ФЕДЕРАЛЬНОЕ АГЕНТСТВО НАУЧНЫХ ОРГАНИЗАЦИЙ
РОССИЙСКАЯ АКАДЕМИЯ НАУК

Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ РАДИОТЕХНИКИ И ЭЛЕКТРОНИКИ
ИМ. В.А. КОТЕЛЬНИКОВА РАН

УДК 004.77

№ госрегистрации АААА-А16-116041910091-9

Инв. №

УТВЕРЖДАЮ
Директор
чл.-корр. РАН _____ С.А.Никитов
«__» _____ 2017 г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

Проблема интероперабельности в информационных системах военного назначения
(Этап 2016 года)

по теме:

АДАПТАЦИЯ ЕДИНОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ ИНТЕРОПЕРАБЕЛЬНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ РАЗЛИЧНЫХ КЛАССОВ С УЧЕТОМ ИХ ОСОБЕННОСТЕЙ

№ 0030-2015-0190, шифр «Аргонавт-4»
(промежуточный)

Научный руководитель
д.т.н. _____ Олейников А.Я.

Москва 2017 г.

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель темы: Г.н. с., д.т.н.,	16.01.17 А.Я. Олейников подпись, дата	(введение, заключение, разделы: 1, 2, 3, приложение Д)
Исполнители темы:		
н.с., к.т.н.	16.01.17 А.А. Башлыкова подпись, дата	(приложение Д)
н.с,, к.т.н.	16.01.17 А.А. Каменщиков подпись, дата	(подраздел 2.2, раздел 3, приложения А, Д)
Ученый секретарь Института, к.ф.-м..н.	16.01.17 И.И. Чусов подпись, дата	(подраздел 2.1, приложение Д)
н.с.	16.01.17 Т.Д. Широбокова подпись, дата	(раздел 3, приложения Б, Д)

РЕФЕРАТ

Отчет 101 с., 15 рис., 2 табл., 58 источников, 5 прил.

Объектом исследования являются методы и средства обеспечения адаптации единого подхода к обеспечению интероперабельности информационных систем различных классов с учетом их особенностей. В данном промежуточном отчете в соответствии с планом на 2016 год рассмотрены возможности применения разработанного ранее и получившего статус ГОСТ Р 5062-2012 единого подхода к обеспечению интероперабельности в информационных системах военного назначения.

ВОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ, ИНТЕРОПЕРАБЕЛЬНОСТЬ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ ВОЕННОГО НАЗНАЧЕНИЯ, КОНЦЕПЦИЯ, АРХИТЕКТУРА, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, МОДЕЛЬ ИНТЕРОПЕРАБЕЛЬНОСТИ, ПРОФИЛЬ ИНТЕРОПЕРАБЕЛЬНОСТИ, СЕТЕЦЕНТРИЧЕСКАЯ ВОЙНА, СТАНДАРТЫ

Цель проекта – исследование особенностей обеспечения интероперабельности в информационных системах военного назначения на основе использования стандартов информационных технологий в условиях сетецентрической войны.

В процессе проведения работы проводились исследования существующих методов достижения интероперабельности, моделей и объектов стандартизации для Вооруженных Сил НАТО, США и других стан, а также Российской Федерации.

В результате исследования разработан проект национального стандарта ГОСТ Р: «Информационные технологии. Военное дело. Интероперабельность. Основные положения».

Степень внедрения – подготовлен проект указанного выше национального стандарта.

Эффективность - результаты исследований позволяют увеличить эффективность вооруженных сил РФ и достичь информационного преимущества в условиях сетецентрической войны, используя профиль интероперабельности, обеспечить «общий язык» между заказчиками, разработчиками информационных систем и пользователями.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящем отчете о НИР использованы ссылки на следующие стандарты:

ИСО/МЭК 7498–1–99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

ГОСТ Р 55062-2012 Информационные технологии. Системы промышленной автоматизации их интеграция. Интероперабельность. Основные положения.

ГОСТ Р ИСО 11354-1-2012 Усовершенствованные автоматизированные технологии и их применение. Требования к установлению интероперабельности процессов промышленных предприятий. Часть 1. Основа интероперабельности предприятий.

ОПРЕДЕЛЕНИЯ

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями:

архитектура: Фундаментальная организация системы, реализованная в ее компонентах, их взаимосвязях друг с другом и с окружающей средой и руководящие правила проектирования и развития системы. Термин «архитектура» определяется в стандартах системной и программной инженерии применительно к системам.

взаимодействие войск: Согласованные по задачам направлениям, рубежам и времени действия участвующих в операции (бою) различных видов вооружённых. сил, родов войск (родов сил), объединении и соединении в интересах достижения общей цели. Необходимость взаимодействия войск возникла с зарождением армии. По мере совершенствования оружия, появления родов войск (пехоты, кавалерии, артиллерии и др.), развития организационной структуры армии и боевых порядков значение взаимодействия возрастало.

единое информационное пространство: Совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей.

интероперабельность: Способность двух и более систем или элементов обмениваться информацией и использовать эту информацию.

интероперабельная система: Система, в которой входящие в неё подсистемы работают по независимым алгоритмам, не имеют единой точки управления, всё управление определяется единым набором стандартов – профилем интероперабельности.

информационная инфраструктура: Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам

облачные вычисления: Модель предоставления повсеместного и удобного сетевого доступа по мере необходимости к общему пулу конфигурируемых вычислительных ресурсов (например, сетей, серверов, систем хранения, приложений и сервисов), которые могут быть быстро предоставлены и освобождены с минимальными усилиями по управлению и необходимостью взаимодействия с провайдером услуг (сервис-провайдером)».

открытая система : Система, реализующая достаточно открытые спецификации или стандарты для интерфейсов, служб и форматов, облегчающая прикладному программному средству, созданному должным образом: перенос его с минимальными изменениями в широком диапазоне систем, использующих продукты от разных производителей (поставщиков); взаимодействие с другими приложениями, расположенными на локальных или удаленных системах; взаимодействие с людьми в стиле, облегчающем переносимость пользователя.

профиль интероперабельности): Согласованный набор стандартов, структурированный в терминах модели интероперабельности.

радиоэлектронная борьба (РЭБ): — Разновидность вооружённой борьбы, в ходе которой осуществляется воздействие радиоизлучениями (радиопомехами) на радиоэлектронные средства систем управления, связи и разведки противника в целях изменения качества циркулирующей в них военной информации, защита своих систем от аналогичных воздействий, а также изменение условий (свойств среды) распространения радиоволн.

реализация: Программно-аппаратная реализация конкретной интероперабельной системы в соответствии с профилем интероперабельности.

семантическая интероперабельность: Способность любых взаимодействующих в процессе коммуникации ИС одинаковым образом понимать смысл информации, которой они обмениваются.

сетецентрическая война: (или «Сетецентрические боевые действия», «Сетецентрические операции») — военная доктрина (или концепция ведения войны на основе сетевых технологий), впервые примененная на практике Министерством обороны США.

стандарт: Документ, согласованный и принятый аккредитованной организацией, разрабатывающей стандарты, который содержит общепринятые и многократно используемые правила, руководства или характеристики для работ или их результатов, предназначенные для достижения оптимальной степени упорядочения и согласованности в заданном контексте.

техническая интероперабельность: Способность к обмену данными между участвующими в обмене системами.

эталонная модель интероперабельности: Трехуровневая модель, зафиксированная в ГОСТ Р 55062 -2012, представляющая собой развитие прикладного уровня эталонной

семиуровневой модели взаимосвязи открытых систем, описанной в ГОСТ Р ИСО/МЭК 7498–1–99.

сверхсложные системы (система систем) – объединение проблемно-ориентированных или разрозненных систем, которые объединяют свои ресурсы и возможности для того, чтобы создать новую сложную систему, обладающую большей функциональностью и производительностью, чем просто сумма составляющих систем.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИС (IS): информационные системы (Information Systems).

ИТ (IT): информационная технология (Information Technology).

ИКТ (ICT): информационно-коммуникационные технологии (Information and Communication Technologies).

ИСО (ISO): Международная организация по стандартизации (International Organization for Standardization)

ЕИП: единое информационное пространство.

ЕИП ВС РФ: Единое информационное пространство Вооруженных Сил РФ

СЦВ: сетецентрическая война

ВД РФ: Военная доктрина РФ

ВС РФ: Вооруженные Силы Российской Федерации.

ВС США и НАТО: Вооруженные силы США и НАТО

МО США: Министерство обороны США

НВС США: Национальная военная стратегия США

РЭБ: радиоэлектронная борьба

ВВЕДЕНИЕ

Общеизвестно, что в настоящее время ни одна область человеческой деятельности не может эффективно развиваться без использования информационно-коммуникационных технологий (ИКТ). Поэтому некоторое время тому назад появились такие понятия как электронная наука (e-science), электронное образование (e-education), электронное здравоохранение (e-health), электронный бизнес (e-business), электронное правительство (e-government) и т.д. , которые являются составляющими электронного общества (e-society). В этом ряду стоит и понятие электронное военное дело (e-military).

Использование ИКТ реализуется в виде информационных систем (ИС) соответствующего назначения и масштаба, причем общая тенденция состоит в том, что эти ИС должны взаимодействовать друг с другом, образуя информационную инфраструктуру (ИИС) , объединяющую информационные, вычислительные и телекоммуникационные ресурсы.

Поскольку, неизбежно, различные ИС реализуются на отличающихся программно-аппаратных платформах, образуемая ИИС представляет гетерогенную среду, в которой возникает проблема совместимости и взаимодействия входящих в него ИС. Мировая практика говорит о том, что для этого ИС должны обладать свойствами открытости, а именно масштабируемостью, переносимостью программ и данных и интероперабельностью. Обобщенно говоря, названные свойства достигаются на основе использования стандартных интерфейсов, а более детально – на основе использования согласованных наборов стандартов ИКТ на протоколы, форматы данных и др., называемых профилями. В последние годы во всем мире особое значение придается обеспечению свойства интероперабельности. Это связано с тем, что недостаточно просто обменяться информацией, но и необходимо правильно истолковать и использовать обмененную информацию, т.е. речь идет о переходе от технической к семантической интероперабельности. Достижение семантической интеропебельности – совокупность сложных научно-технических и организационно-методических задач, получившая название «проблемы интероперабельности».

ИИС, обладающая свойствами открытости, составляет основу Единого информационного пространства. Чем больше масштаб ЕИП, тем выше уровень гетерогенности ИКТ-среды, а следовательно острее проблема интероперабельности. Проблемой интероперабельности во всем мире занимаются многие организации. Авторы более 20 лет занимались проблемой открытых систем и около 10 лет занимаются проблемой интероперабельности. На основе анализа зарубежного и отечественного опыта, а также собственного опыта по созданию открытых систем нами было показано, что проблема

интероперабельности существует для систем всех назначений и любого масштаба, от нано-систем до сверхбольших систем, получивших название «система систем» (System of Systems –SOS). На основе этого обобщения нами предложен единый подход к обеспечению интероперабельности, зафиксированный в государственном стандарте ГОСТ Р 55062-2012. При едином подходе, в зависимости от конкретной области применения, получаемые решения отличаются, что проявляется в составе стандартов профиля на уровнях выше технического.

В течение трех лет авторы в рамках госзадания выполняют проект «Исследования проблемы интероперабельности к информационным системам широкого класса» Все вышеизложенное относится и к области военного дела, и на этапе 2016 г. авторы осуществили попытку применить свой опыт к решению проблемы интероперабельности к ИС в Вооруженных Силах Российской Федерации. Нам представляется, что сейчас такая работа крайне актуальна, поскольку идут боевые действия в Сирии и ведутся разговоры о возможности третьей мировой войны.

Основная часть отчета содержит три главы.

В главе 1 дано краткое описание разработанного авторами и представленного в виде блок-схемы единого подхода к обеспечению интероперабельности ИС широкого класса.

В главе 2 рассмотрена проблема интероперабельности в Вооруженных Силах других государств и Российской Федерации. Следует подчеркнуть, что вся работа выполнена на основе анализа открытых источников, и их список содержит 58 наименований. В главе два раздела. Раздел 2.1 содержит описание основных положений концепции т.н. сетецентрической войны, которая реализуется в Вооруженных Силах большинства других стран, в объединённых силах НАТО и в Вооруженных силах Российской Федерации. Особо подчеркивается, что основным принципом концепции сетецентрической войны, ее «краеугольным камнем» служит обеспечение интероперабельности. Поэтому раздел 2.2 посвящен рассмотрению проблемы интероперабельности в Вооруженных Силах других государств (2.2.1) и Российской Федерации (2.2.2). При этом основное внимание уделяется официальным документам различного уровня (см. приложения А и Б). Отмечается, что в зарубежных документах выделяется роль интероперабельности, а в отечественных прямого упоминания нет. Важно отметить также следующее: кроме концептуальных документов, на сайтах НАТО и Министерства обороны США имеется большое количество подробных многостраничных документов типа приказов и инструкций для практического достижения интероперабельности. В отечественных открытых источниках подобные документы отсутствуют. Авторы ставят вопрос следующим образом: если этих документов нет вообще,

то, ввиду важности проблемы интероперабельности для современных методов ведения войны, возникает угроза национальной безопасности Российской Федерации.

Отдавая себе отчет в том, что для решения проблемы интероперабельности в ВС РФ требуются большие квалифицированные коллективы и весьма значительные ресурсы, авторы тем не менее делают попытку применить разработанный ими единый подход (ключевые этапы) к решению этой проблемы (глава 3). При этом были использованы материалы о создании в Минобороне РФ Национального центра управления обороной Российской Федерации. Авторы предложили концепцию обеспечения интероперабельности в Вооруженных силах Российской Федерации, Архитектуру Единого информационного пространства ВС РФ, модель интероперабельности, представляющую собой расширение эталонной модели интероперабельности, описанной в ГОСТ Р 55062-2012, а также проект профиля интероперабельности Вооруженных Сил Российской Федерации. При этом использовалось положение, содержащееся в Военной доктрине Российской Федерации о том, что ориентация должна вестись на международные стандарты.

Следует отметить, что на основании материалов данного отчета 25 ноября 2016 г. был сделан пленарный доклад на II Межведомственной научно-практической конференции «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации». Конференция была организована Национальным центром управления обороной Российской Федерации, и на основании сделанного нами доклада в принятом Решении отмечена важность проблемы интероперабельности при решении задач в области обороны и безопасности Российской Федерации (см. приложения В и Г).

