УДК 004.728

ИНТЕРОПЕРАБЕЛЬНОСТЬ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В ВОЕННОЙ СФЕРЕ

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

[1] Московский технологический университет (МИРЭА), Москва

[2] Институт радиотехники и электроники им. В.А. Котельникова РАН, Москва

Статья поступила в редакцию 8 декабря 2016 г.

Аннотация. Рассмотрено состояние и перспективы развития двух важнейших направлений информационных технологий в военной сфере: обеспечения интероперабельности и информационного противоборства. Отмечается «антагонистический» характер названных направлений. Подчеркивается, что в современных методах ведения военных действий – сетецентрической войне, интероперабельность выступает как один их «краеугольных камней», и ее достижение представляет сложную научно- техническую и организационно-методическую проблему. Совершенно очевидно, что интероперабельность представляет один из главных объектов информационных атак при информационном противоборстве. Соответственно, обеспечение информационной безопасности и защита информации должны стать необходимыми условиями при обеспечении интероперабельности. Это требование должно сказаться на всех этапах достижения интероперабельности и, в конечном счете, на составе стандартов, входящих в профиль интероперабельности. Обозначены основные задачи, которые должны быть решены при решении проблемы интероперабельности с учетом информационного противоборства.

Ключевые слова: информационное противоборство, интероперабельность в информационной инфраструктуре, барьеры интероперабельности, вооруженные силы, профиль, информационное воздействие, синтетическая модель угроз.

Abstract. The state and prospects of development of the two most important areas of information technologies in the military sphere: the interoperability and information warfare are considered. "Antagonistic" character of these areas is mentioned. It is emphasized that in modern methods of warfare – network-centric warfare, interoperability stands as one of their «cornerstones», and its achievement is a complex scientific - technical and organizational-methodological problem from thus it followed. It follows that interoperability is one of the main targets of information attacks in information warfare. Accordingly, information security and data protection should become the necessary conditions for ensuring interoperability. This requirement should affect all stages of achieving interoperability and, ultimately, on the composition of the standards included in the interoperability profile. The key tasks to be solved in the process of interoperability problem solution taking into account the information warfare are designed.

Key words: information warfare, interoperability in the information infrastructure, barriers of interoperability, the armed forces, the profile, influence, synthetic threat model.

Введение

Настоящая статья представляет продолжение предыдущей публикации, посвящённой вопросам интероперабельности в Вооруженных силах Российской Федерации (ВС РФ) [1]. В [1] подчеркивалось, что во всех современных армиях мира, в том числе в ВС РФ, принята концепция сетецентрической войны (СЦВ). Отмечалось, что важнейшим требованием концепции сетецентрической войны служит обеспечение интероперабельности всех компонентов информационной инфраструктуры (ИИ). Отмечалось также, что в ВС США и объединенных силах НАТО имеются большое количество детальных материалов типа инструкций и директив, содержащих практические рекомендации по достижению интероперабельности. Достаточно сказать, что в самом свежем документе NATO (июнь 2016 г.), состоящем из трех томов общем количеством 227 страниц, содержатся названия более 500 стандартов [2,3,4]. К сожалению, в отечественных открытых источниках отсутствуют

материалы подобного рода. Авторы пришли к выводу, что недостаточное внимание к проблеме интероперабельности в ВС РФ несет угрозу национальной безопасности. На этом основании авторами выработаны конкретные предложения по достижению интероперабельности в ИИ Вооруженных Сил РФ. Предложения основаны на разработанном в Институте ранее и зафиксированном в ГОСТ Р 55062-2012 [5] едином подходе к обеспечению интероперабельности для систем широкого класса. Сделаны предложения по ключевым этапам единого подхода: концепции интероперабельности, архитектуре, модели интероперабельности и профилю. Авторы подчеркивали, что эти предложения следует рассматривать как первое приближение, для эффективного решения требуется привлечение гораздо больших сил и средств и в первую очередь создание коллективного органа (комитета, комиссии, рабочей группы). Предложения получили документированную поддержку от Национального Центра Управления Обороной РФ [6].

