УДК 004.77

ПРОБЛЕМА ИНТЕРОПЕРАБЕЛЬНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ВОЕННОГО НАЗНАЧЕНИЯ

А. А. Каменщиков, А. Я. Олейников, И. И. Чусов, Т. Д. Широбокова

Институт радиотехники и электроники им. В.А. Котельникова РАН

Статья поступила в редакцию 19 октября 2016 г.

Аннотация. На основе анализа открытых источников исследована «проблема интероперабельности» в Вооруженных силах (ВС) за рубежом и в РФ.

Статья содержит три раздела. В первом разделе дано краткое описание разработанного авторами единого подхода к обеспечению интероперабельности информационных систем широкого класса. Этот подход зафиксирован к национальном стандарте ГОСТ Р 55062-2012, не имеющем прямых международных аналогов. Представляется важным, что в этом стандарте впервые в мировой практике зафиксирована трехуровневая эталонная модель интероперабельности.

Во втором разделе рассмотрена проблема интероперабельности в ВС. Отмечается, что проблема взаимодействия в ВС так же стара, как само понятие ВС, но средства обеспечения взаимодействия непрерывно совершенствовались. На сегодня все большей степени доминируют средства информационно-коммуникационных технологий, что изменило и саму концепцию ведения боевых действий, появилось понятие сетецентрической войны (СЦВ). Кратко описываются основные положения концепции СЦВ. В СЦВ взаимодействие ведется на основе распределённых компьютерных сетей типа Интернет. Подчеркивается, что для реализации концепции СЦВ войны обеспечение интероперабельности составляет одно из важнейших условий. Особо подчеркивается, что в ВС зарубежных военных держав и в первую очередь США, а также объединённых ВС НАТО, кроме концептуальных документов, имеются в открытом доступе большое количество детальных документов типа инструкций и директив, позволяющих обеспечить интероперабельность.

Анализ доступных отечественных документов показывает, что вопросам интероперабельности на основе использования ИКТ-стандартов уделяется внимание, но, можно сказать, это − декларативный уровень, детальные документы отсутствуют. В третьем разделе авторы делают попытку применить разработанный ими единый подход к решению проблемы интероперабельности в ВС РФ. Предлагается архитектура единого информационного пространства ВС РФ, проблемно-ориентированная модель интероперабельности, являющаяся расширением эталонной трехуровневой модели, и минимальный профиль интероперабельности.

Ключевые слова: электронное военное дело, интероперабельность, единое информационное пространство, сетецентрическая война, концепция, архитектура, эталонная модель, сертификация, стандарты, профили, дорожная карта, сервис-ориентированная архитектура.

Abstract. The research of the 'problem of interoperability' in the Armed Forces (AF) in Russia and abroad has been based on the analysis of open sources.

The article consists of three sections, the first one provides a brief description of a common approach developed by the authors to ensure the interoperability of a broad class of information systems. This approach is secured in the National Standard (GOST R 55062-2012), which has no direct international analogs. It's important that the standard for the first time in the world practice secures a three-level reference model of interoperability.

The second section addresses the problem of interoperability in the Armed Forces. It is noted that although the problem of interaction in the AF is as old as the very notion of the AF, the means of ensuring interaction have been improving continuously. Nowadays the means of information and communication technologies increasingly dominate, this has changed the very concept of warfare, the notion of network-centric warfare (NCW) has appeared. The main provisions of the NCW concept are briefly described. The NCW is based on the interaction of distributed computer networks such as the Internet. It is emphasized that ensuring interoperability is one of the most important conditions for the implementation of the concept of NCW war. It is

particularly underlined that in the AF of foreign military powers, primarily the United States and the United Armed Forces of NATO, with the exception of the conceptual documentation, a large number of detailed documents (such as instructions and directives) enabling to ensure interoperability are publicly available. Analysis of available national documents demonstrates that the problems of interoperability through the use of ICT- standards are addressed, but, so to say, only on the declarative level, as detailed documents are absent.

In the third section, the authors make an attempt to apply the unified approach they've developed to solving the problem of interoperability in the Russian AF. The architecture of a unified information space of the Russian AF, problem-oriented interoperability model which is an extension of the standard three-tier model, as well as a minimum profile of interoperability are proposed.

Key words: e-military, interoperability, unified information space, net centric war, framework, architecture, base model, certification, standards, profiles, road map, Service-Oriented Architecture (SOA).

Введение

На основе анализа зарубежного и отечественного опыта, а также собственного многолетнего опыта по созданию открытых систем [1] нами был предложен единый подход к обеспечению интероперабельности для информационных систем самого широкого класса [2], зафиксированный в государственном стандарте ГОСТ Р 55062-2012 [3]. При едином подходе, в зависимости от конкретной области применения, получаемые решения отличаются, что проявляется в составе стандартов профиля на уровнях выше технического.

Проблема интероперабельности актуальна и для ИС военного назначения, так в [4] вопросам интероперабельности посвящена отдельная глава. В данной работе авторы делают попытку применить свой опыт к решению проблемы интероперабельности к информационным системам (ИС) Вооруженных Сил Российской Федерации.

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. рисунок 2.

