НАТО уже в России...

В России «практически отсутствует производство конкурентоспособного телекоммуникационного оборудования...»

Из текста «Стратегии развития информационного общества в России» подготовленного ***Л.Д. Рейманом***

«Мы заинтересованы производить телекоммуникационное оборудование. Однако нужно сначала определиться, что мы можем делать лучше всего. У нас, например, очень сильная школа систем космической связи, антенного оборудования, сильная научная школа в области телетрафика и системных решений. То есть, в нашей стране есть очень хорошая база для развития собственного производства в отдельных сегментах, и ее нужно эффективно использовать».

Из интервью с заместителем Министра связи и массовых коммуникаций Р Ф
Н.С. Мардером
По материалам журнала Мир связи. Connect!

«...самое худшее, что сегодня может случиться, – это использование текущей ситуации для сведения счётов, для недобросовестной конкурентной борьбы. В том числе с использованием административного ресурса».

Необходимо «ускорить формирование сильных государственных и частных центров разработки новых технологий. Реально помочь малому и среднему бизнесу в создании инновационных предприятий... привлекая внешние ресурсы, эффективно защищать свои экономические интересы».

«Сейчас нужно активно содействовать нашим компаниям в получении максимальных выгод из открытости российской экономики и из текущей рыночной ситуации, несмотря на всю её сложность. Помогать им повысить свою эффективность и выйти на новые рынки – рынки товаров, технологий, рабочей силы».

из Послания Президента РФ Д.А. Медведева Федеральному Собранию Российской Федерации

Меморандум
Группы компаний «Протон-СЗС»

Президент РФ Д.А.Медведев в интервью российским телеканалам *(31.08.08 г.)* сформулировал пять позиций осуществления дальнейшей внешней политики нашего государства. В соответствии с четвёртой позицией российскому предпринимательскому сообществу гарантирована всесторонняя защита его интересов за границей.

Однако, следует отметить, что не в меньшей защите от недобросовестных конкурентов это сообщество нуждается и в пределах Российской Федерации. Зарубежные компании взятками и подкупом завоёвывают наш рынок *(см. журнал «The Wall Street Journal», газеты «Ведомости» (19.11.07г.) и «Аргументы неделі» (№42 от 16.10. 08 г.)* о скандале немецкого концерна Siemens). В результате за последние 15 лет только сектор разработок и производства отечественного телекоммуникационного оборудования сократился более чем в десять раз (с 360 до 30 предприятий). Сумевшие выжить отечественные производители аппаратуры связи находятся на грани банкротства и из последних сил борются за удержание своих ниш. Новые предприятия в этом секторе уже давно не создаются.

Как следствие – российские валютные средства с ежегодным объемом исчисляемым миллиардами долларов и евро поступают на счета компаний Siemens, Ericsson, Nokia, NEC, Alcatel, Lucent, Iskratel, Nortel, Sumsung и других сорока крупнейших зарубежных компаний.

К настоящему времени в нашей стране все цифровые станции на международном и междугородном уровне – зарубежного производства, на местной телефонной сети – 80 % импортного оборудования, на ведомственных и корпоративных сетях – 90%. А сам набор зарубежных цифровых АТС насчитывает уже более 80 моделей (при норме 3-4 модели).

Об опасности сложившегося положения на протяжении пяти последних лет органы государственной власти предупреждали и учёные, и специалисты связи, и журналисты.

На неё обращали внимание в своих фундаментальных научных работах В. Андреев («Оружие и война: новые тенденции развития»), Р. Луговец, В. Поляков («К вопросу о реализации Концепции национальной безопасности Российской Федерации»), Ю. Уфимцев, Е. Ерофеев в сборнике «Информационная безопасность России». Эти авторы активно предостерегали от *«засоренности отечественного рынка средствами телекоммуникации иностранного производства»*.

В 2004 году член-корреспондент РИА и АТИ генеральный директор НПП «Спецстрой-Связь» А.И. Лучкив организовал и провел в Москве,

специально посвященные этой теме, заседания круглого стола, межрегиональные совещания и Общероссийскую научно-практическую конференцию с участием руководителей большинства отечественных предприятий-разработчиков и производителей телекоммуникационного оборудования.

11 мая 2006 года группа российских учёных обратилась с открытым письмом к Президенту РФ В.В.Путину, Министру обороны С.Б. Иванову, Председателю Совета Федерации С.М.Миронову и Председателю Государственной Думы Б.В.Грызлову, в котором ещё раз обратила внимание руководителей государства на вопиющие нарушения Доктрины информационной безопасности, утвержденной Президентом РФ 09.09. 2000 года .

13 июля 2007 года прошла ещё одна конференции в Москве, которая была организована Комитетом по промышленному развитию Торгово-промышленной палаты Российской Федерации, Ассоциацией «Совет Главных Конструкторов» при поддержке Межфракционного депутатского объединения Государственной Думы РФ «Наука и высокие технологии».

В своем выступлении на этом совещании президент Ассоциации «Совет Главных Конструкторов» М.В. Волошенко отметил, что *«инфотелекоммуникационная сеть России более чем на 90% оснащена оборудованием и ПО зарубежных фирм – нерезидентов, что привело к зависимости работоспособности сетей и от самих поставок из-за рубежа, и от лояльности поставщиков»*.

Этой же теме посвящена статья *«Три проблемы построения и эксплуатации ведомственных и корпоративных сетей электросвязи России»* в журнале «Электросвязь» №4/2008 г.

Военный обозреватель В.Н. Литовкин в своём интервью радиостанции «Эхо Москвы» (28.08.08г.) тоже высказал по этому поводу свою крайнюю озабоченность: *«В России увлеклись закупками импортного телекоммуникационного оборудования. При этом «Газпром» закупает его в одних странах, «Роснефть» – в других, армия – в третьих. Хотя, по всем нормам и правилам все средства связи на территории одной страны должны быть отечественными и должны совпадать. Поэтому в критический момент в России всю связь можно вырубить единовременно»*.

И тому есть подтверждения.

Хрестоматийным примером может служить общее отключение электросвязи Сербии в 1999 году накануне натовских бомбежек. В это же время краткосрочно прекратили свою работу и все АТС SI 2000, произведенные в Словении и установленные на Европейской части России, приближенной к Балканскому региону.

Регистрировались отключения связи и в Ираке накануне нападения США, и в Цхинвали – перед нападением Грузии.

В нынешнем году странным образом исчезла фиксированная и мобильная связь в Дагестане за два часа до покушения на генерального прокурора этой республики.

В ноябре 2008 г. руководитель Общества по защите прав потребителей Феликс Ратавнин направил на имя Министра связи Игоря Щеголева письмо с просьбой провести проверку, связанную с ЧП на мобильной связи МТС, которое происходило с 31 октября по 2 ноября на всём Северо-Западе России. А началось всё в Санкт-Петербурге, где как-то странно повели себя все мобильные аппараты, которые вдруг начали заикаться, а на дисплеях немногих особо чувствительных телефонов стал появляться значок перевернутого ключа, разомкнутого замка или восклицательного знака. И только специалисты связи поняли, что это значит. Хотя сам оператор МТС так и не смог объяснить, почему у него само собой отключилось шифрование каналов связи, а значит передаваемая по сети информация и переговоры абонентов стали на трое суток открытыми для «прослушки» и перехвата. Кто и как воздействовал на оборудование шифрования – осталось загадкой.

С середины сентября т.г. в газетах «Financial Times», «New York Times», «Washington Post» публикуются распечатки телефонных переговоров военных российской армии и южноосетинских ополченцев, которые велись и до начала боевых действий в Южной Осетии и в их процессе. Такие утечки информации в очередной раз свидетельствует о ненадежности даже военной связи, построенной на импортном оборудовании.

14 февраля 2006 года в журнале «Компьютерра» был публикован материал Киви Берда «Цепь случайных совпадений?», в котором подробно освещался телефонный скандал, разразившийся в Греции, где «неизвестные личности» осуществляли постоянный перехват разговоров премьер-министра Греции Костаса Караманлиса и пяти членов его кабинета. Все подслушиваемые телефоны работали в сети одного из крупнейших в стране провайдеров Vodafone Greece, дочернего предприятия британской компании Vodafone. Работала эта сеть на аппаратуре и программном обеспечении компании Ericsson, в которых и была обнаружена недокументированная «закладка» (тоже разработанная компанией Ericsson).

Ещё один скандал связан со швейцарской компанией Crypto AG. Случайно вскрылось, что в программном обеспечении этой фирмы, которое она поставляла в ряд стран, присутствуют закладки, снижающие криптостойкость.

И такие случаи не единичны. Активное вмешательство разведывательных служб в использование телекоммуникационных сетей можно проиллюстрировать множеством примеров.

Уже документально установлено, что немецкий концерн Siemens в течение нескольких десятилетий сотрудничал с немецкой Федеральной службой разведки (BND), о чём сообщал журнал Der Spiegel. По его данным, бывший член совета директоров Siemens Фолкер Юнг (Volker Jung) был ставленником BND.

Компания Siemens прослушивала телефонные разговоры во многих странах мира, включая Россию, а полученную информацию передавала в BND. Кроме того, немецкий концерн часто посылал своих инженеров туда, куда доступ спецслужбам был закрыт.

Наиболее ярким примером может служить серьёзная утечка информации, составляющей коммерческую тайну, из центрального аппарата «Газпрома» *(газета «Аргументы недели» (№42 от 16.10. 08 г.)*. Как впоследствии выяснила Служба безопасности этого концерна, технически обеспечило эту утечку коммутационное оборудование фирмы Siemens, которым укомплектована сеть связи административного комплекса «Газпрома» в Москве на улице Наметкина.

Между тем, в России Siemens присутствует в 30 регионах страны. Численность сотрудников российского подразделения компании составляет около 3 тыс. человек, оборот только в 2006 финансовом году составил 1,2 млрд.

Даже зарубежные конкуренты концерна Siemens, делают вид, что наивно удивляются его успеху в России. На последней выставке ВКСС-2007 один из представителей компании Alcatel сказал: *«Продукция Siemens по качеству никогда не отличалась от основных конкурентов, в том числе и российских, но у неё всегда был зеленый свет в России на всех уровнях — от высшего до глав «электросвязей» на местах»*.

Хотя, надо полагать, этот представитель отлично знал каким образом достигался успех концерна Siemens, который используется немецкой разведкой на территории России со времен Первой мировой войны и Абвера. И если Alcatel, давая взятку совершает сегодня лишь коммерческий подкуп и плодит взяточников, то Siemens на свои деньги всегда приобретал не только выгодные заказы, но и высокопоставленных агентов влияния (газета *«Аргументы недели» (№42 от 16.10. 08 г.)*.

Вся эта информация, очевидно, и стала поводом для проведения 25 июля 2007 года заседания Совета безопасности РФ под председательством Президента РФ В.В. Путина. Именно тогда в своём выступлении Верховный Главнокомандующий констатировал: *«анализ состояния информационной безопасности показывает, что её уровень не соответствует потребностям государства, а в связи с зависимостью от иностранных производителей информационных средств, мы пока не можем гарантировать глобальную защиту информации стратегического значения»*.

Встревоженность всех слоев общества подтвердила и своевременность принятия на этом заседании Совета безопасности РФ «Стратегии развития информационного общества в России», в которой была впервые сформулирована **экстренная необходимость импортозамещения в сфере инфотелекоммуникаций.**

Что же изменилось с тех пор?

Крупнейший российский оператор ОАО «Связьинвест» все последние годы строил свои сети электросвязи на различном импортном оборудовании, среди которого были и словенско-немецкие платформы Iskratel, и немецкие – Siemens, и канадские – Nortel, и шведские – Ericsson. Но на сельские оконечные станции при этом, всё же, допускалось отечественное оборудование. После утверждения Советом безопасности РФ «Стратегии...» и принятия «Связьинвестом» на вооружение дорогостоящей зарубежной технологии NGN руководством ОАО было принято окончательное решение, что на его сети будет допускаться только оборудование фирм Nortel и Siemens, а так же китайское оборудование фирмы Huawei. И, как сообщил технический директор ОАО «Волгателеком» А.Ю. Китков, все отечественные АТС (включая «оконечки») в ближайшем будущем будут демонтированы.

На оборудовании Iskratel строилась и продолжает строиться ведомственная сеть связи Таможенной службы России.

Газпром и большинство энергетических предприятий оставались и остаются верны концерну Siemens . Правда, энергетики после принятия «Стратегии...» стали благосклонно относиться и к оборудованию шведской фирмы Ericsson.

ОАО «РЖД» строило свою общетехнологическую сеть связи на цифровых АТС SI 2000 (Iskratel). После принятия идеологии импортозамещения ОАО перешло на оборудование американской фирмы Avaya.

И лишь силовые структуры ещё недавно проявляли в этом отношении принципиальность.

В прошлом году начальник управления заказов и поставок МО РФ генерал-лейтенанта А.Б. Михайловский заявил, что зарубежное программное обеспечение средств связи не может пользоваться доверием, так как в него *«могут быть умышленно включены закладки – элементы информационного оружия...»* (Федеральный справочник «Информационные технологии и связь в Российской федерации» №6 за 2006-2007 г.г.).

Эта убежденность одного из руководителей Министерства обороны РФ не помешала другим руководителям этого же министерства после утверждения «Стратегии...» заняться лоббированием интересов зарубежных производителей. Вопреки мнению преподавательского состава санкт-петербургской Военной академии связи им. С.М. Буденного, они потребовали перевести обучение слушателей академии на осво-

ение цифровых АТС транснациональной (франко-американской) фирмы Alcatel. На этом же оборудовании по настоянию МО РФ сейчас строится и сеть связи самой Военной академии. Из чего можно сделать вывод, что эти же станции скоро появятся и во всех военных округах.

