Актуальные научно-практические проблемы развития ОАЦСС ВС РФ

Арсланов
Халил Абдухалимович,
начальник Главного управления Связи Вооружённых Сил Российской Федерации —заместитель начальника Генерального штаба Вооружённых Сил Российской Федерации, генерал-лейтенант

Лихачёв
Александр Михайлович,
советник генерального директора ОАО «НИИ «Рубин»

Под информационно-телекоммуникационной системой (сетью) в соответствии с федеральным законом Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. К классу таких систем относится Объединённая автоматизированная цифровая система связи (далее ОАЦСС) Вооружённых Сил Российской Федерации*. Одной из её задач является предоставление комплексных ресурсов (пропускной способности, частотных, позывных, номеров, адресов, имён, эксплуатационных и других) по передаче информации в интересах Национального центра управления обороной Российской Федерации (далее НЦУ) для нужд обороны, которая должна осуществляться без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами. Особенности подключения автоматизированной системы управления связью (далее АСУС) Вооруженных Сил государственных информационных систем к ресурсам ОАЦСС могут быть установлены другим нормативным правовым актом.

На сегодняшний день одной из важнейших критических научно-технических проблем развития ОАЦСС и НЦУ представляется обеспечение их информационной безопасности, которая существенно обостряется в условиях постоянно возрастающих угроз деструктивных воздействий на государственные информационные системы (далее ГИС). Об этом свидетельствует разработка ведущими странами НАТО стратегических и технологических методов и решений ведения информационных и кибернетических войн. Наименее исследованной, а следовательно, и наиболее уязвимой в составе НЦУ как основного элемента технической основы системы управления Вооруженных Сил, представляется система управления связью.

Система управления связью (далее СУС), за создание и развитие которой отвечает Главное управление связи Вооруженных Сил, представляет организационно-техническую систему в составе ОАЦСС Вооруженных Сил и войск связи, являющуюся совокупностью функционально и организационно связанных между собой органов управления связью, пунктов управления связью и служебной технической основы, включающей информационные, вычислительные, служебные телекоммуникационные ресурсы и специальные средства, базирующиеся на комплексах программно-аппаратных средств автоматизации (комплексы средств автоматизации управления связью — КСАУС), и служебной связи технологического тракта управления ОАЦСС, образующих АСУС. Основными функциональными подсистемами СУС являются подсистемы управления: развитием, применением по назначению, обслуживанием, материально-техническим обеспечением, эксплуатацией, оперативно-технической службой узлов связи, информационной безопасностью. Их реализация и степень автоматизации базируется на состоянии жизненного цикла базовых технологических программно-аппаратных модулей КСАУС: сбора, хранения, обработки, распределения и предоставления данных по управлению связью; информационного сопряжения техноло-