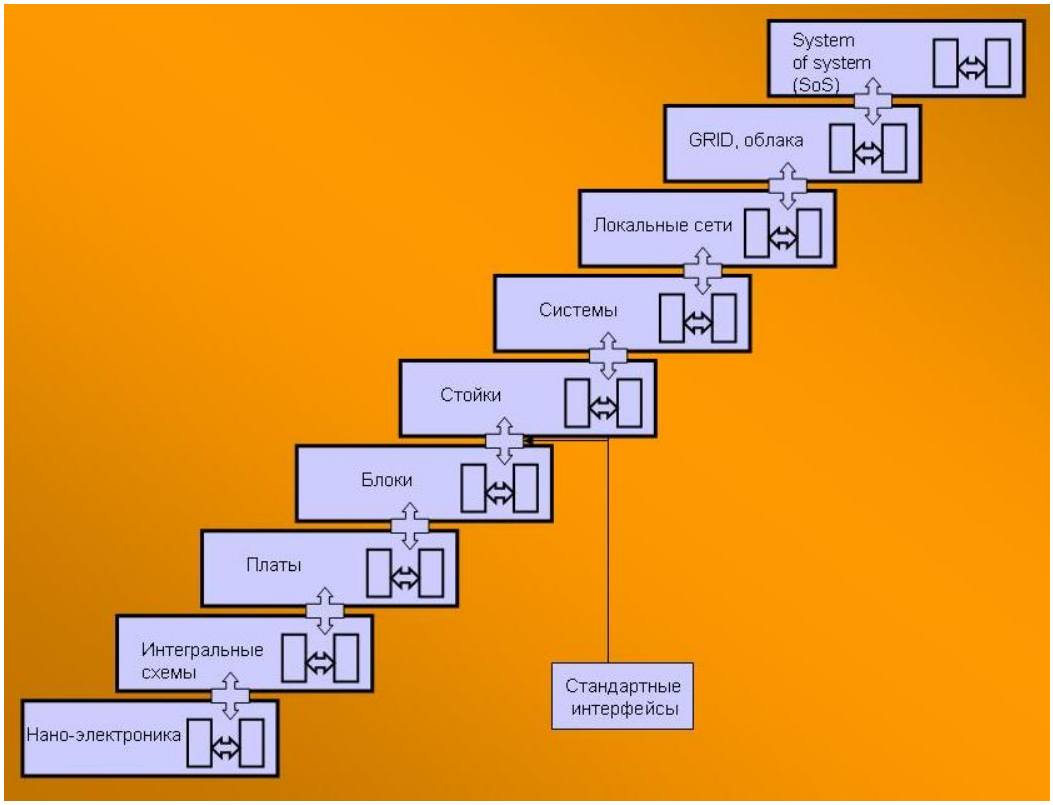


Рисунок 2 — Классификация ИС по масштабу

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).

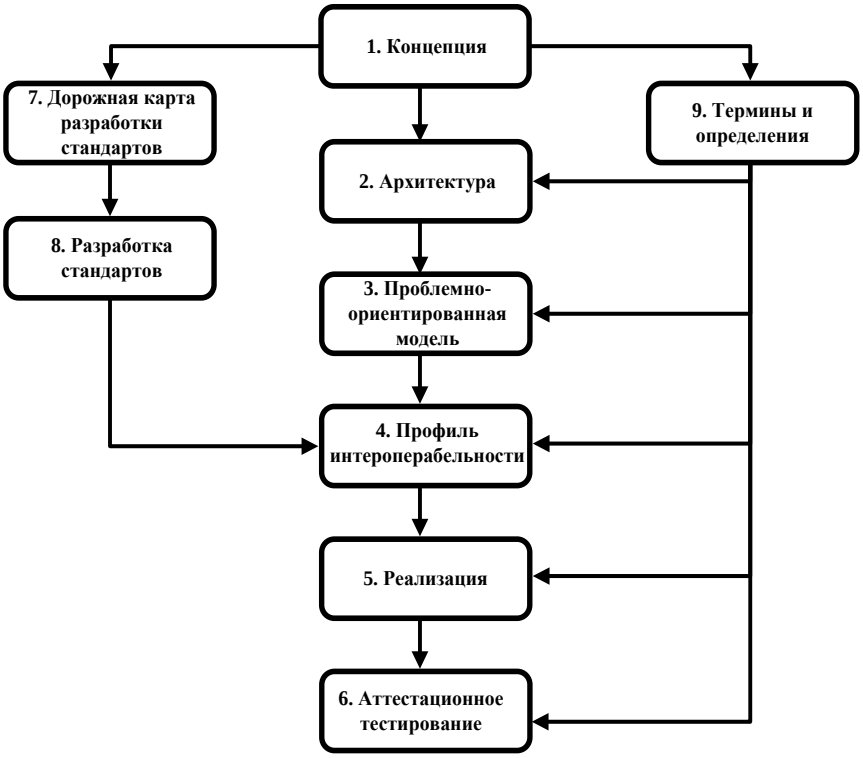


Рисунок 3 — Блок- схема единого подхода к достижению интероперабельности для ИС широкого класса

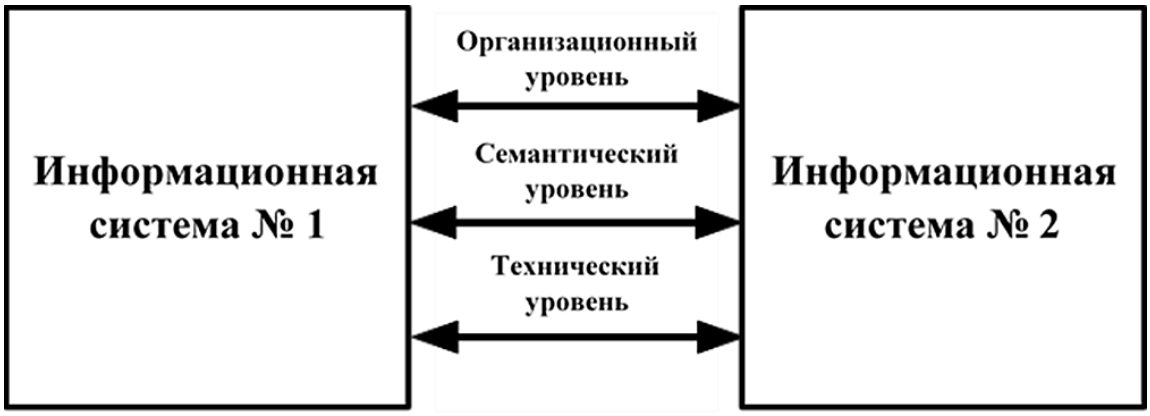


Рисунок 4 — Эталонная модель интероперабельности

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

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 СЦВ 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:

1. Силы, объединённые достаточно надежными сетями, получают возможность качественно нового обмена информацией.
2. Обмен информацией повышает качество информации и уровень общей информированности о происходящем.
3. 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], сменившую 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

Что касается проблемы интероперабельности, то 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. Ввиду 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, но для подробного анализа в журнальной статье нет места. 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.