Отчет содержит ряд приложений, важнейшим из которых служит проект ГОСТ Р «Информационные технологии. Военное дело. Интероперабельность. Основные положения» (см. приложение Д).

1 Единый подход к обеспечению интероперабельности информационных систем широкого класса

Как известно, сегодня практически ни одна область человеческой деятельности не может эффективно развиваться без использования информационно-коммуникационных технологий (ИКТ). Отсюда возникли такие понятия, как электронная наука (e-science), электронное образование (e-education), электронный бизнес (e-business), электронное правительство (e-government) и т.д., которые являются составляющими электронного общества (e-society). В этом ряду стоит и понятие «электронное военное дело» (e-military). Легко убедиться, что для любого из этих понятий существует проблема интероперабельности. Авторы убедились в том, что проблема интероперабельности актуальна практически для любой области человеческой деятельности, что можно изобразить следующим образом (см. рисунок 1). Применение ИКТ реализуется в виде ИС различного назначения.

Рисунок 1 — Компоненты информационного общества – ИС различного назначения.

ИС можно классифицировать не только по областям применения, но и по масштабу (см. рисунке 2).

Рисунок 2 — Классификация ИС по масштабу

Проведя анализ большого количества работ по системам различного назначения и масштаба, мы убедились в том, что проблема достижения интероперабельности - крайне актуальная и сложная многоаспектная научно-техническая и организационно-методическая проблема, над которой работают многие организации и многочисленные исследователи во всем мире. Появляющееся все новые материалы говорят о том, что разные организации и исследователи используют фрагментарные подходы, и проблема далека от своего решения. К наиболее актуальным задачам относятся [2].

- вопросы терминологии;
- виды и модели интероперабельности;
- измерение интероперабельности;
- выбор объектов стандартизации – ключевых интерфейсов;
- исследование особенностей обеспечения интероперабельности для систем различных классов;
- выработка единого подхода к обеспечению интероперабельности - создание нормативно-технических документов: стандартов, профилей, рекомендаций, методик и сводов правил;
- оценка экономического эффекта.

Одной из важнейших задач служит определение модели интероперабельности, поскольку совершенно очевидно, что если разные организации или разработчики будут пользоваться разными моделями, они никогда не найдут общего языка.

Как видим, одной их задач в проблеме интероперабельности служит выработка единого подхода к обеспечению интероперабельности ИС самого широкого класса. В результате авторами был предложен такой подход [2] (см. рисунок 3), зафиксированный впоследствии в виде национального стандарта ГОСТ Р 55062-2012 [3]. Представляется важным, что в этом стандарте впервые в международной практике зафиксирована эталонная модель интероперабельности (см. рисунок 4).

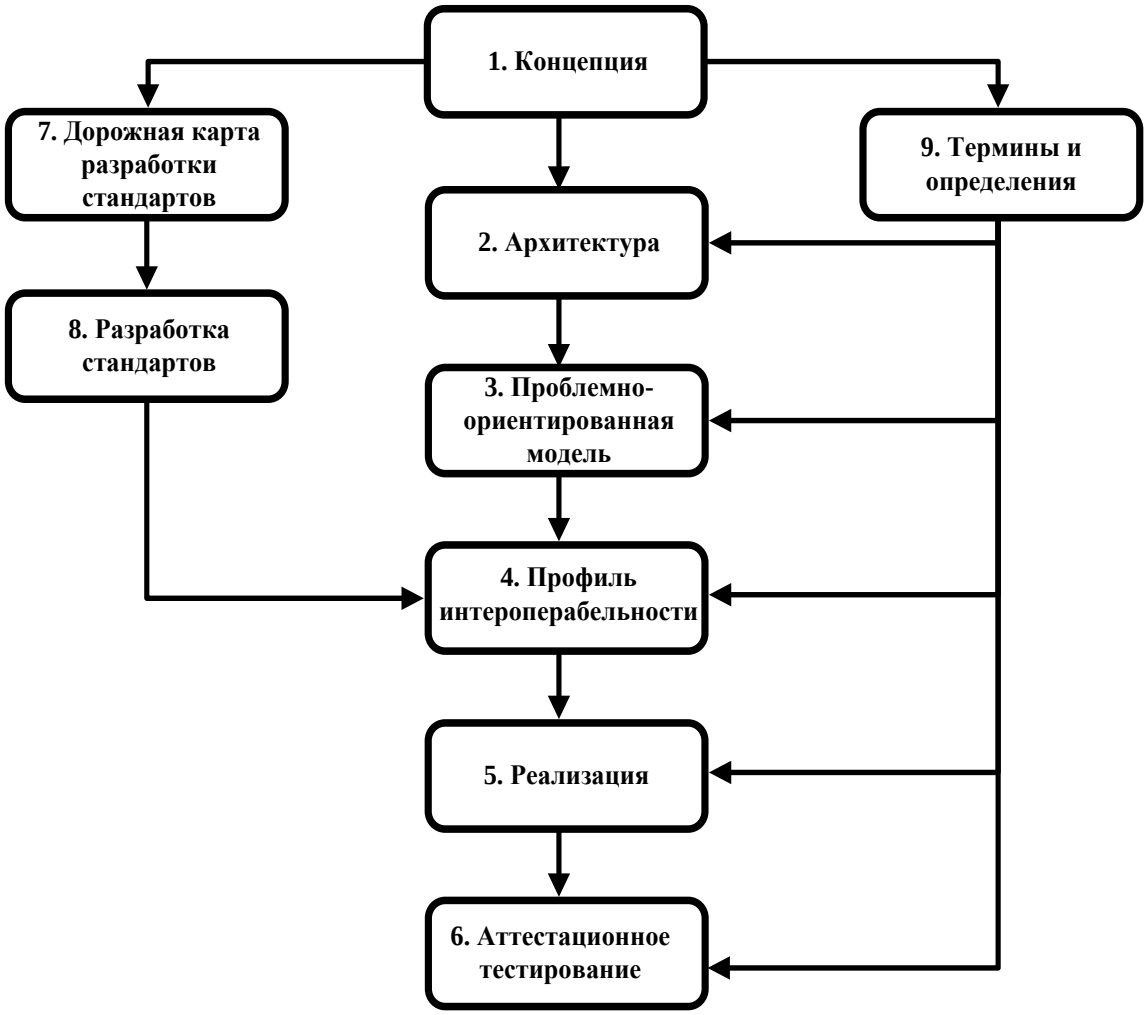


Рисунок 3 — Блок- схема единого подхода к достижению интероперабельности для ИС

К основным этапам ЕП относятся этапы 1-5, а к вспомогательным – этапы 6-9.

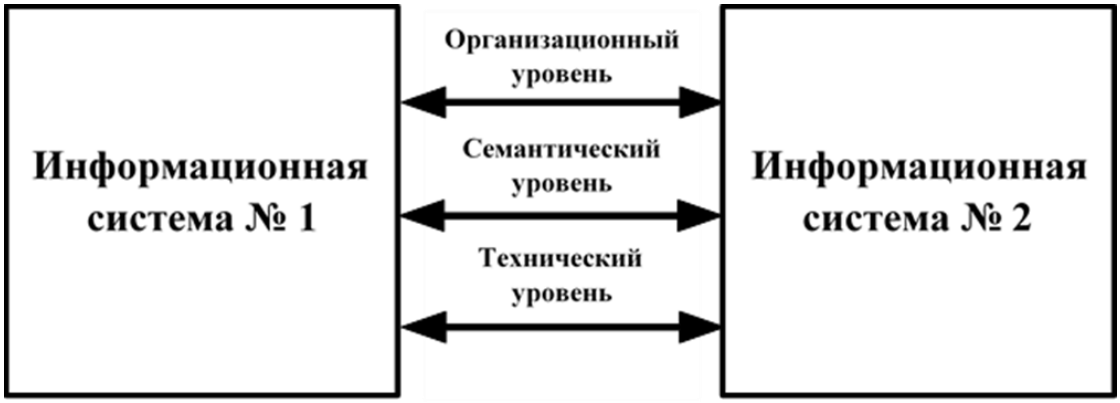


Рисунок 4 — Эталонная модель интероперабельности

Впоследствии предложенный нами единый подход был применен к ИС различных классов [5,6,7].

Следует отметить, что при достижении интероперабельности встречаются барьеры. Подробно о барьерах интероперабельности сказано в ГОСТ Р ИСО 11354-1-2012 [8], в котором, в частности, выделены три категории барьеров: концептуальные, технологические и организационные.

2 Проблема интероперабельности в Вооруженных Силах

Прежде всего следует отметить, что войны можно классифицировать и разбить по поколениям в соответствии с революциями в техническом прогрессе и основными видами применяемого вида вооружения [10] (см. Таблицу 1).

Таблица 1 — Классификация войн по основному виду вооружения

Поколения войн	**Основные виды вооружения**	**Исторический период**
Первое	Для военного противоборства вместо камней и палок воины стали применять специально изготовленные копья, мечи, луки, стрелы, а также доспехи.	Три с половиной тысячи лет из общих пяти с половиной тысяч лет существования цивилизации на нашей планете
Второе	Огнестрельное оружие: ружья, пистолеты, пушки.	XII-XIII века прошлого тысячелетия
Третье	Нарезное оружие	Примерно 200 лет назад
Четвертое	Автоматическое оружие, которое в больших количествах стали устанавливать на танках, самолетах, кораблях. Войны, рожденные четвертой революцией в военном деле, продолжаются и сейчас.	Примерно 100 лет назад
Пятое	Ядерное оружие	1945 г.
Шестое	Информационно-коммуникационные технологии – компьютерные сети, высокоточное оружие, роботы	Последнее десятилетие XX века

Совершенно очевидно, что проблема взаимодействия в ВС так же стара, как само понятие ВС (см. например [9]), но средства обеспечения взаимодействия непрерывно совершенствовались. На сегодня, все более доминируют средства ИКТ, что изменило и саму концепцию ведения боевых действий, появились понятия войны шестого поколения [10], сетецентрической войны, взаимодействие ведется на основе распределённых компьютерных сетей типа Интернет.

2.1 Сетецентрическая война

Описанию понятия, концепции и основных проблем сетецентрической (сетецентричной) войны (СЦВ) посвящено много материалов, в том числе имеются и монографии (см. например [11]).

На рисунке 5 представлена упрощенная схема, дающая представление о сетецентрической войне [12].

Рисунок 5 — Упрощенная схема сетецентрической войны

Следует отметить, что кроме использования компьютерных сетей к характерным свойствам войны 6-го поколения относятся также использование высокоточного оружия и безэкипажных средств (роботов) как наземного, так и других видов базирования. Совершенно очевидно, что сверхточное оружие и роботы также не могут функционировать без использования ИКТ.

Изложение концептуальных положений СЦВ можно найти в Википедии.

Концепция СЦВ это концепция ведения боевых действий, предусматривающая увеличение боевой мощи группировки объединённых сил за счет образования информационно-коммутационной сети, объединяющей источники информации (разведки), органы управления и средства поражения (подавления), обеспечивающая доведение до участников операций достоверной и полной информации об обстановке в реальном времени. В результате достигается ускорение управления силами и средствами, повышение темпа операций, эффективности поражения сил противника, живучести своих войск и уровня самосинхронизации боевых действий. Концепция СЦВ предполагает перевод преимуществ, присущих отдельным ИКТ, в конкурентное преимущество за счет объединения в устойчивую сеть информационно достаточно хорошо обеспеченных, географически рассредоточенных сил. Концепция СЦВ содержит три принципа:

- Силы, объединённые достаточно надежными сетями, получают возможность качественно нового обмена информацией.
- Обмен информацией повышает качество информации и уровень общей информированности о происходящем;

- В результате общая ситуационная осведомленность такова, что позволяет обеспечивать необходимые сотрудничество и самосинхронизацию, повышает устойчивость и скорость передачи команд, что, в свою очередь, резко повышает эффективность выполнения боевой задачи.

Три наиболее отличительные свойства «сетевой войны» по сравнению с традиционной войной в нынешнем её понимании выглядят так:

1. Широкая возможность использования географически распределенной силы. Ранее из-за разного рода ограничений было необходимо, чтобы подразделения и элементы тылового обеспечения располагались в одном районе в непосредственной близости к противнику или к объекту, который обороняется. Новая концепция снимает эти ограничения, и это было практически подтверждено.

2. Сетецентрическую войну способны вести только высокоинтеллектуальные силы. Такие силы, пользуясь знаниями, полученными от всеохватывающего наблюдения за боевым пространством и расширенного понимания намерений командования, способны к большей эффективности, чем при ведении автономных, сравнительно разрозненных действий.

3. Третье отличие — наличие достаточно эффективных коммуникаций между объектами в боевом пространстве. Это дает возможность географически распределенным объектам проводить совместные действия, а также динамически распределять ответственность и весь объём работы, чтобы приспособиться к ситуации.

В концептуально-теоретическом плане модель сетецентрической войны представляет собой систему, состоящую из трех решеток-подсистем: сенсорной, информационной и боевой [13] (см. рисунок 6).

Рисунок 6 — Логическая модель сетецентрической войны

Как видно из рисунка, основу этой системы составляет информационная решетка, на которую накладываются взаимно пересекающиеся сенсорная и боевая решетки. Информационная решетка-подсистема пронизывает собой всю систему в полном объеме. Элементами сенсорной системы являются «сенсоры» (средства разведки), а элементами боевой решетки – «средства поражения». Эти две группы элементов объединяются воедино органами управления и командования.

Следует заметить, что за рубежом, в первую очередь, в ВС США концепция СЦВ войны сформулирована в военных доктринах «Joint Vision 2010», «Joint Vision 2020». Последний, опубликованный 1 июля 2015 г. официальный документ МО США, подтверждающий ориентацию на Концепцию СЦВ «Национальная военная стратегия США» (НВС США) [14], сменивший предыдущую версию, принятую в 2011 году. В документе Пентагона напрямую термин СЦВ не употребляется, но фактически концепция СЦВ составляет одну из основ стратегии. ВС США и НАТО уже достаточно давно перешли к реализации концепции СЦВ на практике, начиная с войны в Ираке.

