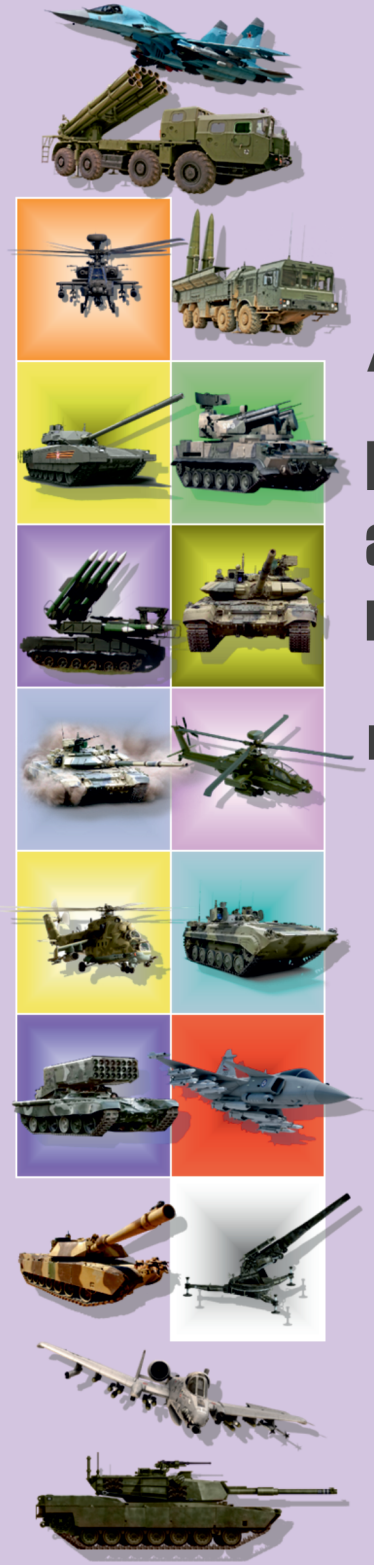


А. А. Бойко

Киберзащита автоматизированных систем воинских формирований

Монография

А.А. Бойко

Киберзащита автоматизированных систем воинских формирований

Монография

Санкт-Петербург
Наукоемкие технологии
2021

УДК 623.62
ББК 32.972
Б72

Рецензенты:

ведущий научный сотрудник Михайловской военной артиллерийской академии д.т.н., профессор, Заслуженный деятель науки РФ *Анисимов В.Г.*;

директор научно-технического центра Научно-исследовательского института радио д.в.н., доцент *Антонович П.И.*;

ведущий научный сотрудник 46 Центрального научно-исследовательского института МО РФ д.т.н., профессор, Заслуженный работник высшей школы РФ *Буравлев А.И.*;

директор по научно-техническому развитию Научно-исследовательского института «Рубин» д.т.н., профессор, Заслуженный изобретатель РФ *Гречишников Е.В.*;

начальник управления 4 Центрального научно-исследовательского института МО РФ д.т.н., профессор *Климов С.М.*;

доцент кафедры программного обеспечения и администрирования информационных систем Воронежского государственного университета д.ф.-м.н., доцент *Кузнецов А.В.*;

ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук д.т.н., доцент *Макаренко С.И.*

Б72 **Бойко А.А.**
Киберзащита автоматизированных систем воинских формирований. Монография. – СПб.: Наукоемкие технологии, 2021. – 300 с.

УДК 623.62
ISBN 978-5-6046688-3-2 ББК 32.972

Монография посвящена защите автоматизированных систем разведки, связи и управления войсками (силами) и оружием (боевыми средствами), применяемых в боевых циклах воинских формирований, от кибератак противника. Защищенность предлагается обеспечивать заблаговременно, в процессе создания (модернизации) таких систем. Для этого генерируется необходимое и достаточное множество тестовых способов реализации кибератак на телекоммуникационное оборудование, отбираются успешные способы, оценивается эффективность ранее известных и отобранных способов с использованием высоко детализированной модели боевой обстановки и выбираются уязвимости, подлежащие устранению при заданных ограничениях. Способы генерируются на основе спецификаций телекоммуникационных протоколов с учетом точности содержания, кратности передачи и своевременности доставки сообщений. Взаимное влияние противоборствующих сторон учитывает объединение в боевые циклы процессов разведки, управления, огневого поражения, связи, реализации кибератак, радиоэлектронного подавления, имитации обстановки, воздействия мощным электромагнитным излучением, нелетального, психологического, радиационного, химического и биологического воздействия.