К этим документах относятся: Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов [41], Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. N ПР-1895[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-вторы, 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 в 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.

Итак, можно сделать вывод, что решение проблемы интероперабельности для ВС РФ для поддержания паритета в условиях СЦВ крайне актуальная 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).

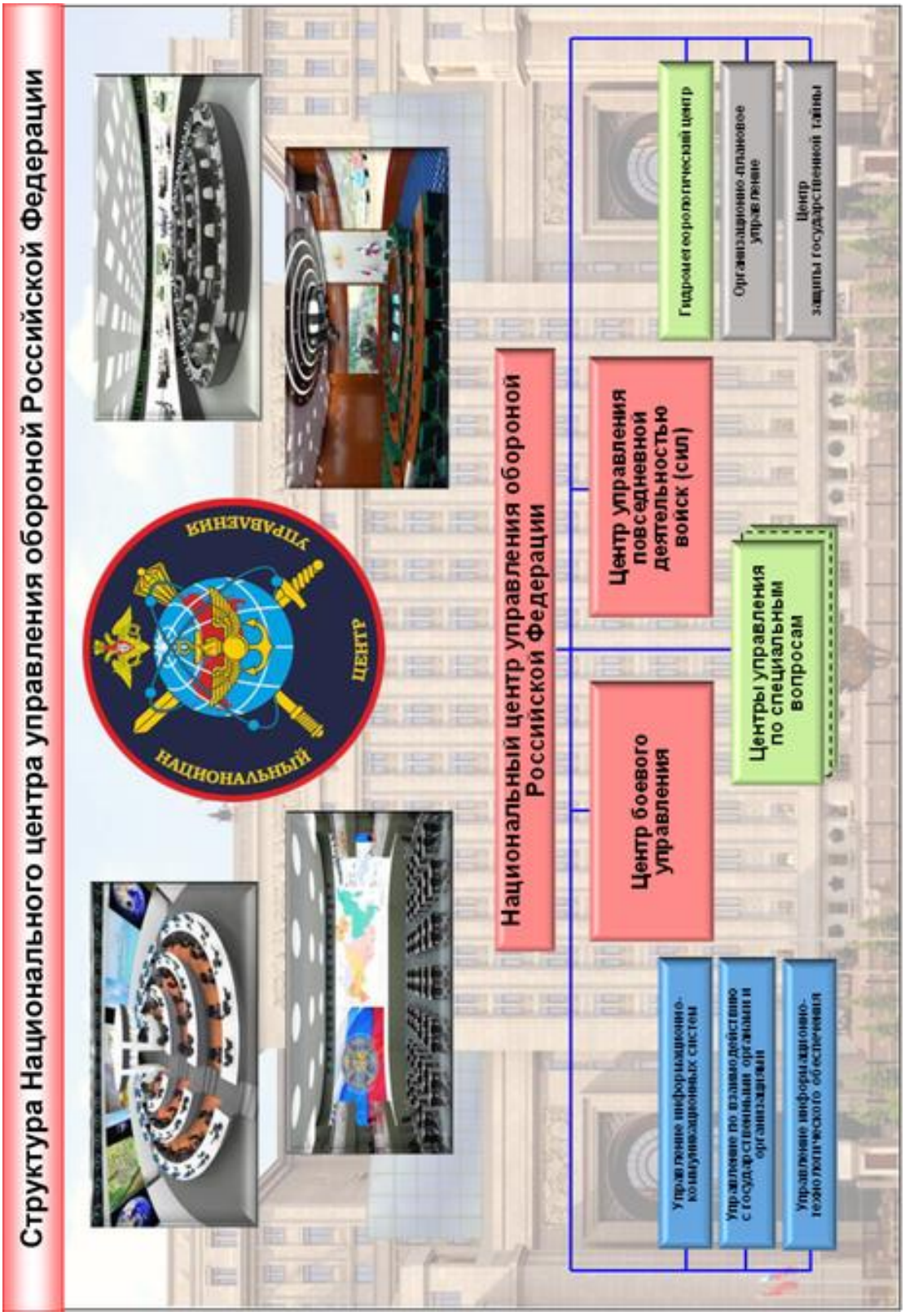


Рисунок 7 — Структура национального центра управления обороной РФ

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

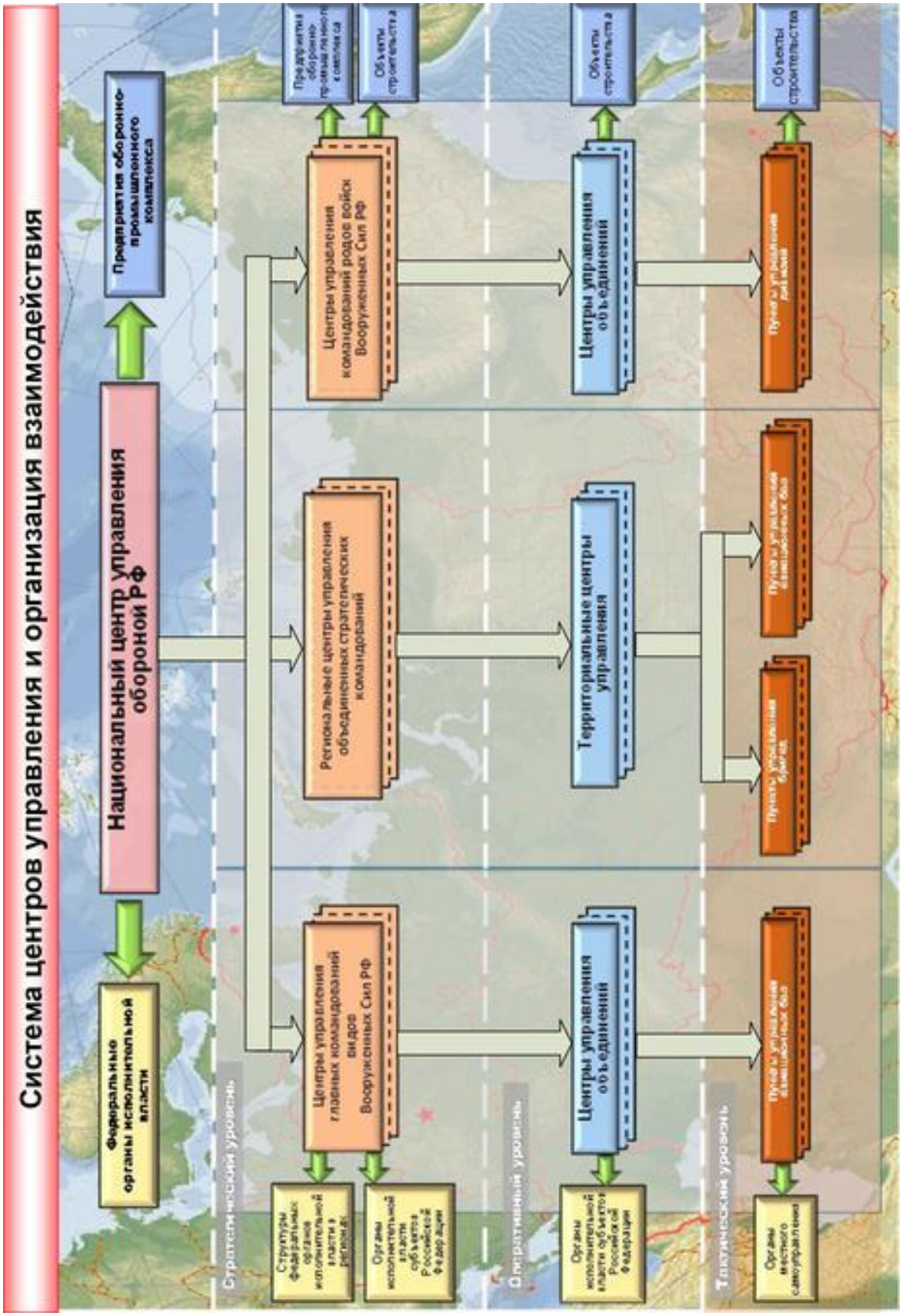


Рисунок 8 — Система центров управления и организация взаимодействия

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).

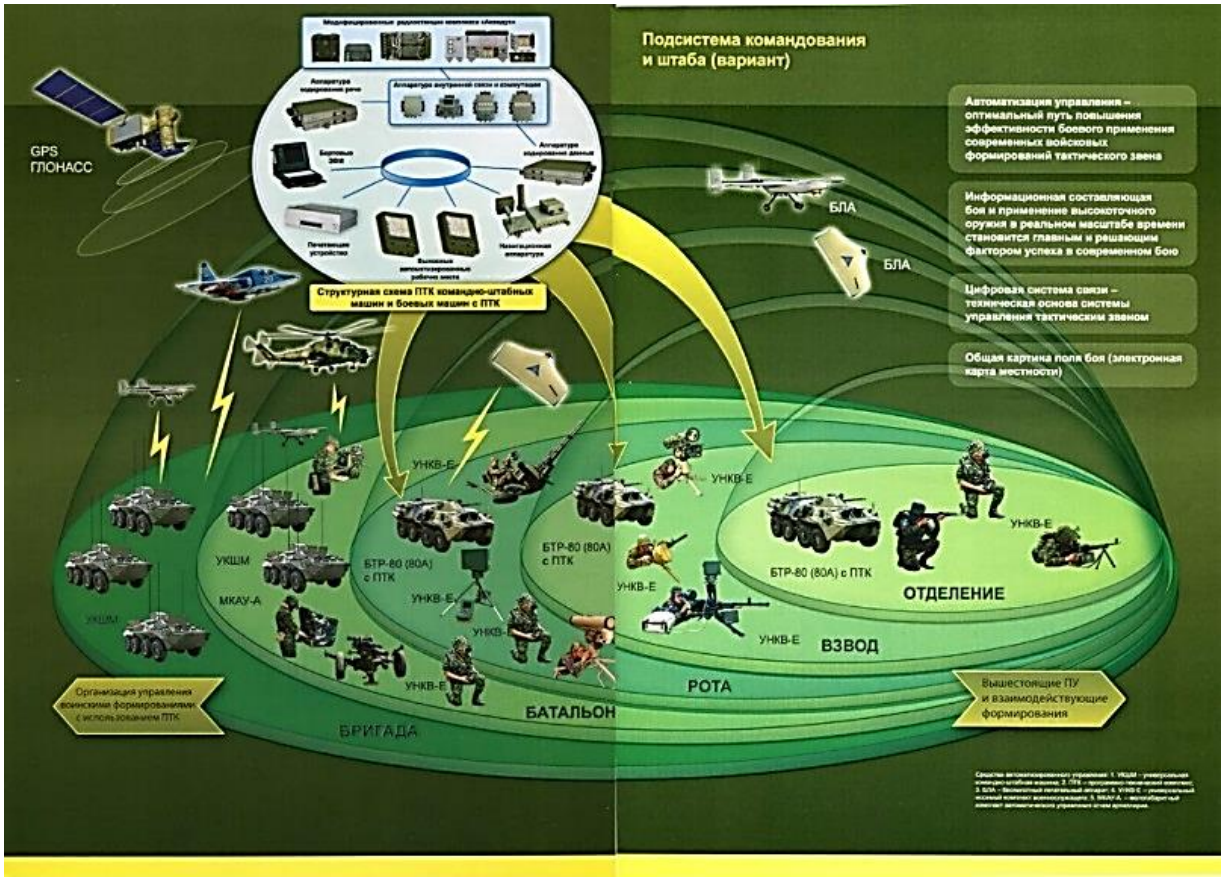


Рисунок 9 — Бригада как современная основа тактического уровня

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].