В нашей же стране, как до последнего времени отмечалось в многочисленных статьях [13, 15-24] имелись разные точки зрения. Но в целом доминировало мнение, что мы также должны принять концепцию СЦВ [15]. Действительно, Указом Президента 25 декабря 2014 г. была утверждена «Военная доктрина РФ» (ВД РФ) [25]. В [26] приведены параллельные тексты обоих документов (НВС США и ВД РФ) на русском языке, что дает возможность провести их сравнительный анализ. Так что можно сделать вывод: и в ВД РФ термин СЦВ не употребляется, но фактически можно считать, что концепция принята. Более того, судя по ряду сообщений, в ВС РФ идет и практическая реализация концепции СЦВ. Было сообщено, об испытании боевого Интернета во время военных действий в Сирии [27], а также о приспособленности танка «Армата» для участия в СЦВ [28]. Одним из доказательств практической реализации концепции СЦВ следует считать и создание Национального центра управления обороной РФ [29].

Из рисунков 5 и 6 становится совершенно очевидно, что с точки зрения применения продуктов информационных технологий создаваемая ИКТ-среда ВС РФ относится к классу сверхсложных систем (System of Systems) (см. также рисунок 2) является сугубо гетерогенной, и проблема обеспечения интероперабельности – особенно актуальной и сложной.

2.2 Проблема интероперабельности в рамках СЦВ

Ниже мы рассмотрим состояние проблемы интероперабельности в зарубежных ВС и ВС РФ.

2.2.1 Зарубежные ВС

Прежде всего, отметим, что понятие «интероперабельность» в зарубежных ВС используется, отличное от данного ИСО. Более того, используется несколько определений. В таблице 2 приведено определение ИСО и три определения из военных источников.

Таблица 2 — Определения понятия интероперабельность в военной сфере

NN п.п.	На английском языке	Источник	Перевод на русский язык
1	The ability of two or more systems or components to exchange information and to use the information that has been exchanged.	ISO/IEC 24765:2009, Systems and Software Engineering -- Vocabulary.	Интероперабельность - способность двух и более систем или компонетов обмениваться информацией и использовать обмененную информацию
2	Interoperability – the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together	Joint Vision 2020 документ Joint Chief of Staff http://archive.defense.gov/news/newsarticle.aspx?id=45289	Интероперабельность – способность систем, подразделений или видов и родов войск вооруженных сил предоставлять или воспринимать услуги другим подразделений или видов и родов войск вооруженных сил и использовать эти услуги так, чтобы сделать возможным эффективное взаимодействие
3	The ability to operate in synergy in the execution of assigned tasks. Source: JP 3-0 The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be	DoD Dictionary of military Term http://www.dtic.mil/doctrine/dod_dictionary/	Способность действовать совместно при выполнении заданных задач Условие, достигаемое между электронными коммуникационными системами или отдельными элементами электронных коммуникационных систем, при котором информация или услуги могут непосредственно и

	exchanged directly and satisfactorily between them and/or their users. Source: JP 6-0		удовлетворительно обмениваться между ними и/или пользователями

Изучив приведенные определения, приходим к выводу, что в современных условиях, когда интероперабельность должна обеспечиваться не только во время боевых действий между подразделениями всех уровней управления, но и с другими ведомствами и организациями, следует пользоваться определением, данным ИСО. При этом легко заметить, что третье определение, данное военными, практически совпадает с определением ИСО.

Следует отметить, что в открытом доступе имеется достаточно много документов НАТО, США и др. стран, содержащих официальные документы по интероперабельности и средствам ее достижения. В приложении А приведены основные зарубежные документы. Материалы расположены по принципу: наиболее поздние наверху, а ниже - ранние по датам.

С точки зрения конечной цели данного отчета следует выделить несколько моментов:

Первое – для обеспечения взаимопонимания между всеми участниками им необходимо рассуждать в терминах одной и той же модели. В ВС НАТО и США в течение многих лет используется модель LISI (см. таблицу А.1. п. 8). Модель LISI представляет собой расширение эталонной модели интероперабельности, зафиксированной нами в ГОСТ Р 55062-2012.

Второе - поскольку профиль представляет собой узловой момент в обеспечении интероперабельности, остановимся более подробно на документе 2 «NATO Interoperability Standards and Profiles NISP) (см. таблицу А.1. п. 2). «Стандарты и профили НАТО, обеспечивающие интероперабельность»

Документ NISP разработан специальной постоянно действующей группой NATO Consultation, Command and Control (C3) Board Interoperability Profiles Capability Team (IP CaT). Первое, на что следует обратить внимание, этот документ совершенно свежий – дата публикации - июнь 2016 г., и в нем выделены обновления по сравнению с предыдущей редакцией. Второе – документ включает 3 тома, общим объемом 230 страниц, т.е. он крайне детальный. Третье – документ выполнен с ориентацией на сервис-ориентированную архитектуру . Четвёртое - приведенные стандарты и профили являются обязательными для участников НАТО.

Том 1 - Introduction and Management: В этом томе описываются основные процедуры для применения NISP в объединённых ВС НАТО.

Том 2 - Agreed Standards: Этот том содержит согласованный перечень стандартов. При этом выделяются «обязательные», «формирующиеся», «устаревающие», «устаревшие» и «неприемлемые» стандарты. Всего перечислено почти 500 стандартов, куда входят стандарты ИСО, корпоративные стандарты, включая стандарты НАТО, охватывающие все виды услуг, в том числе услуги геоинформационных систем, аудио и видео услуги.

Том 3 - Profiles: В этом томе приведены профили интероперабельности и руководства по достижению интероперабельности. Следует подчеркнуть, что ввиду сложности проблемы, приходится говорить о некоторой иерархической классификации профилей, которая называется таксономией и выполнена в соответствии с известным документом ИСО/МЭК ТО 10000-1,2,3:1999 (см. например [1] стр. 56)

Структура профилей НАТО достаточно сложная, но можно говорить и о «Минимальном профиле интероперабельности».

Знакомство с описанным документом приводит к следующему выводу: если наши ВС намерены противостоять сетецентрическим военным действиям НАТО, в которых интероперабельность является важнейшим условием, наша страна должна обязательно иметь документ такого уровня.

Касательно проблемы интероперабельности необходимо также отметить, что в МО США и ВС НАТО она прописана совершенно явственно и обозначена как один из краеугольных камней военной политики [14, 30] Так в [14,26] в разделе «Создание инноваций, подразделе «С» сказано: «Мы улучшаем комплексное взаимодействие. Мы на стадии определения следующего набора стандартов интероперабельности с будущими возможностями. В виду трудностей, связанных с ограничением и воспрещением доступа и маневра мы всё чаще сталкиваемся с тем, что в будущем наши ВС будут вынуждены действовать в контролируемой среде. Ключевым моментом для обеспечения такого доступа будет развертывание безопасных взаимодействующих систем между службами, союзниками, межведомственными организациями и коммерческими партнерами. Приоритетные усилия в этой связи будут направлены на Единую информационную среду (ЕИС), улучшение глобального комплексного снабжения и построение Единого предприятия разведки, наблюдения и рекогносцировки. Результат этих инициатив, особенно усиление связности и кибербезопасности благодаря ЕИС, обеспечит фундамент для будущей интероперабельности».

Важно отметить следующее: кроме концептуальных документов, на сайтах НАТО и МО США имеется большое количество подробных многостраничных документов типа приказов и инструкций для практического достижения интероперабельности. Эти документы касаются терминологии [31], архитектуры [32,33], модели интероперабельности [34], профилей [35] и входящих в них стандартов [36], и др. включая вопросы сертификации [37]. Мы рассмотрели эти документы по возможности детально. Основной вывод: проблеме обеспечения интероперабельности в зарубежных ВС придается очень большое значение, имеются подробные директивы и инструкции по ее достижению [38]. Можно отметить фрагментарность подходов, обусловленную высокой сложностью проблемы, но в последнее время вырабатывается подход на базе сервис-ориентированной архитектуры [39].

2.2.2 Состояние проблемы интероперабельности в ВС РФ

Следует сказать, что авторы впервые выполнили НИОКР по проблеме интероперабельности в интересах ВС РФ в 1998 г. [40]. Реально в этой работе был предложен профиль технической интероперабельности для ВС РФ, который можно назвать профилем интероперабельности ВС РФ первого поколения. К сожалению, эта работа не получила дальнейшего развития, хотя получила одобрение в НИИ 27 Генштаба МО РФ.

За истекшее время появился ряд документов государственного уровня, в которых отмечается важность стандартизации для создания единого информационного пространства с точки зрения безопасности и обороны страны (см. приложение Б).

К этим документах относятся: Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов [41], Доктрина информационной безопасности Российской Федерации (Указ президента РФ №646 от 5 декабря 2016 г.) [42]. К сожалению, документов, посвященных проблеме интероперабельности, подобно существующим во многих странах и в Евросоюзе «e-Government interoperability framework» (Концепция интероперабельности электронного правительства [43] у нас в стране не появилось.

Как видно, российских документов гораздо меньше, чем в других странах, во-вторых в них напрямую не упоминается проблема интероперабельности, если и имеются отдельные положения, то и они представляются спорными. Так, в ВД РФ сказано очень кратко п. 46 г): «качественное совершенствование средств информационного обмена на основе использования современных технологий и международных стандартов, а также единого информационного пространства Вооруженных Сил, других войск и органов как части информационного пространства Российской Федерации». Но, стандарт это передовая практика, зафиксированная в виде документа. Таким образом, получается, что у нас в стране

не должно быть собственных технологий, а ориентация должна быть на зарубежные, что представляется довольно странным для военного дела. Кроме того, это положение прямо противоречит ФЗ «О стандартизации», где сказано, что к документам по стандартизации в соответствии с настоящим Федеральным законом относятся документы национальной системы стандартизации [44]. Директив и инструкций, касающихся достижения интероперабельности в открытых источниках нам обнаружить не удалось, что может говорить либо о высоком уровне закрытости, либо об отсутствии таковых. Следует отметить, что, также, как и зарубежных документах, в отечественных говорится о слиянии Единого информационного пространства (ЕИП) вооруженных сил с ЕИП систем государственного управления. Возможно, в этом и дело, поскольку надо признать, что проблема интероперабельности очень слабо отражена в государственных документах по информатизации, таких как Государственная программа Российской Федерации "Информационное общество (2011-2020 годы)" (утв. постановлением Правительства РФ от 15 апреля 2014 г. № 313) [45], где в перечне мероприятий названо «формирование открытых стандартов взаимодействия информационных систем, в том числе разработка и поддержка профиля открытых стандартов архитектуры государственных информационных систем, форматов и протоколов обмена данными, обеспечивающих совместимость государственных информационных систем и их компонентов». Однако в открытом доступе эти профили пока отсутствуют.

Таким образом, можно сделать однозначный вывод о том, что в отечественных концептуальных документах высокого уровня, какими являются названные выше, вопросам интероперабельности на основе использования ИКТ-стандартов уделяется внимание, но, можно сказать, это − декларативный уровень.

Что касается публикаций о необходимости обеспечения интероперабельности в ВС РФ в том понятии как было приведено выше, нам известны только отдельные публикации [46].

В [47] описано состояние работ по стандартизации ИКТ, где отмечается, что за последние 15-20 лет в РФ наметилось существенное отставание в области ИТ-стандартизации. Такое положение привело к ситуации, когда количество современных Российских ИТ стандартов составляет менее 5% от числа международных. В год в нашей стране принимается всего 30-40 стандартов в области ИТ. Такие темпы приводят к нарастанию отставания от международного уровня.

Необходимо отметить, что в РФ гораздо лучше обстоит дело с разработкой стандартов защиты информации, поскольку совершенно очевидно, что это напрямую связано с вопросами национальной безопасности.

2.2.3 Барьеры интероперабельности в ВС

Необходимо также отметить, что среди барьеров к достижению интероперабельности в ИС военного назначения дополняются барьеры, создаваемые средствами информационного противодействия, в том числе кибератаки и средства радиоэлектронной борьбы. Совместное рассмотрение проблемы интероперабельности и проблемы информационного противоборства – отдельная тема для исследования [А. А. Башлыкова, А. Я. Олейников «Интероперабельность и информационное противоборство в военной сфере». URL: http://jre.cplire.ru/jre/dec16/14/text.pdf].

Итак, можно сделать вывод, что решение проблемы интероперабельности для ВС РФ для поддержания паритета в условиях СЦВ - крайне актуальная тема и представляет собой сложный комплекс научно-методических и организационно-технических задач.

Отдавая себе отчет в том, что для решения проблемы интероперабельности в ВС РФ требуются большие квалифицированные коллективы и весьма значительные ресурсы, авторы тем не менее делают попытку применить разработанный ими единый подход к решению этой проблемы.

3 Применение единого подхода к обеспечению интероперабельности в ВС РФ

3.1 Этап 1. Основные положения Концепции обеспечения интероперабельности в ВС РФ

Прежде всего, следует принять определение понятия «Интероперабельность». Предлагается принять следующее определение «Способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена (ГОСТ Р 55062-2012). Это определение согласуется с определением, приведенном в международном стандарте ISO/IEC/IEEE 24765:2010(E) Systems and software engineering — Vocabulary [48]. Проблема интероперабельности в ВС РФ должна решаться на основе использования ИКТ-стандартов.

Концепция обеспечения интероперабельности в ВС РФ непосредственно следует из Военной доктрины РФ (в редакции 2015 г.) [25], того положения, что ведение боевых действий, должно вестись на основе концепции СЦВ. Концепция СЦВ предусматривает увеличение боевой мощи группировки объединённых сил за счет образования единого информационного пространства, объединяющего источники информации (разведки), органы управления и средства поражения (подавления), и доведение до всех участников операций достоверной и полной информации об обстановке в реальном времени. Концепция

предполагает перевод преимуществ, присущих отдельным инфокоммуникационным технологиям в конкурентное преимущество за счет объединения в устойчивую сеть информационно достаточно хорошо обеспеченных, географически рассредоточенных сил.

ЕИП ВС РФ должно охватывать:

- все функциональные компоненты (разведка, командование, средства поражения);
- все уровни управления;
- все виды и рода войск;

Уровни управления включают, как известно [49]:

- стратегический уровень;
- оперативный уровень;
- тактический уровень;

На сегодня во главе управления ВС РФ находится Национальный центр управления обороной Российской Федерации (НЦУО РФ), созданный в 2014 г. в целях совершенствования системы централизованного управления военной организацией государства и экономикой страны при решении вопросов подготовки к вооружённой защите страны [50] (см. рисунок 7).