Между тем уже имеется прецедент неудачного запуска зарубежных станций в этой академии. Тогда, для дальнейшего изучения, пытались ввести в эксплуатацию платформу SI 2000. После того, как станция была запущена и потребовалось ввести несколько дополнительных её функций, продавцы заявили, что эти функции включаются только с разрешения головной фирмы Iskratel. То есть, проще говоря, для получения этих функций МО РФ должно было получить согласие НАТО.

На оборудовании Alcatel строится сегодня (уже после утверждения «Стратегии...») и ведомственная выделенная сеть связи всех территориальных подразделений МВД РФ. И лишь в двух, не очень спокойных, регионах связисты местных УВД отказались от импортной техники. Они слишком хорошо знают цену информационно безопасной связи. Поэтому Дальний Восток категорически отверг Alcatel, да и Чечня продолжает эксплуатировать и закупать только отечественное оборудование «Протон-СКС».

Как удаётся обойти запреты на использование зарубежной техники объяснил технический директор ООО «Балтийские Телекоммуникационные Системы» Игорь Олегович Соколов:

«Меня не удивляет, что на сети привязки Министерства обороны РФ при их модернизации поставляется аппаратура зарубежной разработки и производства. Требование использовать для этих целей только отечественную аппаратуру обходится очень легко: российская фирма-поставщик заключает с зарубежной фирмой Alcatel соглашение, и аппаратура, пересекая границу России и попадая в руки российских торговцев, формально получает статус «отечественной». Мало того, такую, произведенную за рубежом, аппаратуру поставляют даже с нашей военной приемкой».

Итоги такой практики наиболее лаконично подвёл военный обозреватель В.Н. Литовкин всё в том же интервью радиостанции «Эхо Москвы»:

«У нас почему-то забывают, что связь – это не только комфортная услуга. Связь – это ещё и система автономного и автоматического управления боевыми действиями, это система обеспечения боя, с помощью которой осуществляется взаимодействие всех родов войск. К сожалению Цхинвали показал, что взаимодействия между наземными войсками и воздушными, армейской авиацией у нас не существует. Поэтому и произошли такие потери. Пока у нас всё держится на силе духа русского солдата и офицера. Нужно откровенно признаться, что у нас нет боеспособных войск связи.

К сожалению, по уровню надежности связи мы сегодня во многом беспомощны не только перед военными угрозами.

Сейчас многие политологи и экономисты заняты анализом механизмов развивающегося мирового экономического кризиса. Они предлагают – каждый свои – антикризисные стабилизаторы для России. И, при всём разночтении их мнений, все сходятся в одном: кроме финансовой составляющей, универсальной надобностью перед лицом основных угроз должна стать отлаженная система национальной безопасности (в том числе и информационной), обеспечивающей инфраструктуру территориальной связности внутри России. Главным элементом этой инфраструктуры и является электросвязь. Каким же образом у нас обеспечена эта целостность?

Вся мобильная связь России построена на зарубежном оборудовании, а поэтому и находится (вместе со своим информационным содержимым) 100% под контролем *«фирм – нерезидентов»*. «Надежность» сетей фиксированной связи общего пользования ОАО «Связьинвест» нам обеспечивают, как перечислялось выше, Словения и Германия (Iskratel), Китай (Huawei), Германия (Siemens), Канада (Nortel) и Швеция (Ericsson). Информационная безопасность Таможенной службы России под контролем Словении и Германии (Iskratel). За безопасностью российских предприятий энергетики и Газпрома следят Германия (Siemens) и Швеция (Ericsson). За безаварийность железных дорог ОАО «РЖД» отвечают Словения и Германия (Iskratel) и США (Avaya). Общественную безопасность (МВД РФ) нам будет теперь гарантировать США и Франция (Alcatel).

Что же касается нашей обороноспособности, то здесь следует отметить, что МО РФ не имеет (как в других странах) собственной выделенной сети и арендует каналы связи у ОАО «Ростелеком». А сети связи «Ростелекома», осуществляющего дальнюю связь, во-первых, построены на том же оборудовании, что и ОАО «Связьинвест» и, во-вторых, полностью открыты для всего мирового сообщества. Поэтому франко-американское оборудование (Alcatel) во всех военных округах станет лишь небольшим дополнением к нашей информационной открытости и прозрачности.

Так стоит ли после этого так усердно препятствовать продвижению НАТО на Восток? НАТО уже здесь: в каждом доме, на каждом предприятии, в каждой воинской части...

Обсуждение меморандума в открытой электронной газете

открытая электронная газета
Forum.msk.ru

http://forum.msk.ru/material/lenty/597351.html

Ответить

(без названия) – Серый (2008.11.17 04:20)

Дальний Восток давно «подсел» на оборудование китайского Хуавей.

Ответить

По сеньке – шапка! – Василий (2008.11.17 11:26)

То, что российский чиновник за баксы не только мать, но и Родину продаст – не удивительно. Восхищает другое: даже у рядового отечественного скобаря напрочь отсутствует инстинкт самосохранения. Истинно: у каждого народа то правительство, какого он заслуживает....

Ответить

Проблема существует... – Дед (2008.11.17 14:21)

Проблема существует. Точнее – существовала... Поезд уже ушел! Вся транспортная сеть, а в большинстве экономически развитых регионах и т.н. «оконечка» давно импортная. Все вопросы к Рейману. Он впустил сюда китайцев, люсентовцев и прочих алкателей. И сеть связи модернизировал, и сам хорошо «приподнялся». В конце девяностых генералы от связи пытались противодействовать этому. Да где там! Надо было еще тогда правительству РФ платить Рейману откаты, чтобы он пекся об информационной безопасности страны.

Ответить

Ответ – Василий (2008.11.17 14:30)

Нам и всему миру долго внушали мысль об отставании России «навсегда». Но вот парадокс: ни Iskratel, ни Huawei, ни Siemens, ни Nortel, ни Ericsson ни Avaya, ни Alcatel ни разу не предложили российским разработчикам и производителям цифровых АТС провести совместные стендовые испытания своей продукции А не предложили потому, что знают – будут побиты и по цене, и по качеству, и по надежности, а главное – по информационной безопасности

Ответить

Проблема существует... – 2 (2008.11.17 20:36)

А Верховный в курсах? Не знает, поди...

Ответить

Проблема существует... – Василий (2008.11.17 21:23)

Рейман – питерский ставленник Верховного. Подробности смотрите на «Компромат.ру»

Ответить

(без названия) – yman (2008.11.18 00:39)

Связь, как хроническая болезнь, тянется аж от А. Попова или даже со времен нашествия Батыя и служит важным дополнением к известной всем присказке про плохие дороги и дураков. Зато мы-таки полетим на Марс, чтобы и на Марсе были... плохие дороги, дураки и... Huawei.

Ответить

Слов нет-один мат – SVN (2008.11.18 01:12)

А работы-то, работы – заряжай Иван! Не инженеры и рабочие нужны нашей власти, а каратели! И они будут, потому как месть – чувство звериное, доисторическое, в тяжелые времена спасительное.

Ответить

Все всё понимают – независимый (2008.11.18 01:31)

Верховные скорее всего всё понимают, поэтому и не летают на иностранных самолётах, которые могут по команде слишком быстро опуститься так, что мало не покажется. Мы недавно закупили партию радиостанций Моторола, так они при каждом включении питания передают в эфир короткую серию радиосигналов, по которым со спутников легко определяется их место положения, но стоят они дешевле.

Ответить

На тему – Спец (2008.11.18 10:56)

На стратегические объекты и на сети связи силовых структур допускать телекоммуникационный импорт – преступление! Да и серьёзному российскому бизнесу, который опасается конкурентов, стоит присмотреться к своим средствам связи

Ответить

Проблему создали те же, кто от неё и пострадает – Алексей К (2008.11.1913:32)

Посадка МВД, ФСБ и армии на забугорное оборудование и даже софт дала возможность освоить в личные карманы огромные деньги, которые выбивались из бюджета на «разработку и модернизацию» систем связи. При этом никакие аргументы насчет безопасности никого не волновали. Это показывает, что нашим государством управляют даже не паразиты, а совсем уж конченые наркоманы: знают, что конец приближают себе, но продолжают колоться.

ГОСУДАРСТВЕННАЯ ДУМА
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПЯТОГО СОЗЫВА

КОМИТЕТ ПО БЕЗОПАСНОСТИ

ул. Охотный ряд, д. 1, Москва, 103265 Тел. 692-89-32 Факс 692-95-75 E-mail: csecurity@duma.gov.ru

10 10 2008 г. № 3.15-32/1834

347924, Ростовская обл., г.
Таганрог, ул. С. Лазо, 5-103

В.Г.ФЕДОРОВСКОМУ

Уважаемый Владимир Георгиевич!

Ваше обращение рассмотрено в Комитете Государственной Думы по безопасности и направлено в Правительство Российской Федерации.

Заместитель
председателя комитета В.И.Колесников

Экз. № 1

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЦЕНТР
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

30.10.2008 № 147/ОУ/5-868
Москва

Федоровскому В.Г.
ул. С.Лазо, д.5, кв. 103,
г. Таганрог, Ростовская обл., 347924

Об использовании в России
телекоммуникационной продукции
зарубежного производства

Уважаемый Владимир Георгиевич!

Представленные Вами материалы об угрозах безопасности, связанных с преимущественным использованием в российской информационной инфраструктуре телекоммуникационной продукции зарубежного производства, представляют интерес для Федеральной службы безопасности, являются чрезвычайно актуальными и будут учитываться нами в работе.

Затронутые Вами проблемы связаны с обеспечением обороноспособности и безопасности государства, требуют для их решения определенного времени, выделения значительных финансовых средств, а также принятия дополнительных правовых, организационных и иных мер, находятся в поле зрения руководства страны и соответствующих органов государственной власти, включая ФСБ России.

С уважением,

Заместитель руководителя Службы
контрразведки – начальник Центра В.В.Скорик

НПП «СПЕЦСТРОЙ-СВЯЗЬ»
РАЗРАБОТКА И ПРОИЗВОДСТВО
ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ ПРОТОН-ССС

приемная: т/ф (8634) 312-695
e-mail: main@proton-sss.ru
http: //www.proton-sss.ru

Россия, 347922, Ростовская обл.
г. Таганрог, ул. Шевченко, 2

В ответ на №147/ОУ/5-868 от 30.10.2008 г.

Заместителю руководителя Службы контрразведки – начальнику Центра информационной безопасности ФСБ РФ
В. В. С К О Р И К У

101000, Москва, Б. Лубянка, д.2, ЦИБ ФСБ РФ

Уважаемый тов. Скорик!

Я весьма благодарен Вам за содержательный и оперативный ответ на моё письмо. Рад, что собранные мной материалы, представляют интерес для Вашей Службы. Однако не могу согласиться с резюмирующей частью Вашего ответа. И, главным образом, с тем, что затронутая мной проблема умышленного (с помощью административного ресурса) устранения с рынка отечественных разработчиков и производителей телекоммуникационного оборудования *«находится в поле зрения руководства страны и соответствующих органов государственной власти».* По крайней мере, мне не хотелось бы верить, что именно с позволения руководства страны в принятый Советом безопасности РФ (25.07.2007 г.) текст «Стратегии развития информационного общества в России» Л.Д. Рейманом наконец-то была внесена убийственно констатирующая фраза, о том что у нас в стране *«практически отсутствует производство конкурентоспособного телекоммуникационного оборудования».*

Между тем, мы с 1999 года пытались доказать Министру связи РФ Л.Д. Рейману, что мы существуем, что наша продукция вполне конкурентоспособна, что она имеет те же сертификаты, что и импортная техника, что она уже второй десяток лет успешно эксплуатируется в различных государственных ведомствах (ФСИН Минюста, МВД, Службе речного флота Минтранса), бывшем «РАО ЕЭС России», на атомных электростанциях, в воинских частях. Мы десятками писем, меморандумов, протоколов наших отраслевых совещаний и конференций (собранных по собственной инициативе) обращали внимание Л.Д. Реймана на то, что отечественные разработчики и производители телекоммуникационного оборудования брошены на произвол судьбы, что наши интересы не представлены ни в одном из существующих министерств и ведомств, что даже в Минсвязи нет чиновника ответственного за развитие телекоммуникационной индустрии страны…

И всё это было впустую! Мы по-прежнему остаёмся вне закона, в том числе и вне Закона «О связи». И в этом отношении Рейман прав – наше производство формально (в любых государственных программах и документах) практически отсутствует. Хотя по моим сведениям совокупный продукт всех по-настоящему отечественных разработчиков и производителей телекоммуникационного оборудования уже сегодня мог бы полностью удовлетворить потребность страны в технике связи. Но нас не замечают, нас под любыми предлогами не допускают к торгам, нас всеми способами лишают заказов, которые могли бы оживить и расширить наше производство.

Именно поэтому я не могу согласиться с Вашим выводом, что затронутые мной проблемы *«требуют для их решения определённого времени, выделения значительных финансовых средств, а также принятия дополнительных правовых, организационных и иных мер»*. Время, огромные деньги и правовые меры нужны только Л.Д. Рейману, который, пользуясь нашим *«практическим отсутствием»* и уже загубив наше производство, начнет в ближайшее время создавать собственную, параллельную индустрию телекоммуникаций. То есть произойдёт именно то, от чего и предостерегал в своём Послании Федеральному Собранию Российской Федерации Президент РФ Д.А. Медведев. А он сказал: *«…самое худшее, что сегодня может случиться, – это использование текущей ситуации для сведения счётов, для недобросовестной конкурентной борьбы. В том числе с использованием административного ресурса»*.