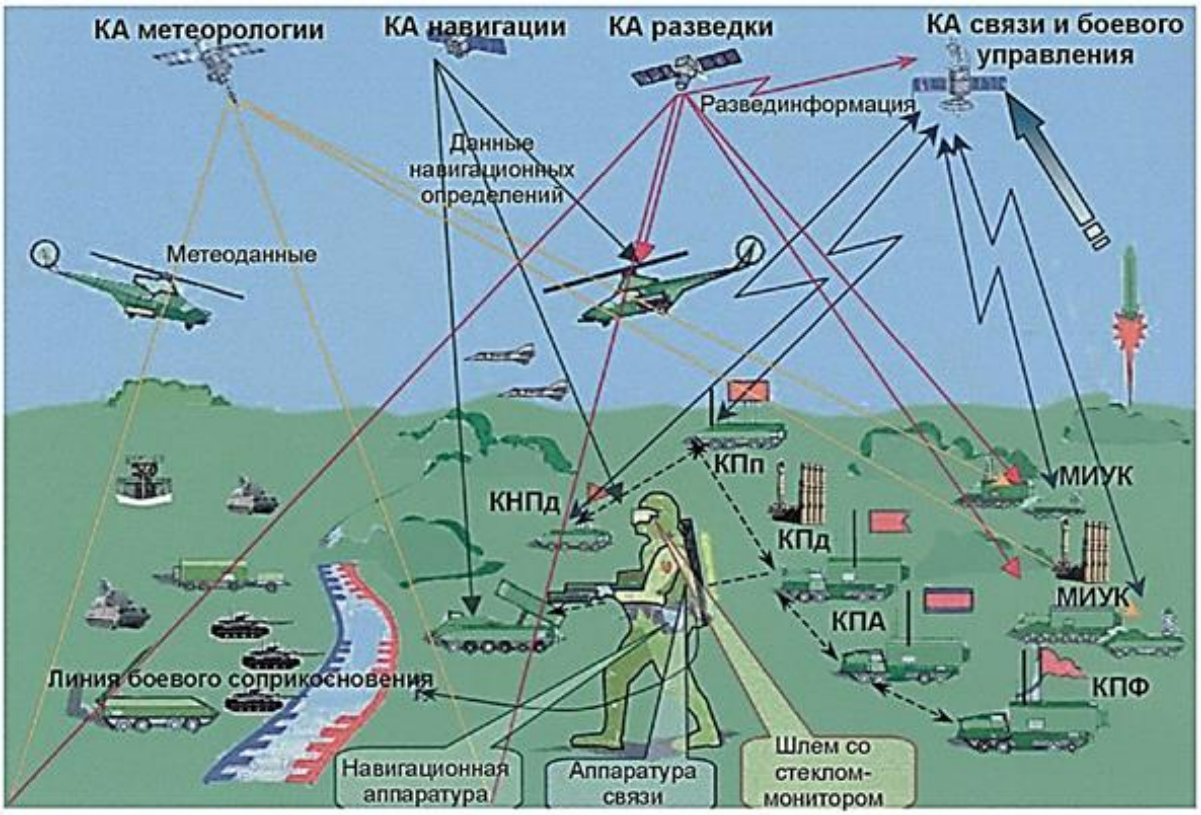
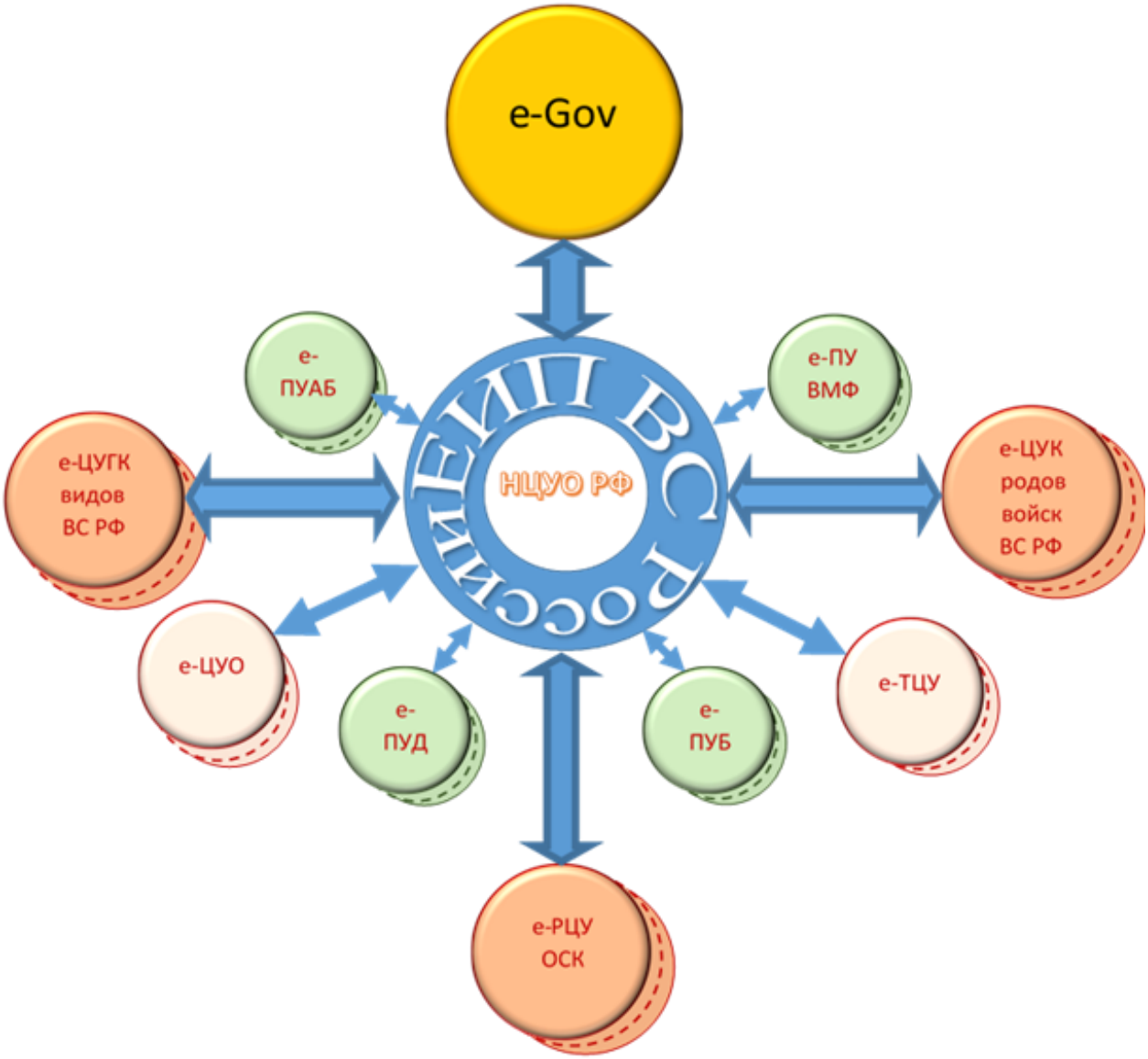


