УДК 004.77

ОБЕСПЕЧЕНИЕ ИНТЕРОПЕРАБЕЛЬНОСТИ КАК СРЕДСТВА БЕСШОВНОЙ ИНТЕГРАЦИИ ФУНКЦИОНАЛЬНЫХ ПОДСИСТЕМ В СОСТАВЕ ПЕРСПЕКТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

А. А. Башлыкова [1,2], А. А. Каменщиков [2], А. Я. Олейников [2]

[1] Московский технологический университет,119454, Москва, пр. Вернадского, 78
[2] ИРЭ им. В.А. Котельникова РАН, 125009, Москва, ул. Моховая 11, корп.7

Статья поступила в редакцию 1 сентября 2018 г.

Аннотация. Проведен анализ известного опыта по созданию информационных систем военного назначения на основе принципов интероперабельности с учетом информационного противоборства. Показано, что обеспечение интероперабельности представляет собой наиболее экономически эффективный способ бесшовной интеграции функциональных подсистем в перспективные автоматизированные системы военного назначения. Интероперабельность – одно из основных требований сетецентрической войны. Показана взаимосвязь понятий единого информационного пространства вооруженных сил, критической информационной инфраструктуры вооруженных сил и инероперабельностьи. Коротко описан отечественный и зарубежный опыт создания автоматизированных систем военного назначения на основе принципов интеропербельности. Проблему интероперабельности следует решать совместно с проблемой информационного противоборства, в связи с чем предложена синтезированная модель интероперабельности и модели угроз, что дает возможность обеспечения информационной безопасности с использованием стандартов информационной безопасности. Предложена модель интероперабельности для информационных систем военного назначения, представляющая собой расширение эталонной модели интероперабельности, зафиксированной в ГОСТ Р 55062-2012. Обоснованы меры по решению проблемы интероперабельности. Первая мера должна быть связана с тем, что решение проблемы интероперабельности совместно с

проблемой информационной безопасности должно осуществляться практически на всех этапах жизненного цикла, предусмотренными в стандартах: ГОСТ 34.601-90, ГОСТ Р ИСО/МЭК 12207-99, и ГОСТ Р ИСО/МЭК 15288-2005. Вторая мера должна заключаться в создании постояннодействующего рабочего органа по обеспечению интероперабельности, включающего три рабочих группы с представителями вооруженных сил российской федерации, оборонно-промышленного комплекса и других заинтересованных ведомств.

Ключевые слова: интероперабельность, информационные системы, критическая информационная инфраструктура, стандарты, системы военного назначения, сверхсложные системы, бесшовная интеграция.

Abstract. The analysis of the known experience in the creation of information systems for military purposes based on the principles of interoperability, taking into account the information confrontation was proposed. It is shown that ensuring interoperability is the most cost-effective way of seamless integration of functional subsystems in advanced automated systems for military purposes. Interoperability is one of the basic requirements of network-centric warfare. The interrelation of concepts of uniform information space of armed forces, critical information infrastructure of armed forces and interoperability is shown. The russian and foreign experience of creation of the automated systems of military purpose on the basis of the principles of interoperability is briefly described. The problem of interoperability should be solved in conjunction with the problem of information warfare, and therefore proposed a synthesized model of interoperability and threat models, which makes it possible to ensure information security using information security standards. The model of interoperability for military information systems, which is an extension of the reference model of interoperability fixed in GOST R 55062-2012 was proposed. Measures to solve the problem of interoperability are substantiated. First, the measure must be related to the fact that the solution to the problem of interoperability in conjunction with the problem of information security should be carried out practically at all stages of the life cycle envisaged in the standards: GOST

34.601-90, GOST R ISO/IEC 12207-99, and GOST R ISO/IEC 15288-2005. The second measure should be to create a permanent working body to ensure interoperability, which includes three working groups with representatives of the armed forces of the Russian Federation, the military-industrial complex and other interested agencies.

Key words: interoperability, information systems, critical information infrastructure, standards, military systems, highly complex systems, seamless integration.

Введение

Перспективные автоматизированные системы военного назначения (ПАСВН) должны быть предназначены для применения в условиях сетецентрической войны. Это означает, что они должны объединять в единую сеть большое множество функциональных подсистем (ФП), реализованных на разнородных программно-аппаратных платформах, и с системной точки зрения должны составлять т.н. «систему систем» (System of Systems). С другой стороны, в ФЗ «О защите критической информационной инфраструктуры», вступившем в силу с 1 января 2018 г., введены такие понятия как «критическая информационная инфраструктура» и «объекты критической информационной инфраструктуры». Из приведенных определений следует, что ПАСВН представляет собой критическую информационную инфраструктуру (КИИ).

