СПЕЦИАЛИЗИРОВАННЫЙ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ
О ПРОБЛЕМАХ БЕЗОПАСНОСТИ

№ 01(5) 2015 Иркутск

СОКРАТ

Система, изменившая уровень безопасности России

Особенности создания ПЦН

Приток-А КОП – новые возможности

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

2015 № 1(5)

Издатель:
ООО Рекламно-издательская фирма «Гвоздь плюс»

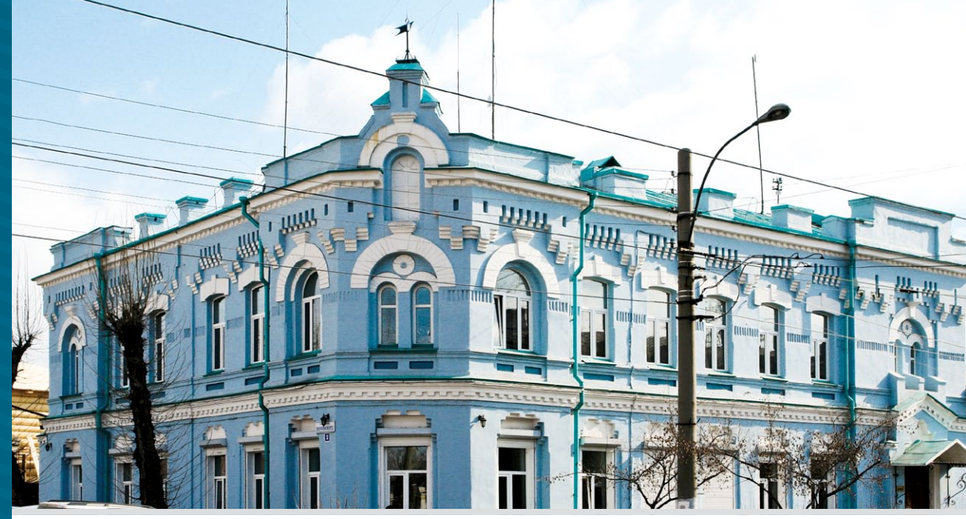
664025,
Иркутск, ул. Марата, 29
Тел.: (3952) 22-33-22, 34-20-79, 33-45-24
E-mail: gvozd@irmail.ru
www.kapitalpress.ru

Подготовка издания:
Константин Куликов

Верстка, допечатная подготовка:
Екатерина Бас

Иллюстрации:
Татьяна Бояркина

Журнал отпечатан в типографии «Репроцентр А1»



Содержание

Четверть века на службе государства

Система безопасности из Иркутска

И все же, наверное, подобный вопрос нужно отнести к категории риторических: «25 лет — это много или мало?». Если в целом для мировой истории с ее многоуровневой толщей веков, то это лишь миг. С другой стороны, именно в четверть века вмещается практически вся новейшая история целого государства — России. А для одного предприятия, начинавшегося в постперестроечное экономическое безвременье и ставшего за эти годы одним из российских лидеров в своей сфере, 25 лет — это целая жизнь.

— 25 лет — это серьезная дата для любого предприятия, для каждого человека, — уверен Анатолий Илюшин, директор ОБ «СОКРАТ». — Четверть века назад мы, несколько инженеров Иркутского КБ радиосвязи, даже не думали, что созданное нами предприятие будет отмечать вот такую дату…

Ровно четверть века назад, в декабре 1989 года, в Иркутске произошло событие, которое теперь считается днем рождения Охранного бюро «СОКРАТ», разработчика и производителя известного на всю Россию охранно-пожарного комплекса «Приток».

— Когда все начиналось, милиция и серьезная электроника, вычислительные машины были понятиями, абсолютно не совместимыми, — продолжает Анатолий Иванович. — Но тот день, когда мы убедились, что наша разработка действительно нужна, отмечается теперь как день рождения предприятия. 25 декабря 1989 года был подписан первый договор на поставку оборудования в иркутское управление вневедомственной охраны. Было понятно, что руководство управления рисковало. Но они поверили в нас. И мы практически за год смогли разработать то, что им требовалось. А вскоре, уже после Иркутска, наш комплекс «Приток» вышел на общероссийский простор: Якутск, Крым — Евпатория, Краснодар и т.д.

— Не раз приходилось слышать, что причина успеха охранного комплекса «Приток», в первую очередь, в том, что вы и ваши коллеги сумели опередить время и предугадать направление будущего развития технологий связи.

— Действительно, еще на стадии первоначального проектирования мы заложили идею, которая и стала основополагающей: «Приток» должен интегрировать в себя все то, что эксплуатировалось в подразделениях вневедомственной охраны и других подобных структурах, и развиваться независимо от того, какие технологии передачи информации в данный момент используются.

Анатолий Илюшин,
директор ОБ «СОКРАТ»:

— Как и почти четверть века назад, продукция предприятия востребована и пользуется устойчивым спросом. И наши заказчики по-прежнему считают, что Иркутск один из немногих в России производит достойные системы безопасности.

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

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

— Это «размножение» — как результат вашего двадцатипятилетнего труда и оценка всей проделанной работы. Какова она сегодня?

— Цифры, которые мы имеем, ответят наиболее красноречиво. Темпы нашего ежегодного роста по выручке, по объемам роста, по номенклатуре сейчас на уровне 10-15%. Это вполне достойный результат. Кроме того, по объемам выручки и по числу сотрудников — 200 человек — наше предприятие уже не умещается в категорию малых. Видимо, вскоре «СОКРАТ» перейдет в категорию средних предприятий.

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

Основной потребитель нашей охранно-пожарной системы — подразделения вневедомственной охраны Департамента государственной защиты имущества (ДГЗИ) МВД РФ. Их сейчас более 500.

Охранный комплекс «Приток» присутствует в Бюллетене технических средств безопасности, рекомендованных к использованию вневедомственной охраной. Этот бюллетень утверждается ДГЗИ МВД России. А по объемам поставок оборудования, которые финансируются через госзаказ и идут в 50 регионов РФ, «СОКРАТ» входит в тройку лидеров среди всех российских профильных предприятий.

Вот с такими результатами мы подошли к четвертьвековому рубежу.

— Охранное бюро «СОКРАТ» всегда было одним из лидеров в сфере разработки и производства систем безопасности. Скажите, а лидировать трудно?

— Лидером можно быть на каком-то этапе, на какой-то период времени. Но удержаться на этом рубеже надолго достаточно сложно. Потому что все видят, кто идет впереди, стараются его догнать и обогнать.

И, наверное, поэтому неправильно было бы представлять, что наша система «Приток» в 90-е годы прошлого века вдруг в одночасье изменила принципы работы российской вневедомственной охраны. Силовые ведомства — не те структуры, чтобы сразу и единым порывом принимать новшества. Пришлось действовать настойчиво, убеждая и доказывая преимущества системы.

Еще в самом начале, когда испытания нашей системы проводились в Балашихе, у нас получилось доказать экспертам научно-исследовательского центра «Охрана» ГУВО МВД России, что и в Иркутске возможны разработка и производство аппаратуры достойного уровня, причем превосходящего отдельные образцы той техники, которая разрабатывалась аналогичными предприятиями России.

Это был первый, но далеко не единственный случай, когда приходилось доказывать специалистам МВД своевременность и перспективность наших разработок.

В 1998-99 годах, мягко говоря, непониманием встретили в столице наше предложение использовать в охране спутниковые технологии, интернет, ввести мониторинг автотранспорта. В 2001-02 годах точно так же отнеслись к предложению применять сотовую связь.

Вехи истории

25 декабря 1989 года
Подписание первого договора на разработку не имеющей аналогов охранной системы «Приток-А» для Иркутского управления вневедомственной охраны. Считается днем рождения ОБ «СОКРАТ»

1991 год, март
Внедрение первого АРМ Приток в Иркутске в Кировском ОВО

1996 год
Комплекс «Приток-А» эксплуатируют уже около полусотни подразделений вневедомственной охраны России

1998 год
Внедрена первая система «Приток-МПО», предназначенная для мониторинга и охраны подвижных объектов (транспортных средств)

В конце концов соответствующие решения, конечно, принимали. Но мы-то времени даром не теряли. К тому моменту мы уже имели модернизированные системы и проводили их эксплуатационные, комплексные испытания. Делали все для того, чтобы эта аппаратура сразу пошла в подразделения.

— Уже 25 лет система «Приток» существует и продолжает развиваться. Какие новые функции и возможности она приобрела в последнее время?

— Благодаря нашим талантливым разработчикам Интегрированная система охранно-пожарной сигнализации «Приток-А» идет в ногу с бурным современным развитием средств связи и коммуникаций. В течение последнего года нашим предприятием активно развивалась линейка новых приборов «Приток-КОП» — это приборы, которые используют современные каналы связи, в частности интернет.

В линейке приборов КОП применяются все технологии, имеющиеся сейчас на рынке, — беспроводной передачи данных, интернет-каналы, мобильные устройства для управления нашими приборами, то есть те гаджеты, которые сегодня есть в кармане практически у каждого человека.

— «СОКРАТ» всегда был коллективом единомышленников. Удивительно, эти отношения вы пронесли через годы...

— Считаю, что те отношения, которые были у нас в коллективе и 20, и десять лет назад, сохранились. Это доброжелательные, дружеские отношения, взаимопомощь, взаимовыручка в любых жизненных ситуациях. Вот это нам помогает жить и работать. Ведь работаем ради людей, и не только тех, кто пользуется нашей аппаратурой в квартирах и домах. Самое ценное — это коллектив. Благодаря совсем небольшому коллективу единомышленников в свое время мы поставили амбициозную цель и достигли ее. Сегодня наши люди — также главное богатство предприятия.

Поэтому в год 25-летия «СОКРАТА» хотелось бы пожелать нашим клиентам спокойствия, которое обеспечивает комплекс «Приток». Нашим партнерам — а их у нас более пятидесяти — почти в каждом областном центре — дальнейшего развития взаимовыгодных отношений. А коллективу предприятия хотелось бы пожелать, чтобы у них было все хорошо дома. Чтобы дети радовали. Хорошей погоды в доме, благополучия и удачи. А наше предприятие все сделает для того, чтобы обеспечить нашим работникам достойную жизнь.

Вехи истории

1999 год
Выпущен тысячный приемно-контрольный охранно-пожарный прибор ППКОП «Приток-А»

2002 год
ОБ «СОКРАТ» въехало в первый собственный офис, отреставрированный и реконструированный на средства предприятия памятник городской архитектуры – построенное еще в 1898 году каменное здание церковно-приходской школы имени Н.Л.Родионова

2005 год
ОБ «Сократ» вышло на первое место в России по обеспечению подразделений вневедомственной охраны МВД РФ (в рамках государственного заказа) оборудованием охранно-пожарной сигнализации

Высшая награда выставки «СибБезопасность-2005» (Новосибирск) — Золотая медаль

Высшая награда выставки «Охрана. Спасение. Безопасность» (Иркутск) — Золотая медаль

2008 год
Диплом и золотая медаль категории «Антикриминал-Антитеррор» в номинации «Качество, проверенное временем» самой престижной национальной отраслевой премии «За укрепление безопасности России» (ЗУБР 2008)

2009 год
Для дальнейшего совершенствования учебного процесса в ОБ «СОКРАТ» разработан и запущен в производство «Учебно-методический стенд» (УМС-1), обеспечивающий демонстрацию основных возможностей и особенностей ИС «Приток-А»

2011 год
К 350-летнему юбилею Иркутска восстановлены еще два памятника архитектуры в границах улицы Тимирязева и переулка Волконского — два деревянных дома, один из которых известен как «Дом жилой с фотосалоном» первой половины XIX века

2013 год
Охранное бюро «СОКРАТ» приняло участие в крупнейшей международной специализированной выставке «Охрана, безопасность и противопожарная защита» — MIPS-2013

Вневедомственная охрана

Наиболее мобильная и оснащенная служба

Ровно 90 лет назад — в феврале 1924 года — было принято Постановление СНК РСФСР о создании ведомственной милиции. Она создавалась для охраны имущества госпредприятий и учреждений, а также — частных организаций, имеющих государственное значение. Каковы сегодня задачи вневедомственной охраны как одной из служб МВД России? Об этом рассказывает Игорь Гвоздев, начальник отдела организационно-методического обеспечения деятельности пунктов централизованной охраны ГУВО МВД РФ.

Основными задачами вневедомственной охраны являются охрана имущества собственников на договорной основе, участие в разработке и реализации государственных мер по упорядочению и совершенствованию охраны материальных ценностей и профилактика преступлений, связанных с хищением имущества различных форм собственности, а также борьба с уличной преступностью и административными правонарушениями, оказывая помощь другим службам ОВД.

На текущий момент вневедомственная охрана является одним из наиболее мобильных, подготовленных, технически оснащенных подразделений Министерства внутренних дел. Она полностью соответствует тем задачам, которые ставит президент перед реформированной полицией — современные, вооруженные новейшими техническими средствами подразделения, нацеленные на охрану правопорядка, имущества, обеспечение безопасности граждан. Согласно социологическим опросам, доля населения, доверяющего и положительно относящегося к вневедомственной охране, является одной из наиболее высоких по органам внутренних дел.

Эффективность деятельности службы определяется, главным образом, уровнем ее технической оснащенности, развитие которой позволяет реализовать комплексную безопасность объектов любой степени сложности и не допустить совершения терактов.

Для предоставления услуг по охране объектов и квартир граждан с помощью технических средств в структуре вневедомственной охраны развернута единая сеть из 1760 пунктов централизованной охраны, то есть подразделения вневедомственной охраны функционируют в большинстве районных центров страны. В настоящее время подразделения вневедомственной охраны обеспечивают охрану 1,4 млн квартир и мест хранения личного имущества граждан (МХЛИГ) и свыше 400 тыс. объектов различных форм собственности, в том числе особой важности, повышенной опасности и жизнеобеспечения. При этом 99% всех объектов и практически 100% квартир охраняется с помощью технических средств охраны (ТСО).

Игорь Гвоздев,
начальник отдела ГУВО МВД РФ, полковник полиции

Ежегодно подразделениями вневедомственной охраны с помощью ТСО предотвращается 15-20 тысяч попыток совершения краж из охраняемых объектов и квартир, задерживаются десятки тысяч преступников и правонарушителей. Почти каждое такое задержание позволяет в дальнейшем раскрыть большее количество краж и других ранее совершенных преступлений. Помимо прямого эффекта — предотвращения преступлений — это позволяет снизить нагрузку на сотрудников ряда других подразделений ОВД, уменьшить число квалифицированных краж и преступлений против личности.

Согласно статистике, из полутора тысяч попыток краж из охраняемых объектов и квартир результативной оказывается лишь одна. Тем не менее и в таких случаях сотрудники вневедомственной охраны без промедления, по горячим следам принимают меры по розыску подозреваемых, блокируют пути их возможного отхода. Это в большинстве случаев дает возможность либо задержать преступника с украденным имуществом, иногда на значительном расстоянии от самой квартиры, либо облегчает дальнейший поиск.

Необходимо отметить, что во многих населенных пунктах в ночное время экипажи групп задержания вневедомственной охраны остаются единственными мобильными подразделениями полиции.

Непрерывно ведется работа по совершенствованию профессионального уровня сотрудников полиции, тактики действий групп задержания, обобщению опыта противодействия квалифицированным кражам. В целях организации контроля работы автотранспорта вневедомственной охраны, охраны транспортных средств физических и юридических лиц и сопровождаемых грузов продолжается внедрение систем мониторинга подвижных объектов. В большинстве подразделений, где есть такая целесообразность, развернуты ДЦ СМПО.

Во многом благодаря работе вневедомственной охраны количество краж в последние годы неуклонно снижается. Анализ статистических данных показывает, что за последние 15 лет на фоне роста количества охраняемых ОВО объектов и квартир прослеживается однозначная тенденция снижения как попыток краж

СОВРЕМЕННЫЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ ПОЗВОЛЯЮТ ОСУЩЕСТВЛЯТЬ ОХРАНУ НЕЗАВИСИМО ОТ НАЛИЧИЯ И СОСТОЯНИЯ ТЕЛЕФОННЫХ ЛИНИЙ

охраняемого имущества, так и общего количества краж. Таким образом, работа вневедомственной охраны оказала существенное положительное влияние на борьбу с имущественными преступлениями по стране в целом.

Это подтверждается опросами граждан, снижением числа попыток проникновения на охраняемые объекты в три раза и поведением самих злоумышленников (зачастую они отказываются от кражи, обнаружив, что объект под охраной ОВО). При этом надежность охраны имущества возросла в разы: в 1998 году было допущено 216 краж из охраняемых квартир, а в 2013 году — только 18.

Осуществление централизованной охраны огромного массива объектов и квартир невозможно без принятия мер по выбору, всесторонней проверке, унификации и оптимизации используемого для этих целей оборудования. Проведение единой технической политики в сфере государственной защиты имущества, в том числе путем организации технического переоснащения, компьютеризации деятельности вневедомственной охраны, является одной из основных функций ГУВО МВД России. Поэтому мы осуществляем разработку и отбор указанной аппаратуры для собственных нужд.

Конкурентоспособность службы определяют широкая номенклатура применяемой аппаратуры сигнализации, ее высокий и постоянно совершенствуемый технический уровень и качество при доступных для массового потребителя ценах.

Все технические средства, применяемые в работе вневедомственной охраны, разрабатываются при участии ФКУ НИЦ «Охрана» МВД России либо проходят техническую экспертизу на соответствие «Единым техническим требованиям к средствам безопасности, предназначенным для применения в подразделениях Вневедомственной охраны». Используемая аппаратура в большинстве своем выпускается на базе российских предприятий (как правило, бывших оборонных), имеющих высокий технологический уровень. Тем самым осуществляется и поддержка отечественного производителя. По всем используемым изделиям проведены необходимые испытания, в том числе эксплуатационные — в подразделениях вневедомственной охраны.

Кроме того, ГУВО и ФКУ НИЦ «Охрана» МВД России осуществляют постоянный контроль качества серийного производства и надзор за вносимыми схемными, конструктивными и программными изменениями, а также проводят оптимизацию по функционально-стоимостным и номенклатурным показателям. Комплекс указанных мер обеспечивает высокий технический уровень, улучшенные потребительские свойства, гарантирует качество и надежность технических средств охраны.

Необходимо отметить, что в течение последних пяти-шести лет нами сделан качественный рывок в части технического перевооружения службы. Принимая во внимание произошедшие структурные и качественные изменения в деятельности службы, достижения научно-технического прогресса, в условиях сокращения штатной численности личного состава и экономии выделяемых бюджетных средств, в целях обеспечения повышения эффективности и надежности охраны на основе анализа состояния дел в регионах ежегодно формируется и реализуется Программа технического перевооружения службы.

В результате на текущий момент мы практически полностью перешли к использованию автоматизированных систем передачи извещений, минимизировали долю аппаратуры, выработавшей срок эксплуатации и морально устаревшей, то есть представляющей угрозу надежности охраны. С автоматизированной, удобной для пользователя тактикой охраняется 95% объектов и квартир. Устаревшие системы заменяются на имеющие большую информативность, возможность работы по всем современным каналам связи, что позволяет брать под охрану большее число объектов. При этом новые системы обладают преемственностью с уже установленной аппаратурой.

Внедряемые средства сигнализации имеют защиту от квалифицированного обхода с использованием эквивалентов, имитаторов, другой специальной аппаратуры. Помимо повышения надежности охраны это позволяет нам ежегодно сокращать количество ложных срабатываний на 8-10%.

Все большее распространение при организации централизованной охраны находят радиоканальные передачи извещений. Активно поступает на вооружение вневедомственной охраны оборудование, работающее с использованием сотовой телефонии, спутниковых систем, цифровых каналов передачи информации. Их преимущество состоит в том, что они позволяют осуществлять охрану независимо от наличия и состояния телефонной связи, что особенно важно для сельских районов и пригородов.

С внедрением на АТС российских городов цифровых технологий связи ГУВО МВД России совместно с предприятиями-

1760 ПУНКТОВ — ТАКОВА В РОССИИ СЕТЬ ПОДРАЗДЕЛЕНИЙ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ

изготовителями организована модернизация эксплуатируемых систем передачи извещений, а также методическая поддержка подразделений вневедомственной охраны с целью обеспечения работы СПИ по любым каналам связи с возможностью объединения в локальные сети, обеспечив тем самым дальнейшее развитие централизованной охраны.

Используемые подразделениями вневедомственной охраны современные СПИ имеют необходимые ретрансляторы, маршрутизаторы и коммуникаторы для организации работы по цифровым каналам связи. Широко внедряются СПИ, работающие по радиоканалу, каналам GSM и Ethernet, что позволяет снизить зависимость от тарифной и модернизационной политики операторов связи. С помощью альтернативных (без использования ретрансляционного оборудования на АТС) каналов связи уже охраняется 45% объектов, 15% квартир и 78% МХИГ от общего числа охраняемых вневедомственной охраной.

Таким образом, представление о ПЦО вневедомственной охраны как об огромном помещении с бесконечным рядом железных ящиков-пультов и десятках операторов, бесконечных телефонных звонках и ложных срабатываниях безнадежно устарело.

Что касается объектового оборудования — все отечественные извещатели последних разработок серий «Фотон», «Астра», «Икар», «Шорох», «Сова» и т.д. (всего более 50 изделий) выполнены по самым передовым технологиям и на современной элементной базе. По техническим характеристикам они не уступают лучшим мировым аналогам, а по стоимостным показателям в 1,5-2 раза ниже.

При этом мы не останавливаемся в своем развитии. Сотрудниками инженерно-технической службы вневедомственной охраны постоянно совершенствуются технические средства, тактика их применения, что позволяет достойно противостоять любым ухищрениям преступников. Также проводится постоянный мониторинг тематических выставок, где представлены новинки, изучаются материалы специализированных семинаров, проводимых отечественными предприятиями-производителями и поставщиками зарубежной техники. Изучаются и новинки из сети Интернет и периодических специализированных изданий.

Международное сотрудничество, знакомство с новыми технологиями и разра-

ботками в области технических средств безопасности влияет на выбор наиболее важных направлений научной деятельности по созданию технических средств охраны, а также формирует потребности в них. Информация, полученная в результате изучения представленных средств безопасности на рынке охранных услуг, позволяет совершенствовать действующие системы безопасности и в то же время проводить разработку систем нового поколения на основе современных информационных технологий. Такого рода информация необходима для выбора оптимальной организации охраны с учетом различных потребностей заказчиков, размеров и удаленности объектов охраны, сроков монтажа и стоимости оборудования.

Внедрение современных СПИ, использование возможностей инновационных технологий позволили получить значительный экономический эффект за счет укрупнения ПЦО, автоматизации процесса охраны, сокращения количества дежурных пультов управления, снижения количества ложных срабатываний СПИ, уменьшения вероятности квалифицированного обхода аппаратуры ОПС и затрат на возмещение ущерба, сокращения расходов по оплате услуг операторов связи, сохранив при этом доступность услуг для всех слоев населения.

Принимая во внимание произошедшие структурные и качественные изменения в условиях деятельности службы, достижения научно-технического прогресса, в условиях сокращения штатной численности личного состава и экономии выделяемых бюджетных средств перед вневедомственной охраной стоят следующие задачи:

- обеспечение возможности организации охраны любых объектов и квартир за счет внедрения современных технических средств охраны, модернизации ПЦО;
- сохранение финансовой доступности услуг централизованной охраны для широких слоев населения;
- повышение квалификации инженерно-технических работников;
- обеспечение бесперебойного функционирования ПЦО;
- сохранение надежности предоставляемых охранных услуг;
- сокращение непроизводительных расходов;
- повышение оперативности реагирования подвижных нарядов полиции по сигналам тревоги из охраняемых объектов, квартир и МХИГ.

ПОД ОХРАНОЙ ПОДРАЗДЕЛЕНИЙ ВО В СТРАНЕ 1,4 МЛН КВАРТИР, МХЛИГ И СВЫШЕ 400 ТЫС. ДРУГИХ ОБЪЕКТОВ

Единая техническая политика
вневедомственной охраны в современных условиях

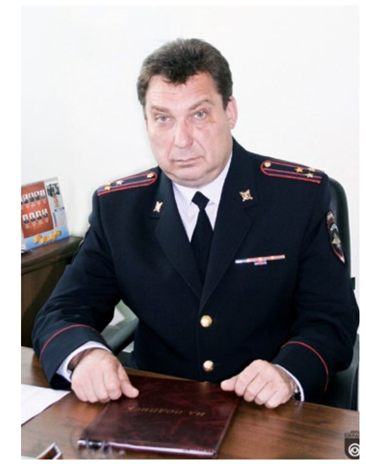
Современные условия диктуют сфере безопасности новые требования. В чем они? Об основных направлениях проведения единой технической политики мы попросили рассказать руководителя ведущей организации в области научно-методического обеспечения вневедомственной охраны — начальника Научно-исследовательского центра «Охрана» МВД России Алексея Зайцева.

Роль технических средств охраны в обеспечении личной и имущественной безопасности в современных условиях чрезвычайно высока. Это находит подтверждение и в мировой практике охранных услуг — устойчивая тенденция на усиление роли технических средств.

Тенденция эта не случайна: многочисленные исследования в области личной и имущественной безопасности показали, что широкое использование технических средств позволяет исключить либо свести к минимуму негативное влияние самого ненадежного звена в системе охраны — человека, которому присущи ограниченные физические возможности, ошибки, преднамеренные несанкционированные действия (саботаж, сговор с преступниками) и т.п.

Организация охраны с помощью технических средств значительно надежней, да и обходится она потребителю дешевле. Именно поэтому все ведущие страны, включая Россию, уделяют большое внимание созданию технических средств на основе последних научных достижений, информационных и коммуникационных технологий.

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



Алексей Зайцев,
начальник ФКУ НИЦ «Охрана» МВД России, полковник полиции

Магистральные направления деятельности

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

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

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

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

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

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

Интеграция усилий с ведущими коллективами

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

Если прежде НИЦ «Охрана» осуществлял разработку приборов самостоятельно, без привлечения сторонних организаций, то с образованием и развитием новых коллективов, которые стали занимать ведущее положение на рынке технических средств безопасности, появилась реальная возможность интеграции усилий. Это позволило существенно расширить фронт работ по созданию ап-

паратуры, повысить технический уровень разработок, сократить время на подготовку их серийного производства, что в конечном итоге дало возможность ежегодно пополнять арсенал вневедомственной охраны 12-15 новыми изделиями, а не тремя-четырьмя, как было при прежнем подходе.

Сегодня тесное взаимодействие по созданию новых ТСО осуществляется более чем с 30 предприятиями-изготовителями Москвы, Санкт-Петербурга, Казани, Рязани, Иркутска и других промышленных центров страны, а также Московской и Челябинской областей. Ежегодный объем выпуска составляет более ста тысяч единиц продукции, что обеспечивает устойчивую производственную загрузку десяткам и сотням рабочих мест российских предприятий. Причем в этих творческих альянсах НИЦ «Охрана» выполняет функции идеолога, головного разработчика, который определяет ключевые технические характеристики нового изделия, тактику применения и другие жизненно важные показатели.

Для повышения результативности групп задержания

Остановлюсь более подробно на задачах, решаемых НИЦ «Охрана» в рамках каждого из направлений своей деятельности.

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

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

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

На выставке «Интерполитех».
Справа — Алексей Зайцев, в центре министр внутренних дел России Владимир Колокольцев

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

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

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

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

Охрана объектов по альтернативным каналам

В продолжение данной темы, с учетом развития высокоскоростных каналов связи, в 2014 году нами организовано проведение работ по созданию устройств объектовых оконечных, обладающих способностью формирования и передачи с охраняемого объекта на пульт централизованного наблюдения (ПЦН) аудио- и видеоинформации. Это значительно повысит эффективность реагирования дежурных нарядов на сигналы тревоги с охраняемых объектов, обеспечит более высокую надежность их охраны.

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

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

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

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

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

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

Пилотная зона с цифровыми каналами

В столичном регионе, где массовое переключение абонентов запланировано на самое ближайшее время, организована пилотная зона для детальной проработки вариантов организации централизованной охраны с использованием различных цифровых каналов передачи информации с объекта непосредственно на ПЦО с учетом обеспечения требуемого уровня надежности охраны. А именно – использование в качестве каналов передачи данных:

- построенной для нужд охраны VPN-сети, арендуемой у поставщика услуг связи;
- собственной корпоративной VPN-сети, построенной за счет средств охраны;
- открытых каналов сети INTERNET.

