



**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО (НИИР)**

СИСТЕМА УСЛОВНОГО ДОСТУПА “РОСКРИПТ-М”



Основные характеристики системы «Роскрипт-М»

В мировой практике разработаны зарубежные системы условного доступа (СУД), в основном предназначенные для защиты коммерческих интересов. В России специалистами ФГУП НИИРадио разработана отечественная система условного доступа «Роскрипт-М», реализующая ряд принципиально новых решений и алгоритмов, что позволило выполнить требования, учитывающие специфику как федеральной, так и коммерческих сетей.

Система условного доступа «Роскрипт-М» позволяет осуществить защиту компонент транспортного потока, кодированных в соответствии со стандартами MPEG-2, MPEG-4 AVC/H.264 при обычном (SD) и высоком (HD) разрешениях. СУД «Роскрипт-М» совместима со стандартами вещания DVB-S, DVB-C, DVB-T. СУД «Роскрипт-М» с 2006г. находится в эксплуатации. Сейчас это готовое решение, получившее довольно широкое распространение на территории РФ. Оборудование СУД «Роскрипт-М» используется крупнейшими операторами связи - ФГУП «Космическая связь», ФГУП «Российская телевизионная и радиовещательная сеть». Система установлена на самой большой в стране сети распространения программ – ОАО «Первый канал» и на других сетях телеканалов.



Надежность системы «Роскрипт-М»

В системах УД предъявляются повышенные требования к надежности оборудования. Разработчиками системы «Роскрипт-М» реализована система с высоким уровнем надежности в целом и, в особенности, комплекта передающей части системы, в значительной мере определяющей качество работы всего цифрового тракта. Кроме того, следует учесть, что в системе «Роскрипт-М» предусмотрена реализация 100%-го горячего резервирования с автоматическим переключением на работу с исправным комплектом.

Ни для кого не секрет, что самым «слабым» местом любой системы условного доступа с точки зрения взлома является абонентская сторона, чаще всего это стык модуль условного доступа - смарт-карта. Поэтому в системе условного доступа «Роскрипт-М» смарт-карта отсутствует. Вместо нее непосредственно на плате установлен защищенный чип, что позволяет использовать сложные алгоритмы криптозащиты.

Как известно, степень безопасности алгоритма зависит от сложности алгоритмов шифрования и длины ключа. В СУД «Роскрипт-М» использует 8 уровней защиты (пароли, базовые ключи, имитовставка и т.д.). Система позволяет частичный или полный UP-Grade через транспортный поток. Принятые решения позволяют обеспечивать высокие требования по надёжности и в коммерческих сетях.



Параметры системы “Роскрипт-М”

- Количество поддерживаемых абонентских устройств - более 20 млн.
- Количество закрываемых сервисов одним скремблером - не менее 50
- Автоматическая система управления обеспечивает многоканальное управление с общим количеством сервисов 2048
- Максимальное количество групп/подсетей - 64000
- Скорость транспортного потока - до 100 Мбит/с
- Система позволяет частичный или полный UP-Grade через ТП
- Длина ключей - 256 бит
- ПО АСВД и АСУ - SQL Server
- Скорость управления абонентскими устройствами - 500 абонентов в секунду при скорости потока EMM 50 кбит/с
- Возможность передачи таблиц управления за счет избыточности ТП

Правовая защита системы “Роскрипт-М”

СУД “Роскрипт-М” соответствует приказу №3 от 11.01.2006г. Министерства информационных технологий и связи Российской Федерации “Об утверждении требований к защите от несанкционированного доступа к программам, транслируемым с применением системы цифрового телевизионного вещания DVB, при их передаче по каналам связи, образованным спутниковыми линиями передачи сети связи общего пользования”.

СУД “Роскрипт-М” соответствует приказу №126 от 07.11.2007г. Мининформсвязи России “Правила применения оборудования систем телевизионного вещания. Часть III. Правила применения оборудования системы условного доступа”. Сертификат Мининформсвязи России от 22.10.2008г.

Сертификат информационной безопасности ФСТЭК (Федеральная служба по техническому экспертному контролю).

Патент на полезную модель “Система защиты информации в абонентских сетях” от 25.06.2008г.