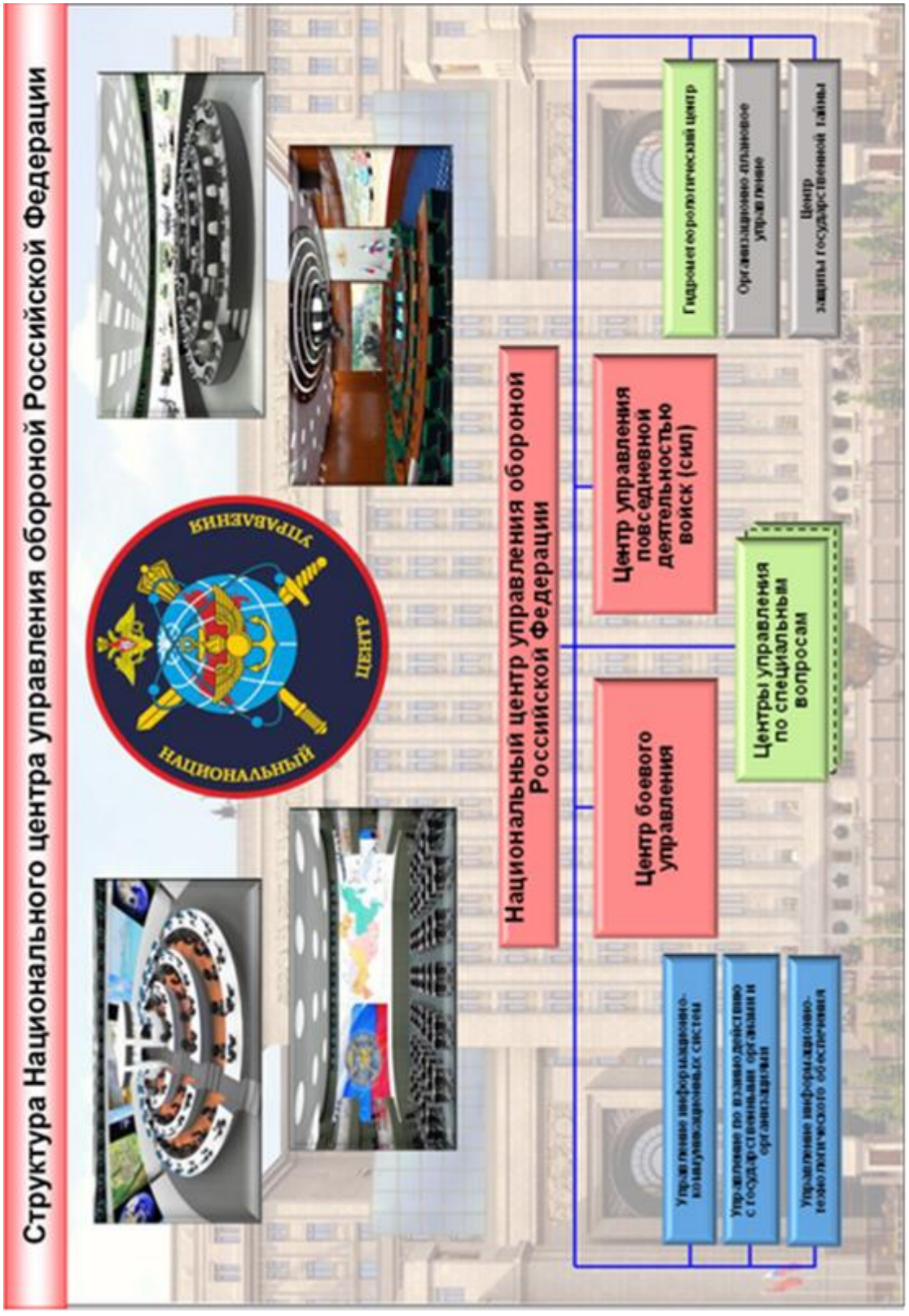


Рисунок 7 — Структура национального центра управления обороной РФ

Под управлением НЦУО РФ находятся центры управления и организации взаимодействия, соответствующие более низким уровням (см. рисунок 8).

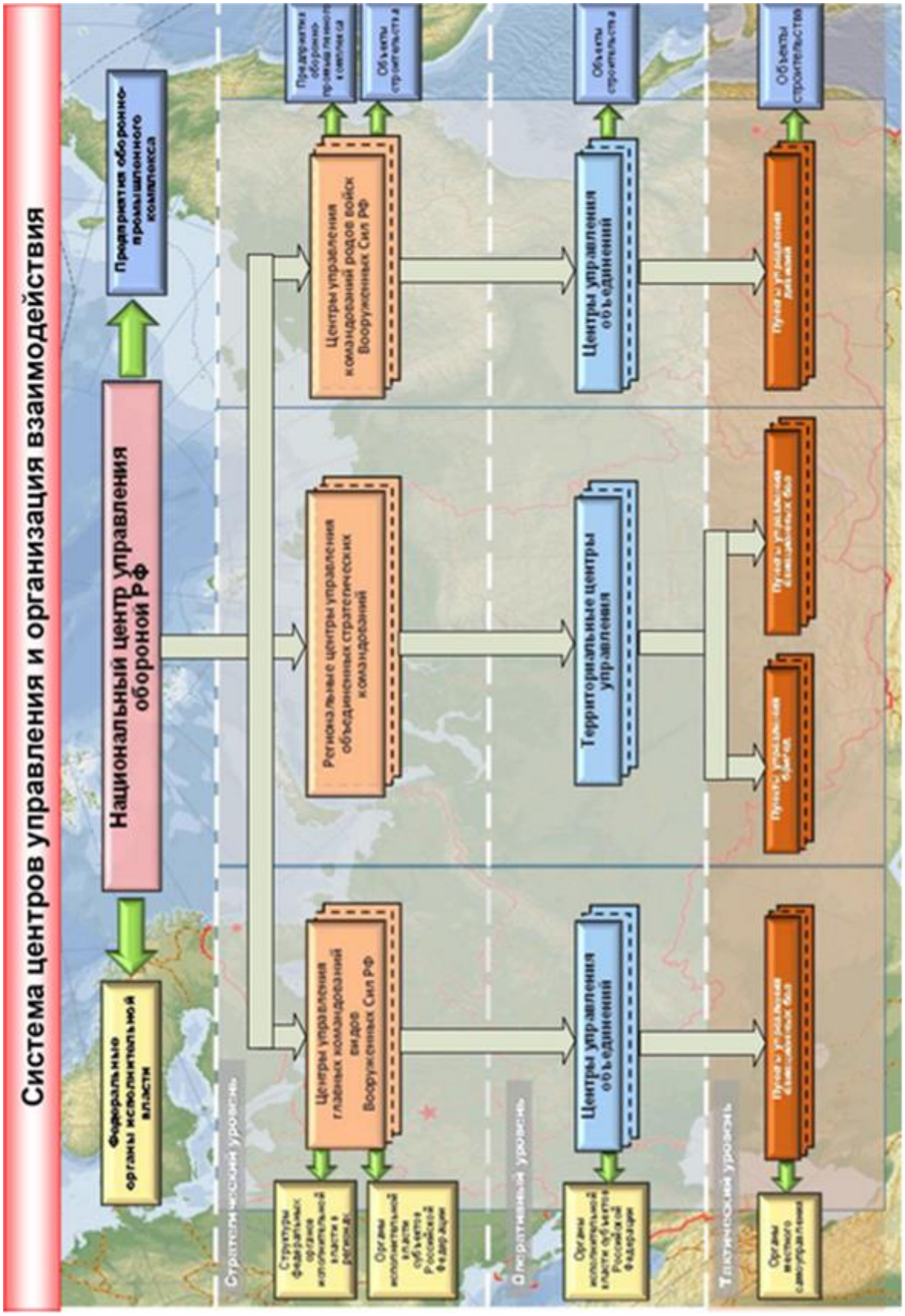


Рисунок 8 — Система центров управления и организация взаимодействия

Остановимся на тактическом уровне управления ВС РФ.

Сегодня тактическому уровню в результате реформы ВС соответствует «бригада», в которую входят батальоны, роты, взводы, отделения [51] (см. рисунок 9).

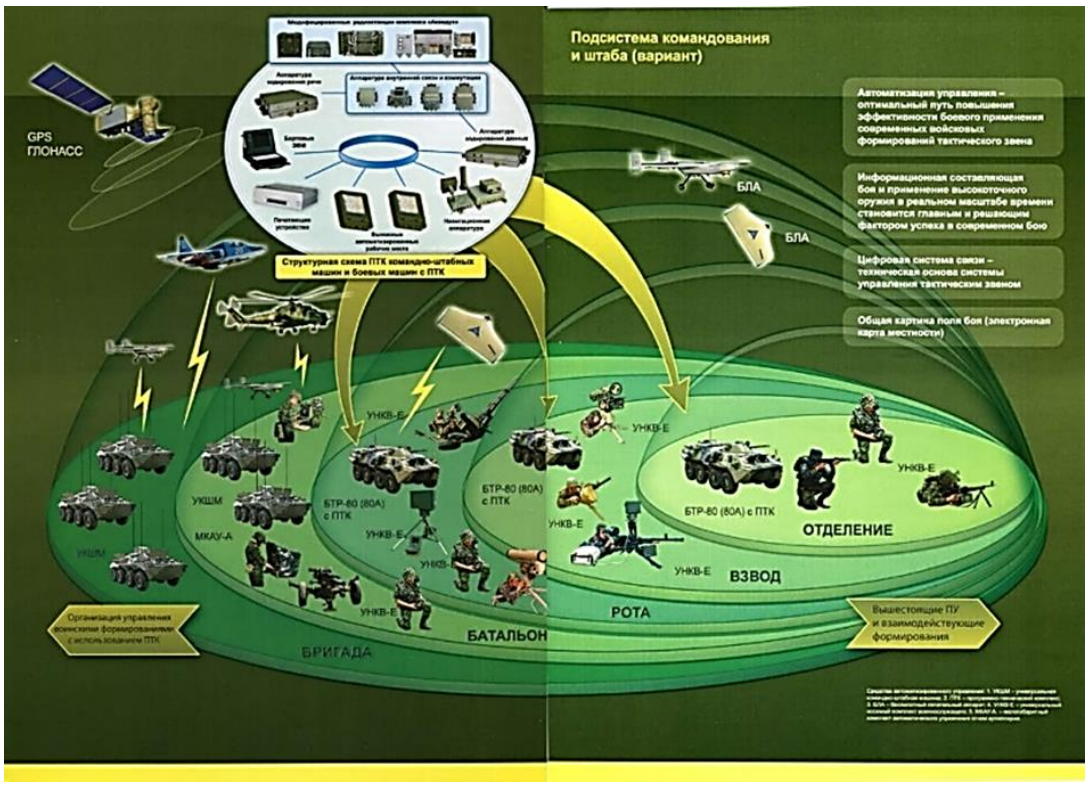


Рисунок 9 — Бригада как современная основа тактического уровня

Нижним звеном тактического уровня выступает рядовой, который как уже говорилось выше, в рамках концепции СЦВ войны называется «солдат будущего», который в отличие от нынешнего традиционного рядового «очень хорошо информирован», т.е. имеет доступ к сети Интернет (см. рисунок 10) [52].

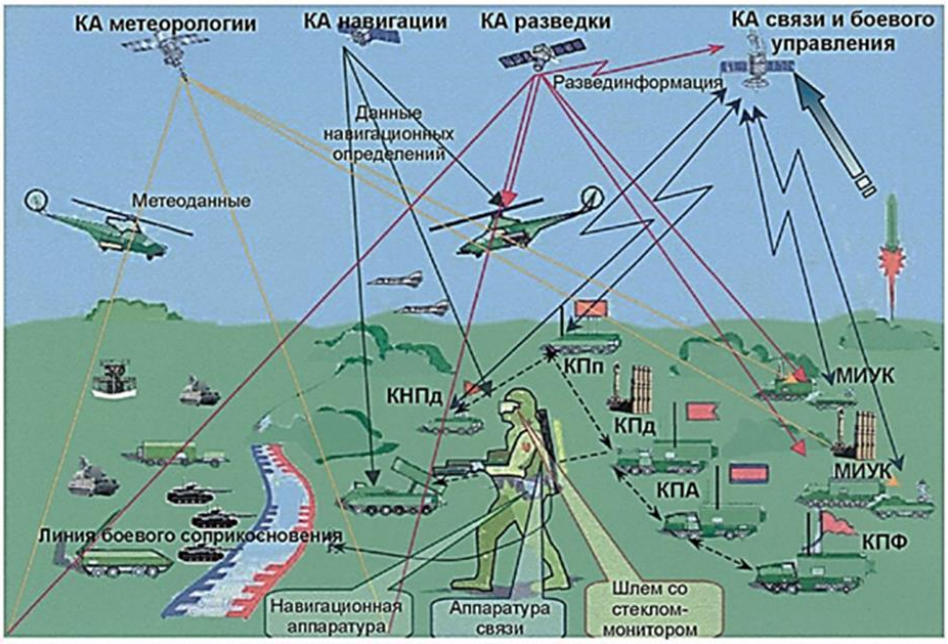
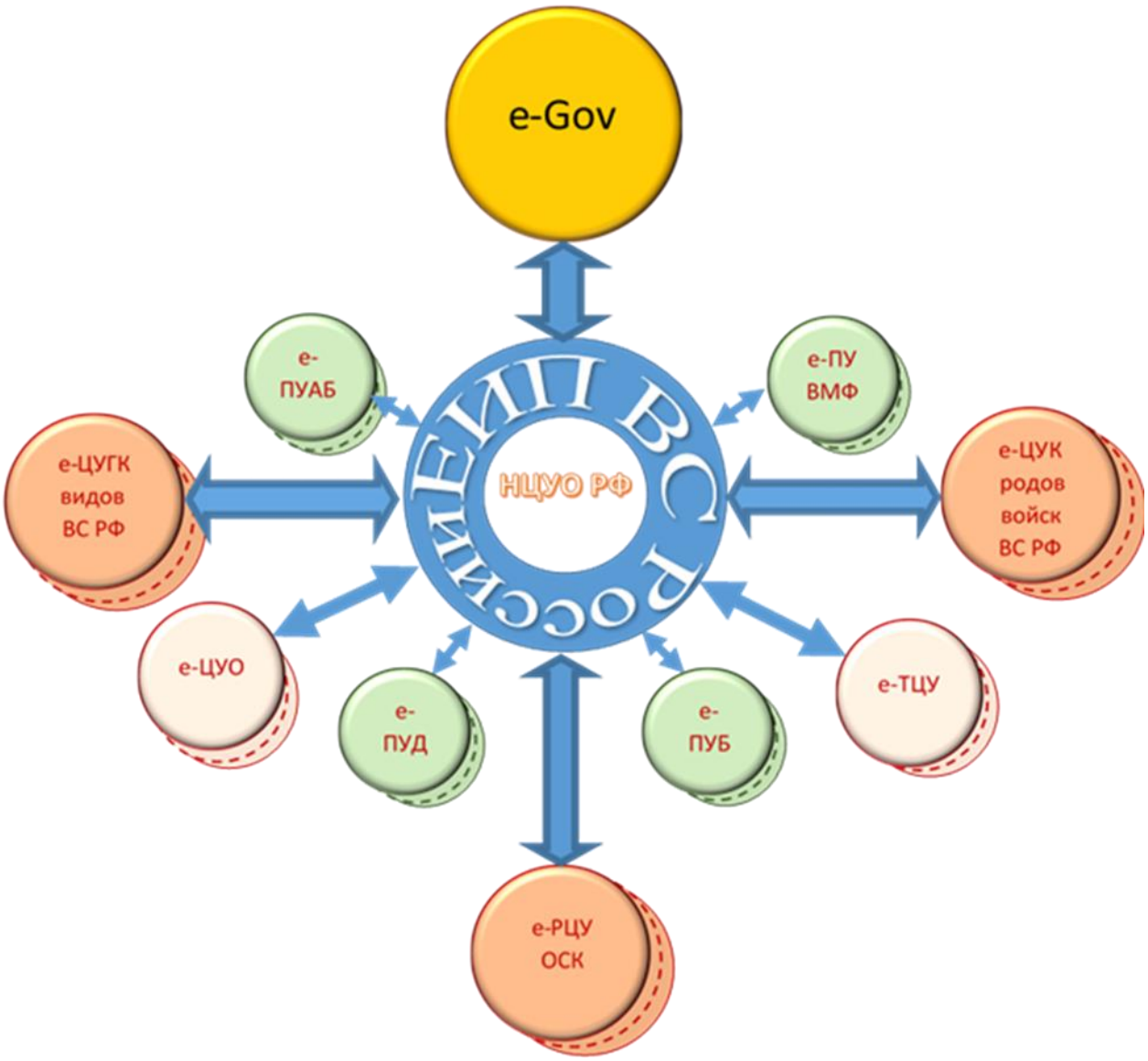