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

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

На выставке «Интерполитех».
С главой ГУВО МВД России генерал-майором полиции Сергеем Лебедевым (слева)

Принцип совместимости со старым оборудованием

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

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

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

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

Отсюда следует, что вновь вводимые в эксплуатацию СПИ должны обеспечивать возможность плавного и поэтапного внедрения с обеспечением поддержки как старого ретрансляционного оборудования (для СПИ, не выработавших установленных сроков службы «Фобос», «Фобос-А», «Фобос-ТР», «Фобос-3»), так и с обеспечением поддержки старого объектового оборудования со стороны новых ретрансляторов (поскольку замена объектового оборудования требует значительного времени, в том числе на работу с клиентами, которых необходимо будет убеждать на приобретение новой техники).

Для этих целей в ОБ «СОКРАТ» был внедрен в эксплуатацию комплект модернизации ретрансляторов «Фобос». Он позволяет модернизировать существующие ретрансляторы СПИ «Фобос-3», исключив расходы на демонтаж, монтаж нового

оборудования, смену кабельных подключений и т. п. Обновленный ретранслятор обеспечивает поддержку уже подключенных УО и позволяет подключать новые, современные приборы охраны.

Без проводов

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

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

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

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

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

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

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

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

Дальнейшее развитие подсистем охраны

Теперь что касается дальнейшего развития объектовых подсистем охраны.

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

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

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

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

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

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

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

Охранное телевидение

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

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

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

В развитие данной темы в текущем году проводятся работы по исследованию возможности создания комплекса технических средств для охраны банкоматов и платежных терминалов от преступных посягательств. Создаваемый комплекс будет включать в себя необходимый набор охранных извещателей, системы передачи извещений по различным каналам связи, технические средства и системы отслеживания текущего местоположения банкоматов с передачей информации на ПЦО и экипажам группы немедленного реагирования, средства активного противодействия преступным посягательствам на банкоматы.

Полноценная поддержка внедрения и эксплуатации

Перехожу к рассмотрению **второго магистрального направления** — организационно-техническое и методологическое обеспечение подразделений вневедомственной охраны в работах по внедрению и эксплуатации технических средств.

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

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

В связи с этим работа по данному направлению в последние годы значительно активизировалась. В частности, в три раза увеличено число работ по созданию нормативно-технических документов. В 2012 году НИЦ «Охрана» подготовлено и направлено в подразделения 11, а в текущем году разрабатывается 12 методических рекомендаций и пособий.

Качественно изменился и состав рассматриваемых вопросов, которые относятся не только к выбору и применению технических средств, как было прежде, но и в большой степени затрагивают различные каждодневные организационные стороны деятельности подразделений. Так, по результатам работ этого года будут подготовлены документы, регламентирующие порядок обследования объектов, принимаемых под охрану, их инженерно-техническую укрепленность, технический надзор за выполнением проектных, монтажных и пусконаладочных работ, проведение входного контроля СЦН и ряд других.

Работа над системой национальной стандартизации

Говоря о направлении методологического обеспечения вневедомственной охраны, нельзя не остановиться на работе НИЦ «Охрана» в рамках Технического комитета по стандартизации ТК 234 «Системы тревожной сигнализации и противокриминальной защиты» Фе-

Александр Демин, начальник сектора НИЦ «Охрана», у стенда ИС «Приток-А»

ШИРОКОЕ ИСПОЛЬЗОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ПОЗВОЛЯЕТ ИСКЛЮЧИТЬ ЛИБО СВЕСТИ К МИНИМУМУ НЕГАТИВНОЕ ВЛИЯНИЕ САМОГО НЕНАДЕЖНОГО ЗВЕНА В СИСТЕМЕ ОХРАНЫ — ЧЕЛОВЕКА

Основные цели НИЦ «Охрана»

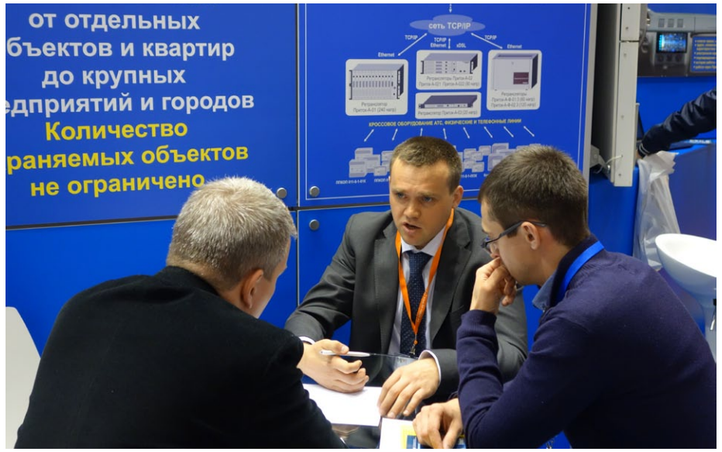
по практической реализации единой технической политики вневедомственной охраны, проводимой ГУВО МВД России

1. Своевременное техническое перевооружение подразделений вневедомственной охраны

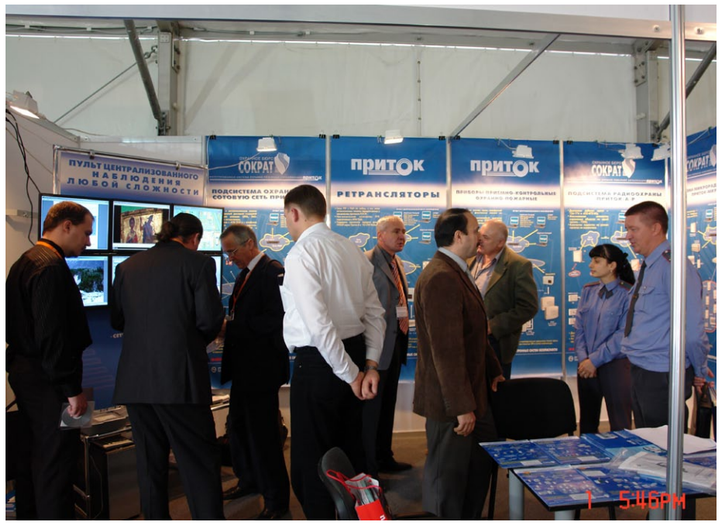
2. Поддержка российского производителя охранной техники

3. Снижение стоимости охраны за счет применения более дешевых, но не уступающих импортным по тактико-техническим характеристикам и адаптированных к российским условиям отечественных средств охраны, которые созданы с учетом внедрения новых информационных и телекоммуникационных технологий

4. Научно-методологическое обеспечение специалистов данной службы



Иван Илюшин во время выставки MIPS 2014 рассказывает о последних разработках ОБ «Сократ»



На стенде ОБ «Сократ» в ходе специализированной выставки в Сочи

дерального агентства по техническому регулированию и метрологии.

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

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

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

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

Объективно оценивая такое положение дел, только за последние два года на основе Программы национальной стандартизации Российской Федерации НИЦ «Охрана» в рамках ТК 234 разработаны и утверждены Росстандартом пять национальных стандартов. В текущем году будут разработаны и переработаны еще пять стандартов, а также продолжена работа в составе рабочих групп в разработке проектов девяти международных стандартов МЭК.

В заключение хочу отметить, что успешной реализации указанных приоритетных направлений научно-исследовательской деятельности НИЦ «Охрана» способствуют, с одной стороны, наше тесное взаимодействие с ГУВО МВД России, как с основным заказчиком научно-технической продукции, а с другой — постоянная обратная связь с подразделениями на этапах испытаний и освоения новой техники, при подготовке нормативно-технических документов. Это позволяет не только концентрировать усилия на решении насущных проблем, стоящих перед службой вневедомственной охраны, но и закладывать прочный фундамент совместной работы на перспективу.

Некоторые вопросы защищенности
цифровых сетей ОВО

Благодаря технологиям средств связи все более доступными для широких масс населения становятся общественные цифровые сети. Поэтому для отделов вневедомственной охраны все актуальнее использование каналов связи, основанных на цифровых технологиях.

На практике в ОВО цифровые каналы используются с конца прошлого тысячелетия. Дальнейшее развитие интернета и GSM, их надежности и плотности проникновения в массы позволяет использовать их для целей централизованной охраны более широко и интенсивно. Интернет дает импульс для развития пультов вневедомственной охраны без привязки к монополии ОАО «Ростелеком», без аренды линий одного из провайдеров и, соответственно, без установки аппаратуры на АТС. А также предоставляет возможность использовать сеть любого интернет-провайдера и возможность его смены. Идеальное решение — это VPN-сеть от ПЦН до каждого объекта, но, как правило, это невозможно. Поэтому дальнейшее использование общественных цифровых сетей для ОВО — это объективный процесс, и без него не обойтись.

На основании накопленного опыта работы и чтобы избежать типовых ошибок, в этой статье попробуем разобрать некоторые вопросы, возникающие при использовании общественных сетей, и меры по защите информации в сетях ОВО. Это не готовые решения, а наши рекомендации и предмет для дальнейшего обсуждения.

Павел Воробьев,
начальник отдела
НИиОКР ОБ «СОКРАТ»

Внешние подключения

1. Правила подключения к сети Интернет

Итак, для целей охраны пульт ОВО необходимо подключить к сети Интернет и (или) к VPN сети любого провайдера. Но любая VPN- сеть — это «привязка» к конкретному поставщику услуг. Надо учесть, что сменить VPN-сеть у клиента, как правило, очень не просто. Выход же в интернет — это возможность легко сменить при необходимости одного провайдера на другого.

Таким образом, все чаще получается, что проще подключиться к интернету как со стороны пульта (ПЦН), так и со стороны объекта, чем пытаться установить прямое VPN соединение «Пульт — Объект».

При подключении как ПЦН, так и объекта сразу встает вопрос о безопасности и сохранности данных. Здесь мы не предлагаем ничего нового, а следуем распространенным на сегодняшний день решениям, наиболее часто встречающимся в интернете для этой задачи. А именно — подключение ПЦН к интернету должно осуществляться через маршрутизатор, в котором используется NAT-проброс одного порта на один компьютер, все остальные связи запрещаются. Мы пока считаем, что этого достаточно для обеспечения безопасного подключения сети ПЦН к интернету. Такое подключение исключает свободный доступ в Интернет любого компьютера сети ПЦО, и «Одноклассников» на рабочем месте оператора мы не увидим.

Вывод. Маршрутизатор с NAT-пробросом обязателен для каждой точки подключения ПЦН к внешней (любой) сети.

Примечание из wikipedia.org. Преобразование адреса методом NAT может производиться любым маршрутизатором, сервером доступа, межсетевым экраном, суть механизма которого состоит в замене адреса источника (англ. source) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. destination) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

2. Правила подключения к любому провайдеру любых цифровых сетей Как мы уже выяснили в предыдущем пункте, факт подключения ПЦН к интернету дает в первую очередь его независимость от одной (пусть и хорошей) организации — ОАО «Ростелеком». Но это ни в коем случае не отменяет взаимовыгодного сотрудничества с любым поставщиком услуг цифровой передачи данных, VPN-сетей и прочих сервисов, позволяющих получить в итоге связь «Пульт — Объект».

Считаем, что и в этом случае для подключения к любой сети любого провайдера достаточно и необходимо использование маршрутизатора с NAT-пробросом одного порта на один компьютер. Все остальные связи отключаются в настройках маршрутизатора.

Вывод. Решение — маршрутизатор с NAT-пробросом для каждой точки подключения — на сегодня подходит почти для всех подключений сети ПЦН к другим сетям.

3. При подключении к чужой цифровой сети всегда устанавливаем «свой» маршрутизатор, независимо от организации чужой сети. Таким образом, подключаем ПЦН к любой сети через маршрутизатор (роутер) с использованием NAT-проброса. Это позволит:

- защитить свою сеть;
- единообразно подключать другие сети.

Вывод. Независимо, есть или нет внятная политика безопасности в чужой сети, ВСЕГДА ставим «свой» маршрутизатор на входе.

4. Выбор маршрутизатора

На сегодня на рынке более 70 различных производителей маршрутизаторов. Поскольку тираж этих маршрутизаторов огромен, есть и отзывы в интернете об их работоспособности. Поэтому стараемся максимально учитывать чужой опыт и использовать маршрутизаторы среднего ценового диапазона, например, фирмы «MikroTik» (маршрутизаторы 751 и 951 серии -RB751G-2HnD или

RB951G-2HnD, более новые маршрутизаторы RB2011). За время использования нескольких сотен маршрутизаторов этой фирмы в различных регионах России зависаний либо отказов пока зафиксировано не было, в отличие от маршрутизаторов D-Link низшего ценового диапазона.

5. Резервирование каналов связи со стороны ПЦН

В вопросе надежности любого подключения исходим из того, что каждое подключение может быть выведено из строя по разным причинам, например с помощью DoS-атаки. Поэтому организуем основной, резервный и аварийный каналы связи для подключения ПЦН к интернету. Считаем, что сам интернет сломать невозможно, но возможно «вырубить» одного из провайдеров. Именно из этих соображений обеспечиваем несколько подключений к интернету через разных провайдеров. И к каждому из них строим маршрутизатор с NAT-пробросом и отдельный компьютер с установленным сервером подключений для обеспечения полностью независимого канала связи для каждого выхода с ПЦН в интернет.

Вывод. Резервирование канала связи со стороны ПЦН — важный момент, и им нельзя пренебрегать. Со стороны ПЦН желательно иметь основной, запасной и резервный каналы связи. И на каждый из них свой маршрутизатор.

6. На всех маршрутизаторах ставим хороший пароль

Любой маршрутизатор имеет имя и пароль доступа к своим собственным настройкам. Так, например, маршрутизаторы (роутеры) D-Link имеют по умолчанию имя «admin» и пароль «пустой». Поэтому для обеспечения безопасности необходимо установить новую пару значений, известную только администратору. Для обеспечения взломостойкости необходимо устанавливать «длинные» имена и пароли (не менее 15 символов), состоящие из букв и цифр.

7. Правила выбора имен и паролей

Категорически запрещено использовать имя и пароль типа: «123456», «qwerty», «йцукен», «password» и тому подобное.

Вывод. Правила выбора пароля относятся не только к маршрутизаторам, но и к любым программам и системам, требующим ввода пароля.

8. Обеспечение безопасности электроснабжения

Одним из важных аспектов надежной работы любой системы является ее бесперебойное функционирование в условиях аварии электроснабжения. Имеет смысл внимательно проверять (не реже чем один раз в год) резервирование питания всех используемых компьютеров, хабов, маршрутизаторов.

Еще лучше, когда и провайдеры интернета также имеют у себя резервные источники питания, обеспечивающие бесперебойную связь даже при «авариях 220В». К сожалению, используемые на сегодня в резервных источниках питания аккумуляторы имеют срок годности не более одного года. В связи с этим важно их проверять и планово менять. Понятно, что такое техническое обслуживание требует финансов, но при ЧП на электросетях и по другим причинам «авария 220В» может очень больно ударить по работе ПЦН.

Вывод. Внимательно проверяем резервное питание ПЦН, всех хабов, модемов, свичей и маршрутизаторов. Ежегодно тестируем источник питания UPS и проверяем автономный генератор. При разумном подходе к тестированию всех резервных источников питания опираемся на следующее.

1. На каждом резервном источнике питания имеем табличку с датой о последней проверке с указанием времени «работы под полной нагрузкой без 220В».

2. Используем все факты «реальных аварийных отключений 220В» для изме-рения времени штатной работы резервных источников питания с выявлением «слабого звена».

3. При стабильном электроснабжении не реже чем один раз в год снимаем с эксплуатации для проверки каждый резервный источник питания и проводим тестирование под полной нагрузкой, не подвергая при этом риску аварийного выключения серверы и компьютеры ПЦН.

9. Обеспечение защиты от «вторжения»

Поскольку на сегодня локальная сеть ПЦН либо с помощь модемов, либо другими способами выходит за пределы ПЦН, то необходимо внимательно учитывать свободные розетки в хабах, маршрутизаторах и модемах, расположенных как на территории ПЦН, так и на внешних участках сети.

Как правило, эти Ethernet-розетки расположены в служебных помещениях, и доступ к ним ограничен. Тем не менее должны быть приняты меры, исключающие возможность «нелегального» подключения через них к сети ПЦН. Как правило, с провайдерами имеется договор, в котором явно указаны все точки подключения, но зачастую в дальнейшем используются хабы и свичи. Если оставить их беспризорными, то возможно «вторжение».

Вывод. По всей сети выявляем свободные точки подключения (Ethernetr незда на хабах, свичах, модемах). Ограничиваем к ним доступ административно либо опечатываем, либо запираем в шкаф.

10. Не объединять без необходимо- сти охранную сеть с другими сетями

Любое объединение любых сетей — это повышение риска потерять данные. Даже если используется маршрутизатор, в котором приходится хоть что-нибудь да разрешать. В данном случае возможен «нежелательный» сетевой трафик, от которого избавиться будет очень сложно. До сих пор не решена проблема установки легальной (обновляемой не реже чем раз в неделю) антивирусной программы на каждый компьютер. Особенно если этот компьютер находится в другой сети и доступ к нему невозможен.

Вывод. Не объединять без необходимости охранную сеть ни с чем.

Внутренние подключения

В современных условиях основа данных ПЦН (БД) находится в компьютерной информационной базе, и ее потеря может привести к непоправимым последствиям. Особенно неприятно, если БД будет скопирована, выложена в интернет и использована в незаконных целях. На сегодня пока не зарегистрировано ни одного подобного случая. Следовательно, этому вопросу руководством уделяется должное внимание.

Вывод. Потеря базы данных либо «слив» наружу ее копии равносильны потере знамени полка. За базой следим всеми силами.

1. Как известно, много вирусов распространяется через флешки и другие внешние носители. Поэтому, по возможности, на всех рабочих станциях блокируем или физически отключаем все внешние USB-носители, дискеты, лазерные диски. Это существенно сократит число попаданий вирусов на ПЦН.

2. Известно, что наличие открытых портов для таких протоколов, как Telnet, http и других, может помочь администрировать сеть. Тем не менее рекомендуем их отключать, пусть и в ущерб удобству. Сам факт наличия открытого порта дает возможность нагрузить трафик сети бесконечными запросами, даже если по этому порту не поднята никакая управляющая программа.

Вывод. Запрещаем все (!!!) протоколы типа Telnet, http и других, кроме необходимых для работы.

3. Из интернета можно скачать много различных сканирующих сеть программ. Более того, эти программы с неизвестными функциями могут быть уже установлены на ПЦН. Имеет смысл разобраться, что это за

программы и для чего предназначены, и ни в коем случае не использовать программы «чужого» производителя.

Вывод. Исключаем работу программ, функции которых нам не известны, особенно сетевых сканирующих.

4. Так же, как и во внешней сети, выявляем свободные точки подключения к внутренней сети ПЦН (Ethernet-гнезда на хабах, свичах, модемах) как по внешнему периметру, так и по внутреннему и ограничиваем к ним доступ административно. Еще лучше не иметь ни одной свободной Ethernet-розетки. При необходимости организовать дополнительное или временное рабочее место — разворачиваем свич, работаем и после работы убираем в сейф.

Вывод. Бесхозная Ethernet-розетка — находка для недоброжелателя. Не надо делать таких подарков. Неизвестно, кто, как и зачем может подключиться к сети.

5. Сервер — это сердце ПЦН. От бес- перебойной работы данного узла зависит работа всего ПЦН. Каждый визит в серверную должен быть только под при- смотром администратора. Помните, что любое необдуманное действие может нарушить работоспособность ПЦН и вы- звать огромное количество различных незапланированных работ. Если произ- водитель системы имеет возможность снабжать подразделения ОВО свежими версиями программного обеспечения (ПО), то обязательно его обновлять не реже, чем один раз в год. Это поможет избежать тех ошибок и трудностей, которые были выявлены и исправлены за это время в других подразделениях.

Вывод. Административно контролируем доступ к серверу. При наличии обновления программного обеспечения обновляем ПО не реже чем раз в год.

6. Работа без установленного антивируса либо (что еще хуже) с антивирусом, но по законченной лицензии приводит к тому, что компьютер начинает «захлебываться» вирусами. Существует риск полной потери данных только из-за вирусов. В локальной сети такой компьютер может быть источником огромного Ethernet-трафика. Все это может отвлекать и мешать работе.

Вывод. На всех работающих станциях устанавливаем свежий антивирус и обновляем антивирусные базы не реже чем один раз в месяц. При этом важно иметь действующую лицензию. На сегодня мы рекомендуем антивирус Касперского. Поскольку данный ресурс платный, необходимо ежегодно приобретать лицензию на его использование.

7. Несмотря на то что мы подключаем пульт к интернету для целей охраны, а именно один порт на одном сервере, для всех остальных компьютеров сети мы этот выход запрещаем, не оставляя возможности запуска никаких сервисов современного общения, включая e-mail, Skype и различные социальные сети. Это существенно сократит необходимость борьбы с вирусами и другими неприятностями.

Вывод. На всех рабочих станциях ПЦН исключаем возможность любого выхода в интернет.

8. Проводим ежеквартальный ин- структаж со всеми сотрудниками, особенно — с имеющими доступ к базе данных.

Нельзя:

- копировать файлы на личные носители (их можно потерять);
- копировать файлы на телефоны и ноутбуки (их можно потерять);
- допускать видеть экран сотрудников ОВО посетителям;
- допускать за служебные компьютеры детей и родственников.

Надо:

- физически утилизировать вышедшие из строя носители;
- хранить копии базы на сервере не менее чем на трех разных дисках;
- по возможности использовать технологию «зеркального» включения дисков.

9. Ежемесячно анализируем детализацию от интернет-провайдера по всем подключениям относительно: • размера входного/выходного трафика; • адресов обращений. В случае обнаружения подозрительной активности просим провайдера блокировать доступ по указанному адресу. Это даст возможность превентивной блокировки потенциально опасных ресурсов.

10. Проводим беседу с увольняющимися сотрудниками (появление вероятных Сноуденов никто не отменял).

11. Физически выключаем или блокируем доступ приборов от клиентов, расторгнувших договор на охрану. По факту расторжения договора на охрану при использовании VPN-сети необходимо принять меры для отключения этого абонента не только от услуг охраны, но и от возможности входа в саму среду передачи данных. Самое правильное — запретить в явном виде доступ для этого абонента к невостребованному ресурсу.

12. Настойчиво говорить и добиваться финансирования защищающих и развивающих цифровую сеть ПЦН программ и работ.

От автора. Надеюсь на ваши отзывы, предложения, а также жду вопросов: wp@sokrat.ru

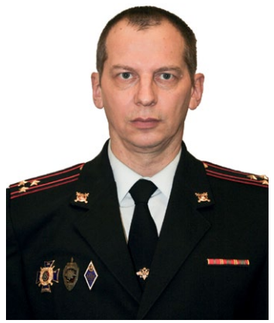
Защита локальных вычислительных сетей

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 неподготовленными к изменившейся ситуации. Во многих случаях пользователи корпоративных сетей даже не подозревают о том, что их данные неожиданно оказались доступны любому пользователю Интернет.



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

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, 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.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ЛВС ПЦО и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), ошибочно введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к 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 возможные 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;

Алексей Смирнов,
начальник сектора обучения
ОБ «Сократ»

- 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, 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

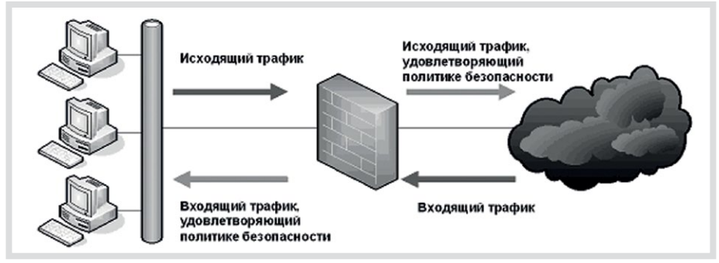


Рис. 1. Контроль периметра сети МЭ (защищаемая сеть слева)

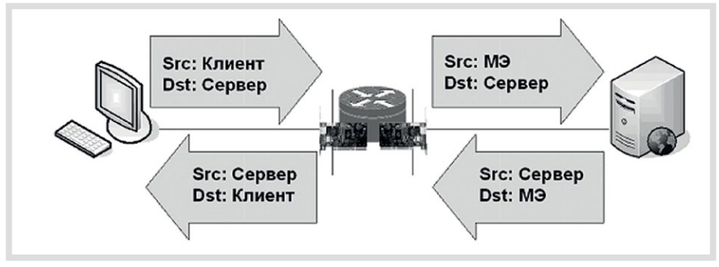


Рис. 2. Технология NAT

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 (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 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 недостатком 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 Интернет.

Рис. 3. Маршрутизатор Mikrotik RB/MRTG

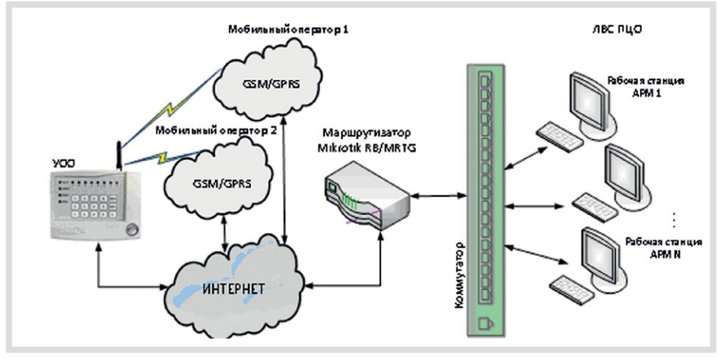


Рис. 4. Типовая схема включения для малого количества охраняемых объектов

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, внесённых в «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, внесённых 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 её 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/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-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 Microtic 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. 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 Интернета 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 четвёртый 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 эксплуатации 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

Настройка 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**;

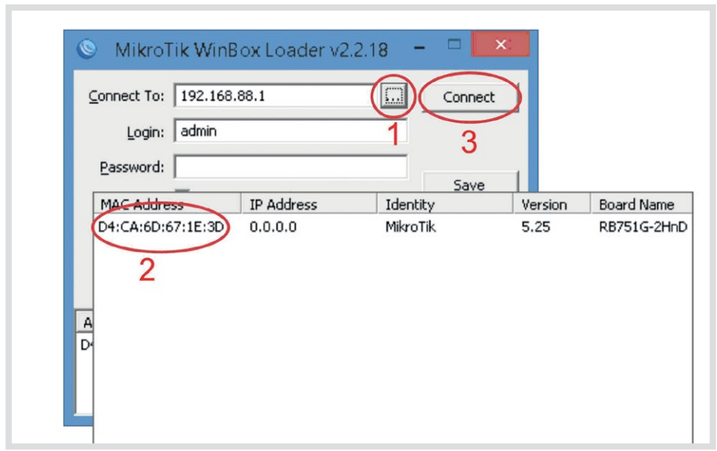


Рис. 5. Подключение к роутеру.

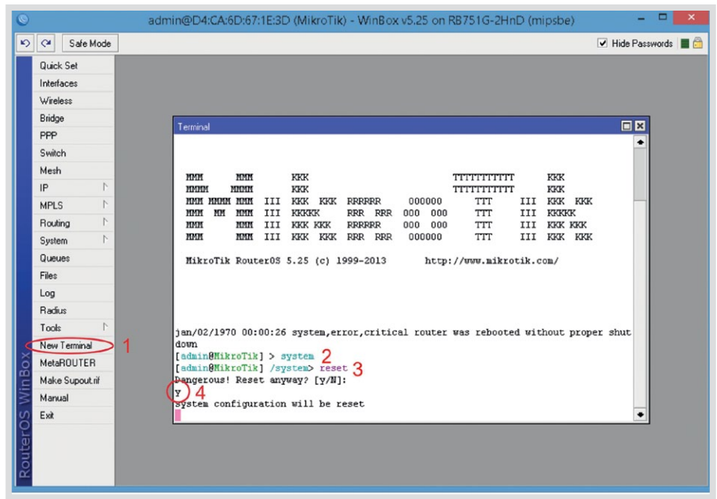


Рис. 6. Сброс настроек.

3. Потом вводим команду **reset**;
4. Нажимаем кнопку у 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 *(рис. 7)*.

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 ещё 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):

1. Открываем меню **Interfaces** *(рис. 8)*;
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».

