

P.I. ANTONOVICH,
S.I. MAKARENKO,
R.L. MIHAYLOV,
K.V. USHANEV

П.И. АНТОНОВИЧ,
С.И. МАКАРЕНКО,
Р.Л. МИХАЙЛОВ,
К.В. УШАНЕВ

ПЕРСПЕКТИВНЫЕ СПОСОБЫ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА СИСТЕМЫ ВОЕННОГО УПРАВЛЕНИЯ В ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

NEW MEANS OF DESTRUCTIVE EFFECTS ON NETWORK CENTRIC MILITARY COMMAND, CONTROL AND COMMUNICATION SYSTEMS IN THE COMMON INFORMATION SPACE

В статье представлен подход к проблеме применения современных средств радиоэлектронного подавления в целях деструктивного воздействия на систему военного управления построенную по сетцентрическому принципу в едином информационном пространстве.

In article presents the new approach to a problem of application means of electronic jamming for the purpose of destructive effect on the network centric military command, control and communication systems in the common information space.

Ключевые слова: система военного управления в едином информационном пространстве, сетевой принцип управления, радиоэлектронное подавление, радиоэлектронная борьба, сеть связи, система связи, устойчивость.

Keywords: network centric control system, electronic jamming, electronic warfare, communications network, communications system, operation stability.

В настоящее время есть все основания полагать, что в ближайшем десятилетии ключевая парадигма ведения вооруженного противоборства, действующая в армиях США и стран НАТО, а также внедряемая в Вооруженных Силах РФ, будет базироваться на концепции управления боевыми действиями по сетцентрическому (сетевому) принципу. Следует напомнить, в общих чертах, что в соответствии с этим принципом в составе привлекаемой к военным действиям группировки войск (сил) выделяются функционально взаимосвязанные подсистемы: информационно-управляющая, сенсорно-разведывательная и боевая (исполнительная). Затем на основе формируемого коммуникационными системами единого информационного пространства (ЕИП) происходит объединение между собой этих подсистем, дающее значительный прирост в эффективности применения войск и оружия. При этом фундаментом такой системы является информационно-управляющая подсистема (или просто система управления), которая объединяет боевую и разведывательную подсистемы [1–4].

Проведенный анализ реализации сетевого принципа управления в ЕИП, отраженный в руководящих документах, научно-исследовательских и опытно-конструкторских работах ведущих зарубежных стран, позволяет выявить ряд основных тенденций в изменении характера вооруженной борьбы между развитыми в техническом отношении государствами на период до 2020 года и дальнейшую перспективу [3]:

стремление к завоеванию и удержанию глобального («всеохватывающего») информационно-пси-

хологического превосходства над противником, достигаемого прежде всего за счет проведения информационно-специальных операций;

расширение масштаба применения космических средств для ведения разведки, управления войсками и оружием группировок сухопутных, военно-воздушных и военно-морских сил, нанесения ударов в космосе и из космоса;

сокращение циклов управления войсками и оружием, а также продолжительности операций (боевых действий), сопровождающееся резкими изменениями обстановки и способов действий войск;

возрастание угрозы нанесения противником упреждающего удара высокоточным оружием и огневыми средствами в сочетании с информационным и радиоэлектронным воздействием на информационную инфраструктуру государства;

переход к избирательному поражению критически важных объектов инфраструктуры страны и ее вооруженных сил высокоточным оружием;

рост влияния на ход и исход операций (боевых действий) радиоэлектронного поражения элементов систем управления войсками и оружием и средств программно-аппаратного воздействия, а также других методов борьбы;

возрастание роли разведки, оперативной маскировки и защиты войск, населения и объектов тыла от высокоточных и перспективных средств поражения;

расширение сфер применения и масштабов использования беспилотных, роботизированных и дистанционно управляемых средств ведения и обеспечения вооруженной борьбы;

возрастание роли применения сил специальных операций для разведывательно-диверсионных действий в глубоком тылу войск противника.

Кроме того, можно выделить некоторые характерные черты вооруженной борьбы, неразрывно связанные с реализацией сетевого принципа управления в ЕИП [4]:

средства вооруженной борьбы являются информационно насыщенными и содержат в своем составе элементы сетевой информационной инфраструктуры;

сокращаются циклы принятия решений, возникает необходимость учета дополнительных факторов в процессе управления, что требует увеличения пропускной способности информационной подсистемы;

принятие управленческих решений происходит с учетом данных получаемых из автоматизированных экспертных систем и систем поддержки принятия решений;

аппаратно-программные средства, обеспечивающие взаимодействие в рамках ЕИП, формируют сложную сетевую глобальную информационную инфраструктуру;

элементы сетевой инфраструктуры (средства вооруженной борьбы, обеспечения, управления и коммуникации) по своей сути являются информационно-вычислительными системами разного уровня сложности и организации.

