УДК 623.62

Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями

Макаренко С. И.

Постановка задачи. *В настоящее время происходит переход архитектуры систем государственного и военного управления от иерархического к сетецентрическому принципу построения. Сетецентрическая система управления является распределённой системой, в которой ее базовые элементы объединены в единое информационное пространство. Такое объединение делает неэффективными существующие способы дестабилизирующего воздействия, ориентированные на подавление или поражение отдельных элементов. В связи с этим требуется предложить новый подход к подавлению распределенных сетецентрических систем управления.* ***Целью работы*** *является формирование общего подхода к подавлению телекоммуникационных систем как базового элемента информационной подсистемы сетецентрической системы управления, а также формирование конкретных предложений по способам такого подавления на основе существующих технических средств.* ***Результат и его новизна.*** *В статье предложены радиоэлектронные информационно-технические воздействия как эволюционное развитие существующих способов радиоэлектронного подавления. Данные воздействия осуществляют подавление сетецентрической системы управления за счет нарушения функционирования протоколов множественного доступа, протоколов маршрутизации и протоколов обеспечения качества обслуживания трафика в телекоммуникационных системах. Ориентированность на нарушение протоколов функционирования канального, сетевого и транспортного уровня отличает предложенные воздействия от существующих способов радиоэлектронного подавления, которые в большинстве ориентированы на подавление отдельных каналов и сетей радиосвязи.* ***Практическая значимость.*** *Предложенные в статье способы радиоэлектронного информационно-технического воздействия могут быть использованы для эффективного нарушения функционирования сетецентрических систем. Кроме того, эти воздействия могут использоваться для тестирования устойчивости собственных сетецентрических систем управления к подобным воздействиям со стороны потенциального противника.*

Ключевые слова*: сетецентрическая система управления, радиоэлектронная борьба, радиоэлектронное подавление, информационное противоборство, информационно-техническое воздействие, телекоммуникационная система, сеть связи.*

Актуальность

В настоящее время происходит переход архитектуры систем государственного и военного управления от иерархического к сетецентрическому принципу построения. Сетецентрическая система управления является распределённой системой, в которой ее базовые элементы объединяются в единое информационное пространство. Объединение элементов в единое информационное пространство повышает возможности информационного взаимодействия

Библиографическая ссылка на статью:
Макаренко С. И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. 2017. № 4. С. 15-59. URL: http://sccs.intelgr.com/archive/2017-04/02-Makarenko.pdf

Reference for citation:
Makarenko S. I. Suppression of a Net-Centric Control System with Radio Cyber Attacks. *Systems of Control, Communication and Security*, 2017, no. 3, pp. 15-59. Available at: http://sccs.intelgr.com/archive/2017-04/02-Makarenko.pdf (in Russian).

всех компонентов системы управления. Одновременно с этим, повышение сетевой связности элементов сетецентрической системы управления делает неэффективными существующие способы дестабилизирующих воздействий, основанные на применении средств радиоэлектронного подавления (РЭП), средств функционального поражения электромагнитным излучением (ФП ЭМИ) и информационно-технических воздействий (ИТВ). Это происходит из-за того, что данные способы ориентированы, в основном на нарушение процессов передачи данных в иерархических системах управления и неэффективны при воздействии на высокосвязную сетевую среду единого информационного пространства сетецентрической системы. В едином информационном пространстве для передачи информации возможно использовать множество путей, при этом нарушение функционирования отдельных линий или подсетей радиосвязи не будет являться критичным для нарушения управления в сетецентрической системе.

Указанные факторы определяют актуальность разработки новых способов дестабилизирующих воздействий – *радиоэлектронных информационно-технических воздействий* (РЭ ИТВ). Предполагается, что они будут воздействовать на процессы передачи информации путем нарушения функционирования сетевых протоколов единого информационного пространства. При этом «точками входа» РЭ ИТВ в сетецентрическую систему управления будут являться радиолинии и радиоканалы в составе сети связи специального назначения, которая составляет техническую основу единого информационного пространства.

Целью статьи является разработка общего подхода к подавлению сетецентрических систем управления, а также формирование конкретных предложений по способам РЭ ИТВ на основе существующих технических средств РЭП. В основу представленного подхода положено обобщение научных результатов автора, полученных им в процессе проведения исследований, связанных с развитием систем РЭП.

Ввиду объемности статьи, она была декомпозирована на следующие подпункты.

1. Сетецентрическая система управления как объект подавления.
   1.1. Основные особенности сетецентрической системы управления.
   1.2. Сетецентрическая среда как основа информационной подсистемы сетецентрической системы управления.
2. Анализ основных уязвимостей сетецентрической системы управления и перспективные возможности ассиметричного противодействия ей.
   2.1. Уязвимости сетецентрической системы управления, обусловленные высокой информационной зависимостью всех ее элементов.
   2.2. Уязвимости сетецентрической системы управления, обусловленные использованием в ней двойных информационных технологий.
   2.3. Возможности ассиметричного противодействия сетецентрической системе управления.
3. Предлагаемые направления разработки новых способов подавления телекоммуникационных систем (ТКС), являющихся составными частями

сети связи специального назначения сетецентрической системы управления.

3.1. Актуальность разработки новых способов нарушения процессов передачи информации в сети связи специального назначения в интересах противодействия сетецентрической системе управления.

3.2. Обоснование целесообразности разработки новых способов воздействия на объекты и процессы телекоммуникационных систем в составе сети связи специального назначения на сетевом и транспортном уровнях модели OSI.

4. Предложения по реализации новых способов РЭ ИТВ для подавления ТКС, являющихся составными частями сети связи специального назначения.

4.1. Способы РЭ ИТВ, ориентированные на подавление отдельных сетей радиосвязи множественного доступа на канальном уровне ТКС.

4.2. Способы РЭ ИТВ, ориентированные на нарушение функционирования протоколов маршрутизации на сетевом уровне ТКС.

4.3. Способы РЭ ИТВ, ориентированные на нарушение функционирования протоколов обеспечения качества обслуживания на транспортном уровне ТКС.

1. Сетецентрическая система управления как объект подавления

1.1. Основные особенности сетецентрической системы управления

Анализ концепции сетецентрического управления, выполненный в работе автора [1], показывает, что ее основная идея лежит в области изменения принципов управления. Точнее говоря, это новый способ организации информационного обеспечения процессов управления как реальный инструмент повышения эффективности сил и средств за счет синергетического эффекта.

При иерархической системе управления в ходе взаимодействия между двумя одноранговыми элементами в работу включается вся иерархическая цепочка, вплоть до общего для обоих элементов лица, принимающего решение (ЛПР).

Сетевая организация допускает непосредственное взаимодействие двух одноранговых элементов. В этом случае, потенциальная эффективность сети линейно увеличивается с ростом числа ее элементов и экспоненциально – с ростом числа связей между ними. Однако при внедрении сетевой системы управления иерархическая структура не упраздняется, а лишь добавляются новые связи между одноранговыми элементами. Эти связи призваны повысить эффективность информационного обмена внутри системы, но не заменить собой существующую иерархическую систему управления. Ускорение циркуляции информации в результате внедрения информационных технологий создало предпосылки для организации управления более сложными структурами, включающими в себя элементы, как классических иерархий, так и сетей. Введение в ор-

ганизационную структуру системы управления сетевых элементов позволяет усилить взаимодействие между отдельными ее звеньями и сделать их более информационно-насыщенными. Ранее это было невозможно, поскольку сложность и запутанность таких организационных структур могли только замедлить, а то и вовсе парализовать процесс управления [2].

Существующий подход к структурному построению систем государственного и военного управления, в основном, основывается на использовании жестких иерархических структурах. В такой иерархической структуре отдельные, и в основном автономные объекты управления, объединены в жестко подчиненную структуру в интересах выполнения отдельной задачи. Такому принципу комплексирования свойственны формальные и бюрократические барьеры для прохождения информации по всем подразделениям при выполнении задач органов управления высшего уровня. В иерархических системах управления зачастую используются штатные или системно-зависимые компоненты пунктов управления (ПУ), которые генерируют данные на основе независимых стратегий обработки информации в интересах информационного обеспечения конкретного вышестоящего ПУ, построенного по иерархическому принципу и, как правило, не имеющего горизонтальной интеграции с другими пунктами управления. Информационная интеграция нижестоящих ПУ осуществляется в вышестоящим ПУ. Результатом этого является то, что иерархические системы управления не обеспечивают полноценных горизонтальных связей, что уменьшает их потенциальную эффективность. Таким системам управления свойственны жесткие механизмы координации действий подчиненных сил и средств, а содержание, скорость доставки, форматы и качество информации, в основном, определяются процессами выполнения формальных требований управления. Такой подход создает ряд неизбежных социальных и технических барьеров циркуляции информационных потоков, которые препятствуют интеграции объектов системы управления на тактическом уровне и, в конечном итоге, снижают общую эффективность действий управляемых объектов. Предполагается, что если объекты и ПУ будут интегрированы в единое информационное пространство и будут полностью использовать доступные информационные ресурсы, то возможности, которые появятся в результате этого, значительно повысят существующую эффективность применения современных систем управления [1].

В работе [3] рядом американских экспертов дается следующее определение категории «сетецентричности».

Сетецентричность – характерное свойство системы, включающей в себя различные компоненты: инфраструктуру, платформы, подсистемы, процессы и людей по устойчивому глобально-взаимосвязанному информационно-сетевому взаимодействию, при котором информация для ее совместного использования предоставляются компонентам системы своевременно и бесшовно [3].

Проведенный в работах [1, 3] анализ использования принципа сетецентричности к построению систем управления войсками и оружием позволил выделить основные свойства сетецентрических систем управления:

- как правило, под сетецентричностью понимается принцип организации систем управления, позволяющий реализовать режим высокой осведомлённости о складывающейся ситуации в окружающей среде благодаря формированию и поддержанию целостного и единого информационного пространства, а также включения в процесс непрерывной актуализации информации, получаемой от как можно большего числа источников первичной информации [4];
- для сетецентрической системы управления при формировании решений и управляющих воздействий характерно использование всей доступной информации [5];
- для сетецентрических систем управления характерны принципы открытости, самоорганизации, слабой иерархии в контуре принятия решений, а также способность формировать цели внутри себя на основе высокой осведомлённости о складывающейся ситуации в окружающей среде [6].

При этом сетецентрическая система управления состоит из следующих основных элементов, объединенных в единое информационное пространство (рис. 1) [3]:

- сил и средств наблюдения, которые обеспечивают непрерывный поток актуальной информации о складывающейся обстановке, об эффектах действия собственных сил и средств, а также сил и средств других сторон;
- пунктов управления, в которых производиться комплексирование информации, поступающей от сил и средств наблюдения, ее обработка, и выработка на ее основе стратегии действий ЛПР;
- управляемых сил и средств, реализующих выработанную стратегию действий.

Таким образом, обобщая вышесказанное можно дать следующее определение сетецентрической системе управления.

Сетецентрическая система управления – система управления распределённой системой, в которой ее базовые элементы, такие как силы и средства наблюдения, ПУ и ЛПР, а также управляемые силы и средства объединены в единое информационное пространство. При этом такая система управления характеризуется принципами открытости, самоорганизации, слабой иерархии в контуре принятия решений и способностью порождать цели внутри себя.

Фактически, сетецентрические системы управления – это матричные информационно-управляющие системы, в основе которых лежит глобальная информационная взаимосвязь ее элементов. При этом для такой системы характерна не только вертикальная интеграция между силами и средствами наблюдения, ПУ и управляемыми силами и средствами, но и широко развитая сеть горизонтальных связей на одном и том же уровне управления между разнород-

ными элементами системы, которые являются источниками и потребителями циркулирующей в системе информации [7].

Рис. 1. Общая структура сетецентрической системы управления

В информационной подсистеме сетецентрических систем, гетерогенной по своей сути, эффективно увязаны [7]:

- различные форматы и типы циркулирующей информации;
- разнородные источники и потребители информации;
- различные способы первичной, вторичной и третичной обработки информации.

Как правило, сетецентрические свойства системы реализуются через базовый функционал матричных информационно-управляющих систем, который включает в себя следующие основные составляющие [7]:

- формирование единого координатно-временного поля и привязка к нему всех элементов системы, а также событий и информации, относящейся к ним;
- сбор и комплексирование разнородной информации (в едином координатно-временном поле), полученной от различных источников с перекрёстным уточнением и добавлением;
- анализ и прогноз развития обстановки на стратегическом, оперативном и тактическом уровнях;
- формирование единого информационно-управляющего поля;
- формирование многокритериальной и многоцелевой среды поддержки принятия решений;
- передача информации и управляющих команд управляемым силам и средствам;

- документирование всех событий системы, команд управления и реакции внешней среды.

Отличительной чертой сетецентрических информационно-управляющих систем специального назначения является их глобальность, как в пространственном, так и в функциональном плане. Они функционируют в режиме реального времени и в асинхронном, относительно потока событий, режиме работы [7].

Современные достижения в области информационных технологий и внедрение сетецентрических принципов существенным образом повышают возможности взаимодействия всех компонентов системы государственного и военного управления по обмену информацией. Это ведет к повышению эффективности действий системы по показателю оперативности управления за счет повышения скорости реализации цикла управления (цикла Бойда): «наблюдение – ориентация – решение – действие» [8]. Повышение возможностей элементов системы по информационному взаимодействию также позволяет повысить непрерывность и устойчивость управления. Кроме того, возможности по интенсивному информационному взаимодействию элементов сетецентрической системы управления позволяет обеспечить совместно-распределенную выработку единого замысла и принятие решения. Таким образом, внедрение сетецентрической концепции позволяет ЛПР:

- транслировать собственное понимание и видение вариантов решения задач своим подчиненным для более качественного их уяснения;
- оценивать возможные варианты действий;
- вырабатывать критерии оценки возможные варианты действий;
- принимать решения о своих дальнейших действиях;
- с большей гибкостью и эффективностью реализовывать принятые решения путем многовариантного использования подчиненных сил и средств.

Таким образом, в рамках сетецентрической концепции повышение качества информационного взаимодействия между элементами направлено на повышение плотности связности элементов, интенсивности информационного обмена, осведомленности и взаимопонимания между всеми ЛПР, в интересах повышения качества принятия решений и координации действий управляемых сил и средств. В конечном итоге это ведет к преимуществу сетецентрической системы управления в оперативности, непрерывности и устойчивости управления по сравнению с «традиционными» иерархическими системами.

Переход от иерархической структуры управления к сетецентрической требует преодоления внутренних и внешних организационных и технических барьеров, стоящих на пути повышения качества информационного обмена и синергического применения возможностей систем государственного и военного управления. Такое изменение должно быть поддержано гарантией того, что компоненты этой системы управления будут иметь технические возможности по использованию информационных сетей, независимо от их местоположения или организационной принадлежности [3].