В октябре 2008г. представителями ФГУП НИИР совместно с представителями МСЭ был составлен, а рабочей группой утвержден проект новой рекомендации по Системам Условного Доступа, куда первой системой вошла СУД “Роскрипт-М”

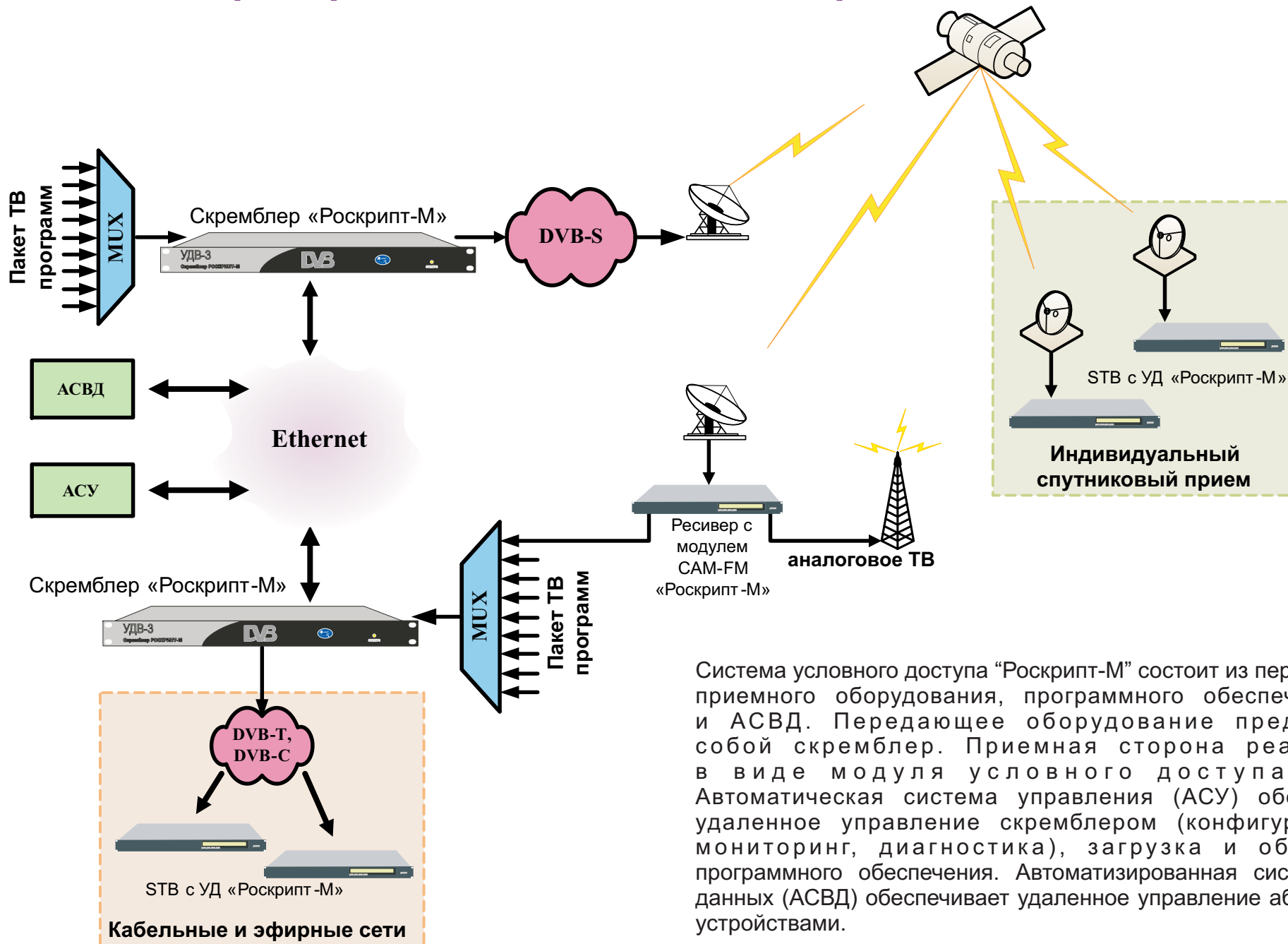
УДВ-3

Скремблер Роскрипт-М



СТАТУС

Область применения системы условного доступа «Роскрипт-М» для распределительных и коммерческих сетей