В то же время система управления, функционирующая в рамках ЕИП, будет малоэффективна, если в результате деструктивного воздействия на нее будет происходить следующее:

разрушение информационных потоков, циркулирующих между элементами системы;

снижение скорости информационного обмена между элементами системы, влекущее за собой значительное увеличение продолжительности цикла «обнаружение — опознавание — целеуказание — поражение» и, как следствие, снижающее эффективность реализации противником сетевого принципа управления в ЕИП;

обеспечение противоборствующей стороной в достаточной мере массированного и длительного вывода из строя сетеобразующих средств.

Таким образом, для реализации такого рода деструктивного воздействия необходимо принять меры по координации действий систем и средств разведки, комплексов и средств радиоэлектронного поражения (РЭПр), связи и управления со средствами огневого поражения и силами осуществляющими захват (вывод из строя) объектов системы управления противника в ЕИП. Также с учетом тенденций развития современных информационных технологий следует активизировать работы в области создания нелетальных средств направленного воздействия, способных нарушать работу автоматизированных систем управления, баз данных и локальных вычислительных сетей, выводить из строя радиоэлектронные объекты основных орга-

нов управления, связи и разведки противника.

Рассмотрим одно из достаточно легко реализуемых на практике перспективных направлений деструктивного воздействия на системы военного управления в ЕИП.

Современная информационно-управляющая подсистема группировки войск (сил), функционирующая в рамках ЕИП образуется вычислительными системами разного уровня сложности, связанными между собой сетями связи (СС). Как известно, одним из основных свойств систем управления (СУ), характеризующих их способность функционировать по назначению, является устойчивость связи. При этом под устойчивостью связи понимается способность СС выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов [5, 6]. В свою очередь, под дестабилизирующими факторами понимается воздействие на СС, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к ней характера, приводящее к выходу из строя элементов сети.

Применительно к СС, функционирующим в составе СУ в ЕИП, в качестве внешних дестабилизирующих факторов принято рассматривать отдельно воздействие обычным и ядерным оружием противника, а также влияние естественных и преднамеренных помех. В рамках существующего подхода устойчивость связи рассматривается как интегральное свойство, которое декомпозируется на [6, 7]:

живучесть — способность СС обеспечивать управление войсками, силами и оружием в условиях воздействия обычного и ядерного оружия противника;

помехоустойчивость — способность СС обеспечивать управление войсками, силами и оружием в условиях воздействия естественных помех;

помехозащищенность — способность СС обеспечивать управление войсками, силами и оружием в условиях воздействия преднамеренных помех противника;

надежность — способность СС обеспечивать связь, сохраняя во времени значения эксплуатационных показателей в пределах, соответствующих условиям эксплуатации, технического обслуживания, восстановления и ремонта.

Исходя из этого можно утверждать, что снижение устойчивости функционирования СС противника приведет к нарушению сетевого принципа управления и, возможно, к разрушения его ЕИП. Очевидно, что данное направление исследований является актуальной военно-прикладной задачей.

Применительно к современным системам управления обычно выделяют три слоя ЕИП, которые могут быть подвергнуты воздействиям:

физический (техническая инфраструктура систем связи),

семантический (данные),

синтаксический (протоколы передачи данных).

Логично, что такого рода подход позволяет определить следующие воздействия:

воздействия на физический слой, направленные на реальную инфраструктуру информационно-управляющих и вычислительных систем, систем передачи данных и подразумевающие их *физическое* разрушение;

воздействия на семантический слой, связанные с нарушением целостности и корректности информации;

воздействия на синтаксический слой, направленные на повреждение данных и нарушение логики функционирования систем.

В настоящее время в силу ряда обстоятельств, при сопоставимом уровне достигаемого результата, воздействия средствами РЭПр на семантический и синтаксический слои ЕИП представляются более простыми, доступными и легкорезализуемыми, чем воздействия на физическом уровне. Как следствие, разработке этих РЭПр для решения такого рода задач уделяется все больше внимания [7-12]. При этом предполагается комплексное сбалансированное применение комплексов и средств РЭПр с одновременным проведением мероприятий по защите своих систем управления и информационных ресурсов.

Ввиду недостаточно разработанной теоретической базы проведения такого рода воздействий, наиболее простым, целесообразным способом воздействия является применение средств РЭПр на сети радиосвязи (СРС) в составе СС с целью снижения

их устойчивости функционирования в интересах нарушения синтаксического слоя ЕИП противника.

Вместе с тем проведенный анализ использования существующей «традиционной» тактики подавления и применения комплексов и средств РЭПр показал, что оно недостаточно эффективно при использовании противником сетевого принципа управления на основе ЕИП.

Основанный на «традиционном» подходе к воздействию РЭПр пример нарушения работы иерархической системы управления (на примере СУ тактической авиации) показан на рис. 1. Как видно из левой части рисунка, нарушения управления достигались при воздействии средств радиоэлектронного подавления (РЭП) на любом уровне иерархической СУ, в результате блокирования прохождения информации к средству поражения, и, как следствие, не выполнения им боевой задачи.

