УДК 621.396

Интероперабельность, информационное противоборство и радиоэлектронная борьба

Р.П. Быстров – д.т.н., профессор, академик Академии военных наук, чл.-корр. академии инженерных наук, вед. науч. сотрудник ИРЭ им. В.А. Котельникова РАН
E-mail: rudolf@cplire.ru
В.Н. Корниенко – к.ф-м.н., зам. директора, ИРЭ им. В.А. Котельникова РАН
E-mail: korn@cplire. ru
А.Я. Олейников – д.т.н., профессор, гл. науч. сотрудник, ИРЭ им. В.А. Котельникова РАН
E-mail: olein@cplire.ru

Приведен анализ зарубежных и отечественных источников по таким понятиям, как военное противоборство (сецецентрические и электронные войны), имеющих место в настоящее время. Рассмотрены современные направления в области развития и применения информационно-коммуникационных систем в условиях уже ведущейся гибридной войны: обеспечение интероперабельности при создании критической информационной инфраструктуры в условиях информационного противоборства и возможности в данных условиях ведения радиоэлектронной борьбы. Показано, что эти тенденции можно рассматривать как «антагонистические», порождающие усиление задачи обеспечения информационной безопасности, которые должны рассматриваться в совокупности. Указаны отдельные варианты возможной оценки функционирования интероперабельности. Отмечен задел, имеющийся в ИРЭ им. В.А.Котельникова РАН по названным направлениям с предложениями объединить ведущиеся работы в одно из главных направлений работ института.

Ключевые слова: *сетецентрическая война, электронная война, критическая информационная инфраструктура, интероперабельность, стандарты, информационное противоборство, информационная безопасность.*

The analysis of the foreign and domestic sources on such concepts as military confrontation (net centric and electronic wars) taking place in now is carried out. The modern directions in the field of development and use of information and communication systems in the conditions of already conducted hybrid war are considered: ensuring interoperability at creation of critical information infrastructure in the conditions of information antagonism and opportunity in these conditions of conducting radioelectronic fight. It is shown that these tendencies can be considered as the «antagonistic», generating strengthening problems of ensuring information security which have to be considered in total. Separate options of a possible assessment of functioning of interoperability are specified. The reserve which is available in Kotelnikov IRE of the Russian Academy of Sciences in the called directions to them is noted with offers to unite the conducted works in one of the main directions works of Institute.

Keywords: *network-centric war, electronic war, critical information infrastructure, interoperability, standards, information antagonism, information security.*

Цель работы – рассмотреть современные направления в области развития и применения информационно-коммуникационных систем в условиях уже ведущейся гибридной войны.

В работах [1–6] констатируется, что в настоящее время в области развития и применения информационно-коммуникационных технологий (ИКТ) наблюдаются две тенденции, которые можно рассматривать как антагонистические. Первая тенденция состоит в построении Единого информационного пространства (ЕИП) на основе использования принципов интероперабельности. Вторая тенденция состоит в развитии информационного противоборства, направленного на разрушение интероперабельности как основы ЕИП. Обе названные тенденции являются результатом развития и применения информационно-коммуникационных технологий (ИКТ) и их следуют рассматривать во взаимодействии. Поэтому на данном этапе исследований понятия интероперабельности является целесообразным рассмотреть основные понятия из области сетецентрической войны, интерпоерабельности, информационного противоборства, радиоэлектронной борьбы как старейшего вида информационного противоборства. Из проблемы информационного противоборста следует и проблема информационной безопасности. В настоящее время уже имеются важные достижения в названных областях, что и рассматривается также в настоящей статье. Подчеркивается целесообразность совместно рассмотрения названных технологий и их совместное взаимодействие. Вот в такой последовательности по тексту и освещаются все имеющие основные и важные поставленные здесь научные вопросы.

Сетецентрическая война

Основные понятия.

Сетецентрическая война (СЦВ) и кибервойна (КВ) – концепции, ставшие реальностью в XXI веке, хотя до сих пор нет общего понимания и согласия среди зарубежных и российских экспертов. По мнению некоторых из них, США уже «… адаптировали свои вооруженные силы к ведению сетецентрических войн» [7]. Утверждается, что военные возможности, прежде всего в области управления, определяются в решающей степени общим состоянием технологической базы и информатики в обществе и государстве. И, прежде всего, речь всегда идет, конечно, о главной области военного искусства – военной стратегии, но и не только. В оперативном искусстве и тактике за последние десятилетия произошли принципиальные перемены, которые требуют от государств радикального пересмотра прежних военных доктрин и критической переоценки всего спектра областей военного искусства. По сути дела сегодня речь идет уже о появлении нового военного искусства, когда прежние оценки, опыт и знания требуют радикального пересмотра, либо даже отказа от прежних взглядов. В первую очередь – в области военно-политического управления, вооружениями и управления стратегическими наступательными и оборонительными войсками. Достаточно сказать, что в последние годы фактически отпала необходимость в массированном использовании сухопутных войск, когда армии воевавших сторон насчитывали миллионы человек, а численность танков и самолетов измерялась десятками тысяч.

Эта изменения затронули, прежде всего, те виды вооруженных сил, которые зависели от этих двух факторов – стремительного развития информатики и связи, и расширении пространственного охвата до космоса и киберпространства. Речь идет о системах ПВО и ПРО, которые, по сути, носят глобальный характер. Даже если районы дислокации противоракет ограничены, пространство (воздушно-космическое и информационное) выходит далеко за пределы национальных территорий. И эти изменения в [8] определяются для военной сферы, следующими особенностями:

область информационного противоборства изначально глобальна и не может быть ограничена ни отдельным ТВД, ни временем, ни системой оружия или военной техники;

эта область не поддается контролю или ограничению за исключением крайне редких случаев (например, ограничений по развертыванию РЛС), то есть не может стать предметом договоренностей;

область информационного противоборства не имеет четких границ ни между формами использования («мягкой» или «жесткой») силы, ни между соответствующими средствами (СПП, например, выполнял в Ираке важную функцию управления);

информационные средства применительно к ВКО фактически являются как частью СЯС, так и средств собственно ВКО. Не только военные, но и гражданские технологии становятся критически важными для ВКО.

При этом считается, что эти особенности и изменения в конечном счете привели к пересмотру многих основополагающих взглядов на военное искусство и военное строительство в начале XXI века, «… воплотившись, – как отмечают эксперты, – в концепцию «сетецентрической войны» (в англоязычной транскрипции – Network Centric Warfare).

Таким образом, концепция сетецентрической войны предоставляет бесспорное преимущество такому государству (или коалиции государств), которое [9]:

во-первых, имеет технологическое превосходство в области информационных технологий самого широкого спектра. В этом смысле сегодня и в среднесрочной перспективе единственным государством, имеющим такое превосходство, являются Соединенные Штаты. Отставание России в этой области является критическим и до сих пор по достоинству недооценивается. Это отставание не может быть ликвидировано технологическими заимствованиями. Хотим мы того или нет, но России нужна сверхпрограмма развития собственных информационных технологий на базе собственных достижений в фундаментальной науке;

во-вторых, политическое, экономическое и финансовое положение США, в том числе и позиции американского доллара, предопределяются, прежде всего, технологическим превосходством США и в создании самых современных концепций и их использования, таких, как «кибероперации», «информационная» или «сетецентрическая война»;

в-третьих, концепции информационных войн позволяют создать потенциал и предоставить возможность ведения любых войн в глобальном масштабе на любом театре ТВД, на любом пространстве – земле, воде, воздухе или в космосе.

Сегодня угроза потери управления рассматривается, прежде всего, как угроза возможного уничтожения центров управления и связи в результате первого удара, что уже не совсем соответствует реалиям. Соответственно и основные усилия направлены на предупреждение о таком нападении.

В последнее время при рассмотрении аспекта в области понятия «сетецентрическая война» стало применяться такое выражение, как «электронная война» [10].

Что понимантся в настоящее время под этим понятием? Прежде всего – это одна из важных составляющих системы сетецентрических войн в информационном противодействия, где в заключительных этапах ее – использование методов РЭБ. При этом особенно важными действиями считаются проведение мер по радиоэлектронной разведке, безопасности и живучести.

В [10] хорошо поясняется, что за последнее время российские средства радиоэлектронной борьбы приобрели ореол некоего супероружия, способного, по мнению обывателей, только одним своим включением вызвать панику у вероятного противника. Поэтому здесь показываются передовые возможности технических средств РЭБ отечественных образцов в сравнении с основными зарубежными образцами. Отмечается, что такие работы местами дублируются и пересекаются, но не следует забывать и о таком явлении, как лоббизм определенных разработок и фирм. Первой попыткой реорганизовать работы в области создания РЭБ стало недавнее назначение указом президента генерального конструктора по направлению РЭБ. Но насколько уникальными средствами РЭБ обладает российская армия, и насколько будет эффективно это решение, покажет время.

Теперь целесообразно рассмотреть вопрос о названных выше тенденциях в области информационно-коммуникационных технологий.

Развитие и применение информационно-коммуникационных технологий.

Как уже говорилось, одна из тенденций состоит в создании ЕИП различного масштаба, построенного на соответствующей информационной инфраструктуре (ИИ), объединяющей информационные и вычислительные ресурсы средствами телекоммуникаций. Утверждается, что фундаментом этой конструкции должна служить интероперабельность и ИКТ-стандарты.

Вторая тенденция состоит в ведении информационного противоборства или кибервойны. Кибервойна ведется как в мирное время, так и во время боевых действий, и получила название гибридной войны.

Далее можно утверждать, что основными объектами кибератак при кибервойне должны стать именно компоненты, обеспечивающие интероперабельность. Поэтому должны быть предприняты особые меры по обеспечению их информационной безопасности, в том числе должны использоваться стандарты информационной безопасности. Констатируется, что наиболее апробированным видом информационного противоборства выступают средства РЭБ.

Какой же задел в этом направлении уже имеется?

Рассмотрим основные понятия из этих сфер: интероперабельности, информационного противоборства, информационной безопасности и радиоэлектронной борьбы, и проведем сравнительный анализ состояния работ за рубежом и в нашей стране в гражданской и военной области с учетом опыта работ специалистов Института радиотехники и электроники им В.А.Котельникова РАН.