Система условного доступа «Роскрипт-М» состоит из передающего и приемного оборудования, программного обеспечения АСУ и АСВД. Передающее оборудование представляет собой скремблер. Приемная сторона реализована в виде модуля условного доступа (САМ). Автоматическая система управления (АСУ) обеспечивает удаленное управление скремблером (конфигурирование, мониторинг, диагностика), загрузка и обновление программного обеспечения. Автоматизированная система ввода данных (АСВД) обеспечивает удаленное управление абонентскими устройствами.

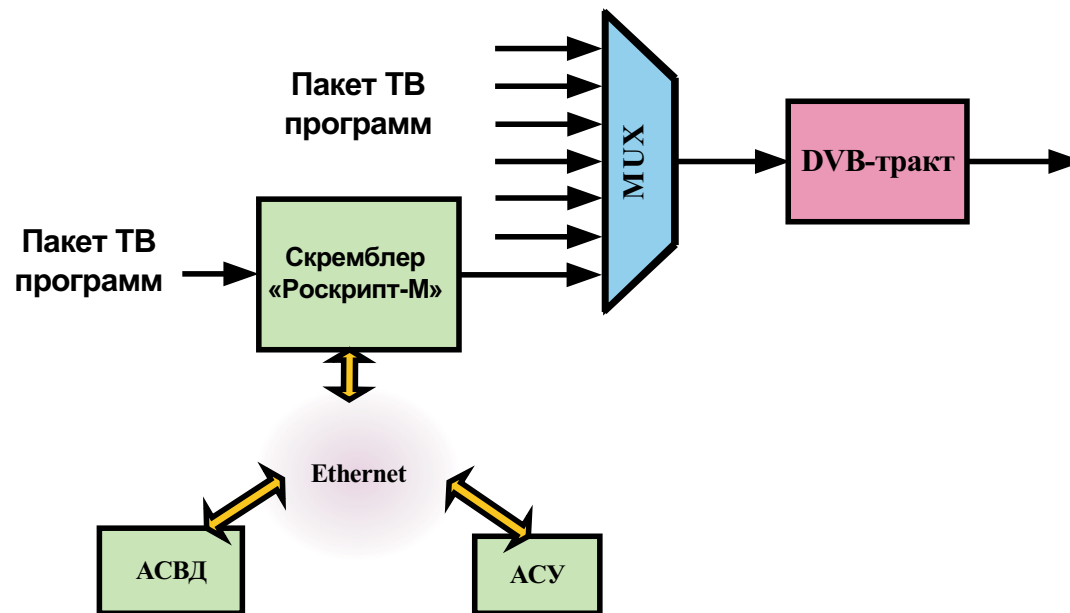
Преимущества различных вариантов подключения передающего оборудования СУД «Роскрипт-М»