Таким образом, формы и способы применения комплексов и средств РЭП, разработанные до появления концепции сетевого управления, будут неэффективны против вооруженных формирований, управляемых СУ в ЕИП. В подобной системе полностью перекрыть каналы информационного обеспечения и управления практически невозможно. Для нарушения работы такой СУ (рис. 1) необходимо исключить все каналы управления и передачи информации или вывести из строя все технические или боевые средства. Фактически эффект может

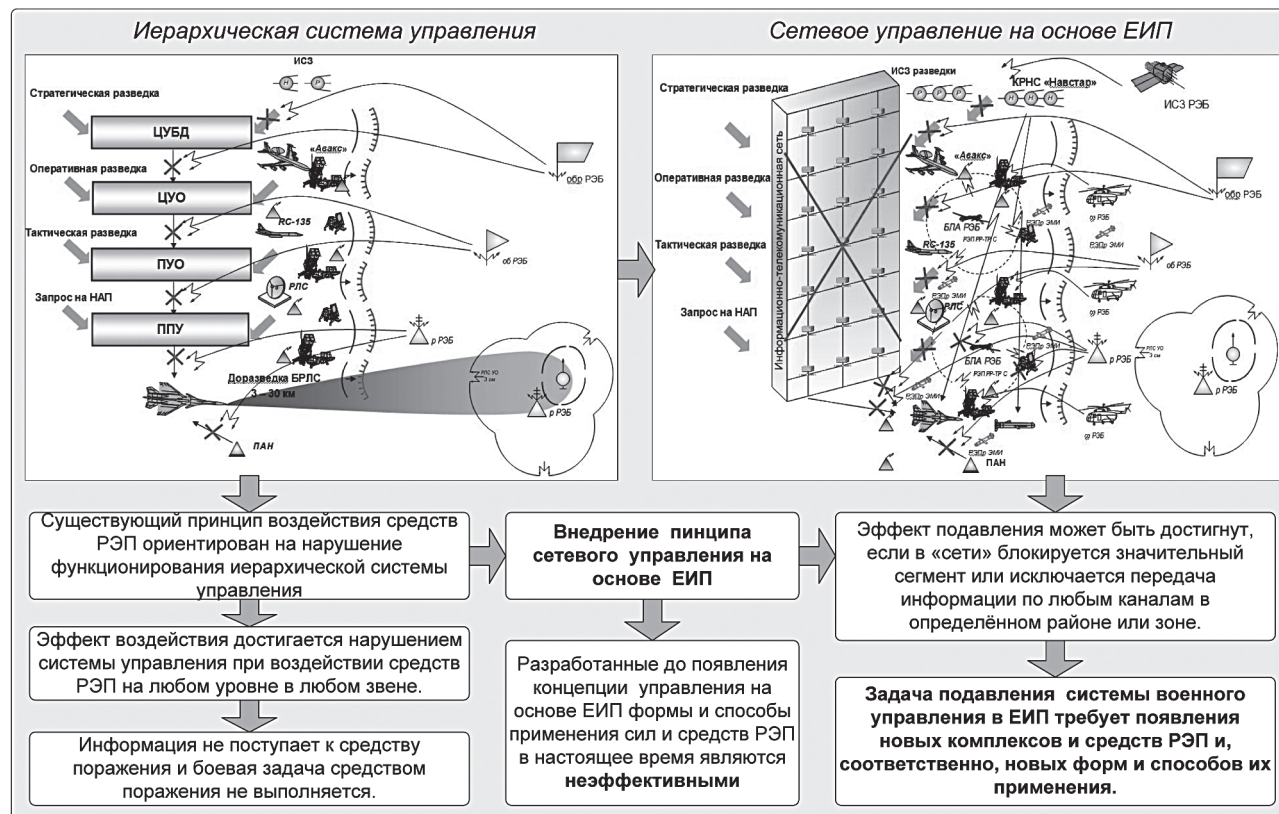


Рис. 1. Применение комплексов и средств РЭПр в интересах деструктивного воздействия на системы управления

быть достигнут, если в системе блокируется значительный сегмент или исключается передача информации по любым каналам в определенном районе или зоне. Решение такой задачи требует разработки новых комплексов и средств РЭП и, соответственно, новых форм и способов их применения. В качестве обобщения можно сделать следующие выводы [11]:

существующий в настоящее время подход по воздействию средств РЭП на отдельные элементы СС и СРС в ЕИП неэффективен;

воздействуя на информационную инфраструктуру системы военного управления в ЕИП, техническую основу которой составляют СС и АСУ, можно достигнуть значимого эффекта поражения данной системы.

Воздействие территориально распределенной разнородной группировки средств РЭП позволит реализовать ряд направлений противодействия системам управления, построенным в соответствии с сетевым принципом в ЕИП, сформулированные ранее:

разрушение информационных потоков;

снижение скорости информационного обмена между элементами системы;

обеспечение достаточно массивного и долговременного вывода из строя сетевобразующих средств.