Как следует из действующей Военной доктрины РФ (см. п 46), ПАСВН должна составлять основу Единого информационного пространства ВС РФ, а фундаментом служит интероперабельность, в основе которой лежит использование согласованных наборов стандартов информационно-коммуникационных технологий – профилей. Мировой и отечественный опыт показывают, что в условиях информационного противоборства проблему интероперабельности следует рассматривать совместно с проблемой информационной безопасности. Одним из способов обеспечения информационной безопасности служит включение в профиль стандартов информационной безопасности.

Таким образом, для реализации бесшовной интеграции ФП в составе ПАСВН необходимо обеспечить интероперабельность каждой из ФП.

Для этого, в первую очередь, необходимо выполнить анализ передового зарубежного опыта создания интегрированных систем военного назначения на принципах интероперабельности, во-вторых построить синтезированную модель интероперабельности и модели угроз и в-третьих обосновать комплекс мер по решению проблем на основе совершенствования процессов в жизненном цикле систем.

В статье проанализированы позднейшие доступные зарубежные и отечественные материалы по созданию систем на принципах интероперабельности в первую очередь материалы НАТО.

1. Интероперабельность. Основные понятия. Методика обеспечения

Согласно общепринятым определениям (ГОСТ Р 55062-2012, ИСО/МЭК/ИЕЕЕ 24765:2010) интероперабельность - способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена.

В основе достижения интероперабельности лежит использование согласованных наборов стандартов ИКТ-технологий – профилей. Обеспечение интероперабельности, по существу, и есть наиболее экономичный бесшовный способ интеграции разнородных функциональных систем. Ведь, совершенно очевидно, что любую систему можно стыковать с любой другой, если, не считаясь с затратами, создать переходный шлюз (модуль). В ГОСТ Р 55062-2012 приведены эталонная модель интероперабельности (Рис. 1) и методика обеспечения интероперабельности (Рис. 2).

Здесь следует подчеркнуть, что использование ИКТ-стандартов обеспечивает только нижний, т.н. «технический» уровень интероперабельности. Полная интероперабельность может быть достигнута на более высоких уровнях - семантическом и организационном.

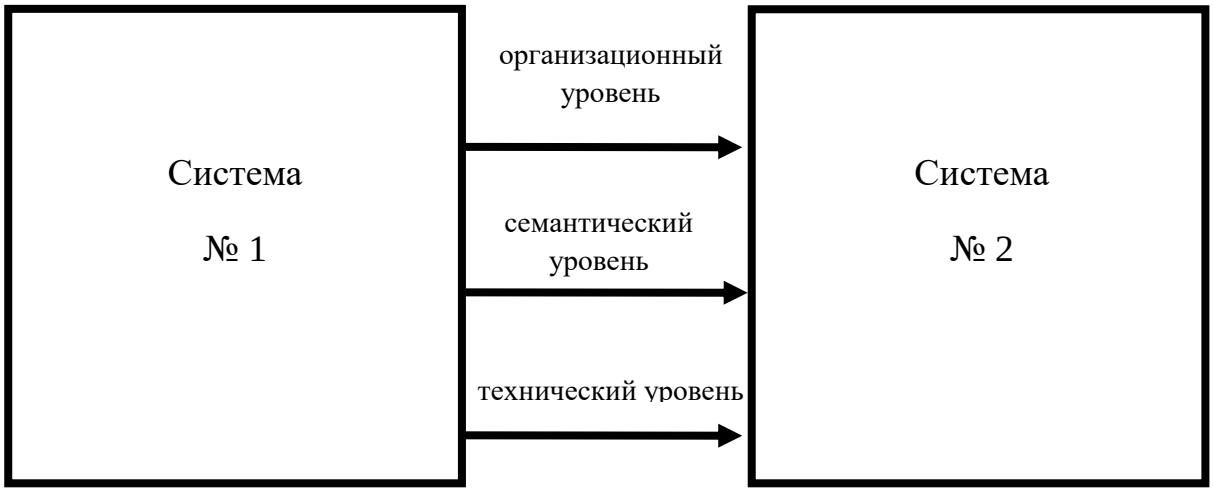

Рис. 1 - Эталонная модель интероперабельности.