Подчеркнем необходимость решения проблемы интероперабельности в условиях информационного противоборства и радиоэлектронной борьбы. Недаром в Военной доктрине РФ эти три направления сведены в одном пункте 46, где названы: г) качественное совершенствование средств информационного обмена на основе использования современных технологий и международных стандартов (читай «*обеспечение интероперабельности*»), а также ЕИП Вооруженных Сил, других войск и органов как части ЕИП Российской Федерации; в) развитие сил и средств *информационного противоборства*; е) создание новых образцов высокоточного оружия и средств борьбы с ним, средств воздушно-космической обороны, систем связи, разведки и управления, *радиоэлектронной борьбы*, комплексов беспилотных летательных аппаратов, роботизированных ударных комплексов, современной транспортной авиации, систем индивидуальной защиты военнослужащих; ж) создание базовых информационно-управляющих систем и их интеграция с системами управления оружием и комплексами средств автоматизации органов управления стратегического, оперативно-стратегического, оперативного, оперативно- тактического и тактического масштаба».

Здесь следует подчеркнуть, что проблемы интероперабельности, информационного противоборства, радиоэлектронной борьбы и особенно их совместное решение имеют целый ряд фундаментальных и

прикладных аспектов, на которых далее целесообразно и остановиться. Особое место в рассмотрении этих вопросов занимает проблема интероперабельности.

Проблема интероперабельности

Основные понятия.

Для дальнейшего изложения представляется целесообразным упорядочить некоторые понятия, используемые в материалах по проблеме 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 [11]. Как следует из рис. 1, имеется иерархия понятий, на вершине которой находится ЕИП, а «фундаментом» служит интероперабельность.

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

Интероперабельность представляет одно из трех свойств открытых систем [12] и определяется следующим образом: «способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена» [3].

Забегая несколько вперед, можно отметить, что нарушение интероперабельности с помощью средств кибервойны неизбежно приведет к разрушению всей иерархической структуры, приведенной на рис. 1.

Следует сказать, что в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации», введенном в действие с 1 января 2018 г., приведены такие понятия как «критическая информационная инфраструктура» и объекты критической информационной инфраструктуры:

критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

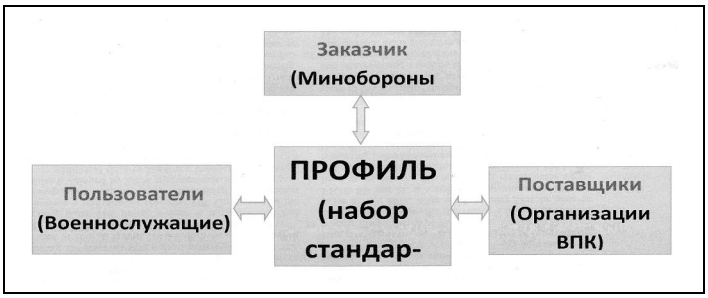

Рис. 2. Роль профиля для достижения интероперабельности(на примере профиля ВС РС)

Важнейшим понятием из области интероперабельности служит понятие «профиля». Согласно мировому опыту, эта проблема решается на основе использования согласованных наборов ИКТ-стандартов – профилей, оформленных, как нормативно-технический документ.

Профиль нужен для того, чтобы пользователи, заказчики и поставщики ИКТ-продуктов могли найти общий язык, чтобы новый ИКТ-продукт легко встраивался в имеющуюся ИИ (рис. 2). Следует отметить, что применение ИКТ крайне важно в системе предприятий оборонно-промышленного комплекса (ОПК), где имеется собственное ЕИП, пересекающееся с ЕИП ВС РФ [13], а следовательно в ОПК должен быть профиль, пересекающийся с профилем ВС РФ.

Уместно также отметить, что в хорошо известном стандарте ГОСТ 34 «ТЗ на создание и модернизацию ИС» имеются пункты, фактически регламентирующие необходимость использования профилей, п.4.1.1.3 «Требования к характеристикам взаимосвязей создаваемой системы со смежными системами» и пп.4.1.13 «Требования по стандартизации и унификации». Но трудно сказать, насколько они выполняются в реальной деятельности по созданию информационных систем (ИС).

Технология достижения интероперабельности – инновационная технология двойного назначения. Необходимо отметить, что обеспечение интероперабельности – сложная научно-техническая и организационно методическая проблема, до конца еще нерешенная во всем мире. Сложность проблемы объясняется тем, что кроме нижнего т.н. «технического» уровня интероперабельности существуют еще более высокие уровни – семантический и др.

Опыт ИРЭ им В.А.Котельникова РАН.

В ИРЭ им. В.А.Котельникова РАН первые работы по интероперабельности были начаты в 1980-х гг., когда решалась проблема автоматизации научных исследований и создания стандартного интерфейса между ЭВМ и экспериментальными установками. Тогда совместно с СКБ РАН, а также с рядом научных и промышленных предприятий были проведены исследования и разработки, налажен производственный выпуск аппаратуры в международном стандарте КАМАК [14]. Позже, после того, как в страну стала поступать разнородная вычислительная техника, стали активно развиваться средства коммуникаций и возникла гетерогенная ИКТ-среда, в которой возникла проблема совместимости и взаимодействия разнородных компонентов.

В ИРЭ им. В.А.Котельникова РАН систематизированные работы по проблеме интероперабельности начали проводиться, начиная с 2007 г., и к настоящему времени сделано достаточное количество научно-технических публикаций, разработано более 10 стандартов. Наиболее значимым следует считать предложенный единый подход, в котором на основании обобщения большого международного и значительного собственного опыта предложен единый подход к обеспечению интероперабельности ИС самого широкого класса – систем различного масштаба (от наносистем до сверхбольших систем – System of Systems) и систем различного назначения. Предложенный единый подход к обеспечению интероперабельности, последовательно был зафиксированн впоследствии в государственном стандарте ГОСТ Р 55062-2012 [12]. Интенсивное применение ИКТ в различных организациях (организациях, предприятиях, исследовательских, образовательных, лечебных учреждениях, военных и др.) привело к обобщенному понятию «электронное предприятие» (E-enterprise). Соответственно, возникло понятие «интероперабельность предприятия» (Enterprise Interoperability). При едином подходе, в зависимости от конкретной области применения и особенностей ИС данного класса, получаемые решения отличаются, что проявляется в составе стандартов профиля. На рис. 3 приведена структурная схема процесса по достижению интероперабельности.

Последовательная реализация этапов 1…5 должна привести к созданию интероперабельной системы. Для успешной реализации всего процесса достижения интероперабельности необходимо также создать «Дорожную карту разработки стандартов» и разработать необходимые стандарты с их постоянной актуализацией. Кроме того, необходимо разработать глоссарий (термины и определения), чтобы все участники (пользователи, разработчики ИС и поставщики программно-аппаратных средств) на всех этапах достижения интероперабельности могли находить взаимопонимание.

Последние годы в соответствие с предложенной блок-схемой (рис. 3) в ИРЭ им В.А. Котельникова РАН ведутся работы по применению предложенного подхода к ИС различного назначения. В 2016 г. было предложено применение единого подхода к системам военного назначения [15,16]. Совершенно очевидно, что совокупность ИС военного назначения составляет одну из важнейших, если не важнейшую критическую инфраструктуру РФ, поэтому результаты исследований были доложены нами на II и III конференциях по межведомственному взаимодействию, которые проводились Национальным Центром управления обороной РФ. В решении II конференции, доложенном начальнику Генштаба, отмечалась *«целесообразность рассмотрения проблемы обеспечения интероперабельности с учетом реализации положений военной доктрины Российской Федерации, утвержденной Президентом Российской Федерации 25 декабря 2014 г., как одно из важнейших средств повышения эффективности и безопасности функционирования системы государственного и военного управления, обеспечения информационною взаимодействия между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, иными государственными органами при решении задач в области обороны и безопасности».* В решении III Конференции эта формулировка была усилена. Однако следует признать, что реальных действий не предпринято, хотя разрыв в уровнях работ по проблеме интероперабельности за рубежом, в том числе в НАТО, и в РФ становится критическим и несет угрозу обороноспособности и национальной безопасности РФ.

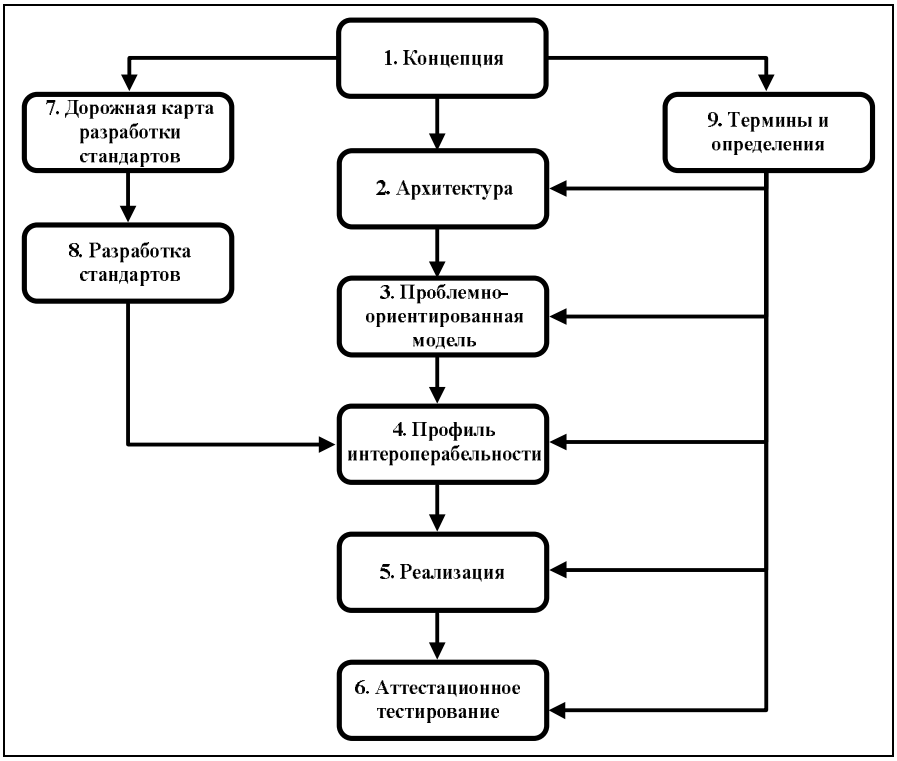

Рис. 3. Схема процесса обеспечения интероперабельности

Рис. 4. Место ПК206 при разработке профилей

Можно предположить, что основная причина, почему не решается проблема интероперабельности – общее отставание РФ в области развития и применения ИКТ. Об этом говорит значение т.н. «Индекса развития ИКТ» (ООН) – Information development index (IDL). Это – комбинированный показатель, характеризующий достижения стран мира с точки зрения развития ИКТ. По результатам 2017 г. РФ занимает 45 место из 176 стран.