Проведенные исследования показывают, что на современном этапе развития систем военного управления в ЕИП, наиболее уязвимыми к деструктивному воздействию будут космические сегменты информационной подсистемы. В первую очередь это связано с тем, что такого рода сегменты с одной стороны, осуществляют глобальные функции информационного обеспечения, а с другой — строятся на основе средств радиосвязи. Как следствие, они весьма чувствительны при воздействии на них средствами РЭП.

В результате возникающее снижение качества функционирования космической группировки приведет к множественным проблемам в работоспособности информационной подсистемы что в свою очередь повлияет на применение многих видов вооружения и военной техники. Последнее утверждение связано с тем, что именно космический сегмент, включающий космические системы разведки, связи, навигации, топогеодезического и метеорологического обеспечения, интегрированные в единый информационно-управляющий контур, является основой архитектуры глобальной информационной подсистемы.

Поражение различных компонентов такого информационно-управляющего контура приведет к невозможности каждой из систем обеспечивать выполнение всех или части присущих ей функций. В частности можно выделить:

в космической разведке — невозможность с заданной своевременностью передавать сообщения об обнаружении объектов, целеуказании и оперативном контроле результатов воздействия ударными

средствами, а также данных о складывающихся условиях обстановки для определения применяемых ударных средств;

в космических системах связи — невозможность с заданным качеством обеспечить передачу сообщений боевого управления, осуществлять обмен данными между воинскими формированиями и органами управления, включая оперативную передачу на пункты управления данных для подготовки ударов, и их результат;

в космических топогеодезических системах — невозможность передавать сообщения по обеспечению органов военного управления всех уровней достоверными топографическими и геодезическими данными с заданной своевременностью, обеспечить войска специальными картами и фотодокументами местности, а также сделать недоступным доступ к цифровым информационным массивам в интересах систем наведения высокоточного оружия;

в космических радионавигационных системах — подавление радиоканалов управления космическими аппаратами приведет к отказу системы и, соответственно, невозможности создания навигационных полей, которые используются при определении местоположения воинских формирований, боевой и другой техники, ударных средств и средств поражения.

Таким образом, из выше приведенного становится вполне очевидным, что именно специфика современного подхода к реализации сетевого принципа при построении систем военного управления в ЕИП, позволяет использовать именно комплексы и средства РЭП как первоочередное и достаточно легко реализуемое средство для их поражения. Исходя из приведенных выше аргументов, представляется возможным сформулировать ряд подходов к реализации деструктивного воздействия на СС, функционирующую в ЕИП.

Современная методология применения средств РЭП ставит своей целью снижение показателей качества обслуживания отдельных сетей и каналов радиосвязи ниже значений, определенных требованиями по качеству связи. До последнего времени основная часть работ по РЭП была посвящена решению задач подавления отдельных линий радиосвязи (ЛРС), т. е. подавлению на физическом уровне модели взаимодействия открытых систем (OSI — Open Systems Interconnect).

Имеются отдельные исследования, посвященные подавлению СРС с учетом их структуры, логики функционирования и ценности передаваемой информации. Вместе с тем, как указано выше, объединение военных СС, в том числе СРС, в глобальную сеть связи и информационного обеспечения на основе ЕИП способствует тому, что подавление отдельных СРС в составе такой глобальной сети не ведет к информационным потерям или снижению своевременности передачи данных. В такого рода системе подавление отдельных СРС приведет к перемаршрутизации информационных потоков в объ-