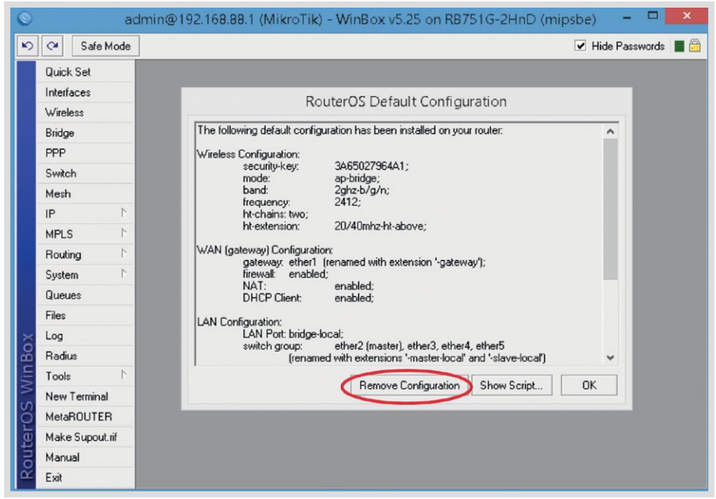


Рис. 7. Перезагрузка роутера.

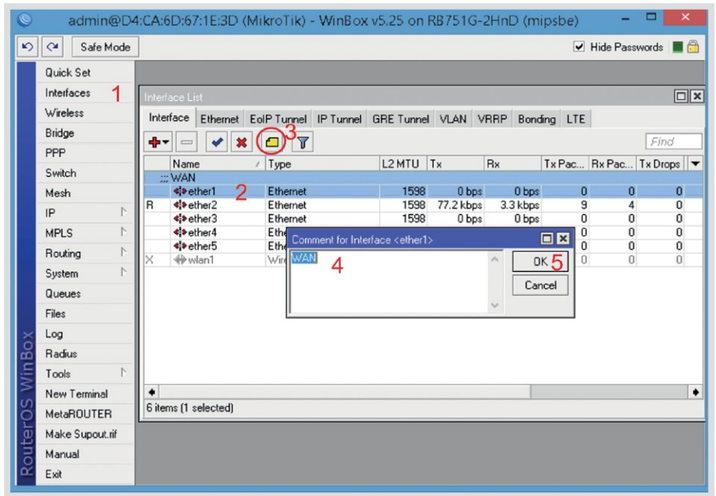


Рис. 8. Сетевые интерфейсы.

Настройка WAN интерфейса

Если провайдер предоставляет Интернет с привязкой по MAC, то произведём 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. 9)*;
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**.

Настоим адрес Интернет шлюза:

1. Открываем меню **IP** *(рис. 10)*;
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. 11)*;
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. 12)*;
2. В появившемся окне нажимаем Add (красный плюс) выбираем из списка **PPPoE client**;
3. На вкладке **General** даём 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. 13)*;
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 выбираем интерфейс **ether2**;
6. Нажимаем кнопку **OK**.

Чтобы изменить пароль доступа к роутеру, выполните следующие действия:

1. Открываем меню **System** *(рис. 14)*;
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. 15)*;
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. 16)*;
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. 17)*;
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**.

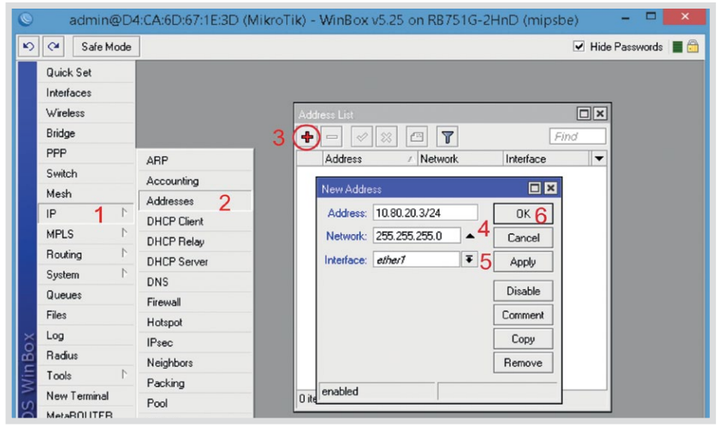


Рис. 9. Статический IP адрес и маска подсети WAN порта.

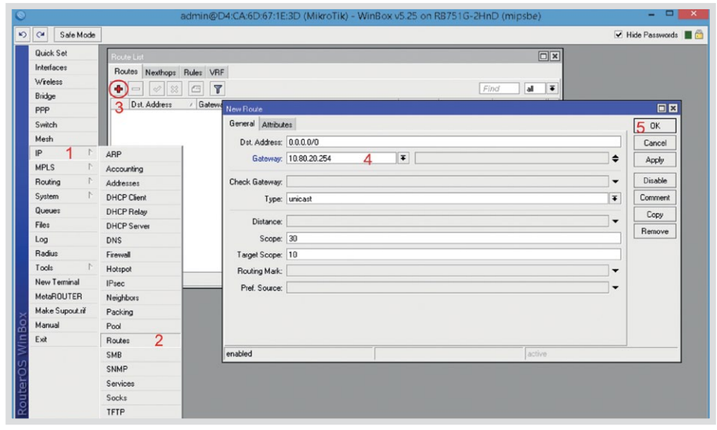


Рис. 10. Адрес Интернет шлюза.

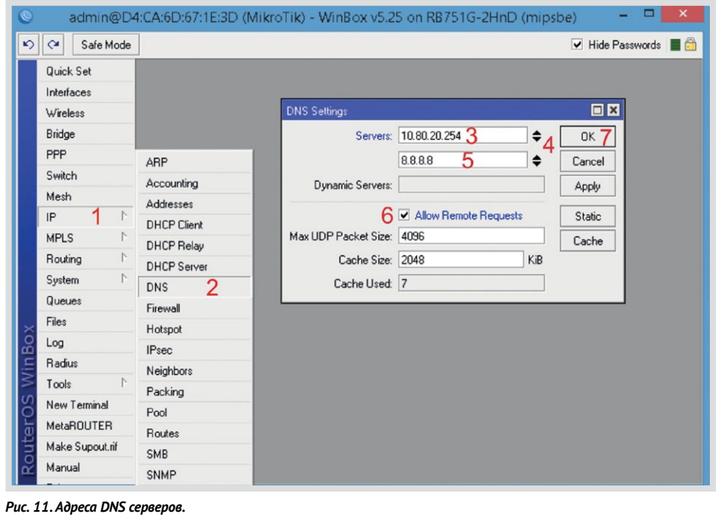


Рис. 11. Адреса DNS серверов.

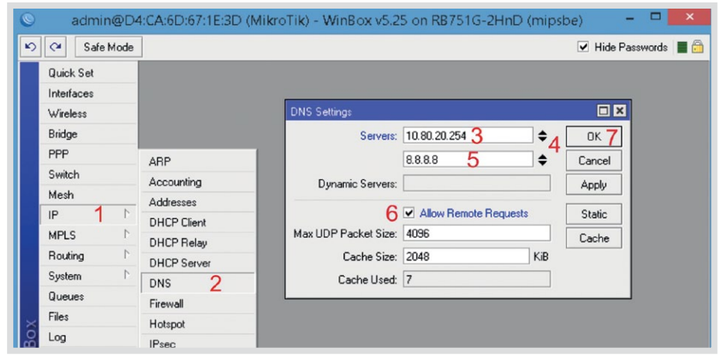


Рис. 12. Подключение через PPPoE.

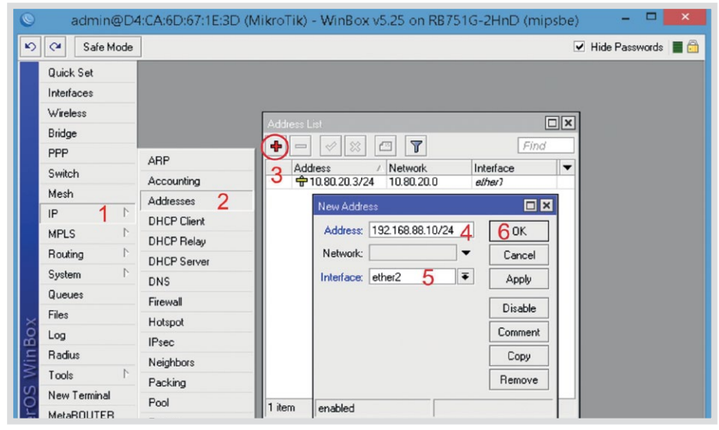


Рис. 13. IP адрес локальной сети.

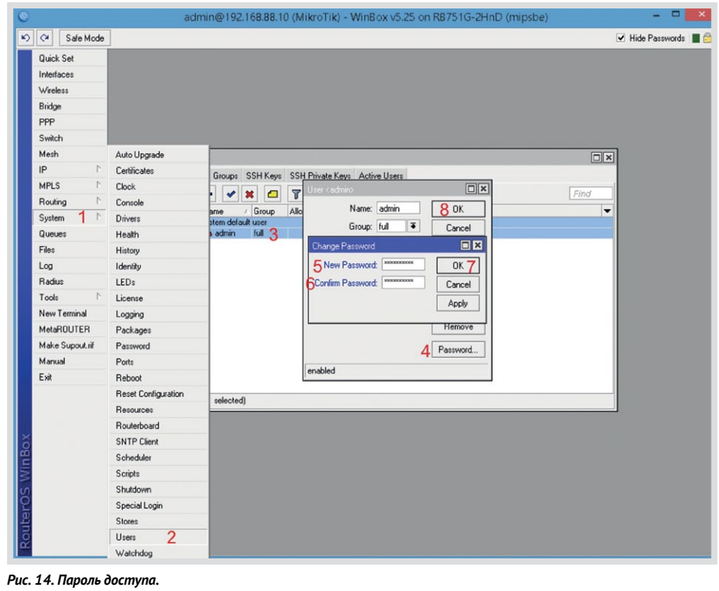


Рис. 14. Пароль доступа.

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. Задаём 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. Создаём 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. Создаём ДВА правила — для двух портов для входящего трафика. И так же создаём ДВЕ цепочки, маркируя трафик соответственно нашим меткам. В итоге у нас получилось **4 правила** — 2 для маркировки соединений и 2 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 определённые 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-po-nastrojke-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.

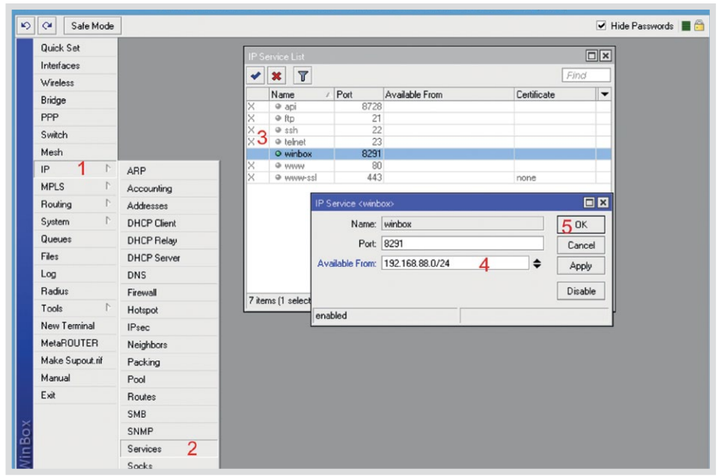


Рис. 15. Отключение ненужных сервисов.

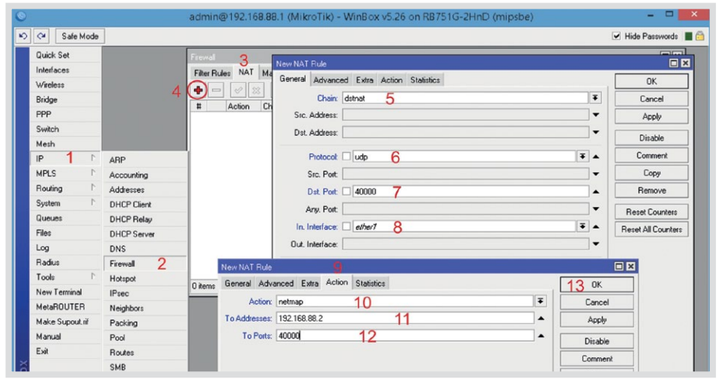


Рис. 16. Проброс портов.

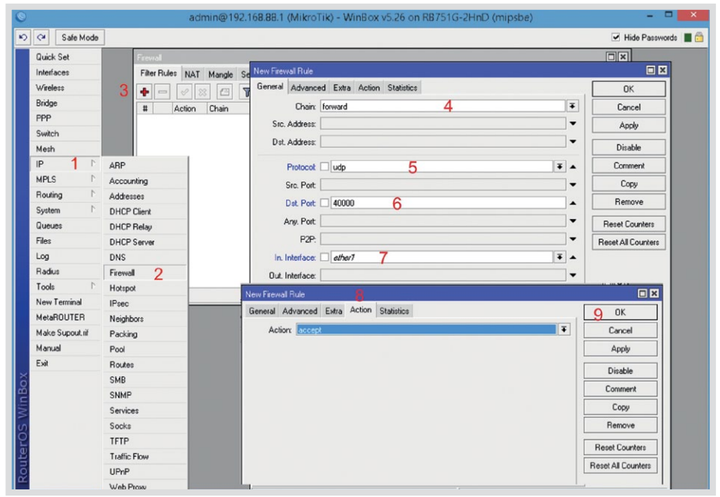


Рис. 17. Правила файрвола.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

2. Указ Президента РФ № 351 от 17 марта 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»).

Пульты централизованного наблюдения (ПЦН)
на основе Интегрированной системы охранно-пожарной сигнализации Приток-А

ИС ОПС Приток-А

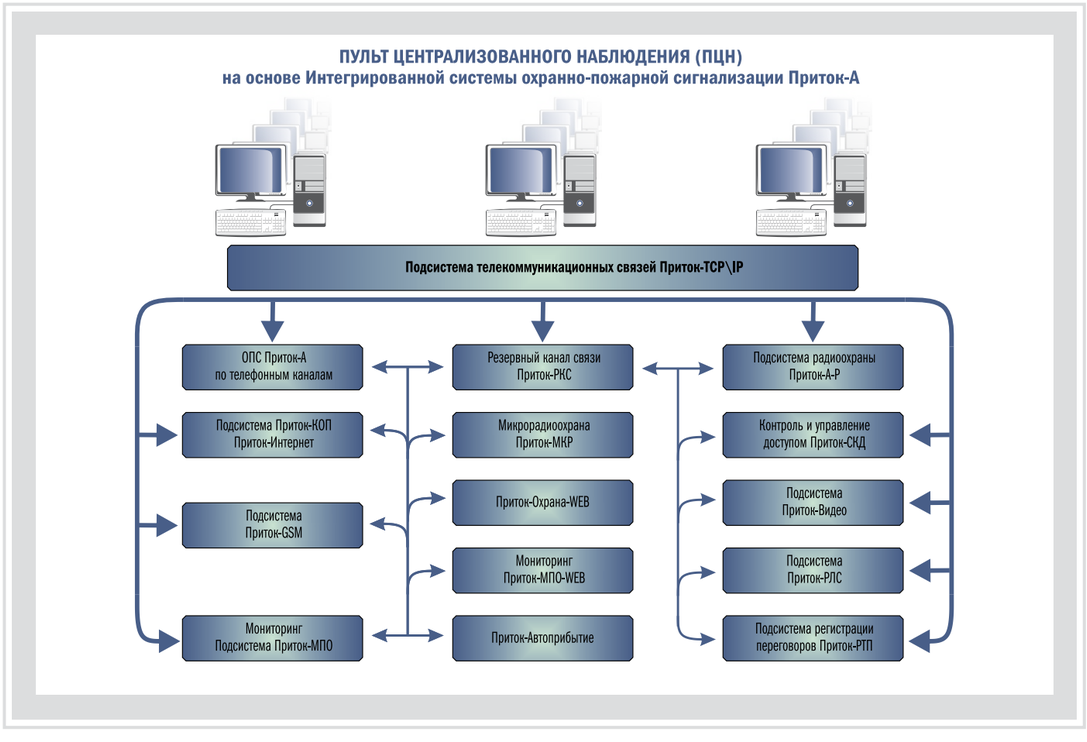
Интегрированная система охранно-пожарной сигнализации Приток-А (в дальнейшем просто — система ИС Приток-А), созданная иркутскими специалистами, в настоящее время успешно функционирует в более чем 50 регионах России, а также в Казахстане и Узбекистане.

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 10мВт, 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 основе 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

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-04 или приборы серии Приток-А-КОП. Для обеспечения доступа в сеть Интернет охранного оборудования и совместного использования одного канала связи на объекте, например пользователями веб-ресурсов, устанавливается маршрутизатор «бытового» уровня — 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 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.

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

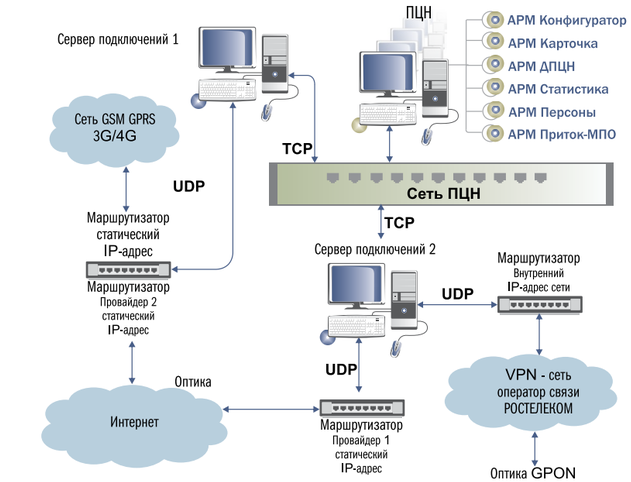
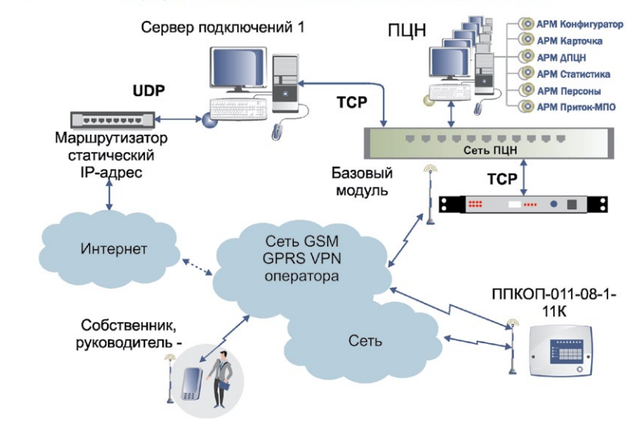


Рис. 3 Структурная схема сети ПЦН ИС Приток-А для работы через GSM сеть



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

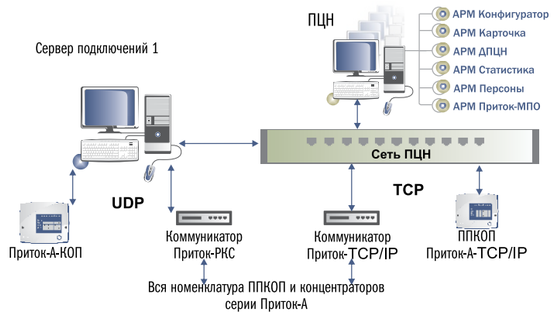


Рис. 5 Структура сети ПЦН с использованием телефонных каналов связи

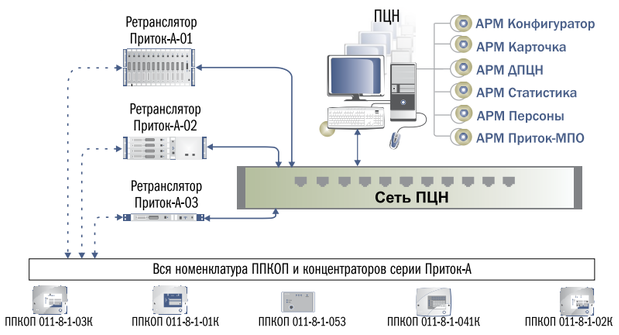
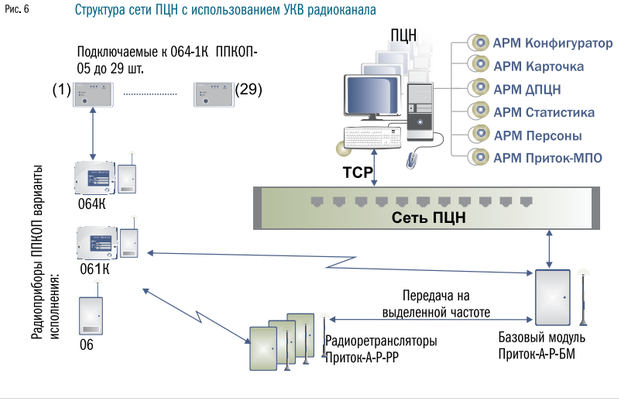


Рис. 6 Структура сети ПЦН с использованием УКВ радиоканала



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 рабочую станцию устанавливается соответствующее программное обеспечение АРМ

Рис. 7 ПЦН с применением безлицензионного диапазона радиочастот

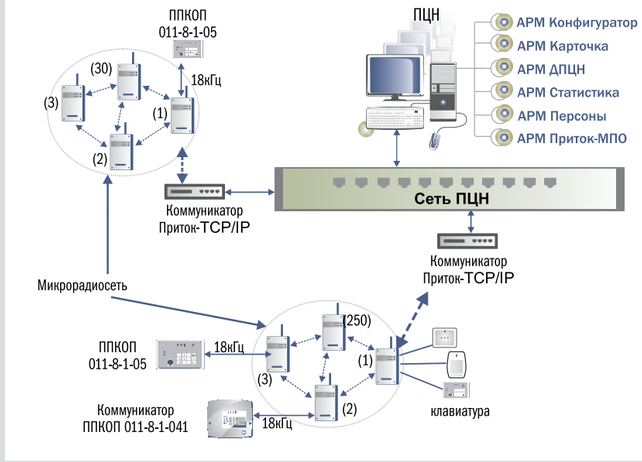
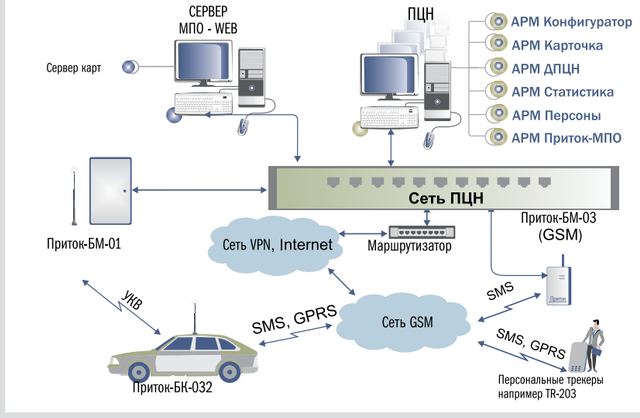


Рис. 8 Подсистема мониторинга и охраны подвижных объектов Приток-МПО



Приток-МПО и необходимые электронные карты.

Рабочая станция позволяет:

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

Для контроля за перемещением и для охраны граждан система Приток-МПО обеспечивает работу с персональными GSM/SMS/GPRS GPS трекерами. При работе с трекерами обеспечиваются функции отображения текущего местоположения, охраны трекера – обработка нажатия на тревожную кнопку SOS, привязки трекера к 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. 11). 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

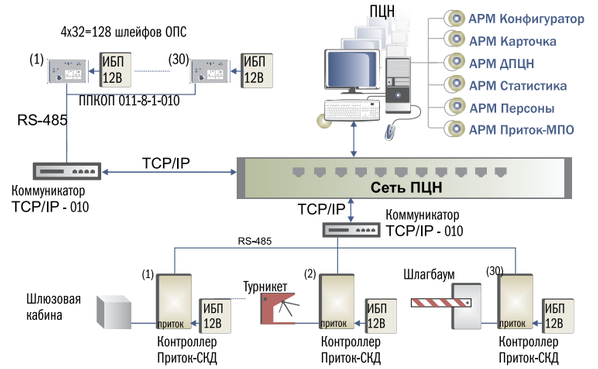


Рис. 10 ПЦН Приток-Видео с применением аналоговых и IP-видеокамер

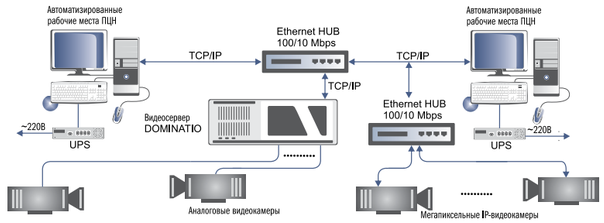
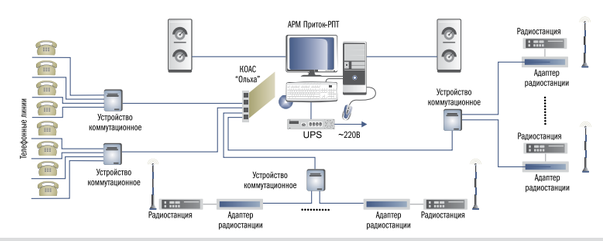


Рис. 11

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 календарного года нами проводились работы по подготовке к выпуску новой версии программного обеспечения. Сегодня для всех пользователей, эксплуатирующих ИС ОПС Приток-А, доступна версия 3.7.0.

Основной целью выпуска новой версии являлось желание разработчиков не просто исправить ошибки и увеличить производительность, а разработать новые автоматические и полуавтоматические функции системы, которые бы реально смогли облегчить работу операторов охраны, позволили бы повысить качество работы персонала, максимально автоматизировать работу всего ПЦН с помощью ПО Приток-А.

Современные идеи и большой опыт общения с нашими заказчиками был заложен в программное обеспечение 3.7.0. Разработано новое серверное ПО, увеличена номенклатура мобильных приложений для ОС Android, значительно обновлен интерфейс некоторых программ.

С появлением Приток-Охрана-WEB версия 3.7.0 призвана внедрить ряд новых организационных и программных механизмов для более эффективного взаимодействия между сотрудниками ПЦН и сотрудниками обслуживающих организаций.

Новые функции системы

Несколько попыток для снятия

Пожилые собственники квартир часто ошибаются при наборе кода для снятия. Установите специальный параметр «Разрешить несколько попыток для снятия» по таким объектам. В течение времени для снятия собственник сможет ввести правильный код после ошибки, а дежурному ПЦН не придется обрабатывать лишнюю тревогу.

Контроль нарушения режимного времени

Запретите автоматическое взятие под охрану вне режимного времени для тех объектов, собственники которых злостно нарушают время охраны по договору. Дополнительно установите контроль снятия после окончания режимного времени. Это позволит избежать увеличения количества часов «переохраны».

Контроль охраны в режимное время

Часто техник, обслуживающий банкомат, забывает поставить устройство под охрану по окончании своей работы. Установите на особо важных объектах «контроль не взятия» и определите индивидуально время, в течение которого объект может быть снят с охраны.

По окончании этого времени система напомнит о том, что объект не под охраной.

Автоматическая обработка тревог

Включите функцию автоматической обработки тревог, чтобы уменьшить количество действий операторов охраны. Система сама проверит объекты, с которыми были разрывы связи. После восстановления связи прибор будет опрошен, и при отсутствии изменений в охранном состоянии тревоги будут обработаны автоматически. Эти действия системы будут видны оператору и дежурному, что обеспечит дополнительный контроль.

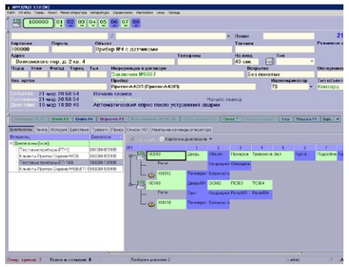
Уведомления пользователей о новых параметрах системы

С каждым обновлением программного обеспечения мы добавляем новые функции в систему. В связи с этим могут появиться новые настройки. Пользователям часто бывает сложно уследить за всеми изменения, поэтому мы разработали специальный механизм привлечения внимания пользователя к новым параметрам системы и новым функциям программ. Проверьте, как это работает в программе АРМ «Конфигуратор» для вкладки «Параметры».