По мнению ряда экспертов [3], к основным признакам сетевых организаций можно отнести следующее [3, 9]:

- наличие единой стратегической цели и отсутствие четкого планирования для нижестоящих уровней управления;
- отсутствие четкой иерархической структуры подчиненности ЛПР, а зачастую и отсутствие центрального руководства;
- децентрализация и параллельность работы ЛПР в различных организациях системы управления;
- многоуровневая структура с разветвленной и сложной системой связей и «вложенных» сообществ исполнителей;
- координация деятельности ЛПР, ПУ и исполнительных сил и средств с использованием возможностей глобальных информационных сетей;
- высокая динамика самоорганизации системы, за счет хорошо налаженного обмена информацией между ее элементами и способности к быстрой их реорганизации в случае необходимости.

Приведенные выше признаки являются характерными для сетевой формы организации, получившие при информатизации общества новый импульс для развития. Эффективность таких сетевых организаций напрямую зависит от интенсивности и качества обмена информацией, при этом данные характеристики должны быть гораздо выше, чем в организациях, построенных на иерархическом принципе [3, 9].

Таким образом, сетецентрические возможности являются эффектом от взаимодействия ЛПР и управляемых сил и средств в едином информационном пространстве. Сетецентрическая система управления получает преимущества за счет того, что может быстрее получать и более эффективно обрабатывать информацию в процессе принятия решений, а также использовать свои информационные возможности для решения поставленных задач более эффективно, целенаправленно и гибко. Это позволяет системам государственного и военного управления, построенным по сетецентрическому принципу, при выполнении задач действовать более эффективно по показателям оперативности, непрерывности и устойчивости управления [3].

1.2. Сетецентрическая среда как основа информационной подсистемы сетецентрической системы управления

Все компоненты сетецентрической системы управления являются информационно-зависимыми и функционируют в так называемой «сетецентрической среде».

Концепция сетецентрической среды описывает возможные способы взаимодействия сил и средств в информационно-сетевой среде. В рамках этой концепции подразумевается, что включение в сеть всех компонентов системы управления создает возможность для беспрецедентного совместного использования информации при взаимодействии, введения адаптивных организационных структур и повышения степени единства действий путем синхронизации и интеграции компонентов сил и средств, в том числе и на самых низших уров-

нях. В данной концепции термины «сеть» и «сетевой» используются как синонимы понятия «сетецентричности» [3].

Сетецентрическая среда – это область, включающая человеческие и технические ресурсы, а также технологии, обеспечивающие эффективное их взаимодействие, функционирующая в интересах ее абонентов и обеспечивающая пользователей необходимой им информацией в понятной им форме и с заданной достоверностью. Эта же среда должна обеспечивать свойства информационной безопасности (конфиденциальности, целостности, доступности) в условиях дестабилизирующих воздействий [3].

Сетецентрическая среда, оперирующая возможностями и условиями (атрибутами), может рассматриваться в виде модели, состоящей из двух обобщенных областей (рис. 2) [3]:

1) области знаний;
2) технической области.

Область знаний включает в себя [3]:

- когнитивную область;
- социальную область.

Техническая область включает в себя [3]:

- физическую область;
- информационную область.

Каждая из областей сетецентрической среды имеет важное самостоятельное значение, но эффективность их совместного функционирования достигается синергией (однонаправленным действием) всех этих элементов. При этом ни одна из этих составных частей сетецентрической среды не может существовать изолированно, так как существуют зависимости между областями, между возможностями внутри самих областей и возможностями в рамках областей. Общие возможности в рамках сетецентрической среды шире, чем просто сумма возможностей области знаний и технической области. Эти две области интегрированы между собой для более полного использования их эмерджентного потенциала [3].

Рассмотрим составные области сетецентрической среды на основе анализа работ [1, 3] более подробно.

Физическая область – это традиционная область размещения ПУ, сил и средств наблюдения, а также управляемых сил и средств. Кроме того, эта область включает в себя физические средства информационно-вычислительных сетей, а также средства сбора, передачи, хранения и обработки информации. Традиционные дестабилизирующие воздействия (такие как средства огневого поражения, средства РЭП и ФП ЭМИ) воздействуют на элементы именно этой области. В сетецентрической системе управления физическую область следует рассматривать как некоторую предельную реально существующую систему, при этом основная часть возможностей и проявлений этой системы управления расположена в других областях, прежде всего, в информационной. Однако достигаемые эффекты в этих областей проецируются обратно на физическую область.

В многослойной модели сетецентрической среды физическая область соответствует *физическому слою*, который содержит все физически реальные средства сбора, передачи, хранения и обработки информации, а также ЛПР, средства поддержки принятия решений и управляемые силы и средства.

В сетецентрических системах государственного и военного управления технической основой, физически связывающей все элементы, включенные в сетецентрическую среду, является *сеть связи специального назначения*.

Сеть связи специального назначения (СС СН) – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [25].

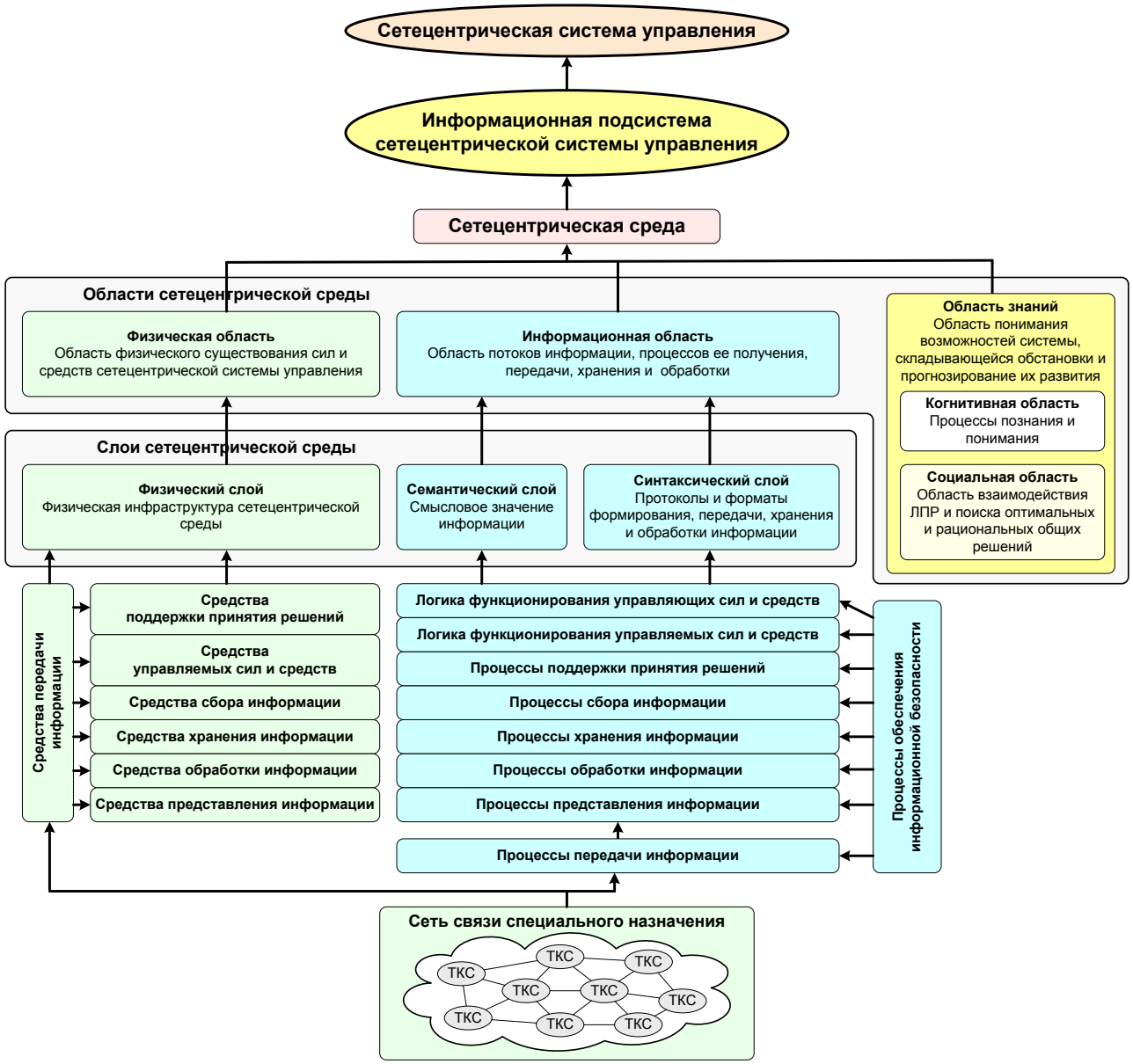

Рис. 2. Структура сетецентрической среды

Информационная область – это область, где создаётся, добывается, обрабатывается и распределяется информация. Эта область включает в себя системы сбора и передачи информации, модели хранения и обработки информации и т. д. Это главная среда сетецентрической системы управления, которая выдели-

лась в самостоятельную категорию – *инфосферу*. Информационная область в сетецентрической системе управления связывает между собой все ее элементы и является ключевой. При этом преимущества или проблемы в накоплении, передаче, обработке и обеспечении безопасности информации приобретают в этой области решающее значение.

В состав информационной области входит два слоя:

1) *семантический слой*, который содержит смысловое значение информации;
2) *синтаксический слой*, который содержит протоколы, форматы и правила формирования, передачи, хранения и обработки информации;

Когнитивная область. Когнитивной областью является сознание ЛПР. Именно в когнитивной области располагаются такие явления, как психика ЛПР, доктрина, тактика, и процессы осознания обстановки. Таким образом, когнитивная область – это сфера сознания, и прежде всего, процессы познания и осознания.

Социальная область. Социальная область представляет собой поле взаимодействия ЛПР. Здесь преобладают исторические, культурные, религиозные ценности, психологические установки и этнические особенности. В социальной области развёртываются отношения между людьми, выстраиваются естественные иерархии в группах – лидеры, ведомые, пассивные массы и т. д., складываются системы групповых отношений.

Функционирование в сетецентрической среде в значительной степени зависит от эффективности функционирования каждой из областей, а также от качества взаимосвязей между областями. При этом *область знаний* включает понимание индивидуальных и коллективных возможностей, а также принятие решений, появляющиеся в результате сетецентрического принципа взаимодействия элементов системы управления.

Сетецентрическая среда обеспечивает коллективное распределение и обработку информации. Создание сетецентрической среды предполагает развертывание мощной информационной инфраструктуры, которая обеспечивает:

- сбор информации с разнородных средств наблюдения в интересах ее последующего комплексирования;
- высокопроизводительную обработку информации в реальном времени с отображением реальной ситуации с высокой степенью достоверности;
- обеспечение непрерывного накопления и хранения информации, а также доступ к этим информационным базам ЛПР, всех уровней управления;
- единое информационное пространство для информационного обмена всех элементов сетецентрической системы управления, а также их непрерывный и глобальный доступ к информационным ресурсам системы;
- устойчивость, непрерывность и оперативность управления распределенными силами и средствами, осуществляющими взаимоувязанный комплекс операций в интересах достижения единой цели;

- обеспечение встроенных способностей к самозащите и противодействию воздействию широкого спектра средств и способов преднамеренного дестабилизирующего воздействия.

2. Анализ основных уязвимостей сетецентрической системы управления и перспективных возможностей ассиметричного воздействия на нее

2.1. Уязвимости сетецентрической системы управления, обусловленные высокой информационной зависимостью всех ее элементов

Анализ, представленный в работе [1], показывает, что массовое объединение территориально-распределенных ПУ различного уровня иерархии и разнородных управляемых сил и средств на основе единого информационного пространства может породить проблемы, как с безопасностью информации, так и со сложностью ее формирования, передачей и обработкой. Чрезмерная опора на новые информационные технологии может привести к возникновению новых уязвимостей, которые, в свою очередь, могут быть использованы для разработки новых способов дестабилизирующих воздействий на сетецентрические системы управления.

Анализ и обобщение опыта использования сетецентрических систем для управления войсками и оружием, представленный в работе [1], выявил ряд их проблемных аспектов. К числу главных из них относятся [1, 10-12]:

- высокая сложность сетецентрических систем управления, многокритериальность управления, необходимость управления и координации разнородных сил и средств, зачастую имеющих различные локальные цели и функции;
- чрезмерная информационная зависимость всех элементов сетецентрической системы;
- учет изменения среды функционирования в сетецентрической системе управления зависит от способности сил и средств наблюдения генерировать новую информацию, а также от быстродействия подсистемы информационного обмена;
- резкое ускорение цикла управления, при этом предельная скорость этого цикла определяется возможностями по обработки информации всеми элементами сетецентрической системы управления;
- недостаточно проработанные методы эффективной и быстрой автоматической обработки больших информационных массивов, а также информации о быстропротекающих процессах на основе технологий «Больших Данных»;
- многократная обработка информации о среде функционирования, ее многоуровневая фильтрация и автоматическое сопоставление с ранее известными фактами, а также ограниченные возможности представления всего массива информации через человеко-машинные интерфейсы,

ведут к упрощенному видению обстановки ЛПР и, в конечном итоге, к ее некорректной оценке;
- переоценка способности человека адекватно перерабатывать большой объем противоречивой информации, а также принимать решения в условиях информационной перегрузки;
- возрастание в сетецентрической системе управления роли информационной подсистемы, ее способности поддерживать устойчивый информационный обмен между элементами системы, гарантировать доступ к информационным ресурсам системы, с заданной своевременностью и достоверностью осуществлять передачу информации, при этом обеспечивая требуемый уровень ее безопасности;
- уязвимость технических средств сетецентрической системы управления к преднамеренным дестабилизирующим воздействиям, в первую очередь к средствам и способам РЭП и ИТВ.

Таким образом, сетецентрические системы управления содержат в себе уязвимости, которые в основном связаны с процессами сбора, передачи и обработки информации, а также с обеспечением информационной безопасности. Анализ опыта применения сетецентрических систем управления для управления войсками и оружием, выполненный сотрудниками корпорации RAND, показал, что по мере того как сетецентрические системы становятся все более эффективными в области управления, они становятся все более уязвимыми к контратакам на свою информационную инфраструктуру [10, 11].

2.2. Уязвимости сетецентрической системы управления, обусловленные использованием в ней двойных информационных технологий

Вероятность эффективного противодействия сетецентрическим системам управления повышается за счет широкого использования для создания технических средств систем специального назначения, в том числе и сетецентрических систем государственного и военного управления, так называемых двойных технологий, и, особенно, относящихся к информационным технологиям.