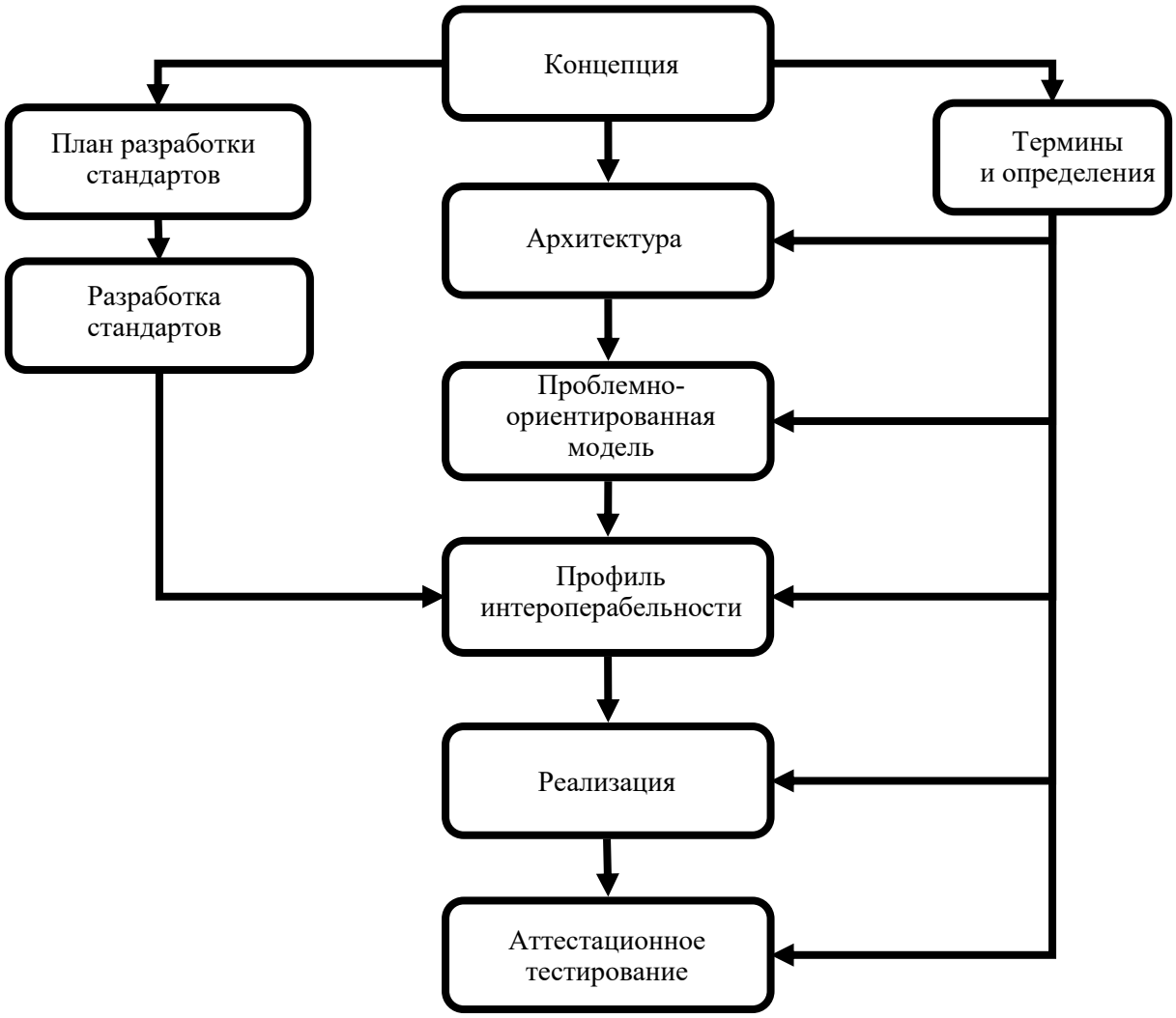

Рис. 2– Блок-схема методики обеспечения интероперабельности.

2. Интероперабельность – основное требование сетецентрической войны

Как известно, в настоящее время большинство зарубежных военных держав, а также НАТО реализуют концепцию сетецентрической войны (СЦВ) (или сетецентрических операций (network) [см. например 1,2]. Основные положения СЦВ изложены в американской военной доктрине «Joint Vision 2020», где подчеркивается, что интероперабельность составляет фундамент СЦВ. В Военной доктрине РФ напрямую об интероперабельности не говорится, а говорится о качественном совершенствовании средств информационного обмена на основе использования современных технологий и международных стандартов, а также единого информационного пространства Вооруженных Сил (ЕИП ВС), других войск и органов как части информационного пространства Российской Федерации (п.46 г). Совокупность отдельных ФП, объединённых средствами телекоммуникаций, составляет ПАСВН, или важнейшую критическую информационную инфраструктуру (КИИ ВС). На рис. 3 показана взаимосвязь между такими понятиями как ЕИП ВС, КИИ ВС, инероперабельность и др.