перед MUX

Организация канала по передаче данных до 2МБит/с

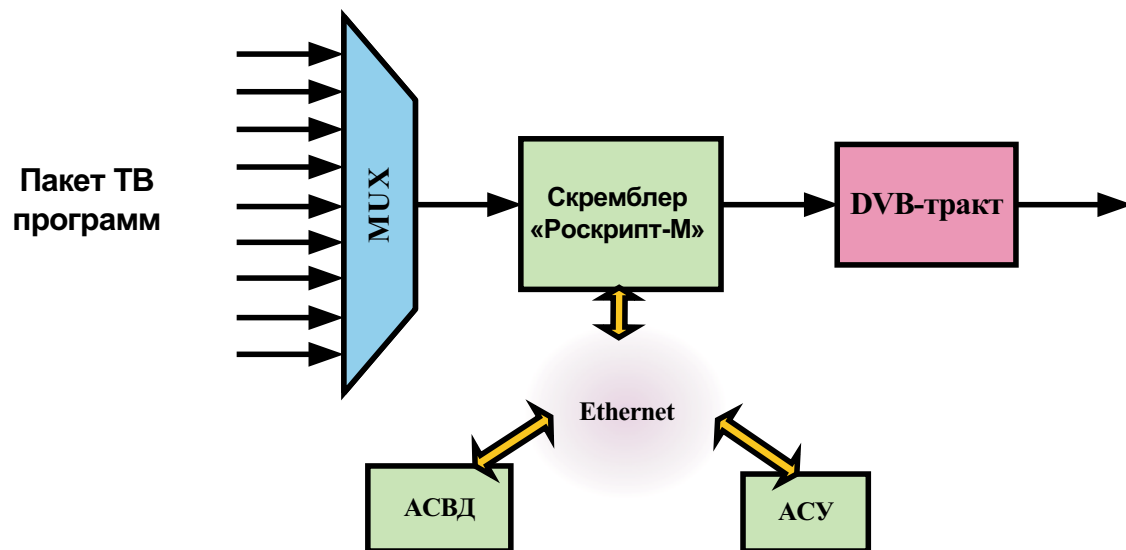
Поддержка закрытия ТП единым алгоритмом DVB SimulCrypt



после MUX

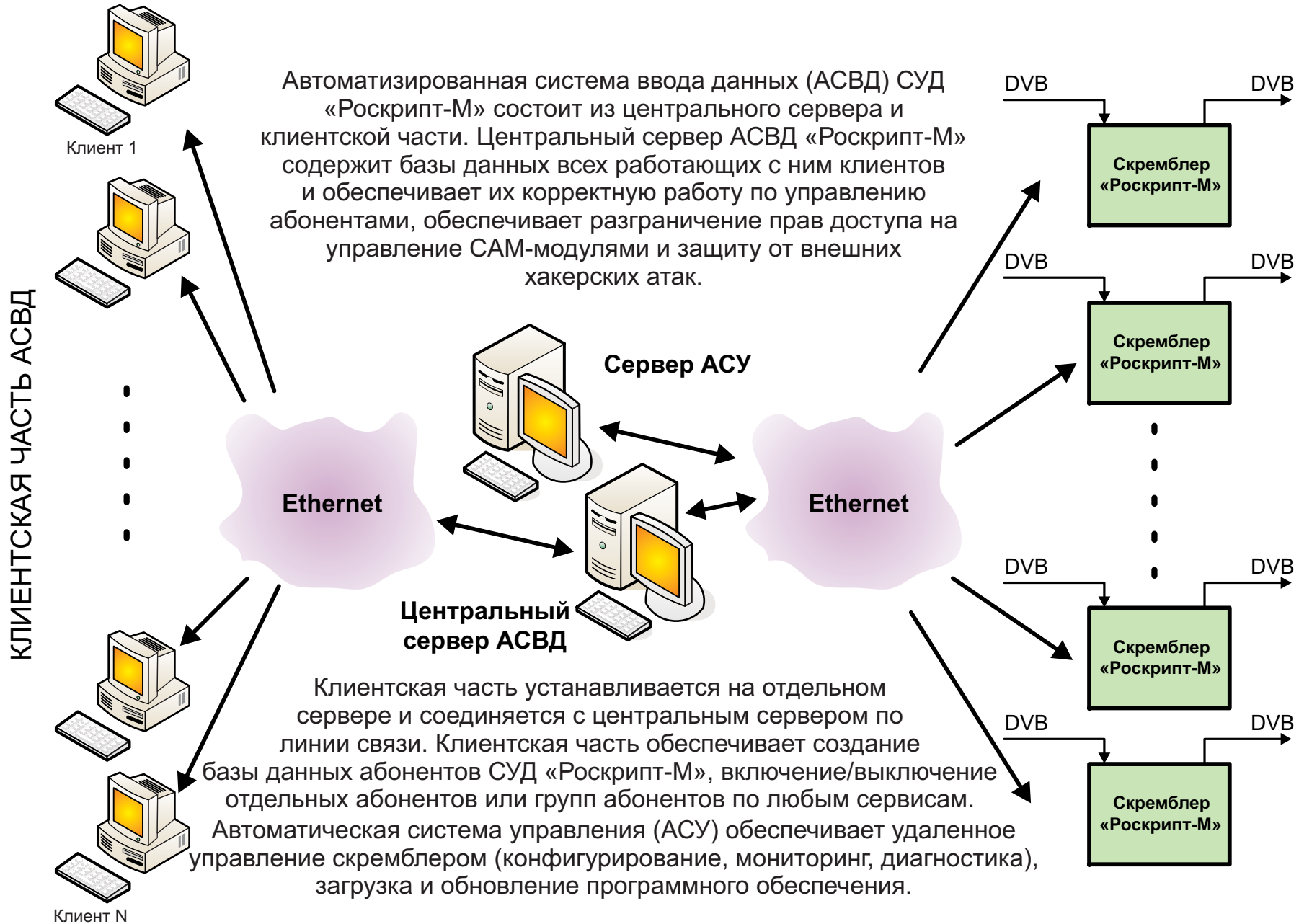
Нет необходимости выделения полосы частот для управления из общего транспортного потока