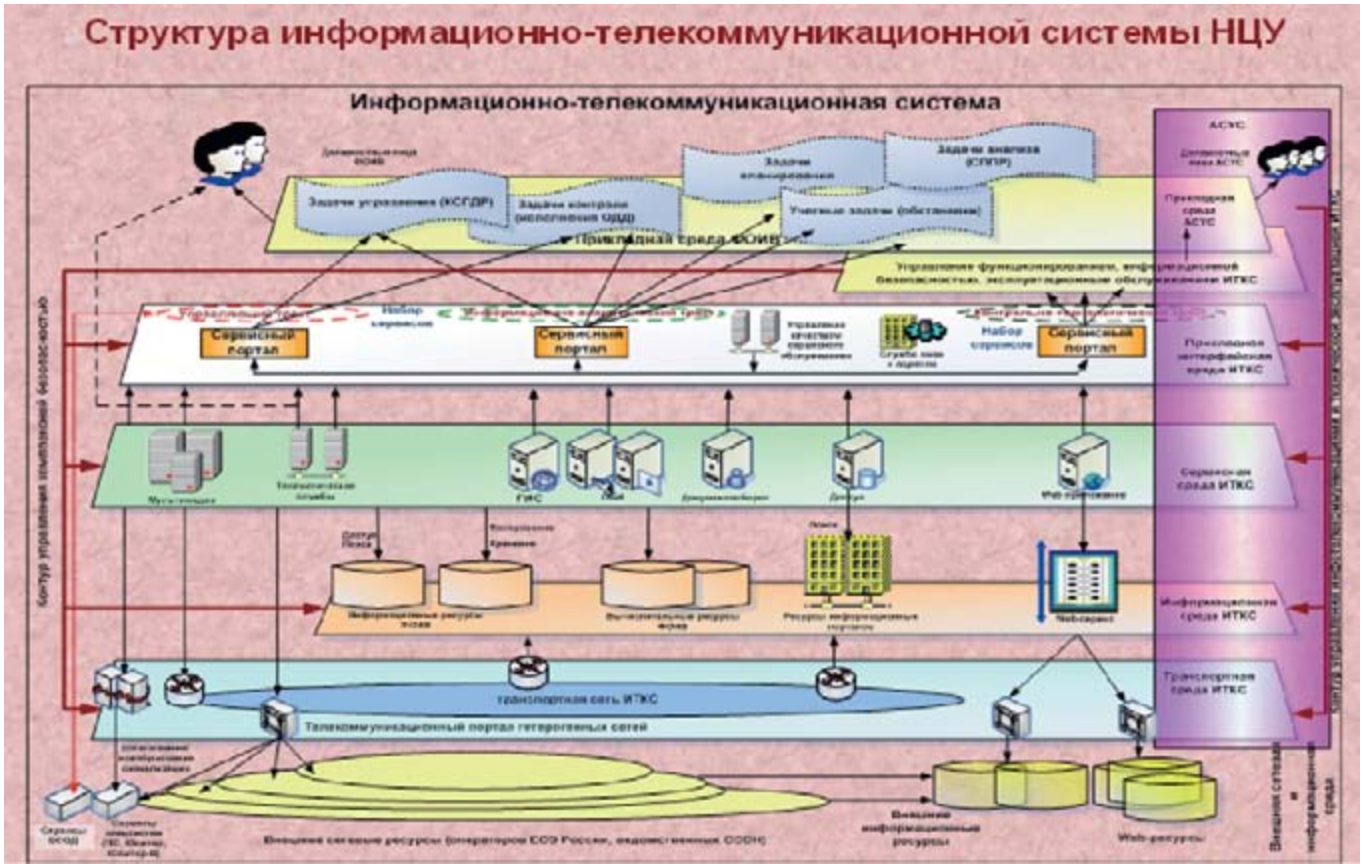

Рис. 1. Структура информационно-телекоммуникационной системы НЦУ

гических трактов управления ресурсами НЦУ; прикладных задач управления связью на основе геоинформационной платформы поддержки управленческих решений НЦУ. Таким образом, разрабатываемые и модернизируемые промышленностью КСАУС для автоматизации процессов управления ресурсами ОАЦСС Вооруженных Сил должны создаваться с учётом уровня технологического развития информационных и телекоммуникационных технологий, обеспечения их информационной безопасности на всём жизненном цикле изделий, включая обеспечение информационной безопасности автоматических технологических подсистем управления сетями тактовой синхронизации и обеспечения единого времени, сигнализацией, нумерацией, адресацией и именами, геоинформационным обеспечением поддержки принятия решений по управлению связью во всех звеньях управления Вооруженных Сил.

Первоочередными объектами воздействий с целью их дезорганизации и вывода из строя в составе АСУС становятся КСАУС ОАЦСС Вооруженных Сил и сетей связи систем государственного управления, базирующихся на ГИС и опирающихся на ресурсы сетей связи общего пользования единой сети электросвязи Российской Федерации (далее ССОП ЕСЭ). Отсутствие в ССОП доверенного (отечественного) телекоммуникационного ресурса существенно снижает устойчивость и безопасность ОАЦСС ВС при обеспечении деятельности НЦУ.

Функционально ведомственные сети связи, объединяемые ОАЦСС ВС (рис. 1) для нужд обороны, в интересах систем государственного управления (далее СГУ) и ГИС реализуют процессы сбора, обработки, накопления, хранения, распределения, поиска и передачи информации между объектами и субъектами управления НЦУ, в том числе АСУС, в соответствии с иерархической организационно-функциональной трёхуровневой структурой, включающей федеральный, региональные и местные уровни.

В настоящее время практически все ведомственные информационные и телекоммуникационные сети так или иначе базируются на ресурсы ССОП ЕСЭ и имеют в своей основе распределенные хранилища (банки) данных ГИС, предоставляющие возможность оперативного доступа к данным потребителям из любой точки сети. Но это несомненное удобство в работе становится весьма спорным, если принимать во внимание вероятность информационных деструктивных воздействий, под которыми следует понимать любое несанкционированное воздействие на средства и комплексы иностранного производства ССОП ЕСЭ. Поскольку ведомственная структура СГУ и видовая Вооруженных Сил подразумевают территориальную распределённость подсистем, включая АСУС, то это облегчает возможность атак на неё со стороны заинтересованных лиц. Существовавшая до настоящего времени концепция обеспечения безопасности информации в АСУС ВС была ориентирована на защиту данных только на локальной территории, что совершенно недостаточно в условиях распределенного взаимодействия по неконтролируемым открытым каналам связи

ССОП в ОАЦСС ВС и невозможно без создания интегральной АСУС для нужд обороны, что является одной из ключевых задач, решаемых в настоящее время Главным управлением связи.