Для специалистов в области информационной безопасности автоматизированных систем военного назначения, моделирования боевых действий, оценки боевой эффективности образцов вооружения и воинских формирований, а также студентов (курсантов), аспирантов (адъюнктов) и докторантов соответствующих специальностей.

ISBN 978-5-6046688-3-2

Посвящается моим
родителям, Елене Николаевне
и Александру Павловичу,
супруге, Александре Сергеевне,
и детям, Светлане, Радомиру,
Милославе и Ладе,
без любви, веры и терпения которых
эта работа не могла бы состояться.

Оглавление

Предисловие

Современные информационные способы и средства борьбы, связанные с воздействиями на компьютерные системы связи и боевого управления (так называемые «кибератаки»), представляют сегодня новый и грозный вид оружия. Применение этого оружия при определенных условиях приводит к значительному эффекту в ходе военных действий различного масштаба. Оценка эффективности применения такого «кибероружия» и разработка способов защиты от него является актуальной теоретической и практической проблемой как современной военной науки, так и целого ряда технических наук.

Предлагаемая читателю монография является чрезвычайно актуальной и представляет собой системное исследование, в котором изложен новый подход к моделированию процессов информационного воздействия на каналы связи и передачи данных в автоматизированных системах управления, оценки степени их «поражения» как на информационном, так и на физическом уровне, приводящих, в конечном счете, к снижению эффективности боевого управления, срыву выполнения боевых задач в ходе боевых действий. Автору впервые удалось связать в рамках предлагаемого подхода к моделированию «информационную» и «физическую» реальность как две ипостаси объективной реальности.

Важным достижением автора является установление связи между информационным «ущербом», возникающим в результате «кибератаки» на компьютерные системы связи и боевого управления, и «ущербом», связанным с потерей управления боевыми (огневыми) средствами в ходе операции (удара, боя). Автор корректно использовал известные в теории боевой эффективности модели, дополнив их связями с информационными моделями боевого управления, что придало им большую общность с точки зрения их применения в научных и прикладных исследованиях.

Материалы монографии будут полезны специалистам, работающим в области информатизации военных систем, обеспечения компьютерной безопасности автоматизированных систем управления, оценки эффективности применения современных боевых информационно-управляющих систем различного назначения, а также профессорско-преподавательскому составу, адъюнктам и докторантам военных учебно-научных центров Министерства обороны Российской Федерации.

Заслуженный работник вышей школы Российской Федерации,
доктор технических наук, профессор
А.И. Буравлев

Введение

«Зри в корень!»

Козьма Прутков

Война современная и тем более война будущего характеризуется значительным использованием в образцах вооружения последних достижений цифровых (или компьютерных) информационных (в том числе телекоммуникационных) технологий. Однако что мы знаем о влиянии этих технологий на ход и исход боя? С одной стороны, они существенно повысили уровень информатизации образцов вооружения, что привело к сокращению длительности боевых циклов и потерь личного состава, освобождая в ряде случаев человека от необходимости присутствия в опасных районах (например, при использовании беспилотных летательных аппаратов). С другой стороны, эти технологии снизили надежность образцов вооружения за счет их многократного усложнения, затруднили процессы освоения и ремонта. Но список возникших проблем этим не ограничивается. Пожалуй, наибольшая опасность от внедрения новых технологий связана с появлением *кибер*оружия. Поражающее действие этого принципиально нового вида информационного оружия основано на использовании средств и технологий разрушения, подавления или поражения информационно-технических средств автоматизированных систем, используемых в образцах вооружения.