Авторы отдавали себе отчет, что при рассмотрении проблемы интероперабельности необходимо учитывать вопросы информационной безопасности (ИБ) и защиты информации (ЗИ), что особенно важно для ИИ ВС РФ, тем более в условиях информационного противоборства. Под информационным противоборством понимается борьба в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем (ИС) и ИИ от подобного воздействия. Конечной целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной, что как раз служит главной целью сетецентрической войны [7]. Важным фактором при подготовке представленной статьи послужила публикация новой версии Доктрины информационной безопасности Российской Федерации (Указ президента РФ №646 от 5 декабря 2016г.) [8] , в

которой естественно уделяется значительное внимание и ИБ в военной сфере, в частности говорится [8]:

П. 21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере.

Обеспечение ИБ и ЗИ само по себе - сложная научно-техническая и организационно методическая проблема, и ее совместное решение с проблемой интероперабельности более чем в вдвое увеличивает их сложность.

Отсюда следует цель данной работы: рассмотреть совместно аспекты интероперабельности и информационного противоборства и обозначить задачи, требующие решения в ВС РФ.

1. Поколения войн и роль интероперабельности

Представляется целесообразным отметить, что по одной из имеющихся классификаций войны можно разбить на поколения в соответствии с революционными изменениями в средствах ведения войны [10].

Проблема интероперабельности – обеспечения взаимодействия между участниками военных действий существовала столько же, сколько существуют войны, только менялись средства (голосовые команды, система жестов, зажигание сигнальных костров, сигнализация флажками, телефон, радио и наконец сегодня - сетевые цифровые технологии). Соответствие поколений и эпох представлены в таблице 1, которые можно рассматривать как развитие классификации, приведенной в [10].

Таблица 1. Поколения войн и эпохи

Поколение	**Характерный признак**	**Эпоха**
Первое	Применение холодного оружия:	Три с половиной тысячи лет шли контактные войны первого поколения в виде рукопашного противоборства с применением холодного оружия мячи копья, стрелы, и др..
Второе	Появление пороха и гладкоствольного оружия.	В XII-XIII веках прошлого тысячелетия первое поколение войн уступило место войнам второго поколения. Вторая революция в военном деле была связана с изобретением пороха, а с ним - огнестрельного оружия: винтовок, пистолетов, пушек. Произошел резкий, коренной переход от одних войн к другим. Войны второго поколения также были контактными, но велись уже совершенно иначе, чем в первом поколении. Поражение противника могло осуществляться на некоторой дистанции. Войны просуществовали порядка 600 лет.
Третье	Применение нарезного стрелкового оружия и артиллерии	Примерно 200 лет назад научно-технический прогресс способствовал изобретению нарезного оружия и технологии его производства. Оружие стало более точным при поражении целей, более дальнобойным, многозарядным и разнокалиберным. Это привело к очередной третьей революции в военном деле и появлению контактных войн третьего поколения, которые приобрели окопный характер, новые оперативные масштабы и требовали большого количества живой силы, владеющей этим оружием.
Четвертое	Применение автоматического оружия, танков, боевых самолетов, появление новых транспортных средств, средств связи	Более 100 лет назад снова произошла очередная, четвертая революция в военном деле ; связана с изобретением автоматического оружия, которое в больших количествах стали устанавливать на танках, самолетах, кораблях. Контактные войны приобрели стратегический размах, и для их ведения также требовалось очень много живой силы, оружия и военной техники. Требовались усилия по охране и обороне границы, поскольку все войны на границе. Войны, рожденные четвертой революцией в военном деле, продолжаются и сейчас.
Пятое	Возможность применения ядерно-ракетного оружия	В 1945 году произошла очередная, пятая революция в военном деле. Она была связана с появлением ядерного оружия, а с ним и впервые возможности бесконтактной ракетно-ядерной войны). Сейчас ряд ядерных стран находятся в постоянной высокой готовности к такой войне. Многие страны стремятся завладеть ядерным оружием. Однако есть надежда, что ядерное оружие не будет применено в войнах будущего, т.к. с его

		помощью нельзя добиться никаких целей.
Шестое	Определяющая роль информационно-коммуникационных технологий (ИКТ) – сетецентрическая война, высокоточное оружие, роботы.	Шестая революция в военном деле произошла на границе 20 и 21 столетия. Она связана, с развитием и применением ИКТ, в первую очередь для организации взаимодействия всех участников военных действий (Интернет) Совершенно очевидно, что и высокоточное оружие и роботы различного вида базирования не могут функционировать без использования ИКТ.