Рисунок 10 — Солдат будущего

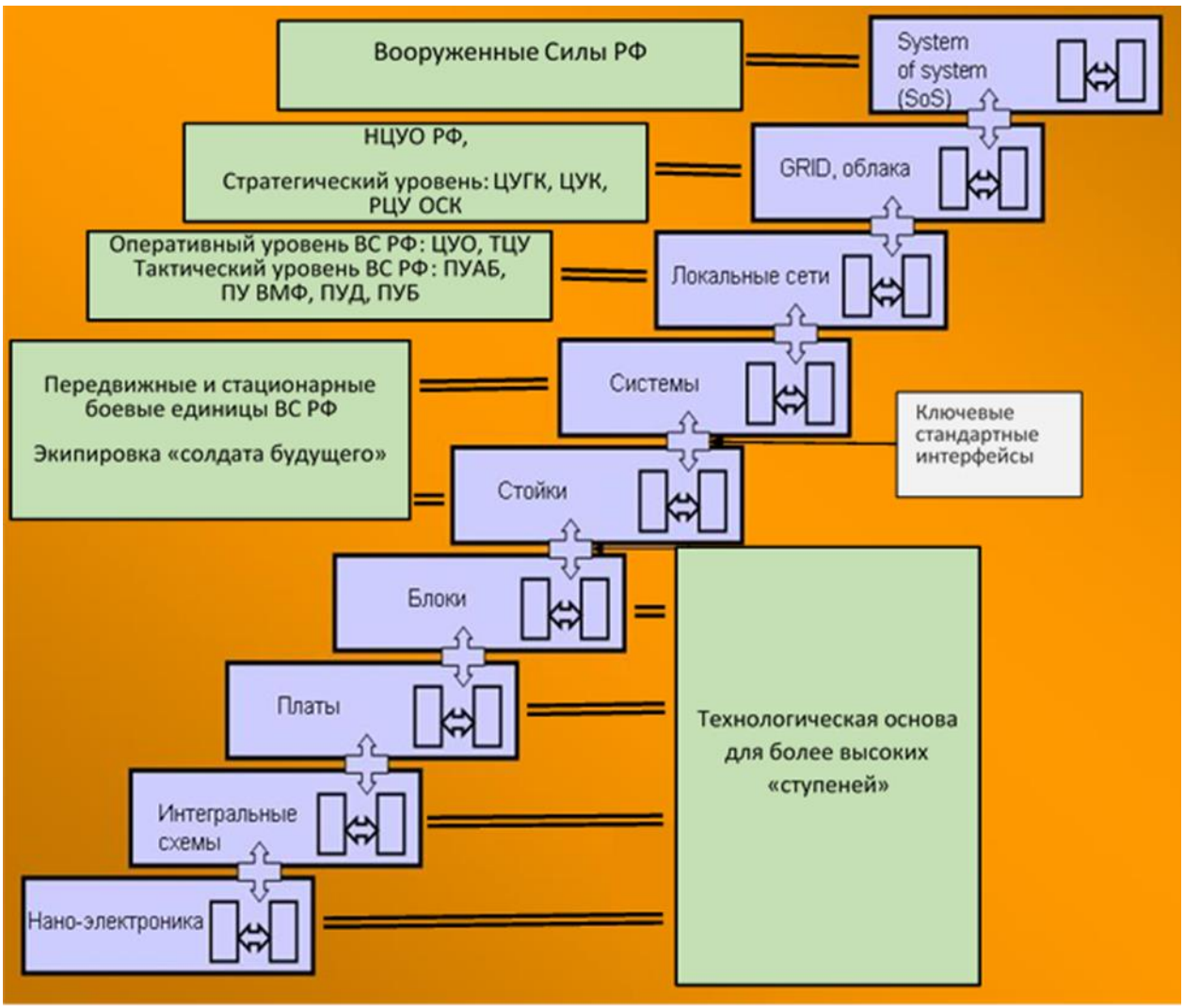
В условиях СЦВ Единое информационное пространство ВС РФ заведомо представляет собой сугубо гетерогенную среду, содержащую разнородные платформы, в которой возникает проблема интероперабельности (см. рисунок 11). При этом осуществляется переход от «технической» интероперабельности к «семантической».



НЦУО РФ – Национальный центр управления обороной РФ; ЦУГК – центры управления главных командований видов ВС РФ; ЦУК – центры управления командований родов войск ВС РФ; РЦУ ОСК – региональные центры управления объединенных стратегических командований; ЦУО – центры управления объединений; ТЦУ – территориальные центры управления; ПУАБ – пункты управления авиационных баз; ПУ ВМФ – пункты управления ВМФ; ПУБ – пункты управления бригад; ПУД – пункты управления дивизий.

Рисунок 11 — Компоненты Единого информационного пространства ВС РФ

ВС РФ относятся к классу «система систем», впитала в себя все нижележащие системы (см. рисунок 12).



НЦУО РФ – Национальный центр управления обороной РФ; **ЦУГК** – центры управления главных командований видов ВС РФ; **ЦУК** – центры управления командований родов войск ВС РФ; **РЦУ ОСК** – региональные центры управления объединенных стратегических командований; **ЦУО** – центры управления объединений; **ТЦУ** – территориальные центры управления; **ПУАБ** – пункты управления авиационных баз; **ПУ ВМФ** – пункты управления ВМФ; **ПУБ** – пункты управления бригад; **ПУД** – пункты управления дивизий

Рисунок 12 — Иерархия ИС военного назначения

Следует различать «внутреннюю» интероперабельность, которая должна существовать, например, внутри одного рода войск и «внешнюю» интероперабельность, которая должна существовать между разнородными компонентами.

Интероперабельность является не абсолютной величиной, а относительной и имеются методы ее измерения [53, 54]. Чем выше уровень интероперабельности, тем в условиях СЦВ выше превосходство над противником.

Перспективные ИС военного назначения для обеспечения интероперабельности должны строиться не как монолитные системы, а на основе программно-аппаратных модулей со стандартными интерфейсами, т.н. Commercial Of the Shelf’s products [55].

3.2 Этап 2. Архитектура Единого информационного пространства ВС РФ

В соответствии с изложенной в п. 3.1 Концепцией, Единое информационное пространство ВС РФ (ЕИП ВС РФ) имеет архитектуру с тремя размерностями (см. рисунок 13).

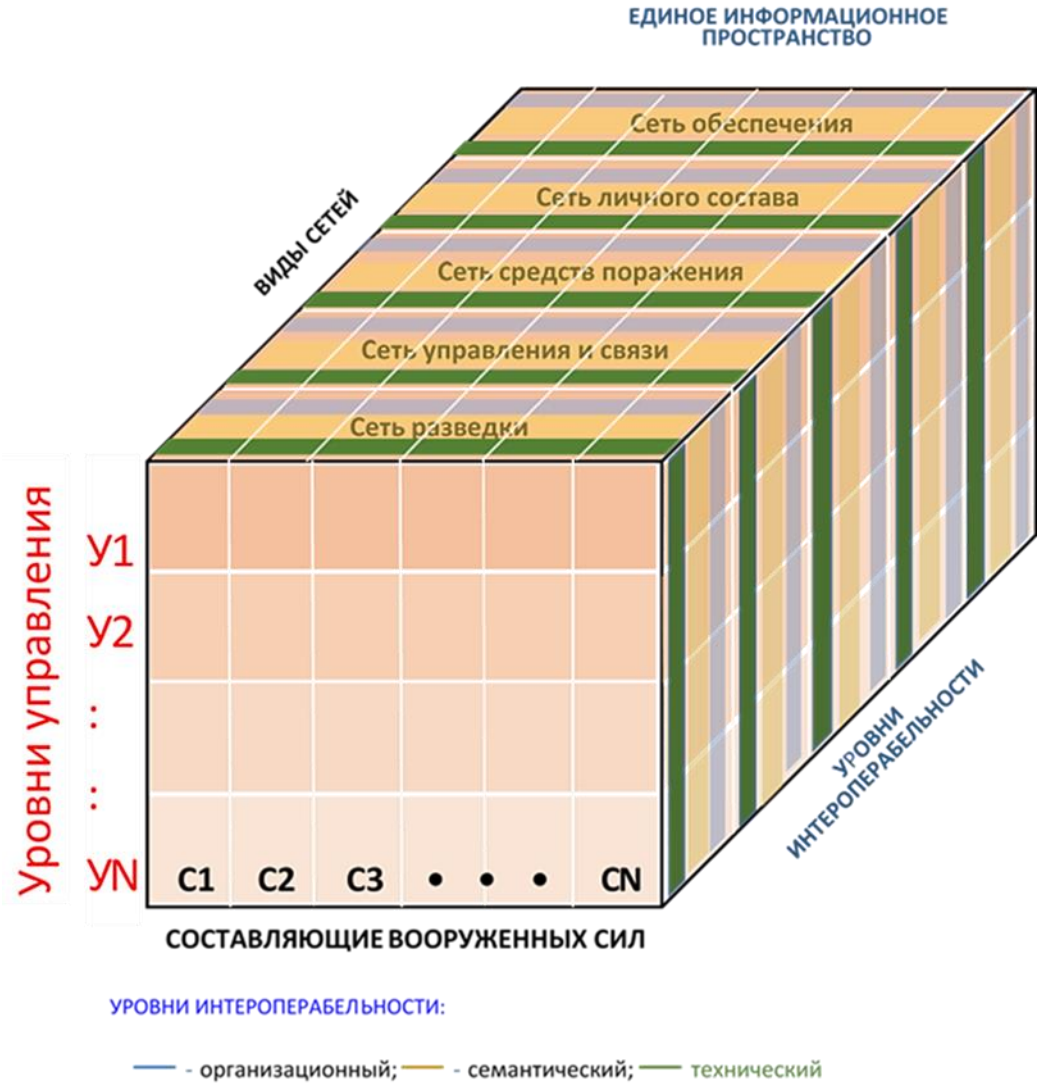


Рис. 13. Архитектура Единого информационного пространства ВС РФ

По горизонтальной оси отложены составляющие ВС РФ (виды и рода войск),

По вертикальной оси – уровни управления (от главнокомандующего до командира нижнего тактического звена)). (См. рисунок 8).

По третьей оси – функциональный разрез: сеть разведки, сеть управления и связи, сеть поражения, а также сеть личного состава и сеть обеспечения [16].

В соответствии с концепцией СЦВ, каждый компонент (ячейка, узел) этого информационного пространства должен обладать свойством интероперабельности по отношению к любому другому компоненту (ячейке, узлу) информационного пространства. Так утверждается, что танк «Армата» имеет интероперабельный программно-аппаратный комплекс, т.е. комплекс, обладающий необходимыми интерфейсами [56].

3.3 Этап 3. Модель интероперабельности ВС РФ

Следующим этапом единого подхода, как следует из рисунка 3, выступает построение проблемно-ориентированной модели интероперабельности, представляющей развитие эталонной модели интероперабельности, зафиксированной в ГОСТ Р 5506-2012. Мы предлагаем следующую модель (см. рисунок 14).

