB-браузера подключаться к ПЦН для проведения технических работ, мониторинга исправности и выполнения заявок вызова техников.

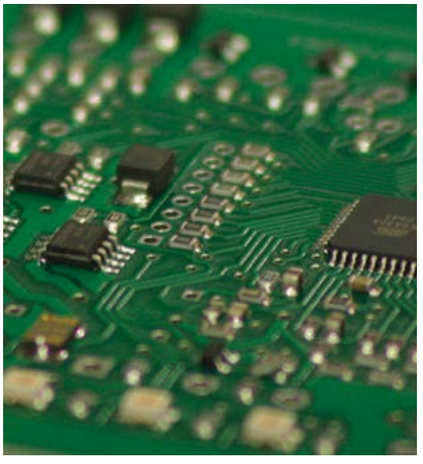
Кроме этого, собственник также получает возможность не только контролировать из любой точки планеты состояние своего объекта на ПЦН (по интернет-каналам с помощью WEB-браузера или приложения для ОС Android или iOS), но и выполнять команды «Взять», «Снять», «Опросить». Собственник может контролировать текущие показания различных датчиков (температура, влажность и др.), управлять исполнительными устройствами, просматривать историю и получать видеоизображение с объекта охраны. Развитие интернет-сервиса со стороны ПЦН позволяет предоставить клиентам охраны дополнительные услуги.

Для установки на объект «Приток» предлагает оборудование для всех существующих современных каналов связи, а также новую серию приборов КОП (Контроллер Охранно-Пожарный). На сегодня имеется КОП-01 (8 или 16 зон с расширением до 128 зон), КОП-02 (4 или 8 зон с расширением до 32 зон) и КОП-03 (8 или 16 зон с расширением до 128 зон, поддержкой каналов Wi-Fi, работа в сети 3G GSM и модули Bluetooth для управления контроллером).

Связь с ПЦН обеспечивается по проводным интернет-каналам или через сети Wi-Fi, и для резерва используется одна или две сим-карты, установленные в приборе. На ПЦН обеспечен контроль канала связи с настраиваемым для каждого прибора временем (время по умолчанию 120 сек) и автоматическим переходом на резервные каналы.

Каждый КОП поддерживает шину расширения RS-485, на которую могут быть подключены различные дополнительные устройства. Это модуль расширения шлейфов, модули подключения беспроводных датчиков «Астра» и «Ладога», модуль беспроводной клавиатуры, модуль контроля температуры и влажности, а также модуль подключения шины из дополнительных 30 приборов «Приток» ППКОП-05. Шина расширения КОП не только позволяет организовать охрану любого (даже крупного) объекта на одном приборе, но и получать данные телеметрии и управлять разнообразными устройствами, используя оборудование в различных сферах деятельности для собственника.

Дальнейшее развитие системы «Приток» предлагает повышения сервиса для ПЦН и клиента охраны. Реализация проектов в ПО и внедрение нового оборудования качественно повысит услуги, предоставляемые организациями охраны, обеспечит собственнику еще более удобный интерфейс контроля собственных объектов охраны, а также доставку на ПЦН по интернет-каналам видео подтверждения тревоги.



Организация централизованной охраны в современных условиях

Технологии в сфере передачи информации по проводным линиям связи в последние годы стремительно развиваются. Это приводит к тому, что организация централизованной охраны объектов и квартир по «классической» схеме уже неприменима.

В крупных городах Российской Федерации региональные операторы активно переключают абонентов с обычных медных на волоконно-оптические линии связи, в том числе выполненные по технологии PON (пассивные оптические сети – от англ. Passive Optical Network). Это позволяет предоставлять абоненту услуги не только телефонной связи, но и цифрового телевидения и высокоскоростного доступа в глобальную сеть Интернет.

Преимущества данной технологии:

– в GPON используются пассивные оптические разветвители, которые можно встраивать непосредственно в магистральный кабель;

– прием и передача ведутся по одному и тому же волокну;

– оптоволоконный кабель устойчив к электромагнитным воздействиям, не является источником электромагнитных волн, привлекателен по массо-габаритным параметрам и защищен от несанкционированного доступа;

– технология GPON позволяет осуществлять настройку оборудования в соответствии с индивидуальными потребностями клиента и предоставлять именно тот уровень сервиса, который ему требуется;

Технология GPON в последнее время все чаще используется операторами связи при построении и модернизации сетей передачи данных. Дальнейшее удешевление данной технологии приведет к ее повсеместному внедрению не только в крупных городах.

В таких условиях становится невозможной организация централизованной охраны объектов и квартир по «классической» схеме, т.е. применение технических средств охраны, передающих информацию между объектовым оборудованием на охраняемом объекте и пунктом централизованной охраны (ПЦО) только по медным телефонным линиям с использованием ретрансляторного оборудования, устанавливаемого на АТС.

Николай Николаев,
сектор автоматизации деятельности ПЦО отдела развития централизованной охраны, старший научный сотрудник ФКУ НИЦ «Охрана» МВД России

В этом случае построение системы централизованной охраны может быть осуществлено следующим образом

Вариант №1. Отказ от проводной связи с использованием радиоканала как основной среды передачи данных.

Вариант №2. Использование полного пакета транспортных услуг на базе закрытой VPN-сети (от анг. Virtual Private Network), построенной на базе волоконно-оптических линий связи по технологии PON. Эта VPN-сеть охватывает все охраняемые вневедомственной охраной объекты и все ПЦО в пределах города и предлагается в аренду региональными операторами связи взамен действующей инфраструктуры медных телефонных линий.

Вариант №3. Применение открытых каналов глобальной сети Интернет для связи устройствами оконечными объектовыми (УОО) и ПЦО.

Рассмотрим каждый из предлагаемых способов построения централизованной охраны.

Централизованная охрана по радиоканалу

Альтернативой по отношению к проводным каналам связи является применение для централизованной охраны только радиоканала (УКВ и/или GSM).

Следует отметить, что внедрение данного варианта потребует существенных затрат на полную замену как аппаратно-программных комплексов на ПЦО, так и оконечного оборудования на объектах и квартирах, а также – установку дополнительных ретрансляторов. Кроме того, как показывает многолетний опыт, радиоканал не обладает достаточной надежностью в условиях сложной помеховой обстановки больших мегаполисов (вблизи мощных энергокоммутирующих установок, в зонах действия радиопередающих станций, районах массовой высокоэтажной застройки).

Указанные обстоятельства ставят под сомнение целесообразность крупномасштабной реализации данного варианта.

Централизованная охрана по арендуемой VPN-сети

При организации системы централизованной охраны объектов с использованием закрытой VPN-сети, предлагаемой в аренду региональным оператором связи, возможно объединение аппаратно-программных комплексов пультов централизованного наблюдения (ПЦН) с УОО в единую сеть, обеспечивающую достаточно высокий уровень информационной безопасности.

Преимущества такого построения в следующем:

1. Обмен информацией между ПЦН и УОО будет происходить по закрытым каналам, которые логически отделены от

сети общего пользования. Для обеспечения конфиденциальности передаваемой информации оператором связи предусматривается ее шифрование.

2. Арендуемая закрытая VPN-сеть обеспечивает надежную передачу данных, поскольку приоритет в обслуживании и устранении неисправностей оператором связи отдан закрытым сетям, а затем уже открытым.

3. Локальные сети территориальных подразделений вневедомственной охраны – управления (УВО), отделов (ОВО), ПЦО, дежурных частей и отдельных батальонов полиции – могут быть интегрированы в данную VPN -сеть, образуя единую корпоративную сеть. Эта сеть позволит оперативно решать достаточно большой спектр организационных и административных задач, в том числе обеспечение местной телефонной связи между всеми подразделениями, возможность проведения видеоконференций, электронный документооборот, доступ к системе межведомственного электронного взаимодействия и др.

4. У вневедомственной охраны появится возможность выводить сигналы на любые ПЦО в зоне действия корпоративной сети вне зависимости от территориальной расположенности объекта, а также при необходимости проводить оперативную перегруппировку ПЦО.

Недостатками такого построения являются:

1. Отсутствие возможности подключения на ПЦО абонентов сетей других операторов связи, работающих на территории городской застройки.

2. Достаточно высокая постоянная арендная плата.

3. Нерегулируемая со стороны вневедомственной охраны тарифная политика за оплату точек подключения к такой сети как для абонентов, так и для структурных подразделений УВО. Затраты на внедрение данного варианта и обслуживание каналов связи в настоящее время детально прорабатываются с региональными операторами связи.

Централизованная охрана по сети Интернет

Также с точки зрения преимуществ и недостатков целесообразно рассмотреть вариант построения системы централизованной охраны, предусматривающий использование глобальной сети Интернет. В качестве преимуществ такого построения можно отметить следующее:

1. Доступность подключения к сети Интернет для каждого объекта и квартиры и невысокая плата за использование данного канала.

2. Отсутствие монополии одного оператора связи и возможность подключения любого клиента, нуждающегося в услугах вневедомственной охраны и обслуживаемого любыми провайдерами, работающими в населенных пунктах. Например, в Москве имеется порядка 400 провайдеров сети Интернет.

Вместе с тем при такой организации охраны имеется ряд проблемных, но вполне разрешимых вопросов:

1. Пульт, подключенный к сети Интернет, может подвергнуться кибератакам. Правонарушитель из любой точки подключения к сети Интернет сможет произвести на аппаратно-программный комплекс ПЦН различные воздействия с применением как одного, так и множества компьютеров.

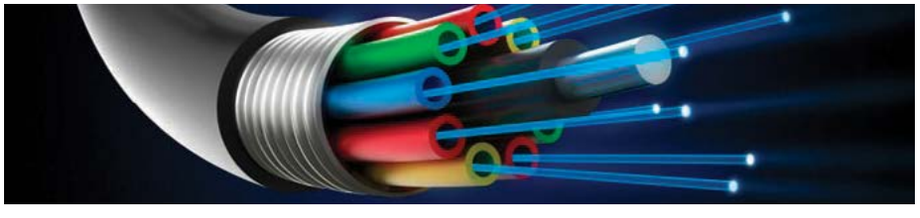
2. Для обеспечения надежности связи аппаратно-программного комплекса ПЦН с объектовыми устройствами ПЦО должен быть обеспечен резервным доступом в Интернет, арендуемым у другого провайдера.

3. Использование открытой сети Интернет в качестве канала передачи данных между объектовым оборудованием и ПЦН возможно только после проведения на ПЦО комплекса мероприятий, обеспечивающих надлежащий уровень информационной защиты локальной вычислительной сети (ЛВС) ПЦО.

Перспективы развития централизованной охраны на цифровых каналах

Использование высокоскоростных и широкополосных цифровых каналов передачи информации, в т.ч. выполненных по технологии GPON, для целей централизованной охраны обеспечивает возможность существенного увеличения количества информации, которую можно получить с охраняемого объекта на ПЦО. Решение этой задачи позволяет, во-первых, оптимизировать действия групп задержания за счет постоянного мониторинга поведения преступника на объекте. Во-вторых, увеличит объем данных о развитии других негативных ситуаций на охраняемых объектах (например – пожара), что напрямую влияет на оперативность принятия обоснованных решений, грамотное распределение сил и средств.

При этом появляется возможность передачи с охраняемого объекта на ПЦО аудио- и видеоинформации, что значительно повысит эффективность реагирования групп задержания на сигналы тревоги с охраняемых объектов и обеспечит более высокую надежность их охраны.



Коллектив отдела почти в полном составе

На стыке двух миров

Отдел внедрения и эксплуатации ОБ «СОКРАТ»

Что-то вдруг пошло не так, и связь компьютера с репликатором исчезла. Или пользователь, установив программные обновления подобно тому, как это делал уже не раз, вдруг обнаруживает, что «всё, ничего не работает…». Это лишь две ситуации из множества, когда требуется спасительный звонок к специалистам отдела внедрения и эксплуатации ОБ «СОКРАТ».

Сегодня в ассортименте оборудования, выпускаемого ОБ «СОКРАТ», более 200 наименований приборов, которые позволяют смонтировать охранный комплекс любого размера. Это может быть пульт централизованного наблюдения на несколько АРМов, а может – система ПЦН, берущая под свою защиту целый город.

В течение последних лет предприятием активно развивается линейка новых приборов «Приток-А-КОП», в которой применяются все самые современные технологии, в том числе – беспроводной передачи данных и интернет-каналы. Для управления приборами системы «Приток» теперь могут использоваться даже мобильные телефоны и смартфоны – те гаджеты, которые сегодня есть в кармане практически у каждого человека.

К тому же инженеры-разработчики ОБ «СОКРАТ» ежегодно выводят на рынок по нескольку обновлений программного обеспечения, совершенствуют сами приборы (более подробно – стр. 28).

В таком изобилии оборудования под любые задачи порой бывает непросто разобраться даже пользователю со стажем, не говоря уже про новичков. Именно здесь на помощь приходят специалисты отдела внедрения и эксплуатации.

Круглосуточная связь

Само название отдела указывает на его основные задачи – внедрение и ввод в эксплуатацию оборудования и программного обеспечения ИС «Приток-А» на объектах потребителей. Причем пуско-наладочные работы специалисты отдела проводят на всей территории России. Также отдел отвечает и за обеспечение дальнейшей бесперебойной работы систем «Приток», что достигается консультациями по телефону техподдержки, по электронной почте, через форумы, а при особой необходимости – и оперативным реагированием на нештатные ситуации, возникающие у клиентов, с выездом на место.

В отделе семь человек, которые работают в две смены. А если учесть количество часовых поясов и то, что оборудование «СОКРАТА» используется в 50 регионах страны, то выходит, что отдел на связи с пользователями почти круглосуточно.

— У нас идет постоянное общение с пользователями: кто-то устанавливает какие-то наши свежие разработки, осваивает их. А у кого что-то не получилось, сломалось – консультируем, – рассказывает начальник отдела Елена Русакова. — Очень много пользовательских звонков. С утра звонки в основном с востока страны, а к обеду подтягивается западная часть, москвичи. Перед Новым годом просто шквал обращений был – люди пытались

до праздников доделать то, что не успели.

Деятельность своего отдела Елена Русакова делит на два направления. Первое – когда приходит новый заказчик, и по его параметрам подбирается комплекс оборудования. А затем этап пуско-наладочных работ на объекте – настройка оборудования, обучение правильному его использованию.

Сюда же можно отнести и общение с постоянными заказчиками. Чаще всего они звонят, интересуясь какими-то обновлениями в программном обеспечении и новинками в ассортименте приборов: «Мы слышали, что у вас что-то новое появилось. А как бы нам это настроить и использовать?»

Музейный экспонат, но работает

— Но бОльшая часть нашей работы, — продолжает Елена Русакова, — это вот такие звонки: «У меня все работало-работало и вдруг сломалось что-то». А дальше начинается самое сложное – сначала понять, что хотел сказать пользователь, а затем – где и какая возникла ошибка. Да, не только проблему искать приходится, но и общий язык с пользователем. Конечно, люди звонят с разным уровнем подготовки. А современные сетевые технологии исключают известный подход из прошлого века. Теперь уже нельзя, как раньше, прозвонить сеть «цешкой»-тестером: о, у меня тут есть напряжение, значит, все в порядке с линией. Новые виды связи – Ethernet, интернет – намного сложнее. Доходит до курьезов. Бывает, приходится пользователю диктовать команды: «Вам нужно команду ping набрать. – А что это, а как набрать? – Видите буквы на клавиатуре? Набирайте».

Один из показательных случаев в отделе рассказывают до сих пор. Давняя история. Звонит из Читинской области техник с пульта: проблема – система не работает. Но объясняет он это так: «Мне прислали жесткий диск по емейлу. Я его вставил, и теперь ничего не работает. Помогите. Здесь нет больше никого, кто хоть что-то понимает в компьютерах».

Долго «сократовцы» отгадывали, что такое в понимании звонившего жесткий диск и как его присылали по емейлу. Потом разобрались: оказалось, что на том пульте был установлен еще «Приток» под MS-DOS, пришло обновление версии на 3,5-дюймовых дискетах, которые, считал техник, и есть «жесткий диск», ведь они не гибкие…

Кое-как с тем «специалистом» разобрались, запустили систему. Показательно, что проблему решили по телефону и выезда за тысячу километров не потребовалось.

Елена Русакова,
начальник ОВЭ:

— Среди наших задач — внедрение новых разработок и помощь пользователям в бесперебойной эксплуатации оборудования.

— Периодически случаются такие звонки, — вспоминают сотрудники отдела. – Пользователь: «У нас висит ваш прибор. Хотим его перепрограммировать и поменять тип шлейфа». – «Что за прибор?» — «Не знаем. Когда и кто повесил — тоже». — «Фото присылайте». Оказывается, это «Приток» 20-летней давности. Не то что мы о таком не слышали, так и более старые спецы его уже не помнят. И программирования шлейфов тогда не существовало. Говорим, присылайте нам в музей – отказываются: «Не отдадим, он нормально работает».

Дочитать до конца

По утверждению специалистов отдела, наиболее часто ошибки, с которыми к ним обращаются, возникают из-за некоторой инерции мышления и недопонимания: прочитал или даже не дочитал пользователь руководство и как понял, так и применил к своим условиям.

— Нередко люди, которые давно эксплуатируют наше оборудование, получая новое, пытаются с ним обращаться точно так же, как ранее. Потом звонят: «Я его программировал, но прибор не работает». – «А как вы его программировали?» – «Как много лет программирую, так и программировал». – «Вы посмотрите руководство, почитайте внимательно. Там есть изменения…» Это же обычная человеческая психология – делать так же, как делал раньше, — сетует начальник отдела.

Много в отдел поступает сетевых вопросов, ведь сейчас очень сложными стали схемы подключения. И уровня простого пользователя теперь недостаточно. Надо понимать, что такое маршрутизация, доступы, нюансы настроек и т.п.

— Или бывает так. Делает человек очень простую вещь: ставит ретранслятор программировать к пульту. Все вроде хорошо и правильно, но связи нет. Начинаешь выяснять самые мельчайшие подробности: ip-адреса у сервера, у ретранслятора, маску, шлюз. И оказывается, что, прописывая ip-адреса, ошиблись в одной цифре. А они в разных сетях и без дополнительного оборудования видеть друг друга не могут. Случается и несколько иное, но с тем же эффектом: Windows обновили, антивирус поменяли. И все – также нет связи.

В особо сложных и аварийных случаях в отделе на специальных стендах моделируются нештатные ситуации – приборы, ретрансляторы и другое оборудование подключаются аналогично тому, как это сделано у пользователя. Пробуются различные версии прошивки и ПО. На такую диагностику уходит время, но метод необходим для поиска и обнаружения возникшей проблемы и эффективен.

«Работа у нас нескучная: все время что-то отгадываем, решаем», — улыбаются сотрудники отдела.

И еще одна важная функция, о которой нужно упомянуть.

— Допустим, выходит новый прибор. Сначала обязательно идет его тестовая проверка внутри «СОКРАТА». Но это все же лабораторные условия, хотя очень стараемся в разных условиях его гонять. И вот когда прибор уходит к потребителю и начинается его реальная эксплуатация, собираем мнения о его работе, пожелания пользователей. Такая обратная связь очень важна для разработчиков, которые, ее получив, могут какие-то функции поправить, доработать. По сути получается, что наш отдел функционирует на переднем крае, на стыке двух миров. У разработчиков «СОКРАТА» свой мир – высокотехнологичный и немного даже фантастический. И мир пользователей, тех людей, кто эксплуатирует наши приборы в реальной жизни. Наш отдел эти два мира объединяет, – подытоживает Елена Русакова.

Защита локальных вычислительных сетей

пунктов централизованной охраны (ЛВС ПЦО) на основе маршрутизаторов

Каждый год ущерб от компьютерных преступлений составляет сотни миллионов долларов. Потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности.

Наибольший ущерб наносит манипулирование доступом во внутреннее информационное пространство: кражи данных и информации из корпоративных сетей и баз данных, подмена информации, подлоги документов в электронном виде, промышленный шпионаж. Наряду с возрастанием числа внешних атак в последние годы отмечается резкий рост распространения вирусов через интернет.

Некоторые ПЦО, до подключения к сети Интернет не сталкивавшиеся с вопросами защиты информации, могут оказаться не подготовленными к изменившейся ситуации. Во многих случаях пользователи корпоративных сетей даже не подозревают о том, что их данные неожиданно оказались доступны любому пользователю интернета.

В системах передачи информации атакам подвергнуто как объектовое оборудование — УОО (устройства объектовые оконечные), ППКО (приборы приемно-контрольные охранные), так и пультовое оборудование — компьютеры АРМ (автоматизированые рабочие места), серверы баз данных, коммутаторы. Целями атак могут быть: захват управления АРМ-ом, копирование базы данных клиентов, корректировка базы данных, блокирование тревожных сигналов с объектов охраны. Возможны различные неприятные последствия, например отсутствие сигнала о проникновении злоумышленников в квартиру и т.д. и т.п. Защита обеспечивается применением дополнительного оборудования — межсетевых экранов.

Угрозы при использовании глобальной сети Интернет в качестве среды передачи данных

После подключения хотя бы одного канала интернет для передачи извещений от УОО на АРМ возникают угрозы,

Андрей Голубев, старший научный сотрудник ФКУ НИЦ «Охрана» МВД России

обусловленные преднамеренными или непреднамеренными действиями физических лиц, а также криминальных группировок, создающих условия (предпосылки) для нарушения функционирования систем централизованного наблюдения и для нарушения безопасности служебной информации (СИн), которые могут привести к ущербу при охране имущества.

Эти угрозы безопасности связаны:

- с перехватом извещений от УОО на АРМ по каналам Интернет с целью их подмены;
- с действиями, которые ведут к невозможности доставки сообщений от УОО на АРМ;
- с несанкционированным доступом в ЛВС ПЦО с целью удаленного управления АРМ ПЦО;
- с несанкционированным, в том числе случайным, доступом в ЛВС ПЦО с целью изменения, копирования, неправомерного распространения СИн или деструктивных воздействий на элементы ЛВС ПЦО и обрабатываемой в них СИн с использованием программных и программно-аппаратных средств с целью ее уничтожения или блокирования.

Основными элементами ЛВС ПЦО являются:

- СИн, содержащаяся в базах данных;
- защищаемая информация от УОО на АРМ (ЗИн);
- технические средства, осуществляющие обработку СИн и ЗИн (аппаратура ЛВС ПЦО);
- программные средства (операционные системы, АРМ, системы управления базами данных и т.п.);
- средства защиты информации.

Если АРМ реализован на базе локальной или распределенной информационной системы, подключенной к сетям общего пользования и (или) сетям международного информационного обмена, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к СИн или реализовываться угроза отказа в обслуживании.

Могут быть атаки различных типов, например:

- путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение;
- путем переполнения буфера серверного приложения;
- путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами. Последствия этих атак возможны различные, в том числе:

• нарушение конфиденциальности, целостности, доступности информации;

• скрытое управление системой.

Процесс реализации угрозы в общем случае состоит из четырех этапов:

• сбора информации;

• вторжения (проникновения в операционную среду);

• осуществления несанкционированного доступа;

• ликвидации следов несанкционированного доступа.

Программно-математическое воздействие — это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

• скрывать признаки своего присутствия в программной среде компьютера;

• обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

• разрушать (искажать произвольным образом) код программ в оперативной памяти;

• выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

• сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

• искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены в процессе эксплуатации АРМ посредством сетевого взаимодействия в результате НСД.

Современные вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционированного исследования параметров АРМ без вмешательства в функционирование АРМ до уничтожения СИн и программного обеспечения АРМ) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

Наличие в АРМ вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, u1087 позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

«Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тысяч сигнатур компьютерных вирусов. Вместе с тем, далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способен внедриться в них. Часто основную опасность представляют новые вредоносные программы.

Защита от угроз при помощи межсетевых экранов

Производители технических средств охраны рекомендуют обычную для небольших компьютерных сетей защиту при подключении ЛВС ПЦО к сети Интернет. Из особенных требований можно выделить:

• использование межсетевых экранов;

• применение трансляции сетевых адресов (NAT);

• организация резервного канала для подключения к хосту в случае выхода из строя основного канала;

• организация третьего — аварийного канала для подключения ПЦН к интернету в случае выхода из строя основного и резервного канала.

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ). В переводной литературе также встречаются термины firewall или брандмауэр.

Межсетевой экран — это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее *(рис. 1)*.

МЭ повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно.

Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию во внутренней области режима конфиденциальности. Кроме функций разграничения доступа, МЭ может обеспечивать выполнение дополнительных функций безопасности (аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий).

МЭ не является симметричным устройством, для него определены понятия «внутри» и «снаружи» (входящий и исходящий трафики). При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

В общем случае алгоритм функционирования МЭ сводится к выполнению двух групп функций, одна из которых ограничивает перемещение данных

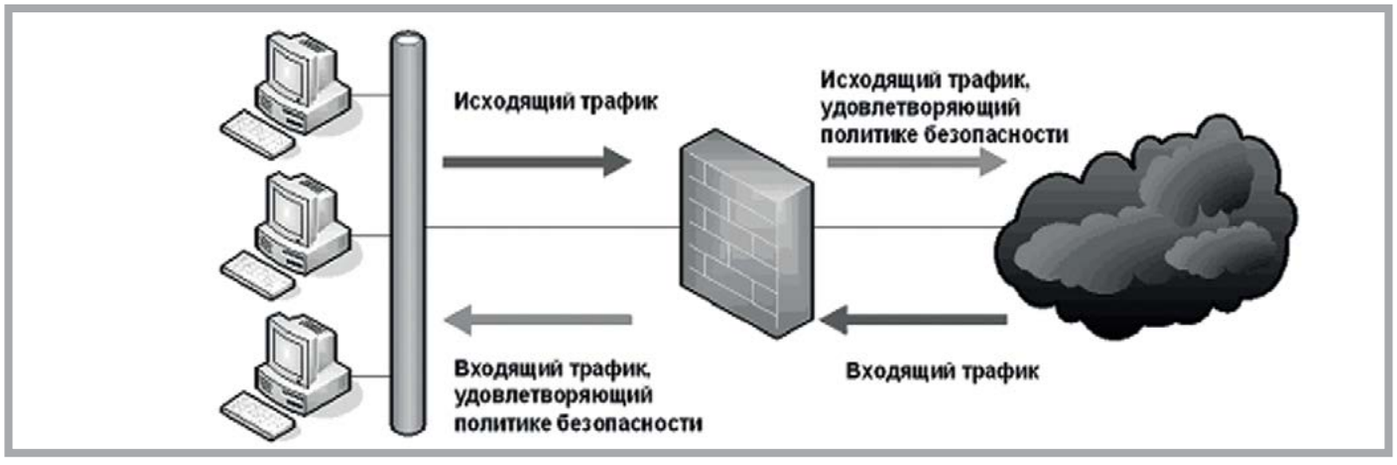


Рис. 1. Контроль параметра сети МЭ (защищаемая сеть слева)

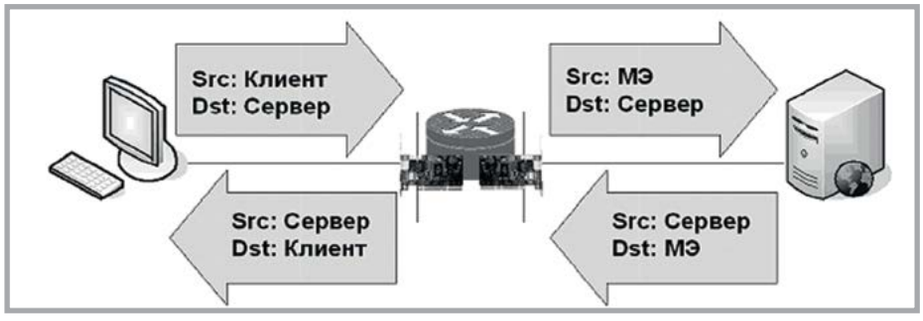


Рис. 2. Технология NAT

(фильтрация информационных потоков), а вторая, наоборот, ему способствует (посредничество в межсетевом взаимодействии). Следует отметить, что выполнение МЭ указанных групп функций может осуществляться на разных уровнях модели OSI. Принято считать, что чем выше уровень модели OSI, на котором МЭ обрабатывает пакеты, тем выше обеспечиваемый им уровень защиты.

Как отмечено выше, МЭ может обеспечивать защиту АС за счет фильтрации проходящих через него сетевых пакетов, то есть посредством анализа содержимого пакета по совокупности критериев u1085 на основе заданных правил и принятия решения о его дальнейшем распространении в (из) АС. Таким образом, МЭ реализует разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного типа между субъектами и объектами. Как следствие, субъекты одной АС получают доступ только к разрешенным информационным объектам другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр. МЭ или один из его компонентов, функционирующий вышеописанным образом, называют пакетным фильтром.

Пакетный фильтр функционирует на сетевом уровне модели OSI. Значимой для функционирования пакетного фильтра информацией является:

- IP-адрес отправителя;
- IP-адрес получателя;
- тип протокола (TCP, UDP, ICMP);
- порт отправителя (для TCP, UDP);
- порт получателя (для TCP, UDP);
- тип сообщения (для ICMP);
- а иногда и другая информация (например, время суток, день недели и т.д.).

В англоязычной литературе рассмотренный компонент МЭ чаще всего обозначают термином «stateless packet filter» или просто «packet filter». Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность АС. Основным недо-

Рис. 3. Маршрутизатор Mikrotik RB/MRTG

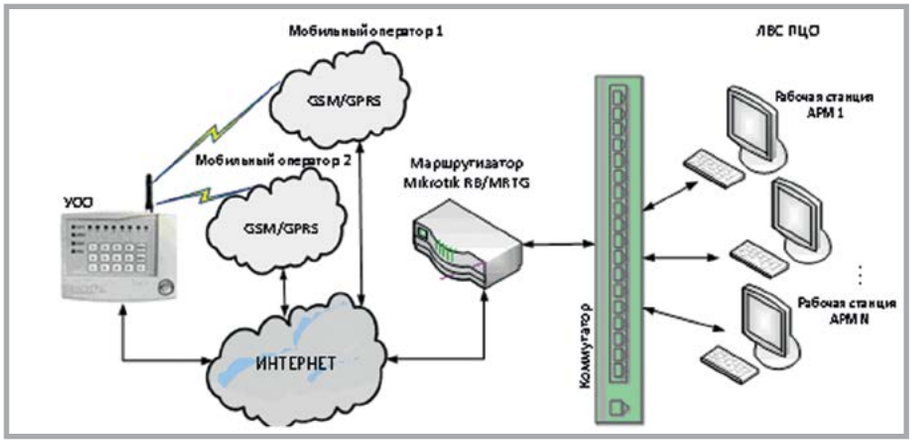


Рис. 4. Типовая схема включения для малого количества охраняемых объектов

статком является их уязвимость при атаке, называемой IP-спуфинг – фальсификации адресов отправителя сообщений. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

При настройке политики межсетевого экранирования рассматривают два аспекта сетевой безопасности: политику доступа к сетевым ресурсам и политику реализации собственно МЭ. Политика доступа к сетевым ресурсам отражает общие требования по безопасности той или иной организации, и при ее разработке должны быть сформулированы правила доступа пользователей к различным сервисам, используемым в организации. Указанные правила описывают, какой внутренний (внешний) пользователь (группа пользователей), когда, с какого внутреннего (внешнего) узла сети и каким сервисом может воспользоваться с уточнением в случае необходимости способов аутентификации пользователей и адресов целевых серверов.

Трансляция сетевых адресов (NAT) — технология, которая позволяет маршрутизатору выполнять функцию прокси-сервера по сокрытию информации об узлах внутренней сети. В целях сокрытия информации о внутренней сети маршрутизатор с NAT функционирует следующим образом:

• при передаче запросов клиентов защищаемой сети во внешнюю сеть заменяет их IP-адреса на IP-адрес своего внешнего интерфейса (может использоваться и диапазон IP-адресов);

• при возврате ответов серверов клиентам производит обратную замену: свой адрес в поле получателя меняет на адрес клиента, отправившего исходный запрос *(рис. 2)*.

Преимущество использования трансляции сетевых адресов состоит в том, что при подключении внутренней сети к сети Интернет технология NAT позволяет существенно увеличить адресное пространство за счет использования IP-адресов из диапазона частных сетей, не обрабатываемых маршрутизаторами интернета.

В зависимости от количества подключенных устройств оконечных – менее 100, от 100 до 1000, более 1000 - рекомендуется выбирать маршрутизаторы низшего, среднего или высшего ценового диапазона. Маршрутизаторы высшего ценового диапазона также следует выбирать при охране объектов, внесенных в

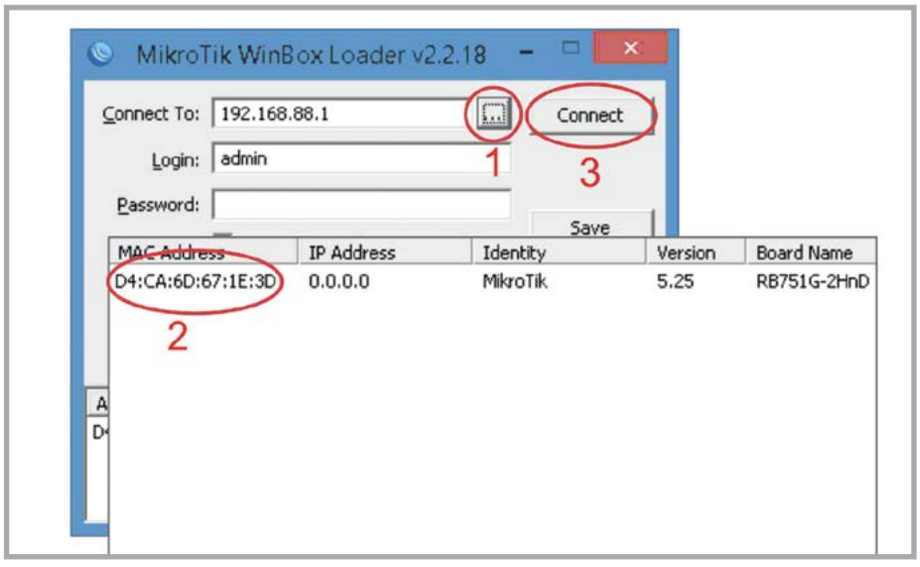


Рис. 5. Подключение к роутеру

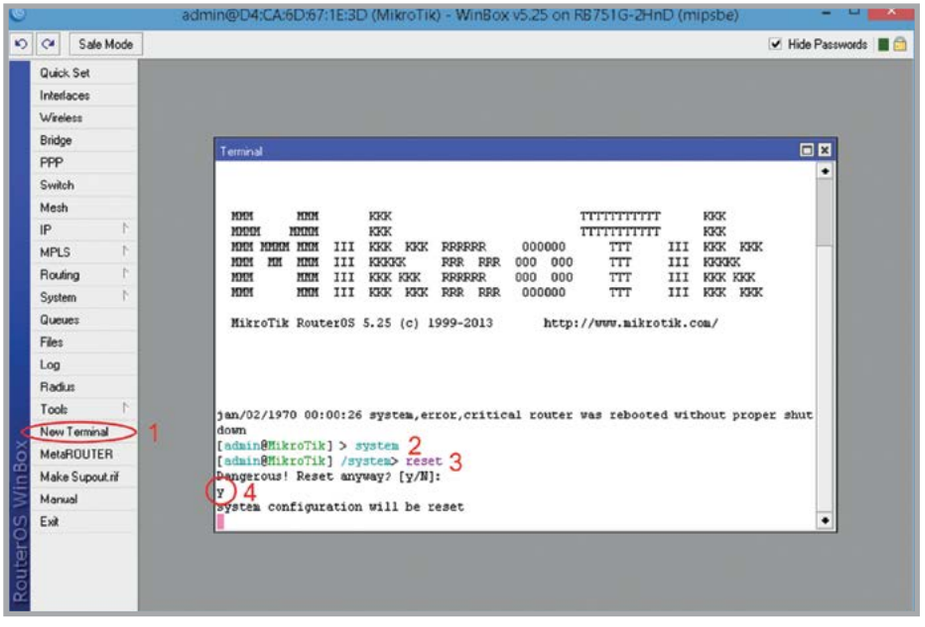


Рис.6. Сброс настроек

«Перечень критически важных объектов РФ» в соответствии с распоряжением Правительства РФ от 23 марта 2006 года №441-РС (в редакции распоряжения Правительства РФ от 18.08.2010 г. № 1361-РС «Об утверждении Перечня критически важных объектов РФ»), а также объектов, внесенных в «Перечень объектов, подлежащих обязательной охране полицией» в соответствии с Распоряжением Правительства Российской Федерации от 10 декабря 2013 года №2324-р.

Марку оборудования для защиты ЛВС ПЦО рекомендуется выбирать из государственного реестра сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 в связи с тем, что:

1. В соответствии с указом Президента РФ от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» « … при необходимости подключения информационных систем … такое подключение производится только с использованием специально предназначенных для этого средств защиты информации … получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для … владельцев … средств вычислительной техники».

2. В соответствии с приказом МВД №734 от 19 сентября 2006 г. «Об утверждении Правил предоставления и использования ресурсов сети «Интернет» в системе МВД России» «Включение технических средств, информационных систем, сетей связи и автономных компьютеров, проводится при обязательном использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических, для подтверждения достоверности информации (антивирусное программное обеспечение, система защиты от несанкционированного доступа, межсетевые экраны и другие средства защиты)».

Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 доступен для ознакомления/скачивания на сайте ФСТЭК по адресу: **http://fstec.ru/tekhnicheskayazashchita-informatsii/dokumenty-posertifikatsii/153-tekhnicheskaya-zashchitainformatsii/dokumenty-po-sertifikatsii/sistema-sertifikatsii/591-gosudarstvennyjreestr-sertifitsirovannykh-sredstv-zashchityinformatsii-n-ross-ru-0001-01bi00**

На сегодня на рынке десятки различных производителей маршрутизаторов. Поскольку тираж этих маршрутизаторов огромен, есть и отзывы в Интернете об их работоспособности. Поэтому надо стараться максимально учитывать практический опыт работы с данными устройствами.

Рассмотрим защиту ЛВС ПЦО на примере маршрутизатора Mikrotik RB/MRTG

Для защиты ЛВС ПЦО с количеством охраняемых объектов менее 1000 рекомендуется использовать недорогой маршрутизатор Mikrotik RB/MRTG *(рис.3)*.

Этот маршрутизатор — оптимальное решение для построения мелких и средних гигабитных сетей. Мощный сетевой процессор Atheros AR7161 и пять портов Ethernet позволяют использовать RB/MRTG в качестве высокопроизводительного маршрутизатора, брандмауэра, а также эффективно управлять полосой пропускания. Устройство имеет гибкую функциональность, которой удобно пользоваться с помощью удобного графического интерфейса.