Таким образом, на границе 20 и 21 столетий в передовых армиях мира начался переход к войне 6-го поколения, когда ИКТ стали фактически видом оружия.

2. Интероперабельность. Основные понятия, роль стандартов, барьеры

Для дальнейшего изложения представляется целесообразным упорядочить некоторые понятия, используемые в материалах по интероперабельности. Так, часто используются понятия «Единое информационное пространство» (ЕИП) и «Информационная инфраструктура» (ИИ), и не всегда указываются их соотношение между собой и с другими понятиями.

На рис. 1 приведено соотношение этих понятий. Как видно на рис.1., имеется иерархия понятий, на вершине которой находится единое информационной пространство, а «фундаментом» служит интероперабельность.

Забегая несколько вперед, можно отметить, что нарушение интероперабельности с помощью средств информационной войны неизбежно приведет к разрушению всей иерархической структуры. В этом смысле ИИ ВС РФ с полным основанием следует отнести к критической ИИ.

Рис. 1. Соотношение основных понятий, связанных с проблемой интероперабельности

Для того, чтобы можно было говорить об этой иерархии, должна существовать соответствующая нормативная база (см. правую колонку на рисунке). В верхней части колонки должны существовать нормативно-правовые акты, соответствующие объему ЕИП (Указы, постановления правительства для ЕИП национального масштаба), на нижнем уровне - в первую очередь ИКТ-стандарты.

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 [11,12].

Что касается информационной инфраструктуры, в Доктрине информационной безопасности РФ [8] дано следующее определение:

Информационная инфраструктура Российской Федерации (ИИ РФ) - совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации [8].

Здесь следует отметить, что ИИ современных ВС, в том числе ВС РФ, относится к классу сверхбольших систем (англ. System of Systems- SoS) представляет собой сугубо гетерогенную среду, для которой проблема интероперабельности особо актуальна, а ее решение особенно сложно, даже при отсутствии внешних атак.

На основе приведенных понятий в [1] кратко описан единый подход к обеспечению интероперабельности и описано применение единого подхода к обеспечению интероперабельности в ВС РФ. Приведены основные положения концепции обеспечения в ВС РФ. В первую очередь, предложено определение понятия «Интероперабельность в ВС РФ:. «Способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена (ГОСТ Р 55062-2012 [5]). Это определение согласуется с определением, приведенном в международном стандарте ISO/IEC/IEEE 24765:2010(E) Systems and software engineering — Vocabulary [15].

Далее подчеркивается, что проблема интероперабельности в ВС РФ должна решаться на основе использования ИКТ-стандартов. Отмечается также, что Концепция обеспечения интероперабельности в ВС РФ непосредственно следует из Военной доктрины РФ (в редакции 2014 г.) [9], того положения, что ведение боевых действий, должно вестись на основе концепции СЦВ.

2.1. Архитектура Единого информационного пространства ВС РФ

В соответствии с Концепцией, ЕИП ВС РФ имеет архитектуру с тремя размерностями (см. рисунок 2).