Принимая во внимание многогранность кибернетики, автор считает важным подчеркнуть, что используемые в монографии слова с приставкой «*кибер-*» относятся только к компьютерным системам, то есть к автоматизированным системам, элементы которых функционируют (в том числе осуществляют информационное взаимодействие) с использованием средств вычислительной техники, то есть компьютеров (от англ. *compute* – вычислять). В России термины с этой приставкой пока еще не являются строго научными, поскольку не имеют «гостированных» определений. Тем не менее эти термины уже прочно вошли в обиход отечественных журналистов и специалистов в области информационной безопасности. К тому же в англоязычной литературе, откуда и пришла к нам эта приставка, термины с ее использованием провозглашаются на уровне государственных концепций. Поэтому, соблюдая баланс между лаконичностью и научной строгостью, приставку «*кибер-*» читателю следует воспринимать как сокращение термина «киберкомпьютерный» или просто «компьютерный». Используемые с этой приставкой термины определены в глоссарии в конце монографии.

С применением *кибер*оружия осуществляются *кибер*атаки – целенаправленное воздействие программными или программно-аппаратными средствами на автоматизированные системы в целях нарушения, прекращения их функционирования или создания угрозы безопасности обрабатываемой этими системами информации. В известной отечественной научной литературе кибератаки называются также компьютерными атаками, программно-

математическим, программно-аппаратным, программно-техническим, программным, радиоэлектронно-информационным воздействием и т.п.

Кибератаки, применяемые на поле боя, по сути ничем не отличаются от кибератак в сети Интернет, но имеют некоторые характерные особенности.

Во-первых, на поле боя, то есть на тактическом уровне, кибератаки реализуются в основном по радиоканалу. Физический доступ к целевому объекту существенно затруднен из-за частого и быстрого изменения его местоположения. Вероятность получения доступа к целевому объекту не по радиоканалу ничтожно мала. Но возможны и исключения, являющиеся следствием диверсионной деятельности, проводимой на оперативном уровне и выше. Поэтому для реализации боевой кибератаки необходимо иметь специальное оборудование, которое, с одной стороны, обеспечивает стабильный физический доступ к целевому объекту, и, с другой стороны, минимизирует, насколько это возможно, угрозу физического уничтожения противником этого оборудования и применяющего его личного состава.

Во-вторых, для того, чтобы реализовать кибератаку в боевых условиях, необходимо знать алгоритмы функционирования целевого объекта и хотя бы одну его уязвимость, эксплуатация которой способна нанести сколь угодно значимый ущерб атакуемой стороне. Такие уязвимости и средства их эксплуатации в сети Интернет не публикуются, а получить возможность исследовать на предмет выявления уязвимостей элемент боевой автоматизированной системы крайне сложно. Поэтому боевые кибератаки не для «скрипт-кидди» (от англ. *script* – скрипт, сценарий и *kiddie* – малыш) – злоумышленников, использующих чужие наработки и не понимающих принципа работы средств реализации кибератак.

Поражающим фактором кибератак является информация, переносимая электромагнитной волной (или электрическим током) в цифровом виде, воспринимаемом программами на целевом объекте в качестве легитимных сообщений. Эти сообщения содержат последовательности бит, называемые специальными программными средствами. Такие программные средства могут либо непосредственно влиять на работоспособность приемо-передающей аппаратуры, представляя собой так называемую *декларативную программную помеху*, либо проникать глубоко внутрь атакуемой системы и приводить ее в нужное для атакующей стороны состояние. В последнем случае специальные программные средства называются *процедурными программными помехами*. Примерами процедурных помех являются вирусы, троянские кони, «черви».