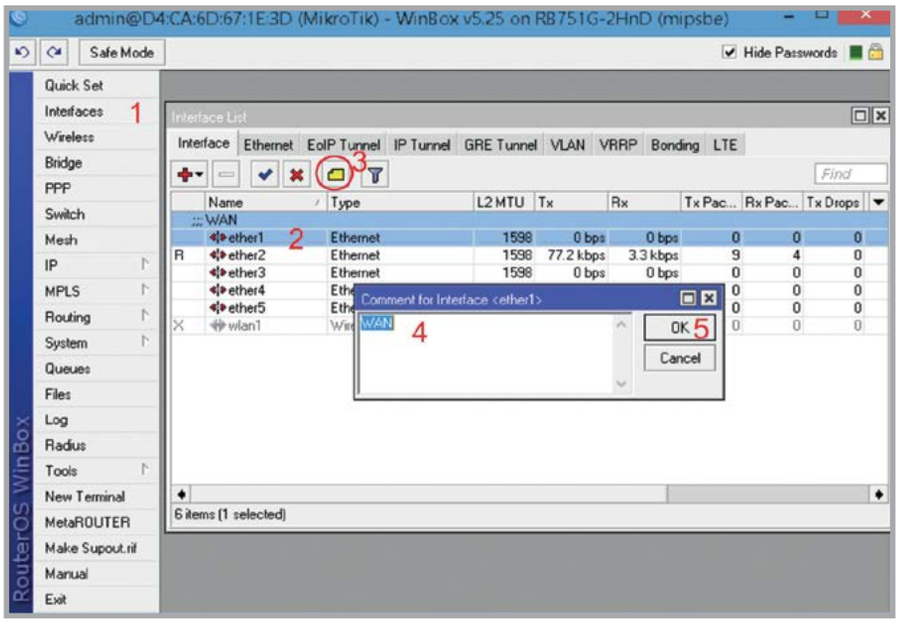


Рис. 7. Сетевые интерфейсы

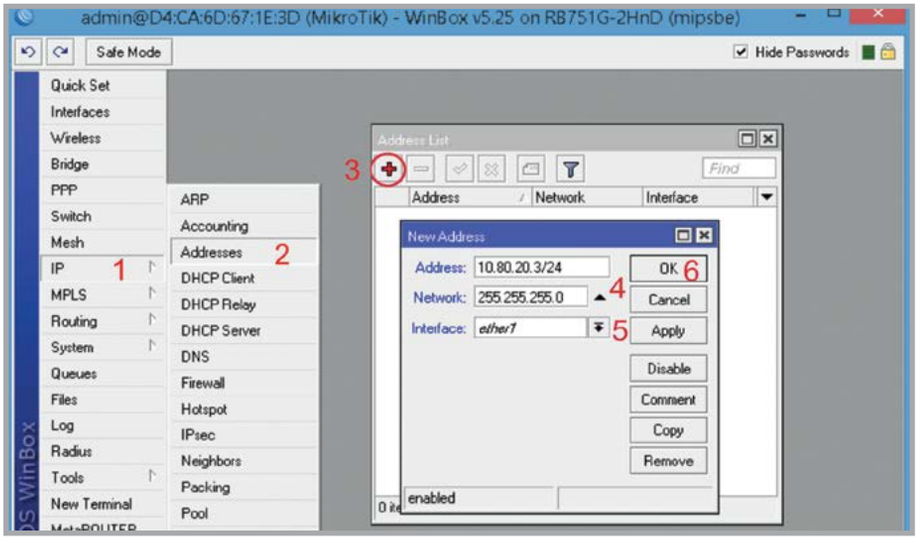


Рис.8. Статический IP адрес и маска подсети WAN порта

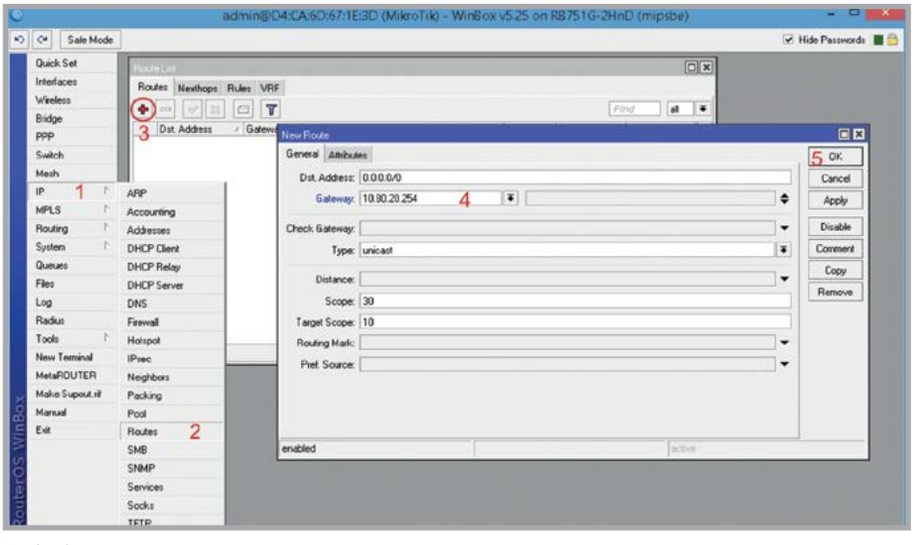


Рис.9. Адрес интернет-шлюза

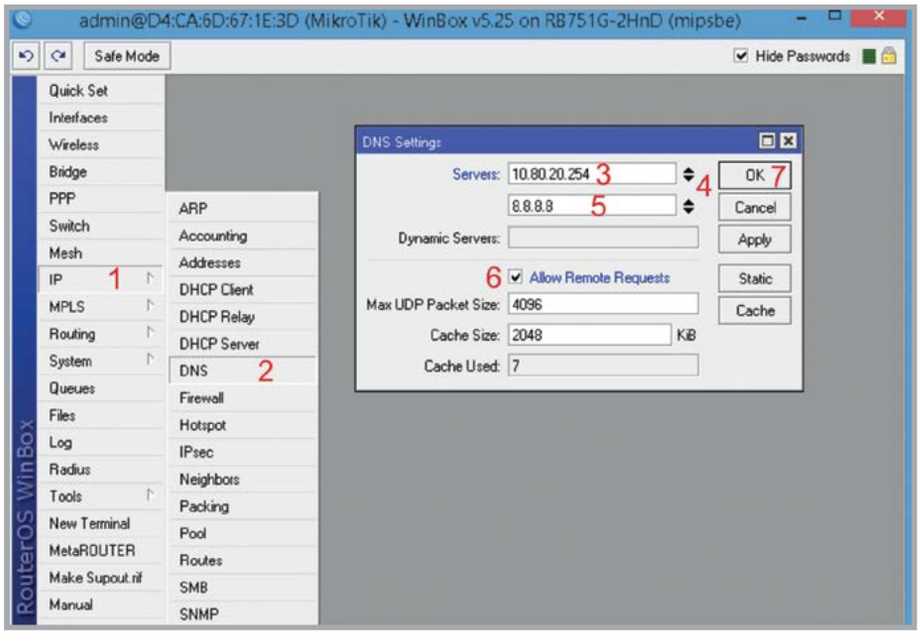


Рис. 10. Адрес DNS-серверов

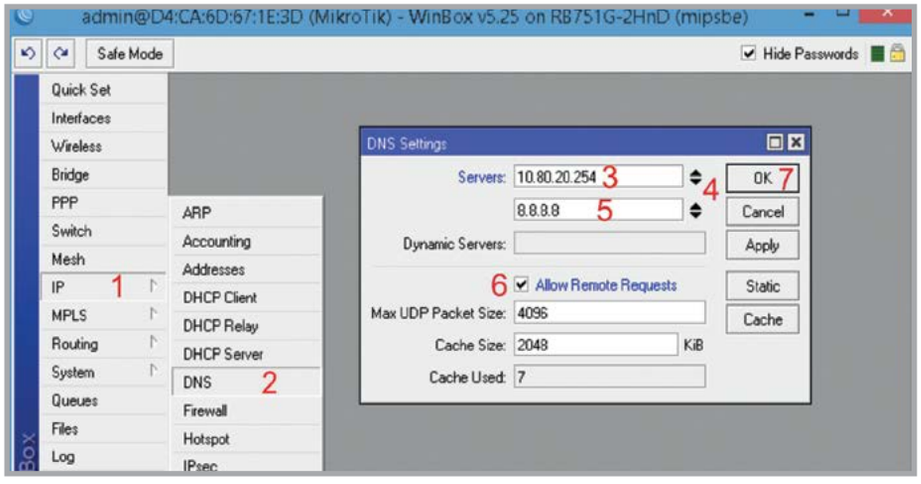


Рис. 11. Подключение через PPPoE

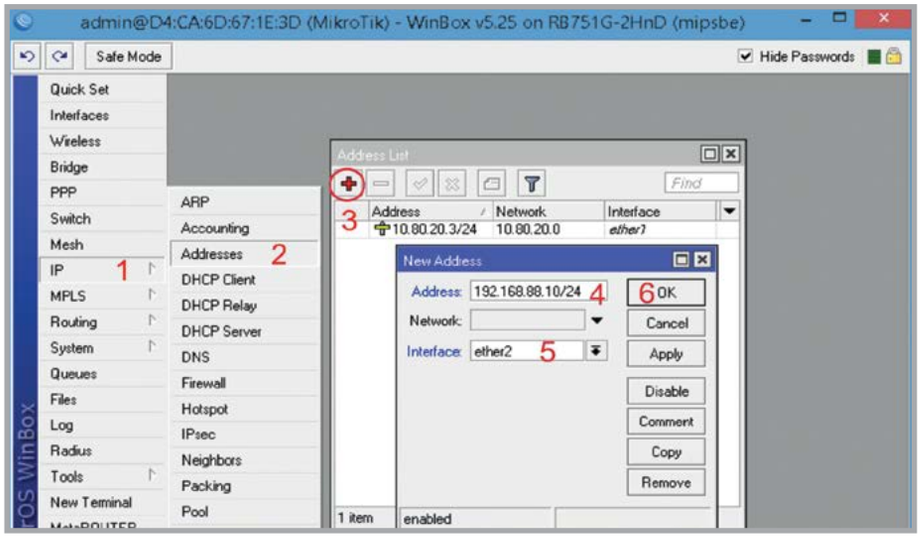


Рис. 12. IP-адрес локальной сети

Интерфейс имеет множество приятных особенностей: применение настроек без перезагрузки, встроенные средства диагностики сети, реалтайм-отображение текущего состояния маршрутизатора (сетевых интерфейсов, правил маршрутизации и т.п.). Для сложных задач имеется встроенный скриптовый интерпретатор с развитыми сетевыми функциями.

Благодаря использованию специализированного ПО (операционная система Linux) система имеет низкие аппаратные требования, что в совокупности с мощными сетевыми процессорами дает высокое быстродействие, малую потребляемую мощность.

Типовая схема включения для малого количества охраняемых объектов приведена на *рисунке 4*. В данной схеме организуется один основной канал связи для подключения ПЦО к интернету. Кабель провайдера подключается в первый Ethernet-порт (ether1) роутера. Кабель от коммутатора ЛВС ПЦО подключается во второй Ethernet-порт (ether2) роутера. Компьютер для настройки роутера подключается в третий (ether3) или четвертый Ethernet-порт (ether4) роутера.

В зависимости от того, каким способом осуществляется подключение к провайдеру, надо получить от него следующие данные:

1. **PPPoE** — надо знать пару: **Логин и пароль.**
2. **DHCP** — ничего не надо, т.к. настройки роутер получит автоматически.
3. **DHCP + MAC** — надо знать MAC-адрес устройства, который ранее выступал в роли роутера, или MAC-адрес на ПК Windows (это можно узнать командой **Пуск ⊠ Выполнить ⊠ cmd;** в черном окне набрать **ipconfig /all**).
4. **StaticIP** — надо знать статический IP-адрес, маску подсети, шлюз и 2 DNS.

После настройки соединения можно проверить, что есть доступ к интернету, при помощи команды ping, например ping ya.ru. Если соединение настроено правильно, будут отображены ответы на запрос ping.

Для обеспечения безопасности необходимо отключить все ненужные сервисы, например telnet, ftp, www, www-ssl, ssh, api. Указать конкретный адрес компьютера, с которого будет запускаться программа конфигурирования, например Winbox.

Необходимо из руководства по экс-

плуатации на СПИ определить, какой порт и протокол используются для соединений АРМ с приборами. Например, для СПИ «Приток-А» используются 40000 порт и протокол UDP. В соответствии с этими данными настроить проброс портов и прохождение пакетов по порту в правилах файрвола по порту ether1.

Пример настройки маршрутизатора Mikrotik

Настройку роутера будем осуществлять через специализированное ПО для семейства ОС Windows – Winbox. Программу Winbox можно загрузить из сети Интернет на сменный носитель и перенести на ПК, с которого будет осуществляться настройка. Или скачать при первом подключении к роутеру через WEB-интерфейс.

Подключаемся к роутеру MikroTik, запустив программу Winbox:

1. Нажимаем кнопку <...> для отображения устройств MikroTik;
2. Выбираем в списке наш роутер;
3. Нажимаем кнопку **Connect**.

Login по умолчанию **admin**, пароль пустой.

Обратите внимание, что при пустой конфигурации роутера на его интерфейсах **нет IP-адреса,** поэтому обращаться к нему из окна выбора утилиты Winbox необходимо через MAC-telnet, кликнув мышкой именно на **MAC-адресе** роутера *(пункт 2 на рис. 5).*

B.2. Начальные настройки

Сбросим все настройки роутера MikroTik через программу Winbox:

1. Выбираем слева меню **New Terminal** *(рис. 6);*
2. В терминале вводим команду **system**;
3. Потом вводим команду **reset**;
4. Нажимаем кнопку Y на клавиатуре для подтверждения сброса настроек.

После перезагрузки устройства заходим еще раз в настройки MikroTik с помощью программы Winbox. В появившемся окне нажимаем кнопку **Remove Configuration** и ждем, пока роутер перезагрузится.

Конфигурация интерфейсов

Для стандартной схемы подключения охранных приборов определим сеть следующим образом: первый порт будет подключен к провайдеру (WAN-порт), остальные порты будут работать в режиме свитча для подключения компьютеров локальной сети. В качестве примера будем разбирать роутер 751 серии. Также добавим еще одного провайдера на порт 5.

Чтобы не путать сетевые интерфейсы, опишем их с помощью комментариев. Записываем для первого порта ether1 комментарий «WAN» (или, например — Ростелеком).

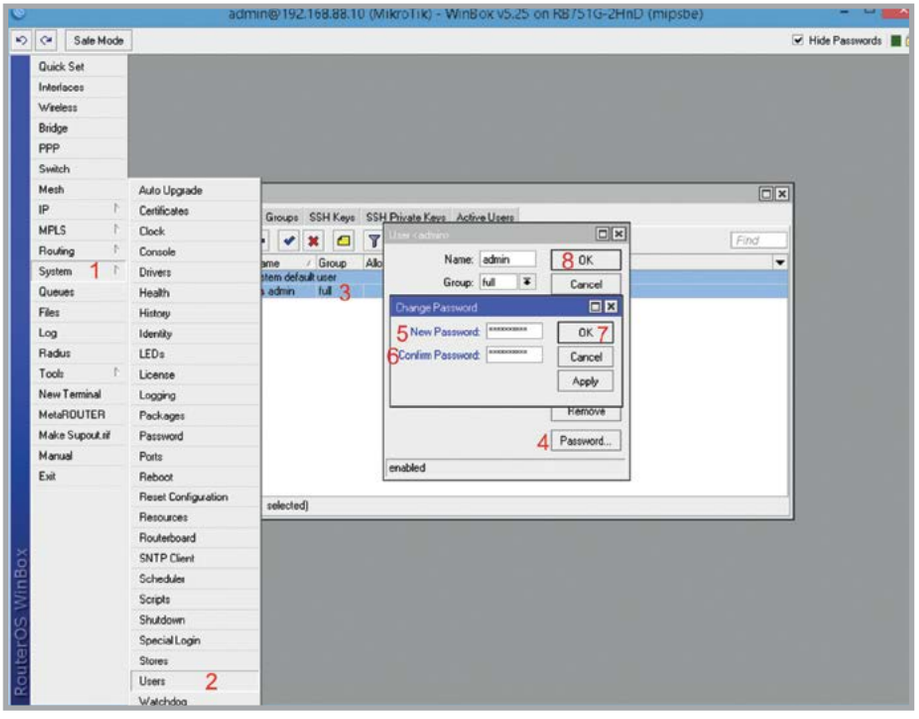


Рис. 13. Пароль доступа

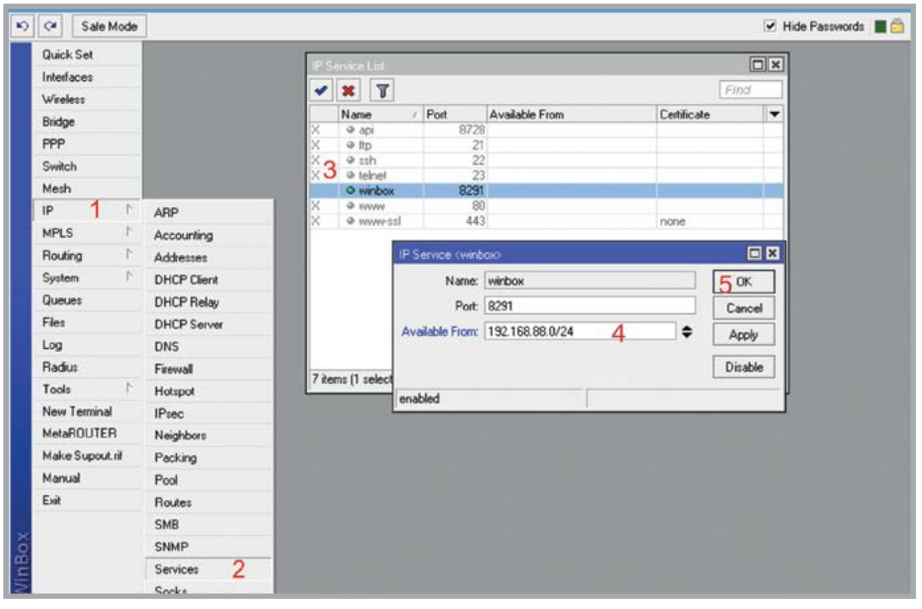


Рис. 14. Отключение ненужных сервисов

1. Открываем меню **Interfaces** *(рис. 7).*
2. Выбираем первый интерфейс **ether1.**
3. Нажимаем желтую кнопку **Comment.**
4. В появившемся окне вводим комментарий **«WAN».**
5. Нажимаем кнопку **OK**.

Аналогичным образом записываем для второго порта ether2 комментарий «LAN».

Настройка WAN-интерфейса

Если провайдер предоставляет интернет

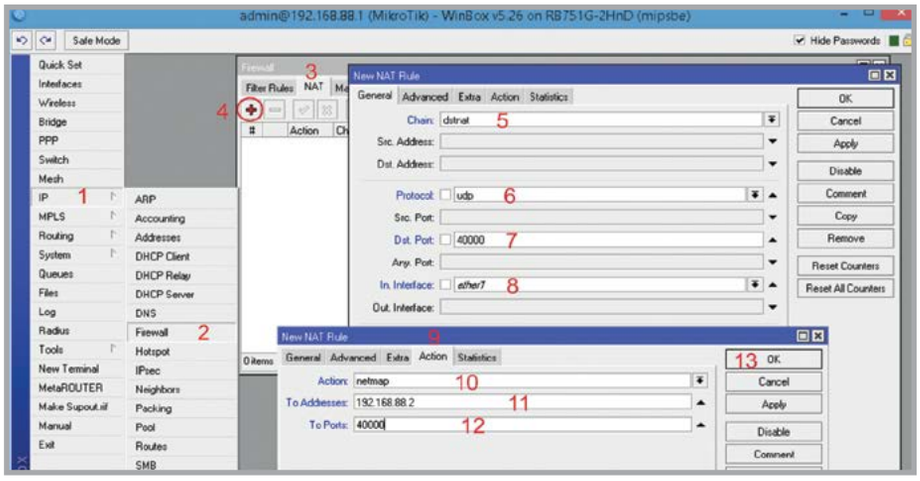


Рис. 15. Проброс портов

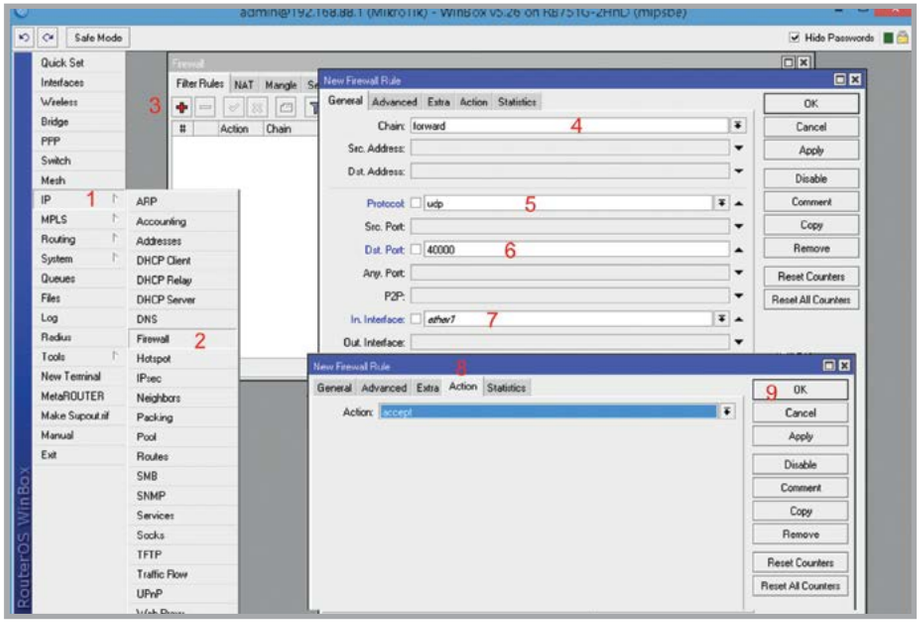


Рис. 16. Правила файрвола

с привязкой по MAC, то произведем данную настройку. Чтобы изменить MAC-адрес порта MikroTik, открываем в программе Winbox меню **New Terminal** и вводим команду: **/interface ethernet set ether1 mac-address=00:01:02:03:04:05**, где **ether1-** имя WAN- интерфейса, **00:01:02:03:04:05 –** необходимый MAC-адрес.

Чтобы восстановить начальный MAC-адрес порта, вводим команду: **/interface ethernet reset-mac ether1**

Если провайдер предоставляет интернет по конкретному адресу в сети, настроим статический IP-адрес и маску подсети WAN-порта.

1. Открываем меню **IP** *(рис. 8)*.
2. Выбираем **Addresses.**
3. В появившемся окне нажимаем кнопку Add (красный плюс).
4. В новом окне в поле **Address**: прописываем статический **IP-адрес / маску подсети.**
5. В списке **Interface**: выбираем WAN-интерфейс **ether1.**
6. Для сохранения настроек нажимаем кнопку **OK**.

Настроим адрес интернет-шлюза.

1. Открываем меню **IP** *(рис. 9)*.
2. Выбираем **Routes.**
3. В появившемся окне нажимаем кнопку Add (красный плюс).
4. В новом окне в поле **Gateway**: прописываем **IP-адрес шлюза.**
5. Нажимаем кнопку **OK** для сохранения настроек.

Добавим адреса DNS-серверов.

1. Открываем меню **IP** *(рис. 10)*.
2. Выбираем **DNS.**
3. В новом окне в поле **Servers**: прописываем IP-адрес DNS-сервера.
4. Нажимаем кнопку «вниз» (черный треугольник), чтобы добавить еще одно поле для ввода.
5. В новом поле прописываем IP-адрес альтернативного DNS-сервера.
6. Ставим галочку **Allow Remote Requests.**
7. Нажимаем кнопку **OK** для сохранения настроек.

В случае если подключение провайдера осуществляется с помощью PPPoE-клиента (например, после ADSL-модема в режиме моста):

Подключение через PPPoE.

1. Выберем пункт **PPP** *(рис. 11)*.
2. В появившемся окне нажимаем Add (красный плюс) выбираем из списка **PPPoE client.**
3. На вкладке **General** даем имя соединению.
4. Указываем интерфейс, который подключен (например к модему ADSL).
5. Переходим на вкладку **Dial-Out.**
6. Заносим логин и пароль, выданный провайдером.
7. Ставим галочку напротив **Use Peer DNS** — использовать службы имен.
8. Выбираем типы шифрования, которые использует провайдер.
9. Нажимаем кнопку **OK**. (можно проконтролировать состояние внизу слева - status)

Настроим IP-адрес локальной сети:

1. Открываем меню **IP** *(рис. 12)*.
2. Выбираем **Addresses.**
3. В появившемся окне нажимаем кнопку Add (красный плюс).
4. В поле **Address** вводим адрес и маску локальной сети, например 192.168.88.10/24.
5. В списке **Interface** выбираем интерфейс **ether2.**
6. Нажимаем кнопку **OK**.

Чтобы изменить пароль доступа к роутеру, выполните следующие действия.

1. Открываем меню **System** *(рис. 13)*.
2. Выбираем **Users.**
3. Делаем двойной клик кнопкой мыши на пользователе **admin.**
4. Нажимаем кнопку **Password...**
5. В поле **New Password** вводим новый пароль.
6. В поле **Confirm Password** подтверждаем новый пароль.
7. В окне **Change Password** нажимаем кнопку **OK.**

8. В окне **User** нажимаем кнопку **OK**.

Для обеспечения безопасности отключаем ненужные сервисы и разрешаем доступ Winbox только из локальной сети.

1. Открываем меню **IP** *(рис. 14)*.
2. Выбираем **Services.**
3. Отключаем все ненужные сервисы кроме Winbox.
4. Делаем двойной клик мыши на строчке сервиса Winbox и на вкладке **Available From** указываем конкретный адрес сети или ПК, с которой будет запускаться Winbox.
5. Нажимаем кнопку **OK**.

Настройка NAT

Для работы с охранными приборами необходимо создать проброс портов.

1. Открываем меню **IP** *(рис. 15)*.
2. Открываем **Firewall**.
3. Открываем вкладку **NAT.**
4. В появившемся окне нажимаем кнопку Add (красный плюс).
5. Цепочка — **dstnat.**
6. Протокол — **udp** – для работы приборов, например Приток.
7. Порт для соединений от приборов — **40000** (или тот, который используется).
8. Входящий интерфейс — **ether1** – интернет от провайдера.
9. Переходим на кладку **Action.**
10. Действие — **netmap.**
11. Адрес ПК с сервером подключений в локальной сети.
12. Порт, на который делаем проброс.
13. Нажимаем кнопку **OK**.

Также разрешаем прохождение пакетов по порту в правилах файрвола.

1. Открываем меню **IP** *(рис. 16)*.
2. Открываем **Firewall.**
3. В появившемся окне нажимаем кнопку Add (красный плюс).
4. Цепочка **forward** – проходящее через роутер.
5. 6. 7. Протокол, порт и интерфейс внешний — куда приходит прибор.
8. На вкладке **Action** проверяем, что значение — **accept** – разрешено.
9. Нажимаем **OK**.

Можно подключать несколько провайдеров и распределять нагрузку между сетями. Для этого можно применять два простых варианта распределения трафика: 1 — основной провайдер работает, при аварии переключаемся на следующего; 2 — все провайдеры работают вместе с распределением нагрузки.

Сначала настройку второго порта производим так же, как и первого — в зависимости от типа. Задаем необходимые настройки, так же, как и делали с первым WAN. Для корректной работы с несколькими провайдерами нам необходимо промаркировать-пометить пакеты для использования данных меток в цепочках маршрутизации.

Создаем правила NAT для прохождения пакетов провайдеров — в данном случае для двух — для каждого интерфейса. Теперь интернет может работать через двух провайдеров. Для определения маршрута соединения маркируем их в роутере. Указываем метку-имя данного соединения — уникальное для интерфейса. Для каждого интерфейса описываем правило и присваиваем метку. Создаем ДВА правила — для двух портов для входящего трафика. И так же создаем ДВЕ цепочки, маркируя трафик соответственно нашим меткам. В итоге у нас получилось **4 правила** — два для маркировки соединений и два для маркировки маршрутизации — для каждого провайдера.

Для первого варианта маршрутизации — с резервированием канала — нам необходимо добавить к существующей системе правило подмены маршрутов. В случае одновременной работы обоих провайдеров — необходимо удалить запись о шлюзе по умолчанию **«add default route=no»** и создать маршрутизацию сразу с двумя шлюзами.

Чтобы сбросить MikroTik к заводским настройкам, выполните следующее.

1. Отключите питание роутера.
2. Нажмите и держите кнопку **Reset.**
3. Включите питание роутера.
4. Дождитесь, пока замигает индикатор **ACT,** и отпустите кнопку **Reset**.

После этого роутер перезагрузится и вы сможете зайти в его настройки со стандартным именем пользователя **admin** без пароля.

На этом начальная настройка роутера завершена. Для более подробной и точной настройки под определенные параметры или потребности необходимо изучить документацию. Например:

- Вики (база знаний) по Микротик (http://wiki.mikrotik.com/wiki/Заглавная_страница)
- Документация от дистрибьютора (http://mikrotik.ru/files/instrukcii-ponastrojke-mikrotik)
- Перевод руководства на роутер (http: //www.mikrotik.ru/ftpgetfile.php?id=13&module=files)

Заключение

Ознакомившись с описанными проблемами, можно сделать вывод, что межсетевые экраны обеспечивают защиту компьютерной сети ПЦО от несанкционированного вмешательства. Межсетевые экраны являются необходимым средством обеспечения информационной безопасности. Они обеспечивают первую линию обороны. При выборе и приобретении межсетевых экранов необходимо тщательно все продумать и проанализировать. Выбрать нужную архитектуру и компоненты межсетевого экрана. Правильно настроить программное обеспечение и тестировать конфигурацию межсетевого экрана.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля2008 г.

2. Указ Президента РФ № 351 от 17марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

3. Приказ МВД № 734 от 19 сентября 2006 г. «Об утверждении Правил предоставления и использования ресурсов сети «Интернет» в системе МВД России».

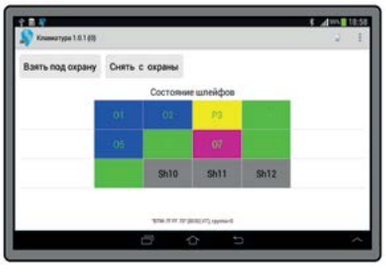
4. Распоряжение Правительства РФ от 23 марта 2006 года №441-РС (в редакции распоряжения Правительства РФ от 18.08.2010 г. № 1361-РС «Об утверждении Перечня критически важных объектов РФ»).

приток

Каталог

- **Пульты централизованного наблюдения**
- **Программное обеспечение АРМ ПЦН**

Новинки ПО
Приток-Охрана-WEB
Охрана Приток-А
Экипаж Приток-А
Трекер Приток-А
Клавиатура Приток-А



В данном разделе представлена информация, раскрывающая общее назначение, структуру и особенности всех подсистем ИС Приток-А

Информация, приведенная в данном разделе, не является документацией и носит только рекламно-информационный характер

Технические характеристики и правила эксплуатации отдельных компонентов и подсистем ИС «Приток-А» указаны в паспортах и руководствах по эксплуатации на конкретные программные и аппаратные руководства

ОП 066 ОС 03 Охрана ССС Минсвязи России

Пульты централизованного наблюдения (ПЦН)

на основе Интегрированной системы охранно-пожарной сигнализации Приток-А

ИС ОПС Приток-А

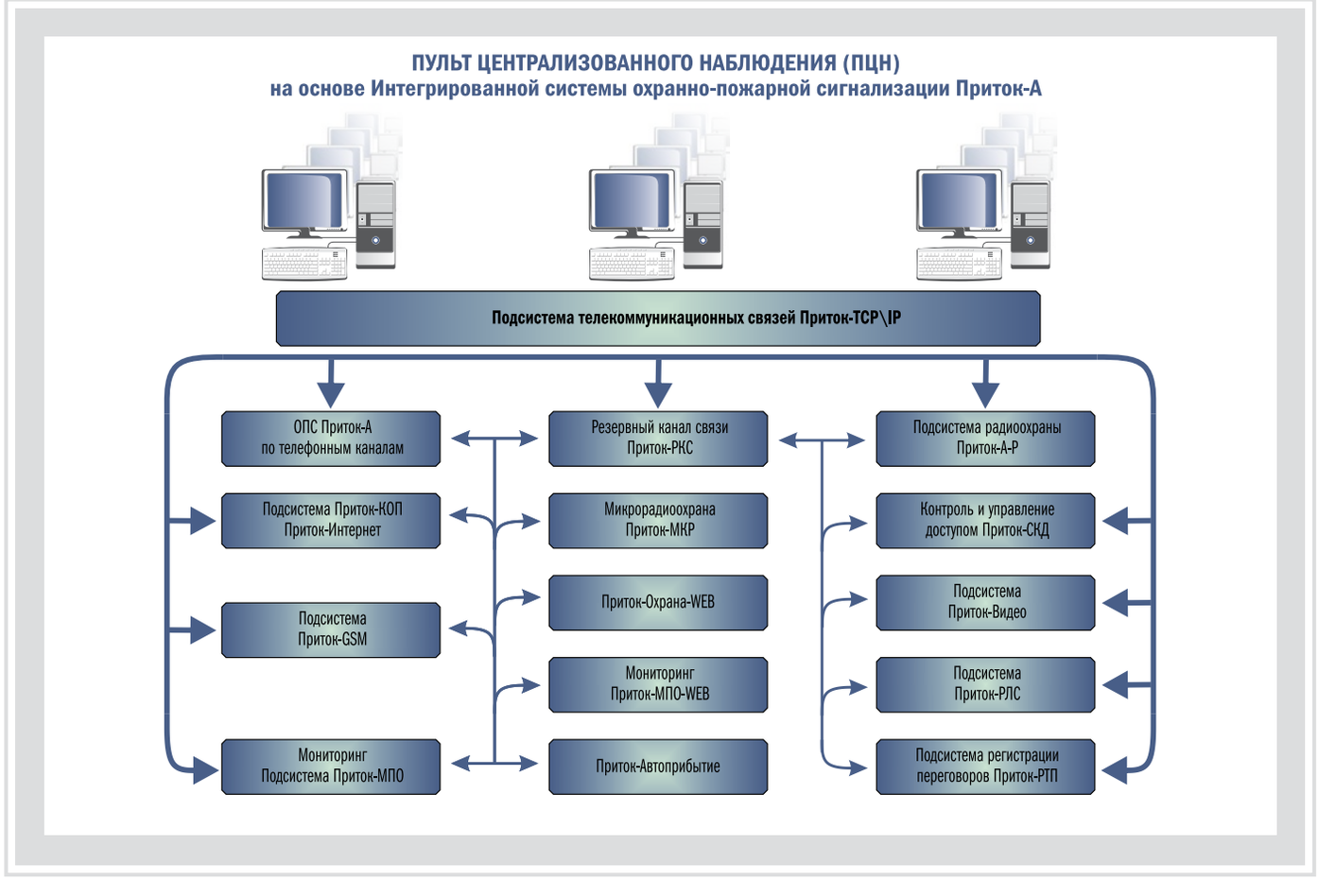
Интегрированная система охранно-пожарной сигнализации Приток-А (в дальнейшем просто — система ИС Приток-А), созданная иркутскими специалистами, в настоящее время успешно функционирует в более чем 50 регионах России, а также в Казахстане и Узбекистане.

Система Приток обеспечивает:

- охрану стационарных и мобильных объектов. При этом количество объектов, транспортных средств и территория их расположения практически не ограничены
- 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), так как уровень ее надежности и защищенности 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 расчета, техники по обслуживанию и т. д.) и только на реально произошедшие события.

ИС Приток-А соответствует «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны», разработанным и утвержденным ГУВО МВД России в 2012 году.



С пультов централизованного наблюдения (ПЦН) ИС Приток-А 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. Все это позволяет своевременно обнаружить возникшую неисправность, принять меры по восстановлению работоспособности элементов системы. Для надежности 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 136-174 и 430-470 МГц**
- **УКВ-радиоканалы безлицензионных диапазонов частот 433,075-434,750**
- **Высокоскоростные цифровые каналы передачи данных, работающие с применением протоколов TCP/IP и UDP, в том числе через оптоволоконные линии связи, VPN сети и каналы открытого Интернета**
- **Каналы сотовой связи стандарта GSM, 3G и 4G**

Программное обеспечение ИС Приток-А позволяет строить как локальные, так и распределенные, высокопроизводительные системы охранно-пожарной сигнализации, контроля и управления доступом, мониторинга подвижных объектов, видеонаблюдения, объединенные 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 начинать строиться на базе одного ПК и развиваться до сотен используемых рабочих мест, обеспечивая универсальную и масштабируемую структуру ПЦН.

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-TCP/IP) — для создания сети ПЦН. Приток-TCP/IP обеспечивает передачу извещений и команд управления между элементами системы по цифровым каналам передачи данных. Подсистема позволяет реализовать взаимодействие локальной вычислительной сети АРМ пользователей системы с техническими средствами безопасности, включенными в состав ИС Приток-А, расположенными в любой точке распределенных сетей предприятий (WAN) и (или) глобальных сетей (типа VPN), независимо от физической среды передачи данных.

2. Подсистема охранно-пожарной сигнализации (ОПС Приток-А) — для организации автоматизированной централизованной охраны стационарных объектов по физическим двухпроводным, выделенным или занятым телефонным линиям связи.

3. Подсистема резервного канала связи (Приток-РКС) — для создания резервного канала передачи команд и сообщений до ПЦН с использованием сетей Ethernet и GSM.

4. Подсистема радиоохраны (Приток-А-Р) — для централизованной охраны по лицензионному УКВ-радиоканалу. Так как и в БМ на ПЦН и в РПДУ на объектах устанавливаются приемопередатчики, 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.

5. Подсистема охраны через открытый интернет (Приток-Интернет) — для организации централизованной охраны через открытый интернет. Приборы Приток-КОП работают с применением двустороннего имитостойкого протокола, защищенного 128-разрядным динамическим кодом. Для реализации резервных каналов связи на ПЦН могут использоваться другие подключения в сеть Интернет (через других провайдеров) и (или) каналы связи через сеть GSM в режиме GPRS.

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

7. 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.

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

9. 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». Передача информации с БК на БМ производится как по УКВ-радиоканалу (136-174 и 430-470 МГц), так и по каналам сотовой связи стандарта GSM, в режимах SMS-сообщений и GPRS.

10. 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.

11. Подсистема регистрации телефонных и радиопереговоров (Приток-РТП) — для записи аудиоинформации с различных каналов на жесткий диск компьютера, поиска и воспроизведения ее по заданным параметрам, организации системы оповещения.

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 надежность работы системы, способствует её дальнейшей модернизации и развитию.

Структура ИС Приток-А такова, что один ПЦН, созданный на ее 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.

ОСОБЕННОСТИ СОЗДАНИЯ ПЦН

Для описания всевозможных способов построения ИС Приток-А и ее отдельных подсистем воспользуемся самым наглядным способом, то есть изображением и рассмотрением структурных схем отдельных подсистем.

За 25 лет, 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 обобщенную структурную схему системы Приток-А в полном объеме не представляется возможным. Для этого потребуется слишком много места и времени.

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 вместе с вами, уважаемый читатель, поставили себе задачу построения различных ПЦН на основе элементов и подсистем ИС Приток-А.

С чего начать?

1. Начнем с самого необходимого: создадим основу, то есть ПЦН для инсталляции программного обеспечения ПО ИС Приток-А без привязки к какой-либо конкретной подсистеме. А затем представим обобщенные структурные схемы ПЦН для всех подсистем ИС Приток-А.

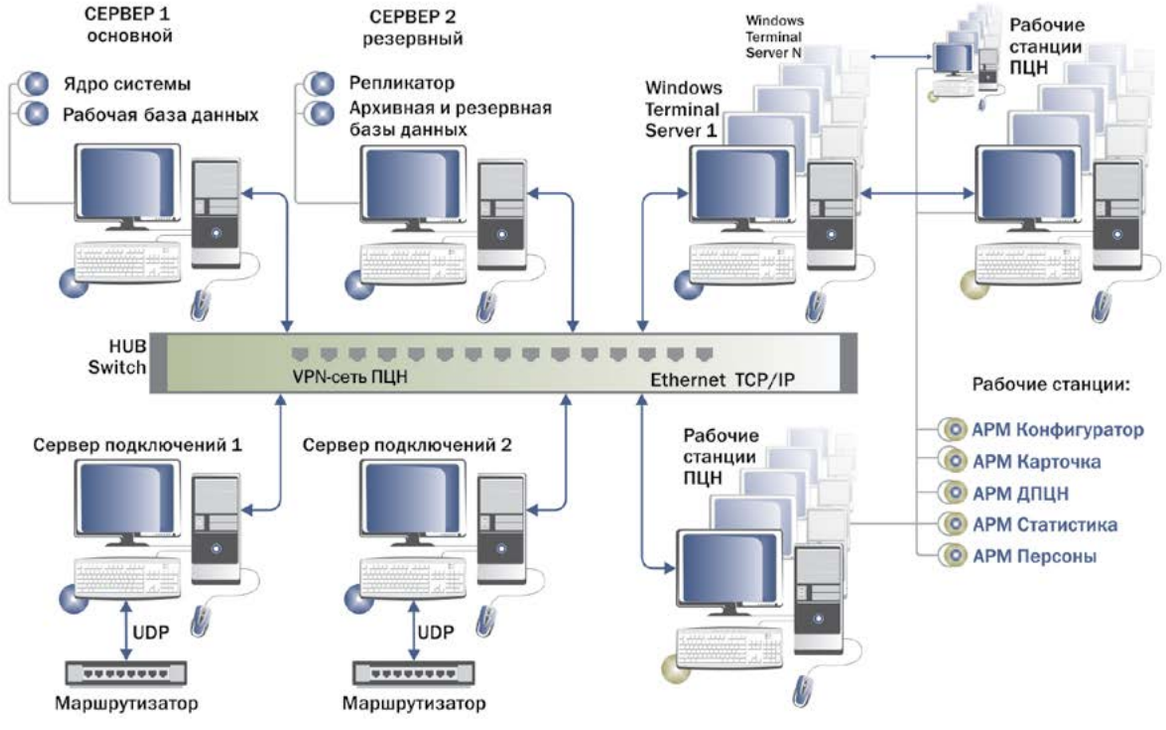
Как мы уже говорили, количество компьютеров в составе ПЦН не ограничено. Для достижения необходимой производительности и надежности целесообразно использовать на ПЦН как минимум два компьютера с разделением функций серверов и рабочих станций. На рабочих станциях могут запускаться различные пользовательские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

Рекомендуемая (оптимальная) схема организации сети современного пульта централизованного наблюдения, позволяющего в дальнейшем использовать все возможности ИС Приток-А, приведена на Рис. 1. Хотя и сервер, и рабочую станцию можно запустить на одном компьютере, мы приводим максимальную структуру сети ПЦН. В конечном счете все зависит от необходимого уровня надежности и количества объектов, которые надо подключить к ПЦН для охраны.

Таким образом, мы создали основу 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 все возможные варианты подключения рабочих станций (АРМ).

Рис. 1

Структурная схема сети ПЦН ИС Приток-А



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. 2.

Сервер Подключений подключается через маршрутизаторы в открытый Интернет. Для надежности подключаемся не к одному, а к двум провайдерам. Каждый провайдер в этом случае выдает свой статический IP-адрес. Подключение сети ПЦН может также быть сделано и через мобильный интернет операторов сотовой связи. Для надежности 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 TCP-модулями, Коммуникаторы TCP/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 WEB-ресурсов, устанавливается маршрутизатор «бытового» уровня — Dlink DIR-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 надежностью 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, ее 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 надежности работы

Рис. 2 Структурная схема сети ПЦН ИС Приток-А для работы через VPN-сети и Интернет

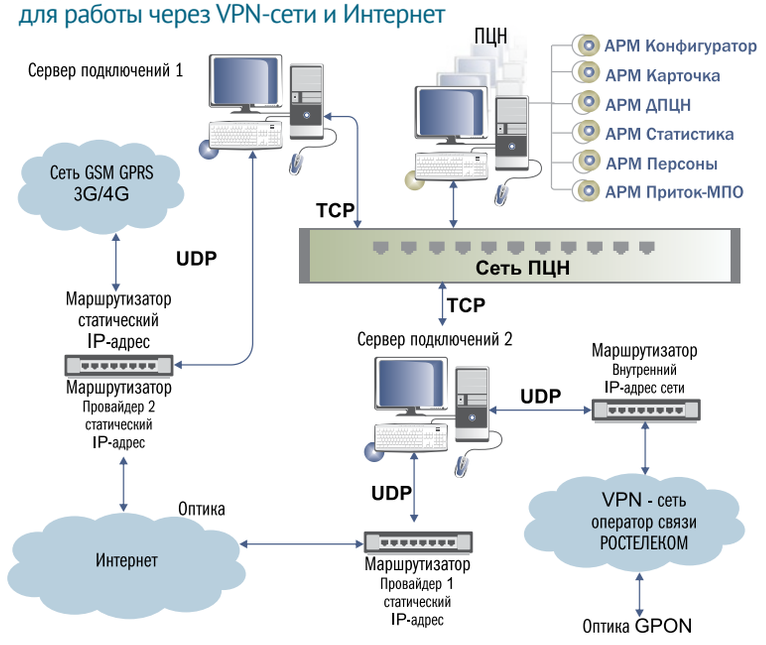
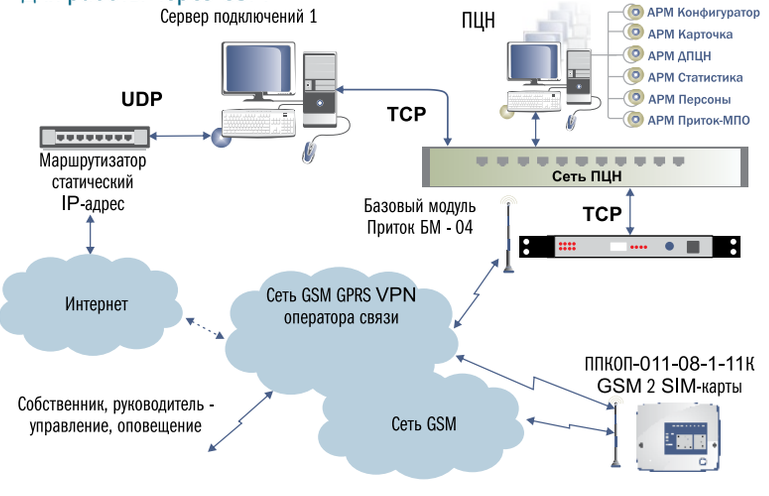


Рис. 3 Структурная схема сети ПЦН ИС Приток-А для работы через GSM



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).

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. 4).

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, это современная серия ППКОП, имеющая встроенные коммуникаторы TCP/IP. Для подключения к такому ПЦН могут применяться коммуникаторы Приток-TCP/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. Причем система охраны может быть построена путем 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. 5). Эта схема наиболее распространенная среди сотен действующих в России ПЦН. 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 приемопередатчиков УКВ-диапазонов 136-174 или 430-470 мгц можно создать подсистему радиоохраны Приток-А-Р. То есть 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. 6.). 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 трех радиоретрансляторов.