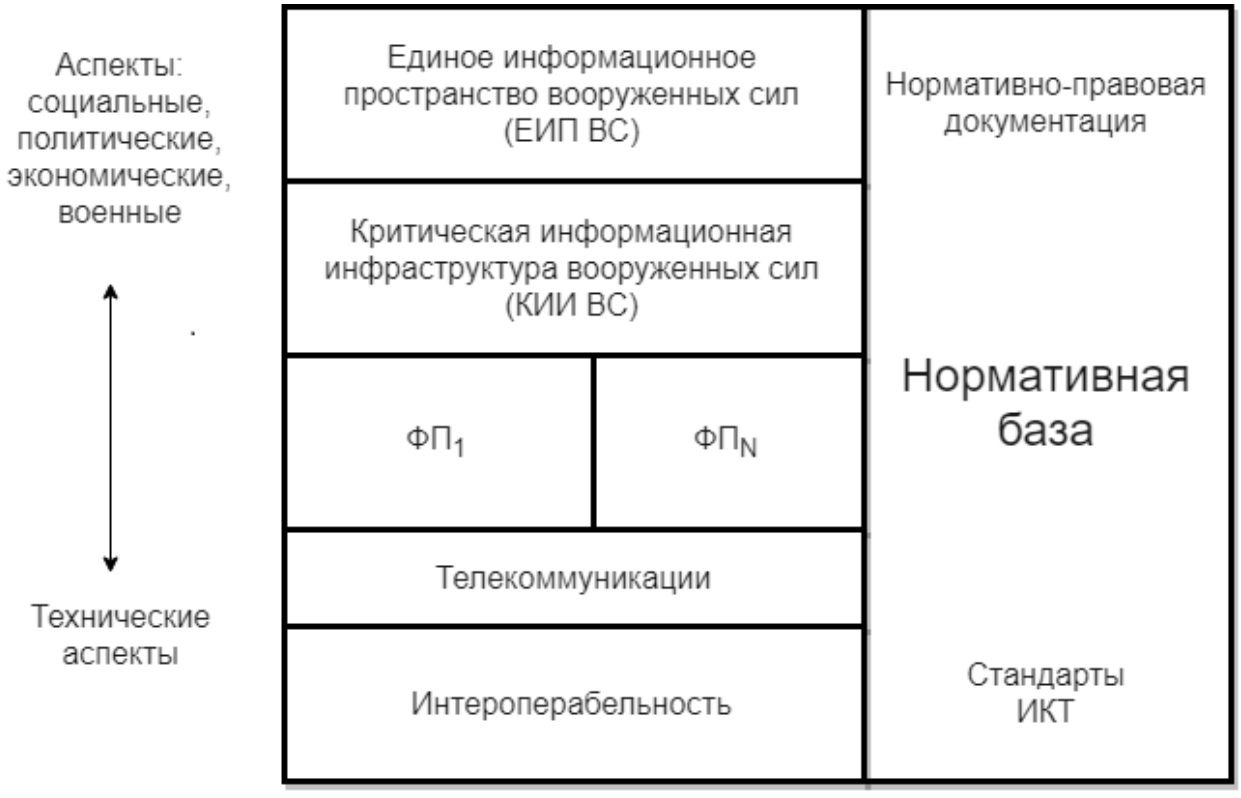

Рис. 3 - Соотношение понятий ЕИП ВС, КИИ ВС, интероперабельность и др. [8]

3 Создание автоматизированных систем военного назначения на основе принципов интеропербельности

3.1 Зарубежный опыт

В НАТО придают большое значение обеспечению интероперабельности при создании информационно-коммуникационных систем. Один из последних документов (февраль 2017 г. - стандарт НАТО STANAG 2525 «AJP-6 allied joint doctrine for communication and information systems» (AJP-6) и, как видим из названия, представляет собой доктрину обеспечения интероперабельности между союзниками НАТО [3]. Данный документ является одним из ключевых стандартов, описывающим необходимость обеспечения интероперабельности вооруженных сил союзников различных стран. Из анализа документа следует, что обеспечение интероперабельности является одной из первостепенных задач объединённых сил НАТО. Документ является концептуальным и не содержит детализированных рекомендаций по обеспечению интероперабельности в том числе по конкретным стандартам.

Более детальный документ, разрабатываемый специальным органом (Interoperability Profiles Capability Team) под названием «NATO standards and profiles» – NISP. Последняя редакция была выпущена 3 августа 2018 г. и опубликована на сайте https://live.nisp.nw3.dk/. Документ содержит 3 тома, 170 страниц, 28 профилей, 529 стандартов и 66 базовых сервисов.

3.2 Отечественный задел

В нашей стране проблеме интероперабельности в военной сфере тоже придается некоторое значение, но далеко не соответствующее важности проблемы. Поэтому надо скорее говорить о заделе, а не об опыте. Специалисты, безусловно, понимают роль интероперабельности [2,4]. Но, как мы видели выше, в действующей Военной доктрине РФ (2014 г.) напрямую не говорится о реализации концепции СЦВ, и не употребляется термин «интероперабельность».