Чтобы это худшее не случилось, я и отправил Вам своё первое письмо. Я надеялся, что оно заинтересует не только Ваш Центр информационной безопасности, но и службы, которые занимаются антикоррупционной деятельностью, которые смогут доложить Президенту о том, что Л.Д. Рейман в личных корыстных интересах пытается загубить, прекрасно существовавшую до него, отрасль телекоммуникационного производства. Отрасль, которой не нужны ни время, ни дополнительные средства, ни особые правовые меры. Мы только нуждаемся во внимании и протекционизме государства и хотим, чтобы органы власти *(«включая и ФСБ России»)* оградили нас от коррупционеров.

В связи с этим убедительно прошу Вас передать моё первое и нынешнее письма по назначению. Надеюсь на ответ и действенные меры.

С уважением

Федоровский Владимир Георгиевич

советник по информации и связям с общественностью

ген. директора ООО НПП «СПЕЦСТРОЙ-СВЯЗЬ»

АРГУМЕНТЫ НЕДЕЛИ
№42(128), четверг 16 октября 2008 года

«ГАЗПРОМ» под колпаком БНД

Кого «Сименс» купил за 2 миллиарда евро для БНД

В Германии коррупционный скандал. Налогоплательщики возмущены. В экономическом гиганте «Сименс» начались облавы, аресты, обыски и допросы. Для начала взяли 11 человек из числа топ-менеджеров концерна. Чтобы получить коммерчески выгодные контракты, они давали иностранным чиновникам взятки. В специальном «черном фонде» «Сименса» для таких операций было 3 млрд. евро. На подкуп успели потратить только 2 миллиарда!

Ну что здесь такого? Подумаешь, один другому взятку дал. У нас труднее найти того, кто не давал «на лапу». А все дело в том, что в ходе разбирательства вскрылась тайная сторона этой обычной, с нашей точки зрения, аферы коррупционеров. Оказывается, в течение нескольких десятилетий концерн являлся главным поставщиком прослушивающего оборудования немецким и иностранным спецслужбам. Используя инженеров «Сименса», внешняя разведка ФРГ (БНД) внедряла в поставляемые зарубежным клиентам системы связи концерна специальную аппаратуру технической разведки и вербовала с помощью «откатов» при таких сделках агентов влияния по всему миру.

Наша история о том, как шпионы под крышей концерна «Сименс» сумели проникнуть в тайны энергетического комплекса России.

Подкрышник БНД курировал коммуникационное подразделение «Сименса»

В интересах разведки ФРГ в состав совета директоров «Сименса» была введена специальная должность ставленника БНД. В последние годы таким «подкрышником» в концерне являлся Фолкер Юнг. Формально он курировал коммуникационное подразделение и отвечал за негласную продажу по всему миру аппаратуры для прослушивания телефонных разговоров. За верную службу при увольнении получил благодарность президента БНД. Было за что. В результате энергичных усилий его людей среди клиентов концерна оказались такие российские структуры стратегического значения, как: Министерство обороны РФ, Государственная Дума, бывшая ФАПСИ, МЧС РФ, Федеральный ядерный центр, «Газпром», Сбербанк России, АО «Мосэнерго», МГТС, ЛУКОЙЛ, ЮКОС, АЛРОСА, «Комбеллга», ГАЗ, РНЦ «Курчатовский институт», АК «Сибур», Международный промышленный банк, Госкомимущество РФ.

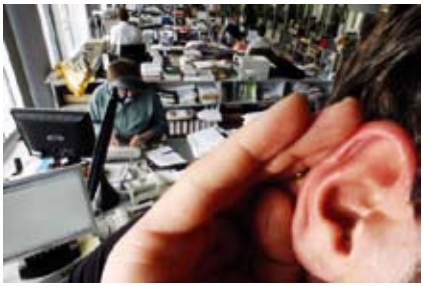
Излишне говорить, что для «технарей» от разведки такие сделки — «манна небесная». Они дают доступ к «прослушке». К тому же по договору при технической необходимости всегда можно послать своих инженеров (читай — разведчиков) на тот объект, куда доступ спецслужбам закрыт. Именно поэтому в этой сфере деятельности тоже дают взятки. Правда, при условии согласия получателя денег на вербовку.

Кто, кому, сколько и за что давал, мы, может быть, узнаем, если арестованные по этому делу начнут «колоться».

Объект проникновения – «Газпром»

Когда в 1989 г. на базе бывшего Мингазпрома был образован Государственный концерн «Газпром» во главе с бывшим министром В. Черномырдиным, на совете директоров было принято решение о строительстве современного административного комплекса в Москве на улице Наметкина. Подряд на строительство отдали турецким рабочим. Они дешевле. При этом заказчики не могли не знать, что турецкая фирма, как и все коммерческие представительства Турции, обязана сотрудничать с МИТ (национальная внешняя разведка, входящая в разведывательное сообщество НАТО). Телефонизацию помещений штаб-квартиры РАО «Газпром» доверили людям из «Сименса», концерна, который используется на территории России немецкой разведкой со времен Первой мировой войны и Абвера.

К моменту завершения строительства здания в 1993 г. Рем Вяхирев решил набрать из элитных сотрудников КГБ Службу безопасности РАО «Газпром». Пригласил на конкурсной основе две команды. Поручил разработать концепцию безопасности РАО «Газпром», а также Положение и Устав Службы безопасности. Кто лучше справится с задачей, тот и получит контракт. Одну группу возглавлял уволенный сразу же после путча генерал-майор запаса Владимир Медведев, бывший руководитель подразделений личной охраны Михаила Горбачева, которого он то ли защищал (от кого?), то ли держал под домашним арестом.



«Большие уши» БНД слушали разговоры в штаб-квартире «Газпрома» круглосуточно

Вторую команду собрал генерал-майор КГБ Виктор Иваненко. В качестве партнеров пригласил П. Грозу, помощника первого заместителя председателя КГБ Г. Цинева; А. Пичугина, помощника первого заместителя председателя КГБ Г. Агеева; С. Лекарева, помощника заместителя председателя КГБ по контрразведке; В. Рубанова, начальника информационно-аналитического управления КГБ, и П. Никулина, первого заместителя начальника НИИ КГБ.

Естественно, что охранника В. Медведева и его ребят из «Альфы», которые брались обеспечить только физическую охрану самого Р. Вяхирева, «академики злых наук» легко переиграли. Они в срок представили научно обоснованную современную концепцию обеспечения экономической, технологической, информационной, физической и политической безопасности концерна. Им и отдали контракт на охрану «Газпрома». Правда, генерал В. Иваненко «слинял», предпочтя уйти в бизнес. Стал вице-президентом НК «ЮКОС». Вместо себя на роль руководителя Службы безопасности «Газпрома» в 1993 г. предложил отправленного в запас полковника КГБ В. Марущенко, который сразу же начал регулярно выезжать в служебные командировки в Германию.

Прокол БНД

Вскоре «Ругаз» выпустил информационный справочник объемом в 1000 страниц под названием «РАО «Газпром». Справочник поразил Р. Вяхирева тем, что в нем приводились сведения, состав-

ляющие коммерческую тайну «Газпрома». Как уже состоявшиеся, указывались назначения на руководящие посты ряда лиц, кандидатуры которых еще только обсуждались на совете директоров РАО. За «утечку» спросили со Службы безопасности. Спецы разбирались недолго. Представили справку о деятельности «Сименса» в России и в этой связи наметили план оперативных мероприятий Службы безопасности. В справке указали на то, что в России «Сименс» работает по всем традиционным направлениям деятельности БНД и присутствует в 30 регионах страны. Численность сотрудников российского «Сименса» приближается к 3 тысячам человек, которые работают на разведку ФРГ.

После этого В. Марущенко постепенно избавился от «мозгового треста» своей службы, отправив под разными предлогами на «заслуженный отдых» П. Грозу, А. Пичугина и П. Никулина.

Много воды утекло с той поры. Сменились кураторы и начальники СБ, а воз и ныне там. До настоящего времени в «Газпроме» пользуются телефонами «Сименса», постоянно рискуя коммерческой тайной. Утешаются тем, что «Ругаз» ввиду отсутствия собственных месторождений газа не конкурент «Газпрому».

Дураку ясно, что вся Россия напичкана немецким оборудованием, которое все прослушивает без всяких спутников. Ясно и то, что ФСБ пора обратить внимание на защиту коммерческой тайны «Газпрома». Последняя составляет тайну национального энергетического комплекса, а значит, государственную тайну, закон о которой нынче обсуждается в Госдуме.

Вячеслав МОРОЗОВ

КОМПЬЮТЕРРА
компьютерный еженедельник
28.10.08
#40 (756)

Национальные особенности шпионажа

Автор: Киви Берд

Параллельные миры

Тема шпионажа вообще и телефонного перехвата в частности представляется здесь очень подходящей по той причине, что позволяет наглядно проиллюстрировать проблему сразу на двух, так сказать, экранах, в параллели. Благодаря этому легче заметить общие черты и выделить принципиально важные моменты происходящего.

Для сравнения возьмем недавние шпионские скандалы в двух странах, США и Греции, высшие политики каждой из которых, независимо от партийной принадлежности, стабильно демонстрируют крайне лояльное отношение к - соответственно Израилю и Америке. другому государству.

О гранд-скандале с массовым прослушиванием телефонов в Греции, где под колпаком американской разведки работали около сотни видных политиков, начиная с главы государства и ключевых министров, «Компьютерра» подробно рассказывала в нескольких номерах 2006 года (№№ 626, 643, 653). Здесь же ударные моменты той истории мы привлечем лишь в качестве фона – для отображения похожих событий совсем другого шпионского скандала, разразившегося несколько раньше в США, однако в силу своей масштабности и глубокой секретности длящегося по сию пору.

В обоих случаях, как часто бывает, тайное стало явным благодаря стараниям прессы, а отнюдь не государственных служб безопасности, изо всех сил пытавшихся скрыть происходящее от народа. Но если в сравнительно небольшой Греции выявление мощной шпионской закладки в крупнейшей сети Vodafone Greece удавалось сохранять в тайне чуть меньше года, то в США – больше четырех лет, с 1997-го до конца 2001-го.

С карьерой несовместимо

В 1997 году, при расследовании одного из дел, связанных с нелегальной торговлей наркотиками в Лос-Анджелесе, было обнаружено, что информация, которой обменивались сотрудники ФБР, Секретной службы, Управления по контролю за наркотиками (DEA) и лос-анжелесской полиции, каким-то образом становилась известна преступникам. Наркодельцы (ведущую роль среди которых играли местные евреи или

выходцы из Израиля) заранее узнавали о ближайших планах полиции, о готовящихся операциях, а также о людях, с которыми контактировали следователи.

Главными подозреваемыми в утечке информации оказались две солидные хайтек-компании, Amdocs и Comverse Infosys, принадлежащие израильтянам. Amdocs делала (и делает) системы биллинга для большинства телефонных компаний в США, а потому имела все возможности для составления детальнейших отчетов-логов о том, кто кому и когда звонил. Вторая компания, Comverse Infosys – разработчик оборудования телефонного перехвата и сетевого мониторинга, которое используют для легального прослушивания правоохранительные органы не только во всех штатах Америки, но и во многих других странах мира.

Из-за тесных связей Comverse с правительством Израиля, которое почему-то оплачивало из государственного бюджета половину всех затрат этой частной фирмы на исследования и разработки, родилось естественное подозрение о наличии в оборудовании «черного хода». Через этот ход, как предполагается, израильская разведка могла бы тоже получать ту информацию, которую перехватывают правоохранительные органы (а может, и более того). Поскольку об этом канале компрометации, если он есть, наверняка известно и кому-то из сотрудников Comverse, нельзя исключать, что через них доступ к информации имели и наркодельцы.

Существенное отличие оборудования, поставляемого Comverse Infosys, от всех аналогов заключается в том, что специалисты изготовителя постоянно имеют доступ к уже работающей аппаратуре и программам. «Дабы обеспечивать их надежное и бесперебойное функционирование в течение всего срока эксплуатации», как разъясняется официально. При этом правоохранительные органы, осуществляющие перехват, как правило, смутно представляют, что за техники приходят проверять их аппаратуру и что именно они там делают (см. врезку «Голландский вариант»).

По свидетельству знающих людей, через ФБР из разных правоохранительных инстанций неоднократно проходили запросы на проведение более тщательного изучения систем Comverse и сомнительной практики их эксплуатации. Однако все эти попытки блокировались высшим руководством еще до того, как дело доходило до анализа оборудования и поиска в нем источников утечек. При этом практически все следователи американских спецслужб, словно сговорившись, признавались в беседах с журналистами, что расследовать или даже подозревать Израиль в шпионаже за Америкой через возможности Comverse равнозначно карьерному самоубийству.

Концы в воду

Эта тщательно скрывавшаяся история была обнародована ведущим журналистом телеканала Fox News Channel Карлом Кэмероном (Carl Cameron) лишь в декабре 2001 года. Как и в Греции, информацию о нехо-

роших делах во власти слили журналистам рядовые сотрудники спецслужб, которые, в отличие от политиков, хотят не только качественно выполнять свою непростую работу, но и оставаться при этом порядочными людьми.

Замалчивать происходящее многим показалось невозможным, поскольку в течение 2001 года в США были арестованы около 140 человек, подозревавшихся как участники огромной шпионской сети Израиля в стране (примерно 80 человек было задержано до 11 сентября и еще около 60 после, из них полдюжины были сотрудниками Comverse). Даже просто информация о высокой активности израильских шпионов в тот момент, когда вся страна пребывала в шоке от терактов и почтовых антракс-атак, была совсем некстати. Но в цикле передач Кэмерона имелось и нечто куда более серьезное – свидетельства тому, что разведка Израиля знала о грядущих терактах и не предупредила США. Фактически это можно было назвать предательством ближайшего союзника и покровителя. Сделанным, впрочем, по понятной причине – с политической точки зрения подобные события были Израилю чрезвычайно выгодны.