Как показал анализ, проведенный в работах [13-15], в последнее время большинство прорывных технологий, используемых в системах специального назначения ведущих зарубежных стран, являются коммерческими разработками, а не результатами специальных исследований. К числу основных факторов, определяющих широкое внедрение двойных технологий, можно отнести [13]:
- высокую стоимость специальных разработок, при этом их функционал, как правило, дублирует коммерческие продукты;
- невозможность столь же масштабного, как в коммерческом секторе, привлечения средств и специалистов к прорывным разработкам и исследованиям;
- трудности в использовании зарубежных прорывных разработок и привлечения иностранных специалистов к исследованиям;

- необходимость снижения стоимости систем специального назначения без потери их функциональности.

Однако эффективность использования двойных и коммерческих технологий создает ряд серьезных проблем, поскольку при этом повышается уязвимость конечных систем [13, 14].

Во-первых, использование двойных технологий в системах специального назначения означает, что они также применяются и в коммерческой сфере. При этом документация и модернизированные технические образцы в коммерческие сфере, как правило, становятся доступны раньше, чем они будут внедрены в производство систем специального назначения. Таким образом, существует возможность заблаговременного получения доступа к новейшим технологиям создаваемых специальных систем.

Во-вторых, использование двойных технологий ведет к тому, что коммерческие системы и системы специального назначения обладают практически идентичными структурой, свойствами, а также характеристиками. Это создает следующее противоречие. С одной стороны, коммерческие системы разрабатываются для эксплуатации в гораздо более благоприятных условиях, чем специальные системы. С другой – заблаговременный доступ к этим двойным технологиям позволяет в сжатые сроки разрабатывать актуальные способы противодействия новым системам специального назначения.

Все вышеуказанное в полной мере относится к сетецентрической системе государственного и военного управления. Как было указано ранее, наиболее критическим элементом такой системы управления является информационная подсистема. И именно в этой подсистеме наблюдается широкое заимствование технологий сбора, хранения, передачи и обработки информации из коммерческой сферы. Определенное запаздывание в конце XX века в использовании результатов информационно-технической революции в системах специального назначения привело к тому, что разработчики данных систем стали активно стали использовать готовые информационные технологии из коммерческой сферы с целью закрыть имеющиеся «информационные пробелы». Как показано в работах М.А. Шнепс-Шнеппе [16-20], В.А. Нетеса [21], Н.А. Соколова [22], а также в предшествующей работе автора [14], непродуманное использование в информационной подсистеме сетецентрической системы управления коммерческих технологий связи может существенно снизить эффективность данной подсистемы, а также стать причиной ее низкой устойчивости и высокой уязвимости.

2.3. Возможности ассиметричного воздействия на сетецентрическую систему управления

В настоящее время в ведущих зарубежных странах резко актуализированы исследования, посвященные поиску возможностей асимметричного противодействия современным высокотехнологическим системам сетецентрического управления [1].

Интересно то, что поиск асимметричных действий актуален как для государств, занимающих позицию бесспорных технологических лидеров, так и для менее технологически развитых государств. Это связано с необходимостью превентивного поиска мер, направленных на устранение уязвимостей систем сетецентрического управления и воспрепятствованию использования против них ассиметричных способов противоборства. Отправной точкой пристального внимания к асимметричным действиям служит понимание того обстоятельства, что, с одной стороны, сетецентрическая система управления дает существенные преимущества, а, с другой, – в ней имеются вышеуказанные уязвимости, которые не позволяют полностью гарантировать устойчивость управления в условиях преднамеренных дестабилизирующих воздействий.

В работе автора [1] был проведен анализ возможностей по асимметричному противодействию по отношению к сетецентрической системе управления на примере систем управления войсками и оружием. Дадим следующие определения.

Асимметричные действия – реализация собственной стратегии действий, отличных от реализуемых или навязываемых противником, которая позволяет добиться преимуществ, использовать уязвимые места противника, завоевать инициативу и достичь большей свободы собственных действий [13].

Асимметричные действия – уход одной из сторон (стороны, не имеющей достаточного количества ресурсов – производственных, интеллектуальных, научных, технологических и т. п.) от прямого противоборства к концентрации усилий в областях, где удалось выявить уязвимость и слабость противника [23].

В технической сфере асимметричное противодействие может выражаться в выводе из строя дорогостоящих и наиболее уязвимых подсистем при помощи дешевых и низко затратных средств. Ассиметричное противодействие является эффективным способом нарушения функционирования сетецентрической системы управления. При этом в работе [10] указывается, что к одному из основных способов ассиметричного противодействия относится информационное противоборство во всех его проявлениях.

Анализ, проведенный в работах А.В. Копылова [11, 12], позволил сформировать следующие критические аспекты сетецентрических систем управления, делающих возможным ассиметричное противодействие им за счет использования средств РЭП и ИТВ:

- применение средств РЭП, средств ФП ЭМИ и устройств генерации направленной энергии против средств физического слоя информационной подсистемы с целью их поражения или временного нарушения работоспособности;
- применение ИТВ против синтаксического слоя информационной подсистемы с целью нарушения корректности процессов формирования, хранения, передачи, обработки и воспроизведения информации, логики функционирования АСУ и т. д.;
- применение ИТВ против семантического слоя информационной подсистемы с целью искажения или уничтожения информации, циркули-

рующей в сетецентрической системе управления, или блокирование доступа к ней.

В работе [1] показано что, против элементов физической инфраструктуры сетецентрической среды применяются, как правило, средства огневого поражения. Более оправданным по критерию эффективность/затраты является применение средств РЭП и ФП ЭМИ, которые могут обеспечить блокирование значительного пространственного сегмента средств сетецентрической системы управления при определенных энергетических затратах, но без существенных затрат материальных средств (таких как оружие и боеприпасы).

Еще более эффективным по вышеуказанному критерию является применение ИТВ, ориентированных на синтаксический или семантический слой информационной подсистемы сетецентрической среды [24].

Наиболее эффективными являются ИТВ, ориентированные на семантический слой. Для этого требуется внедрение ложных информационных ресурсов в сетецентрическую среду или доступ к семантике циркулирующих в ней информационных потоков. Данные ИТВ могут быть направлены на изменение информационных ресурсов, важных для проведения операции, ввод ложной информации или ложных источников информации, которые сформируют некорректное видение обстановки и, в конечном итоге, навяжут сетецентрической систем управления неверную стратегию действий или будут способствовать бескомпроматному перехвату управления ее силами и средствами. Однако в случае корректного функционирования средств обеспечения информационной безопасности в сетецентрической среде, проведение ИТВ на семантический слой является затруднительным. В этом случае могут быть использованы ИТВ, ориентированные на синтаксический слой. При этом наиболее простым вариантом таких ИТВ является нарушение именно процессов передачи информации. Значимое нарушение этих процессов приведет к критическому снижению доступности информационных ресурсов сетецентрической системы, снижению уровня осведомлённости о складывающейся ситуации, увеличению длительности цикла управления, и, в конечном итоге, – к снижению качества управления по показателям оперативности, непрерывности и устойчивости [24].

В качестве источников ИТВ могут быть использованы имеющиеся средства РЭП, а в качестве места приложения данного воздействия – радиосети и радиоканалы в составе сети связи, являющейся физической основой сетецентрической среды. Такие ИТВ могут быть направлены на нарушение процессов информационного обмена, блокировку доступа к критическим информационным ресурсам и разрушению связности информационной подсистемы. При этом для эффективного достижения этих целей такие ИТВ должны учитывать особенности протоколов информационного обмена, а также особенности построения и функционирования сети связи сетецентрической среды.

В значительной мере эффективному воздействию ИТВ, ориентированных на нарушение процессов информационного обмена в сетецентрической среде, способствует факт широкого использования коммерческих технологий связи в составе сетевого и транспортного уровней сетей связи. Это позволяет заблаговременно учесть в способах подобных ИТВ особенности функционирования

протоколов сетевого и транспортного уровня, а также отработать способы применения таких ИТВ на сетях связи общего пользования, использующих аналогичные протоколы, а уже потом использовать их для противодействия сетецентрическим системам государственного и военного управления.

Таким образом, по мере информационного насыщения государственных и военных сетецентрических систем управления повышается не только их эффективность, но и уязвимость. Ассиметричное противодействие сетецентрической системе управления может быть организованно путем выявление критически значимых элементов в информационной подсистеме и их вывод из строя при помощи ИТВ, ориентированных на нарушение информационного обмена. Это может вызвать каскадные и системные эффекты, совокупный ущерб от которых сопоставим с результатами применения по сетецентрической системе управления стратегического оружия.

3. Предлагаемые направления разработки новых способов подавления телекоммуникационных систем, являющихся составными частями сети связи специального назначения сетецентрической системы управления

3.1. Актуальность разработки новых способов нарушения процессов передачи информации в сети связи специального назначения в интересах противодействия сетецентрической системе управления

Анализ структуры построения сетецентрических систем управления показал, что иерархию ее физических элементов, соответствующих процессам информационного обмена, можно представить в виде схемы, представленной на рис. 3.

Информационная подсистема, основой которой является единая система связи, сетецентрических систем государственного и военного управления объединяет средства сбора, хранения, обработки и представления информации.

В соответствии с ГОСТ РВ 52216-2994 системе связи и сети связи даны следующие определения.

Система связи – часть системы управления, представляющая собой совокупность взаимоувязанных и согласованных по задачам, месту и времени действий узлов и линий связи различного назначения, развертываемых или создаваемых по единому плану для управления силами и средствами.

Сеть связи – часть системы связи, состоящая из узлов связи и соединяющих их линий связи и предназначенная для предоставления услуг связи абонентам, принадлежащим системам управления силами и средствами, находящимися в зоне ее функционирования.

При этом в Законе РФ «О связи» [25] конкретизируется категория сетей связи, предназначенных для нужд систем государственного и военного управления.

Сеть связи специального назначения – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [25].

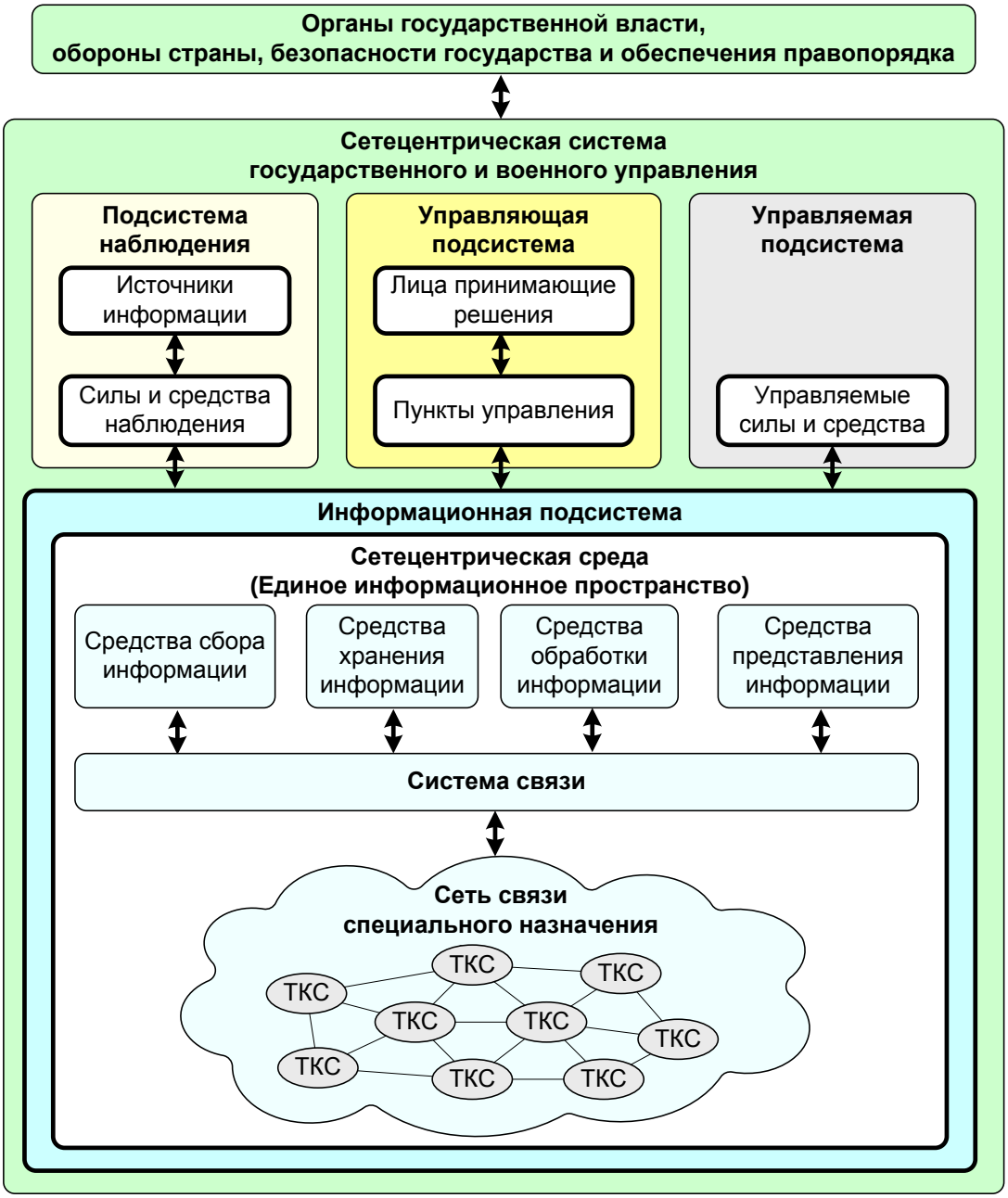

Рис. 3. Иерархия физических элементов сетецентрической системы управления, соответствующая процессам информационного обмена

Таким образом, можно сделать вывод, что технической основой информационной подсистемы сетецентрической системы государственного и военного управления является СС СН, которая состоит из узлов и линий связи. Необходимо отметить, что линии связи в составе СС СН могут быть различного рода (в самом общем случае – радиосвязи, оптико-электронной и проводной связи). При этом узлы в СС СН объединяются в области (домены) маршрутизации, которые соответствуют отдельным ТКС в составе СС СН. В свою очередь ТКС могут включать в себя линии связи различных родов (рис. 4). Еще одной осо-

бенностью построения СС СН в составе информационной подсистемы сетецентрической системы управления является то, что структура такой СС СН становится более гибкой, децентрализованной, сетевой, многоэшелонированной и, кроме того, она более не является жестко привязанной к структуре и иерархии элементов системы управления [14, 15].