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

Рис. 4 Структура сети ПЦН с использованием только подсистемы Приток-TCP/IP

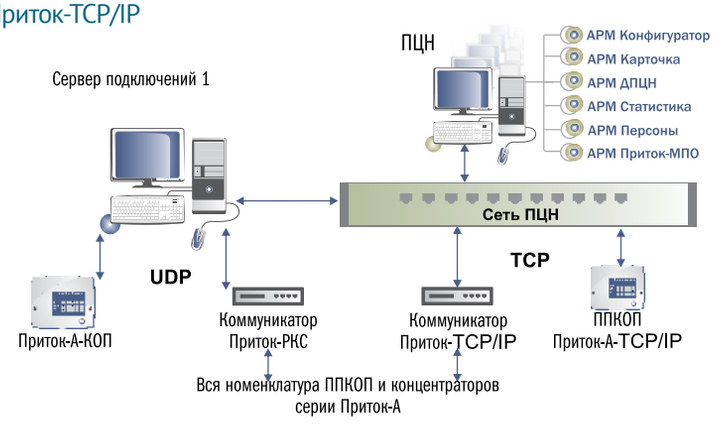


Рис. 5 Структура сети ПЦН с использованием телефонных каналов связи

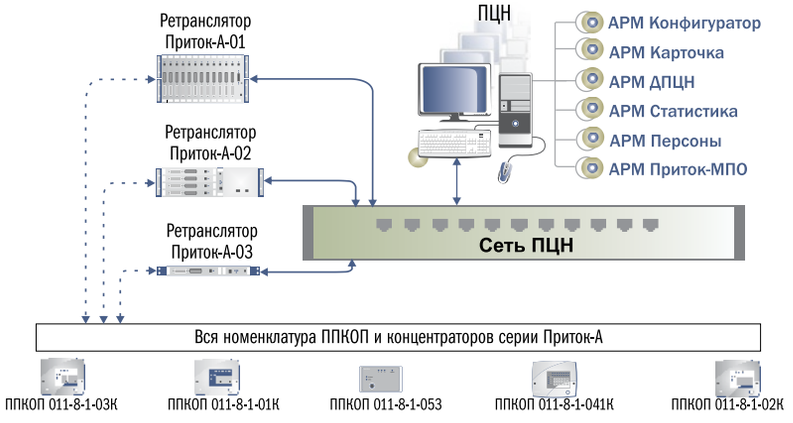
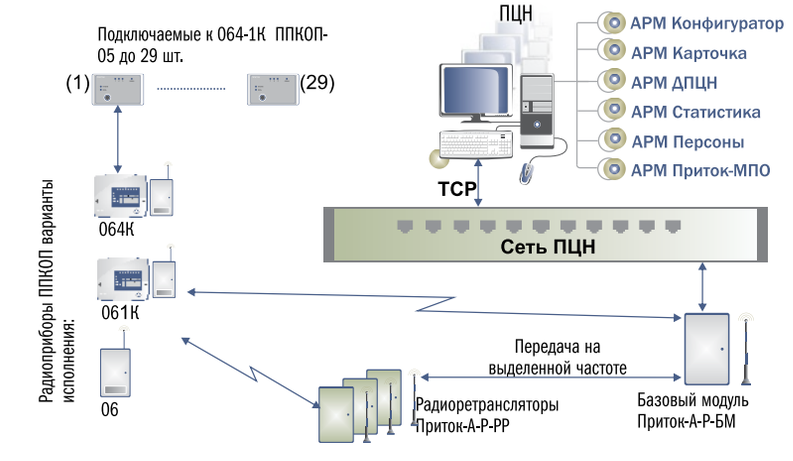


Рис. 6 Структура сети ПЦН с использованием УКВ радиоканала



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

7. Для беспроводного наращивания (удлинения связи) вышерассмотренных схем ПЦН ИС Приток-А создадим подсистему микрорадиоохраны Приток-МКР. Она создается путем использования аппаратуры на основе трансиверов (приемопередатчиков) мощностью не более 10 мВт (см. Рис. 7). 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.

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 подключен 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 создается на основе одного и того же ПЦН и программного обеспечения. Для этого в состав ПЦН дополнительно устанавливается (генерируется) еще 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. 8).

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, то есть 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.

Рис. 7 ПЦН с применением безлицензионного диапазона радиочастот

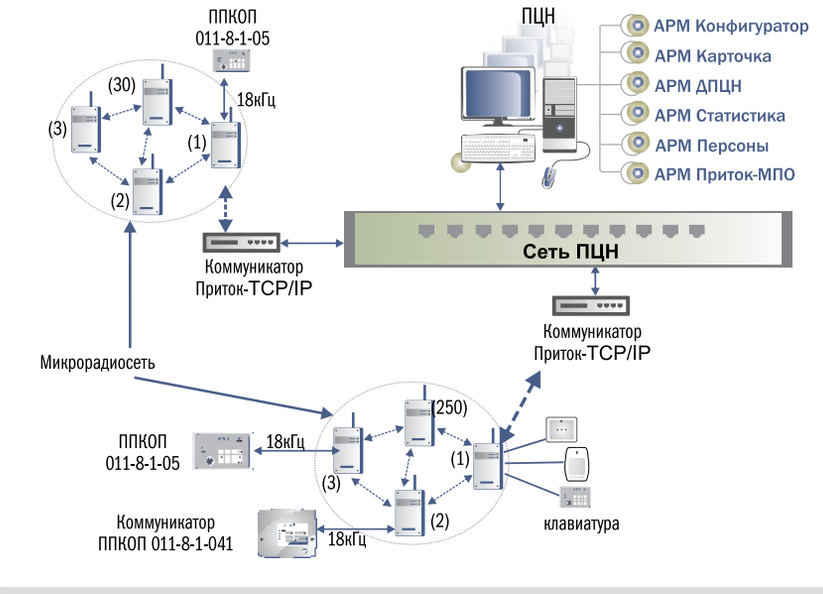
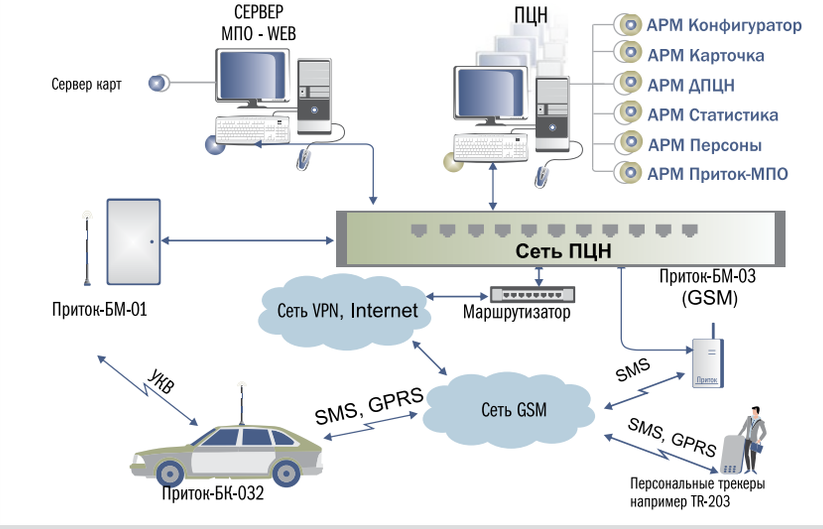


Рис. 8 Подсистема мониторинга и охраны подвижных объектов Приток-МПО



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 определенным 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, то есть управлять дверями, турникетами, шлагбаумами и другими точками прохода/проезда (см. рис. 9.).

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.

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 или IP-видеокамерами (см. рис. 10).

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

11. Подсистема регистрации телефонных и радиопереговоров Приток-РТП создается методом установки плат оцифровки и сжатия речи в одну из рабочих станций, в которую загружается ПО АРМ Приток-РТП (см. рис. 12). Это обеспечивает запись аудиоинформации, поступающей с различных каналов, подключаемых к данной плате, на жесткий 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 создается путем подготовки аудиосообщений, которые воспроизводятся абонентам по заранее подготовленному расписанию или оперативно.

И в заключение. Приведенные 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 нее 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. То есть, 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 МВД РФ. Система установлена в учреждениях власти, в том числе и в Государственной думе РФ.

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

ИС Приток-А – динамически развивающаяся система, которая обеспечивает, а иногда и опережает запросы ее многочисленных пользователей и клиентов.

Рис. 9 ПЦН с элементами системы контроля и управления доступом Приток-СКУД

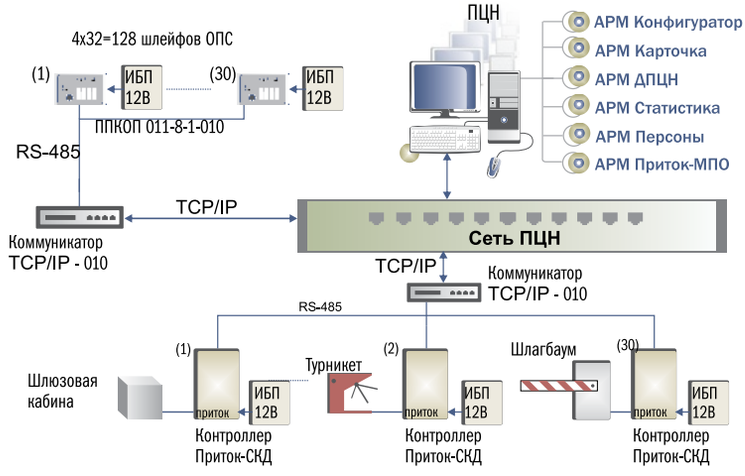


Рис. 10 ПЦН Приток-видео с применением аналоговых и IP-видеокамер

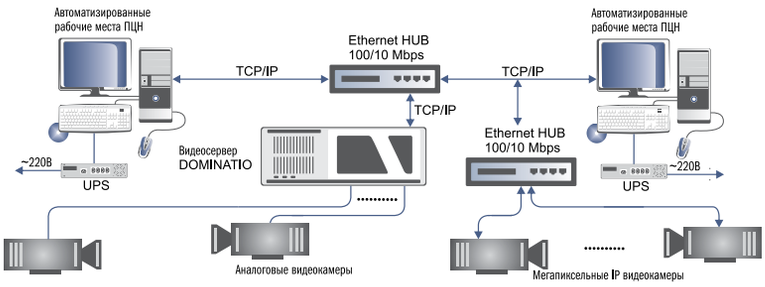
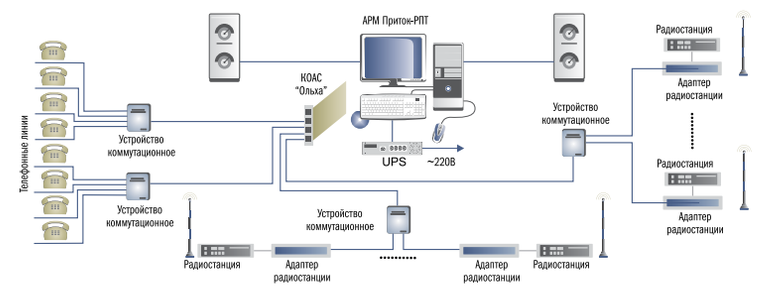


Рис. 11

ПЦН для записи и воспроизведения аудиоинформации Приток-РТП



Программное обеспечение АРМ ПЦН

ПО АРМ — основа ИС ОПС Приток-А

Назначение, принцип действия

Программное обеспечение автоматизированных рабочих мест (ПО АРМ Приток-А) является основной составляющей Интегрированной системы охранно-пожарной сигнализации Приток-А и позволяет строить распределенную масштабируемую высокопроизводительную систему обеспечения безопасности.

ПО Приток-А предназначено для постоянного контроля и обработки в реальном масштабе времени извещений, поступающих от различных подсистем, передачи с АРМ ПЦН команд управления аппаратурой как в автоматическом, так и в ручном режимах, а также управления видеоподсистемой, подсистемой **СКУД** и др.

Использование современных информационных технологий **позволяет реализовать взаимодействие различных программных средств по протоколам TCP и UDP,** независимо от физической среды передачи данных, обеспечивая работу по коммутируемым каналам связи, а также в локальных вычислительных сетях (ЛВС), распределенных сетях предприятий (WAN), глобальных сетях. Поступающие в Ядро системы извещения обрабатываются в соответствии с настройками, сделанными для данного объекта, и типа оборудования, установленного на нем. Информация о событии и об ответных действиях системы и дежурного персонала помещается в базу данных.

Состав компонентов программного обеспечения

Ядро системы предназначено для работы с аппаратурой системы и предоставления пользователям (дежурному персоналу ПЦН) полной информации о ее работе. Ядро обеспечивает надежную защиту от несанкционированного доступа к аппаратуре путем шифрования всего трафика.

АРМ Конфигуратор предназначен для создания модели аппаратной конфигурации системы, необходимой для работы остальных программных средств ИС Приток-А. Конфигуратор обеспечивает настройку и поддержку единого непротиворечивого дерева конфигурации аппаратуры системы, основных параметров работы оборудования, обеспечивает возможность создания пользовательских сценариев для элементов конфигурации.

АРМ дежурного пульта централизованного наблюдения (АРМ ДПЦН) предназначен для автоматизации деятельности оперативного персонала ПЦН с учетом персональных настроек и разделения прав доступа к функциям ПО в зависимости от ролей (дежурных офицеров, операторов, начальников караула, инженеров и т.д.), мониторинга работы системы в режиме реального времени, а также обеспечение пользователя АРМа всей отчетной и другой необходимой информацией.

АРМ Карточка предназначен для ведения БД охраняемых объектов, а также для ведения договорных отношений с клиентами. Информация в карточке объекта содержит следующие данные: характеристику охраняемого объекта; список собственников (хозорганов) объекта с их паспортными данными, адресами, телефонами, идентификационные коды доступа, описание способа блокировки объекта средствами ОПС и т.д.

АРМ Приток-МПО предназначен для организации охраны и контроля за местоположением подвижных объектов, оснащенных бортовыми комплектами (БК) с УКВ или GSM-связью, а также для оценки оперативной обстановки по электронной карте местности при работе как с подвижными, так и стационарными объектами в составе системы ИС Приток-А или автономно. АРМ Приток-МПО позволяет:

- **отслеживать** произвольное количество объектов на одной или нескольких открытых картах одновременно
- **управлять** охраной автомобиля по каналам сотовой связи GSM в режиме SMS/GPRS
- **подготавливать и печатать** различные отчеты на основании архивных и оперативных данных (отчет о пробеге, расходе топлива, истории по охране и др.)
- **отображать** тревожные объекты ИС ОПС Приток-А на карте
- **работать** с различными форматами карт

АРМ Статистика предназначен для предоставления пользователям объективной информации о работе ИС Приток-А. Предоставляет мощные инструменты для анализа работоспособности системы, поиска и устранения неисправностей. Текстовые и графические отчеты позволяют оперативно принимать решения службам технической поддержки. На основе оперативной БД и архивных данных может быть сформировано более 30 различных форм отчетности по работе подсистем, при помощи которых можно проводить анализ ситуации и работоспособности системы.

АРМ Персоны предназначен для работы со всеми персонами системы Приток-А, создания и редактирования отделов, должностей, работы с электронными ключами персон, оперативной работы с уровнями доступа подсистемы Приток-СКД. Служит в качестве основного АРМ оператора бюро пропусков предприятия.

АРМ Приток-РТП обеспечивает регистрацию радио- и телефонных переговоров, поиск и воспроизведение аудиоинформации, организацию системы оповещения оперативного персонала и собственников.

АРМы для обслуживания базы данных:

АРМ АП-Монитор и Репликатор предназначены для создания резервных и архивных баз данных, для создания архивных файлов событий системы, оптимизации структуры оперативной БД.

В состав ПО Приток-А также входят дополнительные компоненты, расширяющие возможности системы:

Сервер сценариев предназначен для выполнения пользовательских подпрограмм, алгоритмы которых заранее не предусмотрены ядром системы, но они были созданы и настроены пользователями в АРМ Конфигуратор.

Сервер подключений предназначен для работы и управления ТСО по протоколу TCP и UDP через различные каналы связи.

Сервер отчетов, Сервер карт, Сервер WEB-МПО, Сервер Приток-РЛС и др. — программные комплексы для реализации расширенных возможностей подсистем ИС Приток-А.

Архитектура программных средств Приток-А

- общее количество АРМ в составе системы не ограничено
- эргономичный, настраиваемый пользовательский интерфейс АРМ
- постоянный контроль исправности программных и аппаратных средств и каналов передачи данных
- подробное протоколирование событий в системе, в том числе и действий пользователей
- формирование и выдача различных отчетов на основании оперативных и архивных данных
- расширение функционала системы при помощи пользовательских сценариев и новых АРМ.

Новинки программного обеспечения

"В течение всего 2015 года нами проводились работы по внедрению версии 3.7.0 интегрированной системы ОПС Приток-А. Многие пользователи отметили улучшенную производительность и безусловную актуальность новых функций системы.

Совместно с версией 3.7.0 в разных городах страны опробовали и внедрили новый программный продукт "Приток-Охрана-WEB". Сотрудники обслуживающих организаций этих городов получили удаленный доступ к электронному журналу "Заявки техникам", что позволило им более оперативно выполнять работы по обслуживанию охранной аппаратуры и более эффективно взаимодействовать с ПЦН. Для собственников охраняемых объектов этих городов стала доступна новая услуга удаленного доступа и управления своим прибором через мобильное приложение "Охрана Приток-А".
Сегодня для всех пользователей, эксплуатирующих ИС ОПС Приток-А, мы представляем версию 3.7.1. В этой статье перечислены самые важные и интересные разработки. Более подробный список изменений опубликован на нашем сайте в описании к версии — Release Notes.
Хочется отметить, что значительная часть изменений выполнена по замечаниям и пожеланиям наших пользователей. Спасибо всем, кто помогает сделать нашу систему более удобной и совершенной!"

Подключение новых приборов клиентов охраны

Теперь вводить в эксплуатацию и подключать новые приборы возможно в более короткие сроки. Установите режим «ПРОВЕРКА» для нового прибора, и сотрудник монтажной организации сможет выполнить его подключение и настройку до того момента, как будет заполнена карточка объекта.

Система примет любой код (ключ) при проверке взятия под охрану и снятия с охраны. Инженер сможет занести список собственников и их коды доступа в карточку объекта уже после окончания монтажных работ (при заключении договора, отключив режим «ПРОВЕРКА»).

Обработка аварий связи

В предыдущих версиях ПО Приток-А при потере связи с прибором все его охраняемые зоны переводились в тревогу. Например, при неустойчивой работе сотовой связи это могло привести к значительному увеличению количества тревог. Дополнительно к этому в стакан «Аварии» помещались все приборы, с которыми была утеряна связь.

В версии 3.7.1 в момент аварии связи с прибором не формируется тревога по каждой охраняемой зоне прибора. Тревога формируется только по карточке прибора (направления). При этом в стакан «Аварии» помещаются только те приборы, у которых на момент потери связи был под охранной хотя бы один шлейф либо действовало режимное время по договору.

Павел Орлов,
начальник сектора разработки программного обеспечения

Теперь оператору/дежурному АРМ ДПЦО станет проще работать с оперативными тревогами и не придется отвлекаться на аварии по приборам, которые не охранялись на момент потери связи.

Сервер подключений

Для программы «Сервер подключений», обеспечивающей работу охранных приборов через интернет-каналы, выполнен ряд доработок по улучшению стабильности. Теперь для инженерного состава доступен новый отчет по входящему и исходящему трафику каждого прибора (по информационным пакетам данных без округления). Важно иметь такую статистику, когда SIM, установленные в приборах, находятся на балансе охранного предприятия / отдела вневедомственной охраны.

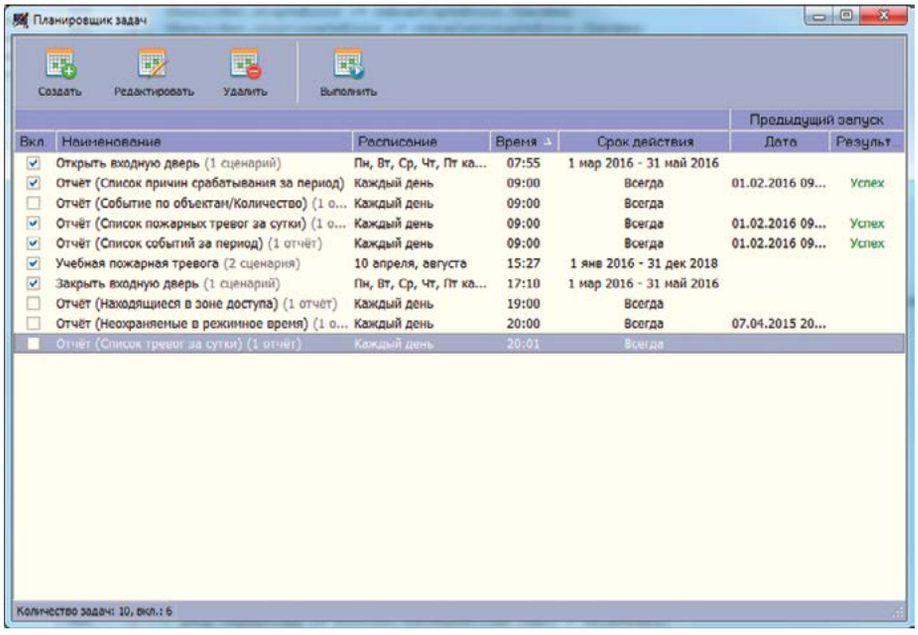
Менеджер авторизации

Во время своей работы пользователи Приток-А часто запускают разные программы системы. Каждый раз при запуске требуется вводить имя пользователя и пароль для авторизации. Мы разработали новое приложение «Менеджер авторизации Приток-А», который запоминает введенные имя пользователя и пароль при первом запуске любой программы на компьютере и использует их в дальнейшем при авторизации в других программах.

Таким образом, «Менеджер авторизации Приток-А» позволяет автоматизировать и ускорить процесс ввода имени пользователя и пароля. Особенно удобно использовать новый менеджер администраторам системы и инженерам.

Сценарии

Разработаны новые функции для сценариев. Теперь из сценария можно сравнивать текущее и предыдущее состояние зон/шлейфов, анализировать текущее и предыдущее состояние датчиков, выполнять новые команды. В интерфейс добавлена подсветка синтаксиса для более удобного написания сценариев.



Планировщик задач

Мы расширили список автоматических задач системы. Теперь наряду с отчетами, выполняющимися по расписанию, могут выполняться и сценарии. Настраивать расписание выполнения отчетов и сценариев удобно из нового «Планировщика задач», в котором гибко настраивается время, период и количество повторений.

Мобильные приложения

Семейство мобильных приложений Приток-А пополнила новая версия программы «Охрана Приток-А» для операционной системы iOS. Теперь и владельцам устройств Apple доступна возможность удаленно управлять и контролировать состояние охраняемых объектов. Работая в фоновом режиме, программа оповещает пользователя о событиях, возникающих на объекте, с помощью push-уведомлений. «Охрана-Приток-А» опубликована и доступна для скачивания в магазине приложений AppStore. Подробнее – на стр. 32.

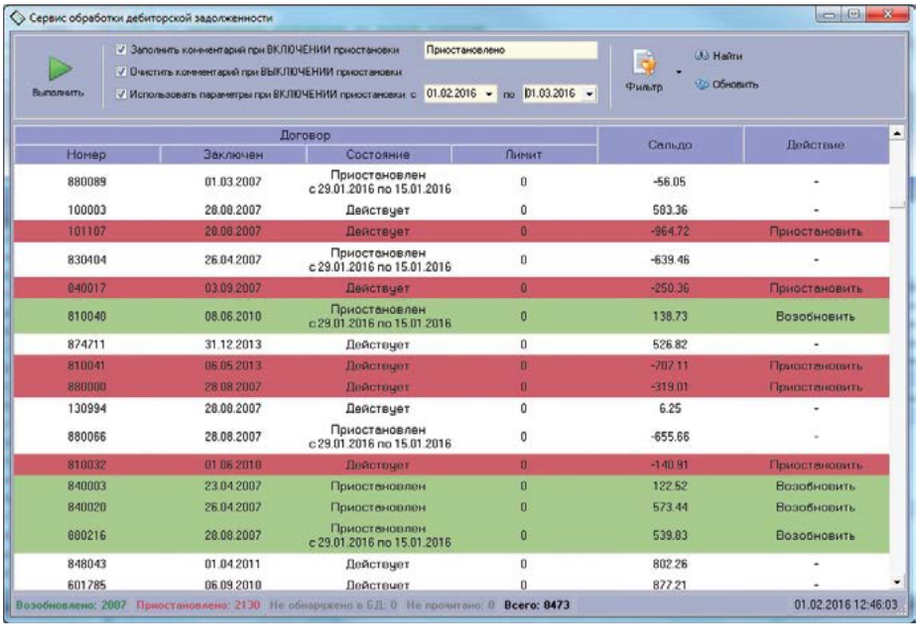
WEB-расширения

После проведения опытной эксплуатации, внедрения и получения отзывов о новом сервисе «Приток-Охрана-WEB» мы подготовили вторую версию. Для интерфейса «Обслуживающие организации» увеличена скорость работы, добавлены новые выборки и отчеты по оборудованию. По пожеланиям пользователей внесены улучшения в интерфейс просмотра журнала «Заявки техникам».

Обработка дебиторской задолженности

Бухгалтерия охранного предприятия / отдела вневедомственной охраны периодически формирует оборотно-сальдовую ведомость по клиентам. Выгрузите эту ведомость из бухгалтерской программы в текстовый файл и обработайте его с помощью нового сервиса в АРМ «Карточка».

Система приостановит действие всех договоров, по которым дебиторская задолженность превысит лимит. Тем клиентам, которые уже погасили задолженность, возможность пользоваться услугами охраны будет возобновлена. Лимит дебиторской задолженности может быть указан индивидуально для каждого договора.



Конфигуратор параметров UniProg

Доступна новая версия программы «Конфигуратор параметров» (UnipProg 3.0.3). Линейка поддерживаемого программой оборудования пополнилась устройствами: Приток-А-КОП-03, Приток-РКС-05, GSM-приборами (-011, -011К, -011М), модулями МБД-02, ВС-05 для шины расширения приборов серии Приток-А-КОП, устройствами СКД-02 и БК следующих версий.

Загрузка, обновление и обслуживание

Теперь загружать, обновлять и обслуживать систему Приток-А стало проще и удобнее.

На сайте www.sokrat.ru появился новый раздел «Загрузка ПО». Вы всегда можете проверить, какая версия актуальна на сегодня, загрузить список изменений и необходимые инструкции, поучаствовать в тестировании новых продуктов.

В версии 3.7.1 внедрен новый механизм обновления структуры базы данных. Теперь все файлы обновлений (апдейты базы данных) находятся в одной библиотеке. Также внесены улучшения и выполнены доработки для системы автоматического обновления программного обеспечения на рабочих местах.

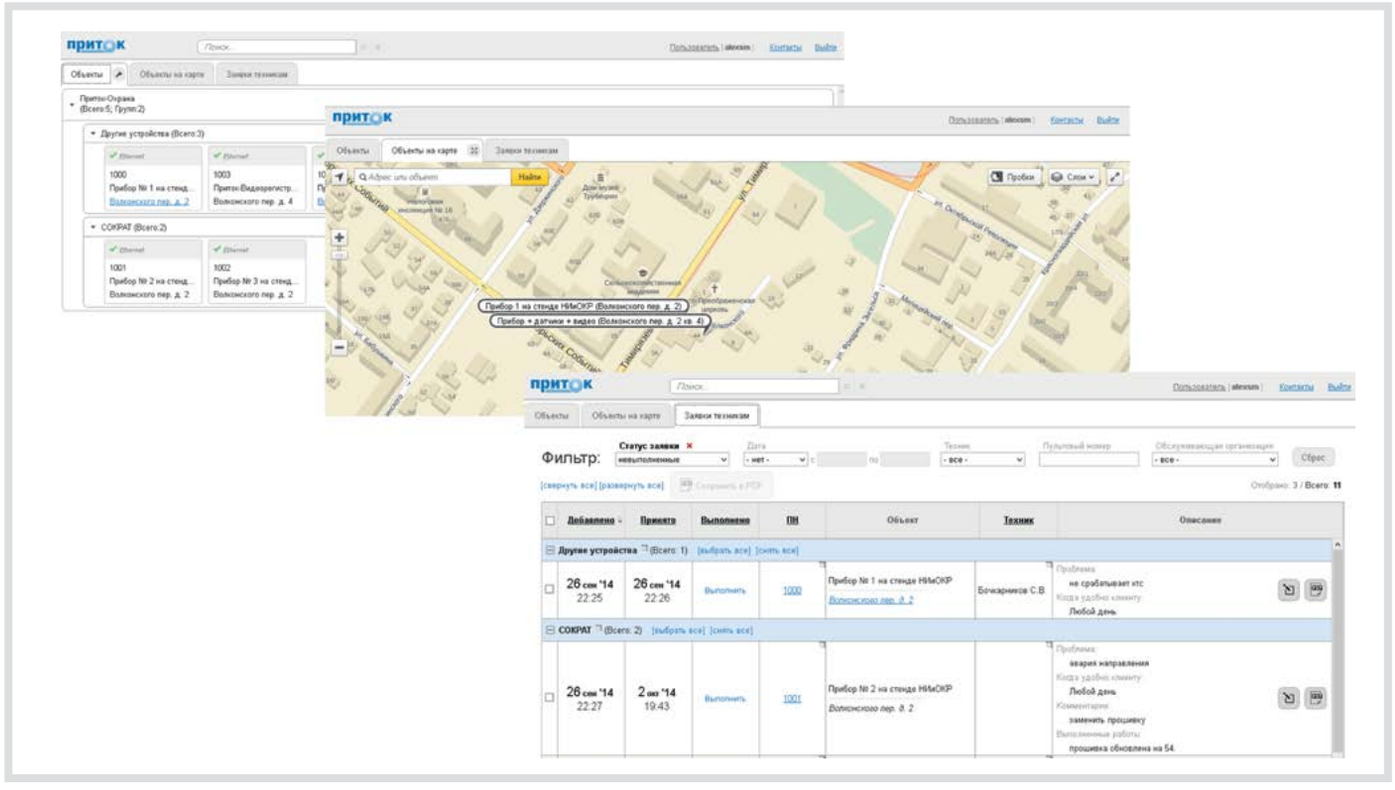
Любая система требует обслуживания. Теперь все протоколы работы системы, журналы по программам хранятся в одной папке на компьютере. При необходимости легко создать архив этой папки и отправить его в отдел технической поддержки.

Приток-Охрана-WEB
Сервис для обслуживаюих организаций и собственников

«Приток-Охрана-WEB» предназначен для организации удаленного доступа сотрудников обслуживающих организаций и собственников квартир (частных домов, гаражей) к информации по охраняемым на ПЦН объектам. Доступ обеспечивается в режиме реального времени (online) через WEB-интерфейс «Организации» и «Частное лицо» соответственно.

WEB-интерфейс для организаций позволяет сотрудникам:

- просматривать список обслуживаемых объектов, охраняемых на различных ПЦН;
- получать информацию о работоспособности прибора, его текущем канале связи с ПЦН;
- запрашивать историю работы прибора за нужный день;
- просматривать и редактировать конфигурацию прибора;
- **работать со списком заявок, полученных с ПЦН, техникам — получать новые заявки и подтверждать их получение, фиксировать выполнение заявок;**
- просматривать на электронной карте местности местоположение объектов, по которым необходимо провести технические работы согласно заявкам*.



Web-интерфейс для собственников позволяет:

- просматривать список своих объектов, охраняемых на различных ПЦН;
- по каждому объекту контролировать охранное состояние шлейфов сигнализации, показания технологических датчиков (температура, влажность);
- выполнять команды постановки на охрану, снятия с охраны;
- выполнять команды управления исполнительными устройствами, подключенными через силовые ключи прибора (открыть автоматические ворота, включить освещение периметра территории и т.д.);
- просматривать историю работы прибора (время постановки под охрану, время снятия с охраны, время возникновения тревожных событий и т.д.) за нужный день;
- просматривать изображение с IP-видеокамер, установленных на объекте;
- получать информацию о работоспособности прибора, его текущем канале связи с ПЦН;
- просматривать и редактировать конфигурацию прибора;
- настраивать параметры SMS-информирования по событиям объекта на сотовые телефоны заинтересованных лиц;
- просматривать местоположение объектов на электронной карте местности*.

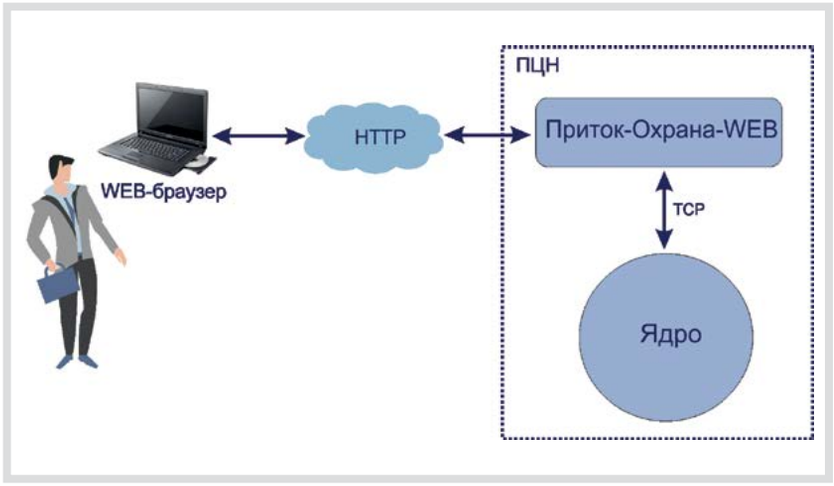
*для демонстрации возможностей используется картографический сервис «Яндекс.Карты». При выполнении лицензионных условий могут быть подключены сервисы других производителей: Google, OpenStreetMap и т.д.

Схема взаимодействия и принцип работы

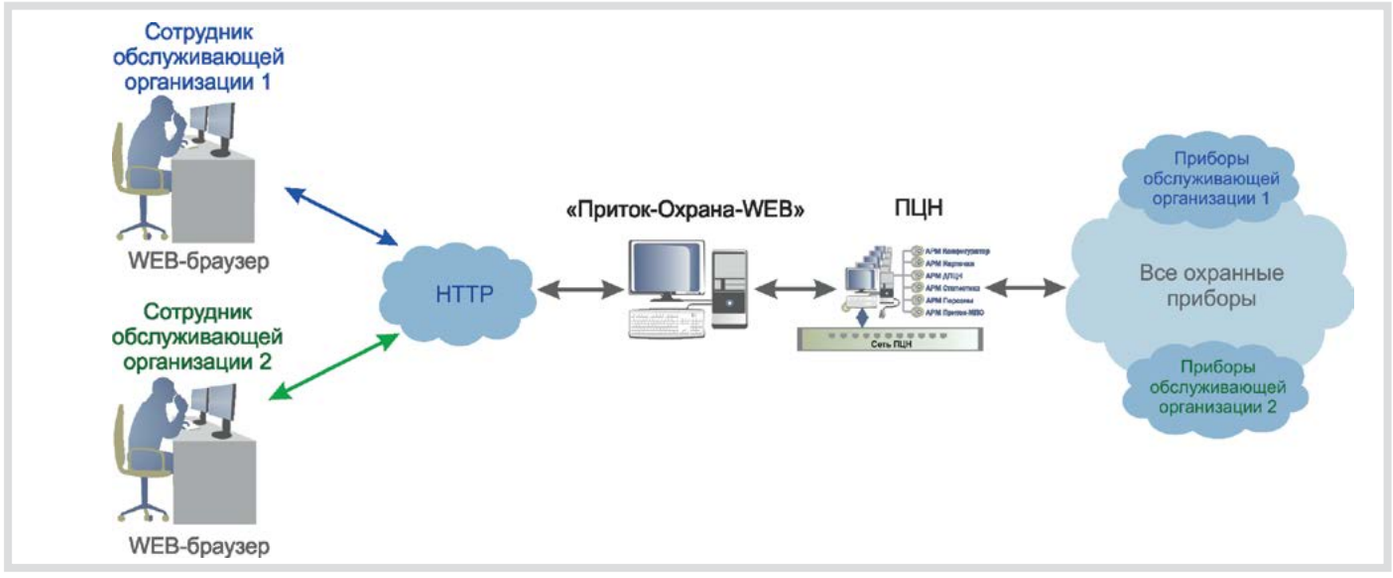
«Приток-Охрана-WEB» устанавливается и выполняется на отдельном сервере, который должен быть обеспечен доступом в Интернет.

Для работы «Приток-Охрана-WEB» необходимо постоянное подключение к Ядру системы Приток-А, которое установлено и запущено на ПЦН. Таких подключений может быть несколько.

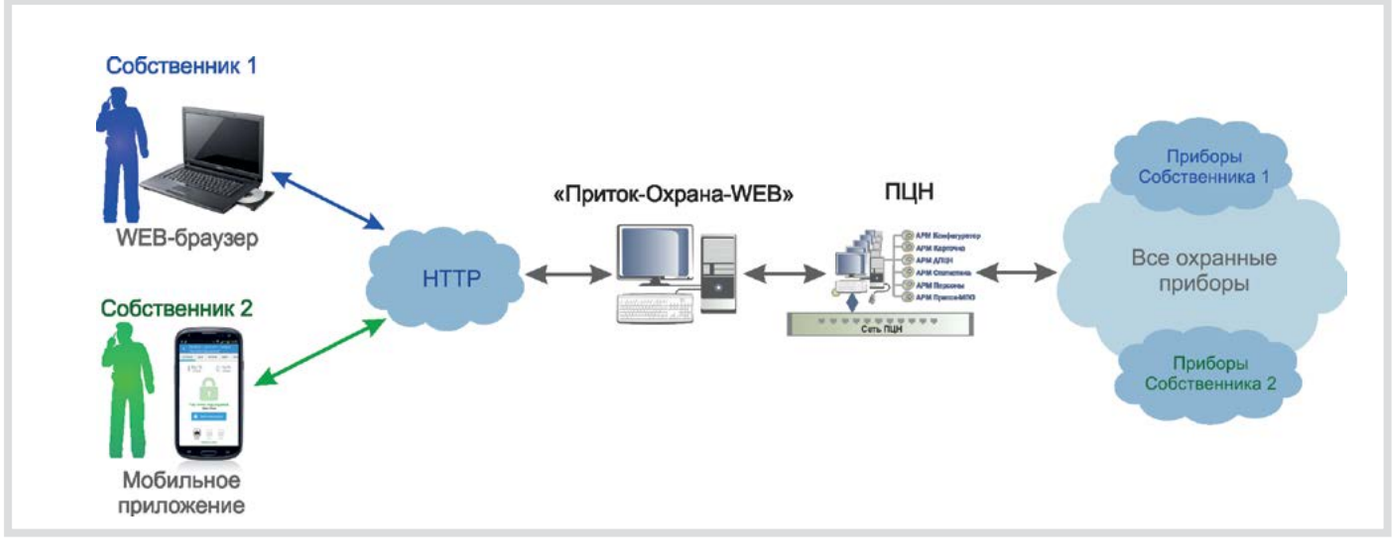
Администратором ПЦН при помощи программы АРМ «Конфигуратор» определяются уникальные имена и пароли для пользователей «Приток-Охрана». С помощью системы прав указывается к каким функциям «Приток-Охрана-WEB» будет иметь доступ пользователь и какие охраняемые объекты будут доступны для просмотра\управления.



Пользователь выполняет подключение к «Приток-Охрана-WEB» через WEB-браузер, указывая при этом уникальное имя пользователя и пароль и выбирая WEB-интерфейс.



Для собственников охраняемых объектов доступ к «Приток-Охрана-WEB» осуществляется при помощи WEB-браузера и мобильного приложения «Охрана Приток-А» (см. стр. 48).



Мобильное приложение «Охрана Приток-А»

«Охрана Приток-А» — программа для мобильных устройств под управлением ОС Android и iOS, являющаяся клиентским приложением сервиса Приток-Охрана-WEB. Программа обеспечивает удаленный доступ собственников квартир (частных домов, гаражей) к информации по охраняемым объектам.

Принцип работы

Программа «Охрана Приток-А» устанавливается и выполняется на мобильном устройстве собственника охраняемого объекта.

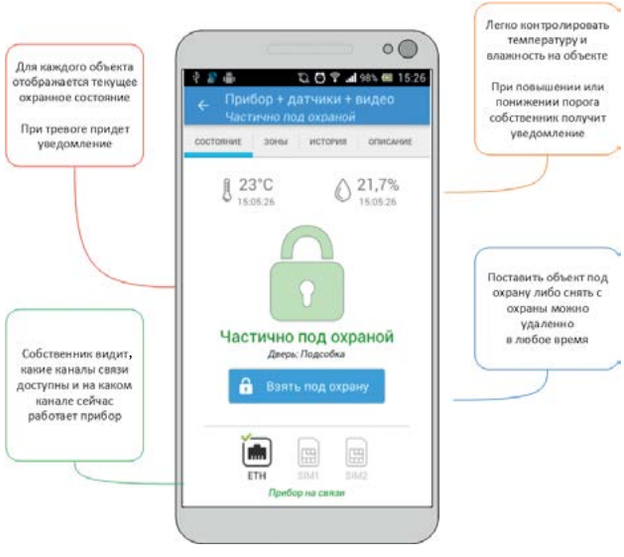
Помещение объекта оборудуется ОПС с использованием приборов серии Приток-А-КОП. К прибору подключаются различные датчики (объемные, протечки воды) и устанавливаются дополнительные модули расширения (такие как модуль беспроводных датчиков МБД-01/02, модуль гигрометра ВС-01 с датчиком влажности и температуры). Прибор подключается к пульту охраны или центру мониторинга.

Пульт охраны, центр мониторинга (либо другая организация) предоставляют доступ собственников охраняемых объектов к сервису Приток-Охрана-WEB. Каждому пользователю создается личный кабинет.

После запуска программа «Охрана Приток-А» подключается к серверу «Приток-Охрана-WEB» по любому доступному каналу связи (wi-fi, gprs , 3g/4g). Собственник вводит свое имя пользователя и пароль и получает доступ к интерфейсу по управлению и контролю за своим объектом. «Охрана Приток-А», работая в фоновом режиме, оповещает пользователя о событиях, возникающих на объекте.

Интерфейс программы позволяет:

- просматривать список своих объектов, охраняемых (подключенных на) ПЦН;
- контролировать охранное состояние шлейфов сигнализации, показания технологических датчиков (температура, влажность);
- просматривать историю работы прибора (время постановки под охрану, время снятия с охраны, время возникновения тревожных событий и т.д.);
- получать уведомления о возникающих событиях на объекте («Взят под охрану», «Снят с охраны», «Тревога» и т.д.);
- выполнять команды управления исполнительными устройствами, подключенными через силовые ключи прибора (открыть автоматические ворота, включить освещение периметра территории и т. д.);
- просматривать изображение с IP-видеокамер, установленных на объекте.



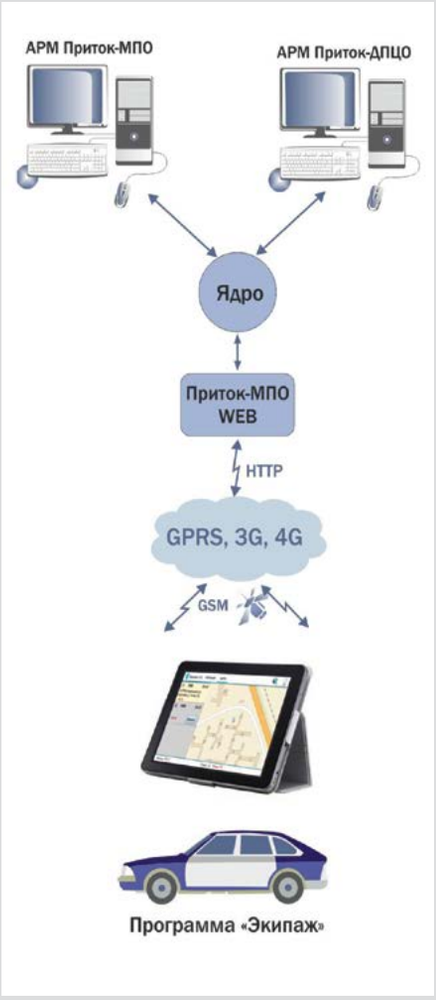
Мобильное приложение «Экипаж Приток-А»

«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 передается голосом в радиоэфире. Для передачи данных используются каналы связи GSM(GPRS)/3G.