Существует действующий документ Министерства обороны РФ РДВ 44.5801-1-2006 «Профиль объединённой автоматизированной цифровой

системы связи Вооруженных Сил Российской Федерации» (Профиль ОАЦСС ВС РФ). Сравнение данного документа с рассмотренным выше документом NIST показывает, что отечественный документ выглядит сильно устаревшим, как функционально (он касается только системы связи и не рассматривает АСУ) а также содержит много устаревших стандартов. К сожалению, запланированное в данном документе его развитие было приостановлено. Авторы настоящей статьи дважды выступали с конкретными предложениями по решению проблемы интероперабельности на научно-практических конференциях «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации», проводимых Национальным центром управления обороной РФ [5,6]. Следует признать, что сделанные нами предложения, хотя отмечены в Решениях конференций, и получили одобрение начальника Генштаба ВС РФ не перешли в стадию реализации. По-видимому, это объясняется общим отставанием в развитии и применении ИК-технологий в нашей стране. Об этом говорит тот факт, что по такому показателю, как «Индекс развития ИКТ» (ООН) - Information development index IDL, характеризующему достижения стран мира с точки зрения развития ИКТ по результатам 2017 г. РФ занимает 45 место из 176 стран. Следствием этого отставания служит и то, что в нашей стране нарастающим темпом идет отставание в стандартизации ИКТ [7]. Доля национальных ИКТ-стандартов составляет не более 5% от числа международных, а достаточно очевидно, что такие документы, как профиль, направленные на обороноспособность страны должны строиться на основе национальных стандартов. В [7] содержатся предложения и рекомендации по совершенствованию процесса нормативного регулирования работ по созданию информационно-телекоммуникационных систем. Следует учесть, что в профиль, кроме стандартов ГОСТ Р и стандартов информационной безопасности, разрабатываемых ФСТЭК, должны входить военные стандарты ГОСТ РВ и т.н. стандарты двойного применения. Работы по всем этим видам

стандартов ведутся независимо, что затрудняет их совместное использование для построения профиля ПАСВН.

4. Необходимость учета военного противоборства и обеспечения информационной безопасности

В настоящее время следует считать общепризнанным, что имеет место гибридная война и осуществляется информационное противоборство [см., например, 1,8]. Совершенно очевидно, что объектами кибератак служат объекты критической информационной инфраструктуры. Этим вопросам посвящен Федеральный закон «О защите критической информационной инфраструктуры. В этих условиях возникает проблема информационной безопасности, отраженная в действующей Доктрине информационной безопасности. Поскольку интероперабельность составляет основу ЕИП информационного пространства и информационной инфраструктуры КИИ (см. Рис. 3), то объектами атак и объектами защиты должны стать объекты интероперабельности. Это означает, что в профиль интероперабельности должны быть включены стандарты информационной безопасности. Для того, чтобы уточнить объекты защиты, необходимо учесть наличие модели информационных угроз и построить синтезированную модель интероперабельности и модели угроз.

5. Построение синтезированной модели интероперабельности и модели угроз

Прежде чем говорить о синтезированной модели рассмотрим модель интероперабельности и модель угроз по отдельности, а затем попытаемся осуществить синтез [9].

5.1. Модель интероперабельности для информационных систем военного назначения

В [2] нами предложена модель интероперабельности для информационных систем военного назначения (см. Рис. 4), представляющая собой расширение эталонной модели интероперабельности, зафиксированной в ГОСТ Р 55062-2012.