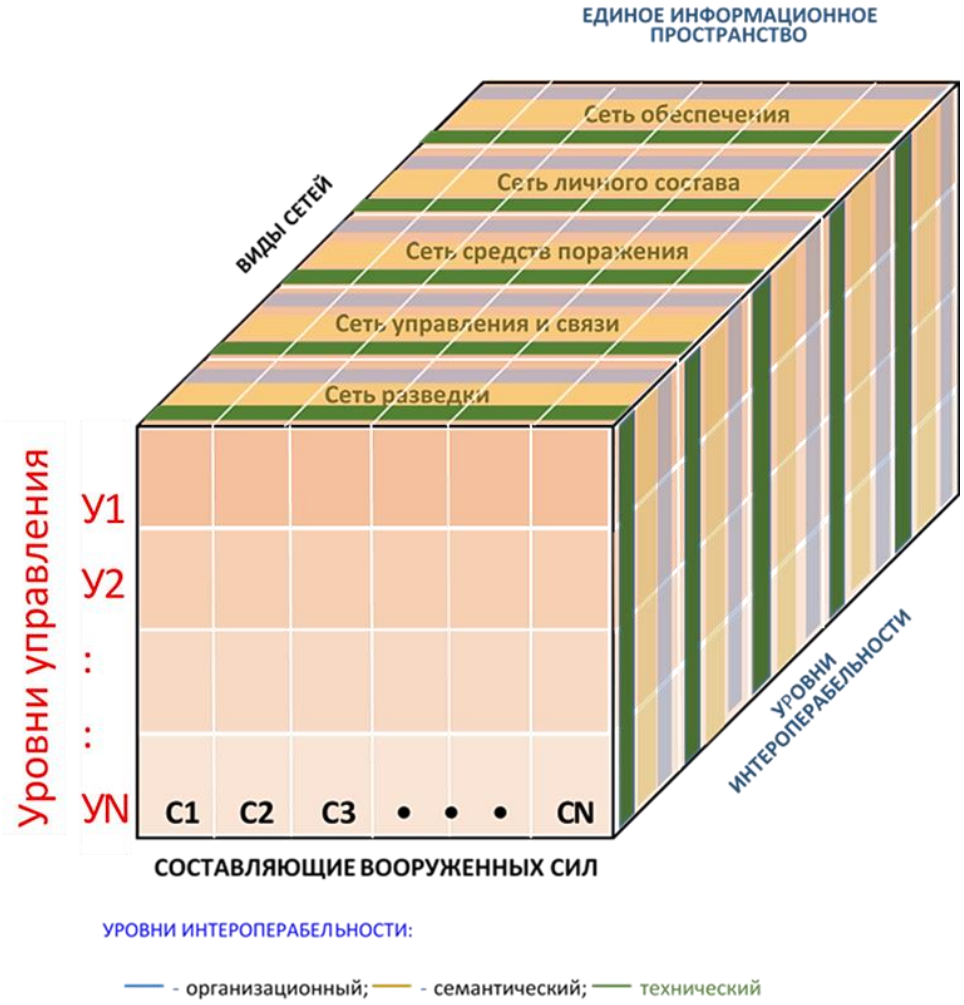

Рис. 2. Архитектура Единого информационного пространства ВС РФ [1]

По горизонтальной оси отложены составляющие ВС РФ (виды и рода войск), по вертикальной оси – уровни управления (от главнокомандующего до командира нижнего тактического звена). По третьей оси – функциональный разрез: сеть разведки, сеть управления и связи, сеть поражения, а также сеть личного состава и сеть обеспечения [1].

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).

2.2. Модель интероперабельности ВС РФ

Следующим этапом единого подхода [1] выступает построение проблемно-ориентированной модели интероперабельности, представляющей развитие эталонной модели интероперабельности, зафиксированной в ГОСТ Р 5506-2012. В [1] нами предложена следующая модель (см. рисунок 3).