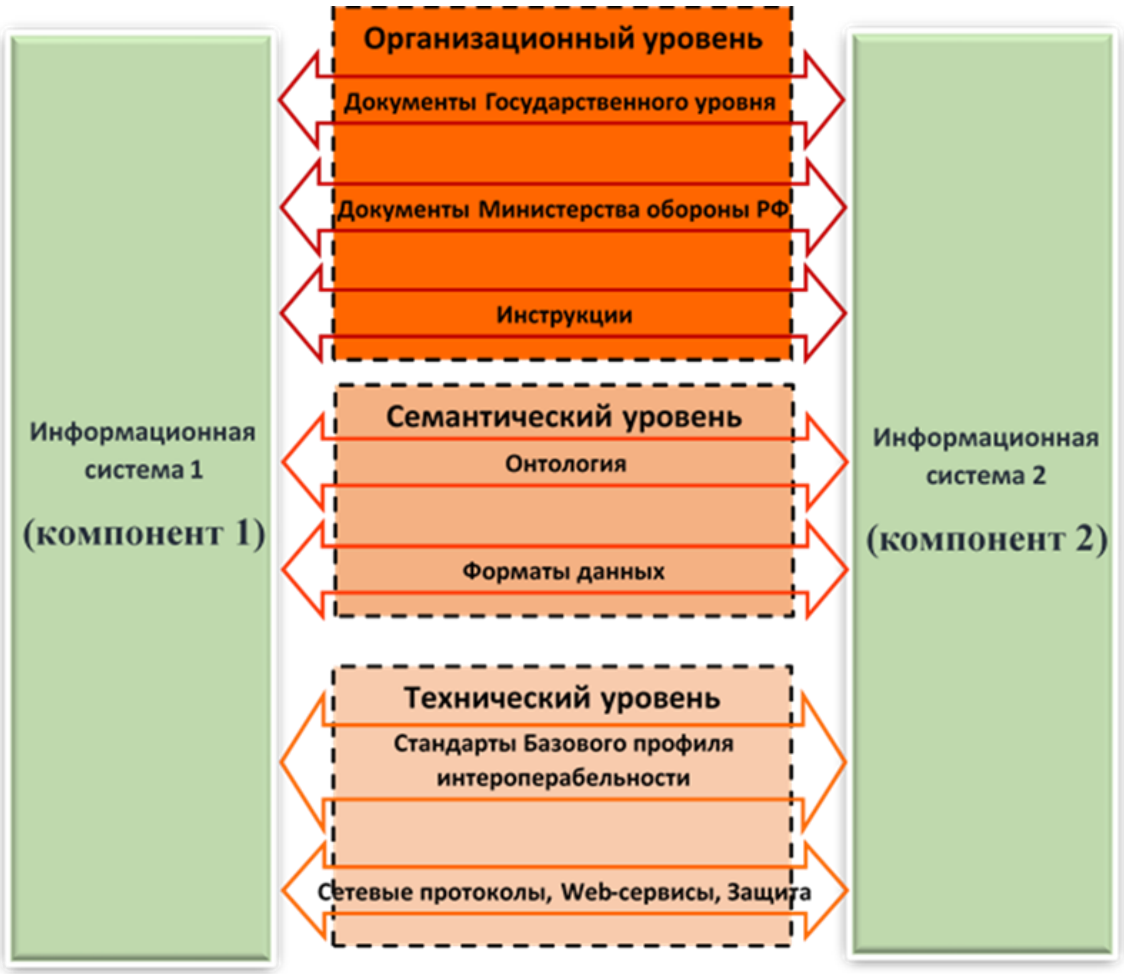


Рисунок 14 — Модель интероперабельности для информационных систем военного назначения

Верхний, организационный уровень «расщепляется» на три подуровня. Верхний подуровень должны составить документы государственного уровня, следующий подуровень – документы Минобороны РФ, такие как ВД РФ, и нижний подуровень должны составить документы уровня приказов, директив, приказаний, указаний, распоряжений, постановлений, положений, уставов, руководств, инструкций, правил и др. [57].

Более подробно об уровнях интероперабельности см. в приложении Д.

3.4 Этап 4. Профиль интероперабельности ВС РФ

Как уже неоднократно подчеркивалось выше, в условиях СЦВ информационная система ВС РФ представляет собой сверхсложную систему (класса System of Systems), включающую большое количество подсистем, вплоть до нано-систем (см. рисунок 12). Это означает, что, по большому счету, обойтись одним профилем очень затруднительно, и должна существовать некая иерархия профилей, получившая название таксономия. Методологический базис по таксономии профилей описан в [35]. При этом по нашему убеждению и в соответствии с ФЗ «О стандартизации» в профили должны входить в первую

очередь национальные стандарты (ГОСТ Р). Однако, в первом приближении, как это делается в данном разделе, поскольку в Военной доктрине РФ рекомендуется ориентация на зарубежные стандарты, можно предложить минимальный профиль, включающий на нижних уровнях стандарты из профилей, разработанных НАТО [58]. Поэтому на рисунке 15 в предлагаемом минимальном профиле ВС РФ представлены на нижних уровнях профили с оригинальными названиями НАТО.

Семантический уровень «расщепляется на два подуровня. Верхний содержит онтологию (термины, которые должны быть общими для всех участников). Нижний подуровень содержит форматы обмениваемых данных.

Что касается профиля организационного уровня, то см. п. 3.3.

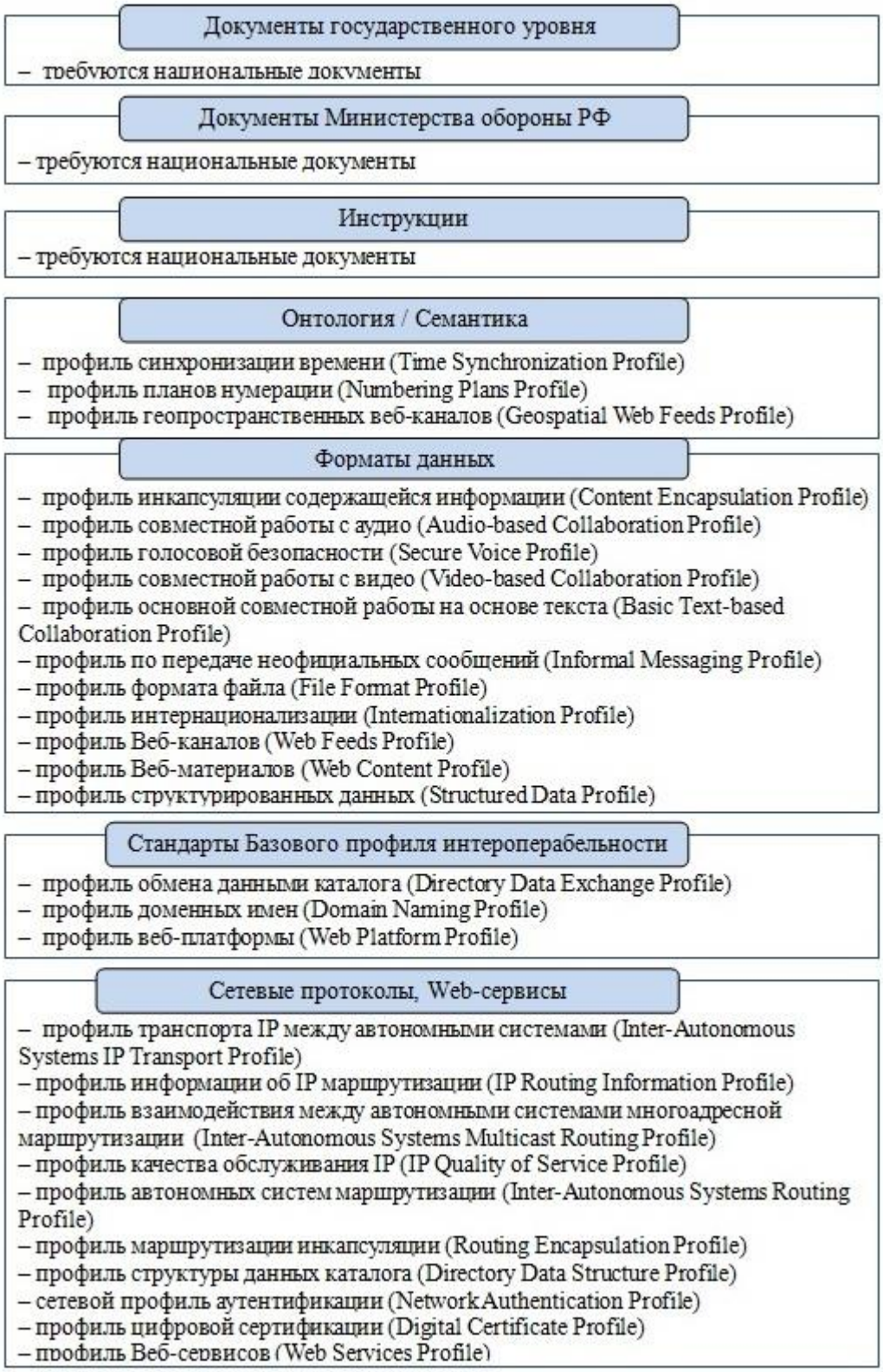


Рисунок 15 — «Минимальный» профиль ВС РФ

В приложении Д приведен профиль интероперабельности ВС РФ , включенный в проект национального стандарта.

3.5 Остальные этапы единого подхода

Как уже говорилось в разделе 1 настоящего отчета, к основным этапам единого подхода (см. рисунок 3) относятся этапы 1-5, а к вспомогательным – этапы 6-9.

Этап 5 - Программно-аппаратная реализация.

Программно-аппаратная реализация всех компонентов ЕИП ВС РФ должна осуществляться в соответствии с профилем, приведенным на рисунке 15.

Этап 6 - Аттестационное тестирование.

Должна быть создана отраслевая система сертификации, в рамках которой должно проводится аттестационное тестирование программно-аппаратных комплексов и их компонентов на соответствие стандартам, входящим в профиль. Общие принципы аттестационного тестирования хорошо известны (см. например [1] раздел 4.2.4).

Этап 7 - Дорожная карта разработки стандартов.

В качестве первоочередного военного стандарта необходимо разработать аналог ГОСТ Р 55062-2012. Далее на основе стандартов, приведенных на рисунке 15, должны быть в определенной очередности (снизу вверх) разработаны национальные стандарты.

Этап 8 - Разработка национальных стандартов.

Разработка национальных стандартов должна вестись в порядке, установленном ФЗ «О стандартизации» и другими нормативными документами за счет средств МО РФ и корпораций, разрабатывающих и производящих программно-аппаратные комплексы и их компоненты в интересах МО РФ.

Этап 9 – Терминология.

Разработка документа, содержащего общие для всех заинтересованных сторон термины – глоссария, крайне важно для общего взаимопонимания всех участников. В качестве прототипа можно использовать документ [31].

ЗАКЛЮЧЕНИЕ

На основании изложенного можно сделать следующие выводы и предложения:

1.Анализ показывает, что проблема интероперабельности крайне актуальна для ВС. Её актуальность прямо следует из концепции сетецентрической войны, которая принята в НАТО, США и других странах и реально принята в нашей стране, что отражено в Военной доктрине РФ.

2.В настоящее время в РФ и ВС РФ отсутствуют необходимые документы, направленные на решение проблемы интероперабельности. Ориентация сделана на использование зарубежных, а не национальных стандартов, что несет угрозу национальной безопасности

3. Предложена адаптация единого подхода к обеспечению интероперабельности для информационных систем широкого класса к системам военного назначения, а практически к их объединению в Единое информационной пространство Вооруженных Сил Российской Федерации

4. На основании разработанного авторами ГОСТ Р 55062-12 разработан проект ГОСТ Р «Информационные технологии. Военное дело. Интероперабельность. Основные положения»

5. Выполненную работу следует рассматривать как первое приближение к решению проблемы нтероперабельности в Вооруженных Силах Российской Федерации.

6. Для дальнейшего развития работ, успешного противостояния военной угрозе уровень интероперабельности ВС РФ должен соответствовать уровню интероперабельности ВС НАТО и входящих в него стран, поэтому должны быть приняты соответствующие нормативные документы концептуального и реализационного уровня.

7. Необходимо срочно сконцентрировать научно-технические ресурсы Минобороны и провести цикл целенаправленных работ по решению проблемы интероперабельности в ВС РФ. С этой целью предлагается:

- от имени Национального центра управления обороной РФ выйти с предложениями в соответствующие инстанции с тем, чтобы придать проблеме интероперабельности необходимое значение.

- предложения должны включать создание рабочего органа (комитета, группы, комиссии), в который должны войти представители Минобороны, Минсвязи, организаций, ведущих разработки вооружения, Росстандарта, институтов РАН и др. заинтересованных ведомств и организаций.

- рабочий орган должен определить техническую политику по решению проблемы интероперабельности в РФ и ВС РФ.

- действия Рабочего органа должны быть предельно открыты для общественности.

- форсировать за счет средств, выделяемых на оборону, превращение необходимых для обеспечения интероперабельности международных стандартов в национальные нормативные документы, установив их очерёдность путем создания соответствующего плана-графика ("Дорожной карты"). При этом целесообразно использовать опыт организаций РАН, в том числе авторов настоящей работы.

- в качестве первоочередного шага на базе ГОСТ Р 55062-2012 разработать военный стандарт ГОСТ РВ с ориентировочным названием «Военное дело. Интеропребельность. Общие положения».

- организовать в военных учебных заведениях, а также в ВУЗах, таких как МГТУ им. Баумана, МИРЭА, СГАУ и др. подготовку специалистов по ИКТ-стандартизации и интероперабельности с привлечением специалистов из институтов РАН.

Список использованных источников

1. Технология открытых систем. Под редакцией А.Я. Олейникова . – М.: Янус-К, 2004. - 288 с., илл. Доступ с сайта BookFi. URL: http://bookfi.net/book/505455 (дата обращения: 27.09.2016).
2. Гуляев Ю.В., Журавлев Е.Е., Олейников А.Я. Методология стандартизации для обеспечения интероперабельности информационных систем широкого класса. Аналитический обзор. // Журнал радиоэлектроники: электронный журнал. 2012. N3. URL: (http://jre.cplire.ru/mac/mar12/2/text.pdf) (дата обращения: 27.09.2016).
3. ГОСТ Р 55062-2012 Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения [Электронный ресурс]: профессиональные справочные системы «Техэксперт». / Консорциум Кодекс. URL: (http://www.cntd.ru/assets/files/upload/050314/55062-2012.pdf) (дата обращения: 27.09.2016).
4. Ю.В. Бородакий, Ю.Г. Лободинский. Информационные технологии в военном деле (основы теории и практического применения). - М.: Горячая линия-Телеком, 2008. - 392 с. [Электронный ресурс]: электронная библиотека «Razym.ru». URL: http://www.razym.ru/tehnicheskaya/electronika/308226-borodakiy-yuv-lobodinskiy-yug-informacionnye-tehnologii-v-voennom-dele-osnovy-teorii-i-prakticheskogo-primeneniya.html (дата обращения: 27.09.2016).
5. Олейников А.Я., Е.И. Разинкин. Профиль интероперабельности в области электронной коммерции.– М.: РАН, Информационные технологии и вычислительные системы, 2013. №4. – С. 74-79
6. Журавлев Е.Е., Иванов С.В., Каменщиков А.А., Олейников А.Я., Разинкин Е.И., Рубан К.А. Интероперабельность в облачных вычислениях. // Журнал радиоэлектроники: электронный журнал. 2013. N9. URL: http://jre.cplire.ru/jre/sep13/4/text.pdf (дата обращения: 12.08.2016).
7. Журавлёв Е.Е., Иванов С.В., Олейников А.Я. Модель интероперабельности облачных вычислений. // Журнал радиоэлектроники: электронный журнал. 2013, N9. URL: http://jre.cplire.ru/jre/dec13/12/text.pdf (дата обращения: 27.09.2016).
8. ГОСТ Р ИСО 11354-1-2012 Усовершенствованные автоматизированные технологии и их применение. Требования к установлению интероперабельности процессов промышленных предприятий. Часть 1. Основа интероперабельности предприятий.