Основные изменения в Приток-А 3.7.0:

- Поддержана архитектура x64 для ОС Windows
- Увеличена скорость обработки сообщений от аппаратуры и скорость работы всех программ
- Новые функции системы:
  - автоматическая обработка тревог*
  - новые алгоритмы по контролю за режимным временем охраны объектов
  - новые алгоритмы предупреждения и обработки неправильных действий собственников/ХО
- 2 новых мобильных приложения для собственников охраняемых объектов:
  - «Охрана Приток-А»
  - «Клавиатура Приток-А»
- Новое серверное программное обеспечение «Приток-Охрана-WEB» для организации удаленного доступа сотрудников обслуживающих организаций и собственников к информации по охраняемым на ПЦН объектам
- Полезные изменения для операторов охраны и дежурных
- Новый механизм более быстрого заполнения карточек охраняемых объектов, разработанный для инспекторов/инженеров ПЦН
- Обновление в системе SMS-информирования:
  - новые уведомления при приостановке действия договора, изменении пороговых значений температуры и влажности
  - распределение нагрузки при отправке SMS
- Uniprog 3 — новая программа конфигурирования приборов серии Приток-А

Изменения для операторов и дежурных АРМ ДПЦО



Дополнительная настройка интерфейса

Теперь каждый пользователь программы индивидуально может настроить расположение информации, размер шрифта в информации по карточке, а также видимость кнопок командной панели. Обратите внимание на кнопку настройки в виде шестеренки в правом нижнем углу панели информации по карточке.

Новая панель с состоянием охраняемого прибора

В верхнюю часть главного окна программы добавлена новая отдельная панель прибора с его шлейфами. При выборе любой карточки прибора панель отображает состояние и тип всех шлейфов прибора. Теперь оператор может оценивать комплексное состояние охраняемого объекта и выполнять команды по нему, не переключаясь на вкладку «Диапазоны».

Просмотр истории по объекту

Добавлена возможность просмотра истории по объекту за любой день (ранее только по оперативной информации из рабочей БД). Теперь оператор или дежурный без использования программы АРМ «Статистика» может просмотреть историю по объекту за нужный день.

Журнал заявок и отметок техников

В окне добавления заявки теперь отображается обслуживающая организация, которая закреплена за объектом. При добавлении заявки поле «Техник» не является обязательным для заполнения.

Сотрудники обслуживающих организаций смогут работать с этими заявками через web-интерфейс «Обслуживающие организации» Приток-Охрана-WEB (см. стр. 40) .

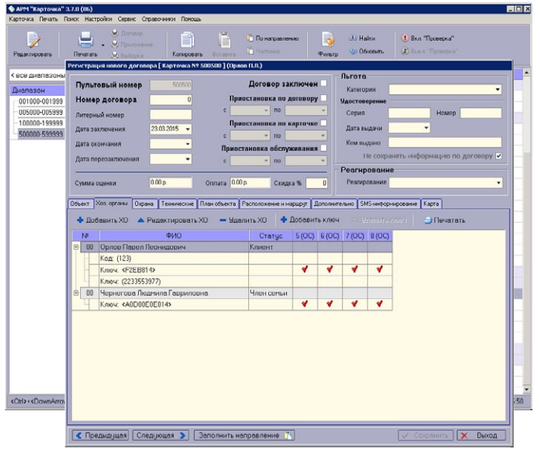
Режим приостановки на время работы техника

Включить режим «ПРОВЕРКА» по объекту теперь можно как бессрочно так и на определенный период (20 мин, 30 мин или указав точное время). Система сама выключит режим «ПРОВЕРКА» по истечении указанного периода. Тревоги по объектам с таким режимом не будут отвлекать дежурного ПЦН.

Изменения в интерфейсе

Много мелких и полезных изменений в интерфейсе программы. Например, теперь дата и время проще считывается с экрана. Было «29.12.14 15:00:02», стало «29-дек 15:00:02» (текущий год не пишется).

Изменения для инженеров АРМ «Карточка»



Дополняемый фильтр

Еще больше увеличивая возможности поиска (фильтра) карточек, разработан механизм, позволяющий выполнять выборку карточек по разным критериям — дополняемый фильтр. Теперь можно выполнить поиск карточек по одному критерию, получить список-выборку и к нему добавить карточки, найденные по другому критерию. Это удобно при формировании сложных отчётов.

Изменения в интерфейсе

Среди изменений в интерфейсе пользователя программы можно особо выделить несколько пунктов:

- на командную панель главного окна программы вынесены наиболее часто используемые функции печати, копирования и вставки карточек, а также управление режимом «ПРОВЕРКА» (убраны редко используемые функции);
- добавлены кнопки перелистывания карточек («предыдущая», «следующая») в окне редактирования карточки;
- изменен интерфейс окна редактирования карточки для закладок «Хоз. органы», «Охрана», «SMS-информирование».

Новый способ заполнения карточек

В версии 3.7.0 разработан новый механизм заполнения информации по карточкам охраняемых объектов. Этот механизм обеспечивает возможность заполнить все карточки зон прибора из одной карточки направления. Теперь инженеры будут тратить значительно меньше времени на занесение данных.

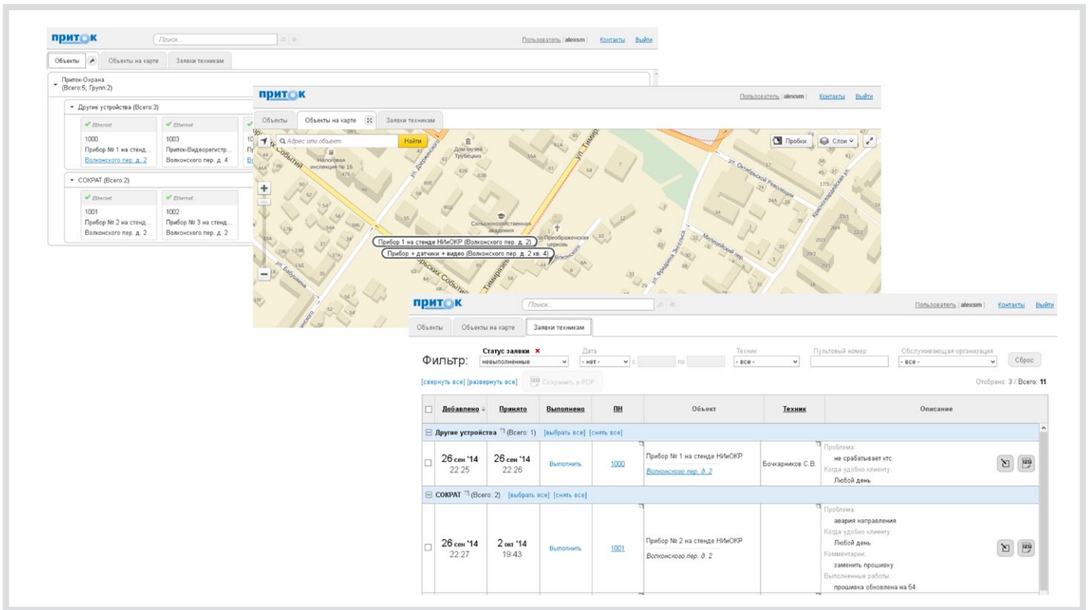
Изменения коснулись вкладки «Хоз. Органы», «Охрана», «SMS-информирование».

Подробнее о всех изменениях в версии ПО Приток-А 3.7.0 можно прочитать в описании версии — Release Notes, который включен в пакет обновления и опубликован на ftp.pritok.ru.

Приток-Охрана-WEB
Сервис для обслуживающих 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*.



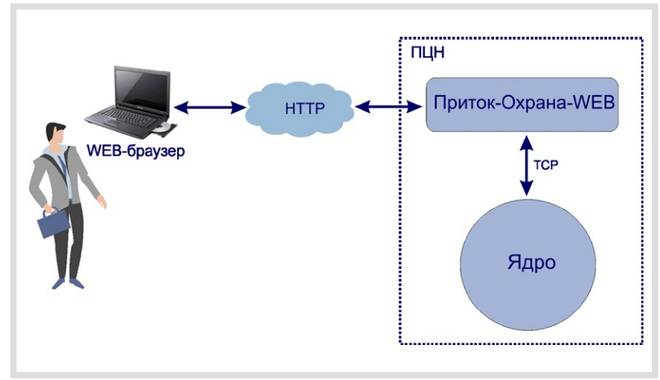
Web-интерфейс для собственников позволяет:
- просматривать список своих объектов, охраняемых на различных ПЦН;
- по каждому объекту контролировать охранное состояние шлейфов сигнализации, показания технологических датчиков (температура, влажность);
- выполнять команды постановки на охрану, снятия с охраны;
- 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

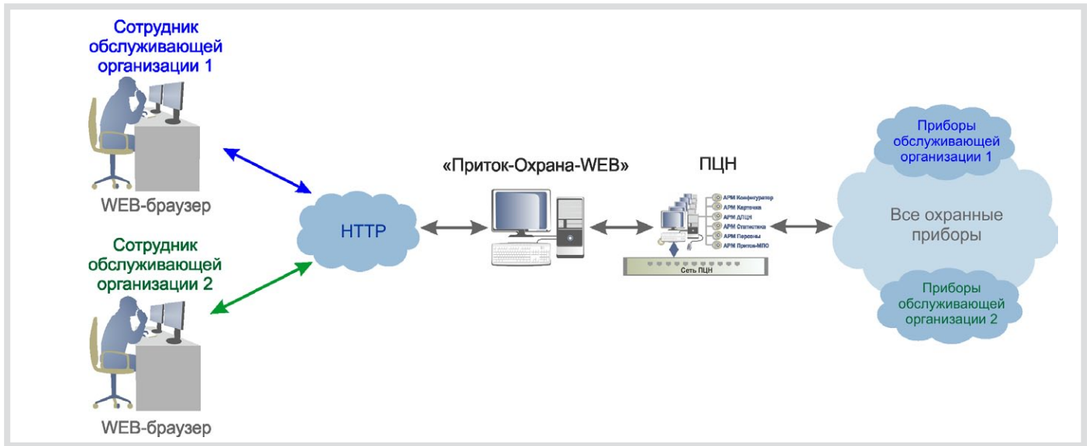
«Приток-Охрана-WEB» устанавливается и выполняется на отдельном сервере, который должен быть обеспечен доступом в Интернет.

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

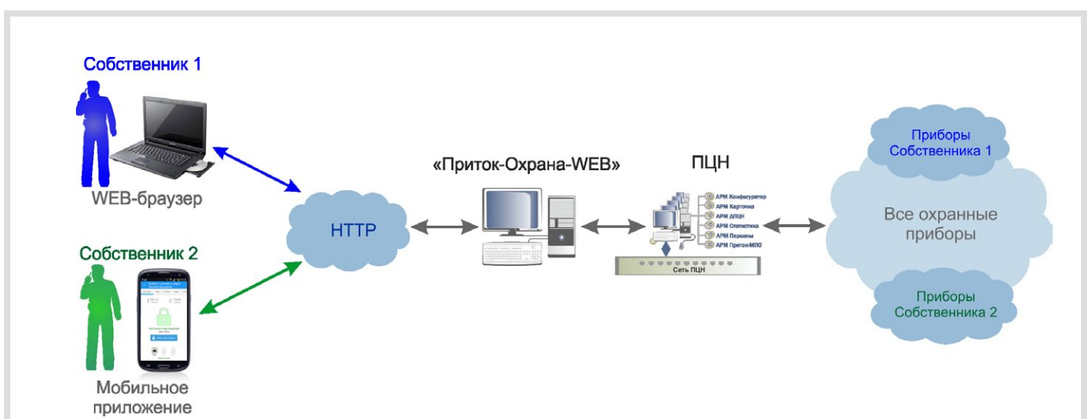


Администратором ПЦН при помощи программы АРМ «Конфигуратор» определяются уникальные имена и пароли для пользователей «Приток-Охрана». С помощью системы прав указывается к каким функциям «Приток-Охрана-WEB» будет иметь доступ пользователь и какие охраняемые объекты будут доступны для просмотра\управления.

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).



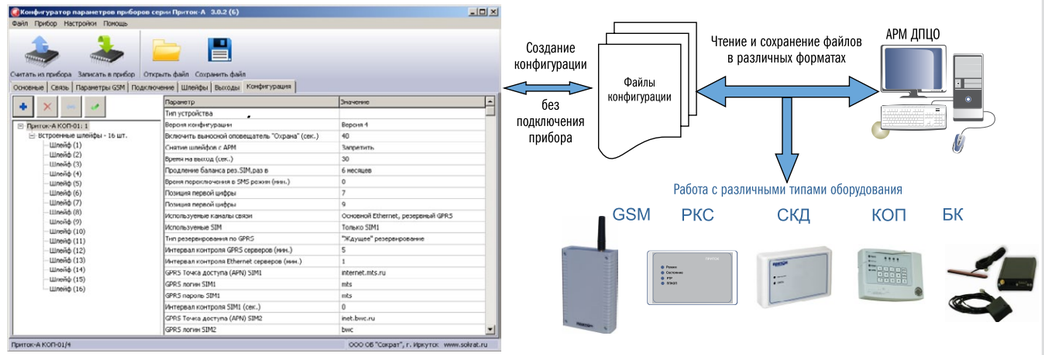
Конфигуратор параметров приборов серии Приток-А

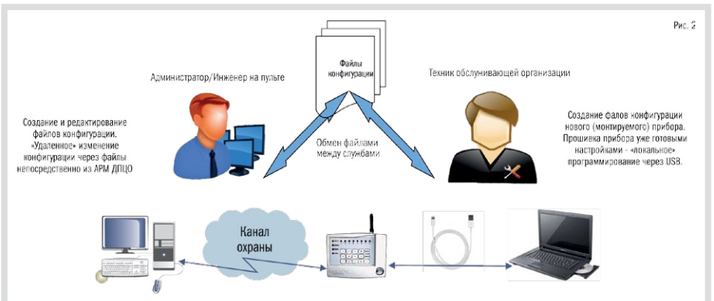
В свежих версиях программного обеспечения Приток-А пользователям доступна новая 3-я версия программы «Конфигуратор параметров приборов серии Приток-А» - UniProg3.exe. Программа предназначена для настройки конфигурации и установки параметров различного оборудования ИС Приток-А - охранных приборов, контроллеров, бортовых комплектов и пр.

Основные возможности программы:

- редактирование параметров приборов в удобном графическом интерфейсе с сохранением в единый файл конфигурации
- чтение и сохранение файлов конфигурации непосредственно из прибора
- редактирование файлов конфигурации полученных по каналам охраны через АРМ ДПЦО
- сохранение последней версии настроек прибора на диске ПК или внешнем носителе.

Конфигуратор параметров приборов серии Приток-А UniProg 3 Рис. 1





Возможность работы UniProg 3 с файлами конфигураций различного формата расширяет его функциональные возможности. Прочитав файл конфигурации уже работающего прибора (используя действующий канал охраны непосредственно из АРМ ДПЦО), открываем его в UniProg, сохраняем необходимые изменения (например, поменяем тип шлейфа или добавим клавиатуру) и, так же «удаленно», записываем его обратно в прибор.

Дальнейшее развитие «Конфигуратора параметров приборов серии Приток-А» сделает его универсальным, функциональным и удобным в использовании инструментом для настройки всех приборов ИС Приток-А.

Список оборудования, который поддерживает 3.0.2.11: Приборы: БК-04, БК-05, БК-06, БК-31, 011К, 011М, РКС-02, РКС-03, РКС-04, СКД-01, СКД-02, КОП-01, КОП-02. (РКС-01 и БК-032 могут конфигурироваться благодаря их совместимости с РКС-03 и БК-031) Модули (В составе КОП-01 и КОП-02): МРШ-02, МБД-01, МС-01, ВС-01, клавиатуры ППКОП.

Особенностью работы UniProg 3 является то, как он работает с конфигурацией различного оборудования — используя готовые шаблоны для всех поддерживаемых приборов. Создать конфигурацию для конкретного прибора (для бортовых комплектов системы мониторинга, охранных приборов по каналам GSM и Ethernet и др.) можно даже не подключая его — просто выбрав необходимый вариант из списка. Сохранив готовую конфигурацию, содержащую все настройки для данного прибора, можно передать этот файл (файлы) любым доступным образом, исключая ошибки и влияние «человеческого фактора».

Например, администратор БД создает из шаблона конфигурацию для РКС-04. В удобном и понятном графическом интерфейсе пользователя UniProg он заполняет все необходимые поля настроек прибора и параллельно копирует обязательные поля в «таблицу железа» АРМ Конфигуратор. Готовый файл передается монтажнику, которому нужно только записать его в уже смонтированный и установленный на объекте прибор, подключившись через кабель USB и выполнив всего пару действий в программе UniProg.

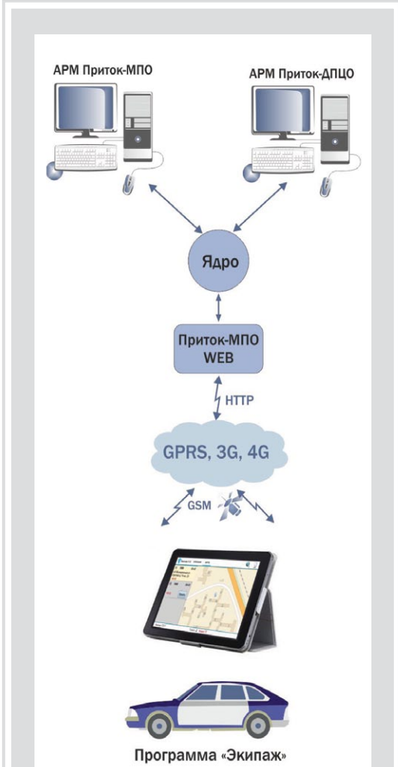
Программа «Экипаж»

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

Программа «Экипаж» позволяет сотрудникам группы задержания оперативно получать, подтверждать и обрабатывать отправляемую дежурным ПЦН информацию, касающуюся тревожного объекта. При этом адрес, характеристика и другая информация не 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.



Программа «Экипаж»

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.

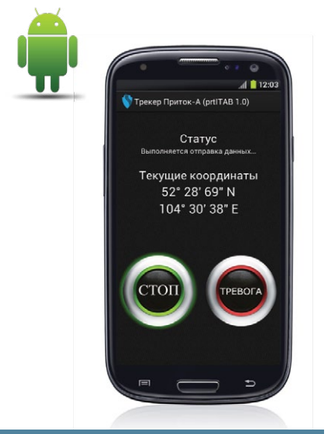
Таким образом, вновь созданные программно-аппаратные средства Приток-Автоприбытие сделали работу ДПЦН по управлению ГЗ более надежной и удобной и исключили возможность перехвата информации в радиоэфире.

Программа «Трекер Приток-А»

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

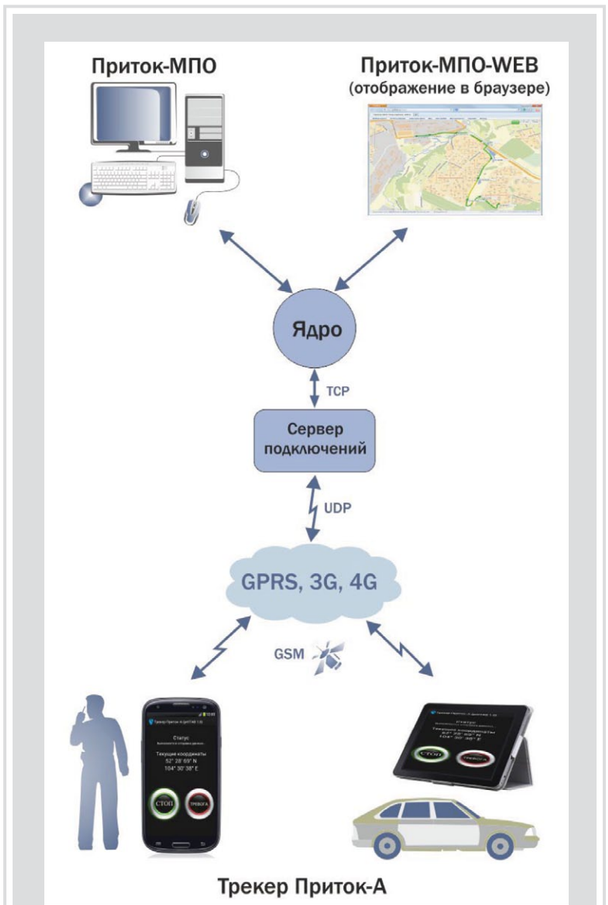
Программа «Трекер Приток-А» позволяет контролировать передвижение сотрудников, клиентов, детей и близких, используя телефон (планшет) со встроенным GPS /ГЛОНАСС приемником.

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.

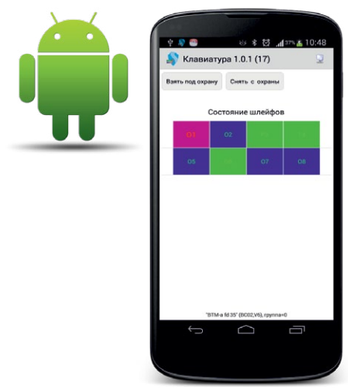
Программа «Клавиатура Приток-А»

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.

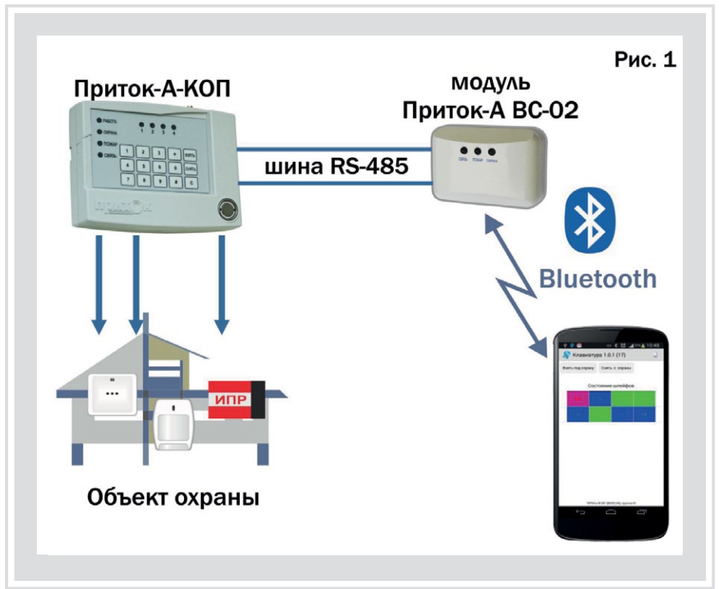
Программа устанавливается на смартфоны и планшетные компьютеры, работающие под управлением ОС Android.

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».

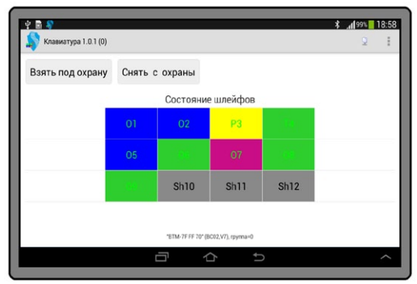


Подключение

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 производится 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).

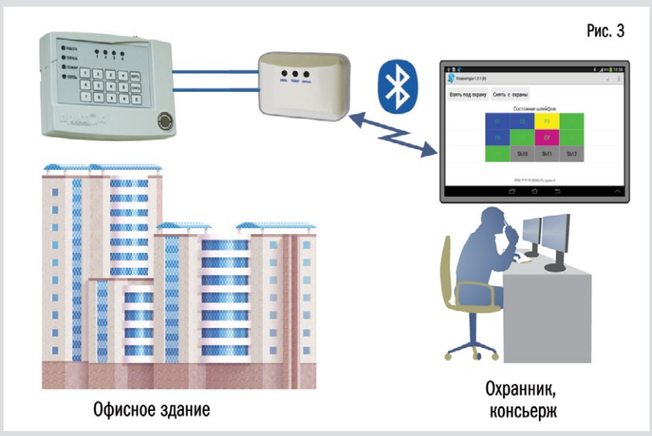


Рис. 3

• 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 (индетификатор) 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.

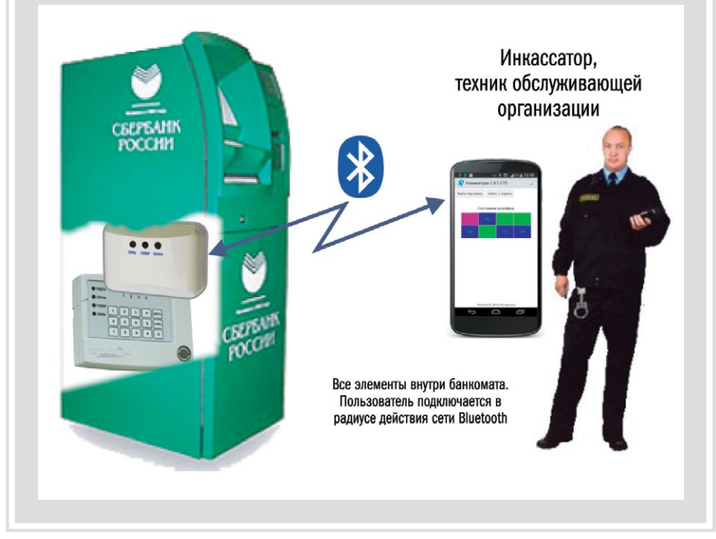
Кроме этого, известно, что любой банкомат требует технического обслуживания. Сотрудник обслуживающей организации при работе с банкоматом не имеет права снимать с охраны все шлейфы банкомата целиком — для снятия ему должны быть доступны только сервисные части банкомата. Инкассатор же, наоборот, может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

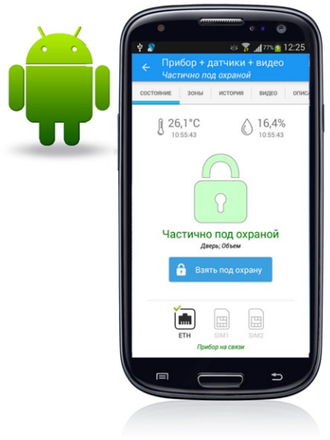


Более подробно про «Клавиатура Приток-А» смотрите на сайте: http://sokrat.ru/pritok/objectp/btkeyboard.htm

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

Программа «Охрана Приток-А»

«Охрана Приток-А» — программа для ОС Android, являющаяся клиентским приложением 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.

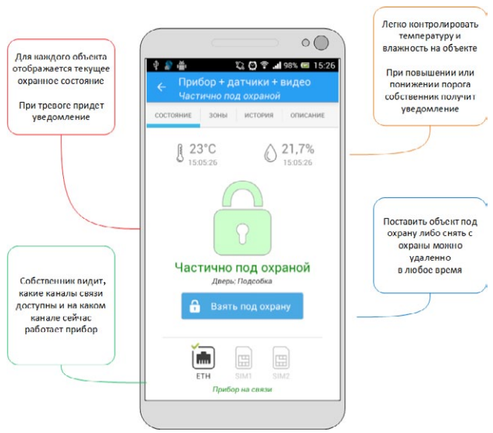
Помещение объекта оборудуется ОПС с использованием приборов серии Приток-А-КОП. К прибору подключаются различные датчики (объемные, протечки воды) и устанавливаются дополнительные модули расширения (такие как модуль беспроводных датчиков МБД-01/02, модуль гигрометра ВС-01 с датчиком влажности и температуры).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

Пульт охраны, центр мониторинга (либо другая организация) предоставляет доступ собственников охраняемых объектов к сервису Приток-Охрана-WEB (см. стр. 40). 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.



КАТАЛОГ

приток

В разделе «Каталог» 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

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).

Контроллер работает с «Сервером подключений» системы Приток-А. «Сервер подключений» — это ПК с установленной и настроенной на нём программой XDevSvc. Предусмотрено резервирование каналов связи для приёма информации на ПЦН. Контроллер поддерживает до четырёх IP-адресов ПЦН для Ethernet-подключения и до четырёх IP-адресов ПЦН для GPRS-подключения (IP-адрес ПЦН – это статический IP-адрес и порт, при отправке сообщений на который данные передаются на «Сервер подключений», можно использовать доменные имена).

Так как сеть Ethernet может не иметь доступа в Интернет (например, организована корпоративная VLAN-сеть по технологии GPON), то предусмотрена возможность задать разные IP-адреса ПЦН для Ethernet и для GPRS-каналов связи.

Контроллер может использовать любое сочетание доступных ему каналов связи. Например: только Ethernet, только GPRS SIM1, Ethernet и GPRS SIM1 и т.д. Приоритет их использования определяется в настройках.

При работе на основном канале связи в контроллере предусмотрено постоянное тестирование резервного канала для безаварийного перехода между каналами.

В зависимости от настройки контроллер выбирает основной канал для работы. В случае потери связи с сервером подключений 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.

В канале GSM (GPRS) контроллер начинает работу по основной SIM-карте. В случае потери связи с сервером подключений 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.