Интерфейс программы позволяет:

- 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.).
- Подтвердить факт получения тревожного сообщения, для этого оператору в ГЗ достаточно прикоснуться пальцем (или специальным стержнем) к транспаранту Тревоги.
- Отображать на карте местоположение ГЗ относительно тревожного объекта.



Основные функции программы

- авторизация по имени пользователя и паролю на сервере Приток-МПО-WEB
- индикация текущего состояния подключения к сети Интернет и с сервером Приток-МПО-WEB
- отображение позывного ГЗ
- отображение списка назначенных для ГЗ тревог, их количества и количества новых
- вибрация и проигрывание звука при получении новой тревоги и при отмене тревоги*
- 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 радиоэфире.

Мобильное приложение «Трекер Приток-А»

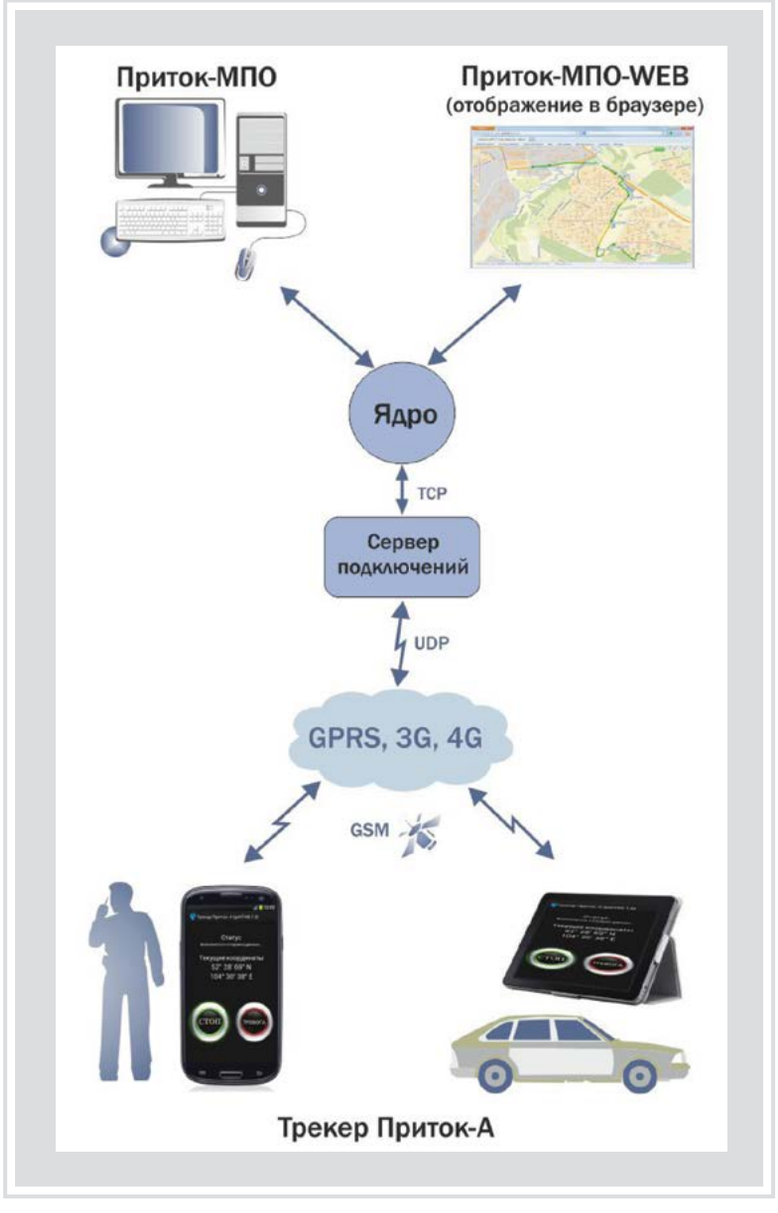
«Трекер Приток-А» — приложение для ОС Android со стандартными функциями программного GPS/ГЛОНАСС трекера.

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

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

Интерфейс программы позволяет:

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



Основные возможности

- 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

Варианты исполнения:

Программа доступна для загрузки из магазина Google Play и поставляется в двух вариантах исполнения: платная и бесплатная.

После установки бесплатной версии приложения на телефон имеется возможность получить индивидуальный идентификатор, логин и пароль в центре мониторинга ООО «ОБ Сократ» и через WEB-сайт mpo.pritok.ru наблюдать в режиме on-line за текущим местоположением, просматривать историю передвижения, формировать различные отчеты.

Получить ID для подключения можно по адресу prtltab@sokrat.ru.

Платная версия предоставляет возможность настроить «Трекер Приток-А» на работу с собственным центром мониторинга (охраны), развернутым на базе ПО Приток-А. В платной версии программы доступна для нажатия тревожная кнопка.

Мобильное приложение «Клавиатура Приток-А»

«Клавиатура Приток-А» — специализированное приложение для ОС Android, входящее в состав интегрированной системы охранно-пожарной сигнализации Приток-А (ИС Приток-А).

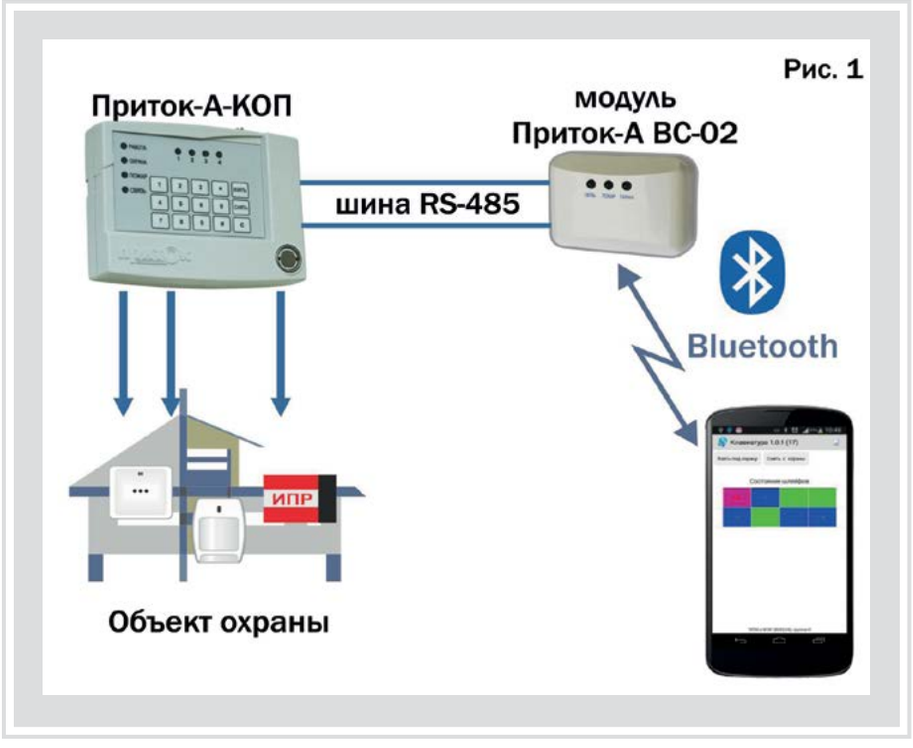
Программа предназначена для подключения к модулю Приток-А ВС-02 шины расширения охранно-пожарных приборов серии Приток-А-КОП. Для подключения используется протокол Bluetooth.

Программа устанавливается на смартфоны и планшетные компьютеры, работающие под управлением ОС Android.

Основное назначение - программная клавиатура для управления прибором.

Интерфейс программы позволяет:

- отображать текущее состояние шлейфов сигнализации;
- выполнять команды «Взять под охрану» и «Снять с охраны» для одного или группы шлейфов;
- отображать текущее состояние подключения к модулю ВС-02 и производить выбор подключаемого модуля;
- производить индикацию звуком состояний «Подключено», «Отключено», «Тревога», «Взятие после выхода».



Подключение

Для работы «Клавиатуры Приток-А» необходимо, чтобы устройство с программой находилось в зоне действия Bluetooth-модуля Приток-А ВС-02 (см. рис. 1).

При старте программа сканирует Bluetooth-устройства, составляя список модулей Приток-А ВС-02. Пользователь выбирает модуль для подключения, через который будет производиться работа с прибором Приток-А-КОП, вводит пароль для подключения к модулю. Клавиатура Приток-А выполняет подключение к модулю по Bluetooth. После успешного подключения к модулю пользователю программы доступны основные функции.

При следующих запусках программа делает попытки восстановить предыдущее подключение. Приложение также позволяет переподключиться к другому модулю Приток-А ВС-02, находящемуся в зоне работы устройства. В случае потери связи или выхода из зоны покрытия «Клавиатура Приток-А» будет пытаться автоматически восстановить связь.

Описание главного окна программы

При запуске программы на экране появляется рабочее поле, на котором после подключения к модулю отображены состояния шлейфов охранного прибора.

Синим цветом отображаются шлейфа, находящиеся в состоянии «снят», зеленым – находящиеся в состоянии «взят», красным – в состоянии «тревога», желтым – в состоянии «неисправность». Серые прямоугольники с надписью «Sh» означают шлейфы, которые не используются в текущей конфигурации.

Внутри каждого активного прямоугольника имеется символ, который индицирует его тип. Символ «О» – это охранный шлейф, «Р» – пожарный шлейф, «Т» – тревожный шлейф. После символа следует порядковый номер шлейфа для выбранной группы. Цвет символа и номера шлейфа зависит от текущего состояния шлейфа, если он в активном состоянии (не в норме), цвет красный, если в норме, то цвет зеленый.

Варианты использования

• Для управления шлейфами прибора программа Клавиатура Приток-А может быть запущена на смартфоне пользователя (собственника охраняемого объекта или имеющего право управления охраной).

При входе на объект пользователь запускает программу, выполняет подключение к модулю Bluetooth, нажимает кнопку «Снять», вводит код идентификации ХО и выполняет снятие объекта с охраны. Уходя с объекта, пользователь нажимает кнопку «Взять», набирает код идентификации ХО, выходит из объекта.

Подключение программы к модулю происходит автоматически, как только смартфон попадает в поле действия связи Bluetooth — восстанавливается сеанс связи (см. рис. 2).

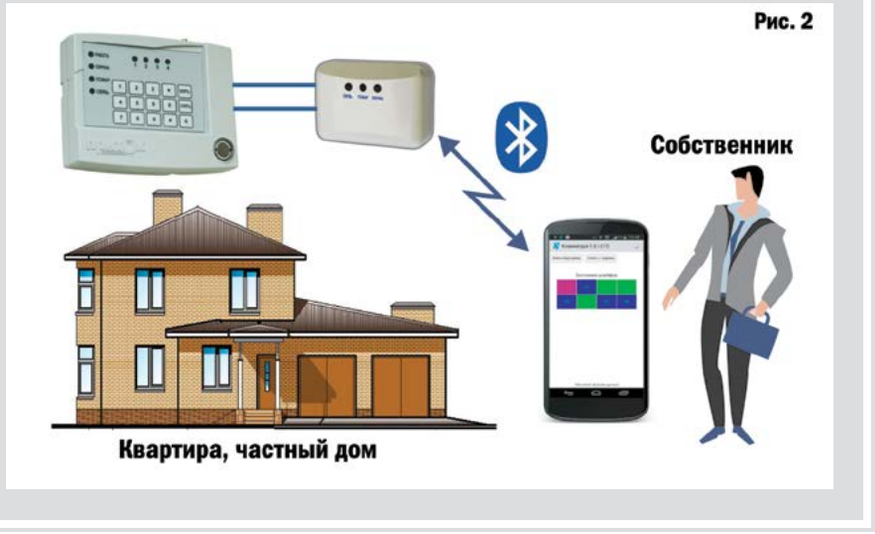


Рис. 2

• При использовании приборов серии Приток-А-КОП для охраны офисных зданий (отдельных помещений)

Клавиатура Приток-А, запущенная на планшетном компьютере, может быть использована в качестве модуля индикации состояния охраняемых шлейфов/объектов. Планшетный компьютер может быть установлен стационарно у охранника на этаже, в здании, у консьержа.

Индикация состояний всех шлейфов объекта (или нескольких объектов) охраны и управление с планшетного компьютера (см. рис. 3).

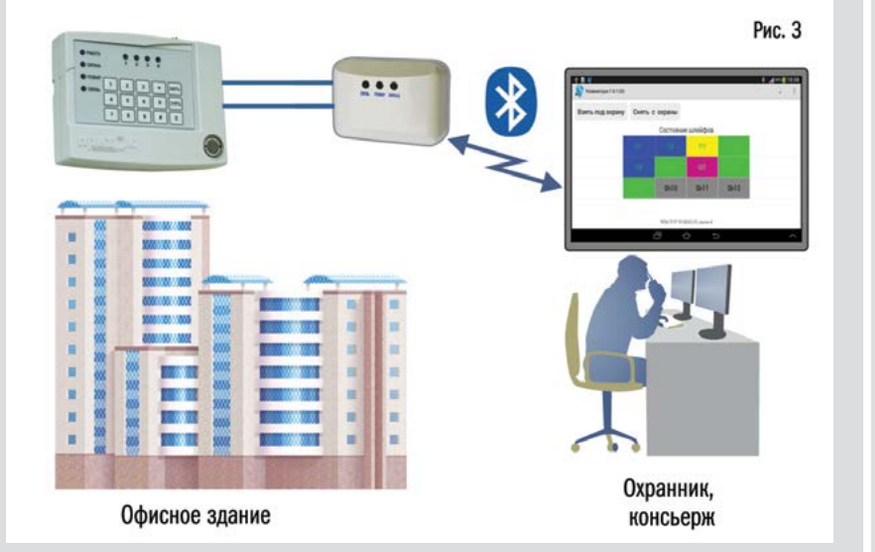


Рис. 3

• Использование планшетного компьютера для подключения к видеодомофону и управление сигнализацией.

Ещё один пример стандартного применения программы «Клавиатура Приток-А» — запуск приложения на стационарном планшетном компьютере с совмещением функции SIP-домофона или видеодомофона.

Видеодомофон (SIP-домофон) подключен по сети WiFi к планшетному компьютеру, установленному стационарно (обычно у входной двери в помещение), и на нём же запущена программа управления шлейфами сигнализации.

Таким образом, планшетный ПК не только выполняет роль клавиатуры для управления шлейфами приборов Приток-А-КОП, но и выполняет роль «видео-глазка» (см. рис. 4).

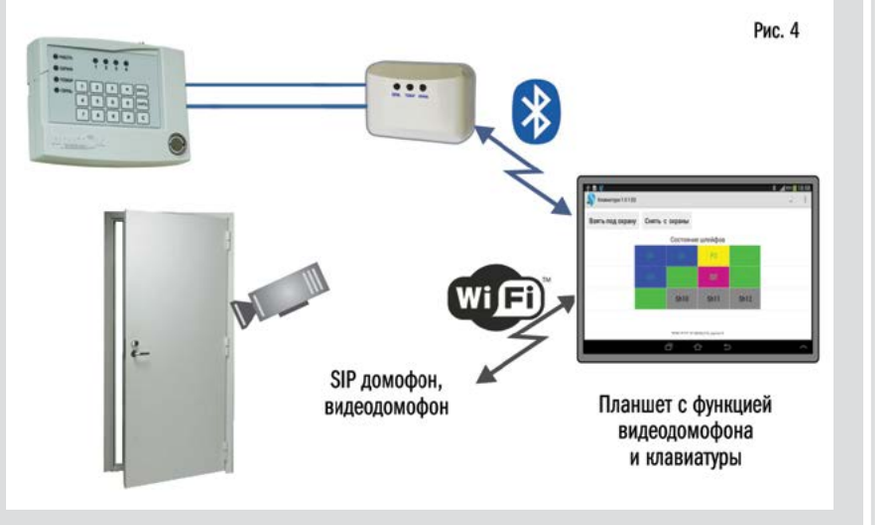


Рис. 4

Охрана банкоматов

В качестве примера применения программы «Клавиатура Приток-А» можно рассмотреть практическую реализацию охраны банкоматов приборами Приток-А-КОП.

Стандартный вариант охраны банкомата предусматривает установку охранного прибора серии Приток-А-КОП внутри банкомата, считывателя ключей TouchMemory — снаружи. Инкассатор прикладывает ключ TouchMemory к считывателю — все охранные шлейфы прибора банкомата снимаются с охраны, прикладывает еще раз — все шлейфы прибора банкомата ставятся под охрану.

В целях повышения уровня безопасности руководящими документами банка и пульта охраны может быть выдвинуто требование снимать с охраны и ставить под охрану банкомат только с использованием клавиатуры (кодонаборной панели) без использования ключей TouchMemory. В связи с такими требованиями вариант установки должен предусматривать вынос клавиатуры наружу — для управления сигнализацией. Сотрудник инкассации сначала набирает PIN-код для разблокировки клавиатуры, а потом набирает код доступа (идентификатор) для снятия с охраны или постановки на охрану. По ряду причин такое решение непрактично. Любое, даже самое аккуратное, исполнение клавиатуры, может испортить (изменить) внешний вид банкомата, а также может провоцировать акты вандализма по отношению к оборудованию.

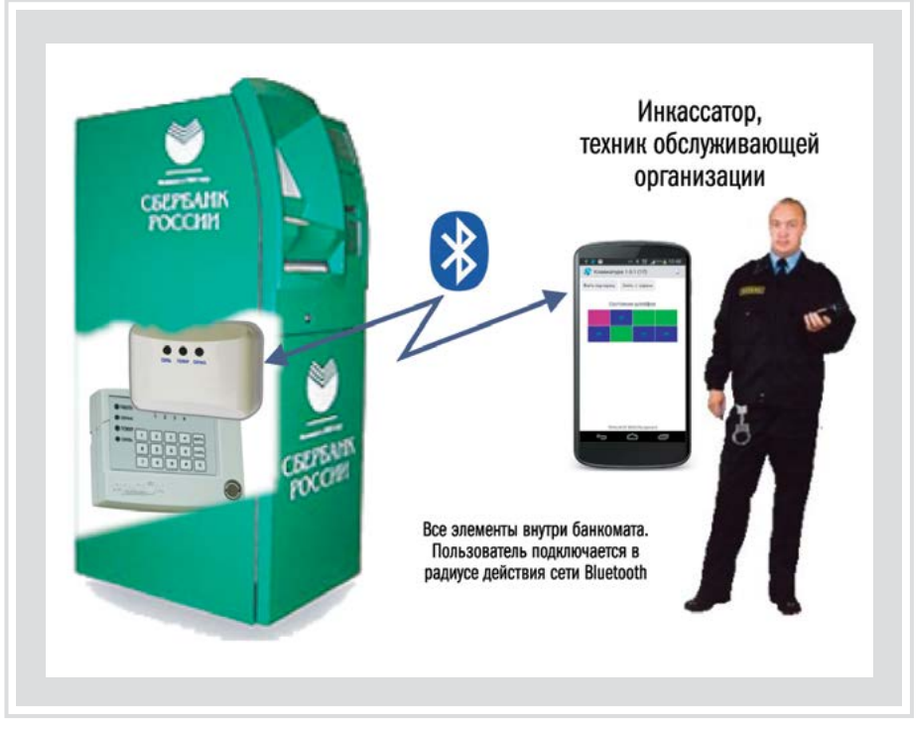
Кроме этого, известно, что любой банкомат требует технического обслуживания. Сотрудник обслуживающей организации при работе с банкоматом не имеет права снимать с охраны все шлейфы банкомата целиком — для снятия ему должны быть доступны только сервисные части банкомата. Инкассатор же, наоборот, может снять с охраны банкомат целиком.

Вышеперечисленные особенности охраны банкомата могут быть реализованы с помощью охранного прибора серии Приток-А-КОП и дополнительной установки в банкомат модуля Bluetooth Приток-ВС-02.

Модуль Приток-ВС-02 подключается к прибору Приток-А-КОП через шину расширения. На телефон (смартфон, планшетный компьютер) инкассатора и техника устанавливается программа “Клавиатура Приток-А” для ОС Android. Программа через встроенный Bluetooth-модуль телефона подключается к модулю Приток-ВС-02 и эмулирует работу стандартной внешней клавиатуры прибора.

При такой схеме не требуется установка прибора или клавиатуры снаружи банкомата и может быть реализована раздельная тактика частичной постановки и снятия шлейфов охраны для инкассатора и техника.

При использовании телефона и модуля Приток-ВС-02 схема работы с банкоматом выглядит следующим образом. Пользователь (инкассатор, техник и пр.) подходит к банкомату в зону действия сети Bluetooth-модуля. Программа, запущенная на телефоне, подключается к модулю Приток — ВС-02 и получает доступ для управления шлейфами сигнализации прибора. Информация при обмене данными между телефоном и модулем прибора шифруется. Подключение возможно только с разрешенных (настроенных) телефонов — при подключении вводится PIN-код для связи с модулем как аналог PIN для разблокировки клавиатуры. После того как соединение установлено, пользователь выбирает определенные шлейфа охраны банкомата (в соответствии с правами доступа), вводит код доступа (идентификатор ХО) для снятия объекта с охраны. Код доступа хранится в базе данных пульта охраны и может быть оперативно удален либо изменен, например, при увольнении сотрудника. Постановка под охрану осуществляется аналогично. Дополнительно к этому в программном обеспечении Приток-А, установленном на пульте охраны, дежурному (оператору) будет сформировано предупреждение в тех случаях, когда инкассатор или техник забыл взять под охрану банкомат после окончания своей работы. Таким образом, программное обеспечение ИС Приток-А помогает обеспечивать постоянный контроль объекта охраны и предотвращает ошибки, вызванные человеческим фактором.



Более подробно про «Клавиатуру Приток-А» смотрите на сайте: http://sokrat.ru/pritok/objectp/btkeyboard.htm

Программа доступна для установки с Google Play маркет: https://play.google.com/store/apps/details?id=com.sokrat.btm

приток

Каталог

- **Приборы**

Приток-А-КОП
Подключение радиоканальных извещателей
ППКОП серии Приток-А

В данном разделе представлена информация, раскрывающая общее назначение, структуру и особенности всех подсистем ИС Приток-А

Информация, приведенная в данном разделе, не является документацией и носит только рекламно-информационный характер

Технические характеристики и правила эксплуатации отдельных компонентов и подсистем ИС «Приток-А» указаны в паспортах и руководствах по эксплуатации на конкретные программные и аппаратные руководства

Охрана

Приток-А-КОП
Контроллер охранно-пожарный

Контроллер охранно-пожарный Приток-А-КОП (далее – контроллер) предназначен для организации охраны объектов и квартир в составе Автоматизированной системы охранно-пожарной сигнализации Приток-А. Охрана осуществляется путем контроля состояния шлейфов сигнализации с включенными в них охранными, пожарными и тревожными извещателями и передачи тревожных и пожарных извещений на компьютеры автоматизированных рабочих мест пульта централизованного наблюдения (АРМ ПЦН).

В зависимости от типа исполнения может контролировать до 128 шлейфов (через шину расширения и мРш-02 — модуль Расширения шлейфов).

Питание осуществляется от внешнего источника питания (ИП)-12В или от сети 220В через встроенный ИП.

Контроллер имеет встроенный звуковой извещатель, клавиатуру, считыватель ключей ТМ.

К контроллеру подключаются внешние световые и звуковые оповещатели, датчики отметки патруля и пр.

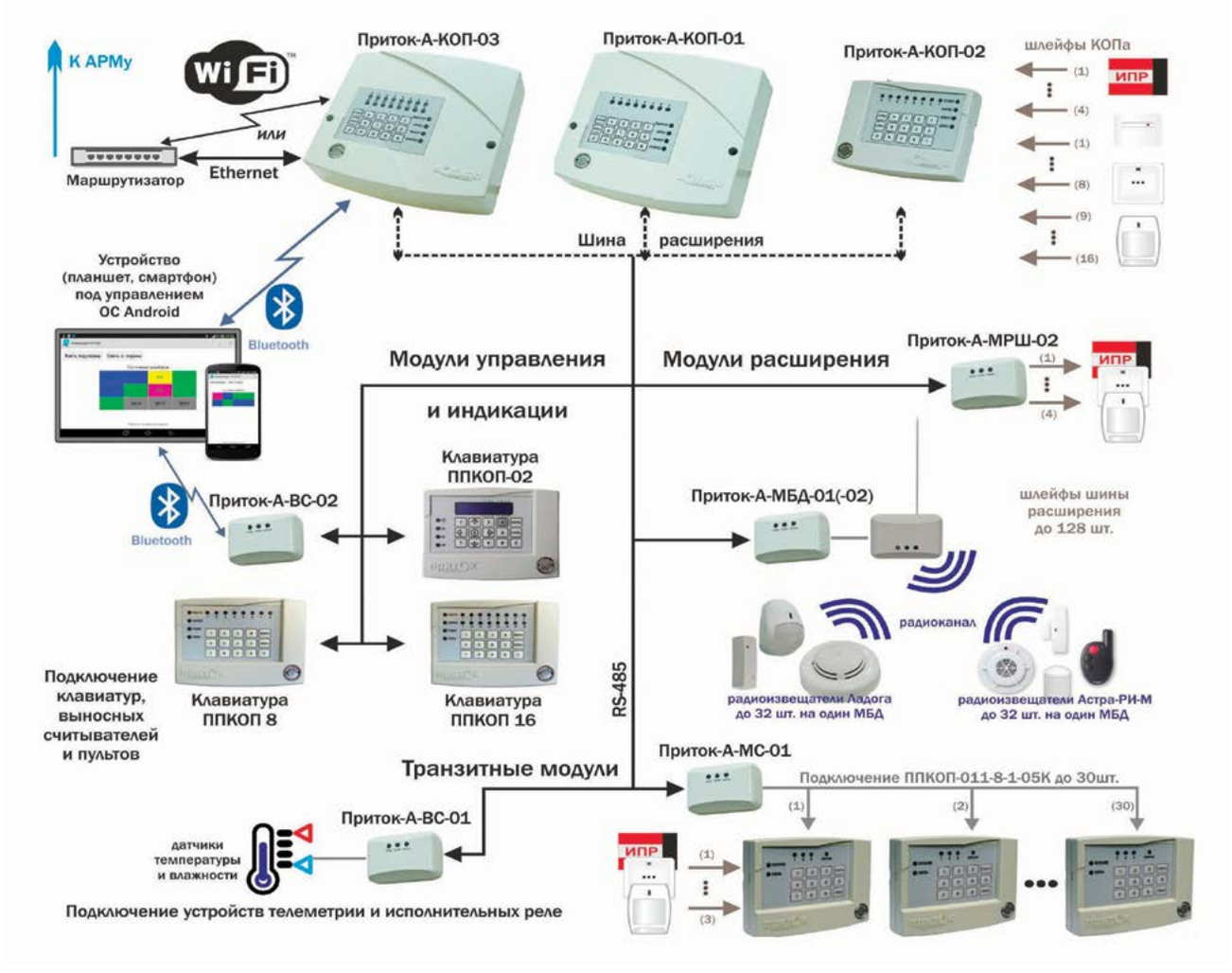
В шлейфы контроллера могут быть включены датчики охранной, пожарной и тревожной сигнализации, а также различные исполняемые устройства — для реализации любых схем охраны.

Особенности контроллера

- работает с ПЦН через «Сервер подключений» по IP-сетям, в том числе через открытый интернет
- при передаче данных используется шифрование AES 128
- для связи могут использоваться несколько каналов — четыре по Ethernet и четыре через GSM/GPRS
- удаленное (из АРМ) техническое обслуживание — конфигурирование параметров связи охраны, обновление прошивки и др.
- запрос параметров прямо из АРМ (уровень GSM-сигнала, текущего канала связи, баланса и пр.)
- подключение через шину расширения дополнительных модулей (клавиатуры, индикация, шлейфы, исполнительные устройства)
- использование для постановки \ снятия тактики код+ключ с возможностью занесения идентификационных кодов в контроллер для автономной охраны
- установка пин-кода на клавиатуре контроллера для блокировки прибора пользователем (вне зависимости от ПЦН)

Отличительные особенности Приток-А-КОП-03:

- **Для производства используется более современная элементная база.**
- **Варианты исполнения контроллера с 2G и 3G модулями связи.**
- **Установка в комплект прибора модуля МС-04 (WiFi и Bluetooth) в любых вариантах — потребитель сам выбирает необходимую базовую комплектацию прибора.**
- **6 управляемых реле в контроллере — управление возможно как с клавиатур (локально), так и с АРМа (удаленно).**
- **Дополнительный вход для подключения внешнего РИП - обеспечение бесперебойного питания.**
- **Доработан алгоритм контроля баланса обоих СИМ карт (основной и резервной).**
- **Реализованы дополнительные команды, передаваемые с АРМ и выполняемые прибором — передача баланса на АРМ, выполнение произвольного USSD запроса, смена СИМ-карты по команде с АРМ, звонок по произвольному номеру и др.**
- **Расширено технологическое меню прибора — дополнительный функционал для тестирования и настройки прибора.**

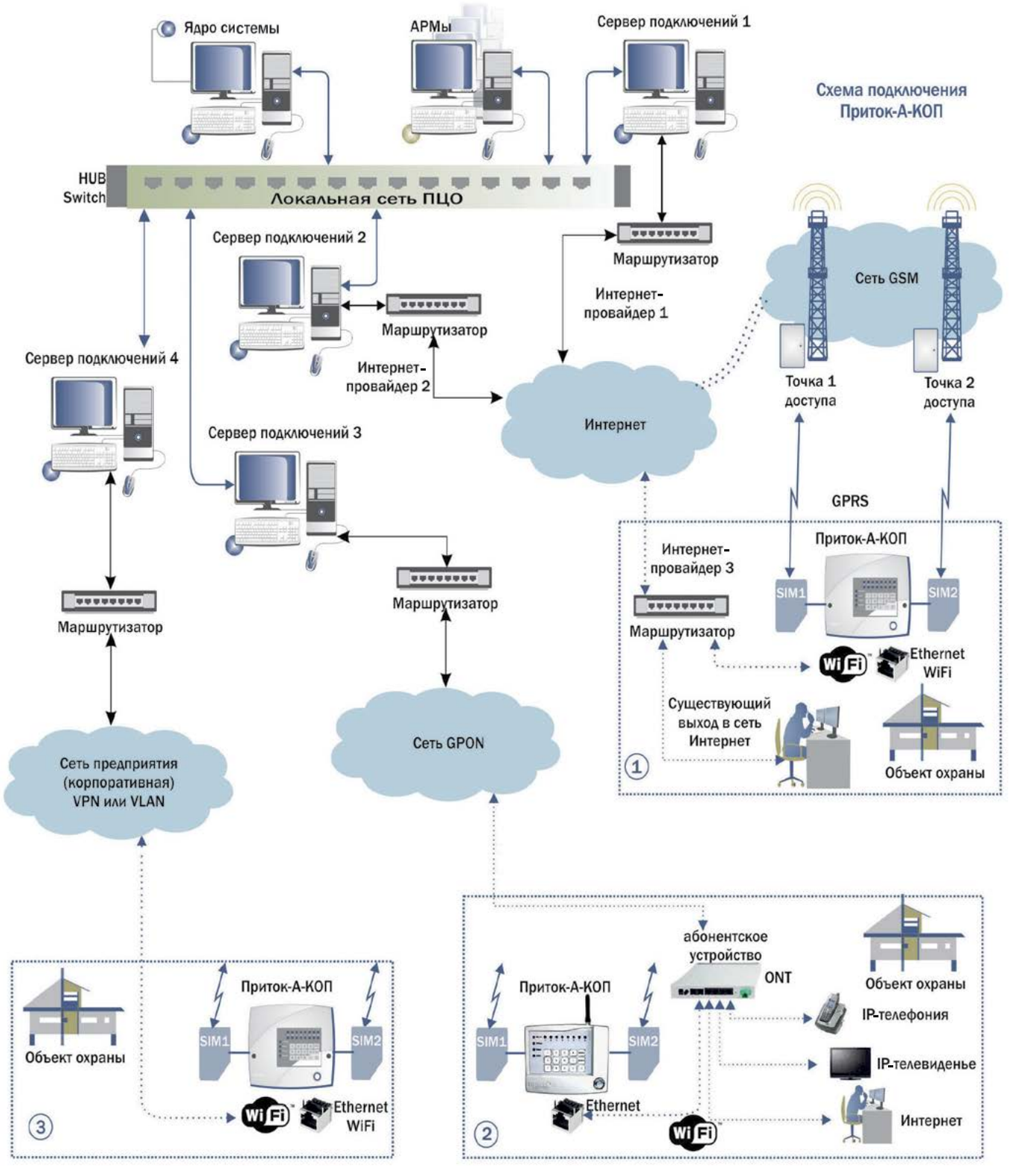


Функциональные возможности подключаемых по шине расширения модулей:

1. Модули расширения шлейфов
предназначены для увеличения количества контролируемых ШС. Возможно подключение до 28 модулей расширения шлейфов с общим количеством используемых ШС до 128, включая 16 ШС на контроллере КОП-01:
• Модуль расширения шлейфов Приток-А МРШ-02 — 4 дополнительных ШС;
• Модуль беспроводных датчиков Приток-А МБД-01 — подключение к одному МБД-01 до 32-х датчиков Ладога-РК через БРШС-РК-485 исполнение 1.

2. Модули индикации
предназначены для отображения состояния контролируемых ШС (до 128). Возможно подключение до 8 модулей индикации:
• Клавиатура ППКОП, Клавиатура ППКОП 16 (М4), Пульт выносной — управление взятием / снятием, светодиодная индикация состояния ШС;
• Клавиатура ППКОП-02 — управление взятием/снятием, отображение информации на ЖК-экране.
• Модуль связи Bluetooth Приток-А-ВС-02 — подключение мобильного устройства (смартфон / планшетный компьютер, работающие на базе ОС Android) в качестве клавиатуры.

3. Транзитные модули расширения
предназначены для расширения функционала системы, например для подключения приборов ППКОП-05(-05К) и РПДУ-03 или для измерения температуры и влажности окружающего воздуха. Возможно подключение до 16 модулей:
• Модуль гигрометра Приток-А-ВС-01 — измерение температуры и влажности;
• Приток-А-МС-01 — подключение приборов ППКОП-05(-05К) (до 30 шт).



Контроллер работает с «Сервером Подключений» (СП) системы Приток-А.

Каждый прибор может быть настроен на работу сразу с несколькими СП — через физически разные каналы связи (Ethernet и GPRS), используя различных провайдеров и поставщиков услуг связи.

Варианты подключений:

1) Подключение через существующий выход в сеть Интернет.

На охраняемом объекте, где есть подключение в сеть Интернет (используется пользователями), устанавливается маршрутизатор или используется уже имеющийся, через который подключается контроллер (подключением через WiFi или разъем RJ-45). Контроллер получает настройки сети и маршрутизации и производит подключение к СП через открытую сеть Интернет. Резервным каналом связи служит подключение через GPRS с использованием одной или двух SIM-карт — то есть можно использовать подключение двух разных провайдеров.

2) Подключение через сеть GPON.

В данном случае контроллер подключается в порт абонентского устройства ONT, который специально сконфигурирован для охраны, и через сеть PON подключается к СП на ПЦН. Резервным каналом связи также служат подключения GPRS через одну или две SIM-карты.

3) На крупных объектах охраны, которые оборудованы собственной локальной сетью, также подключается контроллер. В данном случае возможно непосредственное подключение в сеть (через Ethernet RJ-45 или WiFi) с использованием настроек (например, VPN или VLAN), через которую контроллер подключается к СП, а резервирование также через каналы GPRS с использованием одной или двух SIM-карт.

Порядок работы:

При наличии нескольких каналов связи (Ethernet, GPRS) приоритет их использования определяется в настройках контроллера. В зависимости от настройки контроллер выбирает основной канал для работы. В случае потери связи с СП по основному каналу контроллер переключается на резервный канал связи.

При работе на резервном канале связи контроллер периодически тестирует основной канал. При восстановлении основного канала связи контроллер переключается на него. Все операции по смене канала передаются на ПЦН в виде сообщений с указанием, на какой канал было переключение.

В канале GSM (GPRS) контроллер начинает работу по основной SIM-карте в зависимости от настроек. В случае потери связи с СП по основной SIM-карте контроллер переключается на резервную SIM-карту. При работе по резервной SIM-карте контроллер периодически тестирует возможность возврата на основную SIM-карту. Во время работы контроллер периодически проверяет состояние связи со всеми СП по указанным настройкам. При отсутствии связи с текущим СП контроллер переключается на рабочий СП, следующий в списке доступных.

Таким образом обеспечивается резервирование каналов связи и со стороны контроллера и со стороны ПЦН.

Конфигурирование параметров:

Настройка контроллера может производиться разными способами:

1) Параметры контроллера настраиваются программой, входящей в состав ПО Приток-А. Контроллер подключается стандартным miniUSB-кабелем к ПК под управлением Windows XP/Vista/7/8/10.

По умолчанию программа настроена на чтение настроек и после подключения заполнит поля ввода текущими настройками контроллера. Настраиваются типы шлейфов, тактика работы выходных ключей, параметры подключения по GPRS и Ethernet-сетям и др.

2) После установки контроллера на объекте и подключения его через СП на ПЦН возможно изменение параметров по каналам охраны (Ethernet и GPRS) — из АРМов системы. В АРМ ДПЦО предусмотрено отдельное окно настройки прибора, в котором доступны к изменению основные параметры работы контроллера (шлейфы, каналы связи, параметры переключения и пр.).

При работе через СП из АРМ ДПЦО есть возможность запроса с контроллера различных параметров — запросить версию ПО контроллера, баланс на SIM-картах, текущий канал связи, уровень GSM-сигнала и пр.

Также удаленно можно произвести обновление ПО контроллера ***(рис. 2).***

Контроллеры Приток-А-КОП активно развивающийся тип оборудования. Благодаря встроенной шине расширения, с возможностью подключения множества различных типов оборудования, и встроенным модулям связи WiFi и Bluetooth, с помощью контроллеров можно реализовать охрану объектов любой сложности. Использование нескольких каналов связи, различных типов подключения и управления контроллерами позволяет использовать их для охраны и мониторинга в различных сферах деятельности.

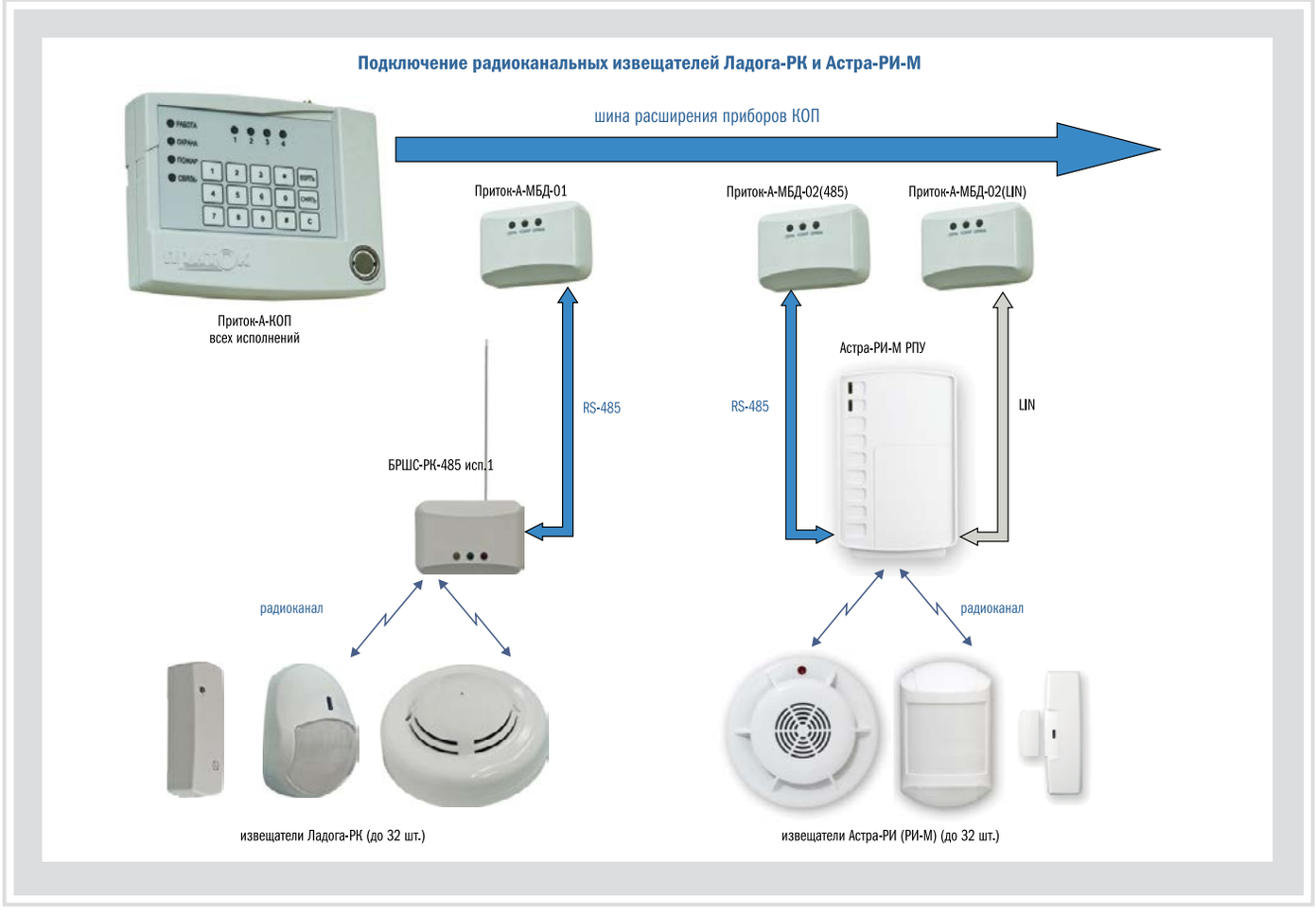
Подключение радиоканальных извещателей Ладога-РК и Астра-РИ-М

Один из вариантов подключаемого на шину расширения приборов серии КОП оборудования - Приток-А-МБД.

Модули Приток-А-МБД предназначены для подключения радиоканальных адресных извещателей и датчиков. На текущий момент выпускается несколько вариантов исполнения Приток-А-МБД для подключения оборудования систем Ладога-РК (ЗАО "РИЭЛТА" г. Санкт-Петербург) и Астра-РИ-М (ЗАО «ТЕКО» г. Казань).

Варианты исполнения:

- **Приток-А-МБД-01** — подключение по протоколу RS-485 к БРШС-РК-485 исп.1 — подключение до 32 извещателей радиоканальной системы Ладога-РК;
- **Приток-А-МБД-02(LIN)** — подключение по интерфейсу LIN к РПУ Астра-РИ-М — подключение до 32 извещателей радиоканальной системы Астра-РИ;
- **Приток-А-МБД-02(485)** — подключение протоколу RS-485 к РПУ Астра-РИ-М — подключение до 32 извещателей радиоканальной системы Астра-РИ.



Принцип работы заключается в определении модулем Приток-А-МБД радиоканальных извещателей мини-сети (радиоканала Ладога-РК или Астра-РИ-М) как своих внешних шлейфов.

В процессе работы Приток-А-МБД запрашивает радиоприемное устройство (БРШС-РК или РПУ) о текущем состоянии контролируемых каналов, и если в канале произошла смена его состояния (норма, тревога, КЗ, обрыв, пожар, низкое питание), то, в соответствии с типом и логическим состоянием шлейфа, на который отображается данный канал, передается соответствующее сообщение на КОП. Приборы серии КОП рассматривает МБД как свои внешние шлейфы.