Создание подкомитета «Интероперабельность».

Учитывая постоянно возрастающую актуальность решения проблемы интероперабельности, как в гражданской, так и в военной областях [16,17], мы убежденно считаем, что должен быть создан межведомственный постояннодействующий орган по решению проблемы интероперабельности. До его создания на базе ИРЭ им. В.А. Котельникова РАН в рамках технического комитета Росстандарта ТК22 «Информационные технологии» создан подкомитет ПК206 «Интероперабельность». Схемное представление в разработке профилей ИТ стандартов приводится схематично на рис. 4. В данном случае отмечено, что начало данной работы оценивается как «стартовая» площадка для уменьшения разрыва с зарубежными работами по интероперабельности. Основной задачей здесь является разработка профилей для различных областей, в первую очередь для ВС РФ и ОПК РФ. Использование возможностей ТК206 для предприятий ОПК рекомендовано НТС ВПК.

Весь последний мировой опыт показывает, что проблему интероперабельности необходимо решать совместно с проблемой информационного противоборства.

Информационное противоборство

Поколения войн.

На рис. 5 в несколько упрощенном виде приведена классификация войн. Как известно, традиционно войны делились на «горячие» и «холодные», причем горячие войны принято делить по поколениям [11] в соответствии с новым видом применяемого оружия. Начиная с границы XX и XXI веков таким оружием стали ИК-технологии. В первую очередь речь идет о сетецентрической войне, о высокоточном оружии и о роботах.

Рис. 5. Классификация войн

Холодные войны тоже можно разделить на два поколения, и признаком второго поколения также следует считать использование ИКТ, создание и использование информационных войск.

Наконец, в последние годы появился термин «гибридная война», само название которой говорит само за себя, хотя это понятие гораздо более сложное.

Непосредственно с приведенными выше понятиями связано понятие информационного противоборства, поскольку в любой войне есть, как минимум, две противоборствующие стороны.

Тематика информационного противоборства в широком смысле этого слова возникла гораздо раньше, чем тематика, связанная с интероперабельностью. По этой тематике имеется весьма значительное число публикаций, а также официальных документов, как зарубежных, так и отечественных, в том числе имеются и монографии [18–21]. В [21] присутствуют два раздела, посвященных информационному противоборству: «Информационное противоборство в технической сфере» и «Информационное противоборство в психологической сфере». Нас, конечно, в первую очередь интересует техническая сфера, связанная с технической интероперабельностью, однако можно высказать предположение, что информационное противоборство в психологической сфере может касаться интероперабельности на семантическом уровне, например операции, направленные на затруднение взаимопонимания сторон или лиц, принимающих решения. Ценность монографии [21] состоит в том, что в ней приведена терминология из области информационного противоборства и классификация большинства известных методов и средств из этой области.

Информационное противоборство.

В первую очередь, приведем определение понятия «Информационное противоборство»: *Информационное противоборство – 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 и информационной инфраструктуры от подобного воздействия. Целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной* [19].

Хотелось бы обратить внимание на то, что в приведенном определении в качестве объекта деструктивного воздействия и одновременно защиты служит информационная инфраструктура. А выше показано, что интероперабельность представляет собой фундамент информационной инфраструктуры, то есть

можно сделать вывод, что объектом деструктивного воздействия и защиты должна служить интероперабельность.

Военные аналитики США сравнивают ущерб от нарушения функционирования информационных систем страны с последствиями применения стратегического ядерного оружия.

При этом информационное противоборство ведется постоянно – как в мирное, так и в военное время. Оно может вестись не только между государствами-противниками, но и между государствами-союзниками во имя достижения своих целей в коалициях [20,21].

В [21] приведены и другие определения из области информационного противоборства, такие как «информационная операция», «информационное оружие». Рассмотрена классификация технологий информационного противоборства, обеспечивающих разработку и применение информационного оружия, классификация информационно-технического оружия, классификация информационно-технических воздействий, классификация удаленных сетевых атак, классификация способов осуществления удаленных сетевых атак, классификация наиболее распространенных способов осуществления атаки «отказ в обслуживании», классификация компьютерных вирусов. С точки зрения интероперабельности как объекта воздействия интересна классификация по уровням эталонной модели OSI, на котором осуществляется воздействие [19]: физический, канальный, сетевой, транспортный, сеансовый; представительный, прикладной. Как отмечено в [11], эталонная модель интероперабельности может рассматриваться как развитие эталонной модели OSI, и в этом смысле приведенная выше классификация может быть дополнена по крайней мере «семантическим» уровнем. Приведены наиболее важные и поздние официальные документы США и НАТО в области информационного противоборства. К этим документам относятся: Отчет Rand Corp MR-963-OSD The Day After … in the American Strategic Infrastructure, National Security Strategy of the United States of America, Cyber Electronics In Full-Spectrum Operations Concept, Cyber Vision 2025.

В РФ в последнее время все большее значение придается вопросам информационного противоборства. Так, в России был создан центр (Ростех) противодействия угрозам [21,22]. Отмечается, что в «Ростехе» организован Корпоративный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак, задача которого – обеспечение электронной защиты предприятий госкорпорации (КЦПКА). С момента создания его сотрудники уже отразили десятки киберугроз, в постоянном режиме осуществляет мониторинг компьютерных систем на оборонных заводах. При фиксации каких-либо отклонений от нормы сотрудники центра должны блокировать утечку стратегических данных и извещать ФСБ о попытке взлома. КЦПКА будет частью государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, осуществляющим защиту информации в корпоративном сегменте. Этот проект ГосСОПКА, реализуемый ФСБ, объединит множество аналогичных организаций с территориальной и ведомственной спецификой ФСБ. ГосСОПКА будет сформирована из главного, региональных и территориальных центров, соответствующих подразделений государственных органов и корпоративных объектов, одним из которых будет новая структура «Ростеха». Структурная схема взаимодействия подразделений в рамках проекта ГосСОПКА приводится на рис. 6.

Предусматривается, что КЦПКА будет защищать критически важные объекты оборонной промышленности, к которым относятся подразделения Объединенной приборостроительной корпорации, Объединенной двигателестроительной корпорации, «Высокоточные комплексы», «Вертолеты России». В будущем году система охватит пятую часть предприятий «Ростеха», а к 2020 г. – 30% всех объектов госкорпорации. Всего в составе госкорпорации около 700 подразделений, в том числе девять холдингов в ОПК, пять – в гражданском секторе и 22 организации прямого управления. Отмечается, что причиной создания КЦПКА стала необходимость анализа тысяч аномалий в системе безопасности, из которых за год фиксировались 1…2 реальные угрозы, например, шпионские вирусы. Кроме защиты собственных предприятий, новая структура может предоставлять услуги по обслуживанию других важных государственных объектов. Таким образом, даже исходя из сказанного, что информационное противоборство предполагает бескомпромиссное соперничество:

субъектов информационного конфликта с целью усиления влияния на те или иные сферы социальных отношений, итогом которых становится получение преимущества одной противоборствующей стороной и утрата подобных преимуществ другой;

социальных систем в информационно-психологической сфере с целью усиления влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают.

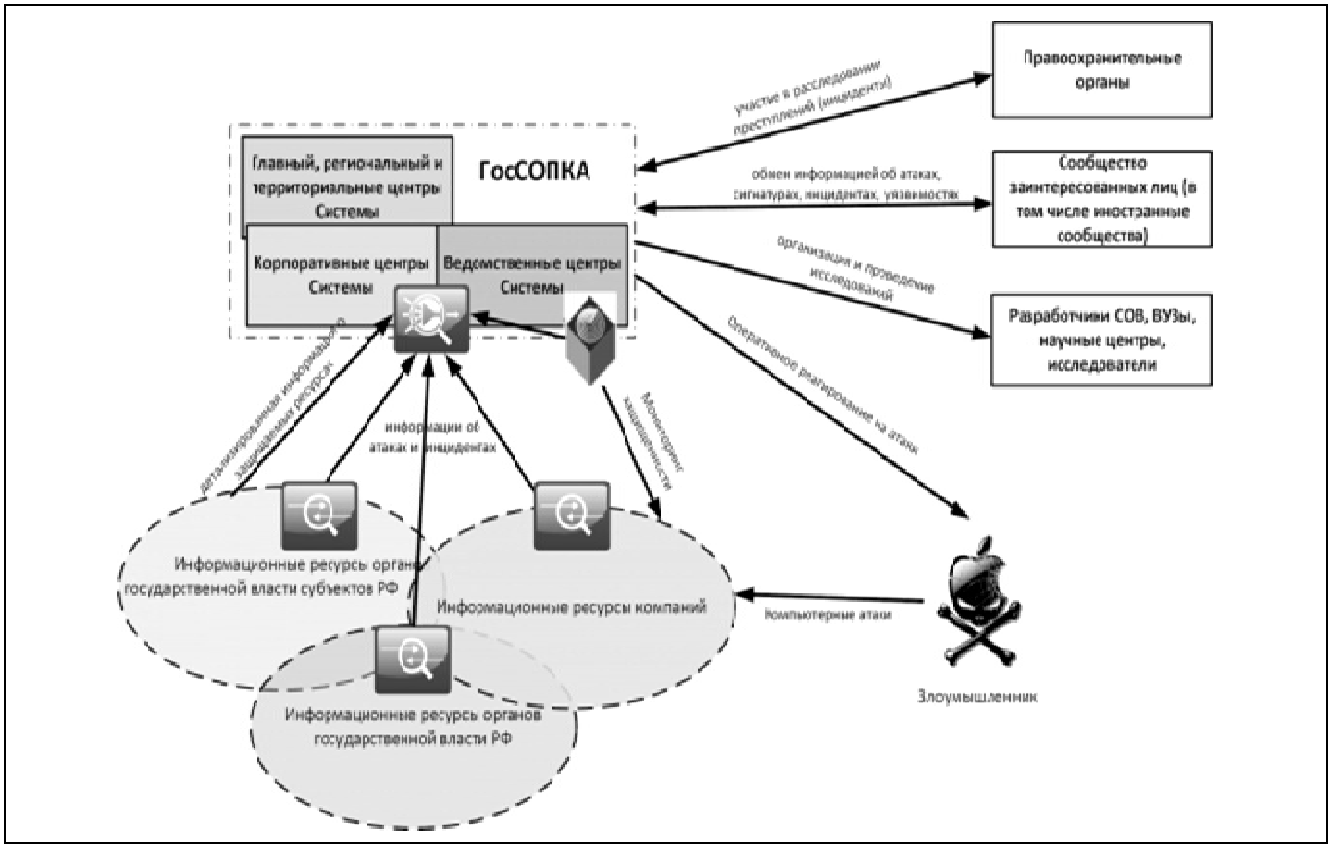

Рис. 6. Схема взаимодействия подразделений в рамках проекта ГосСОПКА

Информационная безопасность

Основные положения.