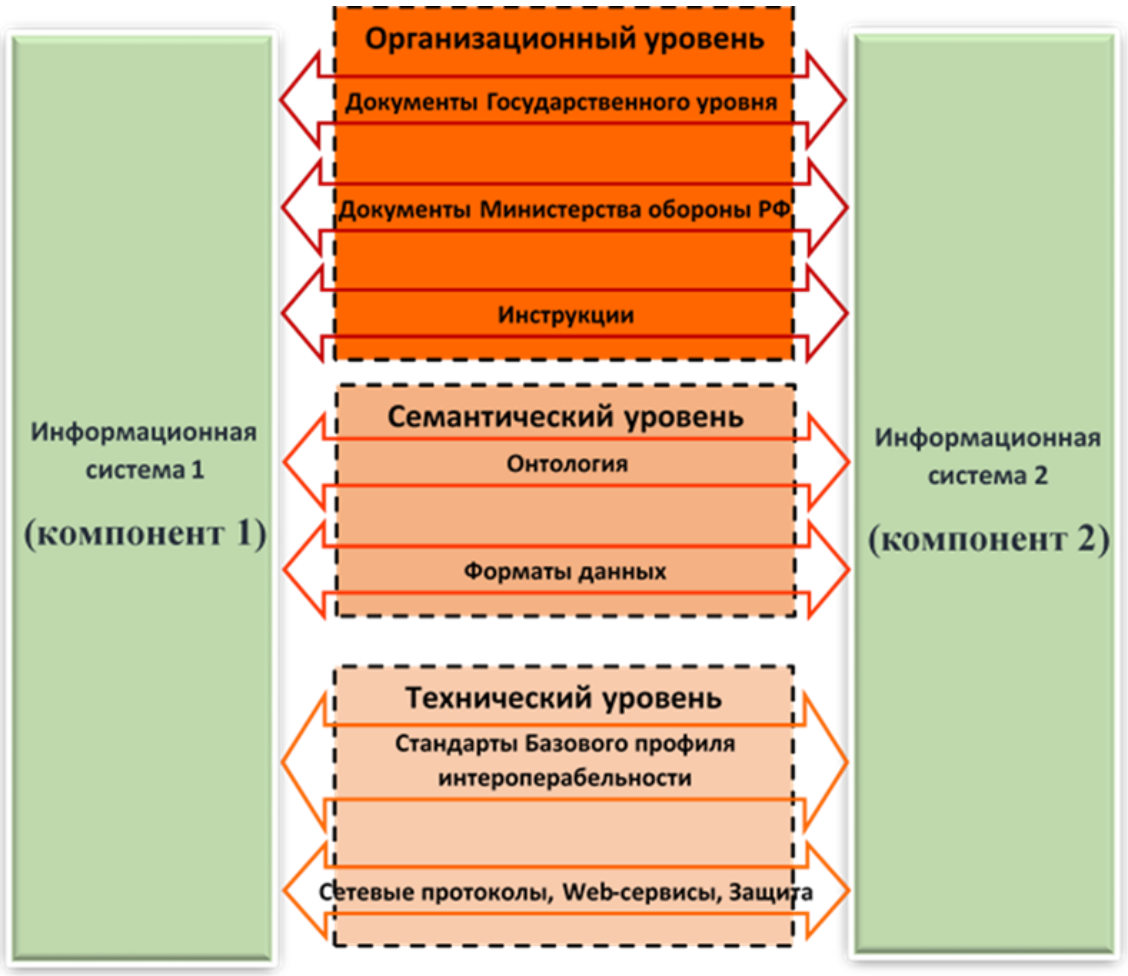

Рис.4 Модель интероперабельности для информационных систем военного назначения [2]

Безусловно, чтобы быть общепринятой и зафиксированной в соответствующем нормативном документе, модель требует коллективного обсуждения.

5.2. Модель угроз

Известно много источников, в том числе монографий [см., например, 1, 10, 11], где обсуждаются такие понятия, как информационная безопасность, защита информации, информационные угрозы и их классификация, модели информационных угроз, уязвимости, риски, стандарты информационной безопасности. Зачастую трактовка этих понятий в различных источниках отличается. Предпочтительным представляется использование терминов, содержащихся в стандартах – международных, отечественных государственных, гармонизированных с международными, стандартов организаций таких как документы ФСТЭК или документы Банка России. Таких

стандартов известно достаточно много (ГОСТ Р 52448-2005, ГОСТ Р 50922-2006, ГОСТ Р 51275-2006, ГОСТР 53114-2008, ГОСТ Р ИСО/МЭК 27002—2012 и др.). Из-за ограниченного объема журнальной статьи мы не будем проводить конкретного обсуждения всех стандартов. Отметим только, что графическое представление модели угроз, подобное приведенному на Рис.4, нам обнаружить не удалось, а имеется лишь описательное: «описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

Обобщив материалы из имеющихся источников, предлагаем в виде первого приближения синтезированную модель интероперабельности и модели угроз (см. Рис.5).