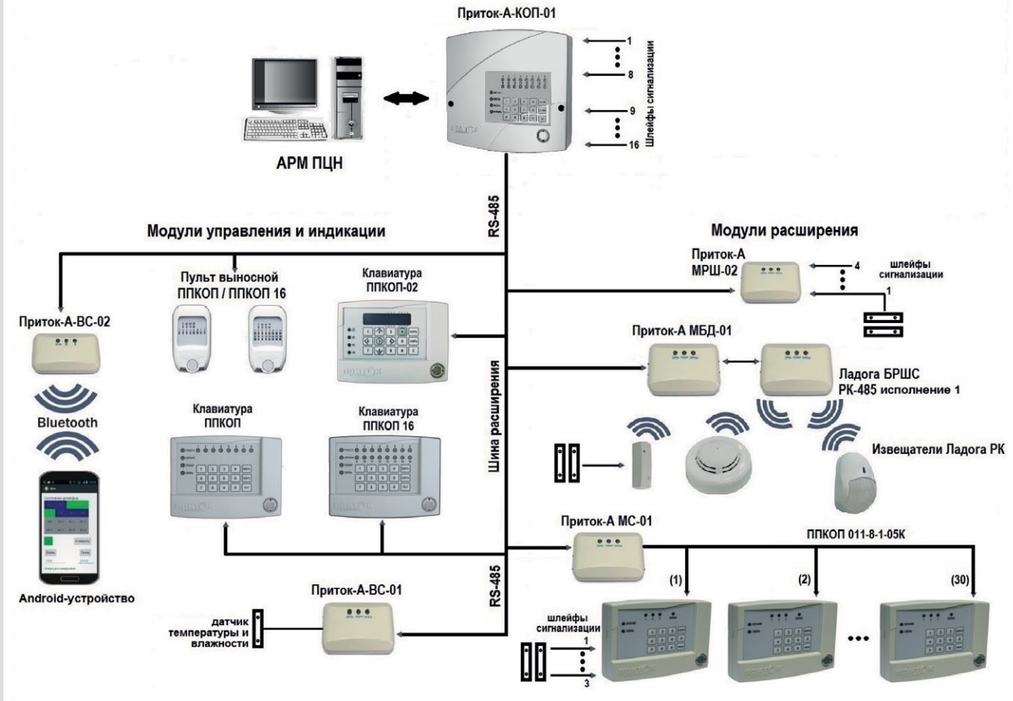
Во время работы контроллер периодически проверяет состояние связи со всеми «Серверами подключений» по указанным в настройках IP-адресам ПЦН. При отсутствии связи с текущим «Сервером подключения» контроллер переключается на рабочий «Сервер подключений».

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)

ВАРИАНТЫ ИСПОЛНЕНИЯ

ТИП КОНТРОЛЛЕРА	КОЛИЧЕСТВО ШЛЕЙФОВ	КОЛИЧЕСТВО ИНДИКАТОРОВ НА ПРИБОРЕ	СВЯЗЬ ЧЕРЕЗ ETHERNET	СВЯЗЬ ЧЕРЕЗ GSM	ИСТОЧНИК ПИТАНИЯ
ПРИТОК-А-КОП-02	4	4	V	V	ВНЕШНИЙ ИП (НЕ ВХОДИТ В КОМПЛЕКТАЦИЮ)
ПРИТОК-А-КОП-02.1	4	4	V	-	ВНЕШНИЙ ИП (НЕ ВХОДИТ В КОМПЛЕКТАЦИЮ)
ПРИТОК-А-КОП-02.2	4 + МРШ-02 (+4 ШЛЕЙФА)	8	V	V	ВНЕШНИЙ ИП (НЕ ВХОДИТ В КОМПЛЕКТАЦИЮ)
ПРИТОК-А-КОП-01(8)	8	8	V	V	ВСТРОЕННЫЙ ИП + АКБ
ПРИТОК-А-КОП-01.1(16)	16	16	V	V	ВСТРОЕННЫЙ ИП + АКБ



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

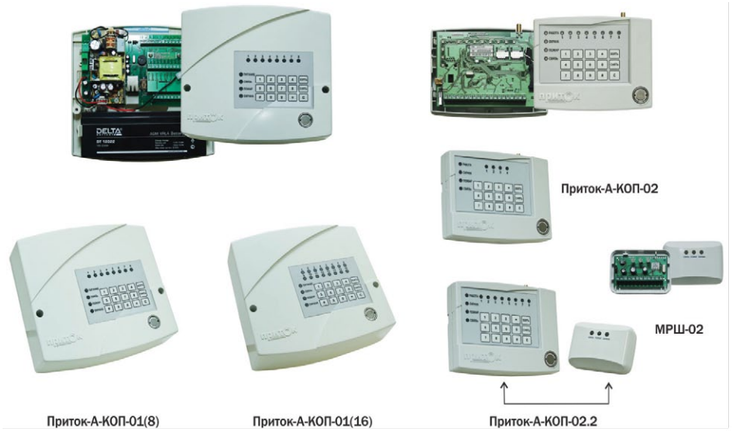
предназначены для отображения состояния контролируемых ШС (до 128). Возможно подключение до 8 модулей индикации:

- 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).



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 — для реализации любых схем охраны.

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 (Рис. 1).

Варианты подключений:

1) Подключение через существующий выход в сеть Интернет. На охраняемом объекте, где есть подключение в интернет (используется пользователями), устанавливается маршрутизатор или используется уже имеющийся, через который подключается контроллер. 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 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. Т**аким 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.

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 внутри контроллера (Рис. 2).

Рис. 1

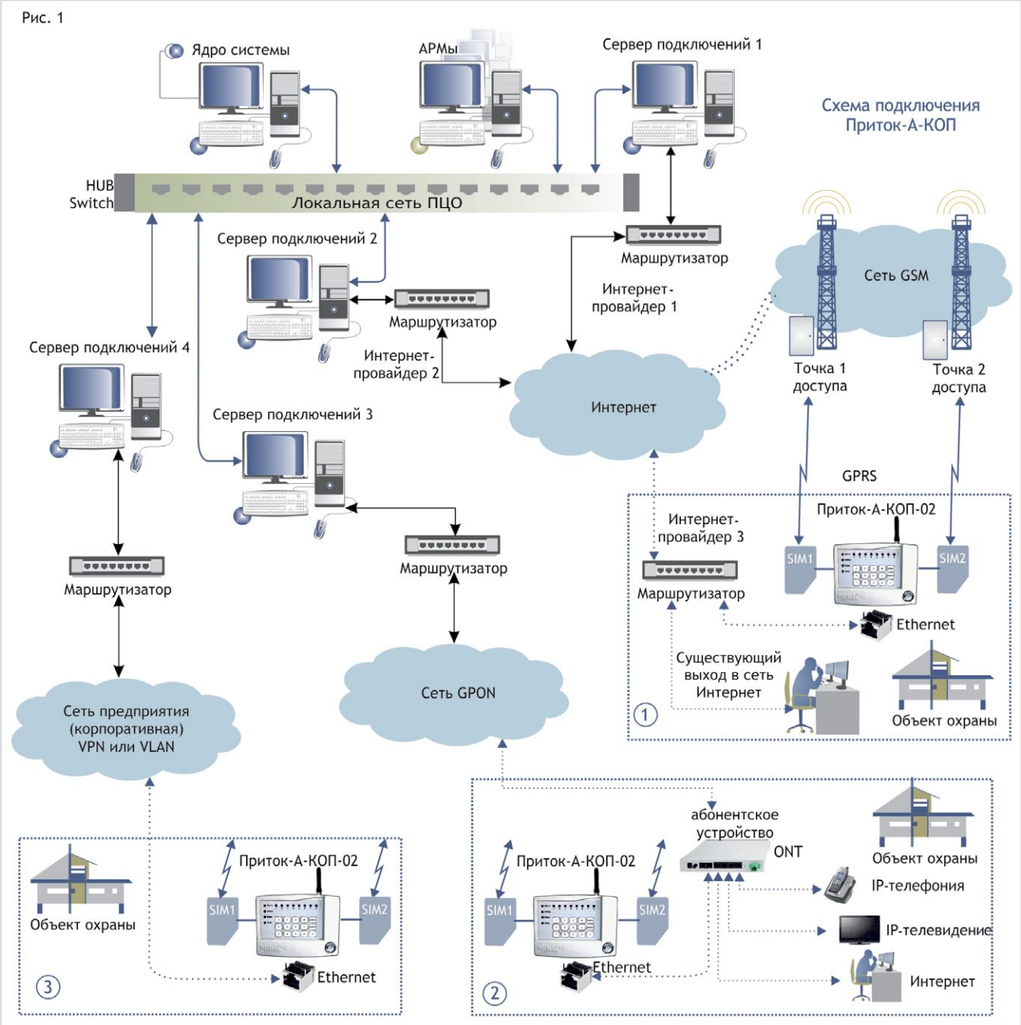


Рис. 2

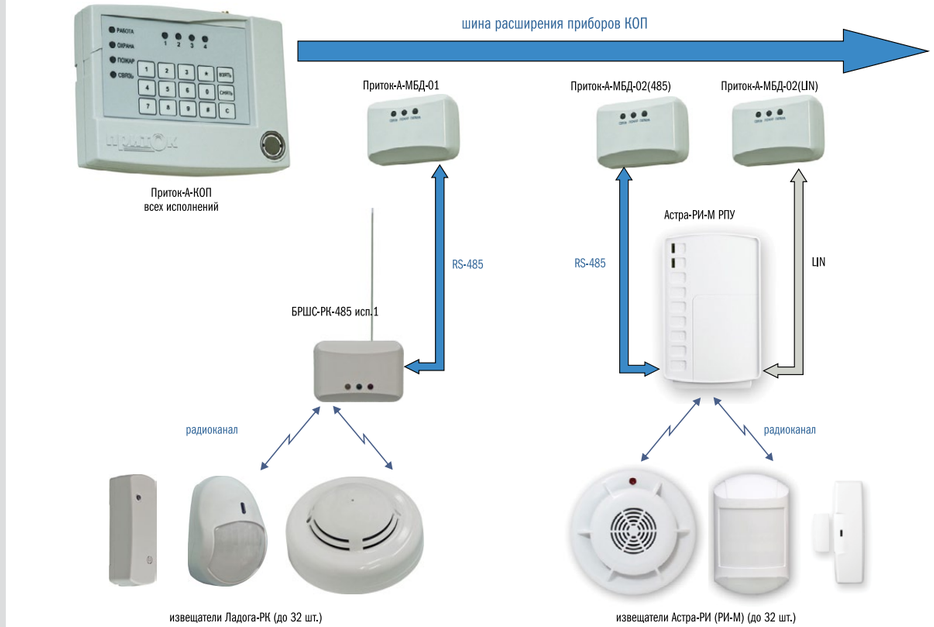
Подключение радиоканальных извещателей Ладога-РК и Астра-РИ-М

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 кокретному 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 P2V

• 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

Приток-ИП-02

Приток-ИП-02 предназначен для бесперебойного электропитания систем охранно-пожарной сигнализации, систем видеонаблюдения, радиостанций и других потребителей с номинальным напряжением 12 В постоянного тока и током потребления до 1,5 А.

Приток-ИП-02

Особенности

Минимальное напряжение сети переменного тока, при котором ИБП обеспечивает стабильную работу нагрузки, составляет 88 В.

ИБП имеет электронную защиту от перегрузки по току и от короткого замыкания на выходе. Защита от переполюсовки аккумуляторной батареи (АКБ) обеспечивается установкой предохранителя.

Принцип действия

При отключении основного электропитания (~220 В) ИБП автоматически переключается на резервное питание подключенной нагрузки от встроенной АКБ.

Если ИБП обеспечивает электропитанием ППКОП-06 серии Приток, то ППКОП-06 получает от ИБП и передаёт на ПЦН извещение об отключении основного питания и автоматическом переходе на резервное питание — «авария 220».

При работе от АКБ ИБП обеспечивает автоматическое отключение АКБ, если напряжение на её клеммах становится менее 10,4 В. Это предотвращает выход АКБ из строя при глубоком разряде.

При восстановлении сетевого электропитания ~220 В ИБП автоматически переключается на работу от электрической сети.

Конструктивное исполнение

Конструктивно ИБП состоит из корпуса с крышкой, внутри которого установлены печатная плата с предохранителями, соединительными колодками и аккумуляторная батарея.

ИБП представляет собой импульсный стабилизированный источник питания с бестрансформаторным входом с частотой преобразования 100 кГц.

Срок службы ИБП — 8 лет, срок хранения до начала эксплуатации — 6 месяцев.

ИБП обеспечивает индикацию состояния сетевого напряжения, АКБ и цепей ее заряда (индикатор «СЕТЬ/АКБ») и индикацию наличия выходного напряжения (индикатор «ВЫХОД»).

Зависимость времени непрерывной работы ИБП при полностью заряженной АКБ от тока нагрузки при температуре плюс 20°С приведено ниже в таблице.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ИБП ПРИТОК-ИП-02

НАИМЕНОВАНИЕ ПАРАМЕТРА	ЗНАЧЕНИЕ ПАРАМЕТРА
ВЫХОДНОЕ НАПРЯЖЕНИЕ, В: — ПРИ ПИТАНИИ ОТ СЕТИ — ПРИ ПИТАНИИ ОТ АКБ	 13,5 — 13,8 10,4 — 12,6
МАКСИМАЛЬНЫЙ ТОК НАГРУЗКИ, А	1,5
ВЕЛИЧИНА ПУЛЬСАЦИЙ ВЫХОДНОГО НАПРЯЖЕНИЯ (ОТ ПИКА ДО ПИКА), В, НЕ БОЛЕЕ	0,3
НАПРЯЖЕНИЕ СЕТИ ПЕРЕМЕННОГО ТОКА, В	220 (+10%, —40%)
МАКСИМАЛЬНЫЙ ТОК ЗАРЯДА ВСТРОЕННОЙ АКБ, А	0,6
НАПРЯЖЕНИЕ НА АКБ, ПРИ КОТОРОМ АВТОМАТИЧЕСКИ ОТКЛЮЧАЕТСЯ НАГРУЗКА, В	10,4 — 10,6
НОМИНАЛЬНОЕ НАПРЯЖЕНИЕ АКБ, В	12
РЕКОМЕНДУЕМАЯ ЕМКОСТЬ АКБ, А/Ч	7 ИЛИ 12
МОЩНОСТЬ, ПОТРЕБЛЯЕМАЯ ОТ СЕТИ, В/А	50
ГАБАРИТНЫЕ РАЗМЕРЫ, ММ	237 Х 165 Х 106
МАССА С АКБ, КГ, НЕ БОЛЕЕ	4

ЕМКОСТЬ АКБ	ТОК НАГРУЗКИ, А	0,25	0,5	1	1,5
7А/Ч	ВРЕМЯ НЕПРЕРЫВНОЙ РАБОТЫ, Ч	24	12	5,5	4
12А/Ч		40	22	9,5	6,5

При температуре минус 10°С время работы от АКБ уменьшается почти на 50%. Время полного заряда АКБ — не более 48 ч.

ИБП рассчитан на круглосуточную эксплуатацию в закрытых непожароопасных помещениях, при температуре от минус 30 до плюс 40 °С, относительной влажности воздуха до 85%, отсутствии в воздухе пыли, паров агрессивных жидкостей и газов (кислот, щелочей и пр.).

РЕЖИМЫ РАБОТЫ ИНДИКАТОРА «СЕТЬ/АКБ»	СОСТОЯНИЕ СЕТИ 220 В	СОСТОЯНИЕ АКБ
СВЕТИТСЯ НЕПРЕРЫВНО ЗЕЛЕНЫМ ЦВЕТОМ	ВКЛЮЧЕНА	ЗАРЯЖЕН
ЗЕЛЕНЫМ ЦВЕТОМ СВЕТИТСЯ ПРЕРЫВИСТО	ВКЛЮЧЕНА	ИДЕТ ЗАРЯД
СВЕТИТСЯ ПРЕРЫВИСТО КРАСНЫМ ЦВЕТОМ	ОТКЛЮЧЕНА	ИДЕТ РАЗРЯД
СВЕТИТСЯ НЕПРЕРЫВНО КРАСНЫМ ЦВЕТОМ	ОТКЛЮЧЕНА	РАЗРЯЖЕН, ЧЕРЕЗ 1 МИН. ИБП ОТКЛЮЧИТСЯ

КАТАЛОГ

В разделе «Каталог» 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

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

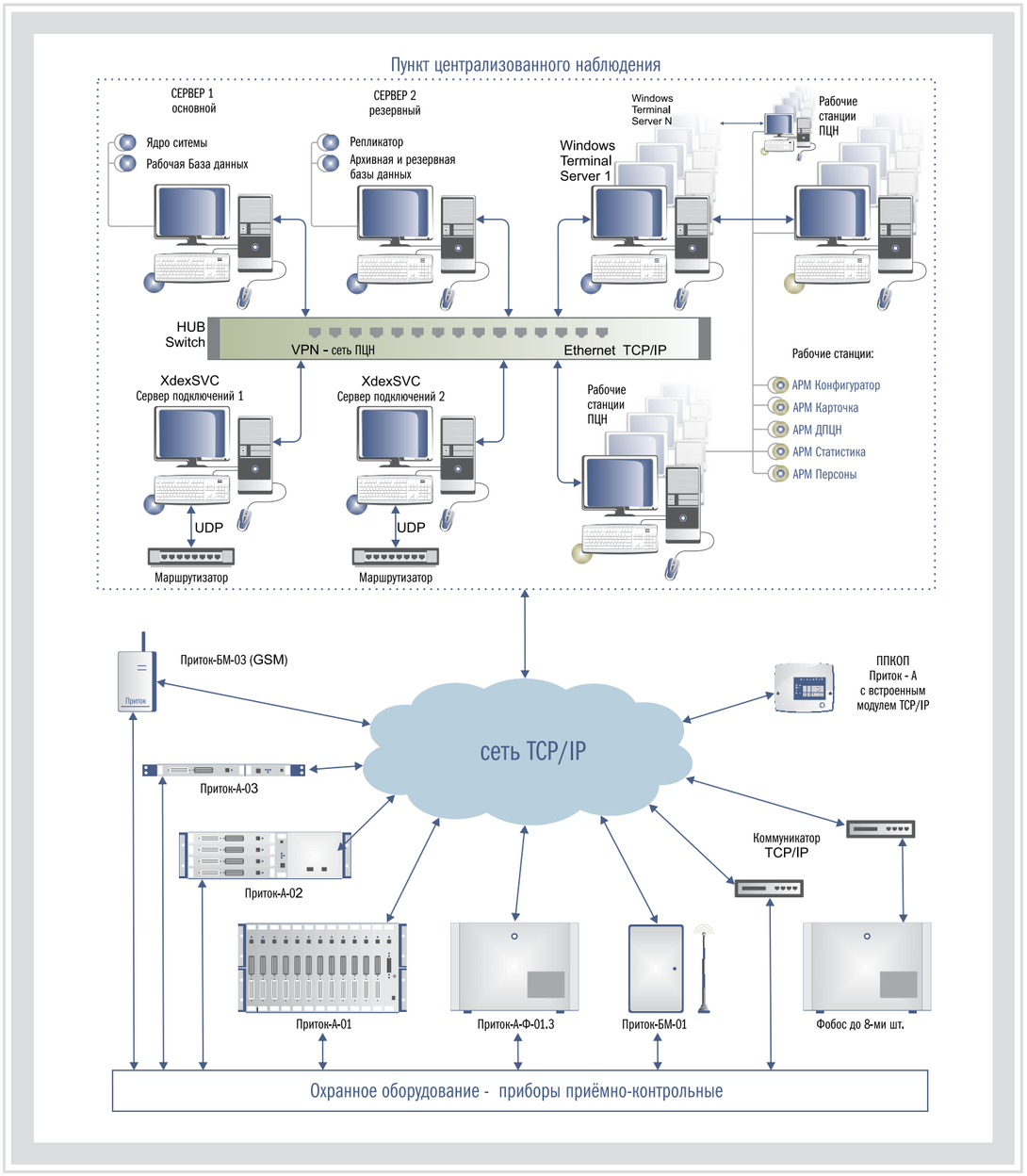
Основным физическим элементом подсистемы Приток-TCP/IP является универсальное устройство **Коммуникатор TCP/IP ЛИПГ.468362.006.** Для передачи извещений в сети ПЦН Коммуникатор TCP\IP преобразует протоколы, по которым работает оборудование, подключаемое к сети ПЦН (в состав ИС Приток-А) в протокол TCP/IP,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


Приток-А-01


Приток-А-03


Приток-А-02 (021 и 022)


Приток-А-Ф-01.03

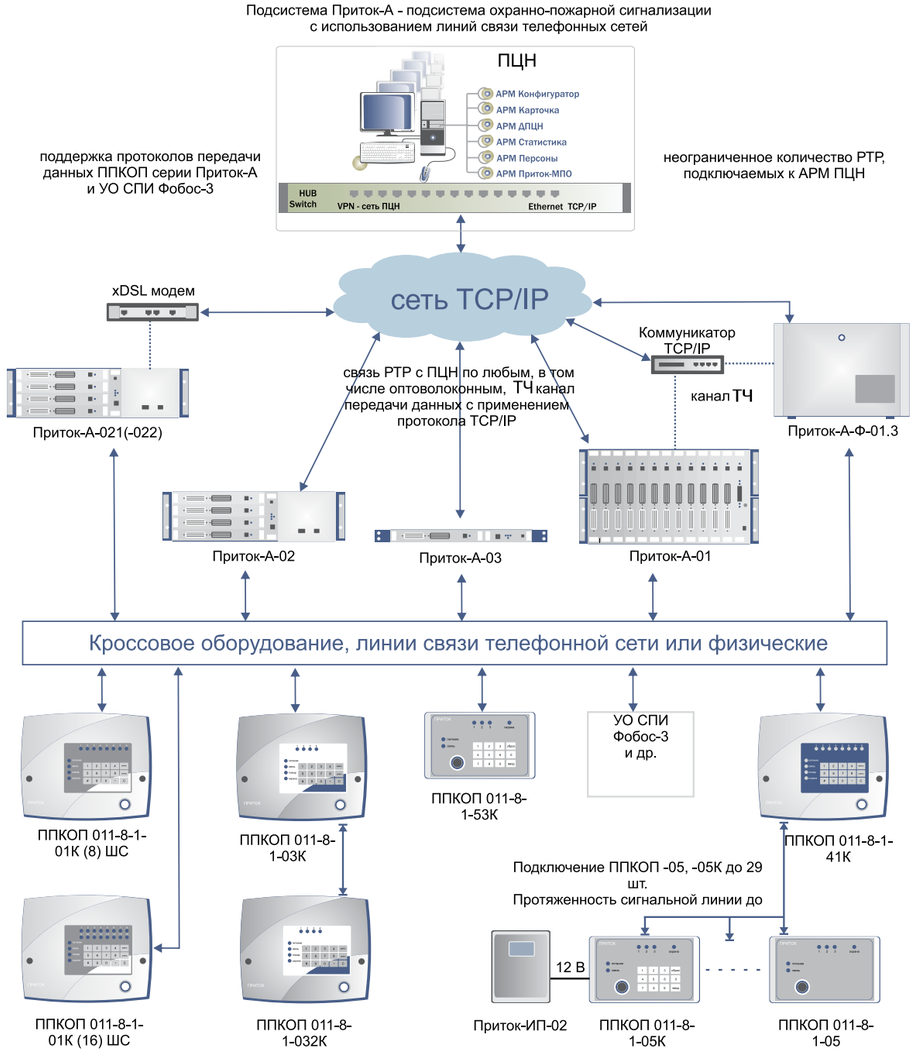
Конструктивно РТР Приток-А выполнены в корпусах стандарта МЭК297 для установки в стойки «Евромеханика 19», РТР Приток-А-Ф-01.3 выполнен в корпусе Приток-А-Ф (Фобос-3). В **таб. 2** приведены отличительные характеристики всех типоразмеров и вариантов, выпускаемых РТР.

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.

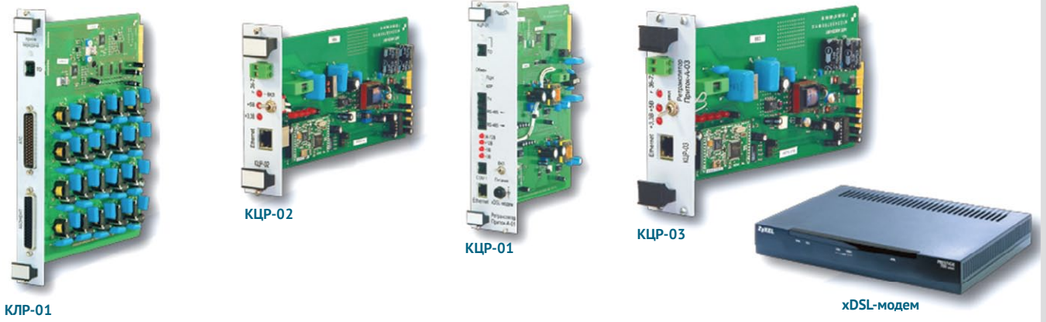
Применение имитостойкого, помехозащищенного протокола передачи данных обеспечивает защиту от подключения на линии связи канала РТР – ППКОП эквивалентов ППКОП, а наличие автоматической подстройки чувствительности приемника в канале РТР – ППКОП под индивидуальные параметры линии связи исключает ложные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

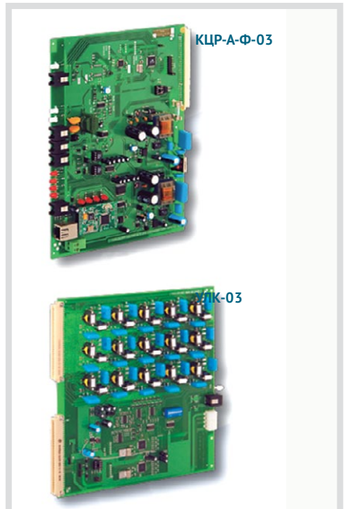
2. Ретрансляторы Приток-А-Ф-01.3 (02.3) конструктивно совпадают с ретрансляторами Фобос-3 и Фобос-ТР и могут устанавливаться непосредственно на место снимаемых ретрансляторов Фобос-3 или Фобос-ТР.

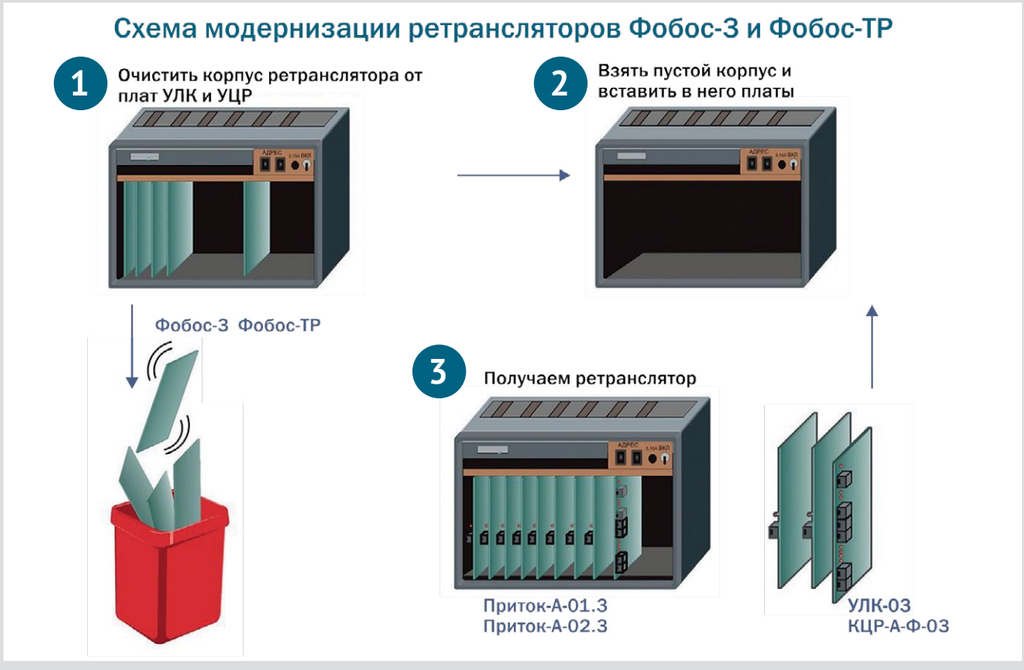
3. Для того чтобы вообще не производить замену корпусов ретрансляторов Фобос-3 или Фобос-ТР, достаточно применять «Комплект модернизации РТР Фобос-3».

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.





ПОДСИСТЕМЫ

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.