В приведенном выше определении информационного противоборства указывается «*с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия*». Это свидетельствует о том, что должно быть уделено особое внимание информационной безопасности. Действительно, правительства всех стран большое значение придают проблеме информационной безопасности. В качестве показательного примера можно привести документ Великобритании «NATIONAL CYBER SECURITY STRATEGY 2016-2021. В РФ существует целый ряд документов государственного уровня на эту тему: Доктрина информационной безопасности РФ, Указ Президента РФ от 5 декабря 2016 г., ФЗ №187 от 26.07.2017 «О защите критической информационной инфраструктуры РФ», Программа «Цифровая экономика РФ, Распоряжение Правительства от 28 июля 2017 г. № 1632-р.

В Доктрине информационной безопасности приведено определение этого термина: *Информационная безопасность РФ – состояние защищенности личности общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.*

Проблемой информационной безопасности занимается большое число организаций и отдельных специалистов, имеется большое число публикаций, в том числе монографий и учебников на русском языке. Обобщенная структура информационной безопасности приводится на рис. 7 [23].

Рис. 7. Обобщенная структура информационной безопасности

Рис. 8. Основные составляющие информационной безопасности

Рис. 9. Место математической модели в реализации концепции и программы ИБ

Требования по обеспечению безопасности в различных аспектах информационной деятельности могут существенно отличаться, однако они всегда направлены на достижение следующих трех основных составляющих информационной безопасности (рис. 8):

целостность – это, в первую очередь, актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения: данные и информация, на основе которой принимаются решения, должны быть достоверными, точными и защищенными от возможных непреднамеренных и злоумышленных искажений;

конфиденциальность – засекреченная информация должна быть доступна только тому, кому она предназначена: такую информацию невозможно получить, прочитать, изменить, передать, если на это нет соответствующих прав доступа;

доступность (готовность) – это возможность за приемлемое время получить требуемую информационную услугу: данные, информация и соответствующие службы, автоматизированные сервисы, средства взаимодействия и связи должны быть доступны и готовы к работе всегда, когда в них возникает необходимость.

Модели информационной безопасности.

В области информационной безопасности существуют свои модели и механизмы их построения. Выделяют концептуальную, математическую и функциональную модели представления информационной защиты. *Математическая модель* может представлять собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер. Расчетные численные значения параметров модели характеризуют функциональные (аналитические, алгоритмические или численные) зависимости, описывающие процессы взаимодействия нарушителей с системой защиты и возможные результаты действий [24]. Именно такой вид модели чаще всего используется для численных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер (рис. 9).

Важно подчеркнуть, что при совместном рассмотрении проблемы интероперабельности и информационного противоборства следует учитывать стандарты информационной безопасности, которых имеется большое количество как международных, так и отечественных [25]. Для этого можно рассматривать два подхода. При *первом подходе*, как это предложено в [11], должна быть создана синтезированная модель интероперабельности и информационной безопасности, и в терминах этой модели построен профиль, учитывающий стандарты информационной безопасности. При *втором подходе* отдельно строится профиль защиты информации. Согласно ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» профиль защиты (ПЗ) – это независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

До настоящего времени им. В.А.Котельникова РАН не занимался вплотную вопросами стандартизации в области информационной безопасности, однако, с 2018 г. начинает вести такие работы в рамках Программ Президиума РАН №27 и №58 с учетом проблемы информационной безопасности, и должен будет привлечь соответствующих специалистов.

Радиоэлектронная борьба

Основные понятия и подходы в области радиоэлектронной борьбы.

Как отмечено в [19,21], важным и исторически наиболее развитым направлением информационного противоборства является борьба с системами управления противника за счет использования средств РЭБ. Следовательно, использование этих средств должно быть учтено при решении проблемы интероперабельности, особенно в условиях современной сетецентрической войны. Ниже будем следовать изложению в [21], где имеется соответствующий раздел с обширной литературой. В разделе «Радиоэлектронная борьба» имеется подраздел « Роль и способы применения РЭБ в сетецентрической войне», содержащий основные термины, определения и классификация систем РЭБ, принятые в ВС США и в отечественной теории РЭБ. В ВС США и отечественной теории РЭБ приняты несколько различающиеся подходы к целям, задачам и классификации мероприятий РЭБ. В отечественной теории РЭБ определяется следующим образом.

Радиоэлектронная борьба – совокупность взаимосвязанных по цели, задачам, месту и времени мероприятий, действий, направленных на выявление радиоэлектронных средств и систем противника, их подавление, радиоэлектронную защиту своих радиоэлектронных систем и средств от средств РЭП противника, а также на радиоэлектронно-информационное обеспечение [19].

Подчеркивается, что РЭБ проводится в тесной взаимосвязи с огневым поражением, захватом и выводом из строя РЭС и радиоэлектронного оборудования (РЭО) в системах управления силами и оружием противника.

В соответствии с отечественной методологией классификация мероприятий РЭБ приведена на рис. 10. В [19] достаточно подробно описываются компоненты, приведенные на рис 10. С точки зрения настоящей статьи важно еще раз отметить, что средства РЭБ, как один из видов вооружения, является компонентом архитектуры интероперабельности при сетецентрической войне. Это подтверждается и зарубежными источниками и означает, что в состав профиля интероперабельности должны входить ИКТ-стандарты, характерные для средств РЭБ в том числе должен быть рассмотрен вопрос о стандартах электромагнитной совместимости.

Опыт работ ИРЭ им. В.А.Котельникова в области РЭБ.

Необходимо отметить опыт работ ИРЭ им. В.А.Котельникова РАН в области РЭБ. Достаточно сказать, что Институт был создан в 1953 г. в рамках Постановления правительства о развитии радиолокации в стране. О роли академика В.А. Котельникова, одного из создателей ИРЭ, возглавлявшего Институт около 30 лет и крупнейшего ученого и инженера, внесшего неоценимый вклад в разработку средств РЭБ, хорошо известно [26]. За годы работы Институт выполнил ряд работ по оборонной тематике в области РЭБ, многие из которых были удостоены высших правительственных наград.

В Институте много лет проработал один из главных создателей важнейшего средства РЭБ – радиолокатора – академик Ю.Б. Кобзарев, под руководством и при личном участии которого был выполнен ряд важнейших работ в области РЭБ. К этим работам можно отнести исследование вопросов техники когерентного накапливания в станциях дальнего пережения, вопросы защиты радиоэлектронных станций от пассивных помех, исследование возможностей создания радиоэлектронной станции для обнаружения воздушных целей над морской поверхностью за пределами горизонта [27]. За время работы в ИРЭ при Ю.Б. Кобзареве возникло и сейчас активно развивается такое направление несомненно двойного назначения, как изучение особенностей теплового излучения различных природных объектов [27].

Еще один выдающийся ученый и инженер, внесший большой вклад в разработку методов и средств РЭБ – академик Н.Д. Девятков, сыгравший значительную роль в становлении и развитии отечественной радиолокации. Разработанные им приборы были положены в основу создания целого ряда отечественных радиолокационных установок.

В отделе Н.Д. Девяткова в конце 1970-х гг. получило развитие еще одно направление работ Института, связанное с РЭБ, как средством информационного противоборства, работы по проблеме предот-

вращения утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) от работающих средств вычислительной техники.