Рисунок 10 — Солдат будущего

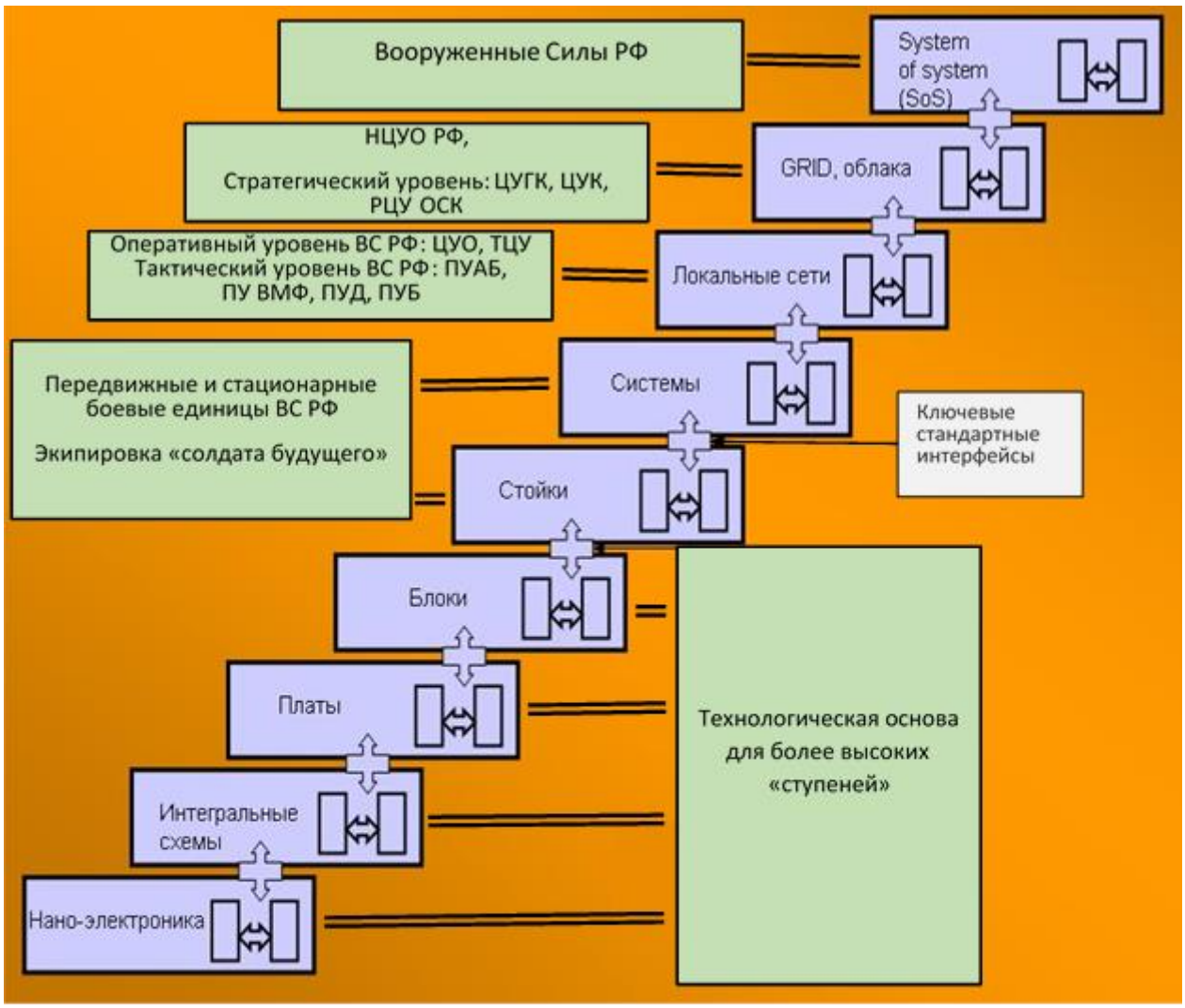
В условиях СЦВ Единое информационное пространство ВС РФ заведомо представляет собой сугубо гетерогенную среду, содержащую разнородные платформы, в которой возникает проблема интероперабельности (см. рисунок 11). При этом осуществляется переход от «технической» интероперабельности к «семантической».