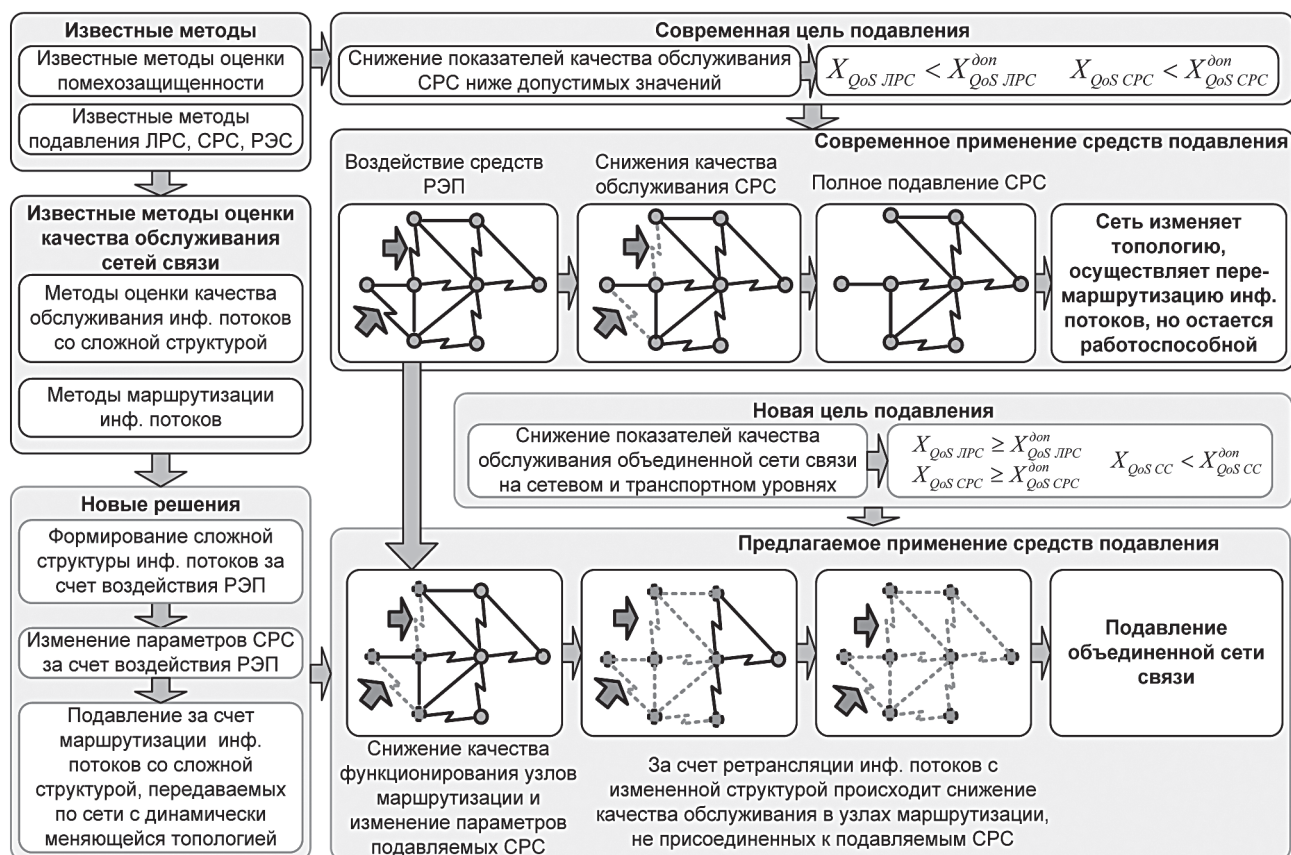


Рис. 2. Предлагаемый способ деструктивного воздействия на системы военного управления на основе ЕИП



Рис. 3. Деструктивное воздействие средств РЭП на уровни транспортной подсистемы модели OSI

единой СС без снижения оперативности и потери работоспособности (рис. 2).

Воздействие средств РЭП на СС происходит на физическом уровне модели OSI, однако в полной мере это воздействие проявляется также и на вышестоящих уровнях транспортной подсистемы модели OSI – канальном, сетевом и транспортном (рис. 3). Именно за счет использования эффектов воздействия средств РЭП на канальном, сетевом и транспортном уровнях OSI предполагается решение проблемы комплексного подавления объединенных СС, являющихся технической основой системы военного управления с использованием ЕИП [4, 8-12, 13-22]. При этом непосредственным объектом воздействия будут отдельные ЛРС и СРС, функционирующие в составе ЕИП.

В настоящее время имеется большое количество работ по исследованию эффективности функционирования СС, коммутационных устройств различного уровня в условиях передачи трафика сложной структуры (наличие самоподобных свойств, непугасоновское распределение времени поступления пакетов и др.), а также по маршрутизации информационных

потоков в СС с динамически изменяемой топологией. В ряде работ указывается на значительное снижение быстродействия обслуживания информационных потоков, особенно при передаче их по СС с динамически изменяющейся топологией [20]. Исходя из этого представляется возможным использовать полученные результаты исследований в области оценки качества обслуживания для обоснования новых направлений решения проблемы подавления объединенных СС за счет разработки новых методов и алгоритмов воздействия средств РЭП на отдельные СРС.

Кроме того, анализ работ по моделированию радиоэлектронного конфликта [11, 12, 18, 19] позволяет сделать вывод о конфликтно-устойчивом характере взаимодействия средств РЭП и СС. Такое взаимодействие описывается на основе теории марковских процессов, при этом рассматривается переход средств СРС между состояниями «работоспособен» – «неработоспособен» (ON-OFF модель). Как правило, целью воздействия средств РЭП является увеличение вероятности нахождения СРС в режиме OFF. В предлагаемом подходе конфликтно-устойчивые ON-OFF модели могут быть использованы для фор-