Особенно же показательно, сколь быстро и эффективно в США подавили нежелательную утечку. Цикл передач-расследований Кэмерона больше не повторялся, а сокращенную текстовую транскрипцию их содержания, выложенную на сайте Fox News, убрали в ту же неделю, когда она появилась. Официальное объяснение такого шага – «чтобы не порождать антисемитские настроения в обществе». Для сравнения: в менее управляемой Греции, чтобы утрясти скандал без последствий для виновных, потребовалось около полугода.

Среди других характерных акций типа «концы в воду» можно упомянуть мягкое, но настойчивое удаление с игрового поля руководителей фирм, невольно оказавшихся в центре скандала. В Греции таким боссом был глава регионального центра Ericsson по Юго-Восточной Европе Билл Зику (Bill Zikou), которого уже к началу лета 2006-го перевели куда подальше – в Австралию. Ericsson поставила Vodafone Greece то самое оборудование, в котором невидимо работала управляемая шпионами подсистема «легального перехвата». Разобраться, как такое вообще стало возможным, грекам не удалось, поскольку Ericsson категорически отказалась предоставить исходные коды программ.

В США дело было сложнее. Здесь требовалось удалить из непосредственного руководства Comverse израильских боссов, в первую очередь генерального директора Якоба «Коби» Александера, который в начале 1980-х годов собственными руками создал эту фирму буквально из ничего. К 2001 году Comverse стоила около полутора миллиардов долларов, сделав основателя очень и очень состоятельным человеком. Судя по всему, Александер наотрез отказался выпустить из рук кормило столь доходного предприятия. Тогда к нему применили другой «метод убеждения» – натравили налоговую и финансовую инспекцию. К весне 2006 года на Александера, а также на финансового директора и главного юрис-

консульта компании была собрана туча материалов, свидетельствующих о подделках и махинациях с ценными бумагами на сотню миллионов долларов. По американским законам это тянуло на 25 лет тюрьмы. Тогда Александер ударился в бега, в коих пребывает и по сию пору, скрываясь от американского правосудия в знойной Намибии. Где он ныне личными накоплениями укрепляет образование и внедряет высокие технологии в жизнь рядовых намибийцев.

Скомпрометированную Comverse Infosys сразу же после скандала переименовали в Verint, а в статьях Википедии, посвященных Comverse и лично Коби Александеру, нет ни слова ни про оборудование перехвата, ни про шпионский скандал.

Жертвы сотрудничества

В греческой истории единственной очевидной человеческой жертвой оказался топ-менеджер Vodafone Костас Цаликидис. Официально его гибель власти трактовали как самоубийство, хотя у следствия была масса убедительных свидетельств тому, что имело место хладнокровное устранение неудобного специалиста, узнавшего о происходящем и, вероятно, отказавшегося держать язык за зубами.

В ситуации со шпионским скандалом в США случайных жертв было неизмеримо больше – три с лишним тысячи человек погибли в результате терактов 11 сентября 2001 года и бездействия «дружественной» израильской разведки, утаившей имевшуюся у нее информацию.

Вместо эпилога

О том, что централизованные шпионские системы для тотального прослушивания и мониторинга коммуникационных сетей – это не только удобное, но и очень опасное обоюдоострое оружие, чреватое злоупотреблениями, давно предупреждают многие видные эксперты по безопасности. Не секрет и то, что хайтек-фирмы Израиля по давно сложившейся традиции имеют тесные связи с национальной разведкой и военными. Качественные системы фирм Amdocs и Comverse (известной отнюдь не только оборудованием прослушивания) тем временем продолжают внедрять все больше и больше стран, включая и Россию. Все подозрения о тайных «черных ходах» в израильской технике связи по сей день формально остаются лишь домыслами, поскольку ни одной закладки еще никто и нигде публично не продемонстрировал. Впрочем, никто их пока всерьез и не искал.

Голландский вариант

Оборудование Comverse/Verint для легального перехвата коммуникаций используют правоохранительные органы десятков стран. Включая и Нидерланды, где хватает политиков, свято чтящих принципы демократии

и пытающихся вынести на открытое обсуждение деликатные моменты в тайной работе полиции и спецслужб. Благодаря этому стало известно, что голландцы получали первые предупреждения о «черном ходе» в израильской аппаратуре прослушивания еще в 1998 году. Но главный скандал разразился в 2002-м, очевидно под влиянием взрывной публикации Fox News в США.

При новых разборках стало известно, что между голландской спецслужбой перехвата LIO и разведкой AIVD с одной стороны и израильтянами с другой было заключено «джентльменское соглашение», согласно которому оборудование Comverse продается со значительной скидкой, но за это доступ к обслуживанию техники будут иметь только специалисты компании. О предоставлении исходных текстов программ речи и тут не шло.

В итоге израильские специалисты получили постоянный доступ к аппаратуре прослушивания, причем все процедуры регулярного обслуживания (включая замену магнитооптических дисков) проходили исключительно с использованием национального языка Израиля (вплоть до специальных клавиатур на иврите). Короче говоря, голландцы не имели ни малейшего представления о том, что происходит при сервисных манипуляциях. При этом оплата израильского премиум-обслуживания обошлась гораздо дороже самого оборудования.

(Публикуется с сокращениями)

Открытое письмо

Президенту Российской Федерации
В.В. ПУТИНУ

Заместителю Председателя Правительства Российской Федерации
Министру Обороны Российской Федерации
С.Б. ИВАНОВУ

Председателю Совета Федерации
Федерального Собрания Российской Федерации
С.М. МИРОНОВУ

Председателю Государственной Думы
Федерального Собрания Российской Федерации
Б.В. ГРЫЗЛОВУ

Глубокую тревогу научного мира России вызывает состояние информационной безопасности нашей страны. Широкое применение зарубежных средств вычислительной и телекоммуникационной техники, программного и информационного обеспечения привело к тому, что сегодня российский рынок информационных технологий более чем на 90% представлен средствами импортного производства. Такая ситуация позволяется сделать вывод о финансовой и технической зависимости от западных поставщиков, что помимо угроз отечественной индустрии информации, возникает целый ряд угроз национальному информационному пространству. За счет активного участия зарубежных фирм в процессе информатизации органов государственной власти практически все информационные ресурсы страны, включая «ресурсы критических систем», оказались под контролем соответствующих иностранных структур. Нельзя не отметить, что этим наносится огромный урон и национальной экономике – ведь за наши государственные деньги развиваются не отечественные, а частные западные компании.

Документами, определяющими политику государства на современном этапе в области обеспечения информационной безопасности, является Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10 января 2000 года и Доктрина Информационной Безопасности, утвержденная Президентом Российской Федерации 9 сентября 2000 года, которая развивает вышеуказанную Концепцию применительно к информационной сфере.

В Доктрине отмечается, что «Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, а также ... обеспечению эффективного использования отечественных информационных ресурсов могут являться:

– закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных

аналогов, не уступающих по своим характеристикам зарубежным образцам ...;

– создание условий для усиления технологической зависимости России в области современных информационных технологий».

К глубокому сожалению, положения данной Доктрины не имеют обязательного характера, вследствие этого не принимаются государственными чиновниками во внимание.

Многие промышленно развитые страны, сознавая подобную угрозу для своих информационных ресурсов, отказываются от использования импортных программно-аппаратных средств и несмотря на значительные затраты, разрабатывают собственные средства информатизации и даже собственные языки программирования. По такому пути уже пошли Германия, Франция, Великобритания; даже в Пентагоне в последние годы наблюдается рост применения собственного программного обеспечения в военных разработках. Интересно, что и в недавно подписанном Джорджем Бушем документе «Стратегии информационной безопасности» накладываются ограничения на использование иностранного программного обеспечения в стратегических отраслях США.

Именно поэтому сегодня так важно, чтобы закон «Об информационных технологиях и защите информации», который в прошлом году в Государственной Думе преодолел первое чтение, а в настоящее время готовится ко второму, содержал положения, препятствующие возникновению угроз безопасности стратегической информации.

С учетом сложившейся ситуацией, ряд депутатов Государственной Думы Федерального Собрания Российской Федерации внесли поправку в проект федерального закона «Об информации, информационных технологиях и их защите», которая предусматривает запрет использования западных программно-технических средств в стратегических отраслях и на особо важных (опасных) объектах. Перечень вышеназванных объектов, должен быть установлен Правительством Российской Федерации в течение одного года с даты принятия закона. Данная поправка позволила бы придать положениям Доктрины нормативный правовой статус.

По нашему глубокому убеждению их суть сводится к тому, чтобы запретить использование зарубежных программно-технических средств в государственных информационных системах, обеспечивающих стратегические отрасли и особо опасные (важные) объекты РФ, а также, помимо прочих мер защиты информации (уже включенных в текст закона), не допускать наличия в программно-технических средствах недокументированных функций. Сегодня эта проблема – использования иностранного программного обеспечения (и системного, и прикладного) – для России очень критична. Чтобы не повторить судьбы Ирака, нам необходим именно законодательный запрет иностранного программного обеспечения для того, чтобы стратегические отрасли обеспечить отечественной ИТ-продукцией. И главное, что такие разработки у нас есть.

Мы отдаем себе отчет в том, что путь предложенных депутатами Государственной Думы законодательных инициатив, позволяющих не только

поддержать отечественных производителей программно-аппаратных средств, но и существенно повысить информационную безопасность, будет не легким: приходится констатировать, что в нашей стране сложилось мощное лобби, помогающее продавливать закупки импортного программного обеспечения, страна просто подсажена на программную иглу. А между тем программисты до сих пор уезжают работать за рубеж, и мы теряем не только человеческий потенциал, но и уверенность в собственной национальной безопасности.

Мы убеждены, что принятие указанных поправок будет способствовать и тому прорыву в инновационной сфере, к которому нас призывает Президент страны.

В этой связи просим вас поддержать поправку, находящуюся на рассмотрении Государственной Думы о недопустимости использования зарубежных программно-технических средств в стратегических отраслях и на особо важных (опасных) объектах Российской Федерации.

Просим считать данное письмо официальным обращением в Ваш адрес:

С глубоким уважением,

д.т.н. Академик РАЕН
Ковалевский С.С.
Зав. сектором ИПУ РАН,
д.т.н., проф., Академик РАЕН /Путов В.А./
Главный научный сотрудник
ИПУ РАН /Косяченко С.А./

Зав. отделом докторантуры и аспирантуры ИПУ РАН,
д.т.н., проф. /Малошик В.Д./

Зам. директора ИПУ РАН
д.т.н. проф /Павлов Б.Н./

Зам. директора ИПУ РАН
д.т.н. проф. /Новиков Д.А./

Зав. лабораторией, д.т.н. /Либерзон В.Г./

Зав. лабораторией ИПУ РАН
д.т.н. проф. Академик РАЕН /Бурковский В.Г./

Главный научный сотрудник ИПУ РАН
д.т.н., профессор /Щербаков П.С./
Зав. кафедрой ВГИСУ
д.э.н. проф. Бурлаков

Кто поддержит отечественных разработчиков и производителей?

Проблемы отечественных разработок и производства телекоммуникационного оборудования за последние 10-15 лет вышли из рамок сугубо технических и технологических и перешли в разряд *политических* проблем, напрямую связанных с задачами обеспечения *информационной безопасности* России. Суть их заключается в том, что, например, США изначально строили для нужд обороны цифровую выделенную сеть связи исключительно на своём отечественном оборудовании и только трёх типов станций. Китай – на основе четырёх типов станций, и опять же своих. И только в России аналогичное оборудование сегодня насчитывает 80 типов, среди которых большинство – импортное. Такое многообразие по числу и принадлежности производителей не безопасно, так как электросвязь, кроме всего прочего, ещё и стратегическое средство управления государством, армией, производством и объектами жизнеобеспечения страны. И передать это средство в руки зарубежных программистов, по меньшей мере, недальновидно, так как это открывает спецслужбам недружественных стран неограниченные возможности для несанкционированного доступа в российскую сеть связи, дистанционного управления ею из любой точки планеты и из космоса, перепрограммирования и даже разрушения системы связи страны в кризисные моменты.

Сегодня более 40 крупнейших зарубежных компаний осуществляют поставки оборудования в Россию напрямую или через своих дилеров. Пользуясь политической и массированной финансовой поддержкой своих правительств, налоговыми льготами, обладая достаточными оборотными и заемными капиталами, эти фирмы практически вытеснили с российского рынка отечественных разработчиков и производителей.

Экономическая экспансия осуществляется с помощью уже хорошо отработанных в странах третьего мира схем. Это и создание с помощью иностранных банков совместных производств на территории завоеванных рынков, что из-за дешевизны рабочей силы почти вдвое снижает стоимость продукции и повышает её конкурентоспособность. Это и предоставление необыкновенно выгодных лизинговых и кредитных схем российским операторам связи для приобретения импортного оборудования. Среди таких схем особо популярно целевое кредитование заказчиков страной, в которой и закупается оборудование. Особенно активно пользуются этой методикой европейские и китайские банки для продвижения продукции своих стран.

Подобное «благодеяние» испытал на себе филиал «Связьинвеста» в Южном федеральном округе ОАО «ЮТК», который при прежнем руководстве активно и по крайне высоким ценам закупал импортное оборудование. Сегодня долг ОАО «ЮТК» составляет свыше 1 млрд долларов,

а компания практически завершила своё развитие и уже не способна выполнить целевую Федеральную программу по телефонизации села.

Это и демпинговые цены, и, так называемые, «подарки» – то есть бесплатные поставки отдельных частей оборудования. Например, предполагается строительство большого коммутационного узла связи у какой-нибудь федеральной структуры. Необходимое условие – проведение конкурсных торгов, которые трудно пройти законно с дорогим импортным оборудованием. Тогда фирма–поставщик в качестве спонсорской помощи дарит элемент своей системы, а потом заказчик вынужден проводить конкурсные торги на доукомплектование (подаренного) оборудования. Отечественный производитель, имеющий конкурентоспособное оборудование, в этом случае просто не будет допущен к конкурсу.