Средства информационной безопасности КСАУС ОАЦСС ВС (как элементов интегрированной АСУС) должны определяться как меры, предохраняющие сети связи, развёртываемые комплексами и средствами связи различных эшелонов, от несанкционированного доступа (далее НСД), случайного или преднамеренного вмешательства в их работу, попыток разрушения их компонентов, в том числе путём генерации несанкционированных команд и сигналов на управление ресурсами синхронизации, сигнализации, нумерации, адресации и именования абонентов и технологического оборудования в ОАЦСС ВС. Обеспечение информационной безопасности (далее ИБ) КСАУС в составе АСУС ОАЦСС ВС включает в себя защиту каналов передачи и связи, оборудования, программного обеспечения, данных и персонала, то есть безопасность связи, технологическую безопасность и безопасность информации пользователей и сетей управления ресурсами ОАЦСС ВС для нужд обороны при обеспечении деятельности НЦУ.

Все методы и средства обеспечения безопасности КСАУС в составе АСУС ОАЦСС ВС можно отнести к одному из следующих трех уровней: средства защиты физического, канального и сетевого уровней. К ним относятся средства охраны зданий и помещений, в которых расположены элементы и узлы АСУС ОАЦСС ВС, физический контроль доступа к компьютерам и терминалам КСАУС НЦУ. Все эти средства встраиваются в аппаратное и программное обеспечение оборудования, в том числе канального уровня АСУС ОАЦСС ВС, которые не в полной мере обеспечивают защиту средств сетевого уровня управления. Поэтому необходима разработка методов и средств обеспечения системного (сетевого) уровня, осуществляющих управление ИБ в ситуационных центрах управления (далее СЦУ) и обеспечения ИБ в АСУС ОАЦСС ВС, которые должны быть представлены в КСАУС НЦУ в виде методических положений, стандартов, планов мероприятий и других документов оперативно-технической службы узлов связи Вооруженных Сил и других ГИС ГСУ (рис. 2).

В настоящее время на рынке оборонно-промышленного комплекса (далее ОПК) радиоэлектронной промышленности представлено большое разнообразие программно-аппаратных доверенных средств защиты отечественного производства, которые могут найти применение в АСУС ОАЦСС ВС, и их условно можно разделить на несколько групп: средства, обеспечивающие разграничение доступа к информации; средства, обеспечивающие защиту информации при передаче её по каналам передачи и связи; средства, обеспечивающие защиту от воздействия программ-вирусов; средства, обеспечивающие защиту от утечки информации по акустическим и электромагнитным полям, возникающим при работе технических средств; материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Прогресс в области информационных и телекоммуникационных технологий ставит целый круг новых задач по обеспечению информационной безопасности создаваемой АСУС ОАЦСС ВС в составе НЦУ. Частая смена программно-аппаратных платформ, непрерывное повышение производительно-