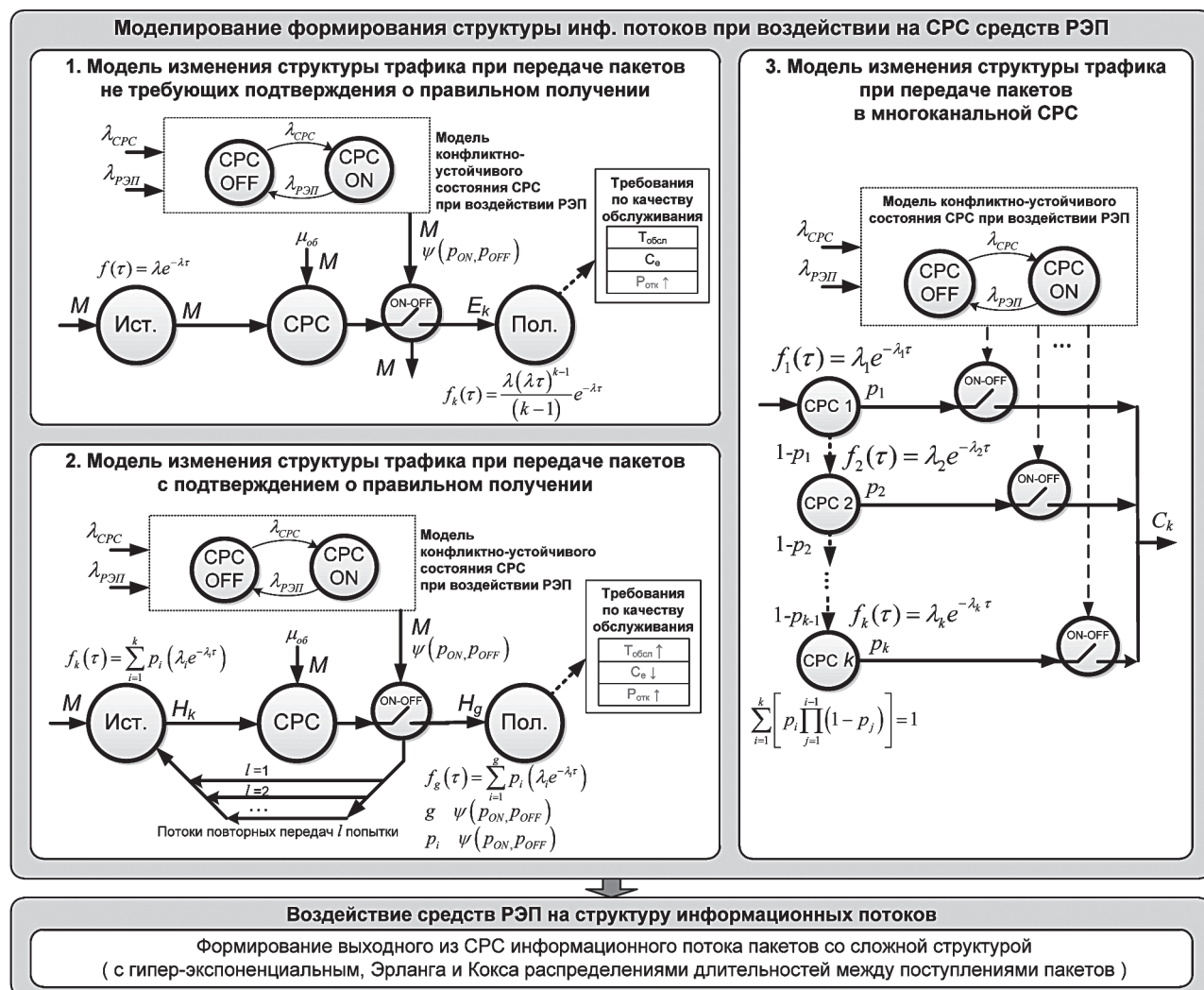


Рис. 4. Использование средств РЭП для формирования трафика сложной структуры

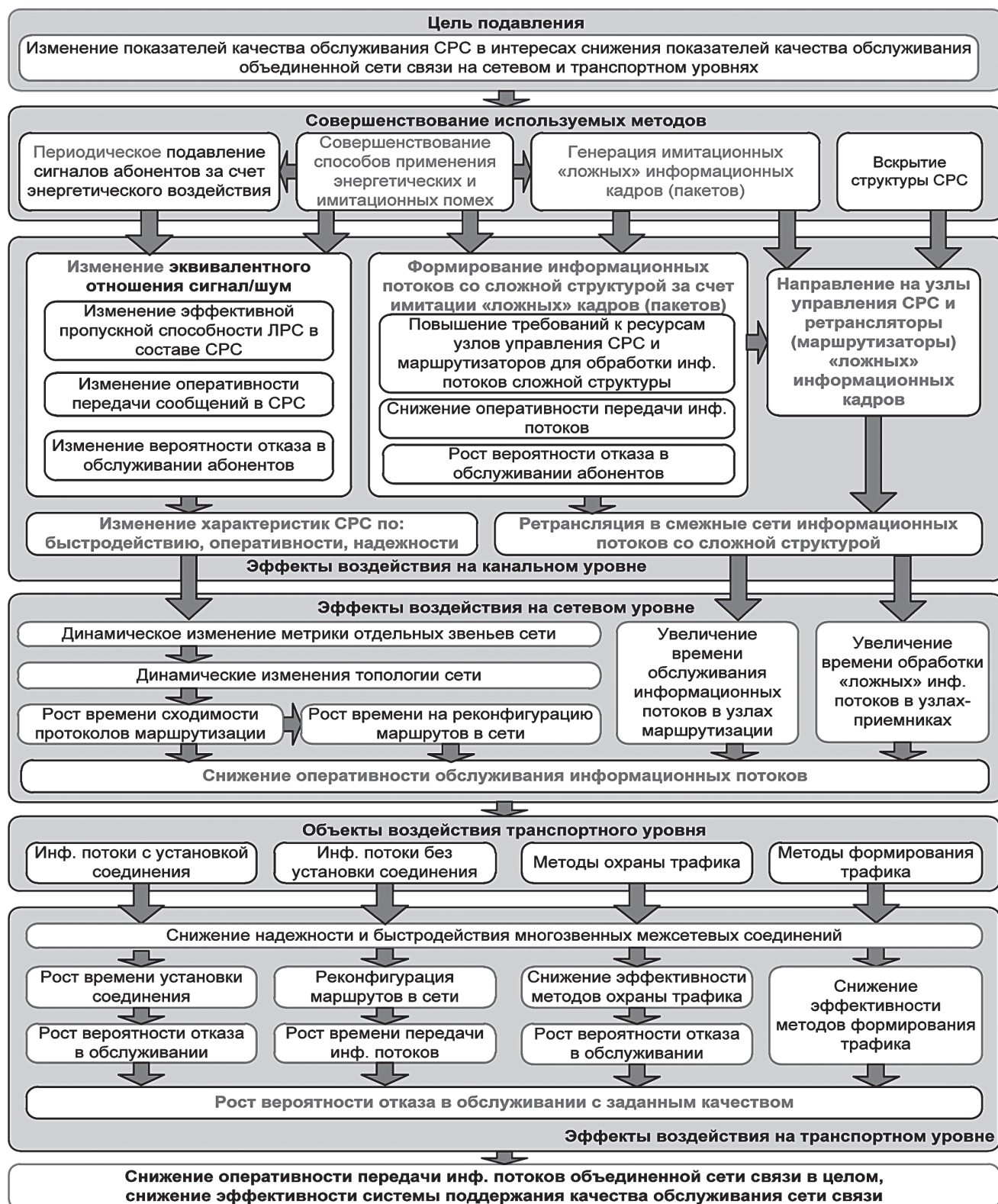


Рис. 5. Решение проблемы деструктивного воздействия на объединенную СС в ЕИП

мирования условий, при которых передаваемые информационные потоки (сетевой трафик) изменяют свою структуру (рис. 4) [21, 22].

Воздействие на структуру циркулирующих в СС информационных потоков позволит решить проблему организации бескомпроматного воз-

действия на информационно-управляющую сеть в ЕИП в обход средств сетевой защиты (средств типа IDS), средств защиты специального программного обеспечения и операционных систем телекоммуникационного оборудования (таких как IOS для телекоммуникационного оборудования Cisco).

Указанное изменение структуры информационных потоков является усложненной реализацией варианта DDoS-атаки на телекоммуникационные узлы, проводимой за счет нового способа применения средств РЭП. Причем эффект подавления достигается в каждом из телекоммуникационных узлов, по которым передается информационный поток, подвергшийся воздействию. Предлагаемый принцип подавления основывается на известных эффектах снижения оперативности обработки телекоммуникационным оборудованием (в 2-6 раз) информационных потоков сложной структуры и имеющих самоподобные фрактальные свойства [21, 22]. При этом информационное содержание сообщений потока не меняется.

Предлагаемый принцип подавления системы связи также может быть реализован за счет применения деструктивных программных средств, внедряемых в программное обеспечение абонентов системы. В этом случае изменение структуры передаваемых информационных потоков будет производиться непосредственно сетевыми протоколами абонентов, находящихся под контролем деструктивных программных средств.