Активно создаются и холдинговые структуры, в которые вовлекаются российские банки и операторы связи, в результате чего операторы опосредованно переходят в собственность своих «инвесторов». А почти полное финансирование всех российских специализированных технических журналов, выставок, конференций, семинаров, повсеместные взятки и «откаты» сделали зарубежное оборудование настолько привлекательным, что сегодня уже практически никто не задумывается над тем, что, в конечном итоге, щедрость зарубежных вендоров оплачивается из карманов российских пользователей электросвязи. И не зарубежье сейчас инвестирует развитие нашей отечественной электросвязи, а Россия инвестирует сохранение и развитие разработок и производства за рубежом.

Особую активность проявляет концерн Siemens, который создал 11 совместных предприятий и одно предприятие со 100-процентным иностранным капиталом, получил крупные заказы на строительство магистральных и местных коммуникационных линий, на выполнение ряда проектов некоторых металлургических заводов, на реконструкцию ТЭЦ и автоматизацию сборочных линий ГАЗа. Концерн приобрел крупные пакеты акций ряда российских предприятий, в частности Калужского турбинного завода, АО «Электросила». При этом продвижение на российский рынок не происходит бессистемно. Siemens образовал структуры для координации своих действий и анализа российских условий. В концерне создан спецотдел, который занимается проблемами организации финансовых потоков в России, выработкой мер для успешного функционирования.

Не менее активна и появившаяся из недр концерна Siemens – компания «Искрател», базирующаяся в Словении и выпускающая телекоммуникационное оборудование под торговой маркой Si-2000 (Si – производное от Siemens). Сегодня это оборудование, но уже как отечественное, продвигает на сети связи Министерства обороны екатеринбургская фирма «ИскраУралТел».

Наступательна и деятельность финской фирмы Nokia, которая заняла одно из ведущих мест на нашем рынке радиотелефонов, пользуется услугами обширной дилерской сети, реализует проекты по созданию телефонных станций, телекоммуникационных линий и систем сотовой связи, поставляет приборы для российских научно-исследовательских институтов.

На российском рынке в реализации оборудования связи и телекоммуникаций, кроме вышеназванных, доминируют японская компания NEC, французский концерн Alcatel, американская компания Avaya, китайские частная компания Huawei Technologies и государственная – ZTE, южнокорейская компания Corecess и другие.

В то же время отечественные разработки и производство телекоммуникационного оборудования брошены на произвол судьбы. Ими не занимается ни одно из существующих российских министерств и ведомств. Они находятся фактически вне закона. Их интересы не представлены ни в Федеральном законе «О связи», ни в реально действующих федеральных программах. Их игнорирует Мининформсвязи РФ, в штате которого нет чиновника, ответственного за развитие телекоммуникационной индустрии страны.

По идее, одним из ведомств, заинтересованных в развитии отечественного наукоемкого производства средств связи, должно быть Минпромэнерго. Но в его руководящих документах, в том числе проекте концепции «Основные направления государственной научно-технической политики в промышленности России», нет ни слова о создании современного телекоммуникационного оборудования. А в структуре министерства не предусмотрены подразделения, ответственные за развитие соответствующего производства.

Таким образом российское производство телекоммуникационного оборудования оказалось вне государственных программ и развивалось стихийно. Большинство образовало всё те же совместные предприятия, использующие зарубежные разработки, технологии, оборудование, комплектующие изделия, программное обеспечение. Такие компании-сателлиты сейчас активно пробиваются с финансовой помощью своих хозяев на закрытые ведомственные сети электросвязи всех силовых структур России. И не безуспешно. Только в «Перечне техники связи двойного назначения, используемой в Вооруженных Силах Российской Федерации», который 18 января 2006 года утвердили заместитель начальника ГШ ВС РФ и руководитель Федерального агентства связи, оказались и словенско-немецкая АТС SI 2000 и наполовину немецкая – DX-500.

Научно-производственное предприятие «СПЕЦСТРОЙ-СВЯЗЬ» – головное предприятие группы компаний – десятый год поставляет на сети электросвязи России цифровые АТС «Протон-ССС», которые являются полностью отечественной разработкой. Эти платформы объеди-

няют в себе спектр оборудования от простой каналообразующей аппаратуры, малой УПАТС, АТС ведомственной связи, сельской узловой, оконечной, центральной АТС до интеллектуальной мультисервисной системы (МСС) городской АТС.

ЦАТС «Протон-ССС» сертифицирована Министерством информационных технологий и связи РФ, имеет ведомственные сертификаты силовых и госструктур. Предприятие получило лицензию № 136 Государственной технической комиссии при Президенте РФ на проведение работ, связанных с созданием средств защиты информации, а ЦАТС «Протон-ССС» сертифицирована (сертификат № 755) Гостехкомиссией при Президенте РФ как оборудование с комплексом средств защиты информации от несанкционированного доступа. Есть и лицензия Б 294940 № 629 ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну. Система менеджмента качества на всех предприятиях-изготовителях «Протон-ССС» соответствует требованиям ГОСТ РВ 15 002-2003 Системы добровольной сертификации «Военный регистр», все они имеют соответствующие заключения и военную приемку.

«Протон-ССС» сегодня успешно эксплуатируются во всех субъектах Российской Федерации, более чем в 400 населенных пунктах России и стран СНГ. Наиболее активно это оборудование используют на своих сетях различные структуры ФСИН Минюста, МВД, МЧС, РАО «ЕЭС» и ОАО «РЖД». «Протон-ССС» используются для восстановления ведомственных сетей электросвязи силовых структур Чеченской Республики, эксплуатируются на объектах Министерства обороны РФ: в штабах и воинских частях ВВС, на узлах связи военно-морских баз и в воинских частях флотилий, в военных комиссариатах краев и областей.

Однако, несмотря на всеобщее (среди связистов) признание, прекрасные отзывы тех, кто уже эксплуатирует «Протон-ССС» и полное отсутствие рекламаций, продвижение нашего оборудования на российском рынке телекоммуникаций испытывает жесточайшее противодействие вендоров.

Серийный выпуск «Протон-ССС» осуществляют предприятия оборонно-промышленного комплекса в Подмосковье, в Ростове-на-Дону, Рязани, Екатеринбурге, Уфе. Ростовское ФГУП «Алмаз» – основной партнер НПП «СПЕЦСТРОЙ-СВЯЗЬ» по выпуску «Протон-ССС» – вошло в состав ОАО «Концерн «Созвездие», созданного в рамках Федеральной целевой программы «Формирование и развитие оборонно-промышленного комплекса на 2002-2006 годы».

Все предприятия-партнеры способны ежегодно выпускать свыше 1 млн портов (номеров) в год, однако им едва удается реализовывать ежегодно около 100 тыс. портов. И такая недозагруженность предприятий оборонно-промышленного комплекса происходит не без «помощи» Министерства обороны РФ.

В Военной академии связи Санкт-Петербурга и Новочеркасском высшем военном командном училище связи (на основании договоров о научно-техническом сотрудничестве с НПП «СПЕЦСТРОЙ-СВЯЗЬ») ЦАТС «Протон-ССС» не только включена в программу обучения, но и используется для проведения научно-исследовательских работ (НИР) и опытно-конструкторских разработок (ОКР) в области телекоммуникаций.

Начальник военной академии связи включил представителя НПП «СПЕЦСТРОЙ-СВЯЗЬ» в состав научно-технического совета, который готовит рекомендации по корректировке и реализации «Программы поэтапного перевода вторичных сетей связи ВС РФ на цифровое оборудование обработки информации и предоставления услуг» и «Программы оснащения полевых войск связи ВС РФ современными системами, комплексами и средствами связи и автоматизации управления». Опыт совместной работы академии с НПП «СПЕЦСТРОЙ-СВЯЗЬ» позволил её руководству рекомендовать начальнику связи ВС РФ и начальнику управления заказов и поставок ВС РФ включить группу компаний «Протон-ССС» в кооперацию предприятий по созданию современной информационно-телекоммуникационной системы ВС РФ на постоянной и долговременной основе.

Со своей стороны и Начальник связи ВС РФ включил представителя НПП «СПЕЦСТРОЙ-СВЯЗЬ» в состав рабочей группы для выработки предложений по созданию защищенной мультисервисной телекоммуникационной сети Минобороны и лично рекомендовал «Протон-ССС» для использования на сетях связи МО.

Однако, когда дело доходит до конкретного сотрудничества с другими структурами Министерства обороны и, главным образом, с управлениями закупок и поставок конкретных воинских частей, в силу вступают совершенно иные принципы взаимодействия, явно противоречащие и компетентным рекомендациям, и Федеральному закону № 94-ФЗ от 08.07.05 г., и Указу Президента РФ № 305 «О первоочередных мерах по предотвращению коррупции и сокращению бюджетных расходов при организации закупок продукции для государственных нужд».

Примером тому может служить конкурс на поставку оборудования для воинской части № 87406, где начальником управления закупок и поставок служит генерал-лейтенант Александр Борисович Михайловский.

Этот конкурс был объявлен 30 декабря 2005 года. В связи с новогодними праздниками никто, из желающих участвовать в конкурсе, готовиться к нему до 10 января не мог. Между тем конкурсная документация была выдана только 16 января, а её сдача назначена уже на 20 января. И, естественно, за четыре дня неосведомленные, то есть «нежелательные» участники (в том числе и дилеры НПП «СПЕЦСТРОЙ-СВЯЗЬ») подготовить эту документацию в полном объеме тоже не успели. В результате к конкурсу были допущены только две пары поставщиков, каждая из

которых предлагала аналогичное оборудование. И у той и у другой пары оборудование стоило в два раза (а по некоторым позициям в 4-5 раз) дороже, чем у поставщиков не допущенных к конкурсу.

Поэтому и само проведение конкурса изобиловало массой нарушений.

Во-первых, конкурс проводился не в соответствии с нормами Федерального закона № 94-ФЗ от 08.07.05 г., а в соответствии с нормами уже отмененного Федерального закона № 97-ФЗ от 06.05.99 г.

Во-вторых, в нарушение ст.22 п.2,3 закона 94-ФЗ в конкурсной документации безальтернативно было указано конкретное оборудование;

в нарушение ст. 15 не велась аудиозапись конкурса;

в нарушение ст. 5 ограничено количество участников конкурса, а конкурс на поставку аналогичного оборудования отменен за день до окончания срока сдачи заявок и т.д. и т.п.

В-третьих, были грубо нарушены требования, изложенные в статьях 5, 22, 44 Указа № 305 Президента РФ.

Аналогичные нарушения в этой же войсковой части были допущены и при проведении конкурса на поставку цифровых междугородних телефонных коммутаторов, который был проведен 6 февраля т.г.

Эти и аналогичные конкурсы свидетельствуют о явной предвзятости и заинтересованности руководителей управлений закупок и поставок воинских частей.

Следовательно, нужна государственная программа поддержки отечественных разработчиков и производителей телекоммуникационного оборудования, закрепление их за определенным министерством.

Эволюция отечественных разработок на рынке телекоммуникаций

Связь – это не только важная составная часть инфраструктуры общества, но и один из основных рычагов управления государства и его силовых структур. Осознание этого постулата в СССР приходится на начало 60-х годов прошлого столетия, когда после десятилетий застоя в сфере разработок отечественного коммутационного оборудования было предпринято несколько попыток создать свои, отвечающие современным требованиям, советские образцы электронных, а затем и цифровых АТС.

Первая из таких попыток проводилась Ленинградским отраслевым НИИ связи (ЛОНИИС). За основу новой разработки была взята платформа финской станции DX-200, которая к 1990 году с помощью специалистов из стран Совета экономической взаимопомощи (СЭВ) и на основе, пока ещё слабо развитой, отечественной элементной базы должна была превратиться в первую цифровую АТСЦ-90. Однако по ряду причин эти разработки не принесли практических результатов.

В связи с этим было принято правительственное решение о закупке за рубежом лицензии на производство электронных АТС и в 1979 году был заключен контракт с французской фирмой «АЛКАТЕЛЬ-СИТ» на поставку конструкторской документации и технологического оборудования для серийного выпуска самого перспективного на ту пору средства коммутации ЭАТС МТ-20/25. Серийное производство этой платформы началось в СССР только в 1988 году.

Параллельно велись поиски и рижскими разработчиками, продукция которых под торговой маркой «Квант» хотя и приобрела известность, но не успела найти широкого применения на Единых сетях электросвязи (ЕСС) СССР.

Процессы перестройки экономики, начатые в начале 90-х годов, остановили на взлёте отечественных разработчиков, разорвали устоявшиеся связи производителей коммутационного оборудования с поставщиками комплектующих изделий, резко снизили качество отечественной микроэлектронной элементной базы, разрушили производство практически всех отечественных АТС. На рынке средств связи образовался вакуум готовый всосать любое предложение. Однако зарубежная продукция в ту пору была для нас слишком дорогой. Годовой бюджет России составлял всего $20 млрд., средняя заработная плата не превышала $20, а стоимость импортной техники, как и сегодня, оставалась константной и составляла всё те же $100 за порт (и выше).

Взрыв спроса и породил активное развитие отечественных компаний по разработке коммутационного оборудования. Мгновенно образовалось (по данным Союза производителей и потребителей оборудования и средств связи) более 350 фирм, заявивших о готовности удовлетворить

спрос рынка. При этом большинство из них интересовалось не проблемами развития телекоммуникаций, а прибылью в кратчайшие сроки.

На этом этапе чётко сформировались два течения разработчиков. У истоков первого – стояли практики-связисты и разработчики, которые пришли с заводов, где они долгое время занимались русификацией зарубежных станций. Эти люди прекрасно ориентировались в технике и хорошо знали стандарты, распространенные на наших сетях связи, а информация о стандартах была тогда одной из самых закрытых тем.