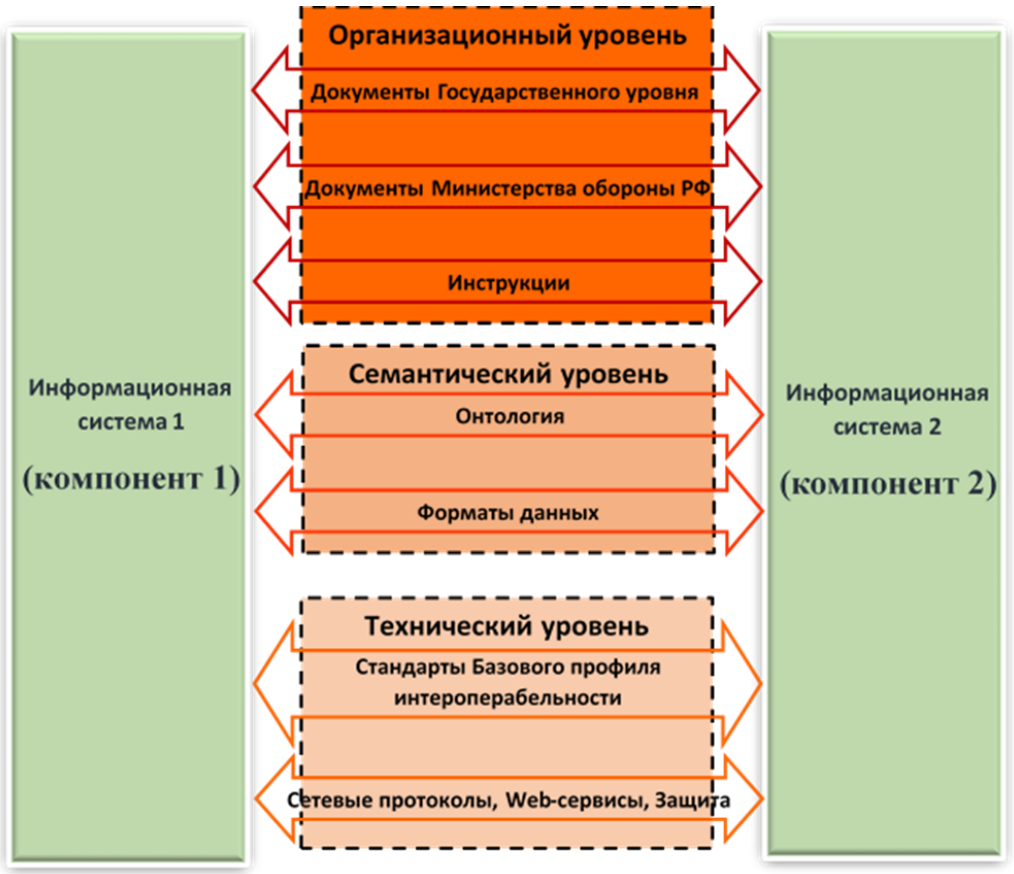

Рис. 3 Модель интероперабельности для информационных систем военного назначения [1]

При взаимодействии ИС через внешние среды, сервисы, могут возникнуть барьеры интероперабельности (interoperability barriers).

Подробно о барьерах интероперабельности сказано в ГОСТ Р ИСО 11354-1-2012 [17], в котором, выделены три категории барьеров: концептуальные, технологические и организационные.

Технологические барьеры интероперабельности проявляются в наличии технологического разрыва на этапах информационного взаимодействия; снижаются при закупке и перевооружении комплексов, входящих в ИИ и ЕИП ВС РФ.

Концептуальные барьеры характеризуются теми несовместимостями, которые не зависят ни от какой методики достижения интероперабельности. Концептуальные барьеры должны детализироваться с учетом синтаксических, семантических и семиотических несовместимостей обмениваемых элементов, в особенности - информационных активов и других активов, связанных со знаниями [17]. Концептуальные барьеры являются наиболее существенными для обеспечения интероперабельности из-за необходимости обмена содержанием между объектами, что в случае ИИ ВС РФ, затрудняется выполнением тайны передачи приказов и данных, с применением шифрования, криптографии и средств спецсвязи.

Организационные барьеры - это барьеры, дополняющие концептуальные барьеры (находящиеся в центре всех информационных проблем) и технологические барьеры, которые зачастую возникают благодаря человеческому фактору, но оказывают влияние на взаимодействие ИКТ-систем [17]. Когда организация и объект ВС РФ с ИИ обладают различными организационными структурами и процессами принятия решений, то перед началом совместных работ, необходимо привести структуры в соответствие, для препятствия развитию организационного барьера.

3. Информационная война и информационная безопасность

В последнее время все чаще поступают сообщения о кибератаках на различные объекты ИИ, в том числе было сообщено об атаке на отечественные банки как на важнейшую часть финансово-экономической системы страны. По существу, это идет проявление информационной войны. Как известно, информационная война (англ. Information war) [20] — термин, имеющий два значения, в первом значении этот термин следует рассматривать, как психологическую войну. Второе значение термина - более соответствующее цели нашей работы: целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам

противника при одновременной защите собственной информации, информационных процессов и информационных систем, что позволяет говорить об угрозах национальной безопасности Российской Федерации в информационной сфере. Усиление информационной войны и привело, по всей видимости, в появлению обновленной Доктрины информационной безопасности, ряд положений которой важны с точки зрения целей нашей работы.

Так, в Доктрине ИБ РФ [8] под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Доктрина ИБ РФ содержит ряд ключевых определений из области информационной безопасности, относящихся к политическим, правовым, организационным научно-техническим аспектам. Нас, как специалистов в области ИКТ, в первую очередь будут интересовать научно-технические аспекты, хотя они тесно увязаны с другими аспектами.