Исследования эффектов воздействия средств РЭП на функционирование протоколов маршрутизации показало, что на сетевом уровне системы связи подавление отдельных СРС будет проявляться в виде снижения эффективности функционирования алгоритмов маршрутизации, увеличения времени на установку соединений и доставку пакетов, а также в снижении устойчивости сети связи [6, 7, 13, 14]. Эффектами воздействия средств подавления на функционирование лавинных (*OSPF – Open Shortest Path First* и *EIGRP – Enhanced Interior Gateway Routing Protocol* и др.) и игровых (*MPLS – Multi Protocol Label Switching*) методов маршрутизации будут увеличение служебной нагрузки, создаваемой протоколами маршрутизации в результате периодического изменения параметров СРС и КС, а также снижение коэффициента готовности сети [6, 7, 15, 16, 20].

Аналогичный эффект достигается и при формировании сложной структуры информационных потоков, циркулирующих в сети [17, 21, 22]. Причем именно игровым методам (на основании которых строятся сети NGN (Next generation network), являющихся технической основой систем связи вооруженных сил технологически развитых государств, в максимальной степени затруднительно поддерживать качество обслуживания абонентов. Это позволяет сделать вывод о принципиальной возможности реализации подавления глобальных СС за счет дестабилизации функционирования протоколов маршрутизации путем воздействия средств РЭП на отдельные СРС.