Для планирования и применения кибератак в вооруженных силах стран НАТО, Китая и других мировых держав уже созданы и активно развиваются *кибер*командования, предназначенные для ведения *кибер*операций в *кибер*пространстве (синоним термина «информационная сфера»). Некоторые военные эксперты провозглашают киберпространство новой сферой ведения боевых действий наравне с землей, воздухом, водой и космосом, закрепляя этот тезис даже в доктринальных документах своих стран. Но так ли это на самом деле? Не вызвана ли такая трактовка недостаточным пониманием сущности явления кибератак лицами, принимающими решение? Не является ли она очередным

маркетинговым ходом оборонной индустрии, представители которой желают поймать крупную рыбу в мутной воде? Тем временем уже даже на тактическом уровне организационно-штатные структуры современных и перспективных воинских формирований стали включать киберподразделения. Примером тому является многодоменная оперативная группа сухопутных войск США (англ. *Multi-Domain Task Force*, MDTF), в состав которой входит батальон разведки, информации, кибероперации, радиоэлектронной борьбы и космических операций (англ. *Intelligence*, *Information*, *Cyber/Electronic Warfare & Space*, I2CEWS). Может быть это заблуждение? Ведь нередко в среде военных специалистов можно услышать и такие мнения, кажущиеся весьма авторитетными:

- «Что это за кибервойна в тактическом звене? В Интернете – другое дело. А в бою, когда главное – решительность, инициатива, сила воли, дух, обеспеченность и натренированность, где место кибератакам?»;
- «Вот, например, гаубица. Выстрелил, и все понятно. А кибератаки и вообще средства радиоэлектронной борьбы что дают?»;
- «Лучшее средство радиоэлектронной борьбы – это тяжелая огнеметная система. Стопроцентное поражение радиоэлектронных средств».

Для однозначного научно обоснованного ответа на эти и аналогичные вопросы нужна единая, понятная для всех мера боевой эффективности, учитывающая взаимное влияние «материи» и «информации» на поле боя. Ведь кибероружие является, в первую очередь, информационным. Но такая общепринятая мера в военной науке сегодня отсутствует, несмотря на то, что материальный и особенно информационный аспекты боевой обстановки приобрели абсолютно новые грани еще в конце XX века. Для эпохи лавинообразного развития технологий такое отставание науки от практики весьма оправдано. Ведь в современных условиях высокоманевренного боя с применением высокоточных средств поражения и практически полной осведомленности о складывающейся боевой обстановке основные закономерности боевых действий стали весьма неопределенными даже без кибератак.

Особая актуальность сокращения такого отставания явилась побудительным мотивом для автора. Конечно же, автор не является первым исследователем столь злободневной тематики. Вопросу исследования кибератак на критически важные системы военного и двойного назначения посвящали свои глубоко проработанные с теоретической и практической точки зрения труды многие отечественные и зарубежные ученые. К пионерским следует отнести работы П.И. Антоновича, Е.В. Гречишникова, С.Н. Гриняева, Е.Б. Дроботуна, С.М. Климова, Н.А. Костина, М.А. Коцыняка, О.С. Лауты, А.Г. Ломако, С.И. Макаренко, Р.В. Максимова, В.Ю. Осипова, А.В. Паршуткина, С.А. Петренко, Ю.И. Стародубцева, М.А. Шнепс-Шнеппе и других видных ученых. Значимость вклада этих работ весьма велика. Однако их результаты требуют обобщения и систематизации. Кроме того, в известных работах оказались недостаточно исследованными два ключевых вопроса. Первый – как же все-таки быстро создавать новые эффективные способы реализации кибератак и достичь приемлемой полноты множества этих способов? Второй – как влияют кибератаки на ход и исход боя? Понимая под *кибер*защитой процесс обеспечения защищенности программного

обеспечения автоматизированных систем от кибератак, который характеризуется *полнотой охвата*, *гарантированностью* и *своевременностью*, с прагматической точки зрения указанные вопросы сводятся к еще одному важному вопросу: как в современных боевых условиях обеспечить киберзащиту автоматизированных систем воинских формирований? Этот вопрос может быть задан и более содержательно: *как создать необходимое и достаточное множество способов реализации кибератак на защищаемую автоматизированную систему, оценить их в заданной обстановке на уровне боевой эффективности противоборствующих сторон (то есть на уровне соотношения боевых потенциалов или остаточной доли численности противника с учетом коэффициентов боевой соизмеримости разнородных элементов боевых порядков) и выбрать подлежащие устранению уязвимости, когда ресурсов для устранения всех уязвимостей не хватает*?