В момент запуска прибора и инициализации шины расширения КОП конфигурирует МБД, определяя рабочие характеристики каждого шлейфа – тип, параметры и номер канала мини-сети, к которому «привязан» данный шлейф.

В рабочем режиме КОП получает информацию о смене состояний шлейфов МБД и, обрабатывая ее в соответствии с установленными алгоритмами, передает информацию на АРМы ПЦО.

Таким образом организуется передача извещений с радиоканальных датчиков различных подсистем.

ППКОП серии Приток-А

Приборы приемно-контрольные охранно-пожарные

ППКОП серии Приток-А предназначены для организации автоматизированной централизованной охраны объектов в режиме двусторонней связи «Объект-ПЦН». ППКОП подключаются к ПЦН через ретрансляторы серии Приток-А.

Принцип действия ППКОП Приток основан на постоянном контроле состояния шлейфов охранной, пожарной и тревожной сигнализации (ШС), обработке и индикации состояния ШС, формировании сообщений о режимах работы ППКОП и передаче их через ретрансляторы Приток-А, управлении световыми и звуковыми оповещателями, приеме и выполнении команд управления (рис. 1).

Передача извещений и прием команд управления между ППКОП и РТР производятся по физическим линиям, выделенным или занятым линиям связи телефонной сети с использованием амплитудно-фазовой манипуляции, в диапазоне частот 18 кГц, на скорости до 600 б/сек. В канале ППКОП-РТР применен двунаправленный с подтверждением приема информации, помехоустойчивый, имитостойкий, защищенный 128-разрядным динамическим кодом протокол передачи данных **P2V.**

При работе по занятым телефонным линиям ППКОП подключаются к ним через специальный фильтр, поэтому его работа не влияет на качество телефонной, факсимильной связи и работу ADSL-модемов стандарта ANNEX-B.

Все это обеспечивает: работу ППКОП без дежурного режима, первоначальную инициализацию ППКОП без участия персонала ПЦН, постоянный динамический контроль канала «Свой-чужой».

ППКОП обеспечивают автоматизированную постановку под охрану и снятие с охраны при помощи идентификационных кодов (ИК). ИК заносятся в базу данных ПЦН по каждому шлейфу. ППКОП передает ИК на ПЦН каждый раз при постановке под охрану, снятии с охраны. Переданный ППКОП ИК сравнивается с ИК, хранящимся в базе данных ПЦН, а также производится проверка других параметров по конкретному ШС (договорные отношения, режимное время и пр.). После получения разрешения на взятие (снятие) ППКОП включает (отключает) контроль состояния ШС и посылает активное сообщение «взят» («снят»). Сообщение фиксируется в базе данных, и на ППКОП отправляется сообщение (квитанция). После получения квитанции ППКОП на объекте информирует пользователя о завершении процедуры с помощью светового и звукового оповещателей.

Технические особенности ППКОП

- ППКОП выпускаются в нескольких вариантах исполнения, отличающихся количеством ШС, режимами работы, способами передачи сообщений.
- ППКОП, которые имеют встроенный резервированный источник питания, при отключении основного (~220 В) питания передают извещения о его пропаже и автоматическом переходе на резервное питание, а при разряде аккумулятора до минимально возможного уровня передают сообщение об отключении ППКОП.
- ППКОП, имеющие функцию концентратора, сами являются ППКОП и обеспечивают возможность подключения к ним по двухпроводной сигнальной линии до 29 шт. ППКОП-05. Коммуникаторы не являются ППКОП, они обеспечивают только обмен информацией между ППКОП и РТР. Протяженность сигнальной линии может быть до 1000 м.
- ППКОП имеют выходы для подключения световых и звуковых оповещателей, выносных считывателей, клавиатур и выносных пультов управления.

ВАРИАНТ ИСПОЛНЕНИЯ ППКОП	КОЛ-ВО ШЛЕЙФОВ	ФУНКЦИЯ КОНЦЕНТРАТОРА (КОММУНИКАТОРА)	ТИПЫ И КОЛ-ВО ПОДКЛЮЧАЕМЫХ ППКОП	ТИП ЛИНИИ СВЯЗИ	СПОСОБ ПОДКЛЮЧЕНИЯ К АРМ ПЦН	ТАКТИКА ВЗЯТИЯ/СНЯТИЯ	ЭЛЕКТРОПИТАНИЕ	РЕЗЕРВНОЕ ПИТАНИЕ (АККУМУЛЯТОР)
-01(8)	8	–	–	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	РАЗД.	~ 220В	2,2А*Ч
-01(16)	16	–	–	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	РАЗД.	~ 220В	2,2А*Ч
-03К	4	–	–	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР, ППКОП -032	ОБЩАЯ	~ 220В	2,2А*Ч
-031	4	–	–	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР, ППКОП -032	ОБЩАЯ	~ 220В	2,2А*Ч
-032	4	+	-031 - 1 ШТ.	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	ОБЩАЯ	~ 220В	2,2А*Ч
-041	8	+	-05 - 29 ШТ.	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	ОБЩАЯ	~ 220В	2,2А*Ч
-05К	3	–	–	ДВУХПРОВОДНАЯ ЛИНИЯ	ППКОП -041	ОБЩАЯ	+12В	–
-053К	3	–	–	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	ОБЩАЯ	+12В	–
КОММУНИКАТОР ППКОП-05	32	+	-05К 30 ШТ.	ТЛФ. ЛИНИЯ	РЕТРАНСЛЯТОР	–	~ 220В	2,2А*Ч

ППКОП-03к

ППКОП-01к (8) ШС

ППКОП-01к (16) ШС

Отличительные особенности ППКОП серии Приток-А

• работают по линиям связи телефонной сети или по физическим линиям на частоте 18 кГц

• автоматизированная постановка под охрану и снятие с охраны при помощи ЭИ и (или) клавиатуры

• двусторонний, имитостойкий протокол в канале ретранслятор (РТР) — ППКОП, защищенный 128-разрядным динамическим кодом — протокол Р2V

• наличие телефонного фильтра на плате прибора

• адаптивная подстройка чувствительности приемника ППКОП под индивидуальные параметры линии связи

• защита входных и выходных цепей

• наличие шины расширения для подключения внешних и внутренних устройств

• наличие встроенной программы тестирования и настройки

• обеспечение настройки параметров шлейфов и приемопередатчика с клавиатуры прибора

• возможность подключения выносной клавиатуры и выносного пульта ППКОП

• наличие двух силовых ключей с контролем исправности нагрузки (в соответствии с требованиями НПБ для «пожарки»)

• для ППКОП исполнения -01, -03, -041, -042 и их модификаций наличие встроенного импульсного блока резервированного питания и возможность подключения внешнего аккумулятора емкостью до 10 А/час

Применение имитостойкого, помехозащищенного протокола передачи данных обеспечивает защиту от подключения на линии связи канала РТР — ППКОП эквивалентов ППКОП, а наличие автоматической подстройки чувствительности приемника в канале РТР — ППКОП под индивидуальные параметры линии связи исключает ложные срабатывания в системе охраны.

ППКОП-05

ППКОП-053к

Каталог

- **Подсистемы**

Приток TCP/IP
Приток-А
Приток-А-Ф-01.3
Приток-GSM
Приток-МКР
Приток-МПО
Приток-РКС
Приток-РЛС
Приток-А-Р
Приток-Видео
Приток-СКД
Приток-РТП

В данном разделе представлена информация, раскрывающая общее назначение, структуру и особенности всех подсистем ИС Приток-А

Информация, приведенная в данном разделе, не является документацией и носит только рекламно-информационный характер

Технические характеристики и правила эксплуатации отдельных компонентов и подсистем ИС «Приток-А» указаны в паспортах и руководствах по эксплуатации на конкретные программные и аппаратные руководства

Приток-TCP/IP
Подсистема телекоммуникационных связей ИС Приток-А

Оборудование и программное обеспечение каналов передачи данных ИС ОПС Приток-А, или Подсистема телекоммуникационных связей ИС Приток-А, работает с применением протокола TCP/IP Transmission Control Protocol / Internet Protocol (Протокол управления передачей / Интернет Протокол).

Этот протокол является современным технологическим средством, на основе которого построена мировая сеть Интернет. Сегодня в мире производится широкая номенклатура изделий, применяемых для передачи информации в высокоскоростных каналах передачи данных, которые используют для этого протокол TCP/IP.

Подсистема телекоммуникационных связей — Приток-TCP/IP предназначена для создания объединенной сети серверов, рабочих станций ПЦН и другого оборудования, включенного в состав ИС Приток-А. Приток-TCP/IP обеспечивает передачу информации (команд и извещений) по цифровым каналам передачи данных, что позволяет строить распределенную, масштабируемую, высокопроизводительную, гибкую по функциям систему обеспечения безопасности.

Приток-TCP/IP, используя возможности протокола TCP/IP и UDP, позволяет реализовать взаимодействие локальной вычислительной сети ПЦН (серверов и рабочих станций пользователей системы) с техническими средствами безопасности, включенными в состав ИС Приток-А (элементами системы), расположенными в любой точке распределенных сетей предприятий (WAN) и (или) глобальных сетей (VPN и Интернет), независимо от физической среды передачи данных.

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

- локальные сети стандарта Ethernet 10/100/1000
- сети Radio Ethernet
- телефонные каналы с использованием xDSL-модемов
- 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).
- сети Ethernet, работающие по каналам сотовой связи стандартов GSM, CDMA, 3G и 4G
- сети открытого интернета и любые другие каналы связи (и в любом сочетании), поддерживающие протокол TCP/IP и UDP и имеющие интерфейс стандарта Ethernet

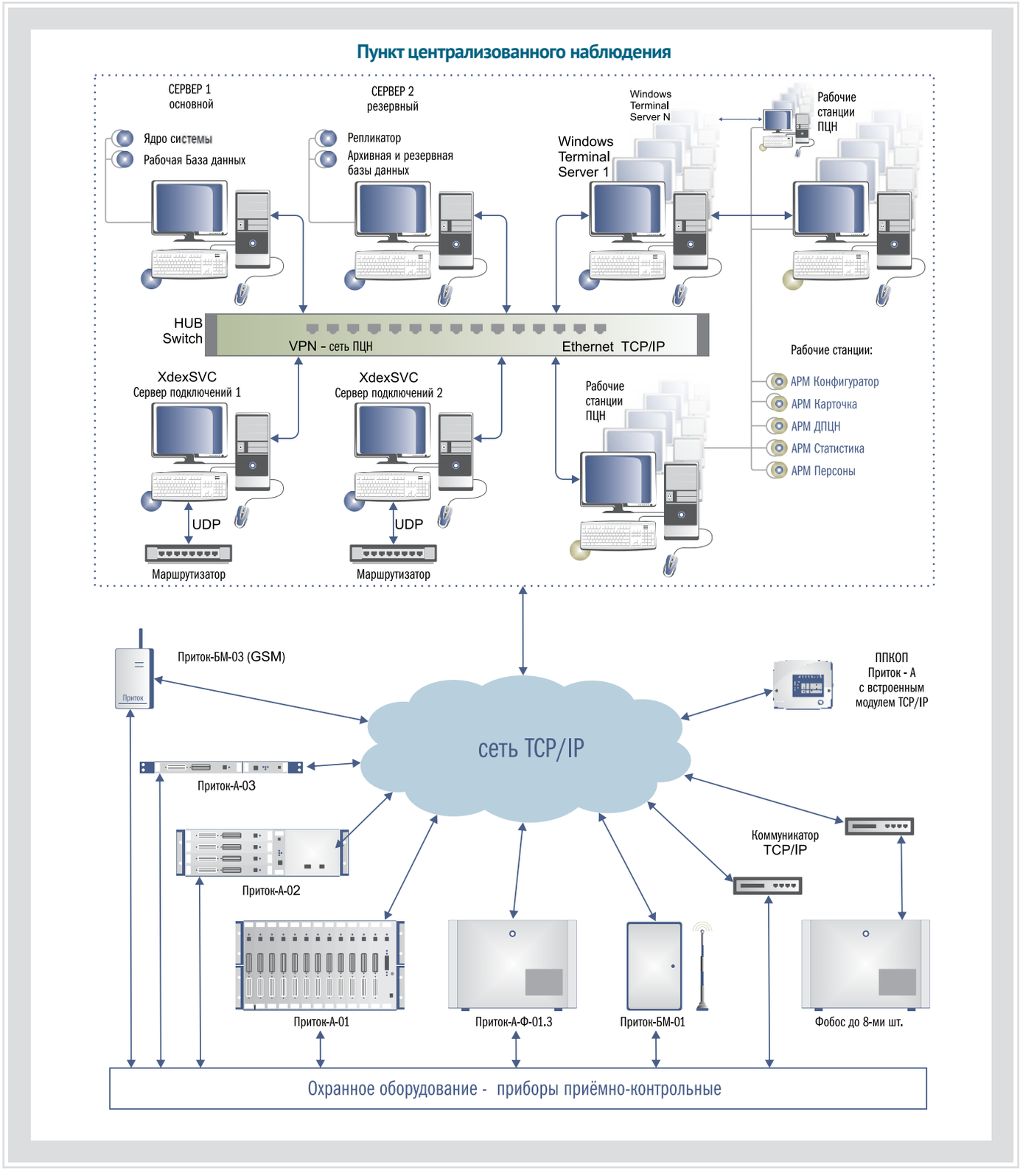
Основным физическим элементом подсистемы Приток-TCP/IP является универсальное устройство **Коммуникатор TCP/IP ЛИПГ.468362.006.** Для передачи извещений в сети ПЦН Коммуникатор TCP\IP преобразует протоколы, по которым работает оборудование, подключаемое к сети ПЦН (в состав ИС Приток-А) в протокол TCP/IP, и обеспечивает передачу информации по всем вышеперечисленным каналам передачи данных.

В настоящее время выпускаются три варианта исполнения Коммуникатора TCP/IP, они отличаются вариантами подключения источников питания (см. прайс-лист). Но чтобы можно было использовать данные коммуникаторы для объединения большого количества разнородной аппаратуры, потребителям системы Приток-А доступны

Таблица 1

ПОДКЛЮЧАЕМОЕ ОБОРУДОВАНИЕ	КОЛ-ВО ПОДКЛ. ОБОР.	ВЕРСИЯ ПО	КАНАЛ СВЯЗИ С ОБОРУДОВАНИЕМ	ИСТОЧНИК ПИТАНИЯ	
				60В	12В
РЕТРАНСЛЯТОРЫ ФОБОС, ФОБОС-А, ФОБОС-3	1-8	F3A	1650 ГЦ (200 БИТ/СЕК)	+	
РЕТРАНСЛЯТОР ПРИТОК-А-Ю	1-5	JUP	18 КГЦ (200 БИТ/СЕК)	+	
БЛОК СОПРЯЖЕНИЯ БС-04(-05)	1	BSS	RS-232 (19200 БИТ/СЕК)	+	
ПРИБОР ППКОП 011-8-1-05	1-30	PPK05	18 КГЦ (200 БИТ/СЕК)		+
ПРИБОР ППКОП 011-8-1-01 (-02, -03, -041, -053), КОММУНИКАТОР ППКОП-05	1	PPKN	18 КГЦ (200 БИТ/СЕК)		+
КОММУНИКАТОР CONTACT-ID	1	MIS	RS-232 (9600 БИТ/СЕК)	+	
ПРИТОК –А-Р РАДИОРЕТРАНСЛЯТОРЫ	1	RR	ТЧ (1200 БИТ/СЕК)		+

Полный перечень вариантов исполнения коммуникаторов и соответствующих им программ приводится в руководстве по эксплуатации поставляемого программного обеспечения. Это количество постоянно увеличивается.



Подсистема Приток-TCP/IP позволяет строить комплексные системы безопасности, не ограниченные как в количественном составе элементов, так и в пространстве, то есть предназначенные как для охраны отдельно взятой квартиры, автомобиля, так и для охраны (мониторинга) крупных предприятий, городов, районов. Таким образом, на предприятиях, в учреждениях, в районах, где развиты высокотехнологичные средства связи по скоростным цифровым каналам, ПЦН комплексных систем безопасности можно строить быстро и с минимальными затратами, применяя технологию подсистемы Приток-TCP/IP.

около трех десятков прикладных программ, созданных для работы коммуникатора в составе ИС Приток-А.

То есть, приобретя одно физическое устройство – Коммуникатор-TCP/IP – и загрузив в него необходимую программу, вы можете использовать его в существующих и будущих вариантах.

Выбор необходимой конфигурации и режима работы Коммуникатора в зависимости от типа поддерживаемого устройства осуществляется конфигурационными перемычками и загрузкой необходимой программы. То есть коммуникаторы отличаются только программным обеспечением, которое загружается в них перед включением в систему.

В таблице приведены некоторые примеры исполнения коммуникаторов (см. таблицу 1).

Полный перечень вариантов исполнения коммуникаторов и соответствующих им программ приводится в руководстве по эксплуатации поставляемого программного обеспечения. Это количество постоянно увеличивается.

Коммуникатор TCP/IP представляет собой универсальный контроллер, который предназначен для связи различных элементов ИС Приток-А и подключения их в сеть ПЦН ИС Приток-А. Этот универсальный контроллер обеспечивает подключение в сеть ПЦН как оборудования ОПС, выпускаемого ОБ «СОКРАТ», так и оборудования ОПС других производителей.

Коммуникаторы, которые выпускаются в отдельном корпусе, обычно применяются для включения в систему оборудования, работающего не по протоколу TCP/IP. Это оборудование, которое выпущено ОБ «СОКРАТ» ранее, или оборудование других производителей. Все современное оборудование, выпускаемое ОБ «СОКРАТ», которое работает с применением протокола TCP/IP, имеет в себе встроенные коммуникаторы.

Ядром Коммуникатора TCP/IP является модуль TCP/IP-01, который разработчики называют «WizARM». Для современного Коммуникатора был разработан свой модуль TCP/IP-01. При разработке применен способ организации программного обеспечения, позволяющий пользователю самостоятельно менять прошивку модуля, или — **«Прикладную управляющую программу».**

Эта технология в свое время применялась при разработке первой версии системы Приток-А еще в 1990 году. По этой причине ИС Приток-А завоевала популярность у пользователей как легко перенастраиваемая система.

Новое — это хорошо забытое старое. Так вот, эта существенно обновленная технология позволяет:

1.1. Иметь один аппаратно разработанный коммуникатор на все случаи жизни (по крайней мере, в обозримом будущем);

1.2. Обеспечить готовность коммуникатора к работе сразу после включения, так как все программы и настройки хранятся во флэш-памяти;

1.3. Производить прямо из АРМ ПЦН по каналам Ethernet установку (замену) прикладной программы, необходимой для работы с подключаемым оборудованием, новой версии работающей программы или принципиально новой по функциям программы, для создания новой системы;

1.4. Специалистам Охранного бюро «СОКРАТ» легко и быстро разрабатывать новые прикладные программы.

Для удобства эксплуатации системы Приток ее потребителям прямо на сайте доступны около тридцати прикладных программ, созданных для работы Коммуникатора в составе ИС Приток-А. **Бери и пользуйся. Результаты доступны всем, хотя могли разрабатываться и внедряться для одного подразделения.**

Таким образом, приобретая одно физическое устройство — Коммуникатор-TCP/IP, вы обеспечиваете себе возможность применять его практически по своему назначению. А если понадобится, то перепрограммировать его для использования в совершенно новых условиях, с новыми функциями.

Очевидно, что эта очень перспективная технология в дальнейшем будет совершенствоваться, развиваться и получит новые свойства. Это очень устойчивая база для всех разработок, проводимых специалистами ОБ «СОКРАТ».

Особенности Приток-TCP/IP

- возможность организации связи оборудования ОПС с ПЦН без применения уже устаревших контроллеров систем передачи извещений и блоков сопряжения
- возможность использования всех существующих каналов передачи данных для организации сети ПЦН
- рентабельность применения при организации малых ПЦН, а также при разветвленной структуре расположения АТС, на которых устанавливаются базовые элементы ИС Приток-А: ретрансляторы Приток-А, БМ-А-Р, БМ-GSM, БМ-МПО и (или) оборудование других производителей, включаемых в состав сети ПЦН

Применяя технологию TCP/IP-коммуникаций, мы практически снимаем ограничение по количеству охраняемых объектов или охраняемой площади. Например, только периметр иркутского авиазавода (корпорация «Иркут»), за которым следит «Приток», имеет длину примерно 47 километров.

Подсистема телекоммуникационных связей Приток-TCP/IP позволила создавать ПЦН, которые могут охранять целые города и даже группу городов. В частности, такие проекты с помощью ОБ «СОКРАТ» реализованы во вневедомственной охране на юге России. Под охраной системы Приток-А находятся 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 учетом того, что сегодня ГУВО МВД РФ ставит задачу перед техническими специалистами вневедомственной охраны производить объединение (укрупнение) ПЦН, система Приток становится наиболее востребованной при решении этой задачи.

Приток-А

Подсистема охранно-пожарной сигнализации с использованием линий связи телефонных сетей

Подсистема предназначена для организации централизованной охраны объектов по физическим линиям, выделенным или занятым линиям связи телефонной сети.

Подсистема была основой для создания и дальнейшего развития всей Интегрированной системы охранно-пожарной сигнализации Приток-А. Она может работать как в составе ИС ОПС Приток-А совместно с другими подсистемами, так и автономно.

Подсистема включает в себя ретрансляторы Приток-А, Приток-АФ-03, а также устаревшие версии ретрансляторов - Фобос, Фобос-А, Фобос-3, Фобос-ТР, Приток-А-Ю, Приток-А-Ф и др. со всеми оконечными устройствами и ППКОП. Так как ретрансляторы серии Приток обеспечивают работу и с УО, работающими по протоколу Фобос-3, то они могут устанавливаться на замену ретрансляторов Фобос-3 и Фобос-ТР.

Основу подсистемы Приток-А составляют ретрансляторы серии Приток-А.

Основные элементы подсистемы

- серия ретрансляторов Приток-А и Приток-А-Ф
- приборы приемно-контрольные, концентраторы и коммуникаторы серии Приток-А
- вторичные источники резервированного питания Приток-ИП

Все эти элементы полностью удовлетворяют современным требованиям централизованной охраны и учитывают тенденцию развития средств связи и коммуникаций.

Ретрансляторы Приток-А

Ретрансляторы Приток-А предназначены для создания подсистемы автоматизированной централизованной охраны объектов Приток-А с использованием приборов приемно-контрольных, охранно-пожарных (ППКОП), подключаемых к ретрансляторам по линиям связи телефонной сети или по физическим линиям, в диапазоне частот 18 кГц.

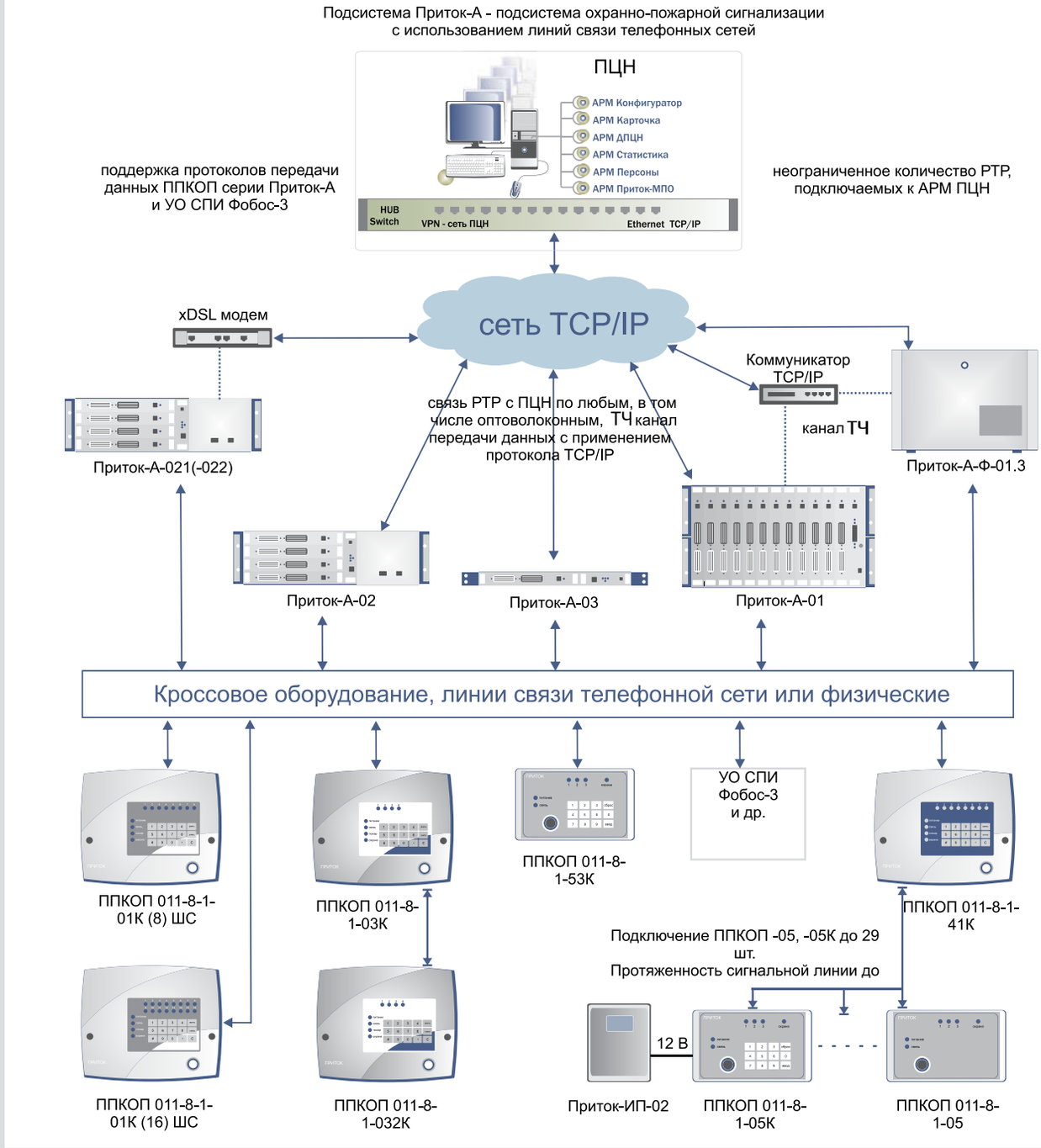
Конструктивно РТР Приток-А выполнены в корпусах стандарта МЭК297 для установки в стойки «Евромеханика 19», РТР Приток-А-Ф-01.3 выполнен в корпусе Приток-А-Ф (Фобос-3). В **таб. 2** приведены отличительные характеристики всех типоразмеров и вариантов, выпускаемых РТР.

Учитывая то, что развитие телефонной сети производится с применением АТС малой емкости (АТС в каждый дом), работающих по оптоволоконным линиям связи, РТР серии Приток идеально подходят для применения их в этих условиях.

РТР серии Приток-А поддерживают протоколы передачи данных ППКОП серии Приток-А вариантов исполнения -01,-02,-03,-041,-042,-053, коммуникаторов Приток ППКОП-05, Приток-С-20, Астра-РИ, Приток-А-РКС, Приток-А-У и приборов других производителей, таких как: Сигнал-ВК исп.5 и УО-1А, УО-2, УО-2А, УО-3К, УО-2А-Р, УО-Фобос-ТР, УО Атлас, Атлас-6.

Отличительные особенности и преимущества РТР Приток-А реализуются при установке на объектах приборов Приток-А. На следующей странице в таб. 1. приведены эти особенности. Совместное применение РТР, ППКОП и коммуникаторов с автоматизированной тактикой постановки-снятия с охраны серии Приток позволяет оборудовать средствами охранной, пожарной и тревожной сигнализаций объекты любой категории сложности. РТР Приток-А-01 может обеспечить охрану до 7200 объектов, контроль до 22800 шлейфов охранной, пожарной и (или) тревожной сигнализаций.

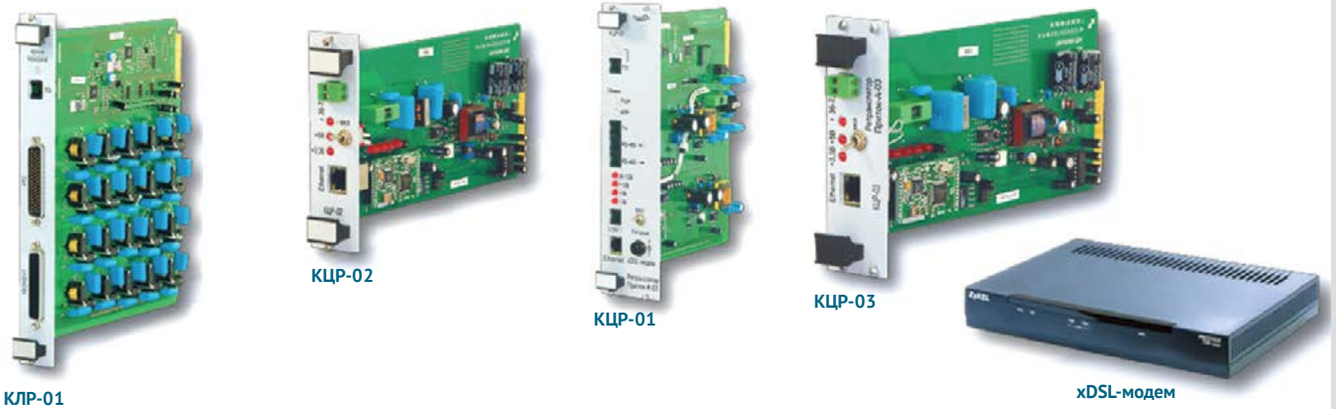
Применение имитостойкого, помехозащищенного протокола передачи данных обеспечивает защиту от подключения на линии связи канала РТР – ППКОП эквивалентов ППКОП, а наличие автоматической подстройки чувствительности приемника в канале РТР – ППКОП под индивидуальные параметры линии связи исключает ложные срабатывания в системе охраны.



Особенности ретрансляторов

- связь РТР с ПЦН по любым, в том числе оптоволоконным, каналам передачи данных с применением протокола TCP/IP
- неограниченное количество РТР, подключаемых к АРМ ПЦН
- поддержка протоколов передачи данных ППКОП серии Приток-А и УО СПИ Фобос-3
- двусторонний имитостойкий протокол в канале РТР—ППКОП, защищенный 128-разрядным динамическим кодом
- установка уровней сигнала передатчика и чувствительности приемника при помощи расширенных команд с АРМ ПЦН и измерение уровня входного сигнала с ППКОП для каждого направления
- адаптивная подстройка чувствительности приемника в канале РТР—ППКОП под индивидуальные параметры линии связи

Ретрансляторы системы Приток-А



КЛР-01 работает с 20 направлениями, УЛК-03 работает с 15 направлениями, в комплект РТР входят:
В Приток-А-01 — 1 контроллер центральный КЦР-01 и до 12-ти КЛР-01.
В Приток-А-02 — 1 контроллер центральный КЦР-02 и до 4-х КЛР-01.
В Приток-А-03 — 1 контроллер центральный КЦР-03 и 1 КЛР-01.
В Приток-А-Ф-01.3 — 1 контроллер центральный КЦР-АФ-03 и до 4-х УЛК-03
В Приток-А-Ф-02.3 — 1 контроллер центральный КЦР-АФ-03 и до 8-ми УЛК-03
Ретрансляторы Приток-А-021 и Приток-А-022 дополнительно комплектуются ADSL-модемами и SHDSL-модемами соответственно. Напряжение питания для всех РТР от 36 до 72 В постоянного тока.

Таблица 1

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ РТР ПРИ РАБОТЕ С ППКОП СЕРИИ ПРИТОК-А	
КОЛИЧЕСТВО ППКОП, ПОДКЛЮЧАЕМЫХ ЧЕРЕЗ КОММУНИКАТОРЫ НА ОДНО НАПРАВЛЕНИЕ	ДО 30 ПРИБОРОВ (ППКОП)
ПРОТОКОЛ ПЕРЕДАЧИ ДАННЫХ В КАНАЛЕ РТР – ППКОП	ИМИТОСТОЙКИЙ, ДВУНАПРАВЛЕННЫЙ, С ПОДТВЕРЖДЕНИЕМ ПРИЕМА ИНФОРМАЦИИ, ЗАЩИЩЕННЫЙ 128-РАЗРЯДНЫМ ДИНАМИЧЕСКИМ КОДОМ
СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ В КАНАЛЕ РТР – ППКОП	АДАПТИВНАЯ, ДО 600 Б/С, В ЗАВИСИМОСТИ ОТ ИНДИВИДУАЛЬНЫХ ПАРАМЕТРОВ ЛИНИИ СВЯЗИ
ВИД МОДУЛЯЦИИ В КАНАЛЕ РТР – ППКОП	АДАПТИВНЫЙ, В ЗАВИСИМОСТИ ОТ ТИПА ПОДКЛЮЧАЕМОГО ППКОП ИЛИ УО
ДИАПАЗОН ЧУВСТВИТЕЛЬНОСТИ В КАНАЛЕ РТР – ППКОП	АДАПТИВНЫЙ, ОТ 20 ДО 200 МВ, В ЗАВИСИМОСТИ ОТ ИНДИВИДУАЛЬНЫХ ПАРАМЕТРОВ ЛИНИИ СВЯЗИ

Таблица 2

ОСНОВНЫЕ ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ РТР				
ВАРИАНТ ИСПОЛНЕНИЯ РТР	КОЛИЧЕСТВО ПОДКЛЮЧАЕМЫХ НАПРАВЛЕНИЙ	КАНАЛ СВЯЗИ АРМ ПЦН-РТР	КАНАЛ ПОДКЛЮЧЕНИЯ ДОПОЛНИТЕЛЬНЫХ РТР	ТИПОРАЗМЕР КОРПУСА
ПРИТОК-А-01	ОТ 20 ДО 240	ТЧ-КАНАЛ, ETHERNET	RS-485. ETHERNET	19»/6U
ПРИТОК-А-02	ОТ 20 ДО 80	ETHERNET	ETHERNET	19»/3U
ПРИТОК-А-021	ОТ 20 ДО 80	ADSL-МОДЕМ	ETHERNET	19»/3U
ПРИТОК-А-022	ОТ 20 ДО 80	SHDSL-МОДЕМ	ETHERNET	19»/3U
ПРИТОК-А-03	ДО 20	ETHERNET	ETHERNET	19»/1U
ПРИТОК-А-Ф-01.3	ОТ 15 ДО 60	ТЧ-КАНАЛ, ETHERNET	RS-485. ETHERNET	ПРИТОК-А-Ф (ФОБОС-3)
ПРИТОК-А-Ф-02.3	ОТ 15 ДО 120	ТЧ-КАНАЛ, ETHERNET	RS-485. ETHERNET	ПРИТОК-А-Ф (ФОБОС-3)

Ретранслятор Приток-А-Ф-01.3

С меньшими затратами к большему эффекту

В связи с тем, что РТР серии Приток-А обеспечивают работу с УО, работающими по протоколу Фобос-3, то они могут устанавливаться вместо отработавших срок и снимаемых с производства ретрансляторов Фобос-3 и Фобос-ТР, это обеспечивается следующим образом:

1. В комплект поставки РТР Приток-А могут входить кабели-переходники, обеспечивающие соединение с разъёмами на кроссе, к которым были подключены Фобос-3 или Фобос-ТР.

2. Ретрансляторы Приток-А-Ф-01.3 (02.3) конструктивно совпадают с ретрансляторами Фобос-3 и Фобос-ТР и могут устанавливаться непосредственно на место снимаемых ретрансляторов Фобос-3 или Фобос-ТР.

3. Для того чтобы вообще не производить замену корпусов ретрансляторов Фобос-3 или Фобос-ТР, достаточно применять «Комплект модернизации РТР Фобос-3».

В этот комплект входят КЦР-А-Ф-03 и УЛК-03. Модернизация производится путём замены платы УЦР ретранслятора Фобос на плату КЦР-А-Ф-03, а плат УЛК на платы УЛК-3 без дополнительного переоборудования места установки ретранслятора. Таким образом, ретрансляторы Фобос-3 или Фобос-ТР становятся ретранслятором Приток-А-Ф-01.3 со всеми характеристиками и достоинствами ретрансляторов Приток-А.

Все способы замены или модернизации ретрансляторов позволяют избежать единовременной замены объектового оборудования при переходе с эксплуатации ретрансляторов Фобос-3 на эксплуатацию ретрансляторов Приток-А.

Все вышеперечисленные характеристики и особенности РТР Приток-А позволяют с успехом применять их как на существующих ПЦН, в процессе их развития и модернизации, так и на вновь создаваемых ПЦН.

КЦР-А-Ф-03

УЛК-03

Приток-GSM

Подсистема охраны, мониторинга, управления и оповещения по каналам сотовой связи

Подсистема Приток-GSM предназначена для централизованной и (или) для автономной (индивидуальной) охраны и мониторинга объектов, для создания системы SMS-оповещения по каналам сотовой связи стандарта GSM 900/1800.

Приток-GSM может работать как в составе Интегрированной системы охранно-пожарной сигнализации Приток-А, так и автономно. Количество контролируемых объектов не ограничено. Особенностью Приток-GSM является то, что извещения о состоянии охраняемого объекта могут передаваться как на ПЦН, так и одновременно на мобильный телефон собственника.

Приборы подсистемы предназначены для организации централизованной или автономной охраны объектов (квартир, дач) с автоматизированной тактикой взятия под охрану и снятия с охраны. Для передачи сообщений и приема команд используется сеть GSM выбранного оператора сотовой связи (ОСС). Приборы имеют возможность в случае неполадок в работе основного ОСС переключиться на SIM-карту резервного. Тревожное или информационное уведомление может производиться дозвоном на заданный телефонный номер, отсылкой SMS сообщений или передачей сообщения в режиме GPRS. Режим GPRS является основным и приоритетным режимом работы прибора.

Основные технические характеристики

- в ППКОП-011 используется 2 SIM-карты для резервирования канала
- ППКОП-011 имеют восемь шлейфов сигнализации с возможностью установки типа шлейфа - ОС, ПС, ТС
- имеется возможность подключения токопотребляющих пожарных датчиков, которые работают от напряжения не ниже 19 В
- ППКОП имеют четыре выхода для подключения звуковых и световых оповещателей, выносных индикаторов и реле управления электрооборудованием
- питание ППКОП-011М производится от внешнего источника питания +12 В
- ППКОП-011-01 и -01К имеют встроенный резервированный ИП, подключаемый к сети переменного тока ~220 В. Низкое энергопотребление ППКОП обеспечивает его работу от резервного источника питания в течение нескольких суток
- в БМ-GSM и в ППКОП-011 могут применяться SIM-карты любых операторов
- в ППКОП-011 может быть записано до шести телефонных номеров, на которые он передает сообщения. Команды управления ППКОП принимает только с номеров телефонов, которые в нем записаны
- для постановки и снятия с охраны при помощи электронных идентификаторов к ППКОП-011 подключаются выносные считыватели, выносные пульты управления или клавиатура ППКОП.
- ППКОП-011 имеют встроенную антенну, а при необходимости подключается выносная

Принцип действия централизованной охраны

Основан на применении приборов приемно-контрольных охранно-пожарных ППКОП-011, устанавливаемых на охраняемых объектах и сотового телефона (телефонов) собственника.

К ППКОП-011 подключаются датчики охранной, пожарной, тревожной сигнализации и/или датчики утечки воды, газа. ППКОП-011 передает сообщения о состоянии датчиков на несколько (до шести) мобильных телефонов — собственника, членов его семьи, доверенных лиц, охраны и т.п., а также принимает и исполняет команды (взять под охрану, снять с охраны, включить, выключить и т .д.) с телефонов, зарегистрированных в ППКОП-011.

Состав подсистемы Приток-GSM

- базовый модуль **базовый модуль Приток-А-БМ-03(-04,-04.01) (GSM) (далее БМ GSM)**
- прибор охранно-пожарный **ППКОП 011-8-1-011М** Приток-А-4(8) (далее ППКОП-011М)
- прибор охранно-пожарный **ППКОП 011-8-1-011-1 Приток-А-4(8)** (далее ППКОП-011-01)
- прибор охранно-пожарный **ППКОП 011-8-1-011-1К Приток-А-4(8)** (далее ППКОП-011-01К)

Принцип действия автономной охраны

Основан на применении таких же ППКОП-011, но передающих сообщения и принимающих команды управления с АРМ ПЦН и с сотового телефона (телефонов) собственника.

Для создания ПЦН Приток-GSM необходимо к АРМ Приток-А подключить БМ GSM. БМ подключается к АРМ ПЦН с применением протокола TCP/IP. Один из шести номеров сотовых телефонов, с которыми ППКОП-011 может работать, в этом случае присваивается БМ.

При работе ППКОП-011 с АРМ ПЦН в режиме GPRS доступ с остальных телефонов собственника прекращается.

Постановка под охрану производится с применением электронных идентификаторов Touch Memory, клавиатуры или бесконтактных карт, а также дистанционно с помощью команд, передаваемых с АРМ ПЦН и (или) с сотовых телефонов собственника, в режиме SMS-сообщений или GPRS, и воспринимаемых ППКОП-011 только в том случае, если они приходят с номеров телефонов, зарегистрированных в его памяти.

Снятие с охраны производится только с применением электронных идентификаторов Touch Memory, клавиатуры или бесконтактных карт.

Дополнительные свойства Приток-GSM

Удобная процедура постановки под охрану и снятие с охраны электронными идентификаторами Touch Memory, клавиатуры или бесконтактными картами, а также контроля, по состоянию внешних индикаторов, за выполнением этих команд.

Управление взятием объекта под охрану может производиться и дистанционно, с помощью команд, подаваемых с АРМ ПЦН или с сотового телефона (телефонов) собственника на ППКОП-011 в режимах дозвона, SMS-сообщений и GPRS. Команды воспринимаются только в том случае, если они приходят с телефонов, зарегистрированных в памяти ППКОП-011.

Гарантированная доставка сообщений обеспечивается методом трех режимов, это означает, что при невозможности передачи сообщения в режиме GPRS, ППКОП-011 автоматически переходит в режим SMS-сообщений и автодозвона на остальные номера телефонов, имеющиеся в его памяти.

Любые сотовые телефоны, зарегистрированные в базе данных АРМ ПЦН, могут использоваться в качестве тревожной кнопки. Таким образом, для оборудования объекта ТС достаточно просто сотового или стационарного телефона с функцией быстрого набора номера — нет необходимости монтажа на временных объектах.

В связи с тем, что зона покрытия сотовой связи стандарта GSM не ограничена, то радиус действия Приток-GSM тоже не ограничен. Практически вы можете проконтролировать свою собственность из любой точки мира.