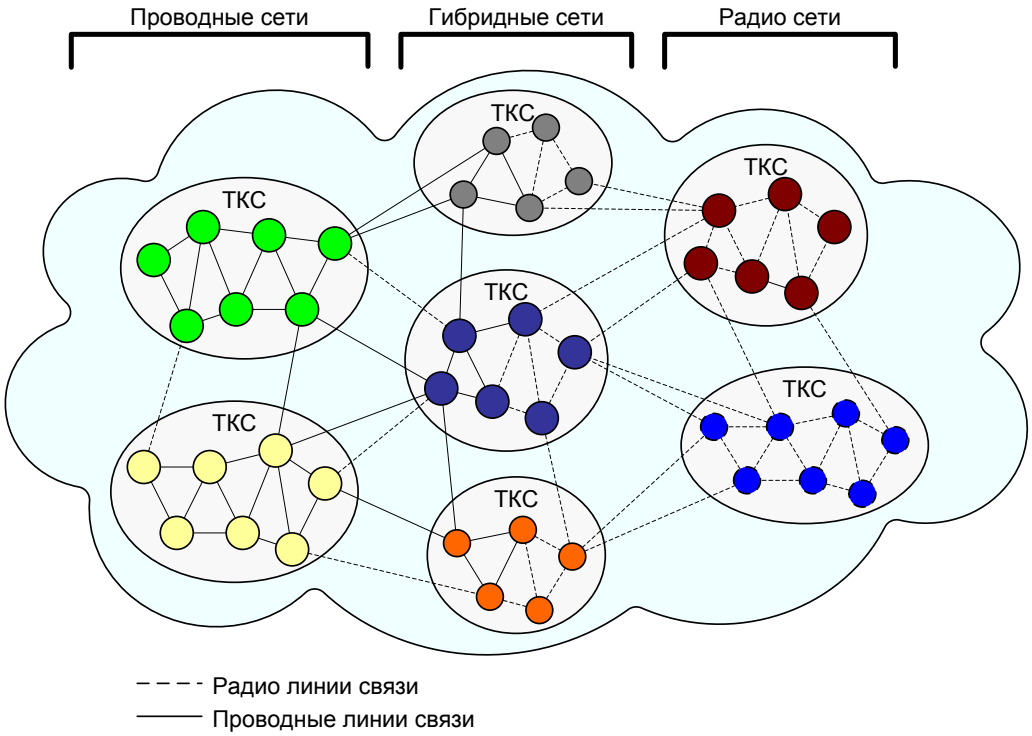

Рис. 4. Телекоммуникационные системы и линии связи различных родов в составе сети связи специального назначения

Эти особенности структурного построения СС СН существенно сужают возможности по эффективному нарушению процессов передачи информации в сетецентрической системе управления по сравнению с «традиционной» иерархической системой.

Традиционно, для нарушения процессов передачи информации против СС СН использовалось огневое поражение и радиоэлектронное поражение (средствами ФП ЭМИ) узлов сети, а также радиоэлектронное подавление линий радиосвязи.

Проведенный в работах автора [1, 24, 26, 27] анализ использования существующей «традиционной» тактики радиоэлектронного подавления и способов применения средств РЭП показал, что оно неэффективно против сетецентрических систем управления. Основанный на «традиционном» подходе к воздействию РЭП пример нарушения работы иерархической системы управления (тактической авиацией) представлен на рис. 5. В этом примере нарушение управления достигалось при воздействии средств РЭП на любом уровне иерархической системы управления, в результате блокирования прохождения информации к управляемому средству, и, как следствие, невыполнения им поставленной задачи. Однако в сетецентрической системе управления полностью подавить пути передачи управляющей информации и команд практически не-

возможно. Для нарушения работы такой сетецентрической системы (рис. 5) необходимо обеспечить радиоэлектронное подавление всех путей передачи информации или вывести из строя все ее технические средства. Фактически значимый эффект нарушения процессов передачи информации в сетецентрической системе управления может быть достигнут, если в СС СН блокируется значительный сегмент или исключается передача информации по всем каналам связи в определённом районе.

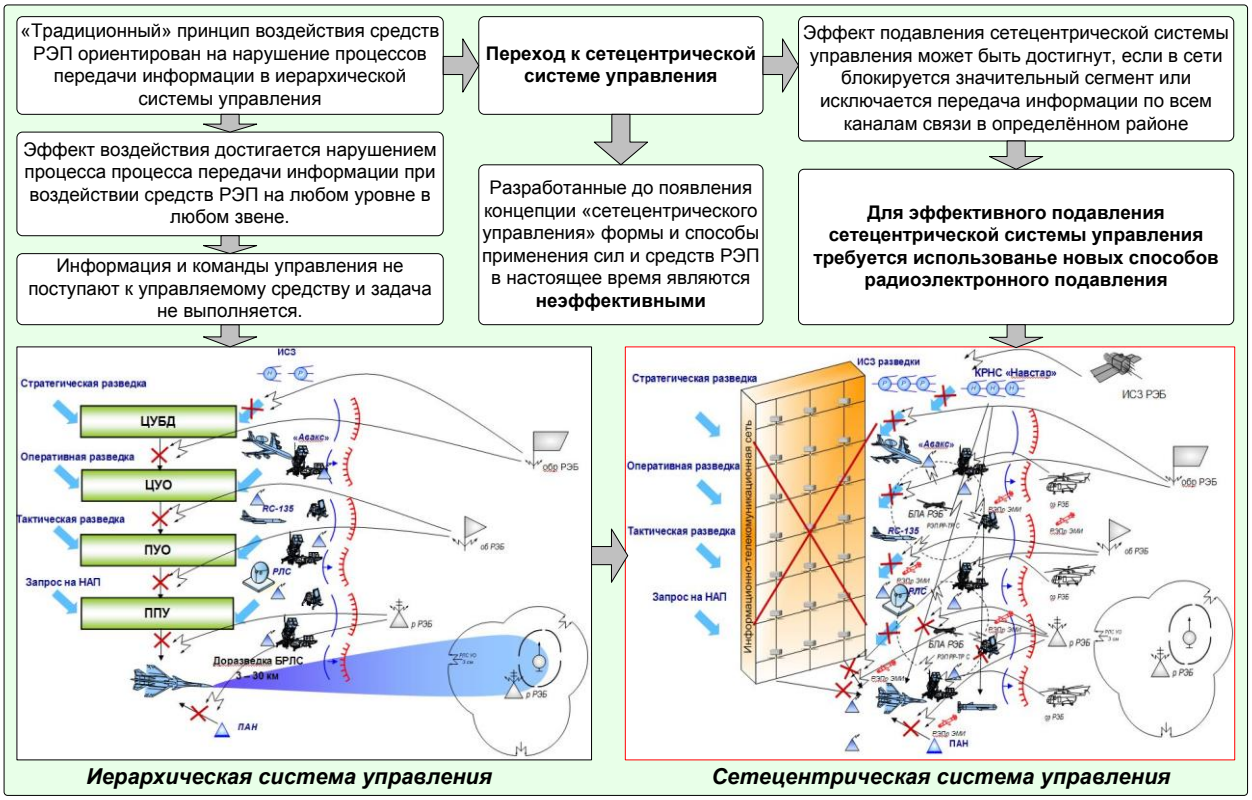

Рис. 5. Примеры нарушения процессов передачи информации путем применения средств РЭП в иерархической и сетецентрической системах управления

Еще одним способом нарушения процессов передачи информации в сетецентрической системе управления является использование ИТВ. Использование ИТВ имеет относительно недавнюю историю, однако формы и способы их применения стремительно развиваются. Как показан анализ, проведенный в работе [1], к наиболее опасным и распространенным ИТВ, ориентированным на нарушение доступности информационных ресурсов, относится удаленная сетевые атаки типа «отказ в обслуживании» – «Denial of Service» (DOS) и «Distributed Denial of Service» (DDOS). Несмотря на свою эффективность, эти атаки с высокой степенью достоверности обнаруживаются и блокируются средствами систем обнаружения вторжений (IDS – Intrusion Detection System) [28]. Кроме того, особенностью таких ИТВ является то, что они ориентированы на нарушение доступности отдельных узлов или подсетей в составе СС СН, что является эффективным для нарушения процессов передачи в низкосвязных или иерархических сетях. Однако, как показано выше, СС СН в составе сетецентри-

ческой системы управления, имея достаточно разветвленную сетевую структуру, может реконфигурировать пути передачи команд и управляющей информации, что делает такие ИТВ эффективными, только если они подавляют всю СС СН или ее значимый сегмент. В дополнении к этому отметим, что для проведения ИТВ типа «отказ в обслуживании» требуется получить доступ и внедрить субъект атаки в СС СН, что представляет существенные трудности для реальных сетей специального назначения, имеющих многоуровневые средства защиты и обеспечения безопасности.

При организации воздействия на процессы передачи информации в СС СН необходимо учитывать еще один важный факт. Воздействие на сетецентрические системы государственного и военного управления без каких-либо ограничений проводится в военное время. Однако в мирное время и в угрожаемый период такое воздействие средствами РЭП или ИТВ с высокой долей вероятности будет расценено как акт военного нападения на критическую инфраструктуру государства. В работе [1] показано, что современное невоенное противоборство между государствами, в том числе и в мирное время может вестись средствами информационного воздействия, при этом совокупность таких воздействий классифицируются как «информационная война».

Информационная война – комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника [1, 9].

Информационная война ведется путем проведения взаимосвязанных по цели, месту и времени информационных операций.

Информационная операция – это комплекс взаимосвязанных по цели, месту и времени мероприятий, акций и воздействий, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника [1, 9].

Как показано в работе [1], воздействия средствами РЭП, а также ведение информационного противоборства путем воздействия ИТВ на критическую информационную инфраструктуру противника является составными частями информационной операции. Достигаемым эффектом информационного превосходства при нарушении процессов передачи информации является блокирование и недопущение доступа противостоящей стороны к собственных информационным ресурсам, а также существенное увеличение длительности цикла управления, и в конечном итоге – критическое снижение качества сетецентрической системы государственного и военного управления, по показателям оперативности, непрерывности и устойчивости.

Характерной особенностью информационной войны является то, что она ведется, в том числе, и в мирное время, и в угрожаемый период. Следовательно, воздействия, осуществляемые в рамках конкретной информационной операции и направленные на нарушение процессов передачи информации в сетецентри-

ческой системе государственного и военного управления, должны носить бескомпроматный характер. Использование бескомпроматных воздействий в мирное время и в угрожаемый период целесообразно в целях недопущения компрометации стороны, проводящей информационную операцию, и, соответственно, перерастания информационной войны в прямое военное противоборство.

Требуется отличать скрытность воздействия от бескомпроматности воздействия.

Скрытность воздействия – способность воздействия (преднамеренного дестабилизирующего воздействия, воздействия средством РЭП, информационно-технического воздействия и т. д.) вызвать заданные структурные и/или функциональные изменения в объекте воздействия и при этом не быть обнаруженным.

Бескомпроматность воздействия – способность воздействия (преднамеренного дестабилизирующего воздействия, воздействия средством РЭП, информационно-технического воздействия и т. д.) вызвать заданные структурные и/или функциональные изменения в объекте воздействия, при этом не обнаружить источник (субъект) воздействия и не оставить улики, его компрометирующие.

Таким образом, свойство бескомпроматности делает акцент на скрытности источника (субъекта) воздействия, а не самого воздействия.

При этом подавляющая часть современных «традиционных» средств и способов РЭП, а также широко распространенных ИТВ типа DOS/DDOS атак не способны эффективно и бескомпроматно нарушать процессы передачи информации в СС СН являющихся частью сетецентрической системы управления. В связи с этим актуальным является формирование направлений исследований в интересах разработки новых способов воздействий, основанных на РЭП и ИТВ, для эффективного и бескомпроматного нарушения процессов передачи информации в СС СН в целях противодействия сетецентрической системе государственного и военного управления.

3.2. Обоснование целесообразности разработки новых способов воздействия на объекты и процессы телекоммуникационных систем на сетевом и транспортном уровнях модели OSI

Исходя из актуальности поиска новых направлений исследований в интересах разработки новых способов воздействий, основанных на РЭП и ИТВ, для эффективного и бескомпроматного нарушения процессов передачи информации в СС СН, представляется необходимым сформулировать ряд принципиальных подходов к реализации указанных способов.

В настоящее время современные силы и средства РЭП традиционно используются для проведения операций с целью дезорганизации систем управления противника. С целью рационального использования имеющегося ресурса техники РЭП, целесообразным является использование новых РЭ ИТВ, основанных на развитии форм и способов применения уже существующих средств

РЭП за счет внедрения новых режимов их работы. При этом предполагается дополнить режимы работы средств РЭП новыми способами постановки радиоэлектронных помех, которые учитывают особенности передачи информации в ТКС входящих в СС СН сетецентрической системы управления.

Как показано выше, СС СН состоит из ограниченного количества взаимодействующих ТКС, причем в составе последних могут находиться как отдельные линии радиосвязи (ЛРС), так и целые сети радиосвязи (СРС). При реализации РЭ ИТВ, ориентированных на бескомпроматное подавление ТКС в составе СС СН, требуется учитывать особенности процессов межсетевого обмена, маршрутизации, а также динамики процессов реконфигурации. При этом, предлагается перейти от принципа подавления отдельных элементов радиосегмента ТКС, таких как ЛРС и СРС, к использованию этих элементов в качестве своеобразных «точек входа» для РЭ ИТВ, которые будут нарушать сетевые процессы передачи информации и распространять свое дестабилизирующее воздействие на ТКС в целом, в том числе и на ее проводной сегмент.