[Электронный ресурс]: электронный фонд правовой и нормативно-технической документации. / Консорциум Кодекс. URL: http://docs.cntd.ru/document/1200102044 (дата обращения: 27.09.2016).

9. Взаимодействие войск это: // [Электронный ресурс]: словари и энциклопедии на Академике, Большая советская энциклопедия. URL: http://dic.academic.ru/dic.nsf/bse/74157/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BE%D0%B4%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D0%B8%D0%B5 (дата обращения: 27.09.2016).
10. Слипченко В.И. Войны шестого поколения. Оружие и военное искусство будущего. – М.: Вече, 2002. - 384 с. С аннотацией можно ознакомиться URL: http://www.chtivo.ru/book/318655/ (дата обращения: 27.09.2016).
11. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию. М.: Евразийское движение, 2011, 130 с. [Электронный ресурс]: geopolitica.ru. URL: http://www.geopolitica.ru/sites/default/files/ncw.pdf (дата обращения: 27.09.2016).
12. «Сетецентрическая война», так ли она хороша на деле. [Электронный ресурс]: Военное обозрение. 2010, 25 декабря. URL: https://topwar.ru/2839-setecentricheskaya-vojna-tak-li-ona-xorosha-na-dele.html (дата обращения: 27.09.2016).
13. И.М. Попов. "Сетецентрическая война": Готова ли к ней Россия? // [сайт «Военная история и футурология»] / сост. и ред. И.М. Попов. URL: http://www.milresource.ru/NCW.html (дата обращения: 27.09.2016).
14. The National Military Strategy of the United States of America 2015. *The United States Military's Contribution To National Security.* 2015, June, 24 p. Available at http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf
15. В. М. Буренок, А. Ю. Кравченко, С. С. Смирнов. Курс – на сетецентрическую систему вооружения. // Воздушно-космическая оборона: электронный журнал. 2009, N5. URL: http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya (дата обращения: 27.09.2016).
16. А. Е. Кондратьев. Информатизация вооруженной борьбы как революция в военном деле. // [сайт «World forecasts» (мирпрогнозов.рф)]: будущее сетецентрических войн. URL: http://www.мирпрогнозов.рф/prognosis/politics/buduschee-setetsentricheskih-voyn/it (дата обращения: 29.09.2016).
17. В. В. Барвиненко. Взаимодействия как не было, так и нет. // Воздушно-космическая оборона: электронный журнал. 2013, N4. URL: http://www.vko.ru/operativnoe-iskusstvo/vzaimodeystviya-kak-ne-bylo-tak-i-net (дата обращения: 29.09.2016).

18. А. Н. Тезиков, О. Д. Мирошниченко. АСУ ВКО: требуется новая система взглядов. // Воздушно-космическая оборона: электронный журнал. 2012, N2. URL: http://wwww.vko.ru/node/232 (дата обращения: 29.09.2016).
19. Копылов И. А. Современные модели Вооружённых Сил: мировой опыт и российская специфика формирования. // [сайт «Человек и наука»]: политические науки. URL: http://cheloveknauka.com/sovremennye-modeli-vooruzhyonnyh-sil-mirovoy-opyt-i-rossiyskaya-spetsifika-formirovaniya (дата обращения: 29.09.2016).
20. Ю.В. Бородакий, Ю.Г. Лободинский. К проблеме обеспечения интероперабельности. - М.: РАН, Информационные технологии и вычислительные системы, 2009.- №5. – С. 16-24. URL: http://www.jitcs.ru/images/stories/2009/05/16_24.pdf (дата обращения: 29.09.2016).
21. С.А. Волков. Средство ведения военных действий (1). // Воздушно-космическая оборона: электронный журнал. 2009, N1. URL: http://wwww.vko.ru/koncepcii/sredstvo-vedeniya-voennyh-deystviy-1 (дата обращения: 29.09.2016).
22. С.А. Волков. Средство ведения военных действий (2). // Воздушно-космическая оборона: электронный журнал. 2009, N2. URL: http://wwww.vko.ru/koncepcii/sredstvo-vedeniya-voennyh-deystviy-1 (дата обращения: 29.09.2016).
23. Чумичкин А.А. Обоснование путей создания эталонной модели данных единого информационного пространства ВС РФ. // Вооружение и экономика, 2009, №1 (5). – С. 35-42. URL: http://www.viek.ru/5/35-42.pdf (дата обращения: 29.09.2016).
24. Забузов О.Н. Военно-информационная политика: модель и особенности ее реализации Минобороны России // Вестник Тамбовского государственного технического университета. – Тамбов. – 2006. – Том 12. – № 4Б. – С. 1223–1227.
25. Военная доктрина Российской Федерации. [сайт Министерства иностранных дел]: внешняя политика, основополагающие документы. URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/976907 (дата обращения: 29.09.2016).
26. Шишкина Н.И. Стратегические документы в военной сфере США и России: сравнение. [сайт Центра Сулакшина (Центр научной политической мысли и идеологии)]: внешняя политика. URL: http://rusrand.ru/events/strategicheskie-dokumenty-v-voennoj-sfere-ssha-i-rossii-sravnenie (дата обращения: 29.09.2016).
27. Армия РФ испытала в Сирии высокоскоростной военный интернет. [сайт ТАСС]: армия и ОПК. 7 апреля 2016 г. URL: http://tass.ru/armiya-i-opk/3183694 (дата обращения: 29.09.2016).

28. "Армата" готова к сетецентрической войне. [сайт «Politforums.net»]: вооруженные силы. 27.04.2015 г. URL: http://www.politforums.net/rmo/1430142557.html (дата обращения: 29.09.2016).
29. Национальный центр управления обороной Российской Федерации. [сайт Минобороны России]: структура. URL: http://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11206@morfOrgEduc (дата обращения: 29.09.2016).
30. Interoperability for joint operations. Available at. NATO *Public Diplomacy Division.* 2006, 12 p. http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120116_interoperability-en.pdf
31. Department of Defense Dictionary of Military and Associated Terms. *Joint Publication 1-02.* November 2010 (As Amended Through 15 February 2016) - 482 p. Available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
32. NATO Architecture Framework v4.0 Documentation (draft). *NATO, OTAN* . Available at http://nafdocs.org/
33. The DoDAF Architecture Framework Version 2.02. *Chief Information Officer. U.S. Department of Defense* Available at http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx
34. E. Morris, L. Levine, C. Meyers, P. Place, D. Plakosh. System of Systems Interoperability (SOSI): *Final Report. CMU/SEI-2004-TR-004*, ESC-TR-2004-004. – 67 p. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/a455619.pdf
35. NATO Interoperability Standards and Profiles. *NISP in PDF. The following documents are PDF versions of the NISP*. Copyright © NATO - OTAN 1998-2016. Available at https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/PDFcoverdoc.html
36. SUBJECT: Information Technology Standards in the DoD. *Department of Defense INSTRUCTION DoDI 8310.01*, February 2, 2015. – 27 p. Available at http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf
37. Testing/interoperability certification. *Defense Information Systems*. Agency Available at http://www.disa.mil/Mission-Support/Testing/Testing-Interoperability-Certification
38. SUBJECT: Interoperability of Information Technology (IT), Including National Security Systems (NSS). *Department of Defense INSTRUCTION DoDI 8330.01*. May 21, 2014. – 43 p. Available at http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf

39. Unified Architecture Framework (UAF) for System of Systems Modeling. *Matthew Hause PTC Engineering Fellow*. April 2016. – 30 p. Available at http://www.acq.osd.mil/se/webinars/2016-04-12-SoSECIE-Hause-brief.pdf

40. Гуляев Ю.В., Журавлев Е.Е., Козлов В.А. Технология открытых систем как технология двойного применения. // Доклад на 1-й межрегиональной конференции-выставки "Информационные технологии двойного применения в системах управления", Ярославль, 1998. Тезисы докладов, с. 11-12.

41. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (документ по состоянию на август 2014 г.). [сайт «Правовая Россия]. URL: http://lawru.info/dok/1995/11/23/n453820.htm (дата обращения: 03.10.2016).

42. Доктрина информационной безопасности Российской Федерации (Указ президента РФ №646 от 5 декабря 2016 г.) [Электронный фонд правовой и научно-технической документации] URL: http://docs.cntd.ru/document/420384668 (дата обращения 10.12.2016).

43. European interoperability framework for pan-european eGOVERNMENT services. Version 1.0. / European Communities, 2004, Printed in Belgium, - 25 p. IDABC EIF. Available at http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529552.pdf?id=19529.

44. Федеральный закон от 29 июня 2015 г. N 162-ФЗ "О стандартизации в Российской Федерации". / - М: Российская газета - Федеральный выпуск №6715 (144), 3 июля 2015 г. URL: http://rg.ru/2015/07/03/standart-dok.html (дата обращения: 03.10.2016).

45. Государственная программа Российской Федерации "Информационное общество (2011 - 2020 годы)" (утв. постановлением Правительства РФ от 15 апреля 2014 г. № 313). [информационно-правовой портал ГАРАНТ.РУ]: документы ленты ПРАЙМ. 12 мая 2014 г. URL: http://www.garant.ru/products/ipo/prime/doc/70544220/#ixzz4M70diTCg (дата обращения: 03.10.2016).

46. А.А. Куприянов. Сетецентрические военные действия и вопросы интероперабельности автоматизированных систем. / Автоматизация процессов управления. -2011, № 3(25). – С. 82-97.

47. Стратегия развития, гармонизации и внедрения на территории Российской Федерации существующих международных политик и стандартов в области информационных технологий и информационной безопасности, а также разработки и продвижения (тиражирования) на международный уровень (в том числе ЕАЭС, СНГ, БРИКС, ШОС, АТЭС и т. д.) разрабатываемых политик и стандартов на 2014-2020 годы, совместно с

планами мероприятий («дорожая карта») и финансирования работ на 2015-2017 годы Российской Федерации. // [сайт]: Стратегия ИТ стандартизации, WWW.ITSTANDARD.RU (TK22@ITSTANDARD.RU).

48. ISO/IEC/IEEE 24765:2010(E) Systems and software engineering — Vocabulary. Ingénierie des systèmes et du logiciel — Vocabulaire./ - INTERNATIONAL STANDARD, 418 p. Available at https://pascal.computer.org/sev_display/24765-2010.pdf
49. Органы управления ВС это: // [Электронный ресурс]: словари и энциклопедии на Академике, Война и мир в терминах и определениях. URL: http://war_peace_terms.academic.ru/530/%D0%9E%D0%A0%D0%93%D0%90%D0%9D%D0%AB_%D0%A3%D0%9F%D0%A0%D0%90%D0%92%D0%9B%D0%95%D0%9D%D0%98%D0%AF_%D0%92%D0%A1 (дата обращения: 03.10.2016).
50. О работе Национального центра управления обороной России. [сайт Ридус]: общество, 01 ноября 2014 г. URL: https://www.ridus.ru/news/170939.html (дата обращения: 03.10.2016).
51. ПТК АСУ ТЗ "Созвездие-2М". [персональная страница]: сост. и ред. А. Хлопотов. URL: http://gurkhan.blogspot.ru/2011/10/2_21.html (дата обращения: 03.10.2016).
52. Меньшиков В.А. Анализ, перспективы развития и повышения эффективности военно-космических средств. / Доклад на военно-научной конференции «Космические войска в системе безопасности государства». 14.12.2010. [социально-просветительский Интернет-портал Труженики космоса]: современные проблемы. URL: http://cosmosinter.ru/art_potential/art_perspective/detail.php?month=04&year=2013&ID=238 (дата обращения: 03.10.2016).
53. Петров А.Б., Стариковская Н.А. Методика сравнительной оценки интероперабельности информационных систем // Информационные технологии и вычислительные системы. Спец. выпуск. Открытые системы. Интероперабельность. – М. ИМВС РАН, 2009. – № 5. – С. 82–90.
54. Батоврин В.К., Королев А.С. Способ количественной оценки интероперабельности // Информационные технологии и вычислительные системы. – 2009. – № 5. – С. 91–95.
55. Commercial off-the-shelf. [the free encyclopedia]. Available at https://en.wikipedia.org/wiki/Commercial_off-the-shelf
56. «Армата» пришла надолго. [сайт Военное образование]: новая бронетехника в системе вооружений, 23 августа 2015. URL: https://topwar.ru/80936-armata-prishla-nadolgo.html (дата обращения: 03.10.2016).