В настоящее время проводятся мероприятия по внедрению сетевого принципа управления в ЕИП в практику войск США, НАТО и ряда развитых в военном и техническом отношении государств. Вместе с тем с внедрением такой перспективной системы управления войска США и НАТО делают возможным применение против себя новых способов РЭП, позволяющих реализовать подавление системы военного управления в ЕИП. В связи с этим чрезвычайно актуальна разработка и внедрение подобных форм и способов военного противодействия в практику ведения боевых действий. Схематично возможная последовательность решения проблемы деструктивного воздействия на объединенную СС в ЕИП представлена на рис. 5.

В заключение необходимо отметить, что в представленной вниманию читателей статье представлены только некоторые аспекты исследуемой темы. В настоящее время авторами продолжают активные научно-поисковые работы в данной предметной области. Промежуточные результаты военно-прикладных исследований в области актуальности противодействия системам военного управления на основе ЕИП опубликованы авторами в работе [4, 23-25], а вопросы технической реализации подобного противодействия – в работах [7, 13-17, 19-22].

ПРИМЕЧАНИЯ:

1. Хант Г. Реализация систем для ведения сетецентрических войн // МКА: мир ВКТ. 2007. № 6. С. 64–70.
2. Макаренко С. И., Бережнов А. Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в ВС РФ // Вестник академии военных наук. 2011. № 4 (37). С. 64-68.
3. Налетов Г.А. К вопросу о разработке концепции нетрадиционных войн и вооруженных конфликтов (Новые формы и способы ведения вооруженной борьбы) // Вестник Академии военных наук. № 1 (38). 2012. С. 29-34.
4. Антонович П.И., Шаравов И.В., Лойко В.В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник Академии военных наук. № 1 (38). 2012. С. 41-45.
5. ГОСТ 5311 – 2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. – М.: СтандартИнформ, 2009. 16 с.
6. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.
7. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы, № 4, 2013. С. 69-79.
8. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47. – URL: <http://www.st-s.su/sites/default/files/files/pdf/2011-03/2011-03-makarenko.pdf>
9. Макаренко С. И. Подавление объединенных сетей связи // Доклад на НТК Инновационные подходы к развитию вооружению вооружения, военной и специальной техники. – М.: ВА ГШ ВС РФ, 2011.

10. Макаренко С.И. Новый подход к радиоэлектронному подавлению сетевых систем военного управления // Военная радиоэлектроника: опыт использования и проблемы подготовки специалистов. Мат. докладов 23 НТК. Ч. 3. – Петродворец: ВМирЭ им. А.С. Попова (филиал ВУНЦ ВМФ «ВМА», г. Петродворец), 2012. С. 14-27.
11. Сафронов А.Л. «Требования к функционированию телекоммуникационных сетей военного назначения в едином информационном пространстве группировки войск (сил) в условиях сетевых атак противника» // Доклад на НТК «Современные тенденции развития теории и практики управления в системах специального назначения. – М.: ОА «Концерн «Системпром», 2012.
12. Стародубцев Ю.И., Семенов С.С., Бухарин В.В. Доклад «Методология оценки защитного ресурса ИТКС военного назначения в условиях техносферной войны» на НТК «Инновационные подходы к развитию вооружения и военной и специальной техники». М.: ВА ГШ ВС РФ, 2011.
13. 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. – URL: www.sbook.ru/itmu/itmu.htm
14. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. – URL: jre.cplire.ru/jre/sep11/4/text.pdf
15. Макаренко С. И. Анализ воздействия преднамеренных помех на функционирование расширенного протокола маршрутизации внутреннего шлюза (EIGRP) // Информационные технологии моделирования и управления. 2010. № 2 (61). С. 223-230. – URL: www.sbook.ru/itmu/itmu.htm
16. Макаренко С. И. Анализ воздействия преднамеренных помех на сетевой уровень модели взаимодействия открытых систем и функционирование протокола маршрутизации оценки состояния канала (OSPF) // Информационные технологии моделирования и управления. 2009. № 7 (59). С. 956–961. – URL: www.sbook.ru/itmu/itmu.htm
17. 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>
18. Владимиров В.И., Владимиров И.В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: ВАИУ, 2008. – 231 с.
19. Макаренко С.И., Иванов М.С., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб.: Свое издательство, 2013. – 166 с.
20. 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, № 2, 2013. – С. 61-68.
21. Макаренко С. И. Анализ математических моделей информационных потоков общего вида и степени их соответствия трафику сетей интегрального обслуживания // Вестник ВГТУ. 2012. Т. 8. № 8. С. 28-35.
22. 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.
23. Антонович П.И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. № 1 (34). 2011. С. 43-47.
24. Антонович П.И. О современном понимании термина «кибервойна» // Вестник Академии военных наук. № 2 (35). 2011. С. 89-96.
25. Антонович П.И. О сущности и содержании кибервойны // Военная мысль. № 7. 2011. С. 39-46.