Решение этого проблемного вопроса, имеющего весьма сложный междисциплинарный характер, способно перевести модернизируемые и создаваемые высокотехнологичные образцы вооружения на новый качественный уровень. К тому же в области сертификации киберзащиты телекоммуникационного оборудования гражданского и двойного назначения элемент такого решения смог бы гарантировать его защищенность от кибератак, в то время как ни одно из известных сегодня коммерческих средств тестирования телекоммуникационного оборудования, генерируя обширное множество типовых тестовых воздействий, такую гарантию не дает. Кстати, требуемую гарантию не обеспечивают и такие известные академические проекты, как, например, «UniTESK» и «BLAST» от Института системного программирования Российской академии наук, Java Pathfinder от NASA (США), «TLA+» от «Microsoft» (США), «Spin» от «Bell Labs» (США), «Uppaal» от университетов Уппсалы (Швеция) и Ольборга (Дания).

В настоящей монографии предлагается авторский подход к решению этого проблемного вопроса. В ней впервые с системной позиции рассматриваются создание способов реализации кибератак на автоматизированные системы разведки, связи и управления войсками (силами) и оружием (боевыми средствами), предназначенные для применения в боевых циклах воинских формирований, и оценка эффективности этих способов на уровне информационных, информационно-боевых и боевых показателей в бою, в котором одновременно противоборствующими сторонами применяются образцы вооружения с функциями разведки, управления, огневого поражения, связи, радиоэлектронного подавления, имитации боевой (в том числе радиоэлектронной) обстановки, воздействия мощным электромагнитным излучением, реализации кибератак, а также нелетального, психологического, радиационного, химического и биологического воздействия на личный состав. Предлагаемые материалы во многом обобщают и систематизируют опубликованные ранее результаты исследований автора, но некоторые результаты излагаются впервые.

Автор не тешит себя иллюзиями, что полученные им результаты смогут удовлетворить всем требованиям и соответствовать всем ожиданиям исследователей в столь емкой и многогранной области знаний. Это на сегодняшний день в принципе невозможно. Ведь данная область еще только формируется. Предлагаемая читателю монография представляет собой всего лишь очередной шаг на длин-

ном пути формирования теоретических основ для получения единой меры взаимного влияния «материи» и «информации» в новых реалиях вооруженной борьбы.

Для работы с монографией от читателя потребуется знакомство с базовыми положениями теории вероятностей, теории массового обслуживания, теории надежности, теории марковских процессов, теории формальных языков и грамматик, теории алгоритмов, теории графов, исследования операций, теории иерархических многоуровневых систем, теории эффективности целенаправленных процессов и теории выбора. Квалификации выпускника высшего учебного заведения по профилю цифровых информационных технологий будет вполне достаточно для ее понимания.

Монография включает шесть глав и заключение. В первой главе представлены результаты анализа автоматизированных систем, применяемых в боевых циклах воинских формирований, и процесса их функционирования в современных боевых действиях и вооруженных конфликтах, а также существующего состояния научно-методического аппарата обеспечения защищенности программного обеспечения этих систем от кибератак противника. Во второй главе изложены модель процесса информационного взаимодействия информационно-технических средств автоматизированных систем по известной процедуре телекоммуникационного протокола и метод генерации кибератак на телекоммуникационное оборудование, используемое в автоматизированных системах воинских формирований. Третья глава посвящена моделированию процессов функционирования компонентов автоматизированных систем воинских формирований. В четвертой главе рассмотрена модель процессов функционирования автоматизированных систем в боевом эпизоде. В пятой главе приведены метод и реализующие его этапы методики оценки эффективности кибератак в боевых действиях. Шестая глава содержит методику киберзащиты автоматизированных систем воинских формирований и предложения по повышению эффективности функционирования этих систем в условиях кибератак противника. В заключении подведены итоги исследования, сделаны выводы по работе и сформулированы дальнейшие направления исследований.