SMS-оповещение собственников о состоянии любого объекта охраны

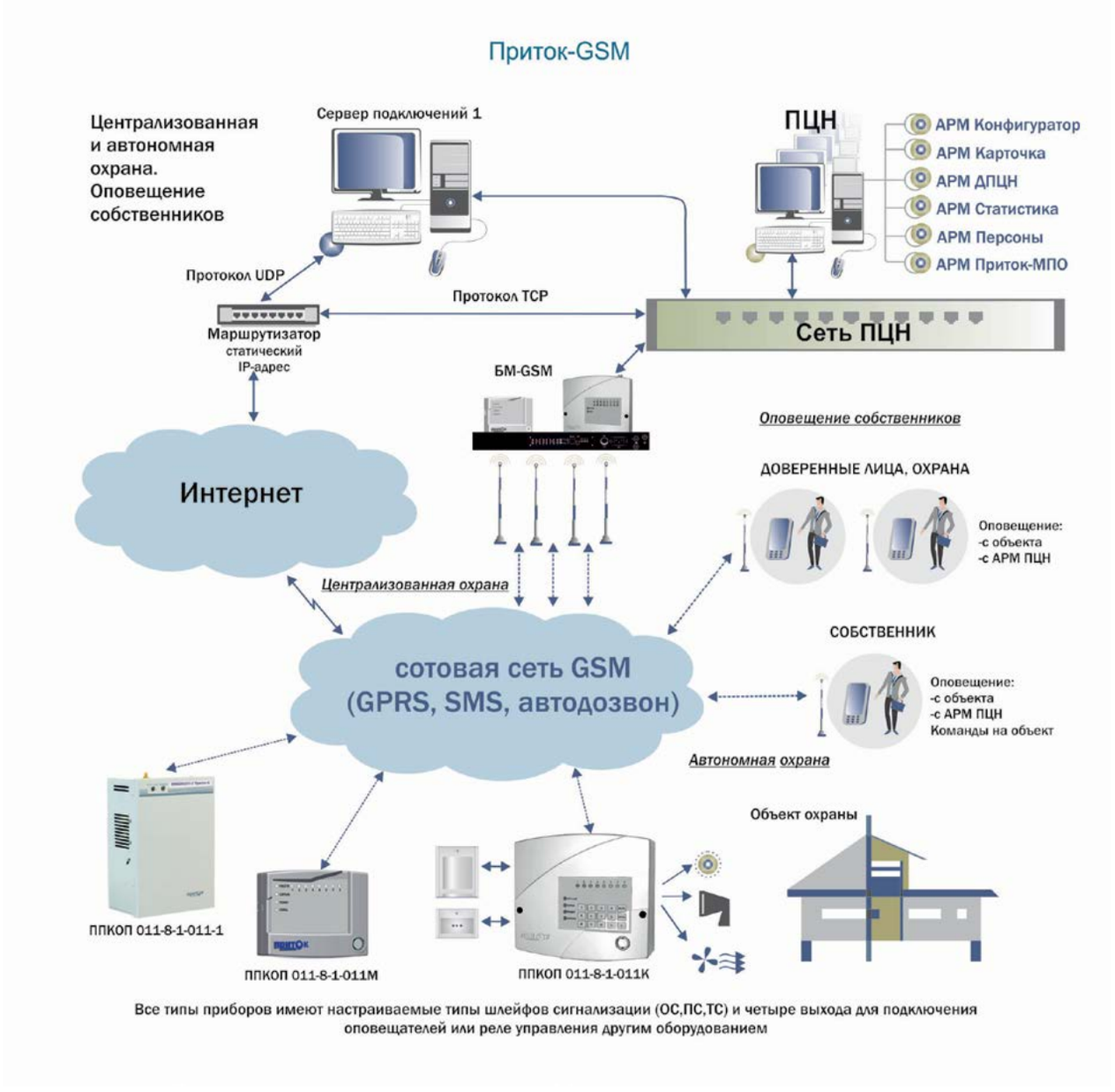
БМ GSM подсистемы Приток-GSM может быть использован для организация оповещения.

SMS-оповещение применяется с целью информирования собственников объектов (пользователей системы) о состоянии охраняемых объектов, о событиях, происходящих в системе.

Принцип действия SMS-оповещения основан на передаче с АРМ ПЦН на телефон (телефоны) собственника SMS-сообщений о состоянии технических средств охраны (ТСО) и о событиях (взятие, снятие, тревога и т.д.), происходящих на охраняемом объекте.

SMS-оповещение производится вручную путем подачи команд с АРМ ПЦН (например подача заявки обслуживающему технику) и (или) автоматически по событиям или по запросу собственника. Для этого в АРМ ПЦН создается библиотека сообщений, из которой вручную или автоматически, по событию, выбирается нужное и передается абоненту.

SMS-оповещение собственников о состоянии ТСО и событиях, происходящих на объектах, может **производиться на всех подсистемах ИС Приток-А,** независимо от типов применяемых ППКОП, коммуникаторов, концентраторов и каналов передачи данных, по которым они работают.



Особенности подсистемы Приток-GSM

- автономная и централизованная охрана с гарантированной доставкой сообщений в режимах: GPRS, SMS-сообщений и автодозвоном по двум SIM-картам разных операторов
- дистанционные с АРМ ПЦН и с телефонов собственника, защищенные паролем, настройка и управление ППКОП и оборудованием на объектах
- процедура постановки под охрану и снятия с охраны с применением электронных идентификаторов и клавиатуры
- радиус действия определяется зоной покрытия сотовой связи
- оповещение о состоянии ТСО и о событиях, происходящих на объекте, независимо от типов применяемых ППКОП и каналов передачи данных, по которым они работают

Приток-МКР

Подсистема микрорадиоохраны

Подсистема Приток-МКР (Приток-МКР) предназначена для беспроводного наращивания (удлинение связи) подсистем Интегрированной системы охранно-пожарной сигнализации Приток-А, а также для создания автономной (или работающей в составе ИС Приток-А) подсистемы микрорадиоохраны, работающей в безлицензионном диапазоне частот.

Технические характеристики Приток-МКР

Расстояние между узлами связи в сети до 1000 м

Количество каналов в пределах диапазона 433,075 – 434,750 МГц до 100

Количество каналов в пределах диапазона 868,0 – 868,2 МГц до 10

Количество узлов связи в радиосети — 30

Количество модулей РПДУ-03 — в пределах одного узла связи 30

Максимальное количество ППКОП, подключаемых к РПДУ-03 до 30

Количество ретрансляторов в сети — 65535 (любой узел связи — ретранслятор)

Шифрование в канале AES128

Принцип действия микрорадиоохраны Приток-МКР основан на создании радиосети с динамической маршрутизацией, в которой каждый узел связи является передатчиком, ретранслятором и прибором приемно-контрольным.

Состав Приток-МКР

Стандартное программное обеспечение (ПО) ИС Приток-А, работающее на пульте централизованного наблюдения.

Модуль РПДУ-03, который является основным элементом Приток-МКР.

Модуль РПДУ-03 выпускается в двух модификациях:

- РПДУ-03 (исп. 01), для работы в диапазоне 433,075–434,750 МГц;
- РПДУ-03 (исп. 02), для работы в диапазоне 868,0 – 868,2 МГц.

Так как он создан на основе трансиверов (приемопередатчиков) мощностью не более 10 мВт, то его применение в вышеуказанных диапазонах частот не требует лицензионного разрешения, то есть оно бесплатное. В дальнейшем будем называть РПДУ-03 **«узлом связи»** радиосети Приток-МКР.

При интеграции Приток-МКР в существующую ИС Приток-А можно использовать различные варианты и способы подключения РПДУ-03 к элементам системы.

Модуль РПДУ-03, который подключается к одному из этих элементов, будем называть **«базовым узлом связи»**, а остальные будут выполнять роль и ретрансляторов, и ППКОП.

Элементом ИС Приток-А, к которому по специальному каналу подключается один из **базовых узлов связи** радиосети Приток-МКР, может быть:

- коммуникатор ППКОП-05, подключенный к ретранслятору Приток-А;
- радиоконцентратор ППКОП-064-1;
- коммуникаторы Приток-TCP/IP;
- коммуникатор резервного канала связи Приток-РКС (GSM-TCP/IP).

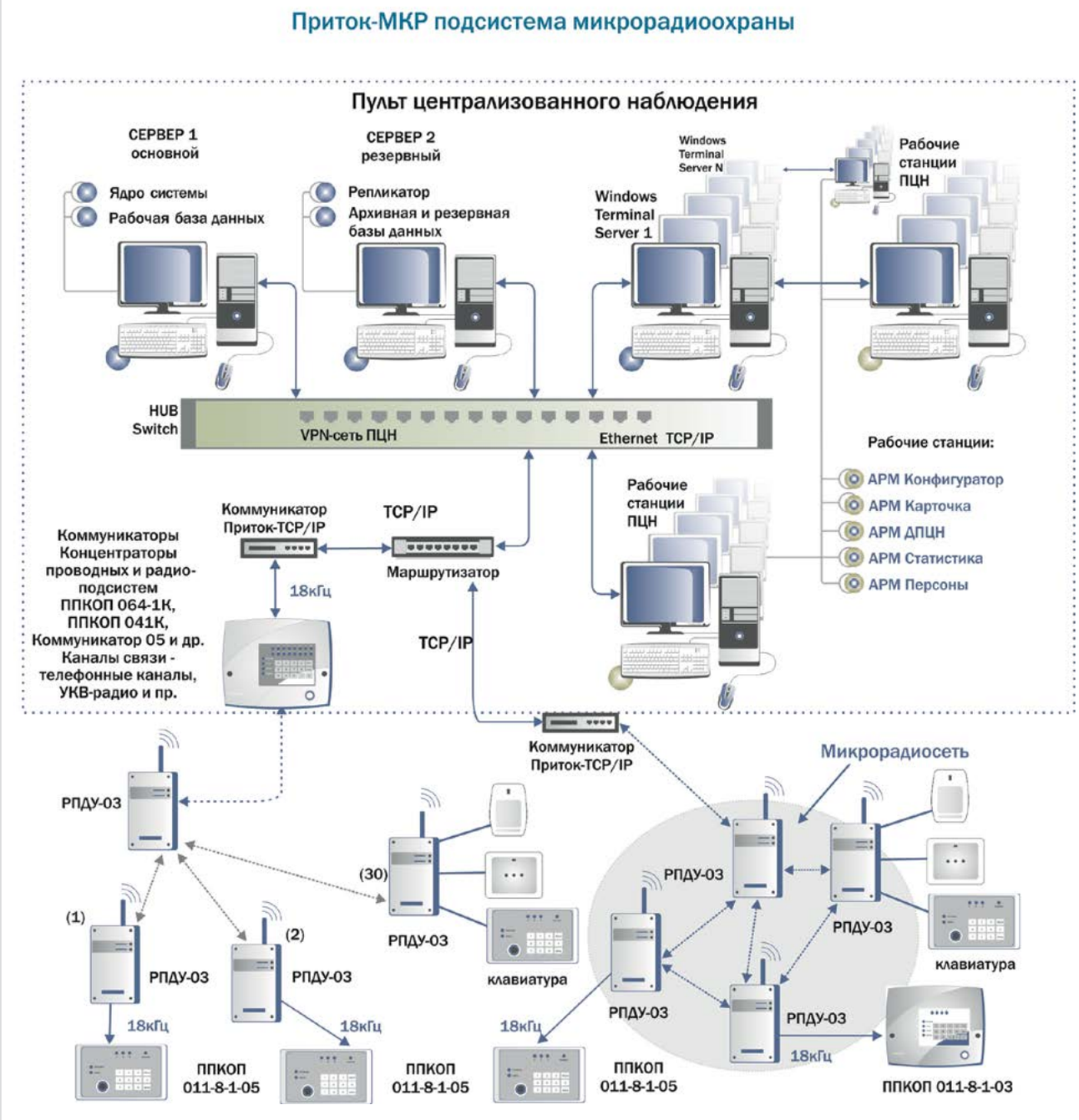
Это означает, что связь РПДУ-03 с сетью ПЦН может осуществляться:

- по физическим двухпроводным или выделенным телефонным линиям;
- по УКВ-радиоканалу (136-174 и 430-470 МГц);
- по высокоскоростным цифровым каналам связи сети стандарта Ethernet, в том числе и по оптоволоконным линиям через медиаконвертеры, с применением протокола TCP/IP и UDP;
- по каналам сотовой связи стандарта GSM 900/1800, в режиме GPRS и 3G.

В качестве приборов приемно-контрольных охранно-пожарных в Приток-МКР могут применяться:

- сам модуль РПДУ-03 (4 охранных шлейфа и 2 ключа);
- все ППКОП серии Приток, подключаемые по 18 КГц;
- до 30 ППКОП-05 (-05К), подключаемые по специальной линии к модулю РПДУ-03.

Если РПДУ-03 используется в качестве ППКОП, то к нему подключаются датчики охранной, пожарной или тревожной сигнализации. Для управления процессом постановки/снятия с охраны подключается клавиатура. С каждым узлом связи обеспечивается контроль канала, а при подключении ППКОП серии Приток, в том числе, и канала типа «свой-чужой».



Таким образом, созданная микрорадиоохрана Приток-МКР позволяет организовать автоматизированную централизованную охрану и централизованный контроль любого множества объектов, оснащенных локальными подсистемами микрорадиоохраны Приток-МКР, в сочетании с возможностью и достоинствами подсистем ИС Приток-А, работающих по различным каналам передачи данных: высокоскоростным цифровым каналам с применением протокола TCP/IP, УКВ-радиоканалу (136-174 и 430-470 МГц), каналам сотовой связи стандарта GSM и линиям связи телефонной сети. Применяя концентраторы и коммуникаторы с использованием микрорадиоканала, мы можем быстро организовать охрану и отдельно стоящих объектов и многоофисных помещений, где любые монтажные работы по прокладке кабеля либо затруднены, либо невозможны. Основной элемент Приток-МКР РПДУ-03 имеет доступную стоимость, которая сопоставима с прокладкой кабеля.

Приток-МПО

Подсистема мониторинга и охраны подвижных объектов

Приток-МПО ГЛОНАСС/GPS предназначен 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.

Одним из основных условий функционирования системы Приток-МПО является наличие установленной в АРМ ПЦН электронной карты местности. Для выполнения работ по подготовке электронных карт ОБ «СОКРАТ» имеет лицензию на **Картографическую деятельность № ВСТ-00600К.**

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 (БМ)** — устройство, которое обеспечивает прием информации с БК и передачу этих данных в диспетчерский центр (ДЦ) Приток-МПО.

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

Приток-МПО поддерживает работу с различными типами **трекеров**. Например, с трекерами GlobalSat.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ БК

ВАРИАНТ ИСПОЛНЕНИЯ БК	СИСТЕМА НАВИГАЦИИ		КАНАЛ СВЯЗИ С ДЦ		ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ О БК
	GPS	ГЛОНАСС	GSM	УКВ	
ПРИТОК-БК-031	+	+	+	+	функции охраны, управления, резервный аккумулятор
ПРИТОК-БК-032	+	+	+	+	функции формализованных сообщений, охраны,управления
ПРИТОК-БК-04	+		+		8 аналоговых входов, вход ТМ, 6 управляемых выходов
ПРИТОК-БК-05	+	+	+		8 аналоговых входов, вход ТМ, 6 управляемых выходов
ПРИТОК-БК-06	+		+		5 аналоговых входов, вход ТМ, 2 управляемых силовых выхода
ПРИТОК-БК-011(-021) сняты с производства	+	+		+	Встроенная УКВ (VHF\UHF) радиостанция, кнопка ТС

Основные функции БК-03

• 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 (136-174 или 430-470 МГц). Скорость передачи данных по УКВ-радиоканалу — не менее 2400 бод

• 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

• дистанционная замена программного обеспечения БК с АРМ ПЦН

• дистанционная настройка режимов работы БК с АРМ ПЦН и (или) с сотового телефона пользователя

• определение координат с точностью до 10 м и скорости движения ТС с точностью до 2 км/час

• постановка под охрану, снятие с охраны с применением электронных идентификаторов (ЭИ) Touch Memory и (или) по команде от пользователя, подаваемой с помощью SMS-сообщений

• контроль напряжения бортовой сети ТС, состояния охранных датчиков и передача сообщений пользователям, в том числе 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 136-174 (VHF) и 430-470 МГц (UHF), 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.

Для организации подсистемы Приток-МПО на ПЦН необходимы:

ПО АРМ Приток-МПО, 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, отображение на карте местности, прием 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:

прием 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.

Бортовые комплекты и трекеры необходимой конфигурации.

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;
- расчет пробега и формирование различных аналитических отчетов с последующим выводом на печать;
- охрану трекера — обработку сообщения после нажатия на тревожную кнопку SOS
- привязку трекера к определенным зонам контроля, маршрутам движения
- контроль превышения скорости движения, отклонения от заданного маршрута движения, выход из зоны контроля.

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

TR-203

TR-206

Рабочие станции (АРМ ПЦН) 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.

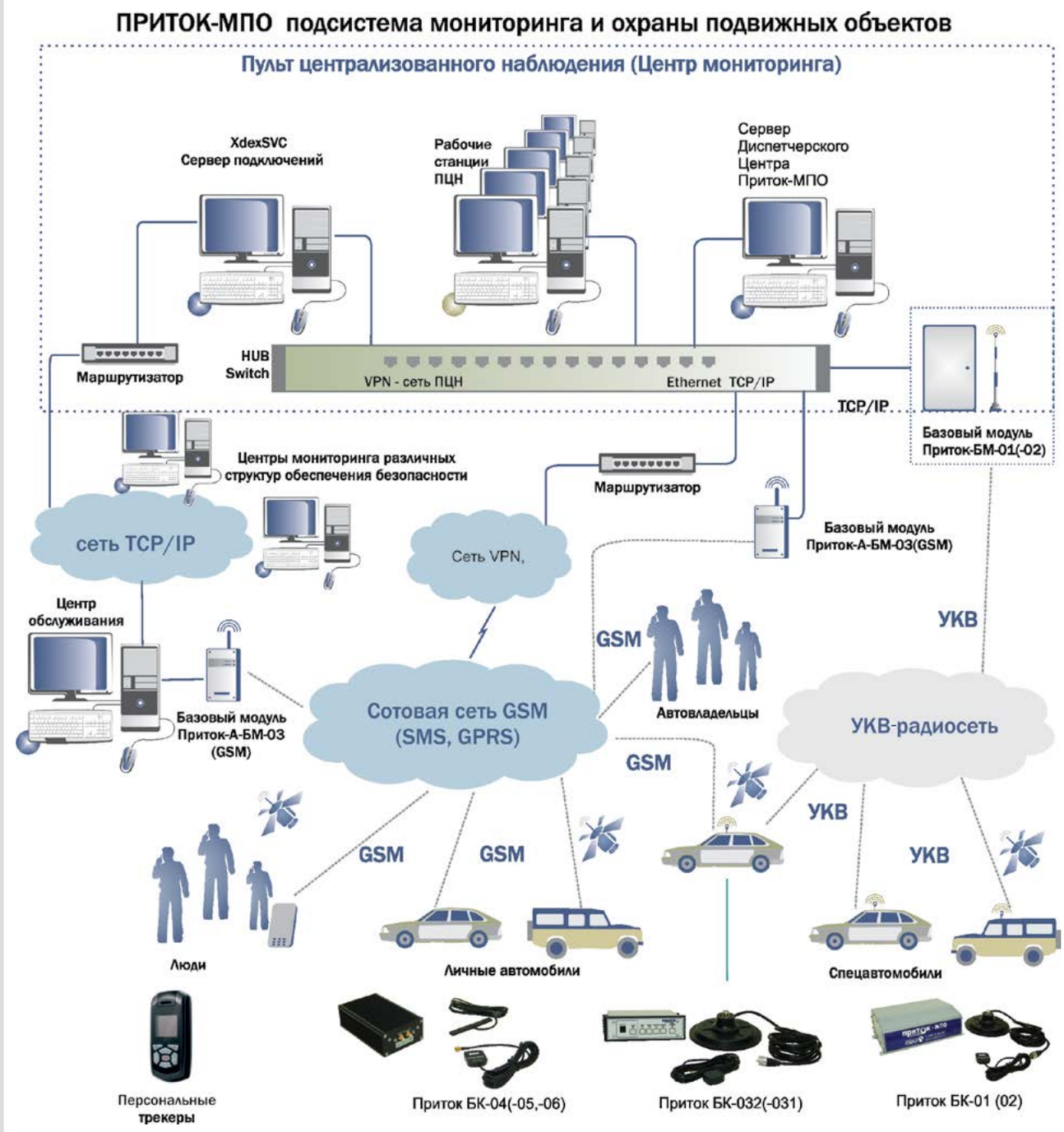
ПО позволяет проконтролировать местоположение, скорость и направление движения ТС, состояние БК (охраняется, не охраняется, тревога и т.д.), работоспособность БК по результатам диагностики, результаты ответов на поданные запросы и результаты выполнения поданных на БК команд управления.

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

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

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

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.

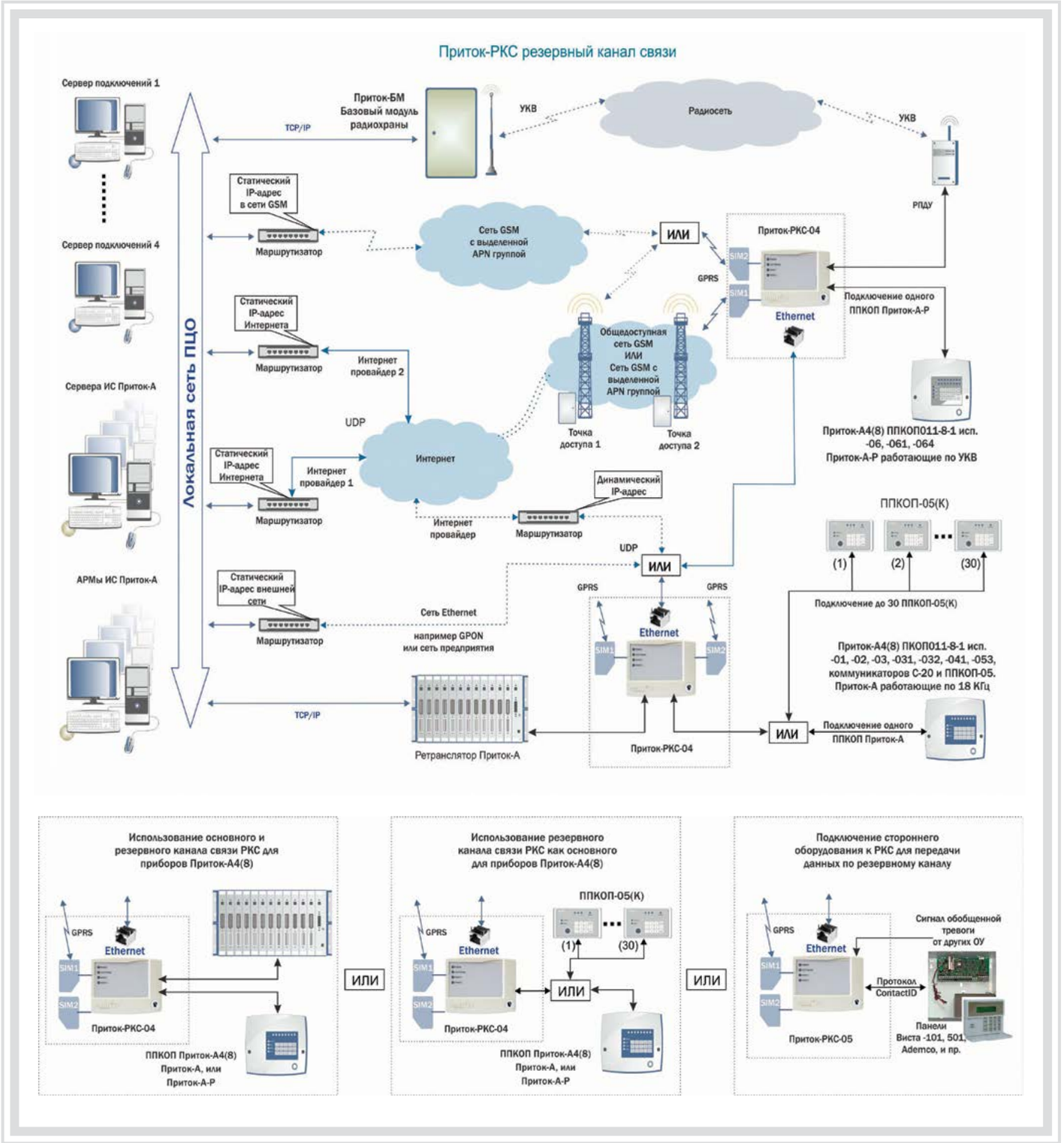


Приток-МПО имеет сертификат соответствия МВД № МВД.RU.0001.Н00563.
Работа Приток-МПО в составе ИС Приток-А позволяет организовывать несколько центров мониторинга, в том числе и работающих через Web-узлы. АРМы ПЦН, входящие в состав одной системы, позволяют объединить работу различных подразделений МВД и МЧС, а также частных охранных предприятий.

Приток-РКС

Коммуникатор резервного канала связи

Резервный канал связи Приток-РКС — это устройство, позволяющее организовать связь с охраняемым объектом при невозможности использования основного канала передачи данных.



Приток-РКС представляет собой отдельный модуль с установленными внутри разъемом Ethernet и (или) двумя SIM-картами для подключения к сети, который подключается к обычному ППКОП, работающему по телефонным каналам связи или по УКВ-радиоканалу.

При неисправности основного канала связи система автоматически или вручную переходит на работу по каналам сотовой связи. Аналогично система автоматически или вручную производит возвращение с резервного канала на основной, если он восстанавливается.

Резервный канал связи использует постоянное соединение GPRS в сети GSM или через сеть Ethernet.

При переходе на резервный канал возникают дополнительные затраты. Эти затраты зависят от стоимости услуг связи выбранного оператора. Для конкретного абонента (охранного прибора) эта услуга оценивается примерно 100 рублей в месяц.

Косвенная затрата — это та часть, которую несет охранная структура за наличие выделенного интернет-соединения до ПЦН.

От ПЦН до оборудования оператора сотовой связи может быть использован туннель VPN или отдельная группа доступа в сети GSM. На сервере ПО ИС Приток-А должен быть проброшен внешний статический IP-адрес (или несколько), с которым и соединяется модуль резервного канала связи.

Наличие двух запасных каналов передачи сообщений по резервному каналу связи на ПЦН (две SIM-карты в модуле и сеть Ethernet) исключает возможность их одновременного выхода из строя либо преднамеренного обрыва.

Получается, вывести такую систему из строя практически невозможно.

Приток-РКС предназначен для создания резервного канала передачи данных подсистем Интегрированной системы охранно-пожарной сигнализации Приток-А, работающих по каналам связи телефонной сети и по радиоканалу сети УКВ **(рис. 1)**.

Так как Приток-РКС создан для обеспечения надежной работы уже существующих подсистем, то модули Приток-РКС обеспечивают эмуляцию протоколов работы оборудования Приток-А, работающего по другим каналам передачи данных. То есть Приток-РКС заменяет эти каналы временно или постоянно.

Коммуникатор РКС для проводных приборов автоматически отслеживает работоспособность основного и резервного каналов связи. Он подключается в разрыв линии связи между ППКОП и ретранслятором или коммуникатором TCP/IP. В случае потери связи по основному каналу (обрыв, короткое замыкание, неисправность) коммуникатор РКС автоматически переключается на Ethernet или GSM-канал. При восстановлении линии связи коммуникатор РКС возвращает управление ретранслятору и переключается в режим слежения за работоспособностью основного канала.

Коммуникатор РКС обслуживает следующие проводные приборы: ППКОП 011-8-1-01, ППКОП 011-8-1-02, ППКОП 011-8-1-03, ППКОП 011-8-1-031, ППКОП 011-8-1-032, ППКОП 011-8-1-041, ППКОП 011-8-1-053, коммуникатор С-20, коммуникатор ППКОП 05, а также работает в качестве коммуникатора для ППКОП 011-8-1-05(к) и РПДУ-03.

Коммуникатор РКС работает со следующими типами ретрансляторов: Приток-А-Ю, Приток-А, Приток-А-Ф, Приток-АФ-01.3.

Коммуникатор РКС для радиоприборов работает со следующими приборами: ППКОП-011-8-1-64, ППКОП-011-8-1-061, ППКОП-011-8-1-06 (в дальнейшем по тексту — радиоприборы).

Коммуникатор включается в разрыв линии связи между радиоприбором и РПДУ. В случае потери связи по основному каналу (неисправность РПДУ, радиопомеха, неисправность радио базы) коммуникатор автоматически организует канал связи по одному из доступных ему IP-совместимых каналов.

Коммуникатор предназначен для работы по радиоканалу как основному каналу связи. Резервными каналами связи (IP-совместимыми) могут быть Ethernet соединение или 2(1) GSM/GPRS-соединение. Коммуникатор поддерживает любую комбинацию резервных каналов (например, только 1 GSM/GPRS, или Ethernet и 1 GSM/GPRS и так далее).

Коммуникаторы РКС передают все виды извещений и команд, которые поступают на прибор или приходят с ППКОП.

Примечание: Возможна эксплуатация коммуникаторов РКС в режиме только резервного канала без использования основного канала связи.

Приток-РКС обеспечивает расширение возможностей ИС Приток-А по созданию каналов передачи данных. Он позволяет реализовывать различные варианты как ручного, так и автоматического подключения и переключения технических средств охраны, работающих в составе ИС Приток-А, используя современные каналы связи.

Приток-РКС

Приток-РКС-04 (GSM+TCP/IP) — предназначен для организации основного и резервного каналов связи радиоприборов и проводных приборов серии Приток-А при централизованной охране объектов и квартир в составе «Автоматизированной системы охранно-пожарной сигнализации Приток-А».

Каналы связи между прибором и АРМ ДПЦО логически разделены на основной и резервный. В рабочем режиме коммуникатор обеспечивает связь прибора с АРМ ДПЦО по основному каналу и в случае выхода его из строя переключается на резервный.

Основные каналы связи:

· линия связи (телефонная) - для проводных приборов;

· радиоканал - для радиоприборов.

Резервный канал связи:

· Интернет (Ethernet или GSM в режиме GPRS).

Каналы связи с ПЦН : GSM (2 SIM-карты, 2 оператора сотовой связи, 4 IP адреса ПЦН) + Ethernet (4 IP-адреса ПЦН).

Дальнейшее развитие технологий резервного канала связи

На сегодняшний день наиболее предпочтительным считается вариант использования резервного канала связи конфигурации Ethernet и GSM. Обе эти технологии доступны для большинства людей, дешевы и в то же время надежны. Именно такое сочетание каналов передачи данных будет востребовано в настоящее время.

Как максимум клиенту нужно поставить все каналы связи. Это особенно важно для крупных предприятий, организаций, банков.

Приток-РКС-05 является дальнейшим развитием системы Приток-А.

В связи с развитием сети Интернет и беспроводного доступа к нему становится актуальным перевод ранее используемых аналоговых каналов передачи информации в цифровые. Так, в прошлом для целей мониторинга объектов широко применялись различные приборы (например «Виста-101») с использованием дозвона и передачи информации по линиям АТС на пульт ПЦН в формате Ademco Contact ID. Массовое применение технологии GPON в некоторых случаях не дает возможности использовать устаревшее аналоговое оборудование. РКС-05 позволяет «поднять в Интернет» ранее установленные Contact ID совместимые приборы и в качестве канала связи вместо АТС использовать Ethernet и GSM.

РКС-05 подключается к приборам Contact ID по двухпроводной линии связи вместо телефонной линии, имитируя для прибора АТС, и осуществляет преобразование протокола Contact ID в протокол Приток-А. Когда прибор Contact ID передает сообщение, то РКС-05 принимает, подтверждает и передает на ПЦН уже по своим цифровым каналам - Интернет (Ethernet или GSM в режиме GPRS).

Каналы связи с ПЦН : GSM (2 SIM-карты, 2 оператора сотовой связи, 4 IP-адреса ПЦН) + Ethernet (4 IP-адреса ПЦН). Допускается работа на двух SIM-картах, без использования Ethernet.

РКС-05 следит за состоянием основного канала связи с ПЦН. В случае аварии основного канала связи, организует работу с прибором по одному из резервных каналов связи. После восстановления основного канала связи РКС-05 переключается на него.

На ПЦН данные от РКС-05 принимает «Сервер Подключений» и передает в систему Приток-А как событие, принятое от Contact ID совместимого прибора.

Дополнительная степень надежности дости-гается при использовании Ethernet-интерфейса и двух SIM-карт. В случае временной не доступности Ethernet канала РКС-05 работает по GSM-каналу и периодически проверяет Ethernet-канал, и, в случае его восстановления, управление возвращается Ethernet каналу.

В РКС-05 реализованы стандартные для системы Приток функции, такие как: удаленное (по каналам Интернет) конфигурирование и обновление версии прошивки с помощью АРМ ПЦН.

РКС-05 имеет обобщенный вход тревог. При возникновении “Тревоги” в Contact-ID-совместимом приборе, он формирует сигнал “Тревога” на контактах “выход” ПЦН. По этому сигналу РКС-05 принимает и формирует событие “Тревога” по номеру зоны, указанному в параметре “номер зоны” своей конфигурации, и это событие «мгновенно» попадает на ПЦН. Уже после этого Contact-ID-совместимый прибор начинает дозвон и передачу события, что может занять некоторое время. Таким образом пульт сначала получает сигнал «обобщенной» тревоги , а затем извещение более подробной информацией о причинах тревоги.

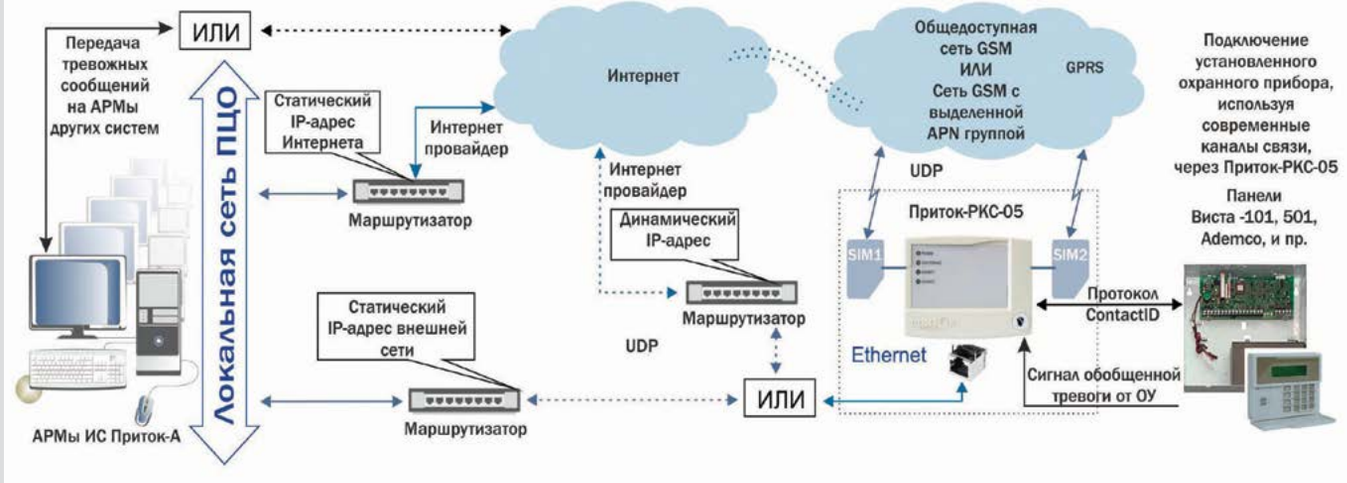
Питание РКС-05 осуществляется от внешнего резервированного источника питания (РИП) 12 В ±2 В.

Приток-РКС

Приток-РКС-05 (TCP\IP+GSM) предназначен для организа ции канала связи устройств, работающих по протоколу **Ademco Contact ID** (далее — приборы Contact ID) с пультом централизованной охраны объектов и квартир в составе «Автоматизированной системы охранно-пожарной сигнализации Приток-А» по каналам Ethernet и GSM.

РКС-05 подключается к приборам Contact ID по двухпроводной линии связи вместо телефонной линии, имитируя для прибора АТС, и осуществляет преобразование протокола Contact ID в протокол Приток-А. Когда прибор Contact ID передает сообщение, то РКС-05 принимает, подтверждает и передает на ПЦН уже по своим цифровым каналам, используя при этом основной (Ethernet) или резервный (GSM) канал, используя либо SIM1 либо SIM2 согласно приоритетам у к а з а н н ы м в н а стройках РКС-05. Использование АТС и телефонной линии при этом исключается.

Рис. 2 Модернизированная схема подключения через современные каналы связи с использованием Приток-РКС-05



Приток-РЛС

Подсистема охраны территорий и периметра с применением радаров

При охране стратегических и особо важных объектов требуется контролировать не только непосредственно объект, но и прилегающие к нему территории, в том числе и в условиях ограниченной видимости (ночь, туман, осадки и т.д.). Для этих целей в состав ИС Приток-А введен новый программно-аппаратный комплекс с применением радаров и работающий в тесной интеграции с подсистемами видеонаблюдения Приток-Видео, мониторинга подвижных объектов Приток-МПО и контроля и управления доступом Приток-СКД.

Начиная с 2012 года данный комплекс прошел опытную эксплуатацию на Иркутской ГЭС и в результате положительной оценки планируется к внедрению на Братской и Усть-Илимской ГЭС.

Комплекс назвали Приток-РЛС

Подсистема Приток-РЛС предназначена для круглосуточной всепогодной охраны внешних и прилегающих территорий, отдельных зон и периметра. Принцип действия основан на радиолокационном наблюдении и обнаружении стационарных и движущихся целей (нарушителей) на дальности до одного километра в условиях ограниченной видимости (ночь, туман, осадки и т.д.).

Обнаружение, измерение координат, скорости, а также распознавание класса обнаруженных целей (человек, группа людей, автомобиль и т.д.) производится при помощи радиолокаторов. Дальнейшее автосопровождение и передача информации на АРМ дежурного пульта (оператора) о проникновении цели на объект как с внешней стороны периметра, так и о появлении транспортных средств или посетителей в контролируемой зоне, производится через дополнительно введенное в состав ИС Приток-А изделие — **Сервер-РЛС**.

В этом случае на АРМ дежурного пульта (оператора) информация выдается в виде плана объекта с нанесенными на нее координатной сеткой, стационарными объектами и условными обозначениями обнаруженных целей.

Доработанный, эргономичный, настраиваемый пользовательский интерфейс АРМ, а также возможность формирования и выдачи различных отчетов на основании статистической обработки оперативных и архивных данных обеспечивают пользователей системы, в первую очередь, дежурных пульта полной информацией для принятия решений при оперативной работе.

Сервер-РЛС — Orwell-R Server

Сервер-РЛС — Orwell-R Server — это обычный персональный компьютер под управлением операционной системы Microsoft Windows с установленным специальным ПО, обеспечивающим работу радара РЛС Orwell-R.

Сервер-РЛС подключается в сеть ИС Приток-А по протоколу TCP/IP и обеспечивает:

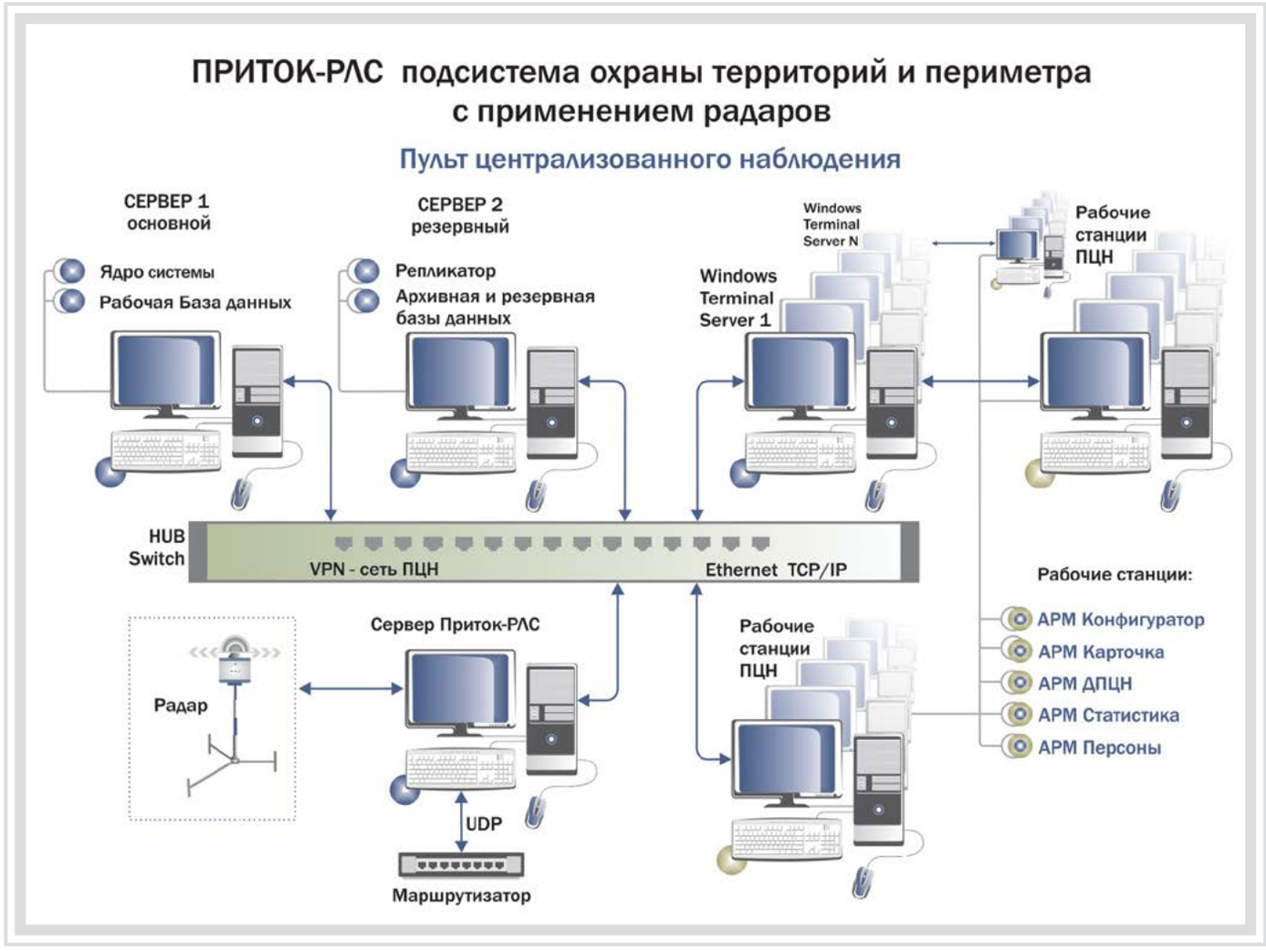
- подключение к нему одного радиолокатора (в дальнейшем Радара);
- управление узлами внешнего оборудования (элементами Радара);
- прием данных от подключенного к нему Радара;
- контроль работоспособности Радара и внутренний контроль Сервера-РЛС;

Состав подсистемы Приток-РЛС

Для работы Приток-РЛС необходимо иметь развернутый программно-аппаратный комплекс ИС Приток-А, в состав которого входят:

- серверы и рабочие станции ИС Приток-А
- программный модуль Приток-РЛС-Сервер, реализованный в виде службы ОС Windows, работающий в составе ИС Приток-А 3.7.
- сервер-РЛС — Orwell-R Server
- внешнее оборудование (радиолокаторы)
- клиентские компьютеры, тоесть АРМ (рабочие станции) из состава ИС Приток-А

Количество компонентов в составе подсистемы выбирается в зависимости от конфигурации и размеров охраняемого объекта. Полностью свои достоинства подсистема Приток-РЛС проявляет при совместной работе с уже существующими подсистемами Приток-Видео, Приток мПО и Приток-СКД.



• поддержку контроля ядром системы каналов связи с Сервером-РЛС;

• выдачу извещения на АРМ дежурного об обрывах / восстановлениях связи с Радаром и о его работоспособности;

• первичную обработку данных (определение участков тревожных зон, подозрительных с точки зрения обнаружения целей);

• анализ целевой обстановки: идентификацию целей внутри тревожной зоны, распознавание целей, измерение их координат и скорости движения, автосопровождение и прогнозирование траекторий движения целей;

• запись целевой обстановки (количество и характеристики целей) в собственный архив;

• автоматическую или по запросу передачу результатов обработки данных о целях на клиентские компьютеры (АРМы) в режиме реального времени.