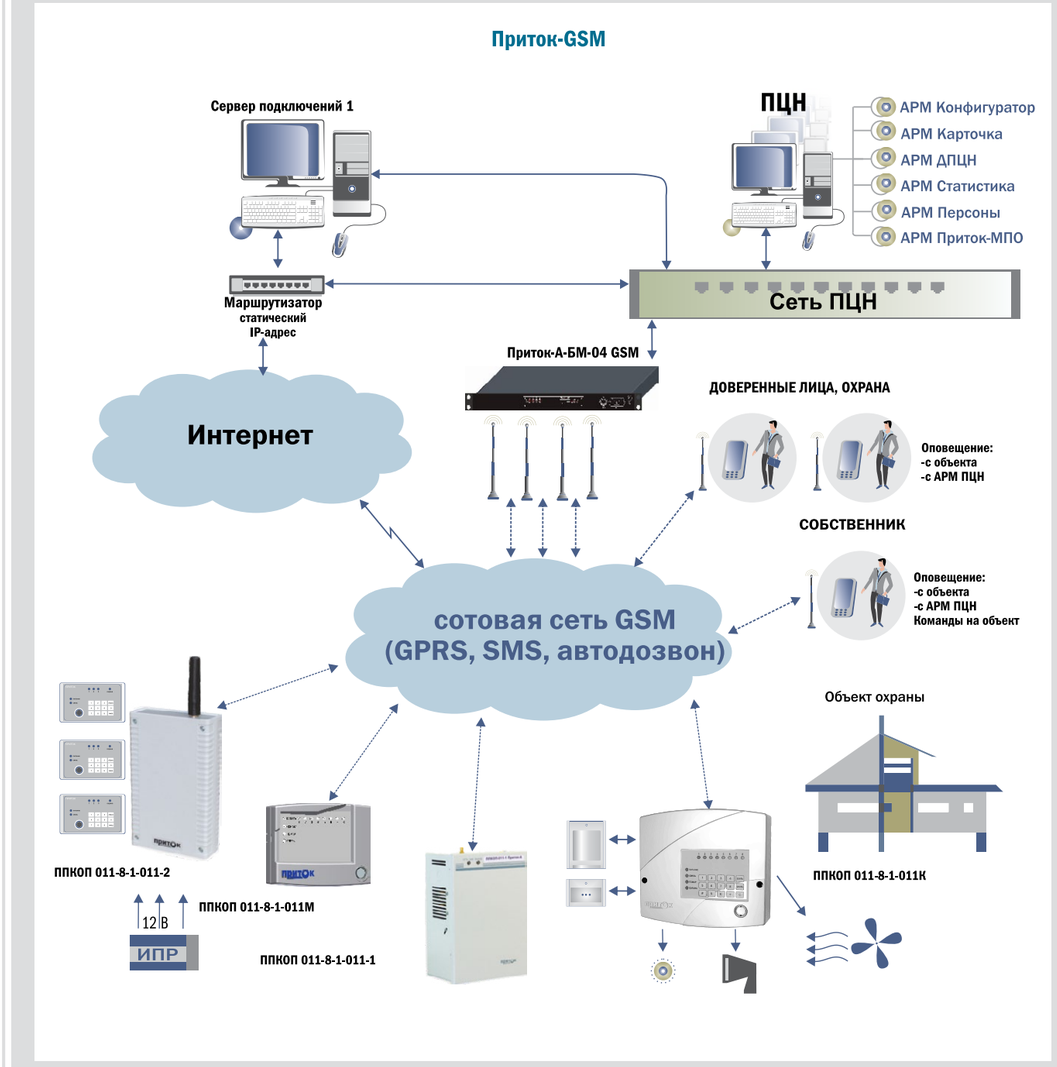
Приборы подсистемы предназначены для организации централизованной или автономной охраны объектов (квартир, дач) с автоматизированной тактикой взятия под охрану и снятия с охраны. Для передачи сообщений и приема команд используется сеть GSM выбранного оператора сотовой связи (ОСС). Приборы имеют возможность 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.

Состав подсистемы Приток-GSM

- базовый модуль **Приток-А-БМ-03 (-04) (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)
- прибор охранно-пожарный **ППКОП 011-8-1-011-2 Приток-А-4(8)** с функцией концентратора (далее ППКОП-011-02)

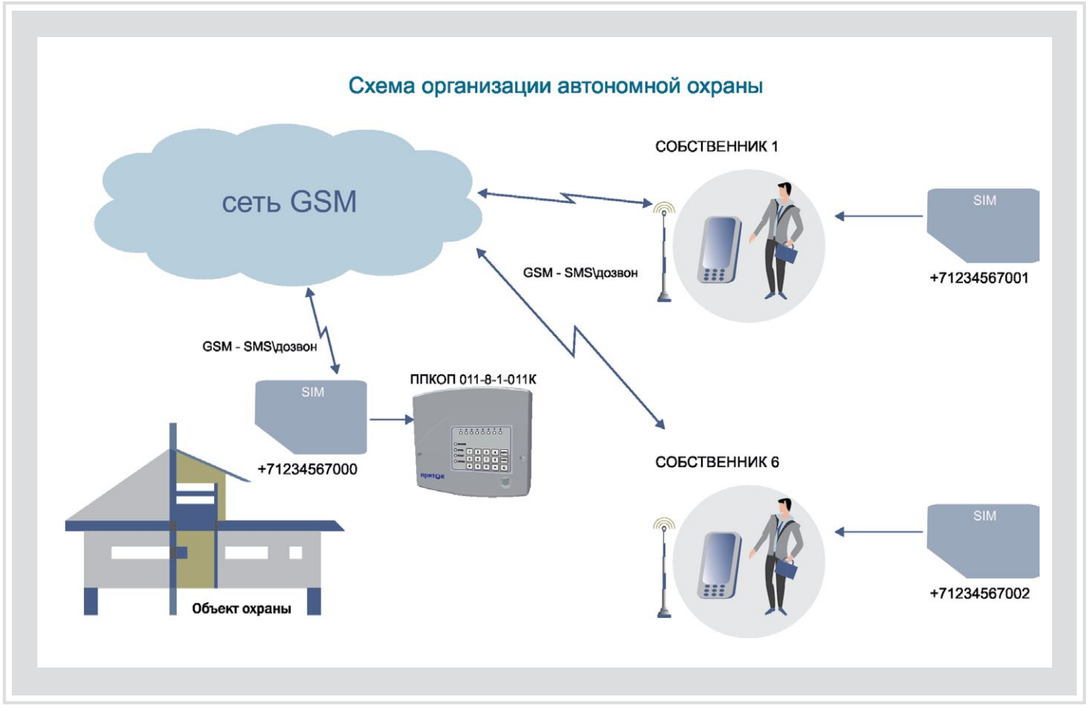
Основные технические характеристики

- в ППКОП-011 используется 2 SIM-карты для резервирования канала
- ППКОП-011- 02 имеет семь шлейфов охранной, пожарной или тревожной сигнализации. ППКОП-011М, ППКОП-011-1К и ППКОП-011-01 – восемь шлейфов
- 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-011-2 и 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-03(04) 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



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

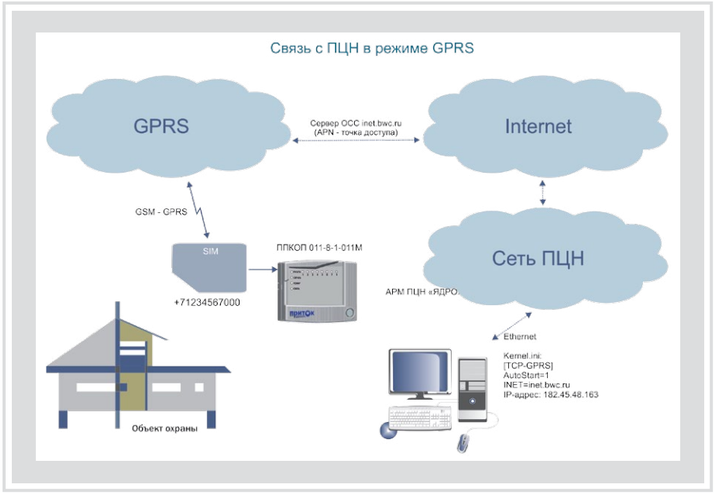


Принцип действия централизованной охраны

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.

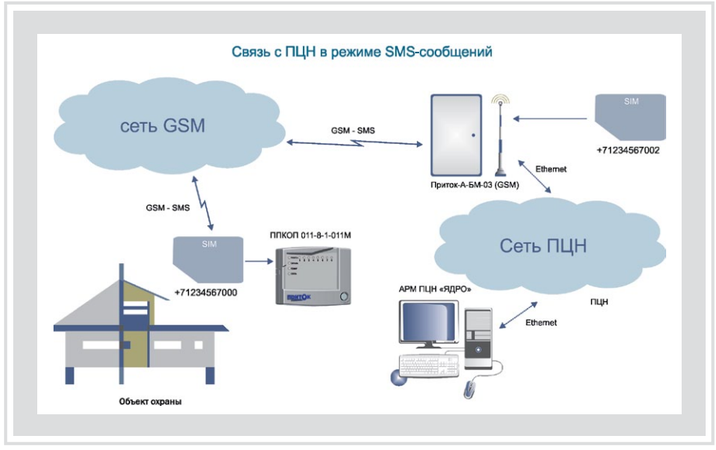
При работе ППКОП-011 с АРМ ПЦН в режиме GPRS доступ с остальных телефонов собственника прекращается. Ниже приведены схемы организации связи в Приток-GSM.



Принцип действия автономной 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. Схема организации автономной охраны приведена ниже.



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 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.

Коммуникатор Приток-GSM
приборы приемно-контрольные охранно-пожарные

В составе подсистемы Приток-GSM создан коммуникатор ППКОП-011-02, который работает по каналам сотовой связи в режимах SMS и GPRS. К нему по двухпроводной сигнальной линии могут подключаться до 29 шт. ППКОП 011-8-1-05, -05к. Протяженность линии может быть до 1000 м.

Учитывая специфику передачи сообщений по каналам сотовой связи, ППКОП-05, -05к будут иметь модернизированное внутреннее программное обеспечение, иными словами, будут иметь другую прошивку. Поэтому ранее выпускаемые ППКОП-05 работать с новым коммуникатором Приток-GSM не смогут (ППКОП-05 старого образца).

Для GSM-коммуникатора можно организовать и беспроводную радиосвязь из подсистемы Приток-МКР. Применяя GSM-коммуникаторы с использованием микрорадиоканала, мы можем быстро организовать охрану и отдельно стоящих киосков и многоофисных помещений, где любые монтажные работы по прокладке кабеля либо затруднены, либо невозможны.

В качестве коммуникатора Приток-GSM в дальнейшем может использоваться модуль резервного канала связи Приток-РКС.

ПОДСИСТЕМЫ

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).

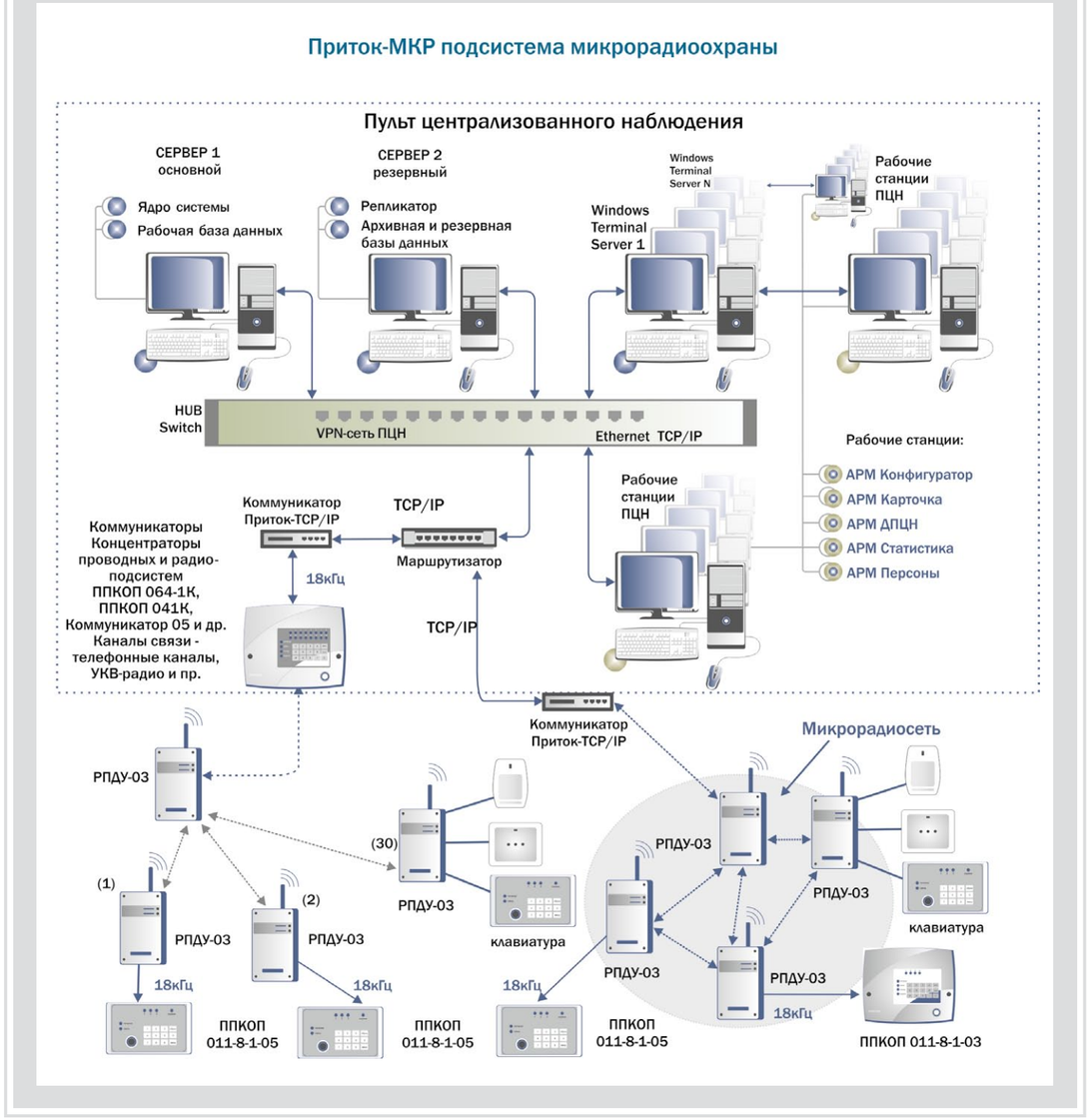
Это означает, что связь РПДУ-03 с сетью ПЦН может осуществляться:

- 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 предназначена для мониторинга и охраны подвижных объектов (транспортных средств — ТС) и оценки оперативной обстановки по электронной карте контролируемого (охраняемого) района, города (местности), а также для контроля за перемещением и охраны граждан.

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 GlobalSatникого.

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 помошью 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.

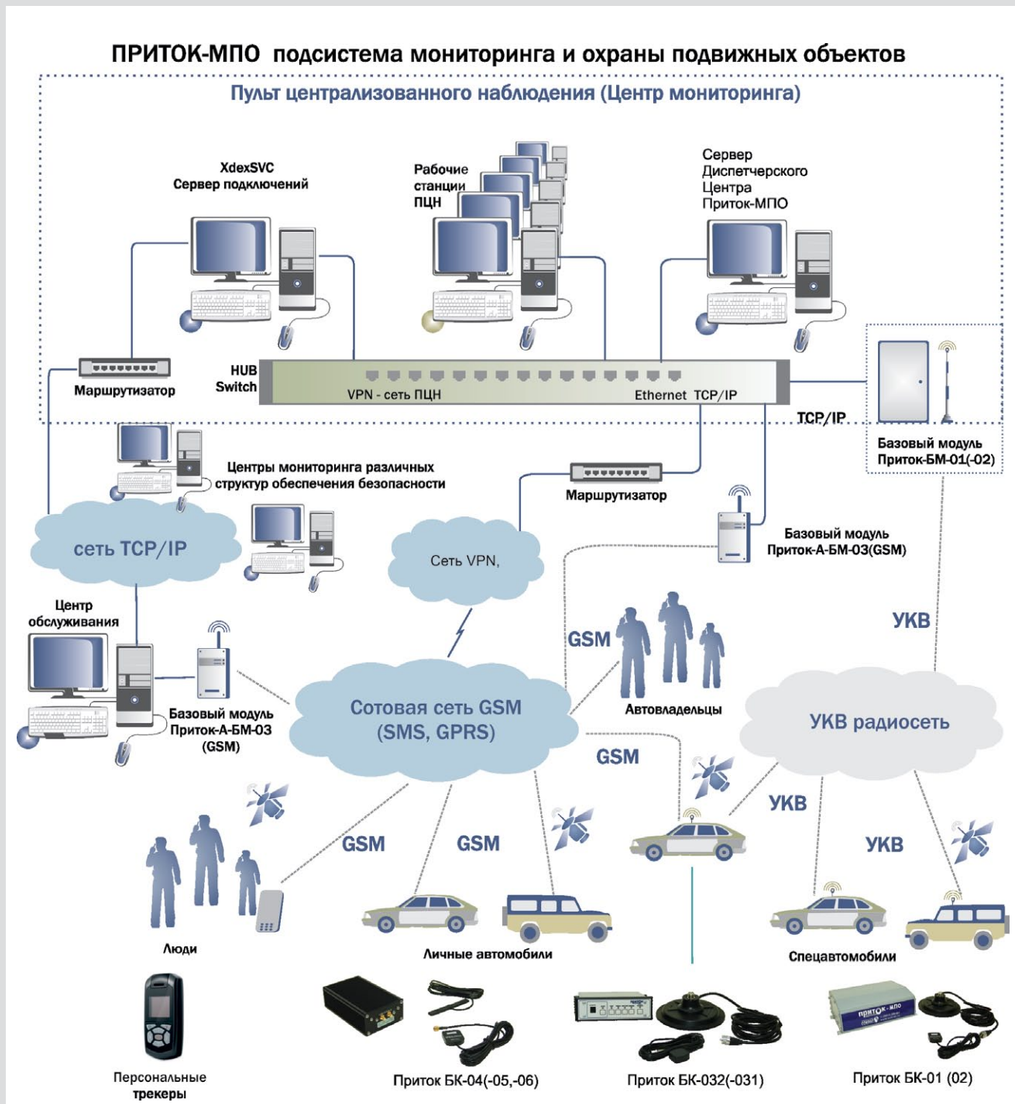
ПО позволяет проконтролировать местоположение, скорость и направление движения ТС, состояние БК (охраняется, не охраняется, тревога и т.д.), работоспособность БК по результатам диагностики, результаты ответов на поданные запросы и результаты выполнения поданных на БК команд управления.

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.

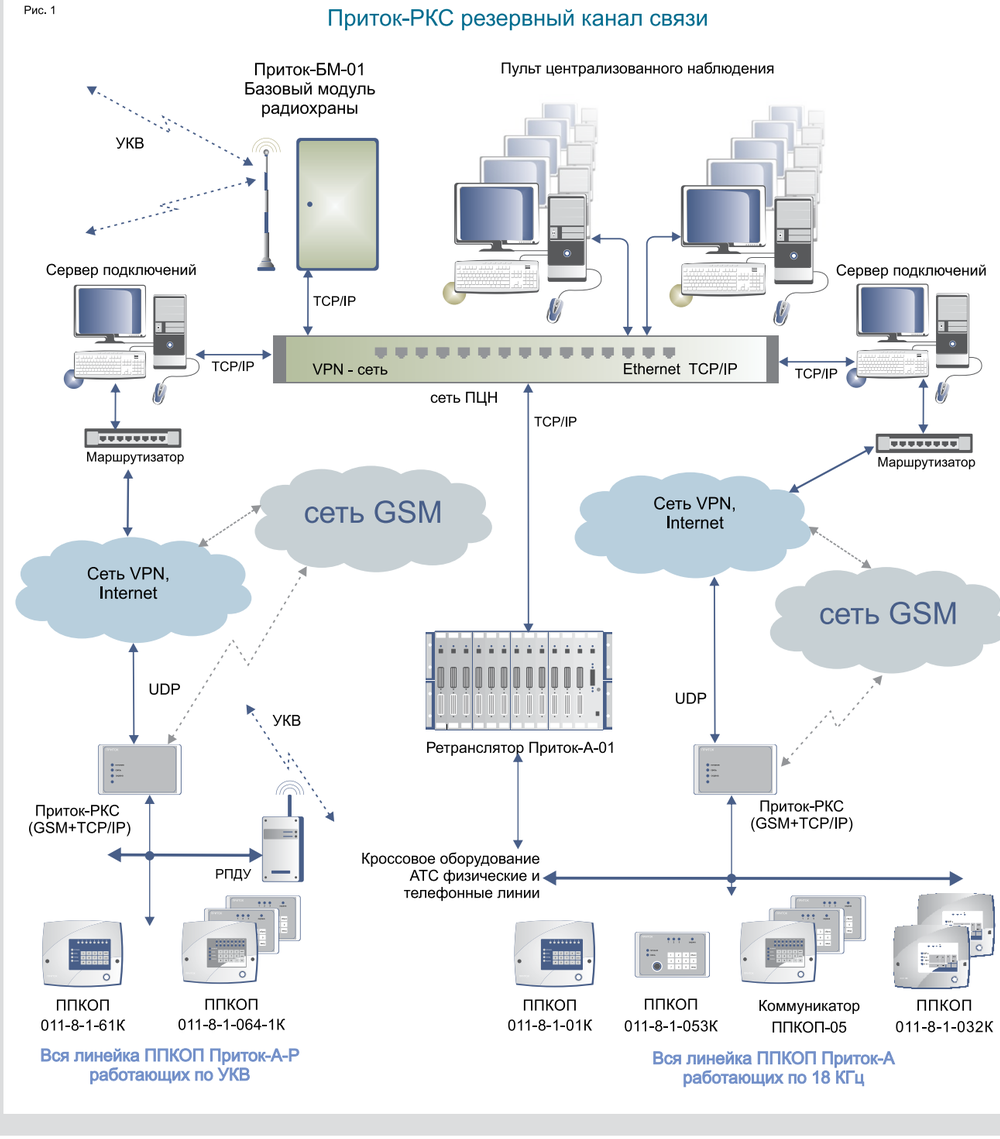


Приток-МПО имеет сертификат соответствия МВД № МВД.RU.0001.Н00563.
Работа Приток-МПО в составе ИС Приток-А позволяет организовывать несколько центров мониторинга, в том числе и работающих через Web-узлы. АРМы ПЦН, входящие в состав одной системы, позволяют объединить работу различных подразделений МВД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

Рис. 1



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 в 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 тунель 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-А-Ф-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 радиобазы) 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-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.

В течение 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 подсистема 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 XP Professional, Windows Server 2003, 2008 с установленным специальным ПО, обеспечивающим работу радара РЛС Orwell-R.

В составе ИС Приток-А проверена работа до десяти **Серверов-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
- программное обеспечение ИС Приток-А 3.7 с поддержкой службы Приток-РЛС-Сервер
- программно-аппаратные средства подсистемы Приток-РЛС

Полностью свои достоинства подсистема Приток-РЛС проявляет при совместной работе с уже существующими подсистемами Приток-Видео, Приток-МПО и Приток-СКД.

Подсистема Приток-РЛС включает в себя:

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

Количество компонентов в составе подсистемы выбирается в зависимости от конфигурации и размеров охраняемого объекта.

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;
- поддержку контроля ядром системы каналов связи с Сервером-РЛС
- выдачу извещения на АРМ дежурного об обрывах / восстанавлениях 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.

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

Уровень электромагнитного излучения Радара соответствует действующим в РФ санитарным правилам и нормам для использования системы в населенных пунктах.

Клиентский компьютер (АРМ)

Клиентский компьютер — это АРМ (рабочая станция) из состава ИС Приток-А, на который установлено дополнительное ПО подсистемы Приток-РЛС. Доступ к данным подсистемы Приток-РЛС осуществляется по системе паролей, существующей в ИС Приток-А. Количество клиентских компьютеров (АРМ), получающих информацию от одного Сервера-РЛС, в системе не ограничено.

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.

Для включения в состав ИС Приток-А новой подсистемы в первую очередь потребовалось доработать ПО, обеспечивающее конфигурирование новой системы – это АРМ Конфигуратор.

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

- создание единого дерева конфигурации оборудования всех подсистем
- настройку и сохранение параметров оборудования в единой БД
- 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.

Основные технические характеристики Радара:

- Режимы излучения – когерентный импульсный или ЛЧМ
- 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
- «Слепая зона» составляет: в импульсном режиме — 50 м, в режиме ЛЧМ — 160 м
- Ошибка измерения дальности не превышает 2 м
- Ошибка измерения азимута не превышает 0,6 град
- Ошибка измерения радиальной скорости не превышает 0,15 м/с
- Угловая скорость обзора составляет от 10 до 40 град/с
- Электропитание Радара осуществляется от сети переменного тока напряжением 220 В
- Потребляемая мощность составляет не более 80 Вт
- Диапазон рабочих температур от -50 до + 50 градусов С

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)
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.

• 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

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.

В состав подсистемы Приток-Видео обязательно входят:

• видеосерверы Domination (с поддержкой аналоговых или IP-видеокамер)
• видеокамеры или тепловизоры, подключаемые к видеосерверам Domination
• Серверное и клиентское ПО Domination
• ПО подсистемы **Приток-Видео ИС Приток-А 3.7**

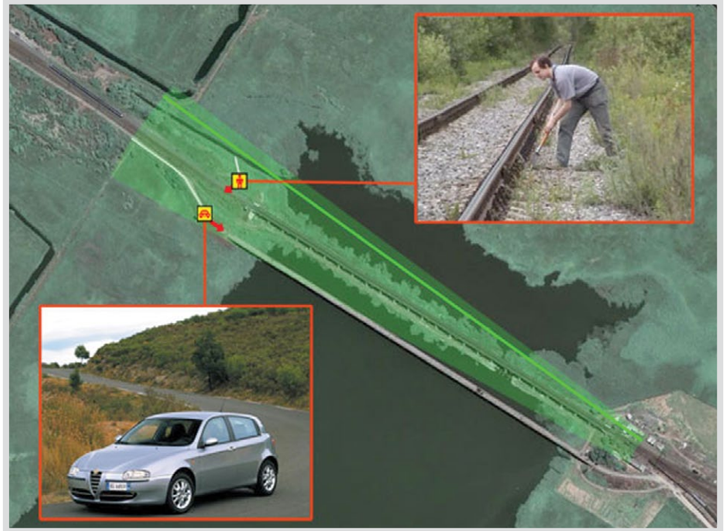
Подсистема Приток-Видео обеспечивает:

• 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

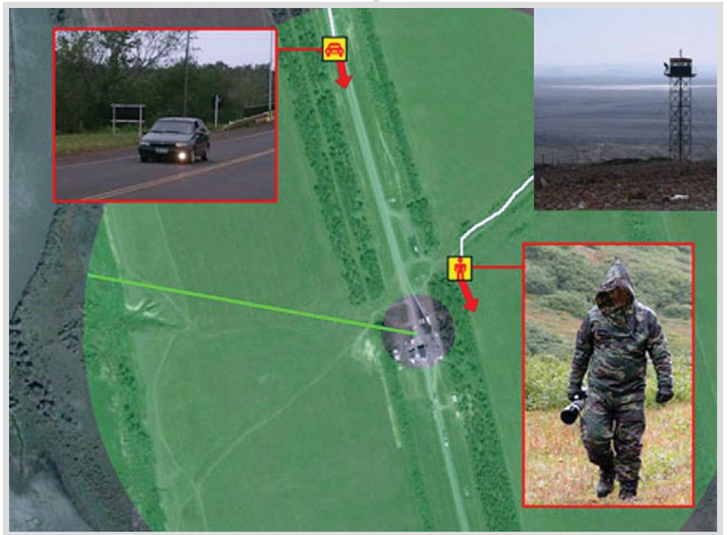
И в заключение, все перечисленные выше возможности подсистемы Приток-РЛС в тесном взаимодействии с подсистемами Приток-Видео, Приток-МПО и Приток-СКД позволяют организовать комплексные системы безопасности для охраны и мониторинга, такие как:

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

охрана железных дорог и железнодорожного транспорта

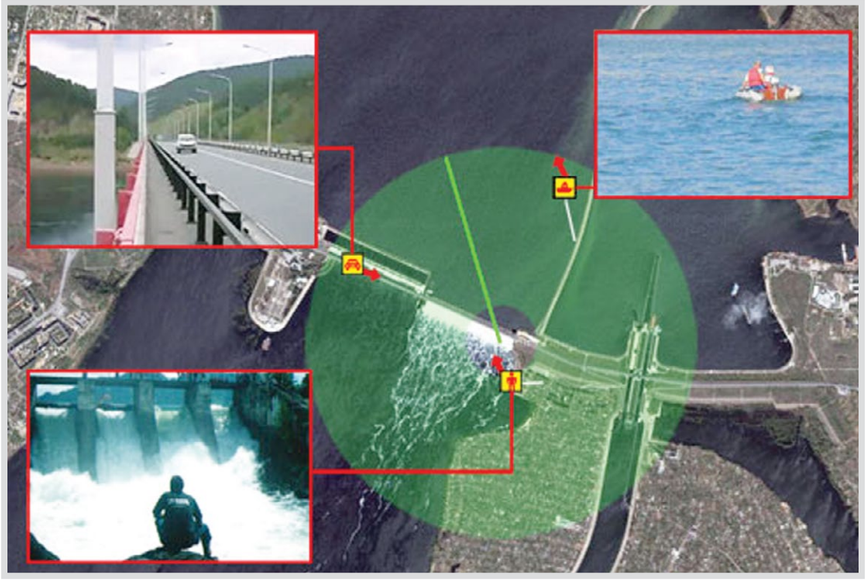


охрана пограничных и контрольно-пропускных пунктов



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.