57. Глава 14. Основные виды документов ВС РФ. Виды служебных документов, их краткая характеристика и основные требования к ним. / Курс лекций. Учебная дисциплина «Управление подразделениями в мирное время». Тема № 1 «Основы работы органов военного управления в ходе повседневной деятельности» (ВУС-390400, 441000, 441400, 491100). // Нижегородский государственный университет им. Н.И. Лобачевского, Учебный военный центр. URL: http://www.ivo.unn.ru/upmv/g14.htm (дата обращения: 03.10.2016).
58. The following documents are PDF versions of the NISP. *NISP in PDF* Available at https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/PDFcoverdoc.html

ПРИЛОЖЕНИЕ А

(рекомендуемое)

Зарубежные документы по интероперабельности в ВС

Таблица А.1

N п.п.	Наименование	Дата выпуска	Краткое содержание	Электронный адрес
НАТО				
1	NATO Architecture Framework v4.0 (NAV)	19.06.2013	Описывается проект создания 4-ой версии концепции архитектуры. Представлена модель и Архитектура Naf 4.0, которая включает в себя MODAF v.1.2.004, NAF 3.x и MODEM 1.0	http://nafdocs.org/, http://nafdocs.org/documents/
2	NATO Interoperability Standards and Profiles - Vol3-v8-release	22.08.2014	Документ, в основном описывающий архитектуру взаимодействия членов альянса и содержит перечни необходимых технических стандартов на всех уровнях интероперабельности. Для каждого стандарта выделяется его уровень сервиса и класс. Вводится понятие «NATO Enterprise Information Environment». Используется подход SOA.	https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/pdf/NISP-v8-release.pdf
3	Multilateral interoperability programme Version 3.1.4	16.02.2012	Многосторонняя программа интероперабельности — программа технологического сотрудничества вооружённых сил, созданная на уровне национальных разработчиков информационных систем управления и контроля войсками с	https://mipsite.lsec.dnd.ca/Pages/Default.aspx

			целью достижения интероперабельности национальных систем. Представляет собой консорциум из 29 стран, как входящих, так и не входящих в НАТО.	
США				
4	The National Military Strategy of the United States of America2015	01.06.2015	Национальная военная стратегия США. Эффективность военных действий зависит от оперативности взаимодействия с союзниками. Данный документ дает общие знания о подходе США в данном вопросе.Большое значение придается проблеме интероперабельности и подчеркивается, что стоит задача разработки стандартов интероперабельности нового поколения	http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf
5	Joint Vision 2020 America's Military—Preparing for Tomorrow	30.05.2000	Концепция развития вооружённых сил США с целью полного доминирования к 2020 году на основе СЦВ. Содержит специальный раздел, посвященный интероперабельности, как одной из основ объединенных действий.	http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID521/pdfdocs/2020/jv2020.pdf
6	Department of Defense Architecture Framework v2.02	19.01.2015	Департамент обороны Architecture Framework (DoDAF) является основой архитектуры для Соединенных Штатов Министерства обороны (DoD). Документ обеспечивает визуализацию инфраструктуры для конкретных заинтересованных	http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx

			сторон проблем на основе viewpoints, организованных различными видами. Документ содержит архитектуру, общую модель и классификацию стандартов.	
7	Information Technology Standards in the DoD	02.02.2015	Инструкция Минобороны США №8310.01 по технической политике в области поддержания развития ИТ стандартов,	http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf
8	Department of Defense INSTRUCTION, Interoperability of Information Technology (IT), Including National Security Systems (NSS)	21.05.2014	Инструкция Минобороны США № 8330.01, определяющая стратегию и процесс испытания на совместимость и сертификацию предприятия предоставляющих услуги для Министерства обороны США. Является одной из составных частей документа Department of Defense Architecture Framework v2.02	http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf Дополнительные материалы: http://www.disa.mil/Mission-Support/Testing/Testing-Interoperability-Certification
9	System of Systems Interoperability (SOSI):	Апрель 2004	Заключительный технический отчет Института программной инженерии Карнеги Меллона, выполненный за заданию Минобороны США. Отчет исходит из того, что военные системы относятся к классу SoS, в которых проблема интероперабельности крайне актуальна. Проведено всестороннее рассмотрение проблемы, включая определения, модели и барьеры по	http://www.dtic.mil/dtic/tr/fulltext/u2/a455619.pdf

			достижению интероперабельности	
10	Unified Profile for DoDAF and MODAF (UPDM) Version 2.1	04.08.2013	Документ является связующим звеном для совместной работы различных концепций: DoDAF/MODAF и NAF.	http://www.omg.org/spec/UPDM/2.1/PDF
Великобритания				
11	British Ministry of Defence Architecture Framework 1.2.004	15.01.2013	Концепция обеспечения военной доктрины Великобритании. Основывается на архитектуре MODAF v.3, которая легла в основу создания архитектуры НАТО NAF 4.0	https://www.gov.uk/government/publications/jdp-0-01-fourth-edition-british-defence-doctrine https://www.gov.uk/guidance/mod-architecture-framework https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/63979/20130117_MODAF_M3_version1_2_004.pdf
Австралия				
12	Defence White Paper Australia 2016	2016	Документ Министерства обороны содержит всестороннее изложение вопросов обороны Австралии. 190 с. Большое венимание уделяется проблеме интероперабельности.	http://www.defence.gov.au/WhitePaper/
Канада				
13	Canadian Forces Joint Publication CFJP 01 Canadian Military Doctrine	2009	Документ, содержит военную доктрину Канады. Большое внимание уделяется проблеме интероперабельности.	http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf
14	Canadian Armed Forces Architecture Framework (DNDAF)		Документа нет в открытом доступе	http://www.forces.gc.ca/en/about-policies-standards/dndaf.page
Новая Зеландия				
15	the 2014–2015 ANNUAL REPORT for the year ended 30 June 2015	2015	Годовой отчет за 2014-2015 г.г. Министерства обороны Новой Зеландии. Содержит основные положения военной доктрины и состояние ее реализации. Большое	http://www.nzdf.mil.nz/downloads/pdf/public-docs/nzdf-annual-report-2015.pdf

			внимание уделяется проблеме интероперабельности	
Китай				
16	Integrated Network Electronic Warfare	?	В открытом доступе полного текста нет, но ясно, что Китай идет по тому же пути, что и другие страны, развивает концепцию сетецентрической войны и должен придавать большое значение интероперабельности.	http://idsa.in/system/files/jds_4_2_dsharma.pdf

ПРИЛОЖЕНИЕ Б

(рекомендуемое)

Отечественные документы по национальной безопасности и обороне

Таблица Б.1

N п.п.	Наименование	Дата выпуска	Краткое содержание Отмечается упоминание взаимодействия, интероперабельности и стандартов	Электронный адрес
	Общегосударственного уровня			
1	Военная доктрина Российской Федерации (в редакции от 2015 г.)	(утв. Президентом РФ 25.12.2014 N Пр-2976)	Военная доктрина Российской Федерации (далее - Военная доктрина) представляет собой систему официально принятых в государстве взглядов на подготовку к вооруженной защите и вооруженную защиту Российской Федерации. Кроме политических, экономических и дипломатических аспектов в доктрине приведены «технические». В разделе «Оснащение Вооруженных Сил, других войск и органов вооружением, военной и специальной техникой» сказано: (п.45). г*) качественное совершенствование средств информационного обмена на основе использования современных технологий и международных стандартов, а также единого информационного пространства Вооруженных Сил, других войск и органов как части информационного пространства РФ.*	http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/976907
2	Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов	Документ по состоянию на август 2014 г. Одобрена решением Президента Российской Федерации от 23 ноября 1995 г. N Пр-1694	В Концепции изложена система взглядов, позволяющая качественно повысить уровень информационно-технического и информационно-аналитического обеспечения деятельности федеральных органов государственной власти, органов власти субъектов Федерации и органов местного самоуправления, а также долговременную программу, формирующую основные направления информатизации российского общества.Особо необходима комплексность проведения работ по стандартизации и сертификации средств и систем информатизации на современном этапе для формирования и развития единого информационного пространства России.	http://lawru.info/dok/1995/11/23/n453820.htm

3	Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. (Указ президента РФ №646)	5 декабря 2016 г.	В документе отмечается необходимость развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;	http://www.femida.info/14/19002.htm
	Министерство обороны РФ			
4	Концепция развития информационных и телекоммуникационных технологий ВС РФ на период до 2025 г.	Утверждена Министром обороны в феврале 2015 г	Полный текст в открытом доступе отсутствует. По данным источника Министр обороны С.К.Шойгу на заседании коллегии Минобороны сообщил: «Не секрет, что в настоящее время меняются традиционные взгляды на ведение вооружённой борьбы и процессы руководства военными действиями, на дальнейшее строительство и применение ВС, их техническое и технологическое оснащение. Информационное превосходство и высокий уровень управления войсками становятся факторами военной силы". *,Т.е., по существу отмечается необходимость перехода к концепции сецентрической войны.*	http://www.rosbalt.ru/main/2015/03/30/1383282.html
5	«Концепция развития системы управления Вооруженных Сил Российской Федерации до 2025 года»	Утверждена Министром обороны Российской Федерации 2009 г.	Полный текст в открытом доступе отсутствует. По данным источника в документе определено, что основу перспективной системы связи Вооруженных Сил, впервые будет составлять объединенная автоматизированная цифровая система связи Вооруженных Сил Российской Федерации, в которую будет входить автоматизированная цифровая система воздушно-наземной связи (АЦС ВНС).	Источник http://federalbook.ru/files/OPK/Soderjanie/OPK-6/III/meychik.pdf
6	Концепция развития системы связи Вооруженных Сил Российской Федерации на период до 2020 года	Утверждена Министром обороны Российской Федерации 2009 г.	Полный текст в открытом доступе отсутствует. По данным источника документом определено, что основу перспективной системы связи Вооруженных Сил, впервые будет составлять объединенная автоматизированная цифровая система связи Вооруженных Сил Российской Федерации, в которую	http://www.jurnal.org/articles/2015/radio4.html

			будет входить автоматизированная цифровая система воздушно-наземной связи (АЦС ВНС). Конструктивно АЦС ВНС создается в целях предоставления необходимых информационных ресурсов и услуг связи требуемого качества с использованием современных телекоммуникационных технологий, объединенных единым управлением и формирующих единое информационно-теле-коммуникационное пространство, охватывающее все органы и пункты военного управления (в космической, воздушной, наземной и морской сферах).	
7	Концепция Единого информационного пространства Вооруженных Сил Российской Федерации.	Утверждена начальником Генерального штаба Вооруженных Сил Российской Федерации 16 декабря 2004 г.	Полный текст в открытом доступе отсутствует. Согласно данным источника приводится определение ЕИП ВС РФ, обсуждается архитектура, структура служб информационных ресурсов и проблемы реализации ЕИП ВС РФ	http://www.avnrf.ru/index.php/publikatsii-otdelenij-avn/nauchnykh-otdelenij/voennogo-iskusstva/204-problemy-postroeniya-edinogo-informatsionnogo-prostranstva-vooruzhennykh-sil-rossijskoj-federatsii-i-vozmozhnye-puti-ikh-resheniya

ПРИЛОЖЕНИЕ В

(рекомендуемое)

Письмо Министерства обороны РФ

МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБОРОНЫ РОССИИ)

**НАЦИОНАЛЬНЫЙ ЦЕНТР
УПРАВЛЕНИЯ ОБОРОНОЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

г. Москва, 119160

«10» ноября 2016 г. № 346/УВГОО/412

На №

Директору Института радиотехники
и электроники имени В.А.Котельникова РАН,
члену-корреспонденту РАН
С.А.НИКИТОВУ
125009, г. Москва, ул. Моховая, д. 11, стр. 7

Уважаемый Сергей Аполлонович!

Выражаю Вам и Вашим сотрудникам искреннюю признательность за весомый вклад в организацию II Межведомственной научно-практической конференции «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации», проведенной 25 ноября 2016 г. в Национальном центре управления обороной Российской

Конференция придала импульс развитию межведомственного информационного взаимодействия и способствует его выходу на качественно новый уровень.

Хочу отметить, что проводимые Вашим Институтом работы в области обеспечения интероперабельности информационных систем представляют интерес для Национального центра управления обороной Российской Федерации с точки зрения реализации Военной доктрины Российской Федерации, утвержденной Президентом Российской Федерации 25 декабря 2014 г.

Надеюсь на дальнейшее плодотворное сотрудничество на благо нашего государства!

С уважением,

Начальник Национального центра
управления обороной Российской Федерации М.Мизинцев

ИРЭ им. В.А. Котельникова РАН
Зарегистрировано
«01» 12 2016 г.
вх. № 914

ПРИЛОЖЕНИЕ Г

(рекомендуемое)

Решение II Межведомственной научно-практической конференции на тему: «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации»

Начальнику Генерального штаба
Вооруженных Сил Российской Федерации –
первому заместителю Министра обороны
Российской Федерации
генералу армии В.В.ГЕРАСИМОВУ

14.12.16

Докладываю.

В целях совершенствования вопросов межведомственного информационного взаимодействия, поиска новых способов и форм совместной работы в интересах обороны Российской Федерации 25 ноября 2016 г. под руководством Министра обороны Российской Федерации проведена II Межведомственная научно-практическая конференция на тему: «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации» (далее – конференция).

В конференции приняли участие руководящий состав и должностные лица главных командований видов Вооруженных Сил Российской Федерации, объединенных стратегических командований военных округов и Северного флота, командований родов войск Вооруженных Сил Российской Федерации, центральных органов военного управления, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, научно-исследовательских организаций, государственных образовательных учреждений высшего образования, организаций промышленности и бизнеса.

В основном докладе были подведены итоги совместной работы федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и организаций в 2016 году, а также отражены перспективные пути совершенствования системы межведомственного информационного взаимодействия в области обороны Российской Федерации.

С целью демонстрации новых подходов к информационно-аналитическому обеспечению и информационной безопасности

системы межведомственного информационного взаимодействия проведена выставка специального программного обеспечения, оборудования и изделий, в которой приняли участие субъекты Российской Федерации, организации промышленности и бизнеса, государственные образовательные учреждения высшего образования, от Министерства обороны Российской Федерации – Национальный центр управления обороной Российской Федерации.

По итогам работы и в целях дальнейшего совершенствования системы межведомственного информационного взаимодействия конференция решила:

1. Считать план конференции выполненным, цели конференции достигнутыми.

2. Обобщить предложения, рассмотренные в ходе пленарной части конференции, по выработке форм и методов, направленных на дальнейшее совершенствование системы межведомственного информационного взаимодействия.

3. Изучить возможность восстановления государственной системы научной и технической информации, как информационной основы системы межведомственного информационного взаимодействия, для достижения целей, предусмотренных в стратегических документах, направленных на научно-техническое и инновационное развитие Российской Федерации.

4. Рассмотреть проблему обеспечения интероперабельности (способность двух или более систем к обмену информацией) с учетом реализации положений военной доктрины Российской Федерации, утвержденной Президентом Российской Федерации 25 декабря 2014 г., как одно из важнейших средств повышения эффективности и безопасности функционирования системы государственного и военного управления, обеспечения информационного взаимодействия между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, иными государственными органами при решении задач в области обороны и безопасности.

5. Рекомендовать к реализации в повседневной деятельности войск (сил) положительный опыт взаимодействия с федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и организациями.

6. Результаты конференции оформить в виде сборника материалов.

Докладываю в порядке исполнения указаний.

Начальник Национального центра
управления обороной Российской Федерации
генерал-лейтенант М.Мизинцев

«02» декабря 2016 г.

Исх. № 346/6419

ПРИЛОЖЕНИЕ Д

(рекомендуемое)

Проект ГОСТ Р «Информационные технологии. Военное дело. Интероперабельность. Основные положения»