К примеру, только в 90-х годах наконец-то стал доступен сборник общегосударственных стандартов телефонии (ОГСТфС), который был выпущен в количестве всего 3000 экземпляров на весь Советский Союз и только для служебного пользования. Такая засекреченность и привела к тому, что после развала Советского союза и ликвидации централизованного управления практически каждый узел связи стал отступать от принятых стандартов сигналов управления взаимодействием АТС (СУВ).

И всё же главным недостатком этого течения разработчиков-практиков была их слабая теоретическая подготовка в области микроэлектронной элементной базы и организации процессорных систем. Они были способны либо совершенствовать то, что уже разработали их предшественники, либо слепо копировать зарубежные образцы.

Второе течение разработчиков вышло из научно-исследовательских институтов, в том числе и из закрытых предприятий, которые занимались космической связью. Они имели прекрасную теоретическую подготовку, были высококлассными системотехниками, но очень слабо ориентировались в нуждах и возможностях российских сетей связи, а о существующих стандартах телефонии вообще знали только понаслышке.

В результате на рынке стало появляться оборудование тоже двух типов. Это были платформы либо слегка модернизированных, но устаревших образцов, либо цифровые станции, не соответствующие стандартам, с совершенно неожиданными техническими характеристиками, которые ставили в тупик опытных связистов.

Например, НПО «Раскат» выпустило АТС «Омега», в которой вызов осуществлялся переполюсовкой 60 вольт вместо синусоиды 95 вольт, 25 герц. Эти же разработчики были убеждены, что ИКМ-поток – это одно направление и были очень удивлены, когда заказчик в Краснодарском крае потребовал выделить из ИКМ-потока несколько направлений.

В это же время компания «Мультиком» вышла на рынок с платформой, которая подавала питание на телефон не 60, а 28 вольт.

Воронежский НИИ связи разработал цифровую АТС на самых современных микросхемах выполненных в золоте. К тому же для оцифровки сигналов разработчики почему-то применили не стандартные фильтры или кодеки, а обычные цифроаналоговые преобразователи. Стоимость оборудования оказалась заоблачной.

ЦНИИС разработал цифровую систему С32, идеология которой была очень современной, но совершенно отличной от всех существующих в мире стандартов связи.

Подобных изысков было множество, и всё же дефицит оборудования и дешевизна отечественной техники вынуждали связистов приобретать экзотические новинки и вместе с разработчиками доводить их уже на сетях связи до необходимой кондиции. На всё это требовались дополнительные затраты времени, финансов и ...нервной энергии, что в конечном итоге и сформировало у эксплуатационников твёрдое и на долгие времена предубежденное мнение о неспособности отечественных разработчиков конкурировать с зарубежными коллегами.

В 1994 году началась структурная перестройка отрасли связи. У акционированных предприятий появилась возможность резкого увеличения ввода номерной емкости и модернизации сетей связи. Однако, уже сформированное предвзятое мнение о соотечественниках и необыкновенная привлекательность лизинговых схем иностранцев вынудили операторов связи направить финансовые потоки не на активизацию отечественных разработок и развитие собственного производства, а на поддержку зарубежных производителей. В результате российские валютные средства с ежегодным объемом $$500-520 млн. стали поступать на счета компаний Siemens, Ericsson, Nokia, NEC, Alcatel, Lucent, Iskratel, Nortel, Sumsung и других сорока крупнейших зарубежных компаний, которые начали осуществлять поставки оборудования в Россию напрямую или через своих дилеров.

При этом следует заметить, что речь идёт лишь об объемах затрат операторов связи. А владельцы ведомственных и корпоративных сетей этот отток капиталов, по меньшей мере, увеличили вдвое. И, что очень важно, наши финансовые вливания пришлись весьма кстати: сегодня уже все аналитики мирового рынка телекоммуникаций отмечают, что именно с 1991 года на этом рынке стали проявляться первые признаки стагнации.

В результате к настоящему времени в нашей стране все цифровые станции на международном и междугородном уровне – зарубежного производства, на местной телефонной сети – 80 % импортного оборудования, на ведомственных и корпоративных сетях – 90 %. Да и в целом ЕСС России стали представлять из себя весьма эклектичное образование, состоящее из нескольких «археологических наслоений»: новейшие цифровые АТС соседствуют здесь и с декадно-шаговыми, и с аналоговыми, и с квазиэлектронными станциями, а сам набор зарубежных цифровых АТС насчитывает уже более 80 моделей.

Это многообразие и породило проблему, о которой впервые заговорили лишь десять лет спустя, хотя критичность сложившейся ситуации ученые и специалисты по информационной безопасности отмечали изначально.

Встревоженность всех слоев общества подтвердила своевременность принятия Советом безопасности РФ «Стратегии развития информационного общества в России», в которой была сформулирована экстренная необходимость импортозамещения в сфере инфотелекоммуникаций.

Впервые за последние 15 лет связисты вновь обратили внимание на отечественных разработчиков, сохраняя при этом своё предвзятое отношение к ним и их продукции. Между тем, за истекшие годы ситуация в этой сфере кардинально изменилась.

Во-первых, два течения разработчиков («практики» и «теоретики») наконец-то слились в единый поток, породив интеллектуальный конгломерат, который по уровню теоретической подготовки уже ни в чём не уступает зарубежным специалистам, а по знаниям специфической практики построения российских сетей электросвязи и многократно их превосходит.

Во-вторых, на порядок уменьшилось количество фирм занятых производством отечественного оборудования, а тех, кто практически занимается его разработкой, вообще осталось считанные единицы. Все, кто видели смысл своего существования в быстром извлечении прибыли, либо переквалифицировались в дилеров зарубежных компаний, либо занялись сборкой их продукции на своих производственных площадях. Не выдержали конкуренции и компании, которые не сумели объединить в своих разработках новейшие мировые тенденции развития телекоммуникаций со специфическими российскими стандартами. В результате только небольшое число компаний Российской Федерации выстояло и адаптировалось в новых экономических условиях. Среди них Группа компаний «Протон-ССС» со своим головным предприятием НПП «СПЕЦСТРОЙ-СВЯЗЬ» (торговая марка «Протон-ССС») фирма АЛС и ТЕК (АЛС), Русская телефонная компания («Элком», «Магеллан»), НПО «Раскат» («Омега»), ЛОНИИС («АТСЦ-90»), «Импульс» («Квант-Е»), ООО «Телеинформ» («Сигма»), ОАО «Псковский завод АТС (PS-2000). Эти предприятия самостоятельно разработали, выпускали и продолжают выпускать современные отечественные телекоммуникационные платформы.

В-третьих, по уровню качества и надежности лучшие образцы отечественной техники, к которым можно отнести и телекоммуникационные платформы «Протон-ССС», сегодня уже не редко превосходят зарубежные аналоги, а по уровню обеспечения информационной безопасности им просто нет равных. И достигнуто такое превосходство тем, что в наших разработках, при всех прочих равных составляющих (элементная база, технологии), дополнительно учтены и отработаны все особенности российских сетей связи, их, так называемое, «бездорожье», все специфические требования связистов различных ведомств, в том числе и силовых структур.

В-четвёртых, отечественная техника сегодня уже не дешевле, а зачастую и дороже зарубежной. И это вполне объяснимо: небольшие объёмы

производства, при всех прочих равных условиях создания аналогичного оборудования, не позволяют снизить её себестоимость. Но стоит изменить объёмы заказов, перенаправить финансовые потоки и российские конвейеры окажутся не менее выгодными для российских заказчиков, чем зарубежные.

И, наконец, за прошедшие годы появилось ещё одно, стратегически важное отличие отечественных компаний разработчиков от зарубежных. Нас отличает маневренность и гибкость.

Любая зарубежная фирма, которая уже давно существует на рынке, крайне консервативна. Она накрепко привязана к своим собственным решениям, которые однажды принесли ей успех, и поэтому никогда не совершает никаких резкий шагов в изменении направления разработок.

У отечественных компаний такой консерватизм ещё не успел созреть. У нас не было и нет безоговорочных авторитетов в сфере разработок. Мы не ориентируемся на большие интегральные схемы брэндовых производителей, а работаем на программируемых логических матрицах. Всё это позволяет нам в меньшей степени привязываться к конкретному производителю комплектующих изделий и сохранять гибкость во всех сложных ситуациях, которые возникали либо ещё будут возникать на рынке. Мало того, после возрождения отечественной элементной базы мы без труда сможем перейти и на её использование в своих разработках.

И поэтому есть надежда, что сегодня, когда так остро встал вопрос об обеспечении информационной безопасности России, вновь, как и полвека назад, вспомнится постулат о стратегической важности связи, которая является не только составной частью инфраструктуры общества, но и одним из основных рычагов управления государства и его силовых структур. И этот рычаг ни при каких обстоятельствах нельзя передавать в руки зарубежных разработчиков.

Три проблемы построения и эксплуатации ведомственных и корпоративных сетей электросвязи России

У большинства крупных ведомств и корпораций России, эксплуатирующих свои выделенные сети электросвязи не одно десятилетие, они, как правило, весьма эклектичны и состоят из многих «археологических наслоений», среди которых нередко встречаются и декадно-шаговые, и аналоговые, и квазиэлектронные станции. И перед владельцами таких сетей, решивших заняться их модернизацией, неизбежно встают два вопроса: «как?» и «кто?».

Как выполнить столь масштабные работы, если в штате ведомства нет специалистов по строительству сетей? Как с минимальными затратами выполнить максимальный объём работ? Нужно ли в процессе модернизации перестраивать всю сеть или достаточно заметить устаревшие АТС на цифровые? Следует ли модернизировать всю сеть сразу, переводя её на технологии NGN, или можно это сделать поэтапно, не торопясь и без больших финансовых затрат?

И не находя самостоятельно ответов, задают себе следующий вопрос: «кто?». Кто грамотно и квалифицированно проведёт предпроектное обследование устаревших сетей? Кто выполнит проектирование новых объектов, систем и сетей связи? Кто интегрирует новые объекты с существующими системами связи и сетями передачи данных? Кто примет на себя функции генеральных проектировщика и подрядчика? Кто примет на себя обязательства по сервисному обслуживанию модернизированных сетей связи? Иными словами, кто сможет оказать полный комплекс услуг инжиниринга?

К сожалению отечественных предприятий, занимающихся инжинирингом в истинном смысле этого слова крайне мало. Зато в избытке фирм, именующих себя системными интеграторами, а на деле, осуществляющих лишь дилерские функции множества зарубежных компаний захвативших уже на 90 % российский рынок. В результате на всех ведомственных сетях от Калининграда до Камчатки насчитывается уже более 80 типов цифровых АТС (ЦАТС) произведенных в США, Канаде, Западной Европе, Израиле, Японии, Южной Корее и Китае.

Это многообразие и породило три основные проблемы построения и эксплуатации современных ведомственных и корпоративных сетей электросвязи.

Первую проблему можно условно назвать «проблемой привязки».

Дело в том, что среди различных представителей высокотехнологичной продукции – ЦАТС можно, безусловно, назвать долгожительницей: средний срок её эксплуатации составляет 15-20 лет. А, принимая во внимание то обстоятельство, что за первой покупкой телекоммуникационного оборудования неизбежно начинается череда его модернизаций, следует иметь

в виду, что первая покупка на долгие годы «привязывает» покупателя к тому производителю, которого он выбрал изначально.

Таким образом, вопрос поддержания на должном техническом уровне ведомственной сети, построенной на новом оборудовании, неизбежно попадает в зависимость и от правильности и своевременности технических нововведений производителя, и от его политики продаж.

Первая проблема с неизбежностью породила и вторую, связанную с необходимостью грамотно эксплуатировать импортное оборудование, обновлять его программное обеспечение и развивать ведомственные сети связи. И если с первой задачей – эксплуатацией – владельцы сетей справляются достаточно легко, так как уровень подготовки их технического персонала узкого профиля позволяет это делать вполне профессионально, то две другие задачи им уже не по силам. И здесь снова приходят на помощь вендоры. Их сервисные центры и системные интеграторы взяли на себя «непосильный труд» модернизации российских ведомственных сетей. В результате за последние 10-15 лет у владельцев сетей задача подготовки собственных квалифицированных кадров связистов и их своевременной ротации отошла на второй план. А процесс подготовки невостребованных кадров в учебных заведениях с одной стороны сократился, а с другой – усложнился: попробуйте, не говоря уже об основных и профилирующих дисциплинах, загрузить студента ещё и обширной информацией об особенностях 80-ти моделей УПАТС, с которыми ему придётся работать на сетях электросвязи России!

Таким образом, вторую проблему ведомственных и корпоративных сетей электросвязи можно обозначить как «проблему кадровую».

О третьей проблеме, порожденной многообразием импортного телекоммуникационного оборудования, впервые заговорили лет пять-семь назад. Хотя критичность сложившейся ситуации стали отмечать значительно позже.

Специалисты силовых структур России своевременно отреагировали на возникновение этой проблемы, о чём свидетельствует статья начальника управления заказов и поставок МО РФ генерал-лейтенанта А. Б. Михайловского в Федеральном справочнике «Информационные технологии и связь в Российской федерации» (№ 6 за 2006-2007 гг.). В ней он прямо говорит о том, что

«Применение информационно-коммуникационных технологий в системе управления ВС РФ привело к качественно новой форме вооруженной борьбы – информационному противоборству, то есть преднамеренному воздействию на автоматизированные системы противника и защиту собственных систем».
И при этом подчеркивает, что «системы связи ВС РФ рассматриваются в качестве первоочередных объектов информационного воздействия противника, и их информационная безопасность во многом определяется доверенностью программного обеспечения...

Этому требованию не отвечают зарубежные программные средства. В них могут быть умышленно включены программные закладки – элементы информационного оружия...»