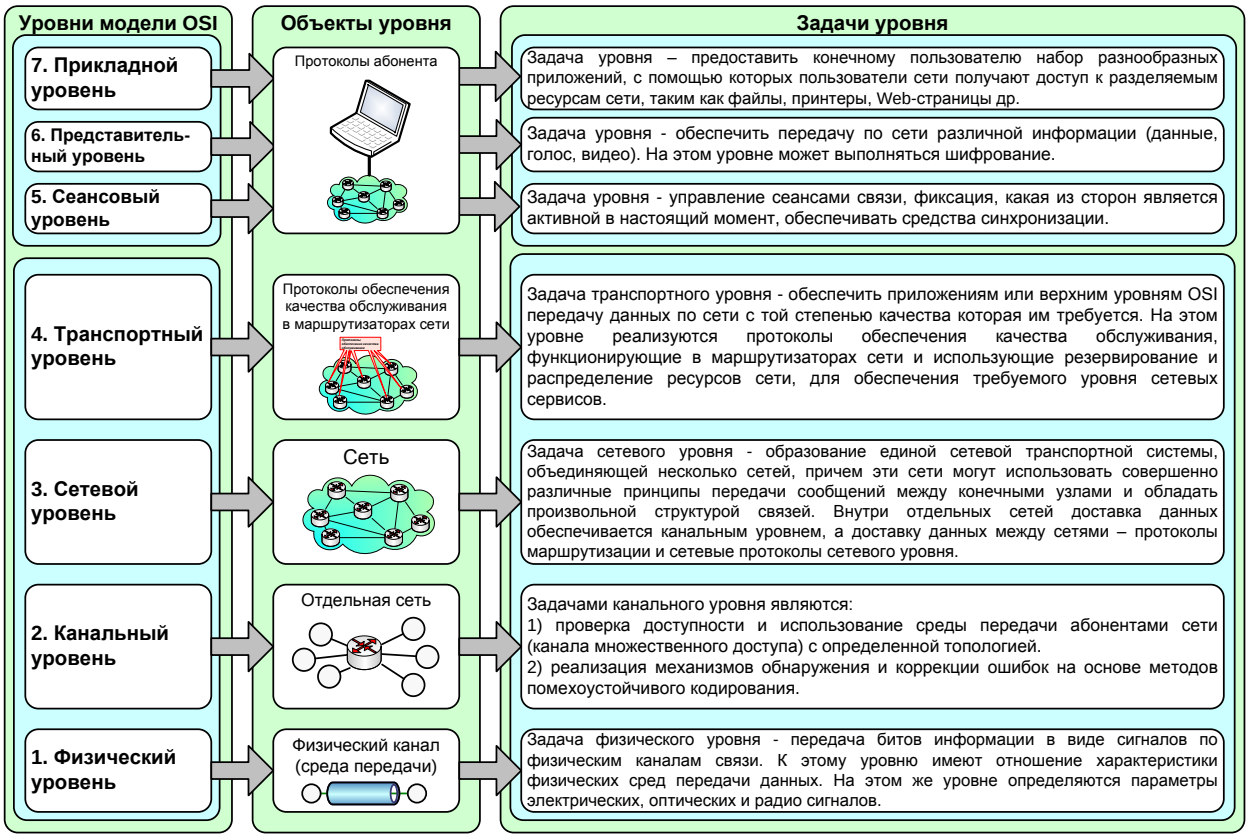

Рис. 6. Функции и задачи различных уровней модели OSI

Логика функционирования систем связи традиционно декомпозируется на семь функциональных уровней в соответствии с моделью открытых систем – OSI (Open Systems Interconnection) – рис. 6. Такая декомпозиция позволяет описать процессы передачи в системе связи с различной степенью функциональной абстракции – от физического уровня, на котором рассматривается передача сигналов в физической среде, до сетевого и транспортного, на которых рассматриваются процессы функционирования систем связи в целом. При этом

следует отметить тот факт, что значимыми для описания процессов передачи в сетях связи (в том числе и для ТКС и СС СН) являются только четыре нижних уровня модели OSI (физический, канальный, сетевой, транспортный), так как именно они соответствуют аппаратно-программным средствам сети. Верхние же уровни модели OSI (сеансовый, представительный, прикладной) реализуются только программными средствами абонента.

До последнего времени основная часть исследований в области радиоэлектронного подавления была сконцентрирована на задачах подавления отдельных ЛРС, т. е. на подавлении объекта физического уровня модели OSI. Имелись отдельные исследования, посвященные подавлению СРС с учетом их структуры, логики функционирования, и ценности передаваемой информации, однако они не носили системно-массового характера.

Вместе с тем, анализируя возможности использования «традиционных» средств РЭП [1], можно прийти к выводу, что с их помощью возможны более глубокие воздействия на ТКС с целью нарушения функционирования и других объектов транспортной подсистемы модели OSI (на физическом, канальном, сетевом и транспортном уровнях).

Объектами радиоэлектронного воздействия на физическом уровне OSI традиционно являются РЭС и ЛРС. На канальном уровне OSI к таким объектам относятся каналы множественного доступа, предназначенные для образования отдельных радиосетей (например, на основе протоколов TDMA, ALOHA, DVB-RSC). К объектам радиоэлектронного воздействия на сетевом уровне OSI можно отнести узлы и каналы связи ТКС, а также протоколы маршрутизации и сигнализации, обеспечивающие процессы передачи данных в ней. На транспортном уровне к объектам радиоэлектронного воздействия следует отнести протоколы и аппаратно-программные средства обеспечения качества обслуживания информационных потоков, передаваемых по ТКС. При этом воздействие средств РЭП приводит к различным негативным эффектам на различных уровнях OSI, некоторые из которых представлены на рис. 7.

Современная методология применения «традиционных» средств РЭП ставит своей целью снижение качества обслуживания QoS (Quality of Service) отдельных ЛРС и СРС ниже значений, определенных требованиями к качеству связи. Таким образом, основная часть исследований по РЭП посвящена решению задач подавления на физическом уровне модели OSI. Однако объединение отдельных сетей, в единую ТКС ведет к тому, что подавление отдельных ЛРС или СРС в ее составе не приведет к значимому ущербу. Подавление отдельных элементов ТКС лишь послужит причиной перемаршрутизации информационных потоков в сети без снижения своевременности передачи, без нарушения доступности информационных ресурсов сетецентрической среды, а также без снижения оперативности передачи управляющей информации сетецентрической системы управления.

Рис. 7. Эффекты, возникающие на различных уровнях функционирования ТКС в результате РЭ ИТВ

Воздействие «традиционных» средств и комплексов РЭП на системы связи происходит на физическом уровне модели OSI. Однако, как было показано ранее, это воздействие проявляется также и на вышестоящих уровнях транспортной подсистемы ТКС – канальном, сетевом и транспортном уровнях модели OSI. Предлагаемые в данном исследовании новые РЭ ИТВ основаны на использовании ранее не рассматриваемых эффектов от воздействия радиоэлектронных помех на канальном, сетевом и транспортном уровнях OSI. Именно за счет применения РЭ ИТВ предполагается решение проблемы подавления ТКС, которые являются базовым элементами СС СН. При этом СС СН, в свою очередь, является технической основой информационной подсистемы сетецентрической системы управления. Предполагается, что непосредственным объектом воздействия РЭ ИТВ будут отдельные ЛРС и СРС, функционирующие в составе ТКС.

В настоящее время для решения задач обеспечения качества обслуживания в ТКС проводятся многочисленные исследования эффективности функционирования сетей связи и коммутационных устройств различного уровня в условиях передачи трафика сложной структуры (наличие самоподобных свойств, непуассоновское распределение времени поступления пакетов и др.), а также маршрутизации информационных потоков в сетях с динамически изменяемой топологией. В исследованиях по этой тематике указывается на значительное снижение пропускной способности сетей и своевременности передачи информационных потоков в них в случае, если топология сети динамически меняется.

Предлагается использовать результаты данных исследований для оценки качества обслуживания ТКС и для разработки новых решений по их подавлению.

Предполагается использовать отображение РЭ ИТВ на физическом уровне на более высокие уровни функционирования ТКС – канальный, сетевой и транспортный. Для формализации таких процессов отображения, ТКС рассматривается как сложная многоуровневая система. При этом, элементами такой системы являются отдельные протоколы, совместно реализующие функционал каждого конкретного уровня. Каждый из протоколов любого уровня может подвергнуться целевому воздействию РЭ ИТВ, что незамедлительно скажется на процессе функционирования других взаимосвязанных с ним протоколов, а также всей ТКС в целом. При этом необходимо сосредоточиться на поиске способов РЭ ИТВ обладающих следующими свойствами:

- бескомпроматными относительно субъекта воздействия на физическом уровне и способными преодолевать меры помехозащиты, используемые в современных средствах радиосвязи ТКС СС СН;
- учитывающие сложность и многоуровневость ТКС, а также ориентированные на усугубление внутренних локальных конфликтов и противоречий между отдельными протоколами в ТКС;
- учитывающие динамические процессы функционирования ТКС ориентированные на перевод протоколов ТКС в нестационарные и нестабильные режимы функционирования, которые, в конечном итоге, приводят к значимому снижению устойчивости ТКС.

РЭ ИТВ обладающие вышеуказанными свойствами, фактически соответствуют новым бескомпроматным способам радиоэлектронного воздействия на физическом уровне, которые, с одной стороны, не будут обнаруживаться и блокироваться существующими средствами помехозащиты, а, с другой стороны, – будут ориентированы на снижение эффективности функционирования протоколов сетевого и транспортного уровня ТКС путем инициализации ряда дестабилизирующих и нестационарных эффектов на этих уровнях (рис. 8).

Широкое внедрение таких РЭ ИТВ в территориально-распределенные средства РЭП позволит реализовать следующие основные направления ассиметричного противодействия сетецентрической системе управления:

- эффективно и бескомпроматно нарушать процессы передачи информации в сетецентрических системах управления при проведении информационных операций в мирное и военное время;
- обеспечивать снижение связности сети информационных подсистем сетецентрических систем управления, снижение скорости и интенсивности информационного обмена в них, а также обеспечивать значимое снижение доступности их информационных ресурсов;
- обеспечить увеличение длительности цикла управления, и, в конечном итоге, – снижение качества управления, по показателям его оперативности, непрерывности и устойчивости.

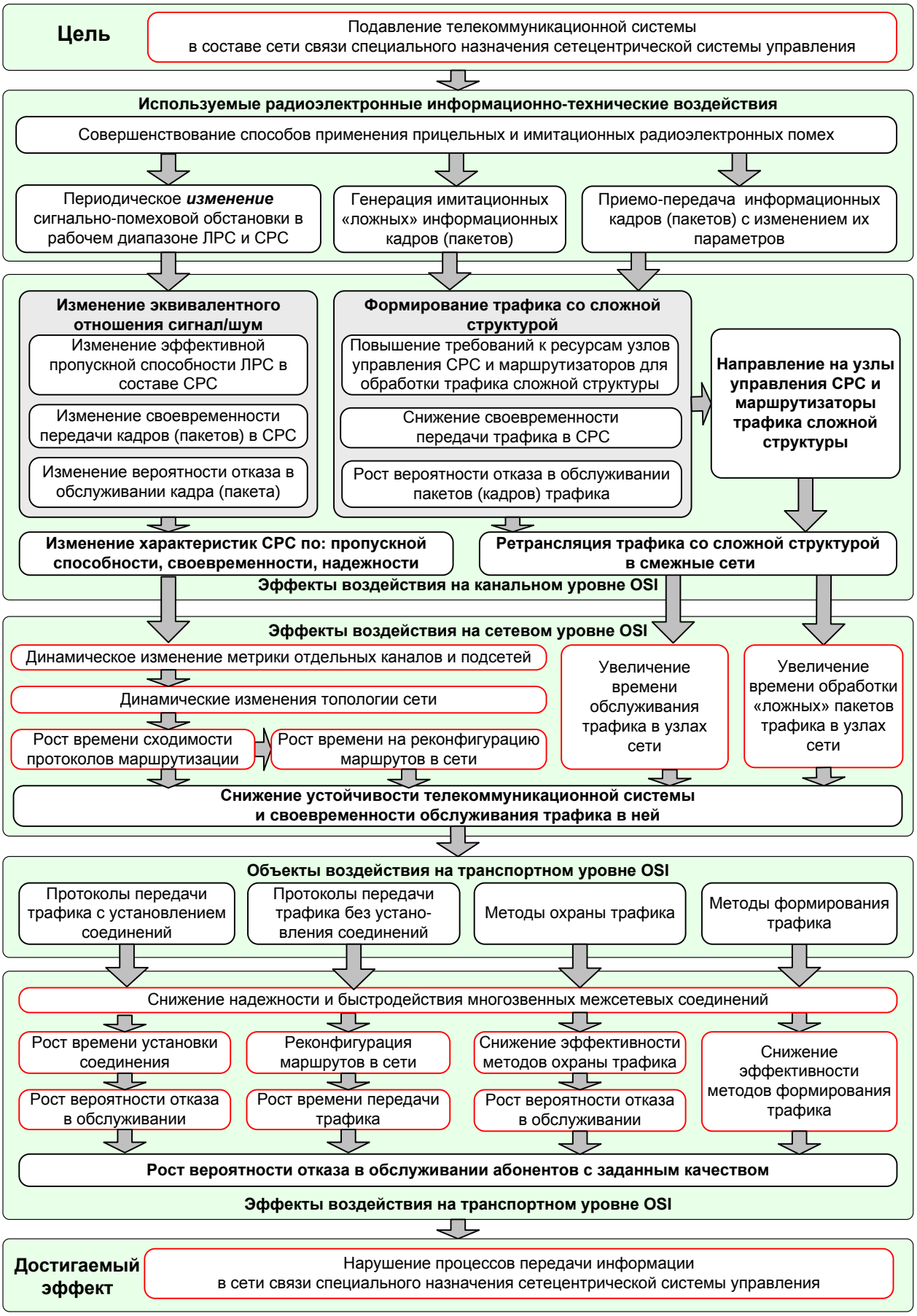

Рис. 8. Порядок воздействия РЭ ИТВ на процессы и объекты сетевого и транспортного уровня ТКС

4. Предложения по реализации новых способов радиоэлектронных ИТВ для подавления ТКС, являющихся составными частями сети связи специального назначения

Кратко рассмотрим основные перспективные направления разработки РЭ ИТВ, ориентированных на подавление ТКС за счет учета особенностей функционирования протоколов на канальном, сетевом и транспортном уровнях модели OSI,. Основными особенностями обосновываемых РЭ ИТВ является учет ими динамических процессов в ТКС при влиянии радиоэлектронных помех, что позволяет использовать для снижения эффективности ТКС динамические нестационарные и переходные режимы, происходящие в ней в результате воздействия периодических помех, а также отображение этих периодических помех на более высоких уровнях модели OSI за счет учета функциональных зависимостей между протоколами ТКС.

Необходимо отметить, что применение всех обосновываемых в данном подразделе РЭ ИТВ целесообразно исключительно против пакетных ТКС с развитой топологией. Применение подобных воздействий против ТКС с древовидной топологией бессмысленно ввиду возможности достижения эффекта подавления таких ТКС «традиционным» подавлением их каналов.

Ниже кратко представлены основные направления разработки РЭ ИТВ, ориентированных на подавление ТКС путем нарушения функционирования протоколов канального, сетевого и транспортного уровней.

В качестве одной из целей для таких РЭ ИТВ целесообразно рассматривать космический сегмент информационной подсистемы сетецентрической системы государственного и военного управления, так как он, с одной стороны, осуществляет глобальные функции информационного обеспечения, а с другой – строится на основе средств радиосвязи и, вследствие этого, уязвим для применения способов радиоэлектронного воздействия.

В целом, новизной разработанных способов РЭ ИТВ является использование «традиционных» радиоэлектронных помех для порождения и развития внутрисистемных конфликтов в ТКС на верхних уровнях ее функционирования. В частности, рассматриваются помехи с динамически изменяемыми параметрами, которые приводят к переходным и нестационарным процессам на верхних уровнях OSI. Достигаемый новый прикладной эффект – это подавление ТКС в целом, в том числе и ее проводного сегмента, за счет воздействия РЭ ИТВ через радиоканалы, как своеобразные «точки входа».