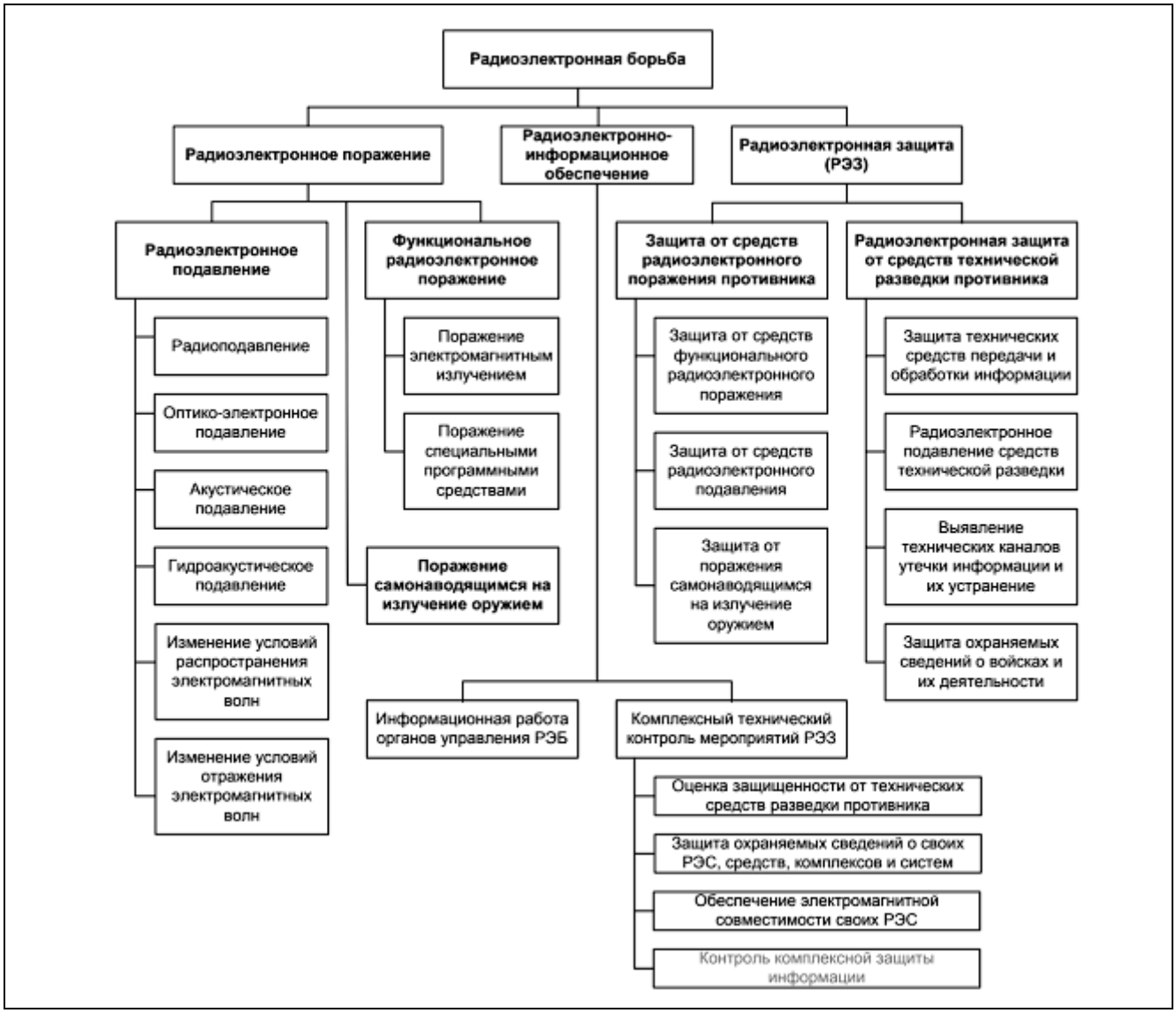

Рис. 10. Классификация мероприятий РЭБ

Сотрудники Института радиотехники и электроники РАН и СКБ ИРЭ РАН разработали способ активной радиотехнической маскировки ПЭМИН средств вычислительной техники [28]. Суть разработанного способа заключалась в формировании и излучении в непосредственной близости от работающих средств вычислительной техники маскирующего шумового сигнала в диапазоне частот побочных электромагнитных излучений и наводок и спектральным уровнем, превышающим уровни ПЭМИН. Устройства, разработанные на основе этого метода, поставлены на промышленное производство и называются «Шатер» [29].

Математические модели оценки интероперабельности

В данном разделе на основе имеющихся в современной печати научно-технических материалов математического моделирования выделим наиболее близкие к применению в оценке отдельных возможностей, относящихся к вопросов в области интероперабельности. Это такие вопросы, как отдельно возможная численная оценка интероперабельности, так и возможные способы моделирования систем информационного противоборства. В системе же информационного противоборства главным методом

остается радиоэлектронное противодействие радиотехническим системам и системам связи и управления. Также коротко отметим особенности воздействия на информационные системы методами создания помех и поражение мощным излучением.

Модели оценки интероперабельности.

В настоящее время имеется целый ряд моделей, поясняющих работу систем интероперабельности [5,11,30], показывающие общие возможности орисания интероперабельности. Наиболее же приемлемыми могут быть модели, изложенные в [31–33]. Особое внимание заслуживает способ численной оценки интероперабельности, предложенный в [33], где предложены наборы показателей и варианты шкал для оценки интероперабельности. Описан механизм решения задачи численной оценки интероперабельности на основе теории нечетких множеств с учетом весов влияющих факторов. Основные ее положения можно в кратком виде представлены ниже, и в перспективе этой моделью пользоваться.

Выбор показателей интероперабельности и лингвистических переменных. Предлагаемый способ может применяться при наличии принятой эталонной модели интероперабельности, позволяющей построить иерархию показателей интероперабельности. В большинстве известных эталонных моделей [34–36] выделяются уровни (слои) интероперабельности – от технических до организационных и бизнес-уровней.

Для примера можно использовать модель, включающую четыре уровня интероперабельности – физический, синтаксический, семантический и организационный и, соответственно, четыре показателя *Xi*, характеризующих эти аспекты интероперабельности (см. таблицу)

При необходимости построение функций принадлежности (ФП) для каждого показателя может быть выполнено с помощью одного из известных методов, например, метода парных сравнений, на основе экспертных или интервальных оценок, с применением параметрического подхода и т.п.

Используемая модель оценки интероперабельности. Предполагается, что имеется распределенная информационная система (ИС), состоящая из N элементов, характеристики которых оказывают влияние на показатель интероперабельности всей системы ($I_{\text{сис}}$).

Таблица. ***Показатели интероперабельности***

Показатель	Обозначение	Описание показателя
Физическая интероперабельность	X_1	Показатель, характеризующий способность различных информационных систем и/или их компонентов к обмену сигналами и данными и на этой основе к совместному использованию данных на основе поддержки согласованных интерфейсов, коммуникационных протоколов и механизмов доступак хранилищам данных.
Синтаксическая интероперабельность	X_2	Показатель, характеризующий способность различных информационных систем и/или их компонентов к обмену данными и, на этой базе, к совместному использованию данных на основе согласования кодов, форматов и типов данных.
Семантическая интероперабельность	X_3	Показатель, характеризующий способность различных информационных систем и/или их компонентов, построенных, возможно, по различным техническим принципам, к согласованному функционированию на основе единой, недвусмысленной, адекватной интерпретации информации, полученной в результате обмена
Организационная интероперабельность	X_4	Показатель, характеризующий способность различных бизнес-субъектов, бизнес-объектов и бизнес-процессов, использующих, возможно, различную информационную инфраструктуру, к согласованному функционированию на основе обмена информацией.

Присвоим каждому такому элементу показатель интероперабельности ($I_{\text{эл}\,i}$). Пусть показатель интероперабельности каждого элемента влияет на показатель интероперабельности всей системы с определенным весом j, тогда

$$I_{\text{сис}} = \left(I_{\text{эл}1}^{j1}, I_{\text{эл}2}^{j2}, \ldots, I_{\text{эл}N}^{jn} \right). \quad (1)$$

Показатель интероперабельности каждого элемента ИС определяется своим набором показателей (X_{i1}, X_{i2}, …, X_{iM}), в таблице таких показателей четыре, каждый из которых имеет вес k, следовательно,

$$I_{\text{эл}i} = \left(X_{i1}^{k1}, X_{i2}^{k2}, \ldots, X_{iM}^{km} \right). \quad (2)$$

Возможны случаи, когда все элементы и/или показатели с точки зрения своего влияния на общее свойство, равноправны, тогда веса не вычисляются.

При этом интероперабельность характеризует способность двух или более систем или элементов к обмену информацией и к использованию информации, полученной в результате обмена, и является одной из ключевых характеристик открытых систем (ОС) [33]. Обеспечение высокого уровня интероперабельности во многих работах рассматривается как одна из главных задач, стоящих перед создателями информационных систем различного назначения. Таким образом, возникает необходимость в численной оценке интероперабельности как при разработке, так и при модернизации информационных систем (ИС).

Поскольку исходные показатели, характеризующие ОС, как правило, не могут быть измерены численно, а только с использованием шкал порядка и таких признаков, как «лучше», «хуже», «больше», «меньше», для оценки состояния управляющей вершины нами использовалась процедура нечеткого логического вывода (НЛВ). Таким образом, в работе [33] предложен способ численной оценки интероперабельности, основанный на упомянутой методике и предположении о том, что интероперабельность в распределенной системе или системе систем [37] определяется потенциальной способностью каждого из компонентов к обмену информацией или использованию информации, полученной в результате обмена, а также влиянием этого элемента на результирующий показатель, которое учитывается весовыми коэффициентами. Таким образом, оценив показатель интероперабельности для каждого из компонентов или системы с помощью подходящей эталонной модели, подобной описанным в [38,39], и системы оцениваемых согласно упомянутой выше методике и привязанных к нечеткой шкале показателей, характеризующих интероперабельность, а также веса элементов, мы сможем численно оценить интероперабельность системы или системы систем в целом.

Правила НЛВ могут задаваться различным образом. Как показал опыт [40], удобно использовать процедуру НЛВ по Мамдани с построением нечеткой базы правил. В [33] приведен фрагмент экспертной нечеткой базы правил для оценки показателя интероперабельности элемента распределенной системы $I_{\text{эл}\,i}$.

Чтобы получить оценку показателя интероперабельности системы, нужно на каждом уровне иерархии осуществить агрегацию правил по соответствующей базе правил. Для этого требуется выполнить операцию пересечения (логический минимум, И – $\otimes$) по каждой строке базы правил и операцию объединения строк (логический максимум, ИЛИ – $\otimes$), соответствующих одному суждению (одному терму). В [33] приводится пример такого вычисления по нечеткой базе правил, как оценки интероперабельности ИС.

При необходимости в рассмотрение могут быть включены и другие уровни интероперабельности, например, концептуальный, характеризующий способность к совместному использованию информации в условиях согласования допущений и ограничений, унифицирующий, характеризующий способность к использованию на метауровнях единых форматов данных для связывания семантически эквивалентных моделей, федеративный, характеризующий способность к использованию общей онтологии, прагматический, характеризующий способность к совместному использованию информации в контексте решаемых задач и т.п.

Для получения численных оценок интероперабельности предлагается поставить в соответствие введенным показателям лингвистические переменные, описываемые набором (X, $T(X)$, U, G, M), в котором X – название переменной, способной, для определенности, принимать значения в интервале от 0 до 100; $T(X)$ – терммножество X, то есть совокупность ее лингвистических значений; U – универсальное множество; G – синтаксическое правило, порождающее термы множества $T(X)$; M – семантическое правило, которое каждому лингвистическому значению X ставит в соответствие значение нечеткой переменной $M(X)$, обозначающее нечеткое подмножество множества U.

Для нахождения терм-множеств $T(X_i)$ необходимо условиться о допустимой степени неопределенности в оценке интероперабельности. В работах [32,41] было показано, что при экспертном оценивании характеристик открытых систем и программных продуктов хорошие результаты получаются при числе термов от трех до пяти, при этом различия между крайними случаями сравнительно невелики. С учетом сказанного будем использовать на нижних уровнях иерархии в качестве синтаксического правила, порождающего лингвистические переменные, или грамматику «Низкий» (Н), «Ниже среднего» (НС),

«Средний» (С), «Выше Среднего» (ВС), «Высокий» (В), или грамматику «Низкий» (Н), «Средний» (С), «Выше Среднего» (ВС), «Высокий» (В), а на верхних уровнях иерархии грамматику «Низкий» (Н), «Средний» (С), «Высокий» (В) с возможным уточнением этой рекомендации по мере накопления экспертной информации.

При необходимости построение функций принадлежности (ФП) для каждого показателя может быть выполнено с помощью одного из известных методов, например, метода парных сравнений, на основе экспертных или интервальных оценок, с применением параметрического подхода и т.п. [33,42].