Возможно использование избыточности ТП для организации канала по передаче данных



Управление системой условного доступа «Роскрипт-М»

Схема построения для крупных операторов



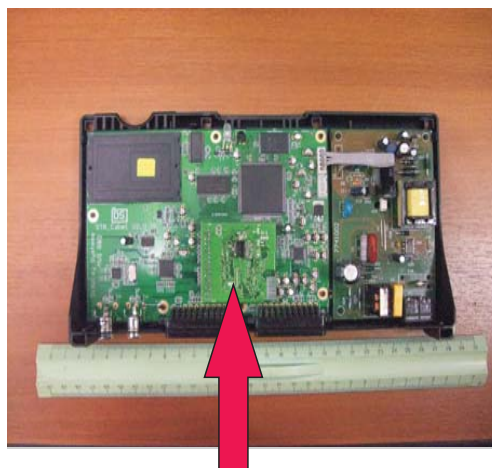
Реализация приемной стороны СУД “Роскрипт-М”



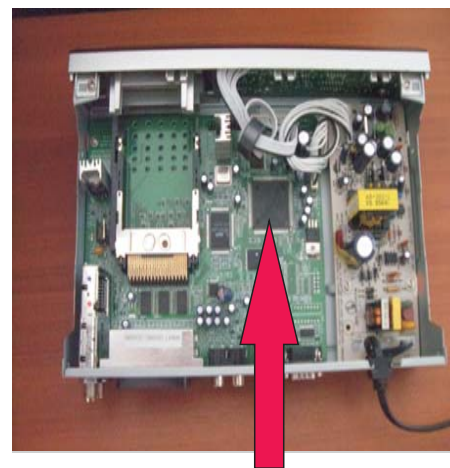
На абонентской стороне прием осуществляется на цифровой спутниковый приемник. Цифровой поток дескрипбируется модулем условного доступа (САМ) “Роскрипт-М”, различная реализация которого представлена ниже. САМ восстанавливает принятый поток с помощью ключей доступа и анализирует информацию управления для данного абонента. В том случае, если обнаружен код запрета или разрешения, САМ соответственно включает или отключает дескрипбирование DVB потока.



Внешний модуль САМ-FM
Подключается к разъему DVB-CI цифрового спутникового приемника по шине PCMCIA в соответствии со стандартом EN 50221



Встраиваемый модуль
Подключается последовательно с выходом декодера канала STB. Обеспечивает открытие/закрытие сервисов в соответствии с командами, поступающими из центра



Программа базового кристалла
(ведутся разработки)