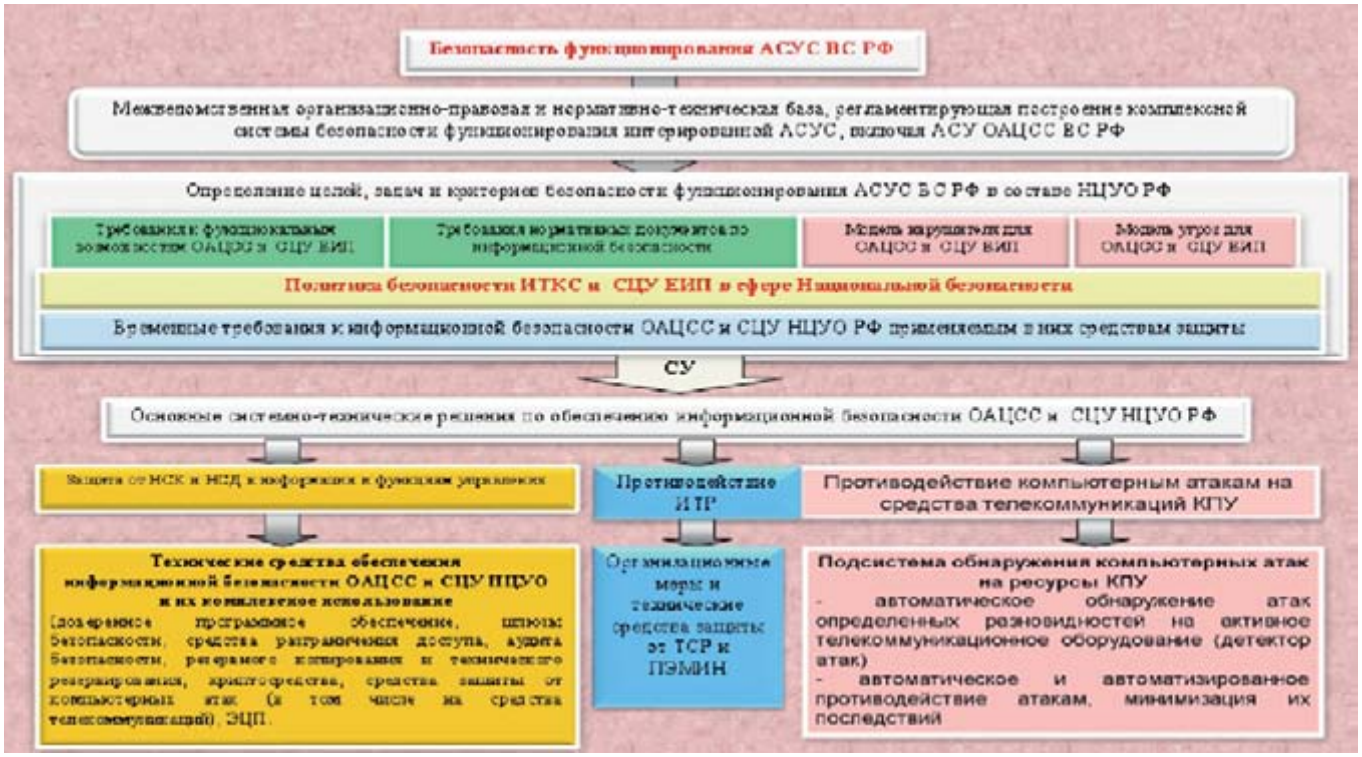

Рис. 2. Мероприятия по обеспечению безопасности АСУС в сфере деятельности НЦУ

сти вычислительных систем и каналов передачи и связи ставят задачу быстрого проектирования и оперативной доработки средств защиты информации КСАУС в составе АСУС ОАЦСС ВС в соответствии с изменившимися условиями эксплуатации.

Известные методики и инструментальные средства концептуального проектирования (в т. ч. CASE-системы) доверенного оборудования КСАУС отечественного производства в интересах АСУС ОАЦСС ВС, развитые в области систем автоматизированного проектирования (далее САПР) и закрепленные стандартами серии IDEF, ориентированы на средства и комплексы связи и автоматизации, но не решают проблем САПР по обеспечению ИБ на системном (сетевом) уровне. Поэтому известные методические подходы не затрагивают проблем генерации и выбора рациональных проектных решений по построению ИБ КСАУС АСУС НЦУ, являющихся главным результатом проводимых проектных работ по построению территориально распределённых ГИС в интересах ГСУ. Проблемы разработки АСУС ОАЦСС ВС для нужд обороны взаимообусловлены особенностями распределения и взаимосвязи компонентов КСАУС ОАЦСС ВС (архитектуры ОАЦСС ВС). Архитектура АСУС ОАЦСС ВС (рис.1) в общем случае включает: среду (уровень, слой) внешних (операторов ЕСЭ России, ведомственных операторов) сетевых и информационных ресурсов; транспортную среду; информационную среду; сервисную среду; прикладную интерфейсную среду, каждая из которых имеет специфику решения задач ИБ, включая защиту от алгоритмических атак и несанкционированных команд и сигналов подсистем автоматического управления ресурсами ОАЦСС ВС и операторов связи ЕСЭ РФ.

Внешняя сетевая среда интегральной АСУС ОАЦСС ВС в НЦУ для нужд обороны на сегодняшний день в основном формируется за счет аренды у операторов ССОП недоверенного телекоммуникационного ресурса средств (каналов передачи и связи, трафика, потоков пакетов в виртуальных операторских сетях и др.).

Транспортная среда ОАЦСС ВС формируется на базе внешних сетевых ресурсов (операторов ЕСЭ России, ведомственных сетей связи). В транспортную среду АСУС ОАЦСС ВС входят такие элементы, как: IP-транспортная сеть ОАЦСС ВС, предоставляющая услуги по присоединению и по пропуску трафика для уровней информационной и сервисной среды КСАУС в составе АСУС ОАЦСС ВС; телекоммуникационные порталы; средства доступа к Web-ресурсам; шлюзы взаимодействия со специальными ведомственными системами управления связью и др. Ориентация на аренду ресурса ССОП обусловливает наличие проблем, связанных с необходимостью обеспечения в КСАУС НЦУ повышенных уровней устойчивости (рис. 2) и ИБ. Использование внешних сетевых ресурсов гетерогенных сетей приводит к необходимости решения проблемы шлюзования с ними. В информационную среду АСУС ОАЦСС ВС входят такие средства, как: информационные и вычислительные ресурсы IP-транспортной сети, в том числе ресурсы информационных порталов, автоматизированных комплексов и средств коммутации и маршрутизации, и информационные ресурсы автоматизированной системы управления связью. Создание информационной среды АСУС ОАЦСС ВС связано с проблемами обеспечения ее унификации, ИБ и взаимодействия с КСАУС в составе АСУС НЦУ с информационной средой ГИС ГСУ, отвечающих за решение задач по связи для нужд обороны, а также взаимодействующих систем управления операторов связи ССОП и ведомственных сетей связи СГУ.