Таким образом, в работе решена задача численной оценки показателей интероперабельности для распределенных информационных систем, для описания которых может быть использована одна из общепринятых многоуровневых эталонных моделей интероперабельности. Предложены наборы показателей и варианты шкал для оценки интероперабельности таких систем. Разработан механизм, позволяющий решить задачу численной оценки интероперабельности на основе нечеткой модели с учетом весов влияющих характеристик. Полученные результаты могут быть практически применены в процессе управления качеством ИС на предприятиях и в организациях.

Модели оценки воздействия помех и мощным излучением.

Радиоподавление путем воздействия на приемные системы РЭС радиоэлектронными помехами. Современные вооружение и военная техника (ВиВТ) характеризуются высокой насыщенностью радиоэлектронным оборудованием, обеспечивающим решение задач автоматического или автоматизированного ведения разведки, связи, управления и наведения оружия. Устанавливаемые на ВиВТ радиоэлектронные средства (РЭС) позволяют получить своевременные и достаточные сведения о противнике в определенном районе и быстро реагировать на изменение боевой обстановки. В качестве информационных каналов РЭС используется электромагнитное излучение в диапазоне от единиц килогерц до десятков и сотен гигагерц, то есть большая часть спектра частот, освоенного техническими средствами.

Итак, коротко остановимся на видах радиоэлектронных помех создаваемых для противодействия радиолокационным системам и системам связи, а также коротко определим возможные дальности действия радиопомех.

А) *Радиоэлектронные помехи* – это непоражающие электромагнитные или акустические излучения, которые ухудшают качество функционирования РЭС, управляемого оружия и военной техники или систем обработки информации. Воздействуя на приемные устройства, помехи имитируют или искажают наблюдаемые и регистрируемые оконечной аппаратурой сигналы или изображения, затрудняют или исключают выделение полезной информации, ведение радиопереговоров и обнаружение целей с помощью РЭС, снижают их дальность действия и точность работы автоматических систем управления. Под действием помех РЭС и системы могут перестать быть источниками информации, несмотря на их полную исправность и работоспособность [43,44].

Классификация помех может быть следующая.

Маскирующие помехи ухудшают характеристики приемного устройства РЭС, что увеличивает число принятых символов, снижающих информативность сообщения, создают фон, на котором затрудняется или полностью исключается обнаружение, распознавание, выделение полезных сигналов или отметок целей. С увеличением мощности помех их маскирующее действие возрастает.

Имитирующие (дезинформирующие) помехи – это сигналы, излучаемые станцией помех для внесения ложной информации в подавляемые средства. По структуре они близки к полезным сигналам и поэтому создают в оконечном устройстве РЭС сигналы или отметки ложных целей, подобные реальным, снижают пропускную способность системы, вводят в заблуждение операторов, приводят к потере части полезной информации, увеличивают вероятность ложной тревоги. Воздействуя на средства управления оружием, они срывают автоматическое сопровождение целей по направлению, дальности, скорости и перенацеливают их на цели, имитируемые помехой, а также вызывают ошибки сопровождения цели. При воздействии имитирующих помех характеристики приемного устройства не ухудшаются.

Эффект воздействия помех сказывается в ухудшении качества обрабатываемой информации в результате ее разрушения либо старения, что увеличивает степень неопределенности при принятии решений.

В зависимости от способа наведения помех, соотношения ширины спектров помех и полезных сигналов маскирующие помехи подразделяют на заградительные и прицельные.

Заградительные помехи имеют ширину спектра частот, значительно превышающую полосу, занимаемую полезным сигналом, что позволяет подавлять одновременно несколько РЭС без точного наведения передатчика помех (ПП) по частоте. Их можно создавать, не имея полных данных о параметрах сигналов подавляемых РЭС.

Особенностью заградительных помех является то, что при неизменной мощности ПП их спектральная плотность мощности G_n, Вт/МГц, уменьшается по мере расширения спектра излучения. При равномерном спектре она представляет собой отношение энергетического потенциала передатчика помех $P_{пп}G_{пп}$ к ширине спектра частот помехи Δf_n. Для сплошной заградительной помехи

$$G_n = P_{пп}G_{пп} / \Delta f_n. \quad (3)$$

Например, если ПП, имеющий эквивалентную мощность 5000 Вт, создает заградительные помехи в диапазоне частот от f_1 = 9500 МГц до f_2=10000 МГц (Δf_n = 500 МГц), то G_n=5000/500=10.

Одним из способов формирования заградительных помех является применение скользящих по частоте помех, образуемых при быстрой перестройке передатчика узкополосных помех в широкой полосе частот. Благодаря этому в полосе частот каждого канала многоканального РЭС или нескольких станций последовательно сосредоточивается достаточно высокая плотность мощности, необходимая для их подавления. Однако при наличии схем защиты эффективность этих помех может оказаться ниже, чем заградительных, создаваемых передатчиком, не имеющим перестройки по частоте.

Прицельные помехи имеют ширину спектра, соизмеримую (равную или в 1,5…2 раза превышающую) с шириной спектра сигнала подавляемого РЭС. Например, прицельные помехи радиолокации имеют спектр 5…10 МГц. Эффективность их воздействия зависит от точности совмещения по частоте с сигналом, спектральной плотности мощности и способов обработки сигналов в приемнике РЭС. Допустимая ошибка в настройке ПП при заданном эффекте подавления зависит от ширины спектра помехи и отношения спектральных плотностей мощности помехи к сигналу подавляемого РЭС. Для некоторых видов передач она не должна превышать половины ширины полосы пропускания приемника, а средняя частота спектра помехи – примерно совпадать с несущей частотой подавляемого устройства. Так как РЭС имеют возможность быстро перестраиваться по частоте, то в составе станции прицельных помех применяется сложная аппаратура обнаружения сигналов, перестройки и наведения по частоте передатчика в широком диапазоне волн.

Прицельные помехи характеризуются высокой спектральной плотностью мощности. Поскольку они излучаются в узкой полосе частот, то могут быть реализованы маломощными ПП. Например, передатчик радиопомех, имеющий мощность излучения всего лишь 150 Вт и $G_{пп}$=100, способен создать в полосе 5 МГц плотность мощности, равную 3000 Вт/МГц, а в полосе 0,5 МГц – 30 кВт/МГц.

Недостатком прицельных помех является то, что они одновременно могут подавлять только одно РЭС, работающее в данном диапазоне волн.

По временной структуре излучения радиоэлектронные помехи подразделяют на непрерывные и импульсные. Непрерывные помехи представляют собой непрерывные электромагнитные (акустические) излучения, модулированные по амплитуде, частоте или фазе. Импульсные помехи имеют вид немодулированных или модулированных радиоимпульсов.

Более подробно все виды активных помех и способы их формирования и их оценка подробно рассматриваются в [43,44].

В настоящее время обосновывается, что при создании новых технологий постановки активных помех (маскирующих, диверсионных и дезинформирующих) и др. и применении радиоэлектронных помех позволяет снизить вероятность обслуживания (обнаружения, наведения и получения радиоинформации) РЭС-источников радиоизлучений постами местоопределения и периодического наблюдения в 3…5 раз. В результате действия дезинформирующих помех снижается вероятность обслуживания постами непрерывного наблюдения в 1,5…1,8 раза.

При этом наиболее важным техническим показателем применения радиоэлектронных помех является дальность таких помех. К наиболее часто применяемым радиопомехам в боевой обстановке относятся активные радиопомехи, поэтому целесообразно дать их характеристику по дальности их действия.

Б) *Дальность действия активных радиопомех.* Дальность РЭП зависит от многих факторов, в том числе от мощности радиопередающих устройств РЭС и средств РЭП, характеристик их антенных систем, чувствительности приемных устройств, условий распространения электромагнитных волн, видов

излучения и способов обработки сигнала, длины рабочей волны, способов помехозащиты. Кроме того, на дальность РЭП оказывают влияние интенсивность помех от местных предметов, земной (водной) поверхности и внеземных источников, характер излучения и рассеяния электромагнитных волн целями, наблюдаемыми РЭС. Учесть все перечисленные факторы чрезвычайно трудно. В связи с этим дальность подавления РЭС и необходимая мощность средств РЭП оцениваются математически по усредненным параметрам и уточняются в процессе натурных испытаний и смешанного моделирования.

Радиоэлектронные средства могут подавляться средствами РЭП только в том случае, когда отношение мощности помехи, попадающей в полосу пропускания радиоприемника, к мощности сигнала превышает некоторое минимально необходимое значение, характерное для данного вида помехи и сигнала. Минимально необходимое отношение мощностей маскирующей помехи $P_п$ и сигнала $P_с$ на входе подавляемого приемника в пределах полосы пропускания его линейной части, при котором достигается требуемая степень подавления РЭС, называют коэффициентом подавления по мощности:

$$K_п = (P_п/P_с)_{вх\ min}. \quad (4)$$

На практике иногда применяют понятие «коэффициент подавления по напряжению»:

$$K_{пн}=(U_п/U_с)_{вх\ min}. \quad (5)$$

Помеха считается эффективной, если отношение ее мощности к мощности полезного сигнала на входе приемного устройства $K= (P_п/P_с)$вх больше коэффициента подавления, то есть $K> K_п$. Значение $K_п$ зависит от вида помехи и сигнала, а также от характеристик приемника подавляемого РЭС. Чем меньше $K_п$, тем при прочих равных условиях легче подавить РЭС помехой. Пространство, в пределах которого $K > K_п$, называется зоной подавления РЭС, а при $K < K_п$ – зоной неподавления. Граница этих зон проходит на уровне, когда $K= K_п$ [44]. Зоной подавления считают область пространства, в пределах которой РЭС подавлена с заданной эффективностью.

Если известен $K_п$, то можно определить зону подавления, в пределах которой создаются эффективные помехи данному РЭС. Для этого надо установить зависимость K от параметров и взаимного пространственного положения станции помех и подавляемого РЭС.

Мощность помех $P_{пс}$ равномерным спектром шириной $\Delta f_п$ на входе приемника в пределах полосы пропускания его линейной части $\Delta f_{пр}$ (при условии, что $\Delta f_п > \Delta f_{пр}$) будет определяться в зависимости от следующих величин: $P_{пп}$ – мощность передатчика помех; $G_{пп}$ – коэффициент усиления антенны станции помех в направлении на приемное устройство подавляемой станции; $D_п$ – расстояние между передатчиком помех и приемником сигнала; $v_п$ – коэффициент, учитывающий различия поляризации помехи и сигнала (может иметь значение от единицы, при совпадении поляризации помехи и сигнала, до нуля, когда поляризации ортогональны или различны по направлению вращения – при круговой поляризации). Если в станции помех применяется антенна с круговой поляризацией, а в приемном устройстве – с линейной, то $v_п = 0{,}5$).