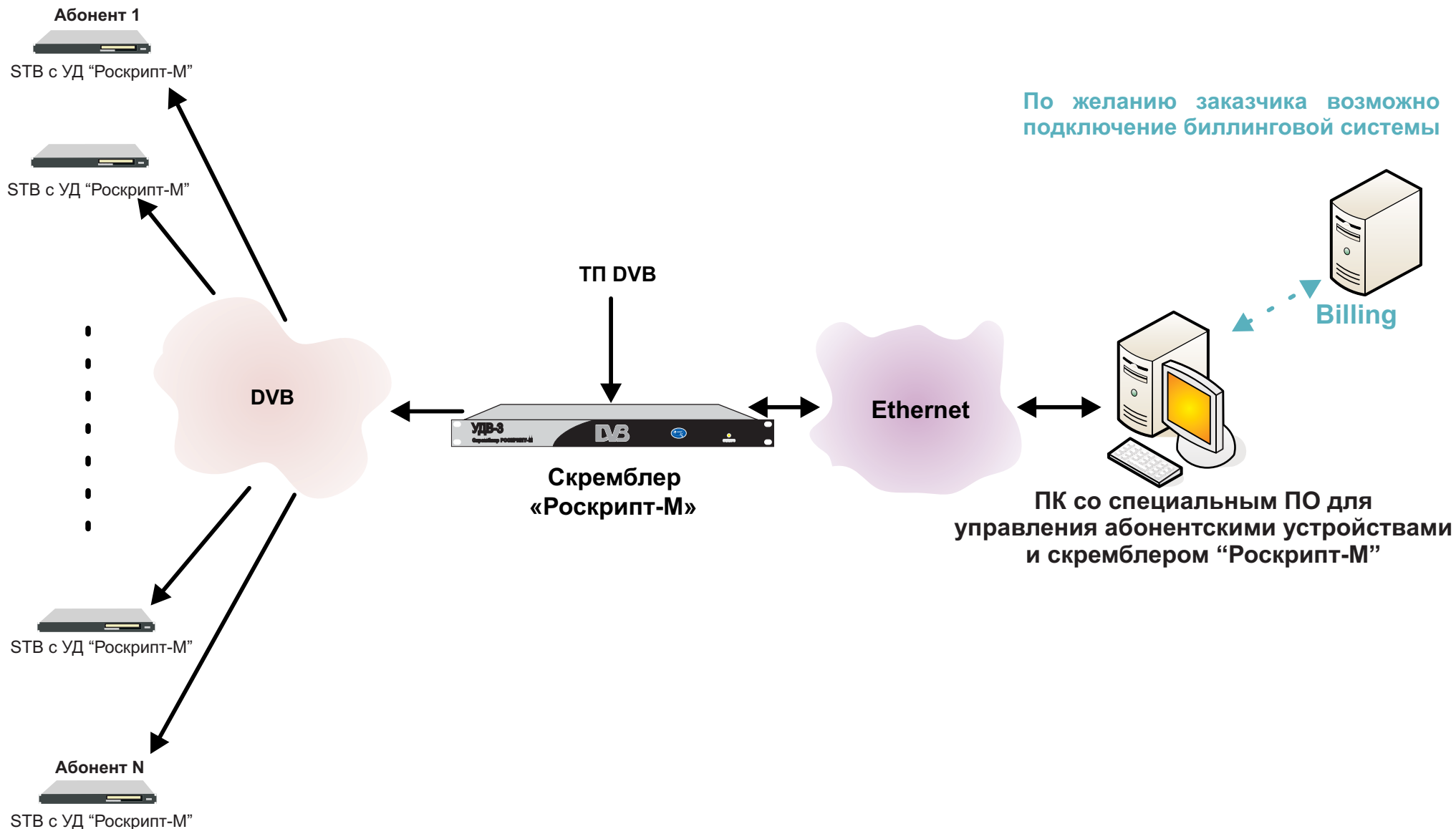


Цифровая телевизионная приставка MPEG-2/4 “НИИР-ЦТВ” со встроенным индивидуальным абонентским модулем СУД “Роскрипт-М”