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, ЕИП ВС РФ имеет архитектуру с тремя размерностями (см. рисунок 13).

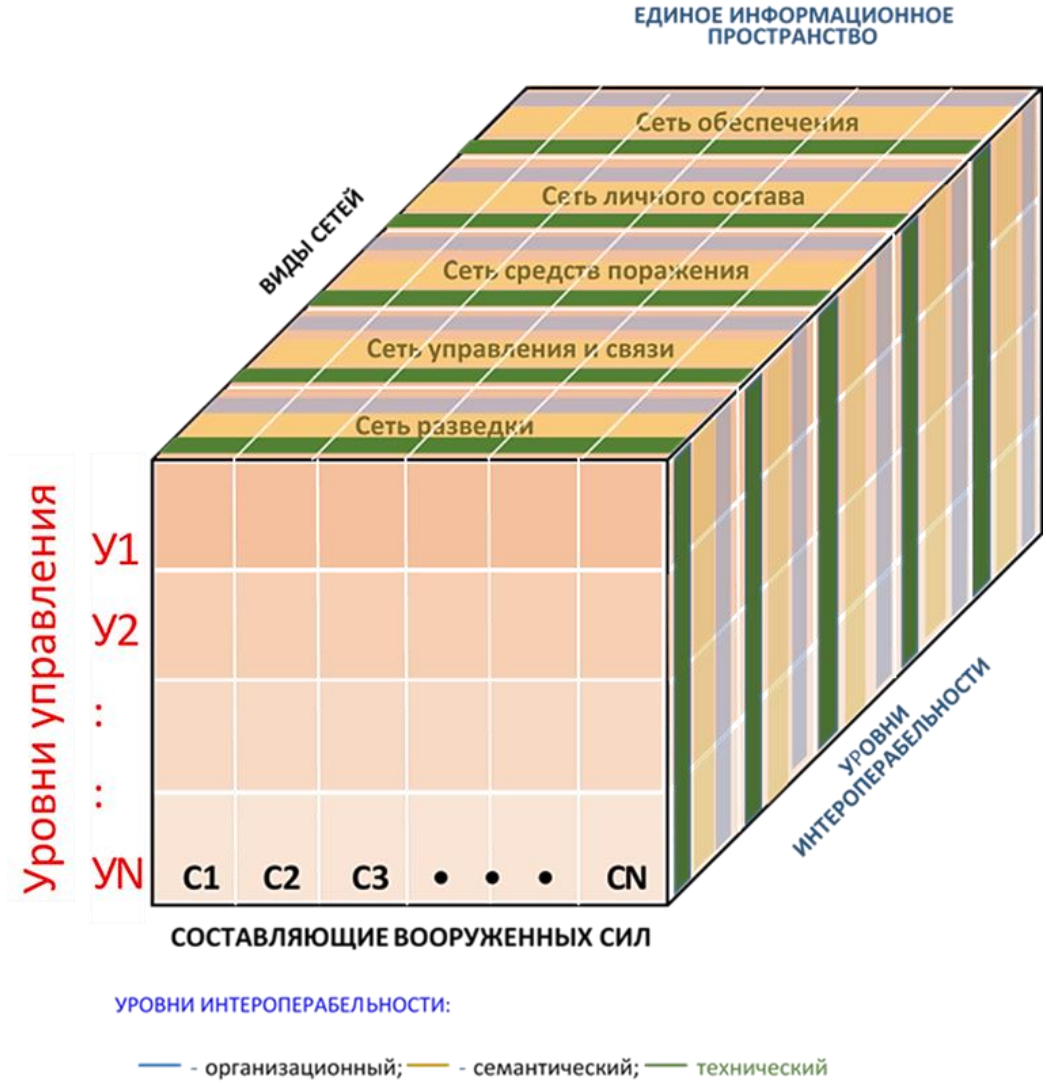


Рис. 13. Архитектура Единого информационного пространства ВС РФ

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

По вертикальной оси – уровни управления (от стратегического до тактического). (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 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).

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].