4.1. Способы радиоэлектронного ИТВ, ориентированные на подавление отдельных сетей радиосвязи множественного доступа на канальном уровне ТКС

Исследования возможностей радиоэлектронных воздействий по подавлению протоколов связи на канальном уровне, которые представлены в предшествующих работах автора [29-33], показали следующее. В работах Л. Клейнрока [34], Д. Бертсекаса и Р. Галлагера [35] показано, что пакетным СРС, использующим для передачи пакетов общий радио канал со СМД, свой-

ственна общая нестабильность функционирования. Такие СРС требуют коррекции при большом времени непрерывной работы. Таким образом, возможна реализация РЭ ИТВ, направленного на подавление СРС на основе общего радиоканала со случайным СМД, путем периодического воздействия преднамеренных помех и за счет использования специфических свойств метода СМД. Данный подход для подавления СРС был впервые предложен С.И. Бабусенко [36-38] и получил развитие в работах автора [30, 31] применительно к СРС на основе протоколов CSMA/CA и S-Aloha.

Процесс обслуживания пакетов в этих СРС со случайным СМД был представлен в виде Марковского процесса гибели-размножения, в котором интенсивность обслуживания пакетов определяется пропускной способностью, которая, в свою очередь, зависит от текущего значения отношения сигнал/(шум+помеха) (ОСШП) в общем канале радиосвязи. Проведенное моделирование показало, что динамическое периодическое радиоэлектронное воздействие на общий радиоканал таких СРС ведет к сносу их в заблокированное состояние даже после снятия радиоэлектронного воздействия. При этом, эффект подавления может быть достигнут без полного подавления радио канала СМД, а за счет частичного снижения его пропускной способности, в пределах 10-20%.

Данный способ РЭ ИТВ ориентирован на канальный уровень OSI и может быть осуществлен «традиционными» средствами РЭП за счет введения режима динамических прицельных по времени и частоте помех, временные параметры которых согласованы с параметрами протокола случайного СМД, используемого в подавляемой СРС.

Современные СРС строятся на основе MIMO технологий, в которых для передачи сообщений абоненту могут быть выбраны несколько путей. В дальнейшем, вышеуказанное направление разработки радиоэлектронных воздействий получило развитие в виде модели многоканальной системы массового обслуживания с блокировкой отдельных каналов, представленной в работе автора [32]. Периодическое радиоэлектронное воздействие в виде подавления отдельных радиоканалов в многоканальной СРС ведет к существенному снижению качества обслуживания такой системы, и, в конечном итоге, – к перегрузке СРС пакетами и переходу ее в заблокированное состояние. Проведенное в работе автора [32] моделирование показало, что при выполнении критерия блокировки системы ее пропускная способность снижется на 30%, а время обслуживания в многоканальной системе радиосвязи увеличивается в 10-20 раз относительно уровня, соответствующего ее нормальному функционированию.

Таким образом, РЭ ИТВ, ориентированные на нарушение протоколов канального уровня за счет динамики своего воздействия, позволяют осуществить перевод СРС в нестационарный режим работы, а также увеличить длительность и глубину переходных процессов в них. Увеличение интенсивности РЭ ИТВ позволяет перевести СРС в заблокированное состояние вследствие снижения интенсивности обслуживания ею входного потока пакетов ниже критических значений.

4.2. Способы радиоэлектронного ИТВ, ориентированные на нарушение функционирования протоколов маршрутизации на сетевом уровне ТКС

Принцип воздействия помехами с динамически изменяемыми параметрами для варьирования пропускной способностью каналов в их рабочем диапазоне ОСШП (с целью исключения срабатывания средств помехозащиты физического уровня) в дальнейшем получил развитие в разработках РЭ ИТВ, ориентированных на подавление ТКС путем нарушения устойчивости функционирования протоколов маршрутизации на сетевом уровне модели OSI.

Для исследования и последующего учета эффектов от динамического радиоэлектронного воздействия на сетевом уровне было проведено моделирование пересчета QoS отдельных сетей и каналов радиосвязи в коэффициенты метрики сети, используемые соответствующими протоколами ТКС при решении задач сигнализации в сети и маршрутизации в ней потоков трафика. Математическая модель, формализующая оценку метрики каналов сети в условиях динамического воздействия помех применительно к спутниковым каналам DVB-S/S2, представлена в работе автора [39]. Проведенное моделирование для канала связи DVB-S2 показало, что периодическое изменение ОСШП в канале (как в сторону увеличения, так и в сторону снижения) приводит к принятию протоколом маршрутизации решения об изменении метрики канала, что подразумевает остановку процесса передачи данных в ТКС и запуск пересчета путей в новой топологии сети. Интенсивность принятия данных решений прямо пропорциональна периодичности и глубине изменения ОСШП в отдельных каналах ТКС, а время между моментами этих решений, в общем случае, может быть аппроксимировано экспоненциальным распределением. Анализ эффектов от воздействия средств подавления на адаптивно-лавинные протоколы маршрутизации (OSPF, IS-IS, EIGRP и др.), которое было проведено в работах автора [39-43], показало, что такое РЭ ИТВ ведет к росту интенсивности перемаршрутизации потоков трафика в ТКС, снижению адекватности таблиц маршрутизации, и, в конечном итоге, – к снижению устойчивости ТКС в целом.

Исследование процесса функционирования маршрутизатора ТКС с адаптивно-лавинным протоколом (на основе OSPF), проведенное в работе автора [40], показало, что вероятность подавления ТКС определяется интенсивностью отказов отдельных ее радиоканалов вследствие воздействия помех, а также параметром протокола маршрутизации, формализующим время ожидания восстановления связи. При этом размер сети ТКС практически не влияет на эффективность ее подавления. Таким образом, существует принципиальная возможность подавления ТКС при воздействии с заданной интенсивностью даже на единственный радиоканал в ее составе.

Для обоснования временных параметров РЭ ИТВ, направленного на нарушение функционирования протоколов маршрутизации без установления соединения, в работе автора [41] была разработана модель функционирования объекта связи в условиях отказов каналов связи в виде Марковского процесса переходов между состояниями «нормальное функционирование» – «отказ кана-

ла» – «ожидание восстановления связи» – «реконфигурация маршрутизатора». Использование данной модели в составе методики обоснования временных параметров РЭ ИТВ для воздействия на протокол маршрутизации по состоянию каналов (на примере протокола OSPF) позволило определить наиболее сложные условия функционирования для этого протокола маршрутизации. Результаты моделирования показывают, что при согласовании временных параметров РЭ ИТВ и временных параметров протокола маршрутизации достигается снижение надежности отдельного маршрутизатора ТКС по показателю коэффициент готовности до уровня 0,5. За счет лавинной рассылки смежным узлам сообщений об изменении метрики каналов связи каждый из маршрутизаторов ТКС снижает свой коэффициент готовности из-за постоянного пересчета кратчайших путей. В результате эффект снижения устойчивости распространяется на всю ТКС в целом. При этом показатель устойчивости сети ТКС по показателю «среднесетевая вероятность устойчивости информационного направления связи» снижается до значений 0,2-0,4. При этом уровень снижения устойчивости сети ТКС пропорционален средней длине направления связи.

Для обоснования временных параметров РЭ ИТВ, направленных на нарушение функционирования протоколов маршрутизации с установлением соединения, в работе автора [42] была разработана модель функционирования информационного направления связи в ТКС, учитывающая не только процесс реконфигурации отдельных ее маршрутизаторов вследствие отказа каналов, но и учет структуры соединений в ТКС, а также принятого в ТКС подхода к резервированию путей передачи. Результаты моделирования эффектов от воздействия РЭ ИТВ на ТКС показывают, что ТКС на основе протокола маршрутизации с установлением соединения снижают свою устойчивость за счет снижения устойчивости соединений, проходящих через узлы, которые подверглись воздействию РЭ ИТВ. При этом уровень снижения устойчивости ТКС пропорционален количеству узлов, на которые осуществляется воздействие РЭ ИТВ. На основе этой модели в дальнейшем была разработана методика обоснования временных параметров РЭ ИТВ для воздействия на протокол маршрутизации с установлением соединений, которая позволяет обосновать временные параметры динамических помех, снижающих устойчивость ТКС до значений ниже требуемых.

Для подтверждения адекватности разработанного научно-методического аппарата обоснования способов РЭ ИТВ и практического подтверждения эффектов функционального подавления ТКС были проведены экспериментальные исследования на основе сети с протоколом OSPF и OADV, результаты которых представлены в работе [44]. Сравнение теоретических расчетов и полученных экспериментальных данных позволяет сделать вывод о практическом подтверждении возможностей таких РЭ ИТВ осуществлять эффективное подавление ТКС.

Вышеуказанные перспективные направления разработки РЭ ИТВ, ориентированных на сетевой уровень ТКС, могут быть реализованы территориально-распределенными «традиционными» комплексами РЭП за счет введения режима динамических низкоэнергетических прицельных по частоте и времени по-

мех, временные параметры которых согласованны с параметрами протоколов маршрутизации, используемых в подавляемых ТКС.

4.3. Способы радиоэлектронного ИТВ, ориентированные на нарушение функционирования протоколов обеспечения качества обслуживания на транспортном уровне ТКС

Перспективным направлением разработки способов РЭ ИТВ, ориентированных на подавление ТКС на транспортном уровне модели OSI, является разработка радиоэлектронных воздействий, ориентированных на формирование трафика сложной структуры и нарушение функционирования протоколов обеспечения качества обслуживания.

Так, перспективными являются РЭ ИТВ, ориентированные на формирование в канале радиосвязи потока пакетов сложной структуры с коэффициентом вариации больше единицы и существенно отличающегося от простейшего. Анализ результатов моделирования обработки потоков сложной структуры в узлах коммутации сети, представленный в работах автора и его коллеги К.В. Ушанева [45, 46], показал, что своевременность обработки таких потоков в десятки, а в некоторых случаях, в сотни раз ниже относительно обработки простейших потоков! При этом, данный эффект наблюдается преимущественно в высоконагруженных маршрутизаторах.

Первый вариант таких РЭ ИТВ представлен в работе автора [47] и основан на внедрении дополнительных имитационных пакетов трафика, что позволяет сформировать выходной поток пакетов из канала радиосвязи со структурой существенно отличающейся от простейшего (коэффициент вариации больше единицы). Отличительной особенностью этих РЭ ИТВ является необходимость внедрения дополнительных пакетов, которые являются копиями ранее переданных пакетов, что в ряде случаев может привести к «разрушению» информационного потока. Кроме того, ряд протоколов ТКС (например, IPSec) нумеруют пакеты внутри сессии передачи данных, что позволяет им обнаруживать внедренные пакеты. Указанного недостатка лишен второй вариант РЭ ИТВ, ориентированный на полный перехват и преобразование структуры потока трафика, методологические основы которого представлены в работах [48, 49].

Оценка результатов воздействия указанных РЭ ИТВ, ориентированных на формирование сложного структуры передаваемого в ТКС трафика, который критичен к задержкам, показал, что устойчивость ТКС снижается за счет снижения своевременности обслуживания трафика в ее узлах и фактической блокировки узлов, передающих сложный трафик. Такие РЭ ИТВ представляют собой вариант бескомпроматной DOS-атаки. Кроме того, эффект воздействия РЭ ИТВ проявляется еще и в том, что сформированные сложные потоки трафика передаются дальше по ТКС, снижая своевременность обработки и в других ее узлах. Таким образом, данные РЭ ИТВ способны адресно подавлять отдельные информационные направления связи в ТКС. При этом уровень снижения устойчивости ТКС при воздействиях таких РЭ ИТВ пропорционален количе-

ству «усложненных» потоков трафика, их скорости, а также средней длине направления связи в ТКС.

Перспективные способы РЭ ИТВ, ориентированные на транспортный уровень ТКС, могут быть реализованы как территориально-распределенными комплексами РЭП, реализующими новые способы имитационных радиоэлектронных помех, так и аппаратно-программными закладками, а также специальными программными средствами (вирусами), внедряемыми в оборудование ТКС.

Выводы

По итогам материала статьи, обобщая вышесказанное, можно сделать следующие основные выводы.

1. В настоящее время происходит переход архитектуры систем государственного и военного управления от иерархического к сетецентрическому принципу построения. Сетецентрическая система управления является распределённой системой, в которой ее базовые элементы, такие как силы и средства наблюдения, ПУ и ЛПР, а также управляемые силы и средства объединены в единое информационное пространство. Подобное объединение повышает возможности информационного взаимодействия всех компонентов системы управления. Это ведет к повышению эффективности действий системы по показателю оперативности управления за счет повышения скорости реализации цикла управления (цикла Бойда) «наблюдение – ориентация – решение – действие». Кроме того, в сетецентрических системах повышается непрерывность и устойчивость управления, за счет увеличения путей доставки информации и команд от ПУ к управляемым силам и средствам.

2. Основой единого информационного пространства сетецентрической системы управления является сетецентрическая среда. Сетецентрическая среда функционирует в физической, информационной, социальной и когнитивной областях. При этом информационно-технические процессы функционирования сетецентрической среды декомпозируется на три слоя: физический, семантический и синтаксический. Физический слой соответствует информационной инфраструктуре сетецентрической среды, которая существует в реальном физическом мире. Семантический слой включает в себя смысловое содержание формируемой, хранимой, передаваемой, обрабатываемой и представляемой информации. Синтаксический слой соответствует форматам, правилам и протоколам процессов формирования, хранения, передачи, обработки и представления информации.

3. Анализ процессов функционирования сетецентрических систем управления на примере систем управления войсками и оружием, использующихся в локальных войнах, позволил вскрыть их уязвимости. В основном, эти уязвимости связанны с процессами сбора, передачи и обработки информации, а также с процессами обеспечения информационной безопасности.

При этом к наиболее критичным уязвимостям сетецентрической системы управления системы относится:

- высокая информационная взаимозависимость всех ее элементов;
- широкое использование в ней двойных информационных технологий.

Наличие этих уязвимостей делает возможным ассиметричное противодействие системе сетецентрического управления за счет нарушения процессов формирования, передачи, хранения, обработки и представления информации в ней.