К этому следует добавить, что третья проблема ведомственных сетей – «проблема доверенности» – гораздо шире, чем её военно-стратегическая

составляющая. И, рассмотренная во всём своём объёме, она даёт ответ и на решение «проблемы привязки».

Во-первых, и это не следует забывать, что электросвязь – действительно стратегическое средство управления. И не только управления армией, но и государством, объектами жизнеобеспечения страны, всей промышленностью. От надежности и информационной безопасности этого средства зависит и конкурентоспособность, и выживаемость любого ведомства и любой корпорации. И передавать это средство в руки зарубежных программистов, по меньшей мере, недальновидно.

В технологически развитых странах это понимали изначально, и поэтому не случайно ведомственные сети США строились исключительно на американском оборудовании и только трёх типов станций. Китай делает это на основе четырёх типов станций, и опять же своих. Да и во всех остальных странах с развитой ИТ-индустрией предпочитают отечественное оборудование. И такая «привязка» к собственному производителю продиктована отнюдь не квасным патриотизмом.

Во-вторых, редко кто из российских покупателей, приобретая импортную ЦАТС, задумывался о степени заинтересованности производителя в развитии тех или иных ведомственных сетей электросвязи России, то есть оценивал покупку с точки зрения геополитики. А геополитика напрямую зависит от состояния мировой экономики, которое сегодня нельзя назвать благоприятным.

Все биржевики видят, как что-то неладное творится на биржах, нефтяные компании видят, как что-то неладное творится с рынком «черного золота», все видят, как что-то неладное творится с рынком продовольствия. Каждый отдельный элемент происходящего специалисты пока ещё пытаются объяснять в рамках действующих экономических теорий. Но все эти элементы, взятые вместе, порождают совершенно необычную картину новой назревающей реальности, в которой все проблемы перемещаются из экономической в общецивилизационную плоскость. Человечество вступает в эпоху глобальных перемен, которые, безусловно, отразятся и на рынке телекоммуникаций. И трудно сейчас сказать, какое место на этом рынке (в том числе и на российском) будет занимать тот или иной зарубежный производитель оборудования через пять, десять, пятнадцать лет. И будет ли он вообще присутствовать на рынках, которые рецессия вынуждает переходить от глобализации к суверенизации, к их защите протекционистскими мерами

Вот поэтому и проблемы «доверенности-привязанности» при выборе поставщиков телекоммуникационного оборудования тоже постепенно перемещаются из экономической в геополитическую плоскость, в рамках которой решается уже не ценовая привлекательность и уровень сервисного обслуживания, а выживаемость наций и народов. При этом надежная и информационно безопасная связь в системе обеспечения этой выживаемости и конкурентоспособности будет играть далеко не последнюю роль.

Таким образом, проблема «доверенности», как бы, сама собой разрешает проблему «привязанности» и выдвигает на передний план «кадровую проблему».

Первыми её остро ощутили всё те же военные ведомства России. Министерство обороны РФ приступило к совершенствованию допризывной подготовки молодёжи по военно-учётным специальностям войск связи, к оптимизации своей системы вузов, готовящей связистов, начало оснащать учебные заведения своего ведомства лучшими образцами исключительно отечественного оборудования.

Хотя и медленно, но включаются в этот процесс и учебные заведения, готовящие специалистов для гражданских ведомств. Например, в Таганрогском технологическом институте Южного федерального университета по инициативе Группы компаний «Протон-СЗС» – разработчиков и производителей отечественного телекоммуникационного оборудования – а так же при поддержке ряда ведомств и операторов связи недавно была открыта новая специальность «Сети связи и системы коммутации». Учебные курсы этой специальности ориентированы не только на сокращение дефицита кадров связистов, но и на выпуск универсальных специалистов, ни в чём не уступающих зарубежным по всем проблемам проектирования, производства и эксплуатации коммутационной техники. Её выпускники овладеют методами построения цифровых узлов коммутации, принципами построения сетей связи, теорией распределения информации, практикой технической эксплуатацией узлов связи и их программного обеспечения, принципами управления сложными телекоммуникационными системами. А уровень их подготовки будет достаточным даже для оказания услуг инжиниринга и дальнейшей работы в качестве разработчиков телекоммуникационного оборудования.

При этом, и что следует особо отметить, практические навыки работы с оборудованием студенты будут приобретать в лаборатории телекоммуникации, специально спроектированной, изготовленной и смонтированной специалистами Группы компаний «Протон-СЗС». В ней представлено только отечественное оборудование, включая цифровые АТС, оборудование беспроводного доступа стандарта DECT, оборудование транспортной сети SDH, оборудование интеллектуальной сети NGN и приложения компьютерной телефонии, средства защиты каналов связи и управления от несанкционированного доступа.

И хотя отечественные телекоммуникационные платформы «Протон-СЗС» представлены и изучаются сегодня уже во многих специализированных учебных заведениях связи России, подобная лаборатория пока только одна. Её уникальность заключается в том, что она одновременно решает триединую задачу:

во-первых, позволяет на небольших площадях создать модель любой ведомственной сети, любой архитектуры и любого уровня;

во-вторых, выполняет функции тренажера, позволяющего студентам на практике комплексно овладеть навыками конфигурирования и эксплуатации оборудования, диагностирования и устранения неисправностей, освоения методов анализа трафика и его распределения, способов определения местонахождения неисправностей и их устранения, обучает пользоваться контрольно-испытательной аппаратурой (иначе говоря, даёт выпускнику возможность освоить навыки инжиниринга);

и, в-третьих, лаборатория телекоммуникации позволяет студентам на практике убедиться в том, что отечественное оборудование по своему качеству, многофункциональности и надежности ни в чём не уступает зарубежным образцам, а по обеспечению информационной безопасности и превосходит его многократно.

И нет сомнения в том, что для выпускников этого вуза проблемы «привязанности» и «доверенности» уже не будут возникать ни сейчас, ни в будущем. Как, надеемся, они не возникнут и у тех, кто после прочтения этой статьи решил впервые приобрести ЦАТС для своего ведомства.

Ещё два десятка лет назад телефонная связь рассматривалась всего лишь как комфортная услуга и своеобразная визитная карточка, характеризующая стиль работы отдельного предприятия или ведомства. Сегодня этот взгляд кардинально изменился. Широкое внедрение новых информационно-коммуникационных технологий на порядки усложнило оборудование связи и перевело его из разряда приложений к системе организации и управления производством в их составную часть. А эффективность ведомственной сети определяется уже не столько количеством комплектующего телекоммуникационного оборудования, сколько его функциональностью и бесконечным множеством возможностей его использования. Да и само оборудование становится не просто технически сложной системой, но и «умной», функционально управляемой компьютером и человеком. Усложняются и принципы его выбора.

Осторожно: NGN!

Проблемы нынешнего состояния отечественных разработок и производства телекоммуникационного оборудования за последние 10-15 лет вышли из рамок проблем сугубо отраслевых и перешли в разряд проблем государственных, напрямую связанных с задачами обеспечения информационной безопасности России.

Суть проблемы заключается в том, что, например, США свою цифровую выделенную сеть связи строят исключительно на отечественном оборудовании и только трёх типов станций. Китай – на основе четырёх типов станций, и опять же своих. И только в России аналогичное оборудование сегодня насчитывает 56 типов, среди которых большинство – импортное. И это не безобидно, так как электросвязь – не только комфортная услуга населению, но и стратегическое средство управления государством, армией, производством и объектами жизнеобеспечения страны. И передать это средство в руки зарубежных программистов по меньшей мере недальновидно, так как это открывает неограниченные возможности для целевого нарушения или изменения трафика и даже разрушения системы связи страны в кризисные моменты.

Между тем, сегодня более 40 крупнейших зарубежных компаний осуществляют поставки оборудования в Россию напрямую или через своих дилеров. Пользуясь политической и массированной финансовой поддержкой своих правительств, налоговыми льготами, обладая высоким научным потенциалом, крупным производством конкурентоспособного оборудования и достаточными оборотными и заемными капиталами, эти фирмы практически вытеснили с российского рынка отечественных разработчиков и производителей.

Особую активность проявляет концерн Siemens, который создал 11 совместных предприятий и одно предприятие со 100-процентным иностранным капиталом, получил крупные заказы на строительство магистральных и местных коммуникационных линий, на выполнение ряда проектов некоторых металлургических заводов, на реконструкцию ТЭЦ и автоматизацию сборочных линий ГАЗа. Концерн приобрел крупные пакеты акций ряда российских предприятий, в частности Калужского турбинного завода, АО «Электросила». При этом продвижение на российский рынок не происходит бессистемно. Siemens образовал структуры для координации своих действий и анализа российских условий. В концерне создан спецотдел, который занимается проблемами организации финансовых потоков в России, выработкой мер для успешного функционирования.

Не менее активна и появившаяся из недр концерна Siemens – компания «Искрател», базирующаяся в Словении и выпускающая телекоммуникационное оборудование под торговой маркой Si-2000 (Si – производное от Siemens). Сегодня это оборудование, но уже как отечественное, продвигает на сети связи Министерства обороны екатеринбургская фирма «ИскраУралТел».

Наступательна и деятельность в России финской фирмы Nokia, которая заняла одно из ведущих мест на нашем рынке радиотелефонов, пользуется услугами обширной дилерской сети, реализует проекты по созданию телефонных станций, телекоммуникационных линий и систем сотовой связи, поставляет приборы для российских научно-исследовательских институтов.

На российском рынке в реализации оборудования связи и телекоммуникаций доминируют японская компания NEC, немецкий концерн Siemens, французский концерн Alcatel, шведская компания Ericsson, американская компания

Avaya, финская фирма Nokia, китайская компания Huawei Technologies, южнокорейская компания Corecess и другие.

В то же время отечественные разработки и производство телекоммуникационного оборудования брошены на произвол судьбы. Ими не занимается ни одно из существующих российских министерств и ведомств. Они находятся фактически вне закона. Их интересы не представлены ни в Федеральном законе «О связи», ни в реально действующих федеральных программах. Их игнорирует Мининформсвязи РФ, в штате которого нет чиновника, ответственного за развитие телекоммуникационной индустрии.

По идее, одним из ведомств, заинтересованных в развитии отечественного наукоемкого производства средств связи, должно быть Минпромэнерго. Но в его руководящих документах, в том числе проекте концепции «Основные направления государственной научно-технической политики в промышленности России», нет ни слова о создании современного телекоммуникационного оборудования. А в структуре министерства не предусмотрены подразделения, ответственные за развитие соответствующего производства.

В результате российское производство телекоммуникационного оборудования оказалось вне государственных программ и развивалось стихийно, прибегая к методам и средствам экстремального выживания, выбирая путь дробления и организации новых производств. Большинство образовало всё те же совместные предприятия, использующие зарубежные разработки, технологии, оборудование, комплектующие изделия, программное обеспечение, и тем самым содействовало ещё большему сокращению ниши отечественных разработчиков и производителей на российском рынке.

Сейчас почти все наши ведущие заводы, а их около 30, производят практически однотипное отечественное оборудование под разными торговыми марками, которое примерно одинаково и по производительности, и по функциональным характеристикам, и по качеству. Каждое из этих предприятий расходует свои крайне скудные финансовые ресурсы на дублирование, по существу, одних и тех же разработок. Малоэффективность таких поисков очевидна.

А между тем зарубежные конкуренты начали массированную пропаганду в России мультисервисных сетей связи будущего поколения – Next Generation Network (NGN), в которых традиционным телефонным коммутаторам вообще нет места. Здесь интеллектуальным ядром сети будет программный коммутатор (Softswitch), который управляет граничными медиашлюзами, преобразующими пользовательский трафик и протоколы сигнализации. А медиашлюзы, и в особенности Softswitch, в сущности, представляют собой программные продукты.

Эта рекламная кампания и пропаганда преследует две взаимоувязанные цели:

– во-первых, всех пытаются убедить (и, кажется, убедили), что NGN уже сегодня является панацеей от всех бед на российском декадно-шаговом бездорожье сетей электросвязи;

– и, во-вторых, (учитывая, что у российских разработчиков нет собственного достаточно конкурентоспособного программного коммутатора Softswitch), что отечественное телекоммуникационное оборудование вообще неконкурентоспособно и не имеет будущего.

Но всем, кто так активно поддерживает зарубежных пропагандистов, следовало бы подумать над тем, что основным протоколом NGN-сетей является SIP. А SIP-телефония, как известно, не соответствует условиям, при выполне-

нии которых ее можно признать телефонной, т.е. регулируемой. Мало того, ряд требований в SIP-телефонии пока не реализуется технологически.

Хотя, безусловно, будущее за NGN и работать над совершенствованием технологий нужно и зарубежным, и отечественным разработчикам.

Однако все предложенные выше меры по созданию технологически независимого от импортеров пространства на сетях электросвязи не означают, что нынешнему NGN-ажиотажу нет альтернативы, что сегодня нужно вообще заморозить процессы модернизации и внедрения технологий NGN на телекоммуникационной сети России.

Эти процессы объективны. Они являются следствием постоянно нарастающей востребованности современных услуг как в объеме традиционной телефонии, так и новых, входящих в состав мультисервисных сетей. Следовательно, думать нужно о том, какими предложениями можно ответить в реальном времени и в реальных условиях на этот спрос. А, задумавшись, мы увидим две основные проблемы, которые заметно тормозят модернизацию.

Во-первых, это острый дефицит инвестиций.

Во-вторых, сеть доступа пока остается наиболее дорогим элементом и «узким местом» современной сети электросвязи. Именно здесь начинается торможение процесса её развития.

Да и объективные геоэкономические факторы, влияющие на развитие сети и услуг, не позволяют обеспечить одинаковое развитие всех сегментов сети одновременно. Ведь существуют и услуги, требующие широкополосного доступа, и те, для которых транспортная инфраструктура не имеет большого значения.