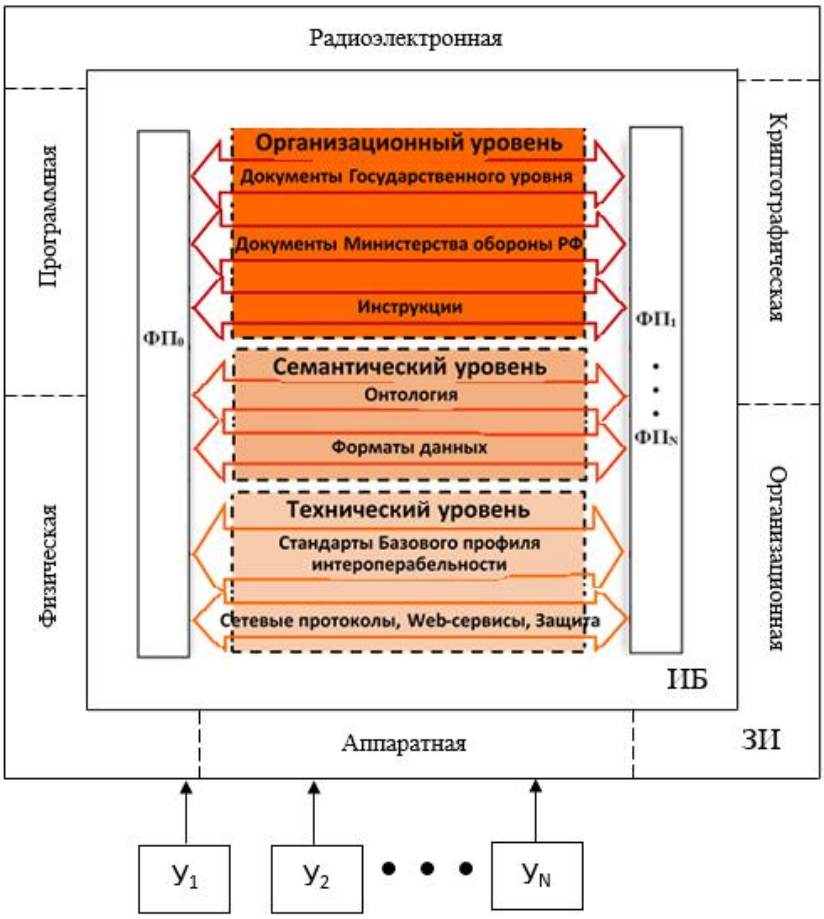

Рис. 5 - Синтезированная модель интероперабельности и модели угроз.

На рис.5 используются следующие сокращения: ФП0, ФП1,…ФПN – функциональные подсистемы; У1, У2, УN – угрозы информационной безопасности (конфиденциальности, целостности, доступности); ЗИ – виды защиты информации.

6. Обоснование комплекса мер по решению проблем на основе совершенствования процессов в жизненном цикле систем

Достижение интероперабельности – сложная комплексная проблема, имеющая научно-технические и организационно методические аспекты, и до конца не решенная во всем мире.

Первая мера должна быть связана с тем, что решение проблемы интероперабельности совместно с проблемой информационной безопасности должно осуществляться, практически на всех этапах жизненного цикла, предусмотренными в стандартах: ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», ГОСТ Р ИСО/МЭК 12207-99 «Информационные технологии. Процессы жизненного цикла программных средств» и ГОСТ Р ИСО/МЭК 15288-2005 «Информационная технология. Системная инженерия. Процессы жизненного цикла систем» Обратим внимание, что этапы методики обеспечения интероперабельности, приведенные на Рис. 2, в большой степени совпадают с этапами и стадиями приведенных стандартов. На стадии разработки концепции необходимо указать, что создаваемая ИС должна обладать свойством интероперабельности, на стадии разработки технического задания должны быть указаны стандарты, входящие в профиль. На стадии реализации ИС в нее должны входить технические и программные средства, соответствующие требованиям выбранных стандартов, для чего должно быть проведено аттестационное тестирование всех средств (см. этап «Аттестационное тестирование» на Рис.2.) В подтверждение сказанного можно указать, что в НАТО подобное тестирование ИС проводится регулярно.

Вторая мера должна заключаться в создании постояннодействующего рабочего органа по обеспечению интероперабельности, включающего три рабочих группы (см. Рис.6) с представителями ВС РФ, ОПК и других заинтересованных ведомств.

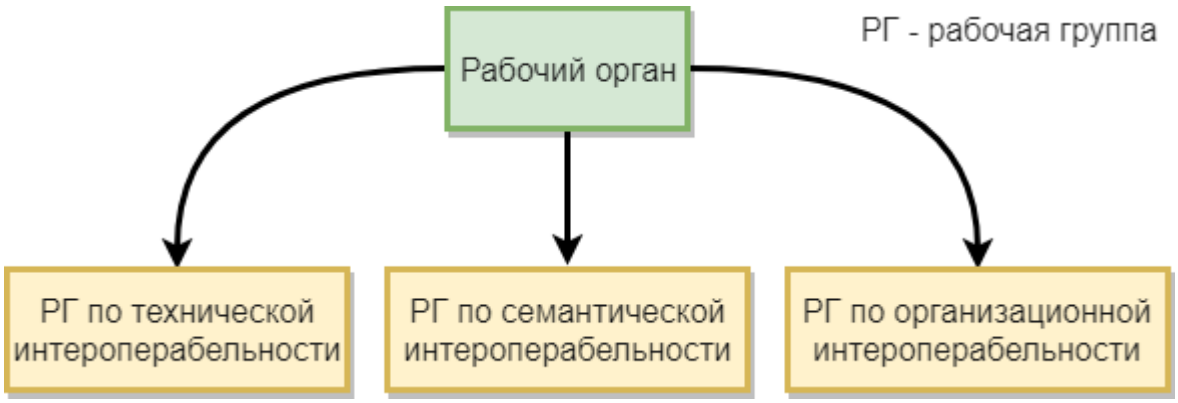

Рис. 6 Структура рабочего органа.