4. Проведенный анализ возможностей использования средств огневого поражения, средств РЭП, средств ФП ЭМИ, а также ИТВ против физического, семантического и синтаксического слоев сетецентрической среды показал, что наиболее эффективным по показателю эффективность/затраты является применение ИТВ, ориентированных на синтаксический слой. При этом наиболее простым вариантом такого ИТВ является воздействие, направленное на нарушение процессов передачи информации, что приводит к критическому снижению доступности информационных ресурсов системы, увеличению длительности цикла управления, и, в конечном итоге, – к снижению качества управления, по показателям оперативности, непрерывности и устойчивости. В качестве источника такого ИТВ могут быть использованы имеющиеся средства РЭП, а в качестве места приложения данного воздействия – радиосети и радиоканалы в составе сети связи, являющейся физической основой сетецентрической среды. При этом для эффективного нарушения процессов передачи информации эти ИТВ должны учитывать особенности протоколов информационного обмена, а также особенности построения и функционирования сети связи сетецентрической среды.

5. Одним из важных элементом сетецентрической среды является СС СН, которая обеспечивает процессы передачи информации в ней. При переходе к сетецентрическому принципу построения систем управления, структура СС СН становиться более гибкой – децентрализованной, сетевой и многоэшелонированной. При этом структура СС СН более не является жестко привязанной к структуре и иерархии элементов системы управления.

6. Существующие преднамеренные дестабилизирующие воздействия, основанные на применении средств РЭП и ИТВ типа «отказ в обслуживании», ориентированны на устаревшие иерархические системы управления, и являются неэффективными против сетевых децентрализованных СС СН так как не обеспечивают значимое снижение их устойчивости. Таким образом, существующие дестабилизирующие воздействия уже не могут эффективно обеспечивать нарушение процессов передачи информации в СС СН, а также значимо снижать уровень доступности информационных ресурсов в сетецентрической системе управления.

7. Современное невоенное противоборство между государствами может вестись и в мирное время, и классифицируется как «информационная война». Преднамеренные дестабилизирующие воздействия (РЭП и ИТВ), осуществляемые в процессе информационной войны в мирное время и в угрожаемый период и направленные на нарушение процессов передачи информации в СС СН

противостоящей стороны должны носить бескомпроматный характер. Это исключит компрометацию той стороны, которая осуществляет это воздействие.

8. Структурно СС СН состоит из взаимодействующих между собой ТКС. Одной из наиболее важных частей СС СН являются ее космический эшелон, который обеспечивает для сетецентрической системы управления глобальную (в масштабах Земли) непрерывность информационного обмена, а также доступность информационных ресурсов системы управления для удаленных пользователей. Устойчивость ТКС космического эшелона СС СН является критически важной для обеспечения требований как по доступности к самой СС СН, так и требований по своевременности и достоверности связи, а также требований к доступности информационных ресурсов в сетецентрической системе управления.

9. Существующие системы и способы РЭП ориентированны на подавление только отдельных каналов и сетей радиосвязи ТКС путем нарушения функционирования протоколов связи на физическом и канальном уровнях модели OSI. При переходе ТКС в составе СС СН к децентрализовано-сетевой структуре, не связанной со структурой системы управления, существующие системы и способы РЭП становятся неэффективными и не обеспечивают значимое снижение устойчивости ТКС.

10. Анализ тенденций развития и построения перспективных ТКС СС СН позволил сформировать основные требования и рекомендации, связанные с практической реализацией новых способов дестабилизирующих воздействий на ТКС путем применения РЭ ИТВ.

- РЭ ИТВ должны реализовываться на физическом уровне OSI и использовать радиоканалы связи как «точку входа» внутрь защищаемого периметра ТКС для осуществления дестабилизирующих воздействий, ориентированных на снижение доступности ее информационных ресурсов;
- РЭ ИТВ должны реализовывать бескомпроматное воздействие, основанное на новых режимах постановки низкоэнергетических радиоэлектронных помех с целью, как эффективного преодоления известных способов помехозащиты средств связи в ТКС, так и возможности быть использованными в мирное и в военное время;
- РЭ ИТВ должны быть ориентированны на нарушение функционирования протоколов маршрутизации сетевого уровня пакетных сетей связи путем динамического изменения их топологии;
- РЭ ИТВ должны быть ориентированы на нарушение функционирования протоколов обеспечения качества обслуживания транспортного уровня пакетных сетей путем усложнения структуры передаваемого трафика или направление дополнительного имитационного трафика на критичные или наиболее загруженные маршрутизаторы сети.

Литература

1. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

2. Буренок В. М., Ляпунов В. М., Мудров В. И. Теория и практика планирования и управления развитием вооружения / Под ред. А.М. Московского. – М.: Изд-во «Вооружение. Политика. Конверсия», 2005. – 418 с.

3. Alberts D. S., Garstka J. J., Stein F. P. Network Centric Warfare: Developing and Leveraging Information Superiority. 2-nd Edition (Revised). – US Department of Defense, C4ISR Cooperative Research Program Publications Series, 2001. – 292 p. – URL: http://www.dodccrp.org/files/Alberts_NCW.pdf (дата обращения 19.12.2017).

4. Дроговоз П. А., Чемезов С. В., Турко Н. И., Куликов С. А. Развитие системы стратегического менеджмента интегрированных структур ГК «Ростехнологии» на основе концепции сетецентричности // Проблемы стратегического менеджмента и механизмы военно-гражданской интеграции в высокотехнологичных отраслях промышленности: Сб. науч. статей. – М.: ЦОП АВН, 2011. – С. 93.

5. Трахтенгерц Э. А. Использование двух сетецентрических принципов модификации экономических целей и стратегий в кризисной ситуации // Управление большими системами. 2013. №. 45. С. 289-329.

6. Ефремов А. Ю., Максимов Д. Ю. Сетецентрическая система управления – что вкладывается в это понятие? // Труды третьей российской конференции с международным участием «Технические и программные средства систем управления, контроля и измерения». – М.: ИПУ РАН, 2012. – С. 159-161.

7. Макаренко А. В. Введение в сетецентрические информационно-управляющие системы // Конструктивная кибернетика. Исследования. Разработки. Консалтинг [Электронный ресурс]. 03.04.2010. – URL: http://www.rdcn.ru/estimation/2010/03042010.shtml (дата обращения: 03.07.2017).

8. Ивлев А. А. Основы теории Бойда. Направления развития, применения и реализации. Монография. – М., 2008. – 64 с.

9. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.

10. Сидорин А. Н. Прищепов В. М., Акуленко В. П. Вооруженные силы США в XXI веке: Военно-теоретический труд. - М.: Кучково поле; Военная книга, 2013. - 800 с.

11. Копылов А. В. К вопросу о критике концепции «сетецентрических» войн (операций) в американских СМИ // Военная история и футурология [Электронный ресурс]. 2011. – URL: http://www.milresource.ru/Kop-NCW.html (дата обращения 03.07.2017).

12. Копылов А. В. О слабых сторонах американской концепции «сетецентрических войн (операций)» // Военная мысль. 2011. № 7. С. 53-62.

13. Бедрицкий А. В. Информационная война: концепции и их реализация в США / Под ред. Е.М. Кожокина. – М.: РИСИ, 2008. – 187 с.

14. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-68. – URL: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf (дата обращения 21.12.2017).

15. Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. – URL: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf (дата обращения 21.12.2017).

16. Шнепс-Шнеппе М. А. Телекоммуникации Пентагона: цифровая трансформация и киберзащита. – М.: Горячая линия – Телеком, 2017. – 272 с.

17. Шнепс-Шнеппе М.А. «Красный телефон» на DISN сети как родимое пятно в среде AS-SIP // International Journal of Open Information Technologies. 2015. Т. 3. № 6. С. 7-12.

18. Шнепс-Шнеппе М. А., Намиот Д. Е. Об эволюции телекоммуникационных сервисов на примере GIG // International Journal of Open Information Technologies. 2015. Т. 3. № 1. С. 1-13.

19. Шнепс-Шнеппе М. А. От IN к IMS. О сетях связи военного назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 1-11.

20. Шнепс-Шнеппе М. А., Намиот Д. Е, Цикунов Ю. В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны // International Journal of Open Information Technologies. 2014. Т. 2. № 10. С. 3-13.

21. Нетес В. А. Надежность сетей связи в период перехода к NGN // Вестник связи. 2007. № 9. С. 1-8.

22. Соколов Н. А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 9. С. 4-8.

23. Бобков Ю. Я., Тютюнников Н. Н. Концептуальные основы построения АСУ Сухопутными войсками ВС РФ: монография. – М.: Издательство «Палеотип», 2014. – 92 с.

24. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.

25. О связи. Федеральный закон РФ от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

26. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47.

27. Макаренко С. И. Радиоэлектронные информационные воздействия на сети связи сетецентрической системы управления // Вестник Военно-воздушной академии. 2016. № 3 (27). С. 108-117.

28. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. О.И. Шелухина. – М.: Горячая линия-Телеком, 2013. – 220 с.

29. Макаренко С. И., Татарков М. А. Моделирование обслуживания нестационарного информационного потока системой связи со случайным множественным доступом // Информационно-управляющие системы. 2012. № 1. С. 44-50.

30. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2-2. – URL: http://jre.cplire.ru/jre/sep11/4/text.pdf (дата обращения 21.12.2017).

31. Макаренко С. И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. № 6. 2012. – URL: http://jre.cplire.ru/jre/jun12/9/text.pdf (дата обращения 21.12.2017).

32. Макаренко С. И., Синицин И. А. Инженерная методика оценки качества обслуживания системы массового обслуживания M/M/n/q с ненадежными каналами и ее приложение для анализа функционирования систем многоканальной связи в условиях помех // Инфокоммуникационные технологии. 2014. Том 12. № 4. С. 24-32.

33. Макаренко С. И. Исследование влияния преднамеренных помех на возможности по ретрансляции сообщения и показатели качества обслуживания канального уровня модели OSI для системы связи со случайным множественным доступом абонентов // Информационные технологии моделирования и управления. 2010. №6 (65). С. 807-815.

34. Клейнрок Л. Вычислительные системы с очередями. – М.: Мир, 1979. – 600 с.

35. Бертсекас Д., Галлагер Р. Сети передачи данных. – М.: Мир, 1989. – 544 с.

36. Исаев В. В., Бабусенко С. И. Статистическое моделирование многопролетных сетей пакетной радиосвязи // Техника средств связи: материалы 18 научно-технической конференции. – Воронеж: НИИС, 1992.

37. Бабусенко С. И., Исаев В. В. Аналитическая модель маршрутизации в пакетной сети // Техника средств связи: материалы 18 научно-технической конференции. – Воронеж: НИИС, 1992.

38. Бабусенко С. И. Модель процесса радиоподавления пакетной радиосети с протоколом ненастойчивого доступа с прослушиванием несущей // Тезисы докладов 31 ВНТК академии. – Л.: ВАС, 1990.

39. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально-помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. – URL: http://jre.cplire.ru/jre/oct14/3/text.pdf (дата обращения 21.12.2017).

40. Макаренко С. И., Михайлов Р. Л. Модель функционирования коммутатора в сети с использованием протокола покрывающего дерева STP и

исследование устойчивости сети в условиях ограниченной надежности каналов связи // Радиотехнические и телекоммуникационные системы. 2013. № 2. С. 61-68.

41. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Том 12. № 2. С. 44-49.

42. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.

43. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. 2015. № 2. С. 45-98. – URL: http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (дата обращения 05.12.2017).

44. Макаренко С. И., Афанасьев О. В., Баранов И. А., Самофалов Д. В. Экспериментальные исследования реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Журнал радиоэлектроники. 2016. № 4. – URL: http://jre.cplire.ru/jre/apr16/4/text.pdf (дата обращения: 05.12.2017).

45. Ушанев К. В., Макаренко С. И. Показатели своевременности обслуживания трафика в системе массового обслуживания Pa/M/1 на основе аппроксимации результатов имитационного моделирования // Системы управления, связи и безопасности. 2016. № 1. С. 42-65. – URL: http://sccs.intelgr.com/archive/2016-01/03-Ushanev.pdf (дата обращения: 05.12.2017).

46. Ушанев К. В. Имитационные модели системы массового обслуживания типа $Pa/M/1$, $H_2/M/1$ и исследование на их основе качества обслуживания трафика со сложной структурой // Системы управления, связи и безопасности. 2015. № 4. С. 217-251. – URL: http://sccs.intelgr.com/archive/2015-04/14-Ushanev.pdf (дата обращения: 26.12.2017).

47. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. 2014. № 3 (4). С. 7-13.

48. Ушанев К. В. Расчет операторов преобразования трафика для преднамеренного повышения структурной сложности информационного потока // Труды учебных заведений связи. 2017. Т. 3. № 2. С. 93-101.

49. Макаренко С. И., Коровин В. М., Ушанев К. В. Оператор преобразования трафика для преднамеренного повышения структурной сложности информационных потоков // Системы управления, связи и безопасности. 2016. № 4. С. 77-109. – URL: http://sccs.intelgr.com/archive/2016-04/04-Makarenko.pdf (дата обращения 05.12.2017).

References

1. Makarenko S. I. *Informatsionnoe protivoborstvo i radioelektronnaia borba v setetsentricheskikh voinakh nachala XXI veka. Monografiia* [Information warfare and electronic warfare to network-centric wars of the early XXI century. Monograph]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2017. 546 p. (in Russian).

2. Burenok V. M., Liapunov V. M., Mudrov V. I. *Teoriia i praktika planirovaniia i upravleniia razvitiem vooruzheniia* [Theory and practice of planning and managing the development of weapons]. Moscow, "Vooruzhenie. Politika. Konversiia" Publ., 2005. 418 p. (in Russian).

3. Alberts D. S., Garstka J. J., Stein F. P. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2-nd Edition (Revised). US Department of Defense, C4ISR Cooperative Research Program Publications Series, 2001. 292 p. Available at: http://www.dodccrp.org/files/Alberts_NCW.pdf (accessed 19 December 2017).

4. Drogovoz P. A., Chemezov S. V., Turko N. I., Kulikov S. A. Razvitie sistemy strategicheskogo menedzhmenta integrirovannykh struktur GK «Rostekhnologii» na osnove kontseptsii setetsentrichnosti [The development of the system of strategic management of integrated structures of "Russian technologies" Corporation on the basis of the Net-centric concept]. *Problemy strategicheskogo menedzhmenta i mekhanizmy voenno-grazhdanskoi integratsii v vysokotekhnologichnykh otrasliakh promyshlennosti* [Problems of strategic management and mechanisms of civil-military integration in high-tech industries]. Moscow, Academy of Military Sciences, 2011, p. 93 (in Russian).

5. Trahtengerts E. A. Use of two network-centric principles of modification of economic targets and strategy in crisis situations. *Large-scale Systems Control*, 2013, no. 43, pp. 289-329 (in Russian).