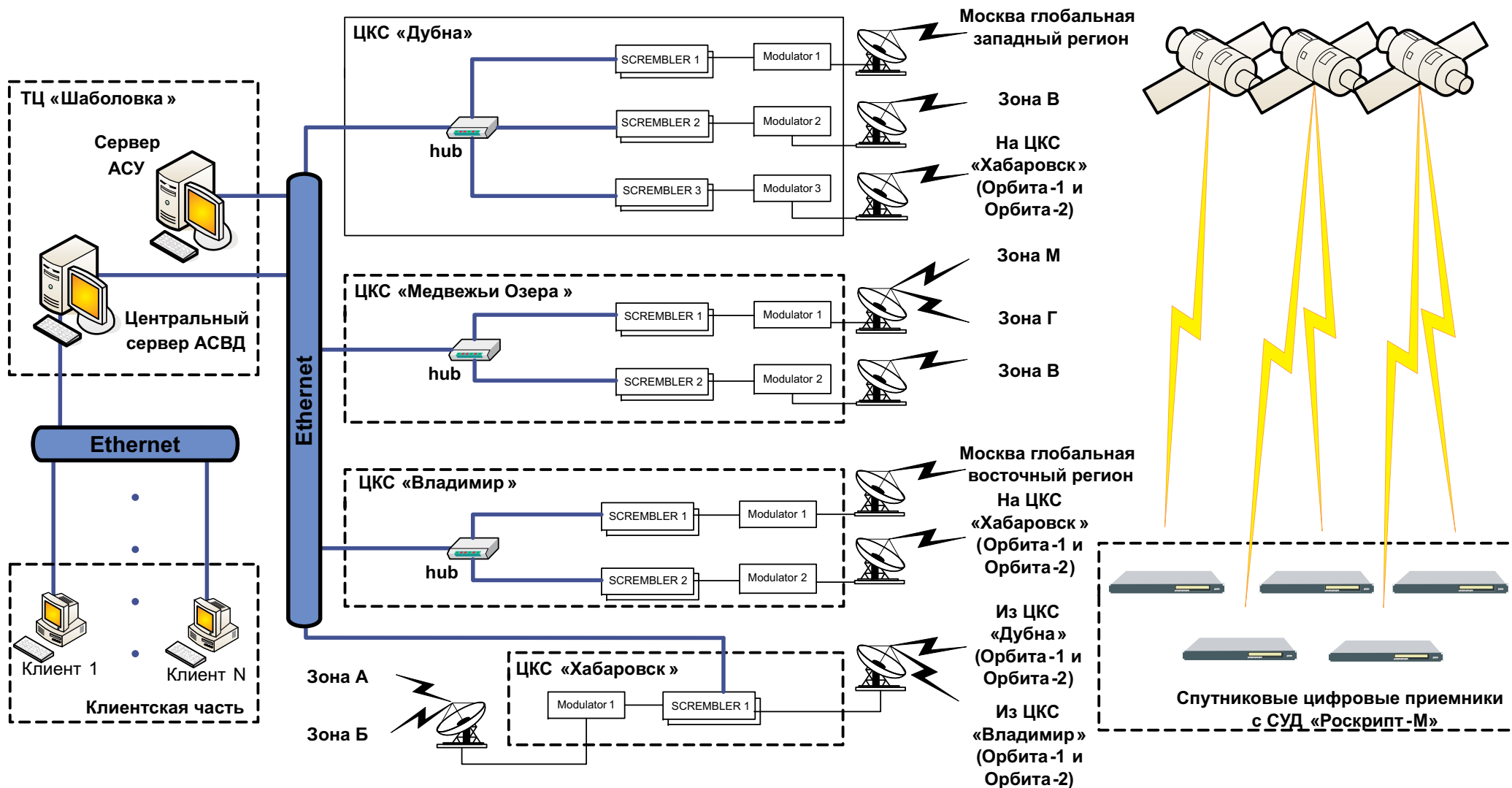
Структурная схема аппаратно-программного комплекса «Роскрипт-М» для средних и небольших операторов



АБОНЕНТСКАЯ ЧАСТЬ



Организация СУД «Роскрипт-М» на действующей спутниковой сети Российской Федерации



Россия, 105064, Москва
Казакова ул., д. 16
Тел.: +7 (499) 261-3694
Факс: +7 (499) 261-0090
E-mail: info@niir.ru
www.niir.ru

СИСТЕМА УСЛОВНОГО ДОСТУПА “РОСКРИПТ-М”

Разработано в НТЦ ТВ

Боловинцев Юрий Михайлович
Лобова Татьяна Ивановна
Шумакович Елена Евгеньевна

Тел.: +7 (499) 261-0693
Факс: +7 (499) 261-0359
E-mail: lyashko@niir.ru
tv-niir@mail.ru