Благодарности. Автор выражает глубокую благодарность рецензентам д.т.н., профессору Анисимову В.Г., д.в.н., доценту Антоновичу П.И., д.т.н., профессору Буравлеву А.И., д.т.н., профессору Гречишникову Е.В., д.т.н., профессору Климову С.М., д.ф.-м.н., доценту Кузнецову А.В. и д.т.н., доценту Макаренко С.И. за ценные замечания, которые способствовали значительному улучшению качества работы, д.т.н., доценту Храмову В.Ю. за то, что заразил любовью к научным исследованиям, и за оригинальные идеи, развитие которых положено в основу исследований автора, д.т.н., доценту Будникову С.А. за то, что зажег пламенный интерес к вопросам информационной безопасности, д.в.н., профессору Донскову Ю.Е. за вдохновение на тернистом пути моделирования боевых действий, а также к.т.н., старшему научному сотруднику Павловичу В.Г. за помощь при подготовке монографии к изданию.

Автор будет рад сотрудничеству в рассматриваемой области исследований. Предложения и конструктивные замечания просьба направлять по адресу: albo@list.ru.

1 Анализ автоматизированных систем, применяемых в боевых циклах воинских формирований, и существующего состояния научно-методического аппарата обеспечения защищенности программного обеспечения этих систем от кибератак

«Если у Вас хватило ума поставить задачу, у Вас должно хватить его и на то, чтобы разрешить ее. По интеллектуальному напряжению эти два процесса приблизительно равны».

Илья Николаевич Шевелёв

1.1 Анализ автоматизированных систем, применяемых в боевых циклах воинских формирований, и процесса функционирования этих систем в современных боевых действиях и вооруженных конфликтах

1.1.1 Особенности современных боевых действий и вооруженных конфликтов. Основные направления развития автоматизированных систем, применяемых в боевых циклах воинских формирований, и угрозы безопасности этим системам

Сегодня боевые действия и вооруженные конфликты характеризуются [40]:

- высоким уровнем интеграции цифровых информационных технологий в образцы вооружения;
- высокими сенсорными возможностями;
- высокой маневренностью;
- большой дальностью действия и точностью средств огневого поражения (ОП);
- применением противоборствующими сторонами широкой номенклатуры средств радиоэлектронной борьбы (РЭБ), средств воздействия на личный состав, а также роботизированных средств, в первую очередь, малогабаритных, которые значительно повышают устойчивость управления воинскими формированиями (ВФ), дальность применения и живучесть элементов боевых порядков (ЭБП).

В таких условиях эффективность применения средств ОП, РЭБ и роботизированных средств во многом зависит от автоматизированных систем (АС) разведки, связи и управления войсками (силами) и оружием (боевыми средствами). АС обеспечивают выполнение боевых циклов ВФ. Вопреки стремлению некоторых специалистов в области военного дела приписать идею боевого цикла американцу Дж. Бойду или кому бы то ни было еще, давая этому процессу новые имена (например, цикл «Красная звезда», OODA-цикл (от англ. *Observe-Orient-Decide-Act* – наблюдение, ориентация, решение, действие), цикл «разведка-поражение»), это понятие не является новым. Боевой цикл является классиче-

ской, известной еще с первобытных времен повторяющейся последовательностью действий по применению любого оружия. Боевой цикл состоит из пяти этапов [175, 272]: сбор информации, ее анализ и осознание, планирование, принятие решения и его исполнение (см. рис. 1). В зависимости от условий боевой обстановки и стоящей задачи боевой цикл может выполняться одним, несколькими ЭБП или ВФ в целом. Настоящая монография посвящена исследованию такого класса АС военного и двойного назначения, который обеспечивает с применением средств вычислительной техники (СВТ) выполнение одного, нескольких или одновременно всех этапов одного или нескольких боевых циклов ВФ.

Рис. 1. Структура боевого цикла

Следует отметить необходимость использования в настоящей монографии термина «боевой цикл», заимствованного из американской научной литературы. Этот термин в известной степени конкурирует с термином «контур управления», под которым понимается замкнутая цепь элементов системы управления, образованная участком прямой и обратной связи, то есть совокупность управляющей и управляемой подсистем [246]. В то же время цикл – это, как известно, повторяющаяся последовательность действий. Несомненно, оба термина рассматривают один и тот же объект. Но термин «контур управления» отражает его структуру, а термин «боевой цикл» отражает процесс применения этой структуры в условиях боевой обстановки.