Внешнее оборудование

В качестве внешнего оборудования применяется когерентный дальностно-доплеровский импульсный или ЛЧМ-радиолокатор Ku-диапазона Orwell 2k-Radar (в дальнейшем Радар). К каждому Серверу-РЛС подключается один Радар.

Радар состоит из антенны, опорно-поворотного устройства, радиочастотного трансивера и цифрового модуля обработки информации и управления.

Радар обеспечивает обнаружение и распознавание целей (человек, автомобиль) по их радиолокационному изображению. Способ обзора – механическое, программно-управляемое сканирование или вращение. Максимальная дальность обнаружения человека в импульсном режиме – 450 м, в режиме ЛЧМ – 1000 м. Максимальная дальность обнаружения автомобиля в импульсном режиме — 1000 м, в режиме ЛЧМ – 1500 м.

Азимутальный размер зоны обзора Радара может быть установлен любым в азимуте 180 градусов, а при вращательном режиме в азимуте 360 градусов.

Режимы излучения – когерентный импульсный или ЛЧМ

Уровень электромагнитного излучения Радара соответствует дей-

ствующим в РФ санитарным правилам и нормам для использования системы в населен ных пунктах.

Программное обеспечение подсистемы Приток-РЛС

Как такового отдельного программного обеспечения подсистемы Приток-РЛС, конечно же, не существует. Выше мы уже говорили о том, что подсистема Приток-РЛС все свои достоинства реализует при ее работе с развернутыми подсистемами охраны – Приток-Видео, Приток-СКД и Приток-МПО. В этом случае в программное обеспечение ИС Приток-А 3.7 добавился программный модуль Приток-РЛС-Сервер, реализованный в виде службы ОС Windows.

АРМ Конфигуратор, функционирующий в составе ИС Приток-А, при работе с вновь созданной подсистемой Приток-РЛС доработан и обеспечивает:

• управление правами пользователей на отдельные элементы ИС Приток-А, а

также на доступ к функциям ПО различных АРМов;

• настройку связей между объектами охраны, точками прохода/проезда, видеокамерами, зонами контроля локаторов, временными зонами и другими элементами различных подсистем.

Например, привязку контролируемых зон (подсистемы **Приток-РЛС**) к карточкам объектов охраны; закрепление за определенной зоной, контролируемой подсистемой **Приток-РЛС**, для наблюдения ее в ручном (по команде дежурного пульта) или в автоматическом (по целеуказанию Радара) режиме видеокамерами и тепловизорами подсистемы **Приток-Видео** и т.д.

АРМ Редактор планов пополнился дополнительными функциями и позволяет производить:

• привязку плана охраняемого объекта (объектов), созданного при помощи примитивов, к топографической карте (топографическим координатам) местности;

• привязку радиолокационной карты подсистемы Приток-РЛС к топографической карте местности подсистемы Приток-МПО;

• сохранение настроек показа для планов (привязанных к карте);

• создание дежурным пульта (администратором) тревожных зон, контролируемых подсистемой Приток-РЛС как на плане объекта, так и на электронной карте местности.

Ядро системы Приток-А 3.7, работающее теперь и с подсистемой Приток-РЛС, дополнилось функциями и позволяет производить:

• прием в режиме реального времени данных со всех работающих экземпляров Приток-РЛС-Сервер;

• анализ и обработку данных в режиме реального времени с учетом информации, поступающей от всех подсистем охраны, Приток-СКД, Приток-Видео, Приток-МПО и Приток-РЛС;

• анализ целевой обстановки, идентификацию целей внутри контролируемых зон, распознавание целей, измерение их координат и скорости движения, а также автосопровождение;

• анализ целевой обстановки внутри контролируемых зон с учетом временных ограничений (временных зон), генерирование и выдачу сигналов **тревога**;

• архивирование данных, поступающих от подсистемы **Приток-РЛС**;

• контроль состояния аппаратных средств и каналов передачи данных подсистемы Приток-РЛС как в ручном, так и в автоматическом режимах, с выдачей сообщений, общепринятых для ИС Приток-А, на монитор АРМ ДПЦО;

• передачу с АРМ ДПЦО команд управления на Приток-РЛС-Сервер и узлам внешнего оборудования.

АРМ ДПЦО становится, в том числе, и клиентским компьютером подсистемы Приток-РЛС и обеспечивает:

• прием оперативной информации о состоянии всех подсистем, в том числе и Приток-РЛС от ядра системы;

• выдачу дежурному пульта информации, представляющей собой карту зоны обзора (план объекта) с нанесенными на нее координатной сеткой, стационарными объектами и условными обозначениями обнаруженных целей;

• сопровождение каждой цели информационным блоком (координаты, класс, скорость и т.д.) в создаваемом специализированном ситуационном окне (окнах) для подсистемы Приток-РЛС;

• вывод в это окно (окна) интегрированной информации о состоянии контролируемых зон, объектов, о характеристиках обнаруженных целей (координаты и скорость цели, класс цели – люди, автомобили и т.д.), поступающей от различных подсистем (охраны, Приток-СКД, Приток-РЛС, Приток-Видео, Приток-МПО);

• одновременный просмотр данных на других мониторах, а также на мониторе с выведенной электронной картой местности (объекта) ;

• детальное наблюдение целей по целеуказанию радиолокационной системы (класс, координаты и скорость целей) при помощи управления вручную и/или автоматическими поворотными видеокамерами или тепловизорами, закрепленными за данной тревожной зоной. Вывод изображений может производиться в отдельное окно АРМ ДПЦН и/или на отдельный, специально предназначенный монитор;

• передачу от дежурного пульта команд управления в ядро системы и отображение процесса их выполнения;

• постановку под охрану и снятие с охраны объектов (тревожных зон) системы вручную или автоматически по заданному дежурным пульта (администратором) расписанию;

• выдачу звукового и визуального (текст) сигнала тревоги при проникновении целей (людей и/или автомобилей) в тревожную зону;

• управление (контроль) дежурным пульта только теми объектами системы, на которые ему даны соответствующие права;

• в любое время получение из архива информации за произвольный интервал времени и просмотр архивных данных о целевой обстановке.

В разных окнах, на разных мониторах могут быть реализованы различные режимы отображения.

Яркостный режим — радиолокационное изображение без использования алгоритмов обнаружения и распознавания.

Режим карты — только карта и неподвижные объекты.

Режим обнаружения и распознавания — указание классов движущихся целей на фоне постоянно обновляемой радиолокационной карты.

Работа Приток-РЛС с подсистемой Приток-Видео

При работе подсистемы Приток-РЛС совместно с подсистемой Приток-Видео обеспечивается детальное наблюдение целей по целеуказанию радиолокационной системы (класс, координаты и скорость движения целей) при помощи управления, вручную и/или автоматически, поворотными видеокамерами или тепловизорами, закрепленными за контролируемыми зонами, которые в свою очередь отображаются на электронной карте (плане) охраняемой территории.

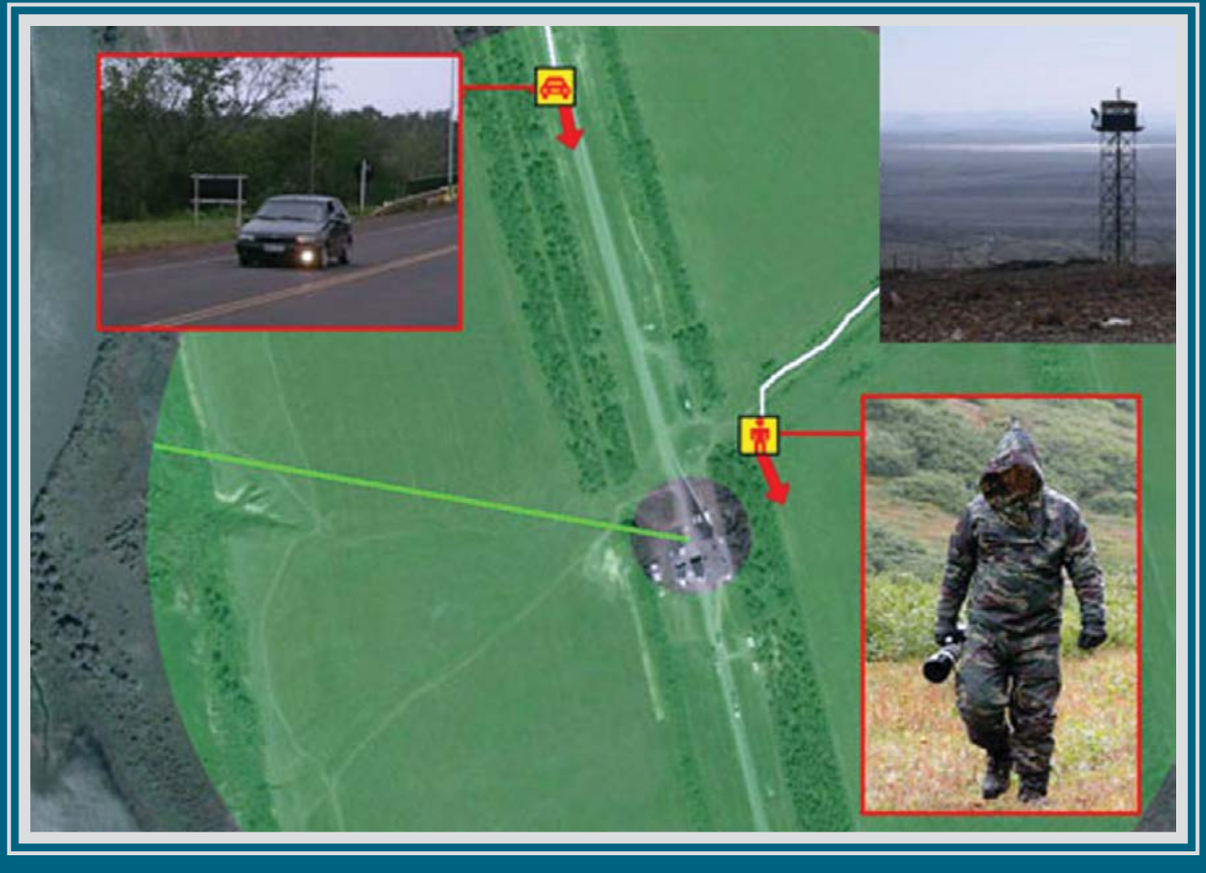
Произведена интеграция (подключение) радиолокационных станций **Orwell 2k-Radar** (Радаров) таким образом, что они выполняют функции обзорных сенсоров (целеуказателей) для поворотных видеокамер или тепловизоров подсистемы Приток-Видео, уже работающих в составе ИС Приток-А и (или) включаемых в момент создания подсистемы Приток-РЛС заново.

Подсистема Приток-Видео обеспечивает:

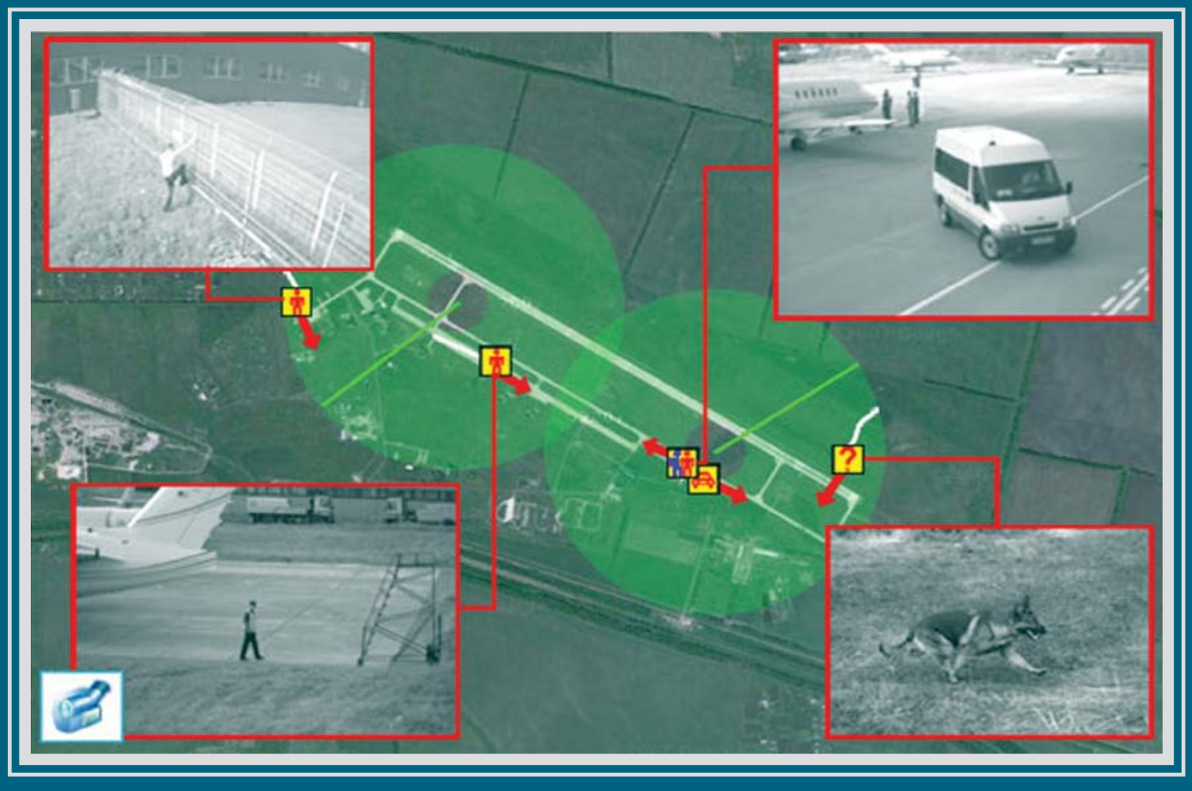
- отображение видеоизображений, поступающих с установленных видеокамер на мониторы, работающие в составе системы;
- прием и выполнение команд управления от ядра системы Приток-А и АРМ ДПЦО;
- ведение видеоархива;
- отображение в автоматическом или ручном режиме видеопотока с камер, которые связаны с зонами контроля подсистемы Приток-РЛС объектами охраны периметра или подсистемы Приток-СКД, с которых поступил сигнал «тревога»;
- управление клиентскими приложениями подсистемы Приток-Видео в автоматическом или ручном режиме;
- доступ к архивной информации с возможностью экспорта необходимых видеофрагментов.

И в заключение, все перечисленные выше возможности подсистемы Приток-РЛС в тесном взаимодействии с подсистемами Приток-МПО и Приток-СКД позволяют организовать комплексные системы безопасности для охраны и мониторинга, такие как (см. ниже):

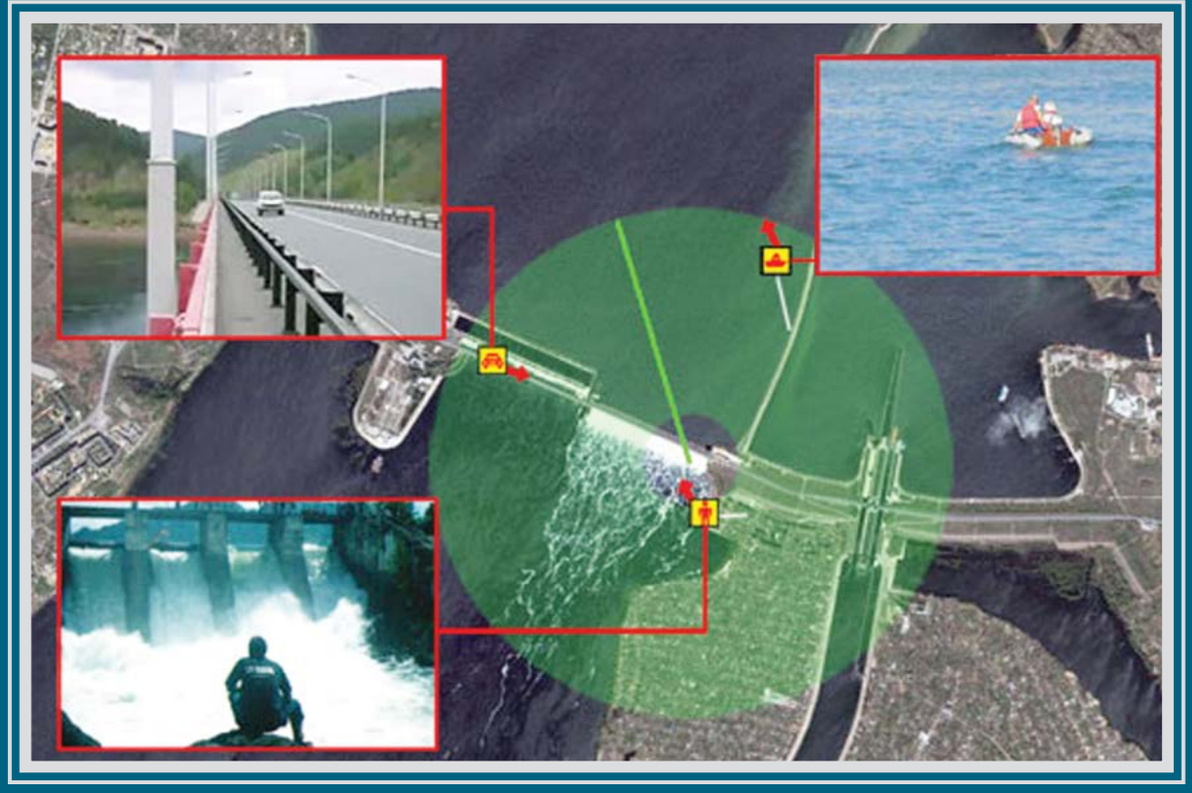
РАДИОЛОКАЦИОННАЯ СИСТЕМА ОХРАНЫ ПЕРИМЕТРА, А ТАКЖЕ ПРИЛЕГАЮЩИХ И ВНУТРЕННИХ ТЕРРИТОРИЙ ОБЪЕКТОВ



Охрана пограничных и контрольно-пропускных пунктов



Охрана взлетно-посадочных полос (ВПП) от проникновения животных, людей и автотранспорта



Охрана гидроэлектростанций и т.д.

Приток-А-Р
Подсистема радиоохраны

Подсистема Приток-А-Р предназначена для организации централизованной охраны стационарных объектов по УКВ-радиоканалу в диапазонах частот 136-174 и 430-470 МГц. Приток-А-Р может работать как в составе Интегрированной системы охранно-пожарной сигнализации Приток-А, так и автономно.

Состав подсистемы Приток-А-Р:

Базовые модули Приток-А-Р-БМ (далее БМ), Радиоретрансляторы Приток-А-РР (далее РР), в которые входят:

- радиостанция типа Motorola-GM-340
- контроллер **(контроллер БМ и РР)**
- резервированный источник питания

К БМ и РР через фидеры подключаются базовые антенны.

Приборы приемно-контрольные, охранно-пожарные:

ППКОП 011-8-1-06 выполнен в одном корпусе с РПДУ, производит контроль, обработку 1-го ШС — охранного или тревожного.

ППКОП 011-8-1-061К производит контроль, обработку и индикацию состояния, раздельное взятие/снятие 8-ми ШС.

ППКОП 011-8-1-064-1К с функцией концентратора для подключения до 29 шт. ППКОП-05К производит контроль, обработку и индикацию состояния восьми ШС. Взятие/снятие в ППКОП-064-1 общее.

Объектовые приемопередающие устройства (РПДУ), к которым через фидеры подключаются объектовые антенны. РПДУ может устанавливаться на расстоянии до 300 м, что позволяет выбрать правильное место для установки антенны.

Общие характеристики ПРИТОК-А-Р

ППКОП, применяемые в составе подсистемы Приток-А-Р, производят контроль состояния шлейфов сигнализации (ШС), обработку и индикацию состояний ШС, управление световыми и звуковыми оповещателями, формирование извещений о режимах работы ППКОП и передачу их на ПЦН, прием с ПЦН и выполнение команд управления.

Двусторонний, имитостойкий протокол обмена АРМ ПЦН — ППКОП обеспечивает постоянный контроль канала, в том числе и определение «свой-чужой».

ППКОП обеспечивают автоматизированную тактику постановки под охрану и снятие с охраны при помощи электронных идентификаторов Touch Memory (ЭИ) и (или) клавиатуры, собственником без участия дежурных ПЦН. Идентификация производится в АРМ ПЦН с выдачей квитанции на ППКОП о выполнении процедуры постановки или снятия. Постановка под охрану может производиться путем подачи команды с АРМ ПЦН.

Принцип действия Приток-А-Р основан на постоянном контроле с АРМ ПЦН, через БМ или через БМ и РР, состояния охраняемых объектов, оборудованных РПДУ с ППКОП-06, -061К, -064-1К; обработке в реальном времени извещений, поступающих от ППКОП; выдаче соответствующих сообщений на экран монитора и передаче с АРМ ПЦН команд управления на ППКОП.

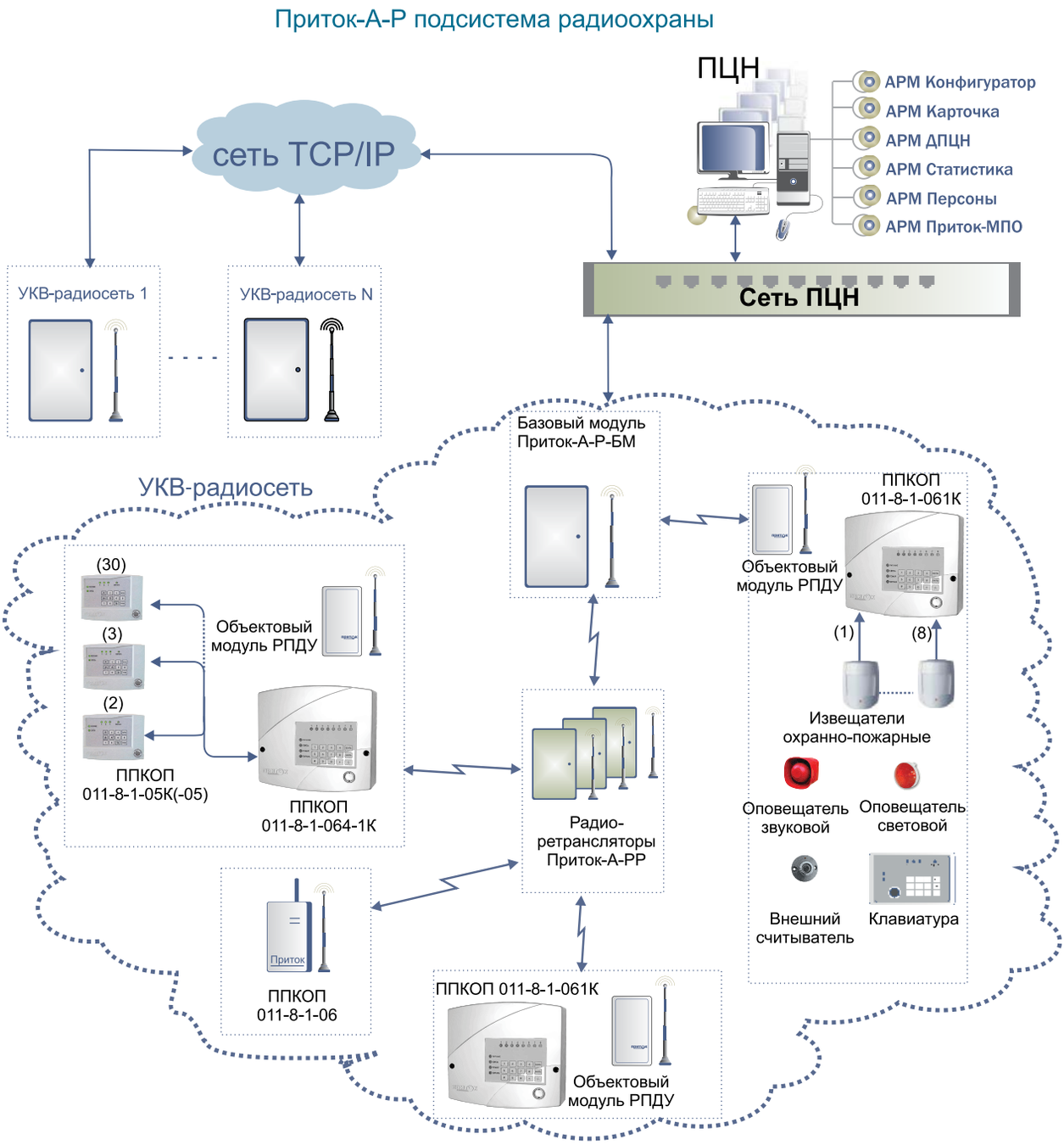
Двусторонняя связь с контролем канала АРМ ПЦН — ППКОП обеспечивается тем, что и в БМ и в РПДУ устанавливаются приемопередатчики. Алгоритм постоянного опроса состояния ППКОП и обмен данными с ППКОП напрямую или через ретранслятор обеспечивает контроллер БМ.

Обмен данными между БМ и АРМ ПЦН производится по любым, в том числе оптоволоконным, каналам передачи данных с применением протокола TCP/IP, поэтому расстояние от АРМ ПЦН до БМ не ограничено, определяется наличием канала передачи данных для протокола TCP/IP.

ПО АРМ ПЦН поддерживает неограниченное количество БМ. Поэтому в составе ИС Приток-А может одновременно работать на разных частотах неограниченное количество подсистем Приток-А-Р.

Возможности подсистемы Приток-РТП

- диапазоны рабочих частот — 136-174 и 430-470 МГц
- количество подсистем на разных частотах не ограничено
- двусторонний, имитостойкий протокол обмена АРМ ПЦН — объект с контролем канала «свой-чужой»
- автоматизированная тактика постановки/снятия с охраны с применением электронных идентификаторов и клавиатуры
- количество РПДУ, контролируемых БМ на одной частоте, — 250
- максимальное количество охраняемых объектов — 7500
- максимальное количество шлейфов сигнализации — 23750
- скорость передачи данных по радиоканалу — 1,2 Кбит/с
- класс излучения — 16KOFD
- несущие частоты — 1300 и 2100 Гц
- мощность радиостанций в БМ и в РР — до 45 Вт — до 5 Вт (программируется от 1 до 5 Вт)
- радиус действия без РР — до 20 км, с РР — до 50 км
- количество РР в подсистеме — 3
- количество РПДУ, закрепляемых за РР, произвольное в пределах 150

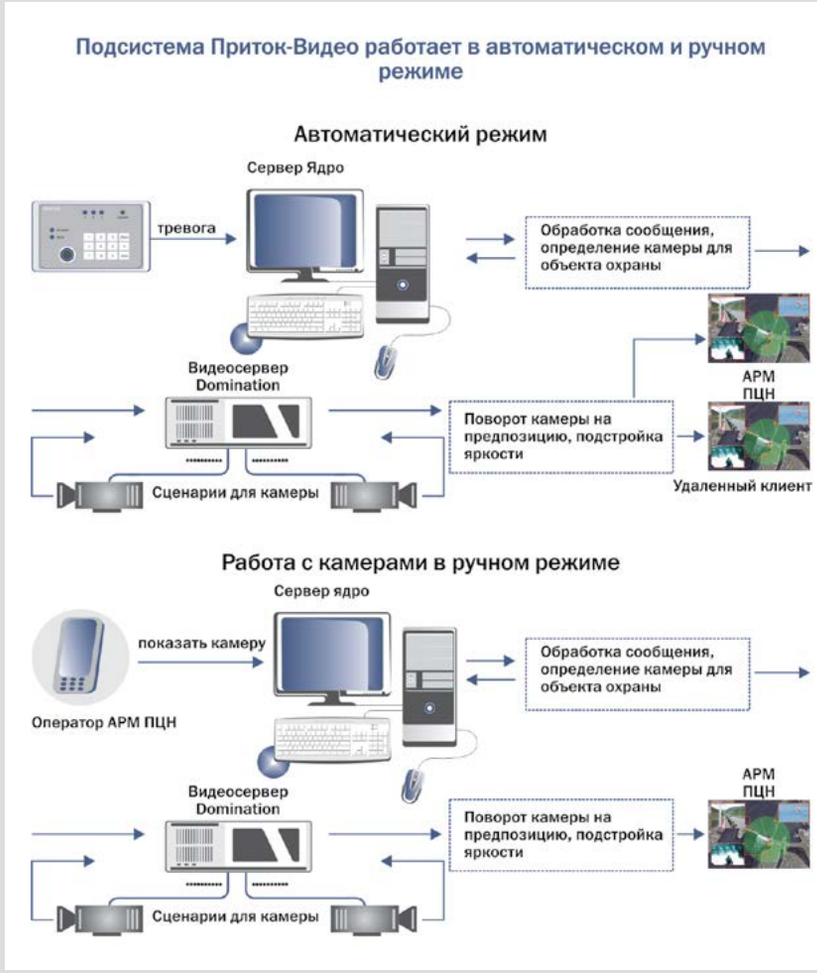


Все вышеперечисленные характеристики и особенности подсистемы Приток-А-Р позволяют с успехом применять ее как в составе ИС Приток-А, так и автономно, на уже существующих и на вновь создаваемых ПЦН.

Приток-Видео

Подсистема видеонаблюдения

Подсистема видеонаблюдения предназначена 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.



Состав подсистемы Приток-Видео

- видеосервер Domination (количество не ограничено)
- аналоговые видеокамеры (до 16 шт. к одному видеосерверу Domination)
- IP-видеокамеры (Axis и Mobotix и другие, количество не ограничено)
- рабочая станция с установленным ПО Приток-А 3.7

Принцип действия

- возможна привязка нескольких камер к одному объекту
- возможна привязка одной камеры к нескольким объектам
- возможно добавление нескольких событий для одного объекта
- отображение картинки с камер в АРМах в отдельном окне по заданному событию или по команде пользователя

Принцип действия

Оператором системы в АРМ «Конфигуратор» создается конфигурация различных видеокамер в БД. Производится привязка определенных камер к устройствам и событиям (см. Руководство пользователя АРМ «Конфигуратор»).

При выполнении в АРМах оператором команды «Показать камеру» будут отображены все камеры, привязанные к карточке. Изображение будет выведено локально в отдельном окне (на АРМ, с которого была подана команда), также получено в клиенте Domination, запущенном на другом компьютере в сети и настроенном для работы с АРМ ДПЦН. Изображение с IP-видеокамер Axis и Mobotix будет отображено только локально.

Функция «Показать камеру» может быть вызвана:

- из выпадающего меню на закладках «Диапазоны», «Тревоги», «Точки прохода»;
- из выпадающего меню в окне «Просмотр планов»;
- из окна «Работа с видео»;
- из выпадающего меню работы с оборудованием (приборы, комплекты и пр.).

При выполнении пункта главного меню «Аппаратура->Работа с видео» открывается окно со списком всех доступных видеокамер. Для того чтобы получить изображение с требуемой камеры, необходимо дважды щелкнуть левой кнопкой мыши на ней. Либо нажать на кнопку «Показать камеру».

Также камеры, подключенные к серверу Domination, могут управляться по событию. Список событий для видеокамер можно создать следующим образом:

- выполнить пункт главного меню «Справочники->Справочник «События Domination»;
- в появившемся окне для ввода событий создать событие с тем же именем, с которым оно было создано на видеосервере Domination (создание макросов на видеосервере подробно описано в его документации).

При использовании подсистемы Приток-Видео в АРМ ДПЦН без видеосервера Domination возможно автоматическое получение изображения с IP-камер по событию «Тревога». Данная настройка доступна для всей конфигурации – устанавливается при привязке камер к оборудованию. Получение изображения с камер по команде оператора регулируется доступом по правам конкретного пользователя системы ИС Приток-А.

Приток-СКД

Подсистема контроля и управления доступом

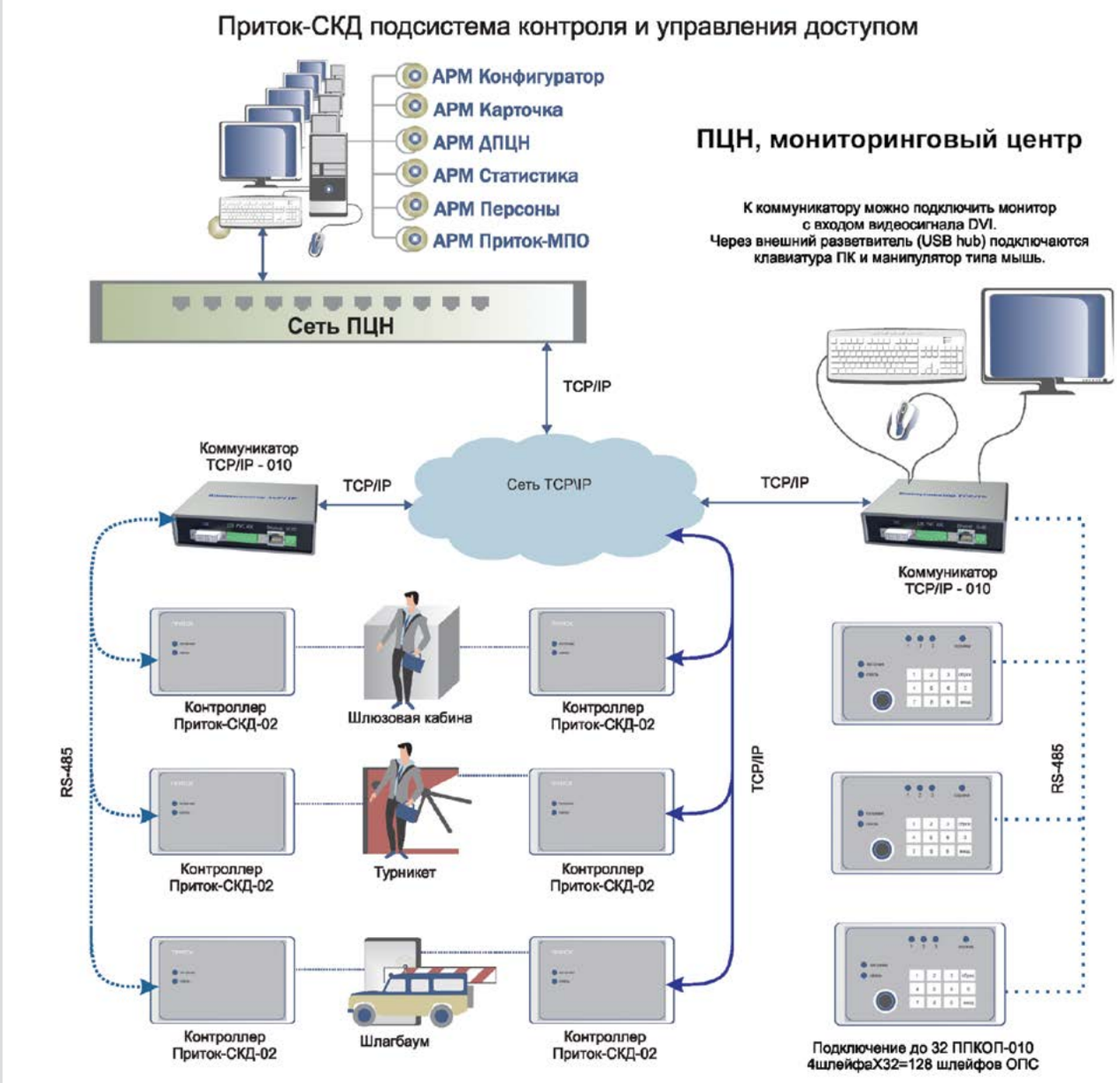
Подсистема Приток-СКД предназначена для организации автоматизированной централизованной охраны объектов (отдельных помещений, зданий, огражденных территорий и т.д.) и централизованного и (или) автономного контроля и управления доступом на объекты персонала и (или) транспорта, с применением интерфейса RS-485. Приток-СКД может работать как в составе Интегрированной системы охранно-пожарной сигнализации Приток-А, так и автономно.

Состав подсистемы ПРИТОК-СКД

- Программное обеспечение **(ПО)** ИС Приток-А, устанавливаемое в АРМ пульта централизованного наблюдения (ПЦН)
- Коммуникатор Приток-TCP/IP-010 (исп. 01 или 02), далее **Коммуникатор**
- Контроллер Приток-СКД, далее **КСКД**
- Приборы приемно-контрольные охранно-пожарные ППКОП 011-8-1 Приток-А-4(8), вариант исполнения -010, далее **ППКОП-010**
- Релейный расширитель, далее **РР**

Основные технические характеристики

- Расстояние от АРМ ПЦН до Коммуникаторов не ограничено, определяется наличием канала передачи данных для работы с использованием протокола TCP/IP
- Количество подключаемых Коммуникаторов не ограничено
- Протяженность линии связи между Коммуникаторами и ППКОП-010, КСКД и РР до 1000 метров
- Возможно подключение до 32 КСКД, РР или ППКОП-010 к каждому Коммуникатору
- В КСКД может храниться до 30000 записей, содержащих коды идентификаторов и индивидуальные или групповые расписания проходов
- Скорость реакции прохода, управляемого КСКД, от 100 мс до 1,5 сек
- ППКОП-010 имеет четыре шлейфа охранной, пожарной или тревожной сигнализации, тип шлейфа программируемый
- ППКОП-010 имеет выход четырех внешних силовых ключей
- ППКОП-010 и КСКД имеют выходы для подключения выносных считывающих устройств
- РР выпускаются в трех исполнениях, отличающихся количеством установленных реле управления: РР-01 — 16 реле, РР-02 — 8 реле и РР-03 — 4 реле
- Ток коммутации 1А, напряжение 30 В постоянного и 125 В переменного тока



Отличительные особенности Приток-СКД

- Связь АРМ ПЦН с точками прохода по любым, в том числе оптоволоконным, каналам передачи данных с применением протокола TCP/IP
- Постоянный контроль исправности программных и аппаратных средств и каналов передачи данных
- Управление проездом с одновременной идентификацией водителя и транспорта и отображением образов (фотографий, госномеров)
- Контроль и управление, автоматически или вручную в режиме реального времени, неограниченным количеством точек прохода из одного центра мониторинга с отображением образов (фотографий)
- Интеграция с видеонаблюдением, ручное управление поворотом видеокамер и автоматический поворот на предпозицию (автотур) по тревожному событию
- Формирование и выдача различных отчетов на основании оперативных и архивных данных

Функциональные особенности

Приток-СКД обеспечивает:

- создание и ведение базы данных персонала и транспорта
- привязку персонала и (или) транспорта к одному или нескольким идентификаторам
- привязку персонала и (или) транспорта к образу (фотография, госномер)
- привязку персонала к транспорту по одному или нескольким идентификаторам
- конфигурирование структуры программно-аппаратных средств под конкретный объект
- создание планов и мнемосхем объекта для наблюдения на экране монитора состояний охраняемых зон и точек прохода, определения текущего местоположения персонала и транспорта на территории объекта
- указание любого количества точек прохода, охраняемых зон для каждого идентификатора (для нескольких)
- настройку времени прохода в течение суток и в соответствии с календарем
- подготовку и изготовление пропусков (постоянных, временных, одноразовых)
- автоматизированный контроль сдачи пропусков с помощью картоприемников (сдал-проходи)
- удаленную запись с АРМ ПЦН расписаний проходов в КСКД
- автоматизированный контроль линий связи и состояния оборудования
- контроль и управление проходом персонала, транспорта или совместно персонала и транспорта:

— в автоматическом режиме, в соответствии с расписаниями, после определения одного или нескольких идентификаторов

— в автоматизированном режиме при отображении фотографий персонала и (или) госномера транспорта после определения одного или нескольких идентификаторов путем визуального сравнения и ручной подачи команды с АРМ ПЦН

— в ручном режиме по одноразовым пропускам, в экстренных случаях (разблокировать все точки прохода) и т. д.

- удаленное считывание информации с КСКД;
- формирование различных отчетов о перемещении персонала и транспорта на территории объекта на основании оперативных и архивных данных.

Принцип действия

Принцип действия централизованной охраны основан на постоянном контроле с АРМ ПЦН через Коммуникаторы состояния охраняемых объектов, оборудованных ППКОП-010; обработке в реальном масштабе времени извещений, поступающих от ППКОП-010; выдаче соответствующих сообщений на экран монитора и передаче с АРМ ПЦН команд управления на ППКОП-10.

Автоматизированная постановка и снятие объектов с охраны производится после прикладывания электронных идентификаторов к считывающему устройству или набора кода на клавиатуре ППКОП-010.

Принцип действия контроля и управления доступом основан на передаче команд блокировки (разблокировки) точек прохода или проезда (далее прохода) в автоматическом или ручном режимах. Ручное управление осуществляется непосредственно с АРМ ПЦН через Коммуникаторы, КСКД и РР. Автоматическое управление производится или с АРМ ПЦН через Коммуникаторы, КСКД и РР, или непосредственно с КСКД через РР, в соответствии с расписаниями, находящимися в АРМ ПЦН или КСКД соответственно.

При потере связи АРМ ПЦН с КСКД последний работает автономно по своему расписанию до восстановления связи. Для управления автоматическими дверьми, турникетами, шлагбаумами и прочими механическими устройствами блокировки (разблокировки), установленными в точках прохода, в качестве элементов управления подключаются ППКОП-010 или КСКД с РР.

Автоматическое, в соответствии с расписаниями, разрешение прохода персонала (транспорта) производится после прикладывания электронного идентификатора к считывающему устройству и (или) набора кода на клавиатуре ППКОП-010 или прикладывания идентификаторов к считывающим устройствам КСКД. Идентификация производится в АРМ ПЦН или КСКД соответственно.

Передача данных между АРМ ПЦН и КСКД (Коммуникаторами) ведется по высокоскоростным цифровым каналам сети стандарта Ethernet, с применением протокола TCP/IP, по физическому кабелю UTP Cat5, по оптоволоконным линиям связи через медиаконвертеры, по выделенным телефонным линиям через DSL-модемы на скорости от 128 Кбит/сек. до 100 Мб/сек. Либо КСКД подключается через интерфейс RS-485 к коммуникаторам Приток TCP/IP-010. Коммуникатор работает под управлением ОС Linux.

Передача данных между КСКД и ППКОП-010, КСКД и РР, КСКД и подчиненными КСКД ведется с применением интерфейса RS-485 по физическим двухпроводным линиям (витая пара) на скорости до 9600 бит/сек.

К коммуникатору можно подключить монитор с входом видеосигнала DVI. Через внешний разветвитель (USB hub) подключаются клавиатура ПК и манипулятор типа мышь.

Таким образом, технические характеристики и функциональные особенности Приток-СКД позволяют организовать автоматизированную централизованную охрану и централизованный контроль любого множества объектов, оснащенных автономными локальными системами контроля и управления доступом, в сочетании с возможностью управления точками прохода как из одного центра мониторинга, так и из множества ПЦН, объединенных в единую сеть.

Приток-РТП

Подсистема регистрации телефонных и радиопереговоров

Приток-РТП используется там, где необходимо обеспечить регистрацию и запись телефонных разговоров, переговоров по радиоканалу и запись микрофона зала. Приток-РТП используется и для автоматического оповещения.

Состав Приток-РТП

В комплект Приток-РТП входит:
- **компьютер под управлением ОС Windows;**
- **контроллер обработки аудиосигнала (КОАС);**
- **программное обеспечение Приток-РТП.**

Для установки КОАС в компьютер используются PCI-слоты. Один контроллер обеспечивает работу от 4 до 16 каналов. Максимальное количество каналов для одного компьютера - 48.

К одному каналу может быть подключено:
- **телефонная линия;**
- **радиостанция;**
- **микрофон;**
- **сотовый телефон через GSM-шлюз.**

Подключение телефонных линий производится параллельно телефонным аппаратам через устройство коммутационное Приток-РТП-8К. Подключение радиостанции производится через адаптер АД-РСТ-01 (-02, -03).