Пока такой орган не создан, целесообразно использовать возможности подкомитета ПК206 «Интероперабельность», входящего в состав Технического комитета ТК22 Росстандарта и созданного на базе Института радиотехники и электроники им. В.А.Котельникова РАН, что рекомендовано и научно-техническим советом Военно-промышленной комиссии.

Заключение

На основании изложенного можно сделать следующее заключение:

- обеспечение интероперабельности представляет собой наиболее эффективный и экономичный путь бесшовной интеграции функциональных подсистем в составе перспективных автоматизированных систем военного назначения;
- проблему интероперабельности следует решать совместно с проблемой информационного противоборства, для чего предложена синтезированная модель интероперабельности и модели угроз, и, в конечном счете, на следующих этапах работы в состав профиля должны быть включены стандарты информационной безопасности;

- обоснованы меры по решению проблемы интероперабельности, заключающиеся в дополнении этапов жизненного цикла информационной системы этапом аттестационного тестирования, в создании постояннодействующего рабочего органа по обеспечению интероперабельности и использовании возможностей подкомитета ТК206/ТК 22 Росстандарта «Интероперабельность» [12].

Литература

1. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. // С-Петербург, «Наукоемкие технологии», 2017. – 546 с.
2. Каменщиков А.А., Олейников А.Я., Чусов И.И., Широбокова Т.Д. Проблема интероперабельности в информационных системах военного назначения. // Журнал радиоэлектроники: электронный журнал. 2016, N11. URL: http://jre.cplire.ru/jre/nov16/8/text.pdf (дата обращения: 27.02.2018).
3. NATO standard ajp-6 allied joint doctrine for communication and information systems [Электронный ресурс]. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/602827/doctrine_nato_cis_ajp_6.pdf (дата обращения: 10.02.2018).
4. А.А. Зацаринный, Э. В. Киселев, Некоторые подходы к формированию нормативно-технической базы в части требований к архитектурному построению информационных систем организаций участников единого информационного пространства России, Системы и средства информ., 2015, том 25, выпуск 3, - С.179–194
5. Корниенко В.Н., Олейников А.Я. Обеспечение интероперабельности на основе использования стандартов информационно-коммуникационных технологий при межведомственном взаимодействии при решении задач в области обороны Российской Федерации // II Межведомственная научно-практическая конференция «Система межведомственного информационного взаимодействия при решении задач в области обороны

Российской Федерации»: сборник материалов. М.: Национальный центр управления обороной Российской Федерации, 2016. - С. 45-48.

6. Корниенко В.Н, Олейников А.Я. Современное состояние и перспективы продвижения проблемы интероперабельности в интересах обороны и безопасности Российской Федерации // III Межведомственная научно-практическая конференция «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации»: сборник материалов. М.: Национальный центр управления обороной Российской Федерации, 2016. - С. 74-77.
7. С. А. Головин, А. А. Зацаринный, С. В. Козлов, Научно-методические подходы к совершенствованию нормативной базы для создания и развития информационно-телекоммуникационных систем, Системы и средства информ., 2017, том 27, выпуск 2, С. 98–112
8. Башлыкова А.А., Олейников А.Я. Интероперабельность и информационное противоборство в военной сфере. // Журнал радиоэлектроники: электронный журнал. 2016, N12. URL: http://jre.cplire.ru/jre/nov16/8/text.pdf (дата обращения: 27.12.2016).
9. Олейников А.Я., Рубан К.А. Модели и стандарты обеспечения интероперабельности // Информатизация образования и науки, 2009, №3, - С. 24-34
10. Галатенко В.А. Основы информационной безопасности. Курс лекций. Учебное пособие. Третье издание. Интернет Университет информационных технологий. www.ituin.ru, Москва, 2006 г. 199 с.
11. Галатенко В.А. Стандарты информационной безопасности. 2-е издание исправленное. Национальный открытый Университет ИНТУИТ 2016 г. – 308 с.
12. Олейников А.Я., Чусов И.И. Проблема интероперабельности в Вооруженных силах РФ. // Вестник академии военных наук. – 2017. - №4. - С. 61-68.

Для цитирования:
А. А. Башлыкова, А. А. Каменщиков, А. Я. Олейников. Обеспечение интероперабельности как средства бесшовной интеграции функциональных подсистем в составе перспективных автоматизированных систем военного назначения. Журнал радиоэлектроники [электронный журнал]. 2018. № 9. Режим доступа: http://jre.cplire.ru/jre/sep18/11/text.pdf
DOI 10.30898/1684-1719.2018.9.11