- Показано, что такие проблемы, как проблема интероперабельности, информационного противоборства и радиоэлектронная борьба тесно связаны между собой и должны решаться совместно. До настоящего времени работы по названным направлениям велись в большой степени без координации, а при совместном рассмотрении, концентрации усилий и соответствующем внедрении могут представить единое направление, важное, в первую очередь, для обороноспособности страны и ее национальной безопасности.

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. *Башлыкова А.А., Камкнщиков А.А., Олейников А.Я., Чусов И.И., Широбокова Т.Д.* Проблема интероперабельности в информационных системах военного назначения / Отчет о научно-исследовательской работе (этап 2016 г.) (промежуточный). URL: http://www.opensys.info/files/data_20170321171734.pdf.
3. *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. № 3. URL: http://jre.cplire.ru/mac/mar12/2/text.pdf.
4. *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 науч.-практич. конф. «Система межведомственного информационного взаимодей-

ствия при решении задач в области обороны Российской Федерации»: сборник материалов. М.: Национальный центр управления обороной Российской Федерации. 2016. С. 45–48.
5. *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.
6. NATO Interoperability Standards and Profiles. NISP in PDF. The following documents are PDF versions of the NISP. Copyright © NATO – OTAN 1998-2016. Available at.
7. *Новичков Н.* США пока полностью не готовы к отражению серьезной кибератаки. А готова ли к этому Россия? // Воздушно-космическая оборона. 2012. № 5 (66). С. 21.
8. *Сиников А.* Управлять – значит предвидеть // Воздушно-космическая оборона. 2012. № 5(66). С. 39.
9. Новости воздушно-космической обороны. 18 мая 2012 г. URL: http://gunm.ru/news.
10. Электронная война – мифы и правда. Автор: *Алексей Рамм* // «Военное обозрение. Вооружение. Армия России»/ 2015. Первоисточник: http://vpk-news.ru/articles/27272.
11. *Олейников А.Я., Чусов И.И.* Проблема интероперабельности в вооруженных силах РФ // Журнал «Вестник» Академии военных наук. 2018. № 4. С.61–68.
12. *Батоврин В.К., Гуляев Ю.В., Олейников А.Я.* Обеспечение интероперабельности – основная тенденция в развитии открытых систем // Информационные технологии и вычислительные системы. 2009. № 5. С. 7–15.
13. URL: http://jre.cplire.ru/mac/mar12/2/text.pdf.
14. *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. № 3.
15. Указ Президента РФ от 10.01.2000 № 24 «О концепции национальной безопасности Российской Федерации»
16. Информационная безопасность (Кн. 2 социально-политического проекта «Актуальные проблемы безопасности социума»). М.: Оружие и технологии. 2009.
17. *Шушков Г.М., Сергеев И.В.* Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сб. науч. трудов III Всероссийской заочной науч.-практич. конф. (23.11.2015 – 30.12.2015 г., Москва) / Под общ. ред. *Е.А. Певцовой*; ред. *Е.А. Куренкова* и др. М.: ИИУ МГОУ. 2016. С. 69–76.
18. *Сергеев И.В.* Информационно-психологическая война как форма эскалации межгосударственных конфликтов // Информационные войны. 2015. № 2(34). С. 38–41.
19. *Сергеев И.В.* Социальные сети в Интернете как средство реализации операций информационно-психологической войны // Международный научно-исследовательский журнал. 2015. № 9(40). С. 101–104.
20. *Сергеев И.В.* Дженнифер Псаки – инструмент информационного противоборства // Евразийский союз ученых. 2016. № 6(27). С. 92–93.
21. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. // СПб: Наукоемкие технологии. 2017.
22. Материалы Международного конгресса «Доверие и безопасность в информационном обществе». 21 апреля 2003 г.
23. Безопасность информационных систем, intuit.valrkl.ru›course-1312/index.html.
24. Информационная безопасность (Кн. 2 социально-политического проекта «Актуальные проблемы безопасности социума»). М.: Оружие и технологии. 2009.
25. Department of Defense Trusted Computer System Evaliation Criteria (TCSEC). USA DoD 5200.28-STD. 1993.
26. *Галатенко В.А.* Общая структура инфломационной безопасности // Зарубежное военное обозрение. 2006.
27. Зарубежное военное обозрение. Новые средства ведения радиоэлектронной борьбы // Военно-воздушные силы / 27 января 2014.
28. А.с. № 1773220. Способ маскировки радиоизлучений средств вычислительной техники и устройство для его реализации // *Дмитриев А.С., Залогин Н.Н., Иванов В.П.* и др. Приоритет от 21.09.1981 г.
29. URL: http://www.bnti.ru/des.asp?itm=674&tbl=04.03.04.01.
30. Технология открытых систем / Под ред. *А.Я. Олейникова*. М.: Янус-К.
31. *Батоврин В.К.* Количественная оценка приемлемости решений при создании открытых информационных систем//Информационные технологии. М.: Новые технологии. 2007. № 3. С. 20–26.
32. *Батоврин В.К.* Количественная оценка приемлемости решений при создании открытых информационных систем//Информационные технологии. М.: Новые технологии. 2007. № 3. С. 20–26.
33. *Батоврин В.К., Королев А.С.* Способ количественной оценки интероперабельности. Работа поддержана Советом по грантам Президента РФ, грант МК-1976.2009.9.
34. *Morris E., Levine L., Meyers C., Place P., Plakosh D.* System of Systems Interoperability (SOSI): Final Report. April 2004. Technical Report CMU/SEI-2004-TR-004 – ESC-TR-2004-004.
35. *Tolk A.* Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. 8th International Command and Control Research and Technology Symposium. Washington, June 17-19, 2003. Washington DC: Command and Control Research Program, 2003. http://www.dodccrp.org/8thiccrts/pdf/084.pdf.
36. European Interoperability Framework for Pan-European E-government Services. Draft for public comments – as basis for EIF 2.0 – 15.07.2008, http://ec.europa.eu/idabc/servlets/Doc?id=31597
37. *Morris E., Levine L., Meyers C., Place P., Plakosh D.* System of Systems Interoperability (SOSI): Final Report. April 2004. Technical Report CMU/SEI-2004-TR-004 – ESC-TR-2004-004.

38. *Tolk A.* Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. 8th International Command and Control Research and Technology Symposium. Washington, June 17-19, 2003. Washington DC: Command and Control Research Program, 2003. http://www.dodccrp.org/8thiccrts/pdf/084.pdf.
39. European Interoperability Framework for Pan-European E-government Services. Draft for public comments – as basis for EIF 2.0.
40. *Батоврин В.К., Королев А.С.* Использование нечеткого логического вывода при проектировании профилей открытых систем // Системы управления и информационные технологии. Воронеж: Научная книга. 2006. № 3(25). С. 68–74.
41. *Батоврин В.К., Королев А.С.* Формализация входных переменных для автоматизированной системы выбора стандартов// Информационные технологии и вычислительные системы. М.: РАН. 2006. № 3. С. 53–61.
42. *Борисов А.Н., Крумберг О.А., Федоров И.П.* Принятие решений на основе нечетких моделей: примеры использования. Рига: Знание. 1990.
43. *Осипов А.С.* Военно-техническая подготовка и военно-технические основы построения средств и комплексов РЭП / Под науч. ред. д.т.н. *Е.Н. Гарина* // Министерство образования и науки Российской Федерации. Красноярск: СФУ. 2013.
44. *Быстров Р.П., Дмитриев В.Г., Меньшиков В.Л., Перунов Ю.М., Потапов А.А.Потапов А.А.* Теоретическая оценка современных методов и способов снижения радиолокационной заметности объектов и систем в условиях радиоэлектронного противодействия // Нелинейный мир. 2015. № 7. Т. 13. С. 3–24.

Поступила 17 апреля 2018 г.

Interoperability, information antagonism and radio-electronic fight

R.P. Bystrov – Dr.Sc. (Eng.), Professor, academician of Academy of military sciences, corresponding member of the Academy of Engineering Sciences, Leading Research Scientist, IRE of V.A. Kotelnikov of the Russian Academy of Sciences
E-mail: rudolf@cplire.ru
V.N. Korniyenko – Ph.D. (Phys.-Math.), Deputy Director, IRE of V.A. Kotelnikov of the Russian Academy of Sciences
E-mail: korn@cplire. ru.
A.Ya. Oleynikov – Dr.Sc. (Eng.), Professor, Chief Research Scientist, IRE of V.A. Kotelnikov of the Russian Academy of Sciences
E-mail: ole-in@cplire.ru

A condition of works in such areas of development and application of information and communication technologies as interoperability and information antagonism, including radioelectronic fight, in the conditions of network-centric war is considered. The basic concepts from area of network-centric war, interoperability, information antagonism, information security and radioelectronic fight are given. The special attention is paid to a condition of works on interoperability and the experience in this area gained at Kotelnikov Institute of radio engineering and electronics of the Russian Academy of Sciences. It is emphasized that interoperability makes «base» of Uniform information space of any scale and that the problem of interoperability needs to be solved taking into account the conducted information antagonism. It is emphasized that so far a problem of an interoperability and a problem of information antagonism were considered independently of one another. Thus it is claimed that joint consideration of a problem of interoperability and information antagonism submits the requirement of time and is aimed at providing defense capability and national security.