6 Efremov A. Iu., Maksimov D. Iu. Setetsentricheskaia sistema upravleniia – chto vkladyvaetsia v eto poniatie? [Network-centric control system – what is embedded in this concept?]. *Trudy tret'ei rossiiskoi konferentsii s mezhdunarodnym uchastiem 'Tekhnicheskie i programmnye sredstva sistem upravleniia, kontrolia i izmereniia'*. Moscow, Institute of Control Sciences RAS, 2012. pp. 159-161 (in Russian).

7. Makarenko A. V. Vvedenie v setetsentricheskie informatsionno-upravliaiushchie sistemy [Introduction to network-centric information management systems]. *Konstruktivnaia kibernetika. Issledovaniia. Razrabotki. Konsalting*, 2010. Available at: http://www.rdcn.ru/estimation/2010/03042010.shtml (accessed 03 July 2017) (in Russian).

8. Ivlev A. A. *Osnovy teorii Boida. Napravleniia razvitiia, primeneniia i realizatsii. Monografiia* [Fundamentals of the theory of Boyd. Areas of development, application and implementation]. Moscow, 2008. 64 p. (in Russian).

9. Griniaev S. N. *Pole bitvy – kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voiny* [Battlefield – cyberspace. Theory, techniques, tools, methods and systems of information warfare]. Moscow, Kharvest Publ., 2004. 426 p. (in Russian).

10. Sidorin A. N. Prishchepov V. M., Akulenko V. P. *Vooruzhennye sily USA v XXI veke: Voenno-teoreticheskii trud* [The U.S. armed forces in the XXI century]. Moscow, Kuchkovo pole Publ., 2013. 800 p. (in Russian).

11. Kopylov A. V. K voprosu o kritike kontseptsii «setetsentricheskikh» voin (operatsii) v amerikanskikh SMI [To the question of criticism of the concept of "network-centric" war (operations) in the American media]. *Voennaia istoriia i futurologiia*, 2011. Available at: http://www.milresource.ru/Kop-NCW.html (accessed 03 July 2017) (in Russian).

12. Kopylov A. V. O slabykh storonakh amerikanskoi kontseptsii ‘setetsentricheskikh voin (operatsii)’ [Weaknesses American concept of "network-centric warfare (operations)"]. *Military Thought*, 2011, no. 7, pp. 53-62 (in Russian).

13. Bedritskiy A. V. *Informatsionnaia voina: kontseptsii i ikh realizatsiia v SShA* [Information warfare: concepts and their implementation in the United States]. Moscow, The Russian Institute of Strategic Research, 2008. 187 p. (in Russian).

14. Makarenko S. I. Prospects and Problems of Development of Communication Networks of Special Purpose. *Systems of Control, Communication and Security*, 2017, no. 2, pp. 18-68. Available at: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf (accessed 21 December 2017) (in Russian).

15. Makarenko S. I. Descriptive Model of a Special Purpose Communication Network. *Systems of Control, Communication and Security*, 2017, no. 2, pp. 113-164. Available at: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf (accessed 21 December 2017) (in Russian).

16. Shneps-Shneppe M. A. *Telekommunikatsii Pentagona: tsifrovaia transformatsiia i kiberzashchita* [Telecommunications Pentagon: digital transformation and cyber defence]. Moscow, Goriachaia liniia – Telekom Publ., 2017. 272 p. (in Russian).

17. Shneps-Shneppe M. A. «Krasnyi telefon» na DISN seti kak rodimoe piatno v srede AS-SIP [The "red phone" on DISN network as a birthmark in the environment AS-SIP]. *International Journal of Open Information Technologies*, 2015, vol. 3, no. 6, pp. 7-12 (in Russian).

18. Shneps-Shneppe M. A., Namiot D. E. Ob evoliutsii telekommunikatsionnykh servisov na primere GIG [The evolution of telecommunication services on an example GIG]. *International Journal of Open Information Technologies*, 2015, vol. 3, no. 1, pp. 1-13 (in Russian).

19. Shneps-Shneppe M. A. Ot IN k IMS. O setiakh sviazi voennogo naznacheniia [About communication networks for military purposes]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 1, pp. 1-11 (in Russian).

20. Shneps-Shneppe M. A., Namiot D. E, Tsikunov Iu. V. Telekommunikatsii dlia voennykh nuzhd: set' GIG-3 po trebovaniiam kibervoiny [Telecommunications for military purposes: the network is GIG-3 according to the requirements of cyberwar]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 10, pp. 3-13 (in Russian).

21. Netes V. A. Nadezhnost' setei sviazi v period perekhoda k NGN [Reliability of communication networks in the period of transition to NGN]. *Vestnik sviazi*, 2007, no. 9, pp. 1-8 (in Russian).

22. Sokolov N. A. Sistemnye aspekty postroeniia i razvitiia setei elektrosviazi spetsial'nogo naznacheniia [The system aspects of the construction and development of telecommunication networks of special purpose]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 9, pp. 4-8 (in Russian).

23. Bobkov Ju. Ja., Tiutiunnikov N. N. *Kontseptual'nye osnovy postroeniia ASU Sukhoputnymi voiskami VS RF: monografiia* [Concepts of ACS of Land forces of armed forces of the Russian Federation. Monograph]. Moscow, Paleotip Publ., 2014. 92 p. (in Russian).

24. Antonovich P. I., Makarenko S. I., Mihaylov R. L., Ushanev K. V. New means of destructive effects on network centric military command, control and communication systems in the information space. *Vestnik Akademii voennykh nauk*. 2014, vol. 48, no. 3, pp. 93-101 (in Russian).

25. *O sviazi* [About the connection]. Federal law of Russia. 2003. (in Russian).

26. Makarenko S. I. Problemy i perspektivy primeneniia kiberneticheskogo oruzhiia v sovremennoi setetsentricheskoi voine [Problems and prospects for the use of cyber weapons in today's network-centric warfare]. *Specialized Machinery and Communication*, 2011, no. 3, pp. 41-47 (in Russian).

27. Makarenko S. I. The radio-electronic information influence on network of net-centric control system. *Vestnik Voenno-vozdushnoy akademii*, vol. 27, no. 3, pp. 108-117 (in Russian).

28. Sheluhin O. I., Sakalema D. Zh., Filinova A. S. *Obnaruzhenie vtorzhenii v komp'iuternye seti (setevye anomalii)* [Intrusion detection in computer networks (network anomalies)]. Moscow, Goriachaia liniia – Telekom Publ., 2013. 220 p. (in Russian).

29. Makarenko S. I., Tatarkov M. A. Model of Service the Non-Stationary Traffic in Communication System with CSMA. *Informatsionno-upravliaiushchie sistemy*, no. 1, 2012, pp. 44-50 (in Russian).

30. Makarenko S. I. The countermeasures of the radio networks with the random multiple access by changing the radionet state to non-stable. *Journal of Radio Electronics*, 2011, no. 9. Available at: http://jre.cplire.ru/jre/sep11/4/text.pdf (accessed 21 December 2017) (in Russian).

31. Makarenko S. I. Estimation of quality of service in radio network with package transmitting in unstationary mode under influence of external destructive factors. *Journal of Radio Electronics*, 2012, no. 6. Available at: http://jre.cplire.ru/jre/jun12/9/text.pdf (accessed 21 December 2017) (in Russian).

32. Makarenko S. I., Sinitsyn I. A. The Evaluation Procedure of the Quality of Service of M/M/N/Q Queuing System with Unsafe Channels and its Annex for the Analysis of Multi-Channel Radio Communication Systems in Noise Effect Environment is Presented. *Infocommunikacionnye tehnologii*, no. 4, 2014, pp. 24-32 (in Russian).

33. Makarenko S. I. Issledovanie vliianiia prednamerennykh pomekh na vozmozhnosti po retransliatsii soobshcheniia i pokazateli kachestva obsluzhivaniia

kanal'nogo urovnia modeli OSI dlia sistemy sviazi so sluchainym mnozhestvennym dostupom abonentov [The Study of the Influence of Intentional Interference at the Relay Capabilities of the Message and the Quality of Service Link Layer of the OSI Reference Model for Communication Systems with Random Multiple Access Subscribers]. *Informatsionnye tekhnologii modelirovaniia i upravleniia*, 2010, vol. 65, no. 6, pp. 807-815 (in Russian).

34. Kleinrock L. *Queueing Systems: Volume II – Computer Applications*. New York: Wiley Interscience, 1975. 576 p.

35. Bertsekas D., Gallager R. *Seti peredachi dannykh* [Data network]. Moscow, Mir Publ., 1989. 544 p. (in Russian).

36. Isaev V. V., Babusenko S. I. Statisticheskoe modelirovanie mnogoproletnykh setei paketnoi radiosviazi [Statistical modeling of multi-span networks, packet radio]. *Tekhnika sredstv sviazi: materialy 18 nauchno-tekhnicheskoi konferentsii* [Proceedings of the 18th scientific and technical conference "Technique of communication"], Voronezh, Research Institute of Telecommunications, 1992. (in Russian).

37. Babusenko S. I., Isaev V. V. Analiticheskaia model' marshrutizatsii v paketnoi seti [Analytical model of routing in a packet network]. *Tekhnika sredstv sviazi: materialy 18 nauchno-tekhnicheskoi konferentsii* [Proceedings of the 18th scientific and technical conference "Technique of communication"]. Voronezh, Research Institute of Telecommunications, 1992. (in Russian).

38. Babusenko S. I. Model' protsessa radiopodavleniia paketnoi radioseti s protokolom nenastoichivogo dostupa s proslushivaniem nesushchei [The process model of the jamming packet radio network Protocol nenastoychiv access with listening of carrier]. *Proceedings of 31 military-scientific conference of the Academy*. Leningrad, Military Academy of Communications, 1990. (in Russian).

39. Makarenko S. I., Mikhailov R. L., Novikov E. A. Issledovanie kanal'nykh i setevykh parametrov kanala sviazi v usloviiakh dinamicheski izmeniaiushcheisia signal'no–pomekhovoi obstanovki [The Research of Data Link Layer and Network Layer Parameters of Communication Channel in the Conditions Dynamic Vary of the Signal and Noise Situation]. *Journal of Radio Electronics*, 2014, no. 10. Available at: http://jre.cplire.ru/jre/oct14/3/text.pdf (accessed 21 December 2017) (in Russian).

40. Makarenko S. I., Mikhailov R. L., The model of the switch functioning in the network which applies the Spanning Tree Protocol and the net stability analysis in the conditions of the communication channels limited reliability. *Radio and telecommunication systems*, 2013, no. 2, pp. 61-68 (in Russian).

41. Makarenko S.I., Mikhaylov R.L. The Model of Functioning of the Router in the Case of Limited Reliability of Communication Channels. *Infocommunikacionnye tehnologii*, 2014, vol. 12, no. 2, pp. 44-49 (in Russian).

42. Makarenko S. I., Ryimshin K. Yu., Mixajlov R. L. Model of functioning of telecommunication object in the limited reliability of communication channel conditions. *Information Systems and Technologies*, 2014, vol. 86, no. 6, pp. 139-147 (in Russian).

43. Makarenko S. I. Convergence Time of IGP Routing Protocol. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 45-98. Available at: http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (in Russian).

44. Makarenko S. I., Afanasev O. V., Baranov I. A., Samofalov D. V. Experimental analysis of the network reaction and the routing effects under conditions of noise-to-signal ratio dynamic changes. *Journal of Radio Electronics*, 2014, no. 4. Available at: http://jre.cplire.ru/jre/apr16/4/text.pdf (accessed 05 December 2017) (in Russian).

45. Ushanev K.V., Makarenko S. I. The Timeliness Indicators of Traffic Service in Queue Systems Pa/M/1 Based on Approximation of Imitating Modeling Results. *Systems of Control, Communication and Security*, 2016, no. 1, pp. 42-65. Available at: http://sccs.intelgr.com/archive/2016-01/03-Ushanev.pdf (accessed 05 December 2017) (in Russian).

46. Ushanev K. V. Simulation Models of Queuing Systems of Type Pa/M/1, H2/M/1 and Research on the Basis of their Quality of Service Traffic with a Complicated Structure. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 217-251. Available at: http://journals.intelgr.com/sccs/archive/2015-04/14-Ushanev.pdf (accessed 26 August 2016) (in Russian).

47. Makarenko S. I. Premeditated formation of the traffic of difficult structure due to implementation in the communication system of additional imitative traffic. *Voprosy kiberbezopasnosti*, 2014, vol. 4, no. 3, pp. 7-13 (in Russian).

48. Ushanev K. V. The Calculation of the Traffic Transformation Operator for Deliberate Increase of the Structural Complexity of Information Stream. *Proceedings of Educational Institutes of Communication*, 2017, vol. 3, no. 2, pp. 93-101.

49. Makarenko S. I., Korovin V. M., Ushanev K. V. The Traffic Transformation Operator for Deliberate Increase of the Structural Complexity of the Information Stream. *Systems of Control, Communication and Security*, 2016, no. 4, pp. 77-109. Available at: http://sccs.intelgr.com/archive/2016-04/04-Makarenko.pdf (accessed 05 December 2017) (in Russian).

Статья поступила 21 декабря 2017 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Заместитель генерального директора по научной работе – главный конструктор. ООО «Корпорация «Интел групп». Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197372, Санкт-Петербург, пр. Богатырский, д. 32, корп. 1 лит. А, офис 6Н.

Suppression of a Net-Centric Control System with Radio Cyber Attacks

S. I. Makarenko

Relevance. *Currently control systems architectures tend to the transition from hierarchical to net-centric principle of structure. A net-centric control system is a distributed system, which base elements are integrated into one information space. Such union makes contemporary destabilizing methods ineffective against net-centric control systems as they suppress and jam only individual components of the system. It is important to create new methods of net-centric control systems suppression.* ***The purpose of this paper*** *is to formulate a concept of new telecommunication systems suppression methods. Telecommunication systems are viewed as basic elements of the united information space in the net-centric control system. This paper also describes specific applications for new suppression methods based on existing technical equipment of electronic warfare.* ***Results.*** *New methods of radio cyber-attacks are presented as the evolution of contemporary jamming methods and are described in the paper. The proposed cyber-attacks suppress net-centric system functions by disrupting the multiple access protocols, routing protocols and QoS protocols of telecommunication systems. Unlike existing methods of radio suppression, which specialize only in disrupting individual network elements (links and network nodes), new methods focus on breaching primary functional telecommunication protocols.* ***Applicability.*** *Methods of radio cyber-attacks that are proposed in this paper can be applied to effectively disrupt the net-centric control systems. They also can be used in stability and firmness tests of net-centric control system elements.*

Keywords*: net-centric control system, electronic warfare, jamming, information warfare, , telecommunications network, network.*

Information about Author

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Chief designer. “Intel Group Corporation” ltd. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197372, Saint Petersburg, Bogatyrskiy prospect, 32, korp. 1, lit. A, office 6N.