В сервисную среду АСУС ОАЦСС ВС входят такие средства, как: а) средства мультимедиа; б) телематические службы ведомственных сетей связи; в) средства геоинформационных систем; г) средства обеспечения безопасности информации; д) средства реализации электронного документооборота; е) средства обеспечения доступа к сервисным порталам прикладной интерфейсной среды и ресурсам информационных порталов информационной среды КСАУС НЦУ.

Указанные средства КСАУС должны обеспечивать формирование, доведение и предоставление мультимедийных услуг как должностным лицам органов управления СЦУ НЦУ, так и пользователям (должностным лицам управления связью на пунктах управления связью) АСУС ОАЦСС ВС на прикладном интерфейсном и прикладном уровнях. Создание сервисной среды АСУС ОАЦСС ВС будет сопряжено с проблемами: унификации служб и услуг (мультимедиа, телематических, ГИС, обеспечения ИБ, документооборота, доступа к информационным ресурсам СЦУ) для двух категорий пользователей — внешних (должностные лица НЦУ, включая должностных лиц АСУС ВС) и внутренних (должностные лица АСУС ОАЦСС ВС); обеспечения ИБ предоставляемых служб в двух контурах (доменах) безопасности — домене должностных лиц СЦУ НЦУ и домене должностных лиц АСУС ОАЦСС ВС. В прикладную интерфейсную среду АСУС ОАЦСС ВС входят такие средства, как: а) сервисные порталы в управляющем, информационно-аналитическом и контрольно-технологическом трактах КСАУС НЦУ и АСУС ОАЦСС ВС; б) средства службы позывных, номеров, имен и адресов АСУС ОАЦСС ВС; в) средства автоматизации управления качеством сервисного обслуживания НЦУ.

Средства прикладной среды должны обеспечивать формирование, доведение и предоставление на прикладном уровне как должностным лицам НЦУ, так и пользователям АСУС ОАЦСС ВС услуг: управляющего тракта по формированию и передаче команд, сигналов подтверждений, директив, донесений и распоряжений по связи, приему и оперативному анализу информации и ответов, донесений, докладов, поступающих от должностных лиц, включая АСУС, подчиненных уровней вышестоящим; информационно-аналитического тракта; контрольно-технологического тракта.

Указанные уровни должны обеспечивать функционирование прикладных сред, как для должностных лиц АСУ НЦУ, так и для должностных лиц управления эксплуатационным обслуживанием ОАЦСС ВС.

Анализ архитектуры АСУС ОАЦСС ВС показывает, что информационно-аналитическое обеспечение деятельности должностных лиц органов управления

связью средствами КСАУС в составе НЦУ является основой формирования транспортного уровня АСУС ОАЦСС ВС. Следовательно, проблемы развития и интеграции автоматизированных систем управления связью СГУ являются неотъемлемой частью проблем создания государственных ресурсов интегрированной АСУС ОАЦСС ВС и подлежат разрешению Главным управлением связи Вооруженных Сил в первую очередь, что и должно стать основой государственной технической политики при развитии и модернизации КСАУС НЦУ в области развития отрасли связи, включая ресурсы доверенного оператора ЕСЭ, в интересах СГУ в любых условиях обстановки, в том числе при чрезвычайных ситуациях и чрезвычайном положении. Реализация изложенных критических научно-технических проблем развития и модернизации АСУС ОАЦСС ВС возможна только при тесном взаимодействии с радиоэлектронным комплексом ОПК России и существенно определяется его научным потенциалом и производственными возможностями.

К основным вызовам и угрозам России, непосредственно связанным с деятельностью радиоэлектронного комплекса ОПК России, следует отнести:

- нестабильность и противоречивость развития геополитической ситуации в мире, существенно сужающие возможности предприятий отечественного ОПК в организации эффективной международной производственной кооперации в области информационных систем, средств вычислительной техники, микропроцессоров и базового программного обеспечения на долговременной основе;
- опережение военной промышленности США и стран НАТО оборонно-промышленного комплекса России в разработке перспективных интеллектуальных образцов радиоэлектронных вооружений, соответствующих 6-му, а по ряду позиций и 7-му технологическим уровням, способных выполнять боевые задачи в рамках новых военных стратегий и концепций;
- санкции США и ЕС против предприятий и оборонных радиоэлектронных отраслей российской экономики, введение ими ограничений или прекращение военно-технического сотрудничества с Россией, что негативно влияет на производственную и финансово-экономическую деятельность предприятий радиоэлектронного комплекса ОПК — участников военно-технического сотрудничества;
- события на Украине, негативно влияющие на процессы военно-технического сотрудничества, в частности на деятельность предприятий радиоэлектронной промышленности российского ОПК, у которых может быть сорван выпуск продукции военного назначения по ГОЗ и на экспорт из-за прекращения поставок комплектующих и материалов, производившихся украинскими предприятиями.