Кроме того, практически все операторы находятся на разной дистанции от условного «финиша»: для одних проблемой остается цифровизация и увеличение абонентской емкости по обычным двухпроводным линиям, для других – оптимизация расходов на внедрение самых современных, но дорогих услуг. Всё это, и в том числе эксплуатация оборудования нескольких поколений на базе разных технологий, не способствует повышению рентабельности бизнеса операторов. Вот поэтому использование одинаковых, стандартных решений для модернизации сетей электросвязи практически исключено. Стратегия перехода для каждого индивидуальна и будет зависеть от многих факторов.

Оптимальными нам представляются решения, основанные на применении коммутационных систем нового поколения «Протон-ССС», которые сохраняют обеспечение поддержки интерфейсов, протоколов и услуг классических телефонных сетей общего пользования. Эти платформы позволяют проводить так называемую островную модернизацию, которая не требует больших инвестиций, а значит, снижает в целом остроту их дефицита при модернизации сетей электросвязи.

Например, базовые услуги сегодня востребованы везде. Поэтому оператор в любых случаях вынужден будет установить экономичные блоки, обеспечивающие телефонные вызовы, дополнительные виды обслуживания, услуги интеллектуальной сети, доступ в Интернет на небольших скоростях. После этого можно приступить к значительному расширению функций системы и реализации уже современных услуг мультисервисной сети. Расширение, основанное на принципах мультимедийности, мобильности, широкополосности, гарантирует оператору целесообразное вложение инвестиций и возможность использования существующих технологий и тех, которые появятся в будущем.

Внедрению такой стратегии модернизации и способствует ЦАТС «Протон-ССС», которая построена на новейших технологиях, с открытым интерфейсом

для развития, но с учетом реалий современной отечественной телекоммуникационной сети. Она имеет свою собственную систему управления, готовую к расширению коммутационной платформы за счет разработки и интеграции новых функциональных блоков.

Принципы построения новых и модернизации существующих участков сети электросвязи могут быть различными для сельских и городских сетей. Ведь наряду с укрупнением коммутационного оборудования городских сетей, расширением участка доступа от помещения абонента до центрального помещения оператора формируется и тенденция применения распределенной коммутации, основанной в первую очередь на технологии IP. И в этом отношении наиболее привлекательной для всех операторов, как уже было сказано, остается коммутационная система «Протон-ССС», которая может применяться и на всех участках сети доступа, и для организации транспортной сети районного уровня.

Любой из уже установленных на сети модулей «Протон-ССС» может быть дооснащён для включения в мультисервисную сеть. Для этого потребуется всего лишь установить блоки IP-шлюза или медиашлюза, шлюза сигнализации и дополнить программное обеспечение. Можно также добавить модули широкополосного доступа. После такой модернизации платформа способна осуществлять взаимодействие с другими элементами конвергированной сети (коммутационными узлами, софтсвитчами) по протоколам H.323/SIP/MGCP/H.248 и предоставлять различные услуг на базе технологии пакетной коммутации.

Подобный переход к мультисервисной сети необходимо осуществлять в несколько этапов, и оператор сам должен определить долгосрочную цель модернизации и выбрать стратегию.

На первом этапе, например, может быть осуществлена замена устаревшего аналогового оборудования на цифровые абонентские выносы и оконечные станции с замыканием внутренней нагрузки. Затем, по мере развития транспортной сети, потребуется увеличение емкости коммутационного поля. Для этого можно будет дополнительно к существующим установить опорно-транзитные и транзитные узлы коммутации «Протон-ССС», воспользовавшись всеми видами транспортных технологий (медь, оптика, радиодоступ).

На втором этапе, возможно, потребуется предоставить пользователям широкополосный доступ и «слить» часть трафика в сеть с коммутацией пакетов. Для этого расширяются выносы к мультисервисному узлу широкополосного доступа с технологией уплотнения линий (установка DSLAM).

На третьем этапе при расширении предоставления большинства услуг через широкополосный доступ оператору потребуется нарастить транспортную сеть и унифицировать интерфейсы, протоколы, способы и методы предоставления услуг. Для этого к базовым модулям «Протон-ССС» добавятся шлюзы, медиашлюзы и оборудование, выполняющее функции гибкого коммутатора с интерфейсом к серверам приложений.

Вот это и есть самый простой и экономичный вариант перехода к сетям связи будущего поколения, на котором коммутационная система «Протон-ССС» станет идеальным тактическим средством и элементом стратегии построения мультисервисной сети. Только эта, полностью отечественная, платформа позволит и рационально использовать инвестиции, не испытывая их дефицита, и безболезненно решить проблему сети доступа.

«Протон-ССС» – гарантия надежности и информационной безопасности

Современная коммуникационная система, предназначенная для применения на сетях электросвязи МВД РФ, должна соответствовать целому ряду вполне определенных функциональных и конструктивных требований.

Во-первых, кроме голосовой связи и передачи данных, она обязана обеспечить работу различных служебных подсистем (приложений). Следовательно – должна быть мультисервисной.

Во-вторых, требования к охвату связью больших территорий предполагают распределенное построение этой системы и использование различных технологий доступа (кабельной, беспроводной, оптической).

В-третьих, различные варианты применения подобной системы (на разных уровнях управления) и необходимость уменьшения эксплуатационных расходов требуют наличия унифицированных программных и аппаратных подсистем.

И, наконец, такая система должна обладать самой надежной защитой от несанкционированного доступа извне.

Всеми этими качествами и функциональными возможностями и обладает, предлагаемая системным интегратором НПП «СПЕЦСТРОЙ-СВЯЗЬ» мультисервисная коммуникационная система (МКС) «Протон-ССС», которая сегодня применяется в качестве:

Виды оборудования	**Примеры действующего оборудования**
центральной АТС ведомственной связи	МВД по Чеченской республике (г. Грозный); ЦУС ФСИН г. Москва …и другие.
учрежденческо-производственной АТС	ГУ НПО «Специальная техника и связь» МВД РФ (г. Москва); ФГУП «СНПО Элерон» (г. Москва); ГУВД Ростовской области УВД г. Таганрога …и другие.
малой учрежденческой АТС	Московский областной филиал Московского университета МВД России (Московская обл., п. Тучково); ГУВД Ростовской области УВД г. Новочеркасска; ВЧ 6688 ВВ МВД РФ (г. Астрахань) … и другие.
системы оперативной и диспетчерской связи	ВЧ 6770 ВВ МВД РФ (г. Моздок); ВЧ 7605 ВВ МВД РФ (г. Екатеринбург); Дивизия им. Дзержинского ВВ МВД РФ (г. Реутов) …и другие.
конвертера сигнализации	ООО «УНИВЕРСУМ-БИТ» (г. Москва); ФГУ «Камводпуть» (г. Пермь) …и другие.
первичного мультиплексора	ООО «Бизнес-Связь» (г. Сочи); УФСИН по Кабардино-Балкарской Республике (г. Нальчик) …и другие
гибкого мультиплексора	Скопинский автоагрегатный завод (г. Рязань); УФСИН России по Кировской области (г. Киров) …и другие.

медиашлюза	Волгодонская АЭС (г.Волгодонск); ОАО «Мастер-Банк» (г.Черноголовка) …и другие.
межсетевого шлюза	АО «Sky Silk» (г. Актау, Республика Казахстан); ООО «ДектТелеКом» (г. Оренбург) …и другие.
каналообразующей аппаратуры	УФСИН России по Белгородской области (г.Белгород); УФСИН России по Курской области (г.Курск) … и другие
интеллектуальной мультисервисной системы	ОАО «КраснодарГорГаз» (г. Краснодар); Северо-Кавказская железная дорога филиал ОАО «Российские железные дороги» (г.Махачкала), «СерДи Телеком» (г. Георгиевск) …и другие.

МКС «Протон-ССС» характеризуется высокой надежностью за счёт схемотехнических и конструктивных особенностей оборудования, распределённого управления и коммутации, резервирования основных функциональных модулей (коммутационных полей, процессоров, источников питания, управляющих шин).

Имеет система и комплекс средств защиты от несанкционированного доступа к информации, гарантирующий информационную безопасность ведения переговоров и устойчивость связи.

Основные преимущества МКС «Протон-ССС» – это полное соответствие требованиям самых различных российских ведомств и силовых структур (в том числе и МВД РФ) и наличие встроенных в оборудование и ПО специфичных (используемых только в России) протоколов взаимодействия сетей, которых либо нет на оборудовании других производителей, либо они требует значительных финансовых затрат для их реализации.

На базе МКС «Протон-ССС» может быть развернута система оперативно-диспетчерской связи (СОДС), в которой, кроме базовых задач (оперативное управление связью, организация и обслуживание очередей входящих вызовов), возможно выполнение ряда дополнительных функций:

• обеспечения оперативной связи на сетях, использующих новые информационные технологии (сети связи NGN);

• организации современного информационного обеспечения оператора СОДС базой данных (справочник абонентов СОДС, подключаемых БД по предметным областям);

• повышения эффективности обслуживания входящих вызовов за счет применения новых информационных сервисов и сервисов цифровой обработки голосовых сообщений;

• предельного упрощения приёмов работы оператора за пультом и методов обучения новым функциям пульта;

• обеспечения средствами контроля и самоконтроля работы оператора.

В составе СОДС могут работать различные терминалы: цифровые системные телефоны, системные IP-телефоны, кнопочные пульты («Вектор-М»), сенсорные пульты («Простор»), различные автоматизированные рабочие места диспетчеров на базе программных телефонов (клавиатурный АРМ диспетчера, Sysphone).

МКС «Протон-ССС» строится на основе мультисервисных узлов коммутации и доступа (МСКД «Протон-ССС»), которые могут применяться в различных телефонных сетях: с коммутацией каналов, с коммутацией пакетов и в конвергентных сетях. Реализуя в одной системе функции оборудования доступа и оборудования управления/коммутации, МСКД могут работать как под управлением программных коммутаторов (softswitch), так и самостоятельно.

Следует особо отметить, что любая из ранее выпущенных и находящаяся в эксплуатации цифровых АТС «Протон-ССС,» может быть доукомплектована для работы в качестве МСКД.

Основными функциями МСКД являются функции медиашлюза и программного коммутатора. Голосовые VoIP-шлюзы «Протон-ССС» могут выпускаться и в автономном исполнении для работы в составе других систем.

На базе VoIP-шлюзов реализуется целый спектр решений не только по связи, но и по комплексной автоматизации. Эти решения включают в себя: объединение телефонных сетей с помощью IP-шлюзов, IP-АТС, IP-Центрекс, IP-Call/Contact-центр, мультисервисный медиасервер DGW IVR «Протон-ССС», система исходящих вызовов (оповещения) DGW Informer «Протон-ССС».

Сертифицированная сетевая система эксплуатации и технического обслуживания оборудования (СЭиТО), разработанная НПП «СПЕЦСТРОЙ-СВЯЗЬ», входит в комплекс МКС и предоставляет:

• удобный интерфейс, ориентированный на максимальную эффективность работы с сетью и каждым сетевым элементом в отдельности;

• управление правами доступа, паролями, возможность настройки политик доступа;

• удалённое выполнение всех операций, включая загрузку программного обеспечения оборудования;

• визуальное отображение обслуживаемой сети на географической карте местности, возможности просмотра реального расположения сетевого элемента, обращения к нему, управления, конфигурирования, тестирования, получения данных статистики, выполнения диагностики и устранения возникших неполадок.

С помощью МСК можно разработать для каждого абонента собственный план нумерации и таблицу маршрутизации, тем самым, организовав абонентскую VPN-сеть.

Наличие в сети единой точки концентрации трафика (МСК) позволяет осуществлять авторизацию и биллинг с помощью единой биллинговой системы, которая может подключаться к МСК либо по протоколу RADIUS, либо для считывания CDR по различным интерфейсам (текстовые файлы, FTP, TCP\IP).

К перечню преимуществ МКС «Протон-ССС» следует добавить, что в процессе её производства используются самые передовые технологии и самые современные комплектующие. А соответствие производства требованиям и стандартам силовых структур (в том числе и МВД РФ) обеспечивает военная приемка, эффективно действующая на нашем предприятии.

Не менее важно и то, что интегрированный научно-технический потенциал Группы компаний «Протон-ССС», головным предприятием которой и является НПП «СПЕЦСТРОЙ-СВЯЗЬ», позволяет предоставлять заказчикам полный комплекс услуг инжиниринга, осуществлять проектные работы любой сложнос-

ти и модифицировать оборудование в соответствии с любыми специфическими требованиями заказчиков.

Для тех же, кто хочет убедиться в преимуществах МКС «Протон-ССС», мы практикуем установку на их объектах систем малой ёмкости в качестве стенда для тестирования. Это позволяет техническим специалистам в короткие сроки обрести практические навыки работы с МКС. А получить теоретические знания они могут как непосредственно на своём рабочем месте, так и в нашем учебном центре в Таганроге.

И, наконец, следует отметить, что эксплуатацию МКС «Протон-ССС» на протяжении всего её жизненного цикла поддерживает круглосуточный сервисный центр НПП «СПЕЦСТРОЙ-СВЯЗЬ».

Соответствие нормативам всех видов оборудования и услуг, которые у нас получает заказчик, подтверждено необходимыми лицензиями и сертификатами.

Игорь Михайлович Домбрин
директор департамента научных исследований
и программного обеспечения
НПП «СПЕЦСТРОЙ-СВЯЗЬ»

Содержание

Концепция, дизайн и верстка ООО «PR-агентство «ПЕРСОНА ГРАТА»
Россия, 347922, Ростовская обл., г. Таганрог, ул. Греческая, 90
тел./факс: (8634) 315-487, e-mail: pr@proton-sss.ru