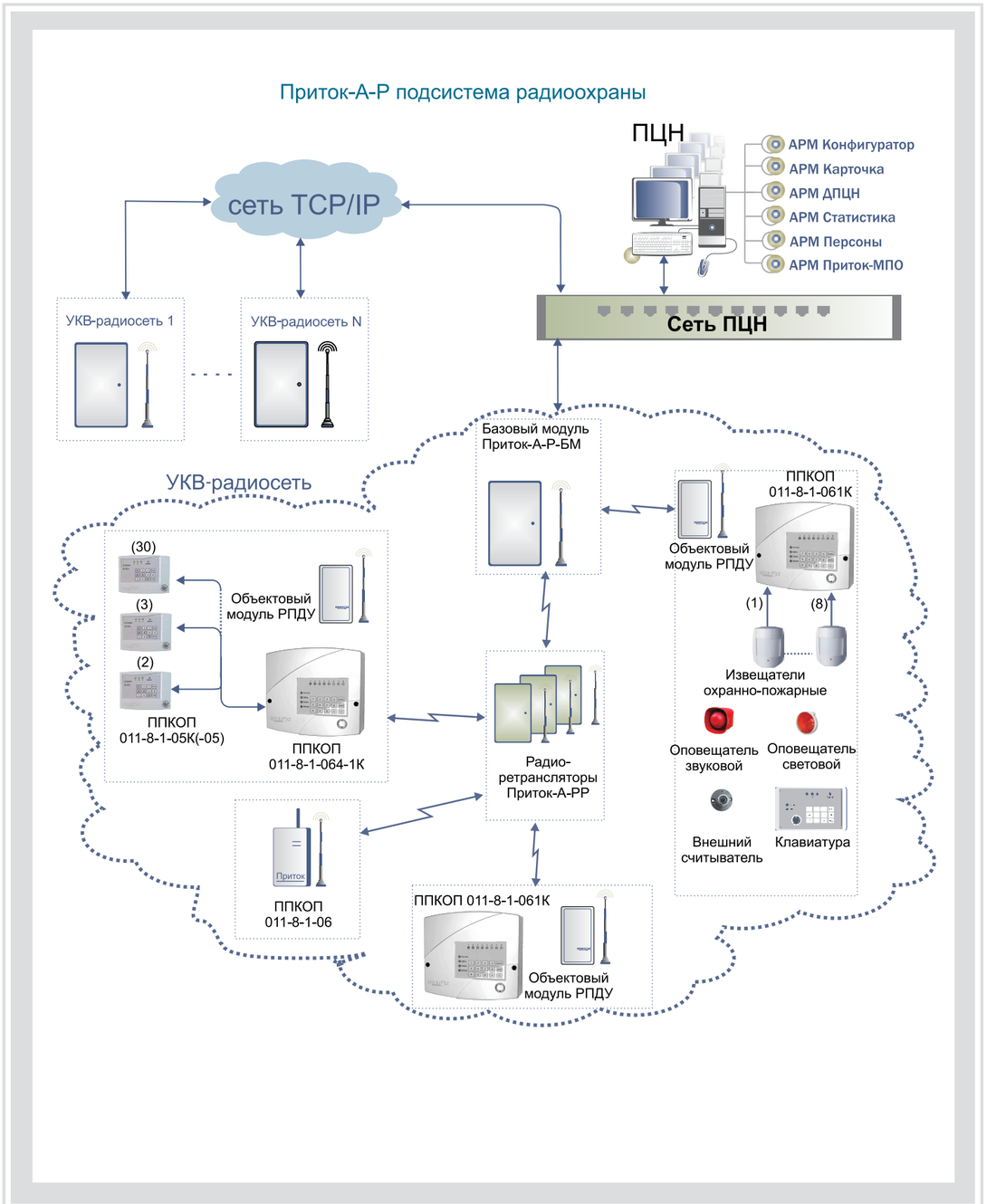
Двусторонняя связь с контролем канала АРМ ПЦН — ППКОП обеспечивается тем, что и в БМ и в РПДУ устанавливаются приемопередатчики. Алгоритм постоянного опроса состояния ППКОП и обмен данными с ППКОП напрямую или через ретранслятор обеспечивает контроллер БМ.

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

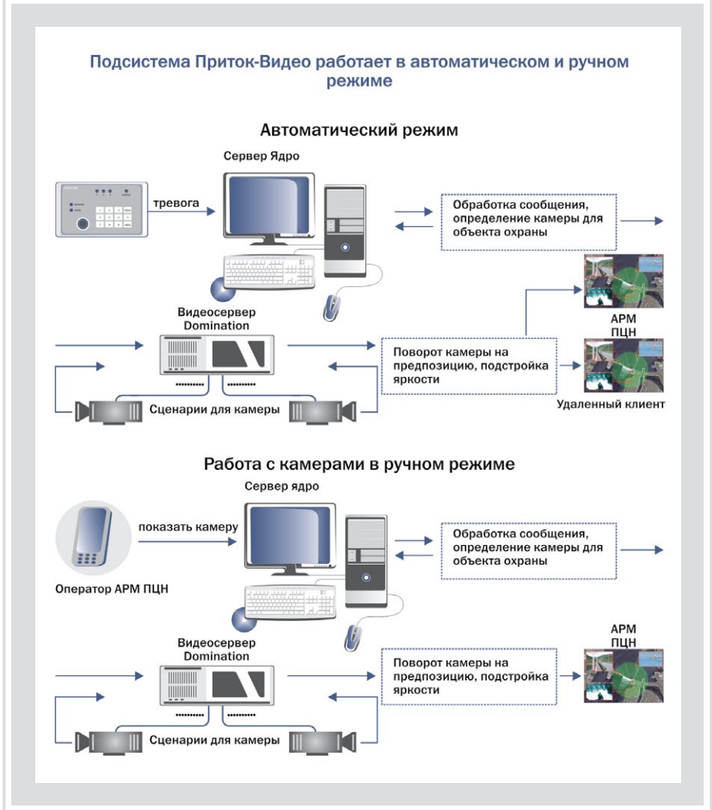
- диапазоны рабочих частот — 136-174 и 430-470 МГц
- количество подсистем на разных частотах не ограничено
- двусторонний, имитостойкий протокол обмена АРМ ПЦН — объект с контролем канала «свой-чужой»
- автоматизированная тактика постановки/снятия с охраны с применением электронных идентификаторов и 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.

ППКОП-010

Коммуникатор

Релейный расширитель

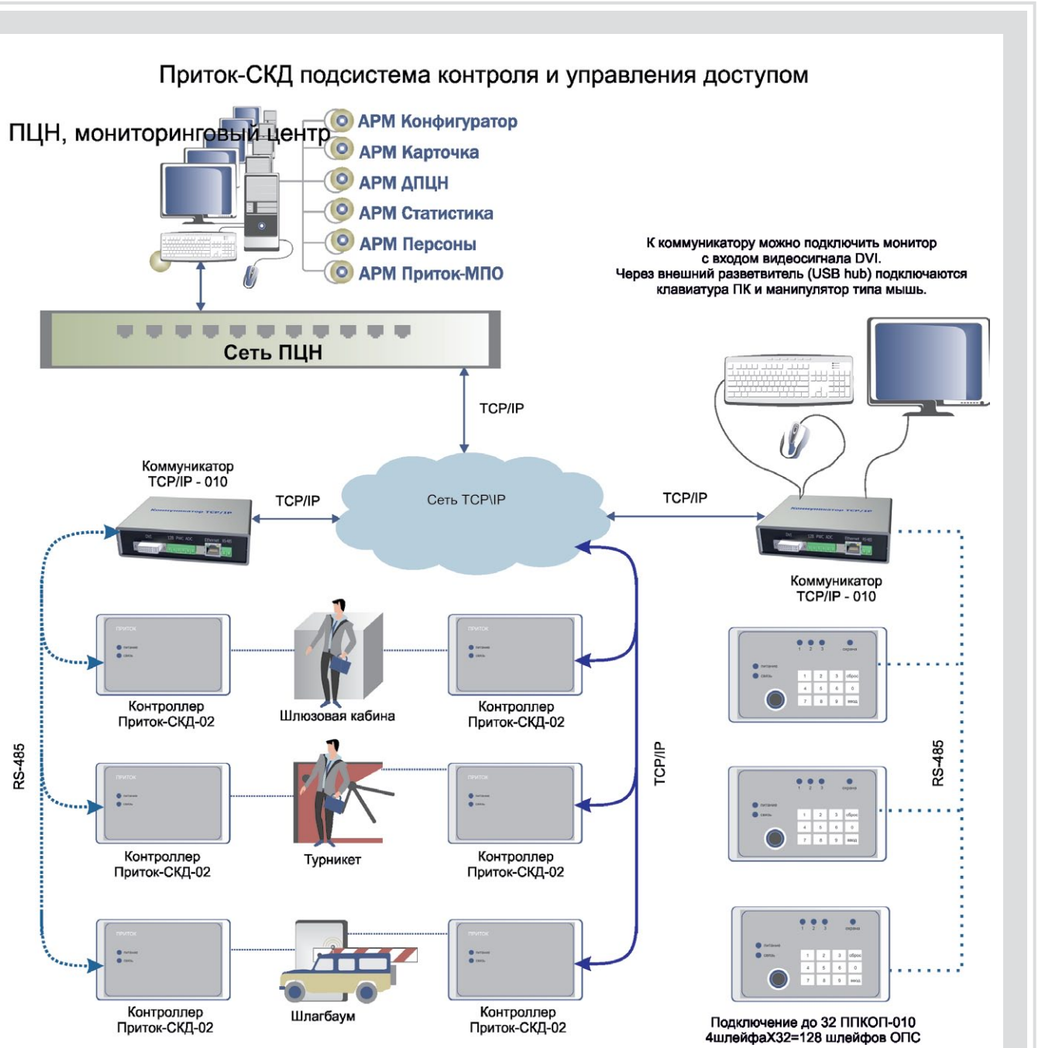
КСКД

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 собенности 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

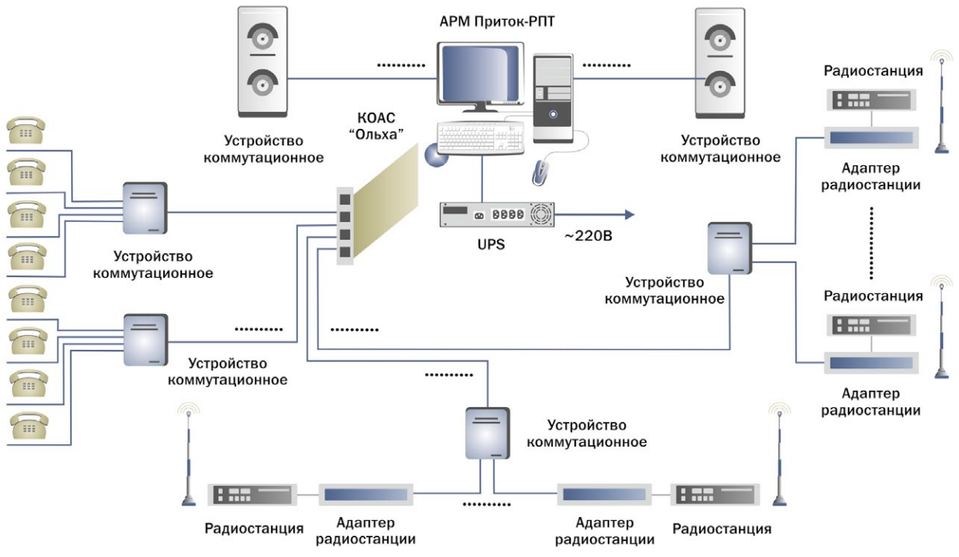
- Включение записи по радиоканалу осуществляется при появлении речевой информации в канале
- Задержка включения записи программируется (от 0 до 500 мсек.)
- Выключение записи по радиоканалу осуществляется при пропадании речевой информации в канале. Длительность паузы программируется (от 1 до 6 сек.)
- 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.

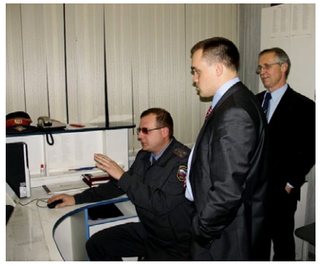
Грамотная эксплуатация современных систем безопасности требует глубоких специальных знаний и регулярного обучения

Обучение навыкам работы с применением ИС Приток-А проходит также в Учебно-методическом экспертном центре (УМЭЦ) ФГУ НИЦ «Охрана» МВД РФ в городе Москве 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.

В 2014 году проведено 15 обучающих семинаров. Обучение на них прошли около 770 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



Обучение проводится как на базе самого ОБ «Сократ» в Иркутске, так и в других учебных центрах страны. Например, в Воронежском институте МВД

различных регионов — Иркутской, Челябинской, 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 Института 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

2014
MIPS 2014 — 20-я Московская международная выставка «Охрана, безопасность и противопожарная защита»

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»

Курсы повышения квалификации технических специалистов

Этапы развития и современное состояние

Александр Демин,
начальник сектора отдела №3
НИЦ «Охрана», майор полиции

В связи с 50-летием создания ФКУ НИЦ «Охрана» МВД России в его адрес сказано много добрых слов. Отмечается тот значительный вклад, который коллектив первоначально СКБ ВНИИПО, а затем НИЦ «Охрана» внес в дело обеспечения надежной защиты от криминальных угроз широкого спектра самых разнообразных объектов. Создание собственной научной школы, высокий технический уровень разработок, массовое серийное производство внушительной номенклатуры средств сигнализации (от простейших извещателей до сложных аппаратно-программных комплексов пунктов централизованной охраны), разработка государственных стандартов и руководящих документов в области безопасности — все это является неоспоримой заслугой НИЦ «Охрана». Его 50-летняя деятельность по праву завоевала признание и уважение в службе вневедомственной охраны, производственных коллективах российских предприятий-изготовителей, среди фирм-разработчиков систем безопасности.

Данная статья посвящена еще одному направлению работы НИЦ «Охрана» — обучению и повышению квалификации технических специалистов, которое занимает важное место в деле подготовки кадров для технической службы вневедомственной охраны и других охранных структур.

Обучение технических работников вневедомственной охраны силами специалистов-разработчиков СКБ ВНИИПО берет свое начало с середины 70-х годов прошлого века. Оно было связано с оснащением вневедомственной охраны Советского Союза системами централизованного наблюдения, внедрение которых потребовало от создателей новой техники оказания реальной помощи практическим работникам. Сейчас, спустя многие годы, можно уверенно сказать, что важнейшую, ключевую роль в освоении подразделениями охраны пульта «Центр-М», радиоканальной системы «Стрела-М», автоматизированных систем «Сатурн» и «Циклон» сыграли высокий профессионализм и активная работа по обучению, которую проводили ведущие специалисты СКБ — Жиряков А.И., Баркова Г.М., Лосков Е.Н., Мурашов В.И., Соломанидин Г.Г., Нилов В.И., Гусев В.И., Акимов Е.Е. и другие сотрудники, неоднократно выезжавшие для проведения занятий в различные подразделения охраны Союза ССР.

В последующем организационная форма обучения несколько изменилась. Все чаще учебные семинары стали проводиться на базе заводов-изготовителей СЦН в заранее определенные сроки. Такой подход явился шагом вперед, т.к. вносил упорядоченность по месту и срокам проведения занятий, при этом использовалась учебно-материальная база предприятия. Именно так было организовано обучение по СЦН «Фобос» на заводе ЭП ЦНИТИ (г. Ногинск Московской области) в период 1991 – 1994 г.г. Учебные семинары проводили разработчики уже следующего поколения — Зайцев А.Г., Петрушков С.В., Морозов А.Н. и другие.

Необходимо отметить, что вся работа СКБ ВНИИПО, НИЦ «Охрана» по обучению проводилась в тесном взаимодействии с ГУВО МВД СССР, ГУВО МВД России. Сотрудники Главка не только принимали участие в подготовке того или иного семинара, но и выезжали совместно с разработчиками для проведения занятий в подразделения вневедомственной охраны и на заводы-изготовители. Активно в этом направлении работали Варижкина Н.Н., Лепешкин В.В., Мастеров В.Е., Зонов А.М.

Основополагающую роль в деле дальнейшего развития и совершенствования учебного процесса сыграл приказ НИЦ «Охрана» ВНИИПО МВД России от 06.03.1995г. №2, который положил начало созданию Учебных Курсов. В частности, в нем говорится: «Организовать учебный процесс подготовки, переподготовки и повышения квалификации сотрудников вневедомственной охраны и служб безопасности на базе учебных курсов (УК) НИЦ «Охрана». Руководство деятельностью Учебных Курсов возлагалось на Методический совет, который составили руководящие работники ГУВО МВД России, НИЦ «Охрана» и ВНИИПО МВД России.

В течение довольно короткого периода были успешно решены организационные и организационно-технические вопросы жизнедеятельности и функционирования Учебных Курсов:

- обеспечено регулярное изучение личным составом государственных и частных охранных структур отечественных и зарубежных средств ОПС на основе утверждаемых учебных планов;
- для организации учета подготовленности кадров введен специальный документ, выдаваемый слушателям в случае успешного усвоения материала;
- определены две формы изучения техники ОПС в виде семинаров для повышения квалификации и в виде курсов для молодых специалистов;
- для повышения качества и стимулирования развития учебного процесса введена оплата преподавательского состава;
- расширена тематика обучения в области обеспечения пожарной безопасности;
- укреплена учебно-материальная база Курсов.

Все это показывает, что обучение и повышение квалификации технических специалистов вышло на качественно новый уровень, который в целом способствовал решению задачи обеспечения

Для изучения техники ОПС определены две формы - семинары для повышения квалификации и курсы для молодых специалистов

высокой конкурентоспособности вневедомственной охраны в условиях проходивших в стране социально-экономических преобразований.

В дальнейшем совершенствование учебного процесса осуществлялось в рамках Учебно-методологического экспертного центра (УМЭЦ) НИЦ «Охрана», который был создан по совместному приказу ГУВО МВД России и ВНИИПО МВД России от 22.08.1996г. № 58. Согласно Положению об Учебно-методологическом экспертном центре его задачами являлись:

- организация дополнительного профессионального образования (повышение квалификации) работников подразделений вневедомственной охраны, а также других граждан Российской Федерации;
- обеспечение регулярного изучения особенностей эксплуатации инженерных и технических средств охранно-пожарной сигнализации;
- сертификации (аттестации) физических лиц для осуществления работ по проектированию, монтажу, наладке, ремонту и эксплуатации (техническому обслуживанию) инженерных и технических средств охраны, охранно-пожарной и пожарной сигнализации.

Руководителем УМЭЦ была назначена к.т.н. Кирюхина Т.Г., костяк преподавательского коллектива составили опытнейшие специалисты — к.т.н. Гудков А.В., Нилов В.И., Морозов А.Я., к.т.н. Антоненко А.А. Была проделана большая работа для получения необходимых лицензий на предоставление образовательных услуг. Обучение проводилось по следующим основным направлениям:

- Проектирование, монтаж и эксплуатация технических средств охраны и охранно-пожарной сигнализации.
- Особенности построения и использования приборов на основе контрольных панелей.
- Радиосистемы передачи извещений.

Начиная с 2000 г. наступил период интенсивного развития УМЭЦ (руководитель — к.т.н. Цыцурин С.Л.) и, соответственно, обновления учебного процесса. Состояние рынка средств безопасности, появление на нем все новой техники обусловило необходимость расширения числа учебных программ, введения в учебный процесс новых семинаров, отвечающих требованиям времени. При этом требовалось сохранить преемственность по отношению к ранее наработанному учебному материалу, внеся в него соответствующие коррективы.

По вновь разработанным программам стало проводиться обучение по интегрированным системам безопасности, системам охранного телевидения, системам контроля и управления доступом, аппаратно-программным комплексам централизованного наблюдения («Ахтуба», «Юпитер», «Альтаир», «Приток» и др.). Получила развитие программа обучения по радиосистемам передачи извещений, в которую были включены средства мониторинга подвижных объектов. Значительно расширилось и обновилось содержание курса по проектированию за счет включения систем дымоудаления, молниезащиты, оповещения и эвакуации при пожаре. Организован новый семинар, связанный с автоматизацией работ по проектированию технических средств. В связи с созданием структуры ФГУП «Охрана» МВД России было обеспечено обучение специалистов для его филиалов по программе «Подготовка электромонтеров по монтажу и эксплуатации технических средств охраны, пожарной и охранно-пожарной сигнализации».

Наряду с этим были и другие нововведения. В соответствии с приказом ГУВО МВД России от 14.12.1999 г. № 119 организован семинар «Охрана труда», который стал особенно актуален в связи с введением в феврале 2002 г. нового Трудового Кодекса Российской Федерации. По предложениям слушателей разработана программа семинара «Основы договорно-правовой деятельности», на котором рассматриваются нормативно-правовые акты, относящиеся к компетенции вневедомственной охраны, практические вопросы договорной и претензионно-исковой деятельности. В течение нескольких лет данный семинар показал свою востребованность. В развитие приказа Министерства образования и науки Российской Федерации от 06.05.2005 г. № 137 «Об использовании дистанционных образовательных технологий» введена дистанционная форма обучения, которая позволяет повысить уровень профессиональной подготовки без отрыва от производства и сократить расходы на обучение, что особенно важно для подразделений отдаленных регионов России.

Претерпел изменения и преподавательский состав УМЭЦ, который пополнили к.т.н. Цыцурин С.Л., Воронков С.Н., Бовин В.Л., Дубровин В.А., Анюхин С.Г., Малемин Н.В. Положительно сказалось привлечение к проведению семинаров признанных авторитетов в области средств безопасности к.т.н. Кокшина В.В., Хомякова Б.И., д.т.н. Членова А.Н., работавших в других организациях.

Заметный вклад в дело подготовки технических специалистов внес Новосибирский филиал НИЦ «Охрана», в Учебно-методическом отделе (УМО) которого в период 2005-2011 г.г. обучались представители Уральского, Сибирского и Дальневосточного федеральных округов. Усилиями Мамаева А.А., Мельника О.В. и других специалистов Новосибирского филиала за короткий срок был достигнут высокий уровень профессиональной подготовки персонала.

В общей сложности за период 1995–2012 г.г. в УМЭЦ НИЦ «Охрана» и УМО Новосибирского филиала прошли профессиональную подготовку и повышение квалификации около 12-и тысяч сотрудников подразделений вневедомственной охраны и различных негосударственных охранных структур.

В настоящее время, после преобразований в рамках общего реформирования МВД России, обучение вновь сконцентрировано на базе НИЦ «Охрана» (отдел № 3, начальник отдела — полковник полиции, к.т.н. Цыцурин С.Л., сектор обучения и методологического обеспечения новых средств защиты объектов, начальник сектора - майор полиции Демин А.А.). В распоряжении Учебных курсов имеются два специально оборудованных помещения. В актовом зале НИЦ «Охрана», где проводятся лекционные занятия, размещены восемь демонстрационных стендов, на которых представлены технические характеристики и показана тактика применения средств тревожной сигнализации, широкой гаммы извещателей с различными физическими принципами обнаружения проникновения — магнитоконтактных, вибрационных, оптико-электронных, комбинированных, совмещенных и других, а также систем централизованного наблюдения. Вторым помещением является учебный класс на 22 места, который оборудован стендами с действующей аппаратурой. Здесь проходят семинарские занятия, на которых слушатели овладевают практическими навыками работы с такими системами, как «Альтаир», «Атлас-20», «Приток», «Юпитер», «Ахтуба», «Протон», «Орион», «Виста». В учебном процессе широко используются средства оргтехники, учебно-методические пособия и техническая литература.

«Концепция развития вневедомственной охраны...» нацеливает на дальнейшее наращивание усилий по обучению и повышению квалификации технических специалистов подразделений ВО

В целом обучение осуществляется по 17-и направлениям. Наряду с уже упомянутыми программами введены две новых: «Системы обеспечения комплексной безопасности и особенности их функционирования по современным каналам связи», «Экспертная оценка состояния технической укрепленности и безопасности различных объектов (Противокриминальная и антитеррористическая деятельность)». Полный список учебных программ и другую информацию об Учебных курсах можно получить на официальном сайте ФКУ НИЦ «Охрана» МВД России: www.nicohrana.ru.

В завершении статьи хочется сказать, что «Концепция развития вневедомственной охраны полиции органов внутренних дел Российской Федерации на среднесрочную перспективу (2012–2015 годы)» нацеливает на дальнейшее наращивание усилий в деле обучения и повышения квалификации технических специалистов подразделений вневедомственной охраны на базе Учебных курсов НИЦ «Охрана».

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:

- Монтаж, техническое обслуживание и ремонт систем пожаротушения и их элементов, включая диспетчеризацию и проведение пусконаладочных работ;
- Монтаж, техническое обслуживание и ремонт систем оповещения о пожаре и управления эвакуацией при пожаре и их элементов, включая диспетчеризацию и проведение пусконаладочных работ;
- Монтаж, техническое обслуживание и ремонт систем противопожарного водоснабжения и их элементов, включая диспетчеризацию и проведение пусконаладочных работ;
- Монтаж, техническое обслуживание и ремонт систем оповещения о пожаре при пожаре и их элементов, включая диспетчеризацию и проведение пусконаладочных работ;
- Монтаж, техническое обслуживание и ремонт противопожарных занавесов и завес, включая диспетчеризацию и проведение пусконаладочных работ;
- Выполнение работ по огнезащите материалов, изделий и конструкций.

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 МВД РФ № МВД RU.0001.Н00563** на Систему мониторинга подвижных объектов Приток-МПО

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
Изготовление производных материалов аэросъемочных работ в фотографическом и цифровом (электронном) видах без выполнения самим аэросъемочных работ с помощью летательных аппаратов

2.) 2.3.0.0.0
Изготовление производных материалов космических съемок в фотографическом и цифровом (электронном) видах

3.) 5.4.0.0.0
Составление, обновление, подготовка к изданию, издание, копирование в графическом, цифровом (электронном) и иных видах тематических (надотровых, туристских, спортивных, экономических, почвенных и др.) карт, планов и атласов специального назначения

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

Основной государственный регистрационный номер записи о государственной регистрации юридического лица или индивидуального предпринимателя: 1033801007690

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**

Как стать партнером ОБ «СОКРАТ»

Сеть представительств и дилеров

«Хочешь быть сильным — уважай других и дружи!» — одно из главных составляющих успеха нашего предприятия

Для успешной деятельности предприятия производителя, для увеличения объемов реализации продукции, привлечения новых потребителей продукции и приближения к потребителям услуг по внедрению, обслуживанию и ремонту продукции как в гарантийный период, так и после его окончания необходимо создание и развитие сети представителей и дилеров (СПД).

На протяжении 25 лет ООО ОБ «СОКРАТ» стремится к созданию идеальной, на наш взгляд, сети представительств и дилеров.

Мы думаем, как и все «наивные» участники предпринимательской деятельности, что для этого необходимо наметить первоначальный план:

1. Сформулировать стратегические цели и принципы создания СПД.

2. Произвести подробное описание существующей СПД и технологии реализации продукции.

3. Довести до всех участников (сотрудников ОБ «СОКРАТ» и СПД) эти стратегические цели и принципы развития СПД.

4. Провести подробный экономический анализ деятельности СПД.