В разделе II «Национальные интересы в информационной сфере» говорится:

П. 7. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

В П.8 б) сказано: «Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее -

критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время.

Как видим, по существу говорится о поддержании интероперабельности ИИ, хотя этот термин и не употребляется, что только подтверждает то обстоятельство, что на государственном уровне проблеме интероперабельности не уделяется необходимого внимания.

В разделе III сказано: «Основные информационные угрозы и состояние информационной безопасности» подчеркивается, что «практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз».

Это утверждение, как видим, прямо относится к теме настоящей статьи - обеспечение интероперабельности в ИИ ВС РФ должно быть увязано с обеспечением ИБ.

В П. 11 подчеркивается, что одним из основных негативных факторов, влияющих на состояние ИБ, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на ИИ в военных целях. А в П. 15 еще сказано: «Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях ...».

В п. 20 сказано: «Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и

представляющих угрозу международному миру, безопасности и стратегической стабильности.

В П. 21 сказано: «В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

В П. 23 сказано: «Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры.

Таким образом, анализ Доктрины ИБ показывает, что проблема информационной безопасности первостепенной значение имеет для военной сферы, что и естественно, и, правда в неявной форме, касается проблемы интероперабельности.

4. Методы и средства защиты информации

Во всех странах правительства, озабоченные проблемой ИБ, придают этой проблеме и вопросам ЗИ большое значение. В нашей стране также этим вопросам уделяется весьма большое внимание и затрачиваются значительные ресурсы, в том числе разрабатываются соответствующие стандарты как на базе международных, так и «собственные».

Подходы к обеспечению ИБ и ЗИ, помимо стандартов [например, 22-27], регламентируются комплектом документов, выпущенных ФСТЭК России [21], включающим общие требования по обеспечению безопасности информации, рекомендации по ее обеспечению, базовую модель угроз и методику определения актуальных угроз безопасности информации [22-27].

Документы ФСТЭК регламентируют не только технические требования к средствам ЗИ в т.н. ключевой системе информационной инфраструктуры (КСИИ), но и требования к организации процессов управления ИБ КСИИ. В целом комплект документов по КСИИ представляет собой хорошо структурированный перечень требований и рекомендаций, построенных на основе анализа угроз и степени критичности ИИ, отнесенной к КСИИ. Документами предусмотрена классификация ИИ по назначению и уровням важности, от этого зависят требования к их защите.

В настоящее время в области обеспечения ИБ в ключевых системах ИИ разработана, утверждена и представлена в [21] система методических документов, основными из которых являются:

– «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»;

– «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»;

– «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

– «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

– «Положение о реестре ключевых систем информационной инфраструктуры».

Итак, применительно к ИИ ВС можно сделать вывод, что поскольку в условиях сетецентрической войны интероперабельность является необходимым условием, то первостепенное значение для достижения интероперабельности приобретают информационные угрозы, информационное противоборство и

методы обеспечения ИБ и ЗИ . Для учета этих факторов следует решить ряд задач.

5. Задачи, требующие решения

По итогам проведенного исследования, можно сформулировать предстоящие задачи:

– дальнейшее исследование проблемы интероперабельности, но с учетом информационных угроз, возникающих в условиях информационных войн и информационного противоборства;

– дальнейшее исследование методов и средств информационной войны, информационного противоборства с учетом того, что интероперабельность представляет один из основных объектов атак;

– развитие концепции обеспечения интероперабельности в ВС РФ с учетом информационных угроз.

– построение архитектуры информационной инфраструктуры ВС с выявлением объектов угроз ВС РФ и угроз, требующих обеспечения информационной безопасности и защиты информации;

– построение синтезированной модели интероперабельности и модели угроз;

– в терминах этой синтезированной модели должно быть проведено построение профиля интероперабельности, включающего стандарты информационной безопасности и защиты информации;

– желательна программно-аппаратная реализация хотя бы одного из компонентов ИИ ВС РФ с учетом профиля;

– проведение оценки урона интероперабельности в зависимости от объектов и уровня угроз;

– реализация вспомогательных этапов единого подхода обеспечения интероперабельности применительно к ВС РФ, в том числе разработка глоссария.