Гораздо более схож с термином «боевой цикл» термин «алгоритм действий командира». Ведь алгоритм (от лат. *algorithmi*) – это способ (программа) решения задач, точно предписывающий, как и в какой последовательности

получить результат, однозначно определяемый исходными данными [45]. Однако и в этом случае имеет место некоторое важное отличие. Ведь цикл – это алгоритм, который кроме всех свойств, присущих любому алгоритму (дискретность, результативность, массовость, детерминированность, понятность), обладает важным отличительным свойством постоянного повторения. То есть указания только лишь термина «алгоритм» явно недостаточно для отражения свойства непрекращающейся повторяемости этого алгоритма до конца боя.

И, наконец, полными аналогами термина «боевой цикл» являются термины «цикл «разведка-поражение», «цикл управления», «цикл боевого управления», «управленческий цикл», «цикл выполнения боевого задания». Автор сделал окончательный выбор в пользу первого термина ввиду его наибольшей лаконичности. Соответствующее определение приведено в глоссарии монографии.

Интеграция АС привела к появлению систем, классифицируемых НАТО как C6ISR (от англ. *Command*, *Control*, *Communications*, *Computers*, *Cyber-Defense and Combat Systems*, *Intelligence*, *Surveillance*, *Reconnaissance* – командование, контроль, связь, компьютеры, системы киберзащиты и борьбы, разведка, наблюдение, распознавание), способных управлять боевыми действиями, в том числе в киберпространстве. Например, в сухопутных войсках (СВ) США на оперативном уровне к таким системам относится ATCCS (от англ. *Army Tactical Command and Control System* – тактическая система командования и контроля армии), а на тактическом уровне возможности системы FBCB2 (от англ. *Force XXI Battle Command Brigade-and-Bellow* – силы XXI века боевого командования бригады и ниже) активно наращиваются для соответствия этому классу [175]. Аналогичная тенденция есть и в Вооруженных Силах (ВС) Российской Федерации (РФ) (например, система управления войсками оперативного уровня «Акация-М» и Единая система управления тактического звена (ЕСУ ТЗ) «Созвездие-М»).

Результаты анализа показывают, что в США и других странах НАТО основными направлениями развития АС, на которые разумно ориентируется и отечественный оборонно-промышленный комплекс, являются [175]:

- доведение автоматизации до солдата или образца вооружения;
- предоставление полной и точной информации о действиях сторон и состоянии противника в масштабе времени, близком к реальному;
- обеспечение боевого управления силами и средствами в едином информационно-коммуникационном пространстве;
- обеспечение полной осведомленности о текущей боевой обстановке;
- предоставление информации в наиболее удобном для восприятия виде.

При этом основными тенденциями развития АС ВФ являются [175]:

- создание так называемых «цифровых» (от англ. *digitized* – оцифрованный) или «компьютеризированных» ВФ;
- значительное удешевление проектирования и производства оборудования за счет применения технологий двойного назначения, то есть так называемых COTS-технологий (от англ. *Commercial Off-The-Shelf* – коммерческое с полки);
- обеспечение эволюционной модернизации в соответствии с темпами технического прогресса на основе перехода к открытым архитектурам;

- интеграция вычислительных и связных ресурсов разнородных АС в единую инфраструктуру;
- формирование полной и точной единой картины боевой обстановки, подготовки данных, в том числе для поражения высокомобильных целей в режиме реального времени;
- обеспечение широкого доступа к единой картине боевой обстановки;
- поражение главных целей без вхождения в зону боевого соприкосновения по данным распределенной в боевом пространстве сети информационных датчиков и космических систем.