Область применения

- Регистрация телефонных и радиопереговоров персонала диспетчерских, аварийных и оперативных служб
- Запись важных деловых переговоров
- Сокращение каналов утечки коммерческой информации
- Повышение качества обслуживания, разрешение конфликтов с клиентами
- Оповещение личного состава
- Система оповещения для служб экстренного реагирования (МВД, МЧС и т.д.)
- Автоматическое оповещение в биллинговых системах

Возможности подсистемы Приток-РТП

- Автоматическая запись радио-телефонных переговоров на жесткий диск компьютера в реальном времени
- Настройка на определенную пользователем конфигурацию подключаемых каналов связи
- Индивидуальная настройка параметров каждого канала по уровню сжатия от 13,6 кБ/с до 128 кБ/с
- Автоматическая проверка свободного места на жестком диске, копирование аудиофайлов на диск постоянного архива, удаление старых и просроченных записей по мере заполнения диска или по параметрам, устанавливаемым пользователем
- Удаленный доступ к записанной аудиоинформации, поиск и воспроизведение записей по заданным параметрам с применением различных фильтров
- Передача аудиофайлов экстренного оповещения, биллинговой системы с использованием различных алгоритмов дозвона до клиентов
- Оперативное (немедленное) оповещение, запускаемое по команде оператора
- Автоматическое оповещение, запускаемое и останавливаемое в установленное время по расписанию без участия оператора, по заранее подготовленным спискам
- Протоколирование хода оповещения с выделением «Оповещенные/Не оповещенные» и формирование отчетов по категориям

Принцип действия

• Включение записи по радиоканалу осуществляется при появлении речевой информации в канале

• Задержка включения записи программируется (от 0 до 500 мсек.)

• Выключение записи по радиоканалу осуществляется при пропадании речевой информации в канале. Длительность паузы программируется (от 1 до 6 сек.)

• Все записи хранятся в виде файлов в подкаталогах с именем даты и времени создания файла. Имя файла содержит информацию о типе записи (радио, телефонная, входящий, исходящий, номера входящих и исходящих звонков), времени и длительности разговора, номере канала, что позволяет осуществлять быстрый поиск и обработку информации

Отличительные особенности Приток-РТП

• Простота настройки

• Работа изделия не влияет на качество радио- и телефонной связи

• Запись радиотелефонных переговоров на жесткий диск ведется автоматически без участия оператора

• Возможность применения различных типов компрессии аудиофайлов

• Автоматическое определение входящих и исходящих номеров

• Одновременная работа в режимах записи и воспроизведения

• Возможность быстрого поиска и обработки нужной информации

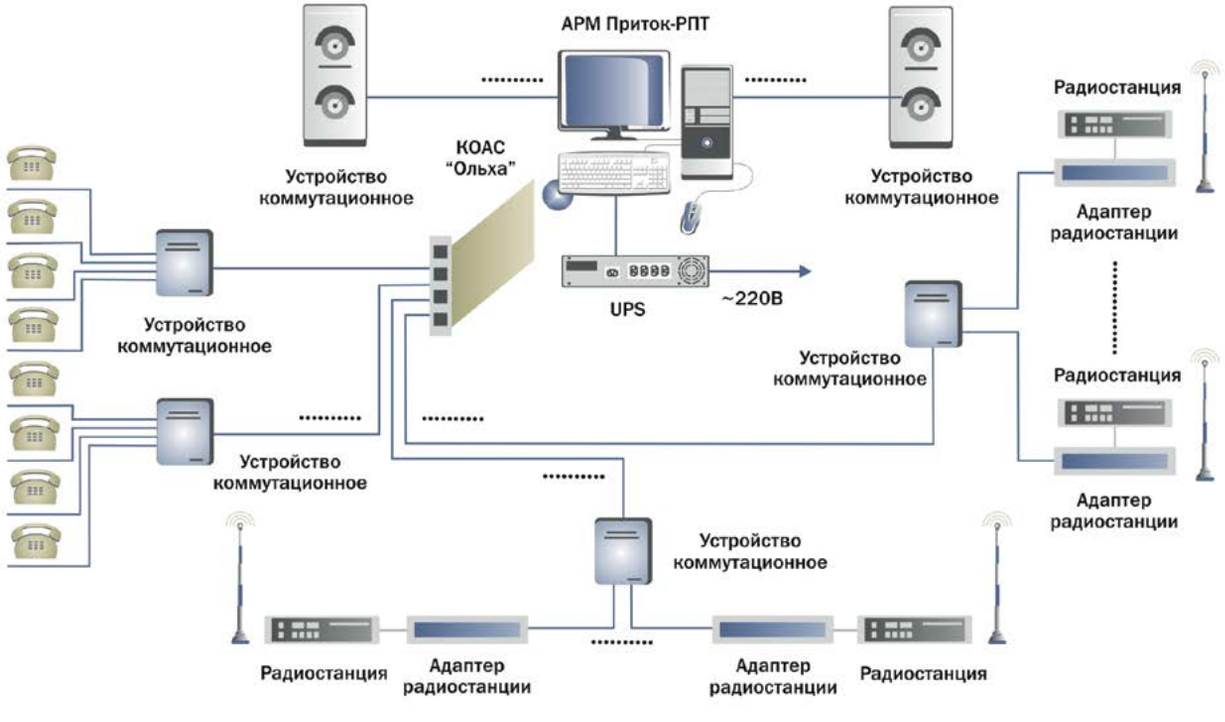
• Автоматическое оповещение по заранее подготовленным спискам абонентов

• Возможность подключения разных типов радиостанций – Motorola, Alinco, Kenwood, Маяк

• Оптимальное соотношение качества и цены

ПРИТОК-РТП подсистема регистрации телефонных и радиопереговоров

Оборудование рабочего места Приток-РТП



Учебно-методическая деятельность

«…Любая, даже самая совершенная, техника не может правильно функционировать в течение длительного времени без участия человека, выполняющего ее обслуживание и ремонт. И так как сегодня на вооружении наших подразделений, осуществляющих охрану объектов особой важности, повышенной опасности и жизнеобеспечения, находятся сложные программно-аппаратные средства, то к их эксплуатации и обслуживанию можно допускать людей, не просто имеющих соответствующее образование, но и обязательно прошедших специальное обучение»

«Государственная политика в области обеспечения безопасности»

Грамотная эксплуатация современных систем безопасности требует глубоких специальных знаний. Для этого охранным бюро «СОКРАТ» постоянно проводится работа по организации обучения специалистов, эксплуатирующих систему Приток. Более того, вопросам учебно-методической деятельности в Охранном бюро «СОКРАТ» уделяют особое внимание.

Подготовку проходят сотрудники подразделений вневедомственной охраны, частных охранных предприятий, курсанты вузов МВД и специалисты других организаций и предприятий, занимающихся эксплуатацией и внедрением системы Приток.

Обучение проводится на базе самого Охранного бюро «Сократ» в Иркутске, а также в других учебных центрах — в Воронежском институте МВД, в учебном центре НИЦ «Охрана» и в учебном центре ГУВД в Москве, а также в учебном центре филиала НИЦ ОХРАНА в Новосибирске.

В процессе подготовки специалистов применяются специальные учебно-методические стенды и материалы, разработанные и выпускаемые Охранным бюро «СОКРАТ».

Основная учебная база – Воронежский институт МВД, где обучение проходят курсанты института и переподготовку – специалисты из подразделений вневедомственной охраны. В институте на двух кафедрах — «Организация деятельности подразделений вневедомственной охраны» и «Технические средства безопасности и связи» — оборудованы классы по изучению ИС Приток-А. Квалифицированные преподаватели проводят занятия по вопросам устройства и эксплуатации ИС Приток-А.

Обучение навыкам работы с применением ИС Приток-А проходит также в Учебно-методическом экспертном центре (УМЭЦ) ФГУ НИЦ «Охрана» МВД РФ в городе Москва и в отделе подготовки кадров (ОПК) Новосибирского филиала ФГУ НИЦ «Охрана» МВД РФ. Кроме этого, созданы учебные классы, и обучение проводится на базе Учебного центра ГУВД Москвы и УВО Иркутска.

Также ежегодно непосредственно специалистами ОБ «СОКРАТ» организуются выездные семинары, на которых с сотрудниками подразделений вневедомственной охраны, УВО, ФГУП «Охрана» и сотрудниками региональных представительств Иркутской, Омской, Свердловской, Томской, Челябинской, Воронежской и Кемеровской областей, Красноярского, Краснодарского, Пермского краев, Республик Бурятия и Башкортостан проводятся занятия по вопросам эксплуатации и развития ИС Приток-А.

На сегодняшний день обучение в общей сложности прошли более 3000 человек.

Одним из знаменательных событий последних лет является ежегодный всероссийский семинар по теме «Перспективы развития ИС Приток-А и вопросы сотрудничества при ее внедрении», который проводится на базе ОБ «СОКРАТ», как правило, в конце июня. Ежегодно в семинаре принимают участие представители различных регионов — Иркутской, Челя-

бинской, Кемеровской, Омской областей, Хабаровского и Красноярского краев и Республики Бурятия и т.д. Традиция проведения таких ежегодных семинаров будет продолжаться.

Для дальнейшего совершенствования учебного процесса в ОБ «СОКРАТ» разработан и запущен в производство «Учебно-методический стенд» (УМС-2), который позволяет изучать основные принципы построения и внедрения ИС Приток-А. УМС-2 обеспечивает демонстрацию основных возможностей и особенностей подсистем Приток-ТСР, Приток-А, Приток-А-Р, Приток-GSM, Приток-КОП и других.

К примеру, в 2014 году изготовлено 60 УМС-2. Поставка стендов проводилась в подразделения вневедомственной охраны, УВО, ФГУП «Охрана». УМС были переданы УМЭЦ ФГУ НИЦ «Охрана», в класс Институт МВД в Иркутске, где они сейчас используются в учебных процессах. Несколько стендов безвозмездно направлены в региональные представительства в различные области России и ближнего зарубежья. Стенды в региональных представительствах применяются для изучения возможностей ИС Приток-А и для демонстрации их потенциальным потребителям системы.

Остальные стенды направлены в региональные управления вневедомственной охраны, внедрившие ИС Приток-А у себя в подразделениях.

Для организации изучения одной из подсистем ИС Приток-А — подсистемы мониторинга подвижных объектов Приток-МПО (ГЛОНАСС/GPS) — в режиме реального времени имеется возможность установки рабочего места Приток-МПО, которое подключается к WEB-серверу центра мониторинга ОБ «СОКРАТ». Такое учебное место создано в Воронежском институте МВД.

Работа в этом направлении продолжается

Участие в выставках

2013
MIPS 2013 — 19-я Московская международная выставка «Охрана, безопасность и противопожарная защита»

2012
Пятый ежегодный всероссийский семинар на тему: «Особенности развития ИС Приток-А и вопросы сотрудничества при ее внедрении»

MIPS 2012 — Московская международная выставка «Охрана, безопасность и противопожарная защита»

2011
Четвертый ежегодный всероссийский семинар: «Особенности развития ИС Приток-А и вопросы сотрудничества при ее внедрении»

MIPS 2011 — Московская международная выставка «Охрана, безопасность и противопожарная защита»

2010
Национальная отраслевая премия «За укрепление безопасности России» («ЗУБР 2010»). Диплом и золотая медаль в категории «Антикриминал-антитеррор»

Третий ежегодный всероссийский семинар «Особенности развития ИС Приток-А и вопросы сотрудничества при ее внедрении»

MIPS 2010 — Московская международная выставка «Охрана, безопасность и противопожарная защита»

2009
Всероссийская научно-практическая конференция «Охрана, безопасность и связь — 2009»

Второй ежегодный семинар, посвященный развитию и внедрению ИС «Приток-А»

MIPS 2009 – Московская международная выставка «Охрана, безопасность и противопожарная защита»

2008
Семинар «Программно-аппаратные средства АРМ» в НИЦ «Охрана»

Первый семинар, посвященный развитию и внедрению ИС «Приток-А»

Правовая основа деятельности

Вся деятельность Охранного бюро «СОКРАТ» защищена соответствующими лицензиями и сертификатами

• **Лицензия Регионального управления Федеральной службы безопасности по Иркутской области № 711** на право проведения работ, связанных с использованием сведений, составляющих государственную тайну

• **Лицензия МЧС РФ №1/15440** на осуществление деятельности по тушению пожаров

• **Лицензия МЧС РФ №2/27199** на осуществление Производства работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений

• **Лицензия Федерального агентства по строительству и жилищно-коммунальному хозяйству № ГС-6-38-02-26-0-3808021624-005430-2** разрешает осуществлять проектирование зданий и сооружений I и II уровней ответственности в соответствии с государственным стандартом

• **Лицензия Федеральной службы по надзору в сфере связи № 45134** на право оказания Услуги подвижной радиосвязи в сети связи общего пользования Федерального агентства геодезии и картографии № ВСТ-00600К на осуществление «Картографической деятельности»

• **Лицензия Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия №58434** на право оказания «Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации»

• **Сертификат соответствия Системы сертификации ГОСТ Р** о том, что система менеджмента качества предприятия «Соответствует требованиям ГОСТ Р ИСО 9001-2008 (ИСО9001-2008)»

• **Свидетельство на товарный знак (знак обслуживания) № 359689 «ПРИТОК»**

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

ЛИЦЕНЗИЯ

№ 6-Б/01410 от 11 ноября 2013 г.

На осуществление: *Деятельность по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений*

Виды работ, выполняемых в составе лицензируемого вида деятельности:

Настоящая лицензия предоставлена: Общество с ограниченной ответственностью Охранное бюро "СОКРАТ"
ООО ОБ "СОКРАТ"

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя): 1033801007690

Идентификационный номер налогоплательщика: 3808021624

№ 107041

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО
на товарный знак (знак обслуживания)
№ 359689

ПРИТОК

Правообладатель: *Общество с ограниченной ответственностью охранное бюро "Сократ", 664007, г.Иркутск, пер.Волконского, 2 (RU)*

Заявка № 2007709256
Приоритет товарного знака 02 апреля 2007 г.
Зарегистрировано в Государственном реестре товарных знаков и знаков обслуживания Российской Федерации *12 сентября 2008 г.*
Срок действия регистрации истекает 02 апреля 2017 г.

Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам *Б.П. Симонов*

• **Свидетельство № 0094-2009-3808021624-С-22** о допуске к работам, которые оказывают влияние на безопасность объектов капитального строительства

• **Сертификат пожарной безопасности № ССПБ.RU/ОП006.В00789** на Автоматизированную систему охранно-пожарной сигнализации Приток-А в полном составе

• **Сертификат соответствия № РОСС RU.ОС03.И00800** на Автоматизированную систему охранно-пожарной сигнализации и подсистему мониторинга подвижных объектов Приток-МПО

• **Декларация соответствия Министерства связи РФ** на Автоматизированную систему охранно-пожарной сигнализации Приток-А в полном составе

• **Сертификат соответствия техническому регламенту (№123-ФЗ от 22.07.2008)** на систему Приток-А

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ГЕОДЕЗИИ И КАРТОГРАФИИ

ЛИЦЕНЗИЯ

№ ВСТ-00600К от "13" декабря 2007 г.

На осуществление картографической деятельности

для выполнения следующих заявленных работ:

1.) 2.2.0.0.0

2.) 2.3.0.0.0

3.) 6.4.0.0.0

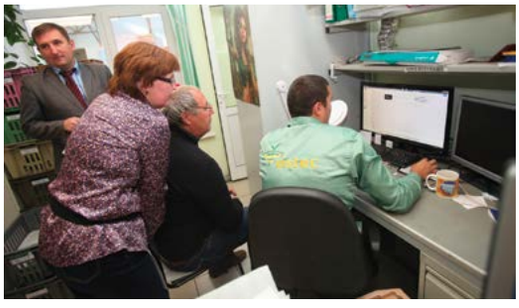
Общество с ограниченной ответственностью "Охранное бюро "СОКРАТ"
ООО ОБ "СОКРАТ"

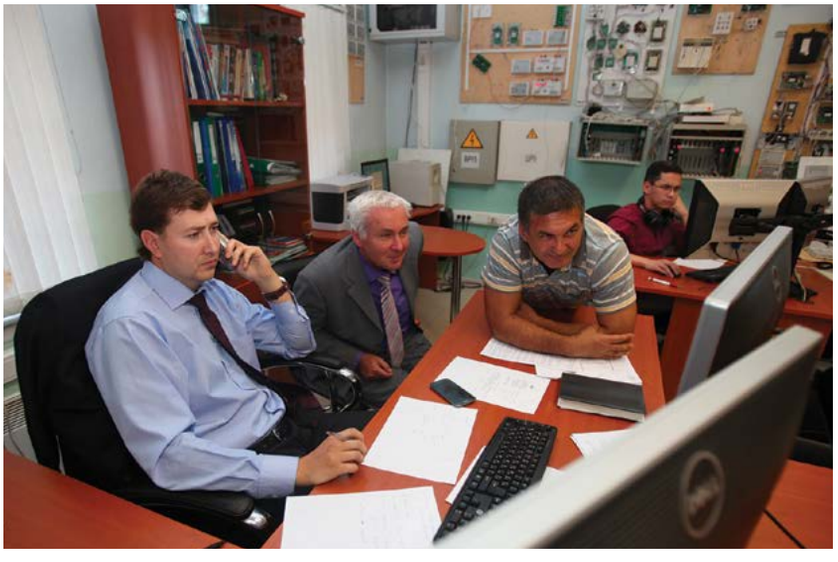
Контактная информация: Иркутск, пер. Волконского, 2, код междугородной связи 3952

Секретарь: 20-66-62 | **Техподдержка: 20-66-70, 20-66-61** | **Бесплатный номер: 8-800-333-66-70**

Так создается «Приток-А»

Это почти уникальная возможность – попасть внутрь Охранного бюро «СОКРАТ» в рабочее время и понаблюдать, как создается известный на всю Россию охранно-пожарный комплекс «Приток-А»...





Представительства ОБ «СОКРАТ»

АЛТАЙСКИЙ КРАЙ

Барнаул

ООО «Элия»
656015, г. Барнаул, ул. Деповская, 7
Тел/факс: 8(3852) 69-12-75, 36-76-04
E-mail: eliya@land.ru
Сайт: www.eliya.barp.ru

АМУРСКАЯ ОБЛАСТЬ

Благовещенск

ООО «СТЭЛС»
675000, г. Благовещенск, ул. Артиллерийская, 17
Тел./факс: (4162) 519-777
E-mail: sale@stels-amur.ru

БАШКОРТОСТАН

Уфа

ООО «АВАКС»
Юр. адрес: 450112, г. Уфа, ул. Ульяновых, 45
Факт. адрес: 450022 г. Уфа,
ул. Бакалинская, 68/6
Тел/факс: (347) 253-64-52,
252-39-98
E-mail: avaks-ufa@yandex.ru,
ronin2030@yandex.ru

ООО ПСБ «Техника Охраны»
450076, г. Уфа, ул. Пушкина, 35
Тел/факс: (347) 2513-403
E-mail: psbtorb@yandex.ru

БУРЯТИЯ

Улан-Удэ

ООО «Контур»
670024, Республика Бурятия,
г. Улан-Удэ, ул. Минина, 4а
Тел./факс: (301-2) 55-22-27, 46-63-58,
46-59-91
E-mail: kontur.bur@mail.ru

ООО «Эликом плюс»
670034, г. Улан-Удэ, пр. 50 лет Октября, 27
Тел./факс: (3012)46-30-55, 55-07-55
E-mail: info@elikomnet.ru

ООО ОБ «Дозор-Р»
670034, г. Улан-Удэ, пр. 50 лет Октября, 13
Тел/факс: (301-2) 46-78-81,
46-78-82, 46-78-83
E-mail: dozor-dogovor@mail.ru

ВОЛГОГРАДСКАЯ ОБЛАСТЬ

Волгоград

ООО «Подмосковье»
400123, г. Волгоград, ул. Маршала Еременко, 21
Тел./факс: (8442) 73-65-06, 28-27-49
E-mail: DIREKTOR@XEPCOH.RU

ВОЛОГОДСКАЯ ОБЛАСТЬ

Вологда

ООО «Система безопасности»
160012, г. Вологда, ул. Козленская, 83, оф. 1
Тел/факс: (8172) 75-21-33, 50-05-90
E-mail: 3osb@rambler.ru

Череповец

ООО Технический центр
«Системы телемеханики»
Юр. адрес: 162600, Череповец,
пр-кт Строителей, 28-А, оф.125
Тел./факс: (820-2) 22-38-43, 22-33-83
E-mail: stm-cher@mail.ru

ВОРОНЕЖСКАЯ ОБЛАСТЬ

Воронеж

ООО «Академия безопасности-Воронеж»
394026, г. Воронеж,
пр-т Труда, 39, офис 212
Тел./факс: (4732) 34-39-30, 34-39-31
E-mail: komdirab@yandex.ru

ЕВРЕЙСКАЯ АВТОНОМНАЯ ОБЛАСТЬ

Биробиджан

ООО «Центр Безопасности»
679000, ЕАО, г. Биробиджан,
ул. Постышева, 6, офис 7
Тел./факс: (42622)21-444
E-mail: safety_centre@e-mail.ru

ИРКУТСКАЯ ОБЛАСТЬ

Иркутск

ООО «Ультра»
664007, г. Иркутск,
ул. Декабрьских Событий, 103А, кв. 88
Тел/факс: (395-2)20-73-84

ООО «СОКРАТ-АВТО»
664007, г. Иркутск, ул. Событий, 109
Тел/факс: 20-54-92, 21-18-54, 21-18-52
E-mail: tsganov.sokrat@mail.ru

ООО «Охранное предприятие
«Иркутскэнерго»
664056, г. Иркутск, ул. Безбокова, 38 «А»
Тел/факс 287-755, 795-980

Ангарск

ООО «Электрон»
665835, г. Ангарск, Ленинградский пр-т,
6, к. А, оф. 301
Тел/факс: (3955)56-32-02, 67-62-71, 56-52-25
E-mail: elektron@elektron-ksb.ru,
elektron@irmail.ru

ООО «Полином»
665813, г. Ангарск, 80 кв-л, 3, помещение 2
Тел /факс: (3955) 52-65-81, 52-45-50,
52-63-44, 52-91-60
E-mail: polinominfo@ang.ru, polinom@ang.ru

Братск

ООО «Сэйфти»
665708, г. Братск, ул. Коммунальная, 21
Тел /факс: (3953) 41-12-99, 41-50-01
E-mail: seifty@mail.ru

Слюдянка

ИП Кузьмина Татьяна Николаевна
665904, Иркутская обл, г. Слюдянка,
ул. Ленина, 3 б, кв.8
Тел/факс: (395-44) 519-39,
моб. 8-914-887-57-15

КАЗАХСТАН

Павлодар

ТОО Бизнес-Линк ПВ
140000, Республика Казахстан, г. Павлодар,
ул. Ак. Сатпаева, дом 254
Тел./факс: (718-2) 20-22-28

Кокшетау

ИП «NOVICAMSEVER»
020000, г. Кокшетау, ул. Горького, 65а, кв.4
Тел./факс: (7162) 25-24-24, 25-60-06

КАМЧАТСКИЙ КРАЙ

Петропавловск-Камчатский

ООО Охранное предприятие
«Альфа Безопасность»
683031, г. Петропавловск-Камчатский,
ул. Топоркова, 1/1, оф. 01
Тел./факс: (4152) 22-72-72, ф. 22-71-71
E-mail: alfakam@mail.ru

КАРЕЛИЯ

Петрозаводск

ООО «Нордспецавтоматика плюс»
185005, Республика Карелия,
г.Петрозаводск, ул. Льва Толстого, 22, пом.33
Тел./факс (8142)76-93-59, 57-62-39,
8-921-727-25-68
E-mail: nsa87@inbox.ru

ИП Бильков Сергей Геннадьевич
Юр. адрес: 185034, г. Петрозаводск,
пер. 4-й Родниковый, 28, кв.2
Факт. адрес: 185031, г. Петрозаводск,
ул. Московская, 3А
Тел./факс (8142)76-41-64, 70-41-64,
33-10-01

КЕМЕРОВСКАЯ ОБЛАСТЬ

Кемерово

ООО Торговый дом «Системы безопасности»
650025, г. Кемерово, ул. Чкалова, 4
Тел./факс: (384-2) 45-23-59, 45-23-58
E-mail: sbtd@rambler.ru

КИРОВСКАЯ ОБЛАСТЬ

Киров

ООО «Щит»
610035, г. Киров, ул. Сурикова, 50
Тел/факс: (8332) 327-500
E-mail: andrey43region@mail.ru

КОМИ

Сыктывкар

ООО «Стандарт безопасности»
167982, г. Сыктывкар, ул. Пушкина, 30/1
Тел./факс: (8212) 28-84-09, 30-24-05,
203-501, 203-502
E-mail: lavina@mkb-gambit.ru

ООО «Лема-Прим»
167023, г. Сыктывкар,
ул. Морозова, 100
Тел/факс: (8212) 32-30-54, 32-30-55
E-mail: ooolemask@gmail.com

Инта

ИП Тучковская Людмила Алексеевна
Юр. адрес: 169849, РК, г. Инта,
ул. Кирова, 20а
Факт. адрес: 169840 РК, г. Инта,
ул. Дзержинского, 27

КОСТРОМСКАЯ ОБЛАСТЬ

Кострома

ООО «Визит»
156013, г. Кострома,
ул. Комсомольская, д 48/16
Тел/факс: (4942) 37-03-51, 55-32-62,
37-30-02
E-mail: vizit-sb@kmtn.ru

КРАСНОДАРСКИЙ КРАЙ

Краснодар

ООО «Радуга-К»
350042, г. Краснодар,
ул. Серова, 50
Тел/факс: (861) 254-28-81
E-mail: raduga-k@list.ru

КРАСНОЯРСКИЙ КРАЙ

Красноярск

ООО «ТРЕАЛ КРАСНОЯРСК»
Юр. адрес: 660118, г. Красноярск,
ул. Урванцева, 12
Факт. адрес: 660079, г. Красноярск,
ул. Матросова, 30 Л, стр. 11
Тел/факс: (3912) 792-792, 792-297,
782-479
E-mail: treal_2003@list.ru

ИП Сергиенко
660025, г. Красноярск, пр-т имени газеты
«Красноярский рабочий», 113, пом.42
Тел/факс: (3912) 45-75-35
E-mail: orion-sb@list.ru

ООО «Витязь-Эксперт»
Юр. адрес: 660135, г. Красноярск,
ул. Взлетная, 28
Факт. адрес: Красноярский край,
г. Норильск, ул. Нансена, 102, оф.101
Тел/факс: (3912)29-93-29,
8-913-506-45-54
E-mail: oooab-vityaz@mail.ru

КРЫМ

Симферополь

АО «ОХРАНА-КОМПЛЕКС-КРЫМ»
295013, Республика Крым,
г. Симферополь, ул. Миллера Ж.А., 4
Тел.: (0652) 54-10-99
E-mail: teremenko.alex@gmail.com

ЛИПЕЦКАЯ ОБЛАСТЬ

Липецк

ООО «Приток-Липецк Сервис»
398036, г. Липецк,
б-р Шубина, 8а - 46
Тел.: 8-904-692-33-20
E-mail: pritok48@yandex.ru

МАГАДАНСКАЯ ОБЛАСТЬ

Магадан

Областное специализированное охранное предприятие «Ягуар»
685000, г. Магадан,
пер. 3-й Транспортный, 12
Тел.: (413-26) 2-39-86, 3-08-10
E-mail: info@jaguar49.ru

МОСКВА

ИП Бухвалов Г.Ю.
117405, г. Москва,
ул. Дорожная, 60 Б, офис 07
Тел.: (499) 558-01-12,
(495) 628-75-48, 625-43-12
E-mail: sokratm@mail.ru

ООО «Охрана Телеком»
Юр. адрес: 107143,
г. Москва, Открытое шоссе, 17,стр.1
Факт. адрес: 125167,
г. Москва, ул. Викторенко, 14
Тел.: (495) 617-02-86

МОРДОВИЯ

Саранск

ООО «ЦАНГ»
Юр. адрес: 430005, РМ,
г. Саранск, ул. Крупской, 29
Факт. адрес: 430030, РМ,
г. Саранск, ул. Титова, 8
Тел.: (8342)23-33-69, 23-18-15
E-mail: zangrm@mail.ru

НОВОСИБИРСКАЯ ОБЛАСТЬ

Новосибирск

ООО Корпорация «Грумант»
630123, г. Новосибирск,
ул. Красногорская, 27а
Тел/факс: (383) 210-52-53, доб. 121
E-mail: vtb@grumant.ru

Представительства ОБ «СОКРАТ»

ООО «АльфаКом СБ»
630075, г. Новосибирск, ул. Народная, 3
Тел/факс: (383) 205-04-59, 363-91-37
E-mail: tender@alfakomsb.ru

НОВГОРОДСКАЯ ОБЛАСТЬ

Великий Новгород

ООО «Охрана-Сервис»
Юр. адрес: 173000, г. Великий Новгород, ул. Федоровский ручей,16-2-31
Факт. адрес: 173014, г. Великий Новгород, ул. Студенческая, 31, офис 2
Тел./факс: (8162) 63-50-07
E-mail: rembodr@mail.ru

ОМСКАЯ ОБЛАСТЬ

Омск

ООО «Системы контроля и безопасности»
Юр. адрес: 644076, г. Омск, ул. Петра Осьминина, дом 13, кв. 64
Факт. адрес: 644065, г. Омск, ул. Нефтезаводская, 38Е, корпус 1. оф. 4
E-mail: skb-omsk@yandex.ru

ООО «Союз-Сервис»
644074, г. Омск, пр-кт Комарова, 15, корп.1
Тел.: (38-12) 70-36-38(факс) 21-51-02, 21-51-03, 70-35-07
E-mail: soyz-servis@mail.ru

ОРЕНБУРГСКАЯ ОБЛАСТЬ

Оренбург

ООО «Компания Энерготрейд»
Юр. адрес: 460520, Оренбургская обл., Оренбургский р-он, пос. Нежинка, ул. Бахчева, 50
Почт. адрес: 460009, г. Оренбург, ул. Орлова, 52
Тел./факс: (3532)57-20-27, 57-22-65, 57-18-38
E-mail: energotreid56@yandex.ru

ПРИМОРСКИЙ КРАЙ

Владивосток

ООО «Сократ-Прим»
Юр. адрес: 690087, г. Владивосток, ул. Шилкинская, 16, кв.115
Факт. адрес: 690014, г. Владивосток, ул. Всеволода Сибирцева, 79, оф.1
Тел/факс: : (4232) 26-63-66, 60-60-02, 60-59-49
E-mail: okdv@bk.ru

Спасск-Дальний

ООО «Приморавтоматика»
692239, Приморский край, г. Спасск-Дальний, ул. Коммунаров, 1в» Тел/факс: (423-52) 3-17-71, 2-87-17
E-mail: primoravtomatika25@mail.ru

ПЕРМСКИЙ КРАЙ

Пермь

ООО «Аксилиум»
Юр. адрес: 614000, г. Пермь, ул. Камчатская, 18, кв. 19
Факт. адрес: 614000, г. Пермь, ул. Краснова, 24
Тел/факс: (342)220-31-76, 220-31-77, 220-31-78
E-mail: info@aks-sb.ru

ООО «Глобал-Трейд»
Юр. адрес: 614002, г. Пермь, ул. Николая Островского, 113, оф. 10
Факт. адрес: 614015, г. Пермь, ул. Краснова, 24
Тел./факс: (846) 200-22-20, +79272601603, +79276973464

САМАРСКАЯ ОБЛАСТЬ

Самара

ООО «Витаком-Трейд»
443030, г. Самара, ул. Черноречeнская, 21, к. 2
Тел/факс: (846)200-22-20
E-mail: vitacom@vitacom.ru

ООО «РОМС»
443050, г. Самара, Серноводский 2-й тупик, 7
Тел/факс: (846) 22-99-186
E-mail: nik.somov.65@mail.ru

САРАТОВСКАЯ ОБЛАСТЬ

Саратов

ООО «Байкал»
410052, г. Саратов, ул. Лунная, 44
Тел/факс: (8452) 35-40-58, 927-623-35-30
E-mail: baikalsar@mail.ru

ООО «Тех-Защита-М»
410052 г. Саратов, ул. Лунная, 44
Тел/факс: (8452) 44-61-23, 44-61-24, 35-53-70
E-mail: teh-zashita@yandex.ru

САХА (ЯКУТИЯ)

Якутск

ООО «Спецавтоматика»:
Юр. адрес: 677000, РС (Якутия), г. Якутск, 202-й мкр, 9, оф.108
Фактич. адрес: 677007, РС (Якутия), г. Якутск, ул. Автодорожная, дом 14А
Тел/факс 8(4112)36-38-39, 40-38-58, 70-27-49
E-mail: ops@sakha.ru

Ленск

ООО «Заслон»
Юр. адрес: 678144, РС (Якутия), г. Ленск, ул. Набережная, 99/35
Факт. адрес: 678144, РС (Якутия), г. Ленск, ул. Набережная, 75
Тел./факс: (41137)4-30-22, 8-924-608-77-75
E-mail: zaslon-security@mail.ru

САХАЛИНСКАЯ ОБЛАСТЬ

Южно-Сахалинск

ООО «СОВА-2012»
693000, г. Южно-Сахалинск, пр. Мира, 20, оф.10
Тел/факс: (4252) 50-52-20
E-mail: elmar1950@mail.ru

СВЕРДЛОВСКАЯ ОБЛАСТЬ

Екатеринбург

ООО «Сократ Урал-МЦ»
Юр. адрес: 620130, г. Екатеринбург, ул. Белинского, 220, к.6, кв.16
Факт. адрес: 620144, г. Екатеринбург, ул. Большакова, 153 Б
Тел/факс: (343)355-55-65, 269-31-61
E-mail: ad@r96.ru

СТАВРОПОЛЬСКИЙ КРАЙ

Ставрополь

ООО «Паритет»
355040, г. Ставрополь, ул. Тухачевского, 21, корпус 2
Тел.: 8-962-445-87-57
E-mail: office@paritet26.ru

Пятигорск

ООО «Сигнал-Сервис»
357532, г. Пятигорск, ул. 295-ой Стрелковой Дивизии, 2, оф. 202

Тел./факс: (879-3) 38-06-19,
32-13-71, 32-21-92
E-mail: signalkmv@mail.ru

ТОМСКАЯ ОБЛАСТЬ

Томск

ООО «Торговая компания Синтекс»
634034, г. Томск, ул. Нахимова, 18
Тел./факс: (3822)900-434
E-mail: gerkontsk@mail.ru

ООО «Галан»
634057, г. Томск,
ул. 79-ой Гвардейской Дивизии, 27а
Тел./факс: (3822)211-757
E-mail: galan-ops@mail.ru

ТЮМЕНСКАЯ ОБЛАСТЬ

Тюмень

ООО «Бруклин»
625019, г. Тюмень, ул. Республики, 206, стр.19
Тел. (3452) 27-42-81, 8-909-189-30-44
E-mail: tyumen14@mail.ru

ООО «Центр-СБ»
625013, г. Тюмень, ул. 50 лет Октября, 63 Б
Тел.: (3452) 500-067
E-mail: zentrsb@gmail.com

Ялуторовск

ООО «Спецмонтаж»
627018, Тюменская область, г. Ялуторовск,
ул. Ворошилова, 61/1
Тел/факс: (345-35) 2-05-80, 2-49-80
E-mail: 72spm@mail.ru

Тобольск

ИП Коршунов Георгий Сергеевич
626150, Тюменская обл..
г. Тобольск, 15 микрорайон, 3, кв. 37
Тел/факс: 8-982-908-83-33
E-mail: korschun@list.ru

ТЫВА

Кызыл

ООО «ГЕРМЕС»
667005, Республика Тыва,
г. Кызыл, ул. Кочетова, 95, кв. 103
Тел.: (39422)2-20-04, 2-12-96
E-mail: germes-tuva@inbox.ru

УДМУРТИЯ

Ижевск

ООО «Торговый дом «Антарис»
426057, Удмуртская Республика, г. Ижевск,
ул. Свердлова, 18, офис 4
Тел/факс: (3412) 65-65-65
E-mail: antaris@udm.ru

ООО «Арго-Системы Безопасности»
426011, УР, г. Ижевск, ул. К.Маркса, 440
Тел/факс: (3412) 900-751
E-mail: bina70@bk.ru

УЗБЕКИСТАН

Шахрисабз

ООО «Mars Electronics»
181300, Республика Узбекистан,
Кашкадарьинская область, г. Шахрисабз,
ул. Ипак йули-100
Тел/факс: (+99875) 221-08-08, 522-80-00,
221-78-09, 525-75-92
E-mail: mars-im@mail.ru

ХАБАРОВСКИЙ КРАЙ

Хабаровск

ООО Торговый дом «Востокавтоматика»
680028, г. Хабаровск, ул. Тургенева, 96 корпус 1
Тел./факс: (4212) 42-20-11, 42-20-05
E-mail: td@vavtomatics.ru

ООО «СОКРАТ-ДВ»
680021, г. Хабаровск, ул. Панькова , 29-Б.
Тел.: (4212) 75-89-19
E-mail: sokratdv@mail.ru

Комсомольск-на-Амуре

ИП Подлесная Светлана Владимировна
681024, Хабаровский край,
г. Комсомольск-на-Амуре,
пр. Первостроителей, 21, кв. 322
Тел.: 8-914-185-11-81
E-mail: videovam@mail.ru

ХАКАСИЯ

Абакан

ООО «Альтернатива»
Юр.адрес: 655017, г. Абакан,
ул. Ленина, 78-14
Факт. адрес: 655000, г. Абакан,
ул. М. Горького, 44
Тел/факс: (3902)21-54-13,
сот. 8-902-996-22-03
E-mail: ra0wbn@yandex.ru

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ

Челябинск

ООО Компания «Регион-Сервис»
454091, г. Челябинск, ул. Российская, 159-в,
оф.201
Тел.: (3512) 64-00-93, 71-59-84
E-mail: regionservis@mail.ru

ЧИТИНСКАЯ ОБЛАСТЬ

Чита

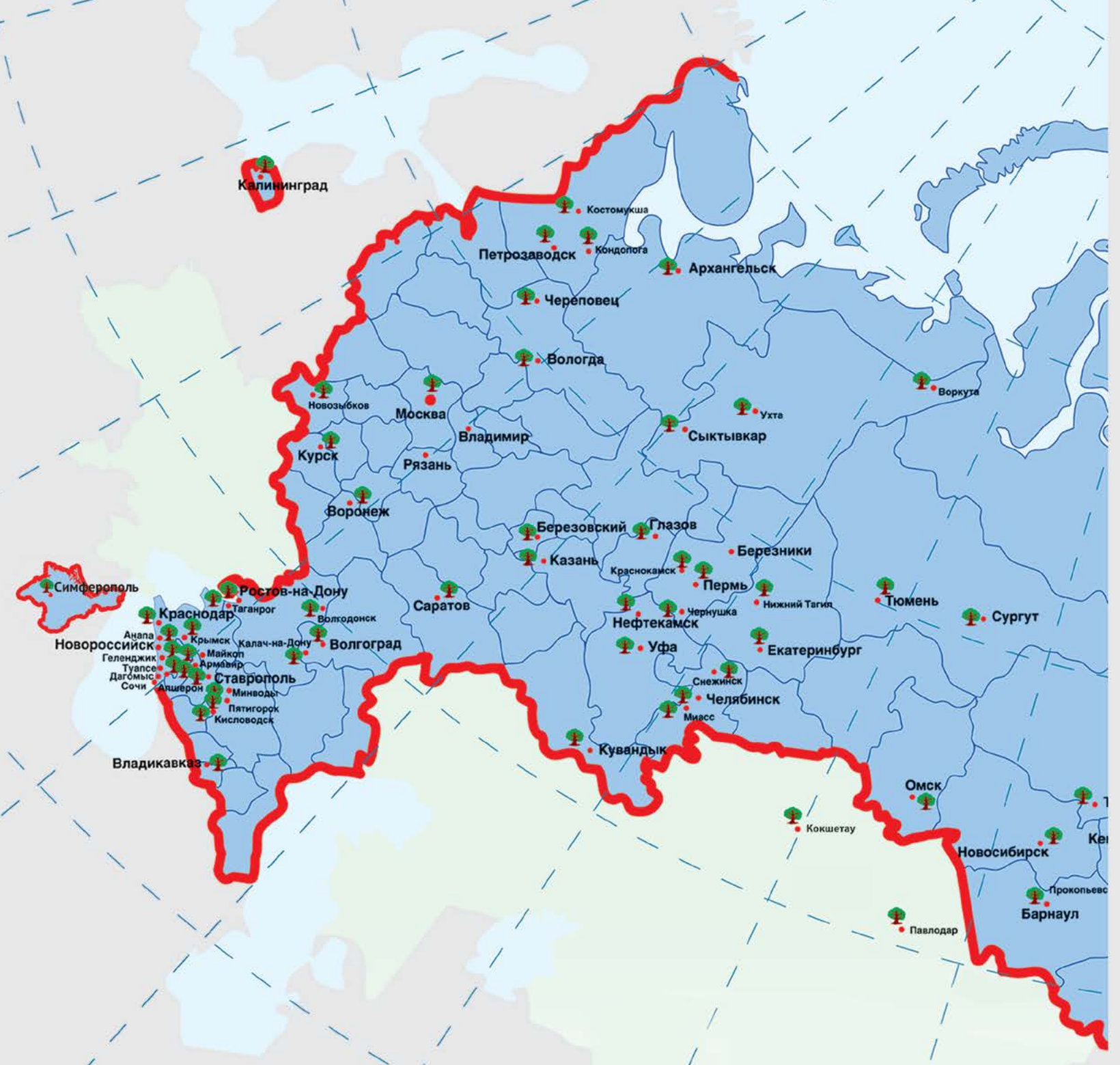
ООО ОБ «СОКРАТ-Чита»
672022, г. Чита, проезд Энергостроителей, 4а
Тел/ф.: (302-2) 310-448, 352-473, 351-888
E-mail: sokrat-chita@mail.ru

ЧУВАШИЯ

Чебоксары

ООО «Роникс»
428022, г. Чебоксары,
Машиностроителей проезд, 1
Тел./факс: (8352) 28-02-88, 28-26-27,
23-04-44
E-mail: sales@ronix21.ru

ИП Порфирьев Сергей Михайлович
428018, Россия, г. Чебоксары,
ул. 2-ая Герцена, 5
Тел./факс: (8352) 55-66-66, 55-08-87
E-mail: tsb21@mail.ru



Карта официальных представительств Охранного Бюро «СОКРАТ»


Норильск
Удачный
Айхал
Якутск
Магадан
Мирный
Ленск
Алдан
Нерюнгри
Бодайбо
Усть-Илимск
Ачинск
Канск
Красноярск
Братск
Тайшет
Северобайкальск
Чернышевск
Нерчинск
Саянск
Черемхово
Новокузнецк
Усолье-Сибирское
Ангарск
Иркутск
Шелехов
Байкальск
Улан-Удэ
Чита
Краснокаменск
Борзя
Петровск-Забайкальский
Гусиноозерск
Комсомольск-на Амуре
Благовещенск
Хабаровск
Лучегорск
Спасск-Дальний
Артем
Владивосток

www.sokrat.ru

СОКРАТ

ООО Охранное Бюро «СОКРАТ»
664007, г. Иркутск, пер. Волконского, 2
Тел./факс: 8 (3952) 20-66-61, 20-66-62, 20-66-63, 20-64-77
Телефон техподдержки: 8-800-333-66-70 (бесплатный)
E-mail: sokrat@sokrat.ru