Данные глобальные вызовы и угрозы порождают следующие группы рисков для решения научно-технических проблем применения доверенного оборудования отечественного производства КСАУС для интегрированной АСУС ОАЦСС ВС в интересах НЦУ, требующих решения в ГПВ на 2016–2025 гг.

Рис. 3. Механизмы взаимодействия науки и практики при развитии АСУС ОАЦСС ВС в сфере деятельности НЦУ

Отечественный рынок РЭА 2013г.

	Сектор рынка	Отечественная продукция	Экспорт	Импорт	ВСЕГО	Доля отечественной продукции
		$млн				%
1	Машины вычислительные	1 380,8	276,6	5 151,7	6 532,5	21,1
2	Связная аппаратура	1 492,2	249,6	7 757,0	9 249,2	16,1
3	Звуковоспроизводящая аппаратура	11,9	100,5	2 104,0	2 115,9	0,6
4	Устройства памяти		96,2	1 508,6	1 508,6	0
5	Радио- теле- передатчики, приемники	4 760,0	609,0	2 447,5	7 207,5	66,0
6	Радиолокация, радионавигация	1 741,4	244,1	423,9	2 165,3	80,4
7	Устройства обеспечения безопасности	263,6	63,8	215,9	479,5	55,0
8	ЭКБ	1 855,8	659,6	6 841,2	8 697,0	21,3
9	Промышленная РЭА, в т.ч. медицинская, автомобильная и др.	3 819,3	685,9	4 846,2	8 665,5	44,1
10	Трансформаторы, преобразователи	2 586,9	117,8	1 214,3	3 801,2	68,1
	ИТОГО:	17 911,9	3 103,1	32 510,3	50 422,2	36,0

Структура отечественного рынка РЭА в 2013г.

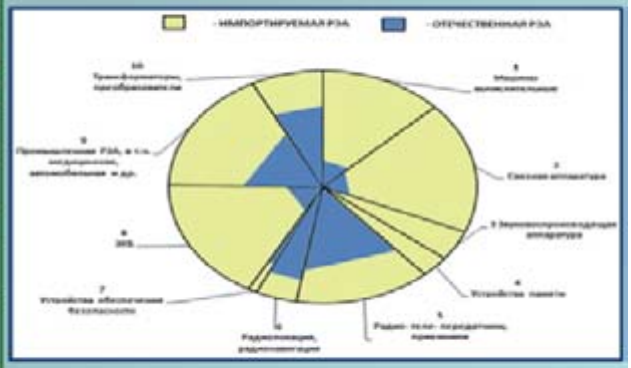

Рис. 4. Структура отечественного рынка РЭА

1. Риски в научно-технической сфере связаны с исчерпанием российским радиоэлектронным комплексом ОПК научно-технического задела СССР, а также с отсталостью и низкой эффективностью деятельности многих российских научно-технических организаций, взаимодействующих с ОПК. Такое положение уже существенно сказывается на темпах развития технологического потенциала оборонных отраслей радиоэлектронной промышленности.

Кроме того, риски этой группы усугубляют высокие темпы развития информационных и радиоэлектронных технологий за рубежом, и, прежде всего, в сфере разработки интеллектуальных информационных и телекоммуникационных систем. При этом вместо анализа и изучения новых технологических решений, позволяющих создавать качественно более эффективные средства вооруженной борьбы, КСАУС АСУС ОАЦСС ВС, постановка требований заказчиков вооружения сводится лишь к достижению существующих характеристик зарубежных аналогов.

Действующие механизмы формирования ГПВ слабо чувствительны к военно-политическим реалиям, экономическим и технологическим оценкам и стратегическим прогнозам развития информационных и телекоммуникационных технологий, средств информационных и кибернетических войн.

В этом отношении особо следует указать на практическое отсутствие связей между фундаментальной и прикладной наукой и практической деятельностью предприятий радиоэлектронного комплекса ОПК (рис. 3), что препятствует технологическому развитию ОПК и способствует возможному отставанию новейших образцов российского радиоэлектронного вооружения от современных средств вооружения.

Так, по состоянию на 2013–2014 годы степень перекрытия Перечня базовых и критических важных технологий исследований и разработок в области информационных систем, средств вычислительной техники, микропроцессоров и базового программного обеспечения составлял 35–40%, а Перечня приоритетных направлений фундаментальных прогнозных и поисковых исследований в интересах обороны и безопасности Российской Федерации — 30%. И такие примеры не единичны.

2. Риски в производственно-технологической сфере. В настоящее время производственно-технологический задел радиоэлектронного комплекса ОПК практически исчерпан, утрачен ряд уникальных производств, в том числе технологии производства около 40% стратегических материалов и возможность изготовления отдельных радиоэлектронных комплектующих изделий ВВСТ, включая КСАУС АСУС ОАЦСС ВС.

При этом темпы обновления оборудования радиоэлектронного комплекса в объеме 5–10% обеспечивают лишь поддержку состояния имеющегося парка КСАУС в СУС.