Заключение

Таким образом, на основании изложенного можно сделать следующее заключение:

– Показано, что при решении проблемы интероперабельности в Вооруженных Силах РФ, которая представляет «краеугольный камень» современного ведения боевых действий – сетецентрической войны, обязательно следует учитывать информационные угрозы, неизбежно возникающие в условиях информационной войны;

– учет этих угроз должен неизбежно сказаться на всех этапах достижения интероперабельности, в том числе на составе стандартов, входящих в профиль интероперабельности, а именно включать стандарты информационной безопасности и стандарты защиты информаци;

– проведено независимое рассмотрение проблемы интероперабельности в и проблемы информационного противоборства Вооруженных Силах РФ и показано, что их совместное решение абсолютно необходимо для современных ВС и, с другой стороны, представляется крайне сложным.

– перечислены задачи, которые предстоит решить.

Последующие работы авторов будут посвящены решению названных задач.

Литература

1. Каменщиков А.А., Олейников А. Я., Чусов И. И., Широбокова Т. Д. Проблема интероперабельности в информационных системах военного назначения.. Журнал радиоэлектроники [электронный журнал]. 2016, №11, URL: http://jre.cplire.ru/jre/nov16/8/text.pdf

2. Интероперабельность. Стандарты и профили НАТО. Том 1 Введение (издание 2015 г.), Союзная публикация 34 (ADatP-34(I)) Отдел обеспечения интероперабельности профилей СЗВ, 6.06.2016г. – 34стр.

3. Стандарты и профили интероперабельности НАТО Том 2 Утвержденные стандарты (версия 2015 года) Союзная публикация 34 (ADatP-34(I)) Отдел обеспечения интероперабельности профилей С3В, 2015г.– 50 стр.

4. Стандарты и профили интероперабельности НАТО Том 3 Профили (Издание 2015) Публикация данных союзников 34 (ADatP-34(1)) Отдел обеспечения интероперабельности профилей С3В,6.06. 2016г.– 143 стр.

5. 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: 14.11. 2016г.).

6. 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: 29.11 .2016).

7. Информационное противоборство, википедия, http://ru.rfwiki.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2%D0%BE%D0%B1%D0%BE%D1%80%D1%81%D1%82%D0%B2%D0%BE (дата обращения 20.11.2016г).

8. Доктрины информационной безопасности Российской Федерации (Указ президента РФ №646 от 5 декабря) http://docs.cntd.ru/document/420384668 (дата обращения 10.12.2016г.)

9. 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: 29.10.2016).

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: 27.11.2016).

11. Единое информационное пространство, http://life prog.ru/view_zam2.php?id=104& (дата обращения: 27.11.2016).

12. 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: 03.11.2016).

13. Баранюк В.В., Основные направления создания единого информационного пространства ВС РФ «Военная мысль» №11. 2004г.(стр.29-34) режим доступа http://militaryarticle.ru/voennaya-mysl/2004-vm/9421-osnovnye-napravlenija-sozdanija-edinogo (дата обращения 08.11.2016).

14. Копытко В.К., Шептура В.Н., Проблемы построения единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения, 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?limitstart&showall=1 (дата обращения 08.11.2016).

15. ISO/IEC/IEEE 24765:2010(E) Systems and software engineering — Vocabulary – 15.12.2010г.

16. Кондратьев А. Е. Будущее сетентрических войн [электронный ресурс]. URL: http://www.mirprognozov.ru/prognosis/politics/buduschee-setetsentricheskih-voyn/

17. 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: 27.10.2016).

18. Эмерджентность, «системный эффект». Источник: Википедия http://ru.wikipedia.org/wiki/ (дата обращения: 27.10.2016).

19. Кибернетические протесты http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2002-zvo/6859-amerikanskie-jeksperty-ob-jeskalacii (дата обращения: 27.10.2016).

20. Информационная война [электронный ресурс] URL: https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0 (дата обращения: 30.10.2016).

21. Руководящий документ ФСТЭК «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 25 июля 2014 г. N 240/22/2748

22. ГОСТ Р ИСО/МЭК_15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель, 2013г

23. ГОСТ Р ИСО/МЭК ТО 15446 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности , 2009г.

24. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности, 2011г.

25. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения, 2008 г.

26. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения, 2014г.

27. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения, 2009 г.