5. На основании результатов экономического анализа описать «идеальную», с точки зрения производителя и потребителя, систему реализации продукции, то есть СПД.

6. Произвести оценку затрат на создание «идеальной» СПД.

7. После этого произвести корректировку (исключить несоответствие между существующей и «идеальной») СПД.

Теперь необходимо выполнить намеченный план. Хотя на этом работа не заканчивается.

Сформулировав задачи и реализовав их однажды, нельзя почивать на лаврах. Необходимо добиться, чтобы эти процедуры производились регулярно, с учетом изменения современных условий на рынке.

Все вышеизложенное приводим для того, чтобы постараться ответить на вопрос, который часто задают нам: «Как стать партнером ОБ «СОКРАТ»?»

Можно ответить коротко: «Начинайте работать!»

Но этого недостаточно, и потенциальному партнеру необходимо объяснить, что мы хотим от него.

Партнером (представителем) ОБ «СОКРАТ» могут стать предприятие, частный предприниматель, которые соглашаются с условиями «Договора о сотрудничестве». Его основные положения приведены ниже.

И еще один немаловажный фактор: «Стороны должны честно выполнять условия подписанного договора». Главное, чтобы мотивации сторон совпадали.

Сформулировав стратегию создания и развития сети представительств и дилеров (СПД), ОБ «СОКРАТ» стремится к тому, чтобы в каждом регионе РФ, как правило, был один региональный представитель. В исключительных случаях, с учетом специфики региона (наличие обособленных центров потребления продукции), рекомендаций регионального УВО и других потребителей продукции ОБ «СОКРАТ», а также учитывая другие факторы, в регионе могут создаваться несколько представителей.

Инициатором создания представителя в регионе может быть ОБ «СОКРАТ» или субъект предпринимательской деятельности, желающий стать представителем. Потенциальный партнер делает запрос и направляет в адрес ОБ «СОКРАТ» копии следующих документов:

• свидетельства о государственной регистрации;

• свидетельства о постановке на налоговый учет;

• документ, подтверждающий право заниматься деятельностью, связанной с монтажом, эксплуатацией и обслуживанием средств ОПС;

• другие документы и сведения, подтверждающие или характеризующие его деятельность.

Решение о создании в регионе первого и единственного, или еще одного, представителя принимает заместитель директора по развитию ОБ «СОКРАТ». Он делает это на основании анализа исходных материалов (сведений о предполагаемом партнере), предложений от регионального УВО или других потребителей продукции. И после этого потенциальному партнеру направляется проект договора «О сотрудничестве», основные положения которого заключаются в следующем.

Представитель обязан:

1. Проводить маркетинговые исследования в регионе с целью всестороннего продвижения продукции ОБ «СОКРАТ» на рынке указанного региона.

2. Ссылаться на ОБ «СОКРАТ» и его продукцию в своих рекламных и информационных материалах.

3. Проводить реализацию, монтажные и пусконаладочные работы и ввод в эксплуатацию продукции ОБ «СОКРАТ», указанной в прайс-листе. Всесторонне содействовать расширению рынка сбыта и увеличению объемов реализации продукции.

4. В случае необходимости реализации, а также монтажа и пусконаладки продукции с измененными составом и характеристиками, такие изменения согласовывать с ОБ «СОКРАТ» в письменном виде.

5. Вести учет объемов реализованной и введенной в эксплуатацию продукции и регулярно, в соответствии с правилами, предоставлять в ОБ «СОКРАТ» сведения

об объемах реализации и ввода в эксплуатацию продукции в регионе.

6. Проводить техническое обслуживание и сопровождение, гарантийный и послегарантийный ремонт реализованной и введенной в эксплуатацию продукции. В том числе, проводить техническое обслуживание и сопровождение, гарантийный и послегарантийный ремонт и продукции, поставляемой ОБ «СОКРАТ» в регион по государственному контракту, в адрес УВО, ФГУП «Охрана», а также другим крупным корпоративным клиентам. При этом региональный представитель обязан заключить с данными контрагентами от своего имени договор на выполнение вышеуказанных работ.

7. Предоставлять в ОБ «СОКРАТ» данные о проведенных гарантийных ремонтах с указанием причин ремонта и перечнем установленных деталей, запасных частей и элементов.

8. Проводить анализ результатов эксплуатации продукции и не реже одного раза в полгода направлять в ОБ «СОКРАТ» предложения по улучшению ее технических характеристик и потребительских свойств. Участвовать в подготовке и согласовании технических заданий (ТЗ) на вновь разрабатываемую и модернизируемую продукцию.

9. Проводить обучение в ОБ «СОКРАТ» своих специалистов по вопросам эксплуатации и ремонта продукции. Иметь полный комплект рекламно-информационных материалов эксплуатационной и документации на продукцию ОБ «СОКРАТ» в объемах, необходимых для выполнения своих обязанностей и реализации своих прав.

10. Выполнять экономические условия сотрудничества, в том числе:

- проводить реализацию продукции ОБ «СОКРАТ» по специально согласованным ценам;
- не допускать задолженности по оплате полученной продукции сверх установленных норм.

Согласие потенциального партнера с перечисленными обязательствами означает, что ОБ «СОКРАТ» поручает, а представитель принимает на себя обязательства по проведению работ, связанных с реализацией, внедрением и эксплуатацией программно-аппаратных средств Интегрированной системы охранно-пожарной сигнализации Приток-А (в дальнейшем «продукция ОБ «СОКРАТ»). И в соответствии с условиями договора «О сотрудничестве» становится официальным представителем ОБ «СОКРАТ» в указываемом регионе.

Получив в соответствии с условиями «Договора о сотрудничестве» статус официального представителя, партнер начинает работать: получать и реализовывать продукцию ОБ «СОКРАТ» по специальной цене и иметь установленные в этом случае скидки.

Поставка продукции ОБ «СОКРАТ» в адрес представителей производится на льготных условиях по специальной согласованной цене.

При подписании договора, как правило, величина скидки устанавливается на уровне минимальной и может изменяться в зависимости от объемов реализованной продукции.

Если в течение первого квартала работы представитель справляется с экономическими показателями, установленными для него при заключении договора «О сотрудничестве», то он вносится в официальный реестр представителей ОБ «СОКРАТ».

Реестр представителей ОБ «СОКРАТ» (в дальнейшем — реестр) является документом, определяющим состав сети представителей ОБ «СОКРАТ», содержащим основные и дополнительные сведения о представителях и дилерах.

Реестр ведется в ОБ «СОКРАТ» специалистом (экономистом), отвечающим за организацию деятельности СПД. Он публикуется на официальном сайте ОБ «СОКРАТ» и в других рекламно-информационных материалах.

Реестр содержит информацию о представителях и состоит из разделов:

- Основные сведения
- Сведения о технической вооруженности
- Сведения о наличии лицензий на виды деятельности
- Сведения о кадровом составе и квалификации специалистов
- Экономические показатели деятельности

Количество разделов и их содержание могут изменяться в зависимости от изменения показателей деятельности СПД.
Реестр и оригиналы других документов (договоры, копии свидетельств и лицензий и т.д.), относящихся к организации деятельности СПД, хранятся в бухгалтерии ОБ «СОКРАТ».

Курирует работу представительств и дилеров заместитель директора по развитию ОБ «Сократ».

Представительства ОБ «СОКРАТ»

АЛТАЙСКИЙ КРАЙ
Барнаул
ООО «Элия»
656015, г. Барнаул, ул. Деповская, 7
Тел.: (385-2) 69-12-75,
(385-2) 69-12-75, 36-76-04
www.eliya.barp.ru

АРХАНГЕЛЬСКАЯ ОБЛАСТЬ
Архангельск
ООО «Техно-Безопасность»
163045, г. Архангельск, ул. Комсомольская, д. 36, литера А, пом. 2-Н
Тел./факс: (8182) 21-22-37, 47-77-09

АМУРСКАЯ ОБЛАСТЬ
Благовещенск
ООО «СТЕЛС»
675000, г. Благовещенск,
ул. Артиллерийская, д.17
Тел./факс: (4162) 519-777, 525-777, 777-888

БАШКОРТОСТАН
Уфа
ООО «АВАКС»
Юр. адрес: 450112, г. Уфа,
ул. Ульяновых, д. 45
Почтовый адрес: 450065,
г. Уфа, ул. Бакалинская, д. 68/6
Тел./факс: (347) 252-39-98,
253-64-52
www.avaksufa.ru

БУРЯТИЯ
Улан-Удэ
ООО ОА «Центр безопасности Эликом»
670024, г. Улан-Удэ, ул. Минина, д. 4а
Тел./факс: (301-2) 46-63-58,
46-66-37

ООО «Охранное агентство Дозор»
670034, г. Улан-Удэ, 50 лет Октября пр-т, д. 13
Тел./факс:(3012) 44-82-11, 55-39-13

ООО «Контур»
Юр. адрес.: 670024, г. Улан-Удэ, ул. Минина, 4а
Факт. адрес: 670034, г. Улан-Удэ,
ул. Хоца Намсараева, д. 7А
Тел./факс (3012) 52-22-27, 46-63-58

ИП Овчинник Алексей Борисович
Юр. адрес: 670034, г. Улан-Удэ, 50 лет Октября пр-т, д. 27
Факт. адрес:670047, г. Улан-Удэ,
ул. Павлова, 78-105
Тел./факс:(3012) 46-30-55,
55-07-55

ООО «Эликом-плюс»
670034, г. Улан-Удэ, 50 лет Октября пр-т, д. 27
Тел./факс:(3012) 46-30-55, 55-07-55

ВОЛГОГРАДСКАЯ ОБЛАСТЬ
Волгоград
ООО «Подмосковье»
400123, г. Волгоград,
ул. Маршала Еременко, 21
Тел./факс: (8442) 73-65-06

ВОЛОГОДСКАЯ ОБЛАСТЬ
Вологда
ООО «Система безопасности»
160012, г. Вологда, ул. Козленская,
д. 83, оф. 1
Тел./факс: (8172) 75-21-33, 50-05-90

ИП Коротков С.В.
160901, г. Вологда, ул. Сокольская,
д. 58-А, кв. 11
Тел./факс: (8172) 75-21-33, 55-98-01

Череповец
ООО «Технический центр Системы телемеханики»
Юр. адрес: 162600, Череповец,
пр-т Строителей, д. 28, кор. А, кв. 11
Факт. адрес: 162600, Череповец, пр-т Строителей, д. 28а, офис 125
Тел./факс: (820-2) 22-38-43,
22-33-83

ВОРОНЕЖСКАЯ ОБЛАСТЬ
Воронеж
ООО «Академия безопасности»
394026, г. Воронеж, пр-т Труда, д. 39
Тел./факс: (473) 234-39-30,
234-39-31
http://абворонеж.рф

ЕВРЕЙСКАЯ АВТОНОМНАЯ ОБЛАСТЬ
Биробиджан
ООО «Центр Безопасности»
ЕАО, г. Биробиджан, ул. Постышева, дом 6, офис 7
Тел./факс: 8(42622) 21-444,
8-914-818-62-72
E-mail: safety_centre@e-mail.ru

ИРКУТСКАЯ ОБЛАСТЬ
Ангарск
ООО «Электрон»
665813, г. Ангарск, Ленинградский просп., д. 6, кор. А, оф. 301
Тел./факс: (395-5) 56-52-25,
67-62-71, 56-32-02

ООО «Полином»
665813, г. Ангарск, 80 кв-л, дом 3, помещение 2
Тел./факс: (395-5) 52-65-81,
52-45-50

Братск
ООО «Сэйфти»
665708, г. Братск, ул. Коммунальная, д. 21
Тел./факс: (395-3) 41-12-99,
41-50-01
ИП Абрашкина
665708, г. Братск, ул. Коммунальная, д. 21
Тел./факс: (395-3) 41-12-99,
41-50-01

Иркутск
ООО «СОКРАТ-АВТО»
664007, г. Иркутск, ул. Декабрьских событий, д. 109
Тел.: (395-2) 205-492, 211-854

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

ИП Шипагин
Юр. адрес: г. Иркутск, ул. Халтурина, 26-32
Факт. адрес: 664009, г. Иркутск,
ул. Ширямова, д. 22
Тел./факс: (3952) 211-777 (доп. 207)

ООО Охранное предприятие «ИркутскЭнерго»
Юр. адрес: 664000, г. Иркутск,
ул. Сухэ-Батора, 3
Факт.адрес: 664025, г. Иркутск-25, а/я 220
Тел./факс: (3952) 793-698

ЗАО «ИНЭКС-ГРУПП-СЕРВИС»
664007, г. Иркутск, ул. Партизанская, 28 В
Тел./факс: (3952) 707-607

ПБОЮЛ Блинов Владимир Павлович
664033, г. Иркутск, ул. Лермонтова, д. 265-1
664025, г. Иркутск, ул. Ленина, д. 6, оф. 3
Тел./факс: (3952) 24-15-57, 20-01-68

ИП Шагалова
664007, г. Иркутск, ул. Ямская, д. 4
Тел./факс: (3952) 207-479, 607-420

Усолье-Сибирское
ПБОЮЛ Блинов Владимир Павлович
Юр. адрес: 665451,
г. Усолье-Сибирское, у
л. Машиностроителей, 4А-21
Факт. адрес: 665451,
г. Усолье-Сибирское, рынок «Элегант-3» (СтройДвор), пав. 218
Почт. адрес: 665460,
г. Усолье-Сибирское-10, а/я 75
Тел./факс:(3952) 24-15-57, 20-01-68

Слюдянка
ИП Кузьмина Т.Н.
665904, г. Слюдянка, ул. Ленина, 3Б-8
Тел./факс: (395-44) 519-39, моб: 8-914-887-57-15, 8-914-887-57-15

КЕМЕРОВСКАЯ ОБЛАСТЬ
Кемерово
Торговый дом «Системы безопасности»
650025, г. Кемерово, ул. Чкалова, д. 4
Тел./факс: (384-2) 45-23-58,
45-23-59

ИП Валетов С.И.
650025, г. Кемерово, ул. Чкалова, д. 4
Тел./факс: (384-2) 45-23-59

КОМИ
Сыктывкар
ООО «ЛЕМА»
Юр.адрес: 167023, г. Сыктывкар,
ул. Морозова, д. 100
Факт.адрес: 167000, г. Сыктывкар,
ул. Савина, 4
Тел./факс: (821-2) 22-83-46,
22-83-47, 22-83-49, 22-83-66

ООО «Стандарт безопасности»
167000, г. Сыктывкар, ул. Пушкина,
д. 30/1
Тел./факс: (821-2) 22-84-09,

22-84-08, 24-42-42, 203-501,
203-502

КРАСНОДАРСКИЙ КРАЙ
Краснодар
ООО «Радуга-К»
350042, г. Краснодар, ул. Серова, 50
Тел. /факс (861) 254-28-81

КРАСНОЯРСКИЙ КРАЙ
Красноярск
ИП Сергиенко
Юр. адрес: 660025, г. Красноярск,
ул. Шелковая, 3
Факт. адрес: 660025, г. Красноярск, просп.
имени газеты «Красноярский рабочий»,
113-42
Тел./факс: (391-2) 45-75-35

ООО «Треал Красноярск»
660079, г. Красноярск, ул. Матросова,
30 Л, стр. 11
Тел.: (391) 279-27-92, 279-27-92,
279-22-97, 278-24-79, 278-42-10

КАЗАХСТАН
Павлодар
ТОО «Бизнес-Линк ПВ»
140000, г. Павлодар,
ул. Ак. Сатпаева, 254
Тел./факс: (718-2) 20-22-28,
66-00-00

Алматы
ТОО «Seralex Almaty»
г. Алматы, ул. Ауэзова, д. 82, оф. 606
Тел./факс: 8-701-252-73-15,
8-727-277-52-08

Кокшетау
ИП NOVICAMSEVER
г. Кокшетау, ул. Горького, д. 65А, кв.4
Тел./факс: 8-7162-25-24-24,
8-701-959-34-42,
25-60-06
Караганда
ТОО «Novicam-Karaganda»
г. Караганда ул. Пригородная, 3/2
Тел./факс: 8-7212-56-06-01,
8-777-570-88-55

Астана
ТОО «ГК KAZKAT»
г. Астана, ул. Достык, д. 5, офис 63
(ЖК «Северное Сияние»)
Тел./факс: 8-7172-75-50-90,
8-701-324-54-79

КАБАРДИНО-БАЛКАРИЯ РЕСПУБЛИКА
Прохладный
ООО ЧОП «Капитал-Инвест-Охрана»
361045, Россия, г. Прохладный,
ул. Боронтова, д. 99
Тел./факс: (866-31) 47-1-42

КАМЧАТСКИЙ КРАЙ
Петропавловск-Камчатский
ООО Охранное предприятие
«Альфа Безопасность»
683031,
г. Петропавловск-Камчатский,
ул. Топоркова, 1/1, оф. 01
Тел./факс: (8142)76-93-59, 57-62-39

КАРЕЛИЯ
Петрозаводск
ООО «Нордспецавтоматика плюс»
185005, г. Петрозаводск, ул. Льва Толсто-
го, 22 (пом. 33)
Тел./факс: (4152) 22-72-72,
ф. 22-71-71

КАЛМЫКИЯ
Элиста
ООО «Сократ-Юг»
Юр. адрес: 358000, г. Элиста, 1 мкр, д. 1,
к. 1
Факт. адрес: 358014, г. Элиста, 6 мкр, д.
22, кв. 43
Тел./факс: 8-927-646-30-00,
8-961-546-10-15, 8-961-546-10-15

КИРОВСКАЯ ОБЛАСТЬ
Киров
ООО «Щит»
Юр. адрес: 610035, г. Киров,
ул. Комсомольская, д. 63
Тел./факс: (8332) 705-557, 777-335

КОСТРОМСКАЯ ОБЛАСТЬ
Кострома
ООО «Визит»
г. Кострома, ул. Комсомольская, 48/16
Тел./факс: (4942) 37-30-03, 37-30-02

ЛИПЕЦКАЯ ОБЛАСТЬ
Липецк
ООО «Приток-Липецк Сервис»
398036, г. Липецк, б-р Шубина, 8а - 46
Тел. моб.: 8-904-692-33-20,
8-904-692-33-20

МАГАДАНСКАЯ ОБЛАСТЬ
Магадан
ОП «Ягуар»
685000, г. Магадан, пер. 3-й
Транспортный, 12
Тел.: (413-26) 2-39-86,
(413-26) 2-39-86, 3-08-10

МОСКОВСКАЯ ОБЛАСТЬ
Москва
Московское представительство
ООО Охранное бюро «СОКРАТ»
ИП Бухвалов Георгий Юрьевич
117405, г. Москва, ул. Дорожная,
д. 60 Б, офис 07
Тел./факс: (499)558-01-12,
моб: 926-693-17-00
e-mail: sokratm@mail.ru

МОРДОВИЯ
Саранск
ООО «ЦАНГ»
430030, г. Саранск, ул. Титова, 2а, стр. 2
Тел./факс: 8(8342) 22-47-77

НОВОСИБИРСКАЯ ОБЛАСТЬ
Новосибирск
ЗАО Корпорация «Грумант»
630049, г. Новосибирск,
ул. Кропоткина, 92/3
Тел./факс: (383)210-52-53,
226-75-41,
227-27-96, 216-60-60

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

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

ОМСКАЯ ОБЛАСТЬ
Омск
ООО «Союз-Сервис»
Почт. адрес: 644074, г. Омск,
пр-т Комарова, д. 15, корп. 1, оф. 2-П
Тел.: (38-12) 21-51-02,
21-51-02, 70-36-38 , 70-35-07

ООО «Системы контроля и безопасности»
(ООО «СКБ»)
Юр. и почтовый адрес: 644076,
г. Омск, ул. Петра Осминина, 13, кв. 64
Факт. адрес: 644065, г. Омск,
ул. Нефтезаводская, д. 38Е,
корпус 1, офис 4
Тел.: (3812) 67-31-50, (3812)
67-31-50,
факс: (3812) 66-87-19

ПЕРМСКИЙ КРАЙ
Пермь
ИП Сивкова Олеся Вадимовна
Юр. адрес: 614000, г. Пермь,
ул. Быстрых, д.14, кв.14
Тел./факс: (342) 220-67-70,
доб 123, 323

ООО «Аксилиум»
614015, г. Пермь, ул. Краснова, д. 24,
корпус 1
Тел./факс: (342) 220 -31 80,
220-31-76
info@aks-sb.ru
www.aks-sb.ru

ПРИМОРСКИЙ КРАЙ
Владивосток
ООО «Сократ-Прим»
690014, г. Владивосток,
ул. Всеволода-Сибирцева, 79
Тел./факс: 8 (423) 260-60-02,
260-59-49, 226-63-66

Спасск-Дальний
ООО «Приморавтоматика»
Адрес: 692239, г. Спасск-Дальний,
ул. Коммунаров, д. 1В
Тел./факс: (423-52) 3-17-71,
2-87-17

РЕСПУБЛИКА КРЫМ
Симферополь
ЧАО «Охрана-Комплекс-Крым»
295013, г. Симферополь,
Центральный р-он, ул. Миллера, 4
Тел.: 8 (978) 712-17-188,
(978) 712-17-18
М.Т.: +3-80-50-910-89-70,
+3-80-50-910-89-70

РОСТОВСКАЯ ОБЛАСТЬ
Ростов-на-Дону
ЗАО «Системы безопасности»
344022, г. Ростов-на-Дону,
Тел./факс: (863) 299-44-26,
299-44-87

САМАРСКАЯ ОБЛАСТЬ
Самара
ООО «Витаком»
Юр./факт адрес: 443030, г. Самара, ул.
Черноореченская, д. 21 оф. 241
Почтовый адрес: 443030 г. Самара ул.
Черноореченская, д. 21 оф. 308
Тел./факс: (846) 278-45-47,
22-750-22, 8-937-201-79-04,
8-937-201-79-04

САРАТОВСКАЯ ОБЛАСТЬ
Саратов
ООО «Байкал»
410052, г. Саратов, ул. Лунная, д. 44
Тел./факс: (845-2) 35-40-58,
927-623-35-30

ООО «Тех-Защита-М»
410052, г. Саратов, ул. Лунная, д. 44
Тел./факс: (8-8452) 44-61-23,
44-61-24, 35-53-70

САХАЛИНСКАЯ ОБЛАСТЬ
Южно-Сахалинск
ООО «СОВА-2012»
693000, г. Южно-Сахалинск,
пр. Мира, д. 20, оф.10
elmar1950@mail.ru

СВЕРДЛОВСКАЯ ОБЛАСТЬ
Екатеринбург
ООО «Сократ-Урал»
620144, г. Екатеринбург,
ул. Большакова, 153 Б
Тел./факс: (343) 269-31-61,
220-98-03, 355-55-65

Каменск - Уральский
ООО ЧОП «Синара»
623401, г. Каменск-Уральский,
ул. К. Маркса, д. 70
Тел./факс: (3439) 327-433, 32-76-70,
32-72-59

САХА (ЯКУТИЯ)
Якутск
ООО «Спецавтоматика»
Юр. адрес: 677000, г. Якутск,
мкр-н 202, корп. 9, кв. 108.
Факт. адрес: 677013, г. Якутск,
ул. Дежнёва, 72.
Тел./факс: 8(4112)36-38-51,
35-51-85, 35-07-19

Ленск
ООО «Заслон»
678144, РС (Якутия), г. Ленск,
ул. Набережная, 99/35
Тел./факс: (41137)4-30-22, 4-11-77,
8-924-608-77-75, 8-924-608-77-75

СТАВРОПОЛЬСКИЙ КРАЙ
Пятигорск
ООО «Сигнал-Сервис»
357532, г. Пятигорск, ул. 295-ой Стрелко-
вой дивизии, д. 2, офис 402
Тел./факс: (879-3) 38-06-19,
32-13-71, 32-21-92

Ставрополь
ООО «Паритет»
355040, г. Ставрополь,
ул. Тухачевского, д. 21, корпус 2
Тел.: 8-962-445-87-57,
8-962-445-87-57

ТОМСКАЯ ОБЛАСТЬ
Томск
ООО «Торговая компания Синтекс»
634045, г. Томск, ул. Ф.Лыткина,
д. 3, кор. 1
Тел./факс: (3822) 41-50-33,
41-22-81

ООО «Галан»
г. Томск, ул. 79 Гвардейской
Дивизии, 27а
Тел./факс:(3822) 211-757
tel:+73822211757, 729-757

ТЮМЕНСКАЯ ОБЛАСТЬ
Тюмень
ООО «Бруклин»
625019, г. Тюмень, ул. Республики, 206,
стр. 19
Тел.: (3452) 27-19-61, 27-19-61

Ялуторовск
ООО «Спецмонтаж»
627010, Тюменская область,
г. Ялуторовск, ул. Красноармейская, д. 32
Тел./факс: (345-35) 2-05-80,
2-49-80

Тобольск
ООО «Русич»
Юр.адрес:626150, г. Тобольск,
7 мкр, д. 22
Факт. адрес: 626150, г. Тобольск,
9 мкр, дом 17, офис 30
Тел.: (3456) 22-98-00, 22-98-00,
сот. 8-950-497-10-03,
8-950-497-10-03

УДМУРТИЯ
Ижевск
ООО ТД «Антарис+»
426011, г. Ижевск, ул. Холмогорова, 14-
266
Тел./факс: (3412) 65-65-65,
51-05-09, 51-05-06

ИП Широков
426057, г. Ижевск, ул. Свердлова,
дом 18
Тел./факс: (3412) 65-65-65

ООО «Арго-Системы Безопасности»
426011, г. Ижевск, ул. К.Маркса,
д. 440
Тел./факс: (3412) 900-751

УЗБЕКИСТАН
Шахрисабз
ООО «Mars Electronics»
181300, Кашкадарьинская область,
г. Шахрисабз, ул. Ипак йули, 100
Тел./факс: (+99875) 221-08-08,
522-80-00, 221-78-09,
525-75-92

УКРАИНА
Киев
ООО «АБСОЛЮТ-ТЕХНОЦЕНТР»
02049, Украина, г. Киев,
ул. Красногвардейская, 22
Тел.: +38 044 501 60 55,
+38 044 501 60 55,
+38 067 354 16 23,
+38 067 354 16 23

ХАБАРОВСКИЙ КРАЙ
Хабаровск
ООО Торговый дом «Востокавтоматика»
680000, г. Хабаровск, ул. Тургенева, дом
96/1
Тел./факс: (421-2) 42-20-11,
42-20-05

ООО ПКП «Востокавтоматика»
680007, г. Хабаровск, ул. Тургенева, дом
96/1
Тел./факс: (421-2) 48-57-64, 48-57-38

ООО «Сократ ДВ»
Юр. адрес: 680000, г. Хабаровск,
ул. Фрунзе, дом 5
Факт. адрес: 680000, г. Хабаровск,
ул. Панькова, 29Б
Тел./факс: (4212) 29-44-88, 75-89-19

ХАКАСИЯ
Абакан
ООО «Альтернатива»
Юр./почт. адрес: 655017, г. Абакан,
ул. Ленина, 78-14
Факт. адрес: 655000, г. Абакан,
ул. Складская, д. 9, оф. 318
Тел./факс: (3902)21-54-13,
сот. 8-902-996-22-03,
8-902-996-22-03

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ
Челябинск
ООО Компания «Регион-Сервис»
454006, г. Челябинск, ул. Российская,
д. 159-В, оф. 306
Тел.: (3512)71-59-84,
(3512)71-59-84, 64-00-93

ЧИТИНСКАЯ ОБЛАСТЬ
Чита
ООО ОБ «СОКРАТ-Чита»
Юр./факт.адрес: 672022,
г. Чита, пр. Энергостроителей, 4а
Почт. адрес: 672012, г. Чита-12,
а/я 416
Тел./факс: (302-2) 352-473,
351-888

ИП Вольф Е.А.
Юр.адрес: 672012, г. Чита,
ул. Девичья, д. 15
Факт. адрес: 672012, г. Чита,
ул. Костюшко-Григоровича, д. 23
Тел./факс: (302-2) 351-888

ЧУВАШИЯ
Чебоксары
ООО «Роникс»
428022, г.Чебоксары, проезд
Машиностроителей, д. 1
Тел./факс: (8352) 28-26-27, 28-02-88,
23-04-44

ИП Порфирьев Сергей Михайлович
428018, г. Чебоксары,
ул. 2-ая Герцена, д.5

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Карта официальных представительств Охранного бюро «СОКРАТ»

СОКРАТ

ООО Охранное Бюро «СОКРАТ»
664007, 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
www.sokrat.ru