Продаваемое России производственное оборудование для радиоэлектронного комплекса ОПК, как правило, относится к предыдущим технологическим укладам и морально устаревает уже в ближайшей перспективе.

В результате модернизация предприятий радиоэлектронного комплекса ОПК не направлена на создание научного и производственного ядра 6-го технологического уклада, а обновление производственного оборудования осуществляется в основном в рамках 3 и 4-го технологических укладов, что не позволяет ожидать значимого производственного и технологического рывка в перспективе до 2020 года.

Для достижения необходимого уровня производственно-технологической базы радиоэлектронного комплекса ОПК, способной обеспечить качество и конкурентоспособность производимой продукции, потребуется увеличение доли современного оборудования к 2020 году до уровня мировых стандартов — до 75%. Для этого темпы обновления должны быть не менее 10–12% в год (рис. 4).

3. Риски в сфере организационно-управленческой деятельности организаций радиоэлектронного комплекса ОПК. Риски вызваны несогласованной и противоречивой деятельностью ос-

новных субъектов существующей системы управления процессами развития радиоэлектронного комплекса ОПК, начиная от расстановки приоритетов в этой сфере (рис. 5) и заканчивая проведением конкурсных процедур по реализации программных мероприятий.

В настоящее время в результате реализации мер по развитию и государственной поддержке радиоэлектронной промышленности оборонно-промышленного комплекса удалось только стабилизировать ситуацию в данной области.

Одна из основных причин такого положения дел в сфере управления (рис. 6) связана с недостаточностью прав и полномочий Военно-промышленной комиссии Российской Федерации, которые не обеспечивали ее полноправного участия в многоуровневом формировании государственных программ развития вооружений и оборонно-промышленного комплекса (рис.5), в том числе в интересах НЦУ, развития АСУС ОАЦСС ВС.

В настоящее время вне сферы эффективного влияния Военно-промышленной комиссии находятся вопросы согласования проектов общих технических и тактико-технических требований к образцам радиоэлектронных ВВСТ, в том числе КСАУС, регламентированного взаимодействия с интегрированными структурами радиоэлектронного комплекса ОПК, подотчетности перед ВПК государственных заказчиков, федеральных органов исполнительной власти, участвующих в выполнении Гособоронзаказа.

Одной из причин недостаточной эффективности выполнения федеральных целевых программ развития оборонных отраслей радиоэлектронного комплекса является слабое использование потенциала интегрированных структур в системе их управления.

Следует отметить, что в условиях завершения этапа становления интегрированных структур необходимо осмысление их роли в системе управления оборонными отраслями, включая развитие ГИС, ОАЦСС ВС, НЦУ.

Кроме того, актуальным может стать разработка механизмов государственного влияния на диверсификацию интегрированных структур радиоэлектронного комплекса ОПК — Государственной программы диверсификации ОПК в интересах НЦУ, включающей рекомендации по формированию облика диверсифицированного предприятия радиоэлектронного комплекса ОПК, направлениям диверсификации, рынкам, технологиям, а также механизмы контроля и ответственности.

4. Риски в сфере работы с кадрами связаны с недостаточной адаптацией управленческих и производственных кадров радиоэлектронного комплекса ОПК к новым реалиям ведения промышленного бизнеса, к требованиям Заказчиков, особенно в области создания и развития территориально распределённых систем, к классу которых относятся ГИС ГСУ, ОАЦСС ВС, НЦУ.

В настоящее время доля профессионально подготовленных управленческих кадров, способных обеспечить качественное развитие предприятий радиоэлектронного комплекса в интересах решения задач НЦУ, остается недостаточной. Имеющийся управленческий персонал интегрированных структур,

Рис. 5. Этапность реализации и зоны ответственности за реализацию АСУС ОАЦСС ВС

Рис. 6. Характеристика управленческой деятельности в сфере развития НЦУ

особенно руководящего звена, зачастую обладает преимущественно навыками поиска государственных заказов, знаниями в области эффективного экономического менеджмента и управления потоками полученных финансовых средств, что недостаточно для создания современных военных системных информационных и телекоммуникационных комплексов и средств на мировом уровне.

Дефицит управленческих, инженерных, рабочих квалифицированных кадров является одной из самых острейших проблем радиоэлектронного комплекса ОПК.

5. Риски в информационно-аналитической сфере. В сложившихся условиях актуальным становится анализ и проектирование эффективного управления и развития радиоэлектронного комплекса ОПК в интересах результативности решения задач, возлагаемых на НЦУ и её ядро ОАЦСС ВС, что может быть реализовано при соответствующем аналитическом обеспечении Главного управления связи Вооруженных Сил, ВПК, НЦУ.