References

1. *Kamenthikov A. A., Oleyjnikov A.Ya., Chusov I. I., Shirobokova T. D.* Problema interoperabeljnosti v informacionnihkh sistemakh voennogo naznacheniya // Zhurnal radioehlektroniki: ehlektronnihyj zhurnal. 2016. № 11. URL: http://jre.cplire.ru/jre/nov16/8/text.pdf.
2. *Bashlihkova A.A., Kamknthikov A.A., Oleyjnikov A.Ya., Chusov I.I., Shirobokova T.D.* Problema interoperabeljnosti v informacionnihkh sistemakh voennogo naznacheniya / Otchet o nauchno-issledovateljskoyj rabote (ehtap 2016 g.) (promezhutochnihyj). URL: http://www.opensys.info/files/data_20170321171734.pdf.
3. *Gulyaev Yu.V., Zhuravlev E.E., Oleyjnikov A.Ya.* Metodologiya standartizacii dlya obespecheniya interoperabeljnosti informacionnihkh sistem shirokogo klassa. Analiticheskiyj obzor // Zhurnal radioehlektroniki: ehlektronnihyj zhurnal. 2012. № 3. URL: http://jre.cplire.ru/mac/mar12/2/text.pdf.
4. *Kornienko V.N., Oleyjnikov A.Ya.* Obespechenie interoperabeljnosti na osnove ispoljzovaniya standartov informacionno-kommunikacionnihkh tekhnologiyj pri mezhvedomstvennom vzaimodeyjstvii pri reshenii zadach v oblasti oboronih Rossiyjskoyj Federacii // II Mezhvedomstvennaya nauch.-praktich. konf. «Sistema mezhvedomstvennogo informacionnogo vzaimodeyjstviya pri reshenii zadach v oblasti oboronih Rossiyjskoyj Federacii»: sbornik materialov. M.: Nacionaljnihyj centr upravleniya oboronoyj Rossiyjskoyj Federacii. 2016. S. 45–48.
5. *Bashlihkova A.A., Oleyjnikov A.Ya.* Interoperabeljnostj i informacionnoe protivoborstvo v voennoyj sfere // Zhurnal radioehlektroniki: ehlektronnihyj zhurnal. 2016, N12. URL: http://jre.cplire.ru/jre/nov16/8/text.pdf.
6. NATO Interoperability Standards and Profiles. NISP in PDF. The following documents are PDF versions of the NISP. Copyright © NATO – OTAN 1998-2016. Available at.
7. Novichkov N. SShA poka polnostjyu ne gotovih k otrazheniyu serjeznoyj kiberataki. A gotova li k ehtomu Rossiya? // Vozdushno-kosmicheskaya oborona. 2012. № 5 (66). S. 21.
8. *Sinikov A.* Upravlyatj – znachit predvidetj // Vozdushno-kosmicheskaya oborona. 2012. № 5(66). S. 39.
9. Novosti vozdushno-kosmicheskoyj oboronih. 18 maya 2012 g. URL: http://gunm.ru/news.
10. Ehlektronnaya voyjna – mifih i pravda. Avtor: *Alekseyj Ramm* // «Voennoe obozrenie. Vooruzhenie. Armiya Rossii»/ 2015. Pervoistochnik: http://vpk-news.ru/articles/27272.
11. *Oleyjnikov A.Ya., Chusov I.I.* Problema interoperabeljnosti v vooruzhennihkh silakh RF // Zhurnal «Vestnik» Akademii voennihkh nauk. 2018. № 4. C.61–68.

12. *Batovrin V.K., Gulyaev Yu.V., Oleyjnikov A.Ya.* Obespechenie interoperabeljnosti – osnovnaya tendenciya v razvitii otkrihtihkh sistem // Informacionnihe tekhnologii i vihchisliteljnihe sistemih. 2009. № 5. S. 7–15.
13. URL: http://jre.cplire.ru/mac/mar12/2/text.pdf.
14. *Gulyaev Yu.V., Zhuravlev E.E., Oleyjnikov A.Ya.* Metodologiya standartizacii dlya obespecheniya interoperabeljnosti informacionnihkh sistem shirokogo klassa. Analiticheskiyj obzor // Zhurnal radioehlektroniki: ehlektronnihyj zhurnal. 2012. № 3.
15. Ukaz Prezidenta RF ot 10.01.2000 № 24 «O koncepcii nacionaljnoyj bezopasnosti Rossiyjskoyj Federacii»
16. Informacionnaya bezopasnostj (Kn. 2 socialjno-politicheskogo proekta «Aktualjnihe problemih bezopasnosti sociuma»). M.: Oruzhie i tekhnologii. 2009.
17. *Shushkov G.M., Sergeev I.V.* Konceptualjnihe osnovih informacionnoyj bezopasnosti Rossiyjskoyj Federacii // Aktualjnihe voprosih nauchnoyj i nauchno-pedagogicheskoyj deyateljnosti molodihkh uchenihkh: sb. nauch. trudov III Vserossiyjskoyj zaochnoyj nauch.-praktich. konf. (23.11.2015 – 30.12.2015 g., Moskva) / Pod obth. red. *E.A. Pevcovoyj*; red. *E.A. Kurenkova* i dr. M.: IIU MGOU. 2016. S. 69–76.
18. *Sergeev I.V.* Informacionno-psikhologicheskaya voyjna kak forma ehskalacii mezhgosudarstvennihkh konfliktov // Informacionnihe voyjnih. 2015. № 2(34). S. 38–41.
19. *Sergeev I.V.* Socialjnihe seti v Internete kak sredstvo realizacii operaciyj informacionno-psikhologicheskoyj voyjnih // Mezhdunarodnihyj nauchno-issledovateljskiyj zhurnal. 2015. № 9(40). S. 101–104.
20. *Sergeev I.V.* Dzhennifer Psaki – instrument informacionnogo protivoborstva // Evraziyjskiyj soyuz uchenihkh. 2016. № 6(27). S. 92–93.
21. *Makarenko S.I.* Informacionnoe protivoborstvo i radioehlektronnaya borjba v setecentricheskikh voyjnakh nachala XXI veka. Monografiya. // SPb: Naukoemkie tekhnologii. 2017.
22. Materialih Mezhdunarodnogo kongressa «Doverie i bezopasnostj v informacionnom obthestve». 21 aprelya 2003 g.
23. Bezopasnostj informacionnihkh sistem, intuit.valrkl.ru›course-1312/index.html.
24. Informacionnaya bezopasnostj (Kn. 2 socialjno-politicheskogo proekta «Aktualjnihe problemih bezopasnosti sociuma»). M.: Oruzhie i tekhnologii. 2009.
25. Department of Defense Trusted Computer System Evaliation Criteria (TCSEC). USA DoD 5200.28-STD. 1993.
26. *Galatenko V.A.* Obthaya struktura inflomacionnoyj bezopasnosti // Zarubezhnoe voennoe obozrenie. 2006.
27. Zarubezhnoe voennoe obozrenie. Novihe sredstva vedeniya radioehlektronnoyj borjbih // Voenno-vozdushnihe silih / 27 yanvarya 2014.
28. A.s. № 1773220. Sposob maskirovki radioizlucheniyj sredstv vihchisliteljnoyj tekhniki i ustroyjstvo dlya ego realizacii // *Dmitriev A.S., Zalogin N.N., Ivanov V.P.* i dr. Prioritet ot 21.09.1981 g.
29. URL: http://www.bnti.ru/des.asp?itm=674&tbl=04.03.04.01.
30. Tekhnologiya otkrihtihkh sistem / Pod red. A.Ya. Oleyjnikova. M.: Yanus-K.
31. *Batovrin V.K.* Kolichestvennaya ocenka priemlemosti resheniyj pri sozdanii otkrihtihkh informacionnihkh sistem//Informacionnihe tekhnologii. M.: Novihe tekhnologii. 2007. № 3. S. 20–26.
32. *Batovrin V.K.* Kolichestvennaya ocenka priemlemosti resheniyj pri sozdanii otkrihtihkh informacionnihkh sistem//Informacionnihe tekhnologii. M.: Novihe tekhnologii. 2007. № 3. S. 20–26.
33. *Batovrin V.K., Korolev A.S.* Sposob kolichestvennoyj ocenki interoperabeljnosti. Rabota podderzhana Sovetom po grantam Prezidenta RF, grant MK-1976.2009.9.
34. *Morris E., Levine L., Meyers C., Place P., Plakosh D.* System of Systems Interoperability (SOSI): Final Report. April 2004. Technical Report CMU/SEI-2004-TR-004 – ESC-TR-2004-004.
35. *Tolk A.* Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. 8th International Command and Control Research and Technology Symposium. Washington, June 17-19, 2003. Washington DC: Command and Control Research Program, 2003. http://www.dodccrp.org/8thiccrts/pdf/084.pdf.
36. European Interoperability Framework for Pan-European E-government Services. Draft for public comments – as basis for EIF 2.0 – 15.07.2008, http://ec.europa.eu/idabc/servlets/Doc?id=31597
37. *Morris E., Levine L., Meyers C., Place P., Plakosh D.* System of Systems Interoperability (SOSI): Final Report. April 2004. Technical Report CMU/SEI-2004-TR-004 – ESC-TR-2004-004.
38. *Tolk A.* Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. 8th International Command and Control Research and Technology Symposium. Washington, June 17-19, 2003. Washington DC: Command and Control Research Program, 2003. http://www.dodccrp.org/8thiccrts/pdf/084.pdf.
39. European Interoperability Framework for Pan-European E-government Services. Draft for public comments – as basis for EIF 2.0.
40. *Batovrin V.K., Korolev A.S.* Ispoljzovanie nechetkogo logicheskogo vihvoda pri proektirovanii profileyj otkrihtihkh sistem // Sistemih upravleniya i informacionnihe tekhnologii. Voronezh: Nauchnaya kniga. 2006. № 3(25). S. 68–74.
41. *Batovrin V.K., Korolev A.S.* Formalizaciya vkhodnihkh peremennihkh dlya avtomatizirovannoyj sistemih vihbora standartov// Informacionnihe tekhnologii i vihchisliteljnihe sistemih. M.: RAN. 2006. № 3. S. 53–61.
42. *Borisov A.N., Krumberg O.A., Fedorov I.P.* Prinyatie resheniyj na osnove nechetkikh modeleyj: primerih ispoljzovaniya. Riga: Znanie. 1990.
43. *Osipov A.S.* Voenno-tekhnicheskaya podgotovka i voenno-tekhnicheskie osnovih postroeniya sredstv i kompleksov REhP / Pod nauch. red. d.t.n. *E.N. Garina* // Ministerstvo obrazovaniya i nauki Rossiyjskoyj Federacii. Krasnoyarsk: SFU. 2013.
44. *Bihstrov R.P., Dmitriev V.G., Menjshikov V.L., Perunov Yu.M., Potapov A.A.Potapov A.A.* Teoreticheskaya ocenka sovremennihkh metodov i sposobov snizheniya radiolokacionnoyj zametnosti objhektov i sistem v usloviyakh radioehlektronnogo protivodeyjstviya // Nelineyjnihyj mir. 2015. № 7. T. 13. S. 3–24.

Недочеты:

1. Нет расшифровки некоторых сокращений (выделены желтым)

2. Повтор в списке литературы одних и тех же источников (выделены желтым)