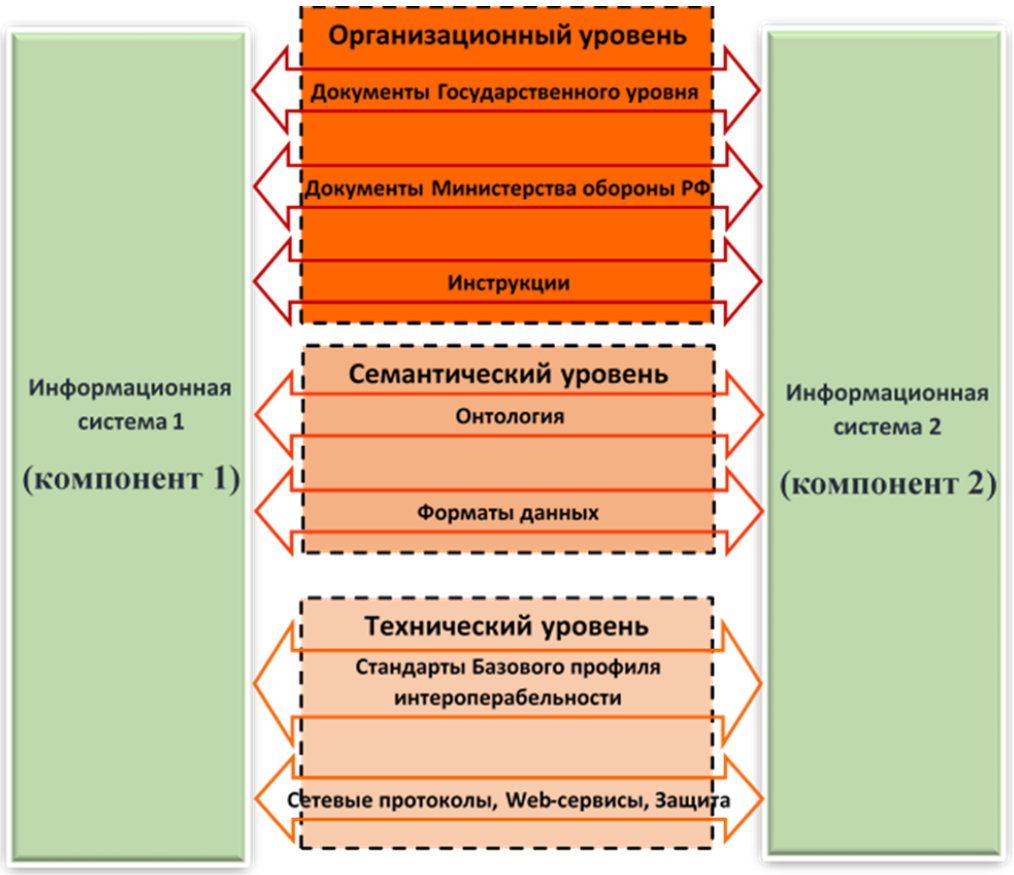


Рисунок 14 — Модель интероперабельности для информационных систем военного назначения

3.4 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.

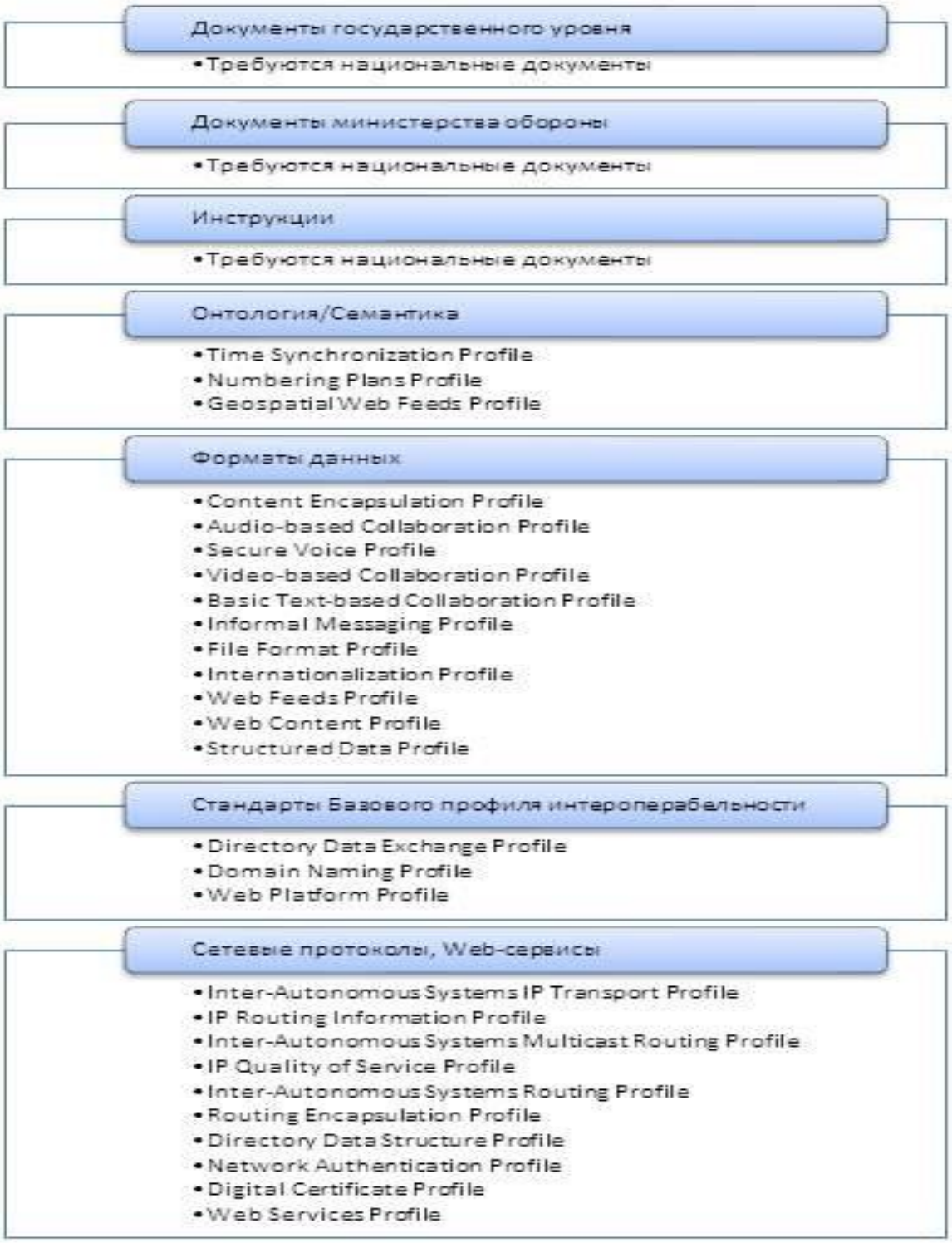


Рисунок 15 — Минимальный профиль ВС РФ

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

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

3.5 Остальные этапы единого подхода (см. рисунок 3)

Этап 5 - Программно-аппаратная реализация.

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

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» 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. Для 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 у реализационного уровня.

3. Необходимо срочно сконцентрировать научно-технические ресурсы Минобороны и провести цикл целенаправленных работ по решению проблемы интероперабельности в ВС РФ. При этом целесообразно использовать опыт организаций РАН, в том числе авторов настоящей работы.

Литература

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%B

8%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-2 (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 от 9 сентября 2000 г. N ПР-1895. [сайт «Правовая Россия]. URL: http://www.femida.info/14/19002.htm (дата обращения: 03.10.2016).
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. Виды служебных документов, их краткая характеристика и основные требования к ним. Глава 14. Основные виды документов ВС РФ. / 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