В условиях недостаточности показателей государственной статистики, применяемой для анализа и прогнозирования развития радиоэлектронного комплекса ОПК, программных и аппаратных средств и комплексов ОАЦСС ВС, включая КСАУС и НЦУ, существенно искажается видение процессов, происходящих в ОПК в области проектирования, производства и эксплуатационного сопровождения информационных и телекоммуникационных средств и комплексов СГУ, ГИС (в том числе геоинформационных платформ), средств вычислительной техники, микропроцессоров и базового (общего, общесистемного, информационной безопасности, специального) программного обеспечения, что не позволяет сформировать адекватную картину состояния и динамики развития радиоэлектронного комплекса ОПК для результативной реализации задач, поставленных Главным управлением связи Вооруженных Сил, по развитию и модернизации АСУС ОАЦСС ВС.

Вместе с тем мировая практика показывает, что для анализа и проектирования эффективного управления и развития требуются подходы к контентной аналитической деятельности, в которых ключевыми являются форма, содержание и измеримость критериев (рис. 6), их адекватность целям анализа, высокий уровень абстрактности, а также лидирующая роль арбитражных разработок.

Это позволяет применять современные методологии исследования будущего радиоэлектронного комплекса ОПК, АСУС ОАЦСС ВС, НЦУ и управления ими, к которым относятся форсайт, национальное программирование, планирование и проектирование (рис. 5, 6).

В этой связи актуальным становится задача организации непрерывного воздействия на происходящие процессы, в том числе средствами системы управления рисками, Заказчиками, в том числе Главным управлением связи по развитию и модернизации АСУС ОАЦСС ВС в составе НЦУ во взаимодействии с ВПК РФ в развитии радиоэлектронного комплекса ОПК.

Представляется, что ядром этой системы могут стать контентные аналитические структуры НЦУ, образующие систему аналитического обеспечения радиоэлектронного комплекса ОПК, в основу которых могут быть положены рассмотренные риски, предлагаемые механизмы их минимизации, а также мониторинг полученных результатов деятельности по реализации ГОЗ и ГПВ.

В связи с изложенным представляется целесообразным совместно

ВПК, Заказчикам, в том числе Главному управлению связи Вооруженных Сил в части развития и модернизации ОАЦСС ВС и её АСУС, Минпромторгу России:

- разработать и внести изменения в Основы государственной политики в области развития радиоэлектронной промышленности оборонно-промышленного комплекса Российской Федерации, ОАЦСС ВС РФ и НЦУ обороной РФ на период до 2020 года и дальнейшую перспективу с учетом современных вызовов, угроз и рисков в деятельности оборонно-промышленного комплекса страны;
- разработать Военно-экономическую стратегию Российской Федерации развития радиоэлектронного комплекса ОПК, определяющую механизмы согласованного развития оборонной и гражданской сфер в области проектирования, производства и эксплуатационного сопровождения СГУ, ГИС, ОАЦСС ВС, НЦУ (в том числе геоинформационных платформ), средств вычислительной техники, микропроцессоров и базового (общего, общесистемного, информационной безопасности, специального) программного обеспечения, гармонизации экономического и оборонного строительства в региональном масштабе, а также механизмы государственно-рыночной модернизации ОПК в интересах решения задач НЦУ;
- обеспечить усиление мер государственного влияния на процессы развития радиоэлектронного комплекса ОПК и в этой связи уточнить права и полномочия Военно-промышленной комиссии в части наделения функций нормотворчества, регламентированного взаимодействия с интегрированными структурами радиоэлектронного комплекса, планового информирования ВПК со стороны федеральных органов исполнительной власти, должностных лиц НЦУ и государственных Заказчиков, в том числе Главного управления связи Вооруженных Сил в части развития и модернизации ОАЦСС ВС и её АСУС;
- разработать Государственную программу диверсификации радиоэлектронного комплекса ОПК, включающую рекомендации по формированию облика диверсифицированного предприятия ОПК, направлениям диверсификации, рынкам, технологиям, а также механизмы контроля и ответственности;
- разработать механизмы эффективного использования потенциала генеральных конструкторов ВПК в проектировании будущего, формировании планов фундаментальных и поисковых исследований в области проектирования, производства и эксплуатационного сопровождения ГИС ГСУ, ОАЦСС ВС, НЦУ, информационных систем (в том числе геоинформационных платформ), средств вычислительной техники, микропроцессоров и базового (общего, общесистемного, информационной безопасности, специального) программного обеспечения, а также оценки достигнутых результатов;
- развернуть инфраструктуру контентного аналитического обеспечения радиоэлектронного комплекса ОПК в составе НЦУ и обеспечить повышение его возможностей путем привлечения интеллектуального потенциала независимых высококвалифицированных аналитических структур, имеющихся в стране.
- Представляется, что предлагаемые меры позволят обеспечить выполнение поставленной Президентом Российской Федерации задачи по развитию НЦУ, ОАЦСС ВС, её АСУС и радиоэлектронного комплекса ОПК без существенного увеличения запланированных ранее финансовых ресурсов.