Внедрение в АС последних достижений цифровых информационных технологий (далее этот процесс называется информатизацией), в том числе программно-определяемого (конфигурируемого) радио, искусственного интеллекта, «больших данных», позволило вывести боевые возможности ВФ на качественно новый уровень. При этом в АС почти стерлась грань между СВТ и радиоэлектронными средствами (РЭС). Отсутствие четкой грани привело автора к необходимости использовать термин «информационно-техническое средство» (ИТС) [16]. Этот термин собирательный. Он обозначает любые РЭС, СВТ, а также их конструктивно единую комбинацию друг с другом или со средствами электронной автоматики, которые управляют техническими средствами других классов, называемых в этой работе устройствами (например, автоматическое оружие, механический привод антенны, двигатель). Сущность понятия ИТС показана на рис. 2.

Рис. 2. Сущность понятия «информационно-техническое средство»

ИТС выполняют в АС ВФ три класса задач: информационно-расчетные задачи (ИРЗ), задачи управления устройствами (ЗУ), а также задачи разведки, связи, РЭБ и навигационно-временного обеспечения, которые в монографии обобщенно называются задачами обеспечения (ЗО). ИТС включает в свой состав технический компонент (ТК), включающий электронную компонентную базу и другие технические устройства, и программное обеспечение (ПО), которое, в свою очередь, согласно ГОСТу [84] делится на общее (ОПО) и специальное (СПО).

Информатизация привела к значительному усложнению ПО ИТС. Из мировой практики разработки ПО широко известна закономерность: чем сложнее программа, тем больше в ней ошибок [132]. Многообразные, многопоточные и вариативные программы ИТС современных АС ВФ не являются исключением. Результаты обобщения ряда исследований (например, [14, 44, 94, 115]) дали возможность выделить три класса причин уязвимостей ПО АС, не позволяющих считать эти системы абсолютно безопасными: конструктивные, технологические и эксплуатационные. Основные из этих причин показаны на рис. 3. Конструктивные причины уязвимостей устраняются в основном в процессе разработки АС, а технологические и эксплуатационные причины устранить крайне сложно. Поэтому если в XX веке основными угрозами функционирования АС считались уничтожение или захват противником, радиоэлектронные помехи средствам радиосвязи, реализуемые на физическом уровне эталонной модели взаимодействия открытых систем (ЭМВОС) [100], ошибки операторов, сбои и отказы устройств, то сегодня к ним добавились кибератаки (КА) противника, эксплуатирующие уязвимости ПО, обусловленные технологическими и эксплуатационными причинами.

В данном контексте следует отметить, что, несомненно, информационное обеспечение АС может иметь уникальные уязвимости. Однако в настоящей монографии оно рассматривается в той мере, в которой используется или реализовано в ПО, то есть доступно легитимному пользователю АС или противнику.

Согласно [88, 231] КА – это целенаправленное воздействие программными и/или программно-аппаратными средствами на АС в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой такими системами информации. В известной литературе процесс реализации КА называется радиоэлектронно-информационным, программно-математическим, программно-техническим, программно-аппаратным, просто программным воздействием, поражением специальными программными средствами (СПС) и т.п. (см., например, [24, 65, 101, 116, 167]). КА используют уязвимости (то есть недостатки, слабости) ПО или АС в целом.

Средства реализации КА нарушают и искажают логику, алгоритмы работы ПО и информацию АС на канальном и вышестоящих уровнях ЭМВОС, используя нижний физический уровень только в качестве среды доставки последовательностей символов, содержащихся в характеристиках радиоволн (преимущественно используемых в тактическом звене), тока в проводных каналах связи и электромагнитных волн оптического и инфракрасного диапазонов в оптоволокне. Эти символы согласно алгоритмам, строго регламентируемым стандартами телекоммуникационных протоколов, преобразуются в целевом ИТС АС в последовательности бит, воспринимаемых как данные (декларативная программная помеха) или как программа (процедурная программная помеха) [60]. Эти последовательности бит называются СПС. Выполнение таких программных средств не предусмотрено штатным режимом работы АС. В то же время другие виды средств информационно-технического воздействия (ИТВ), то есть радиоэлектронного подавления (РЭП) и воздействия мощным электромагнитным излучением (ЭМИ) (имеется ввиду «радиочастотное оружие», поражение электромагнитным излучением и т.д.) воздействуют только на физическом уровне ЭМВОС (см. рис. 4).

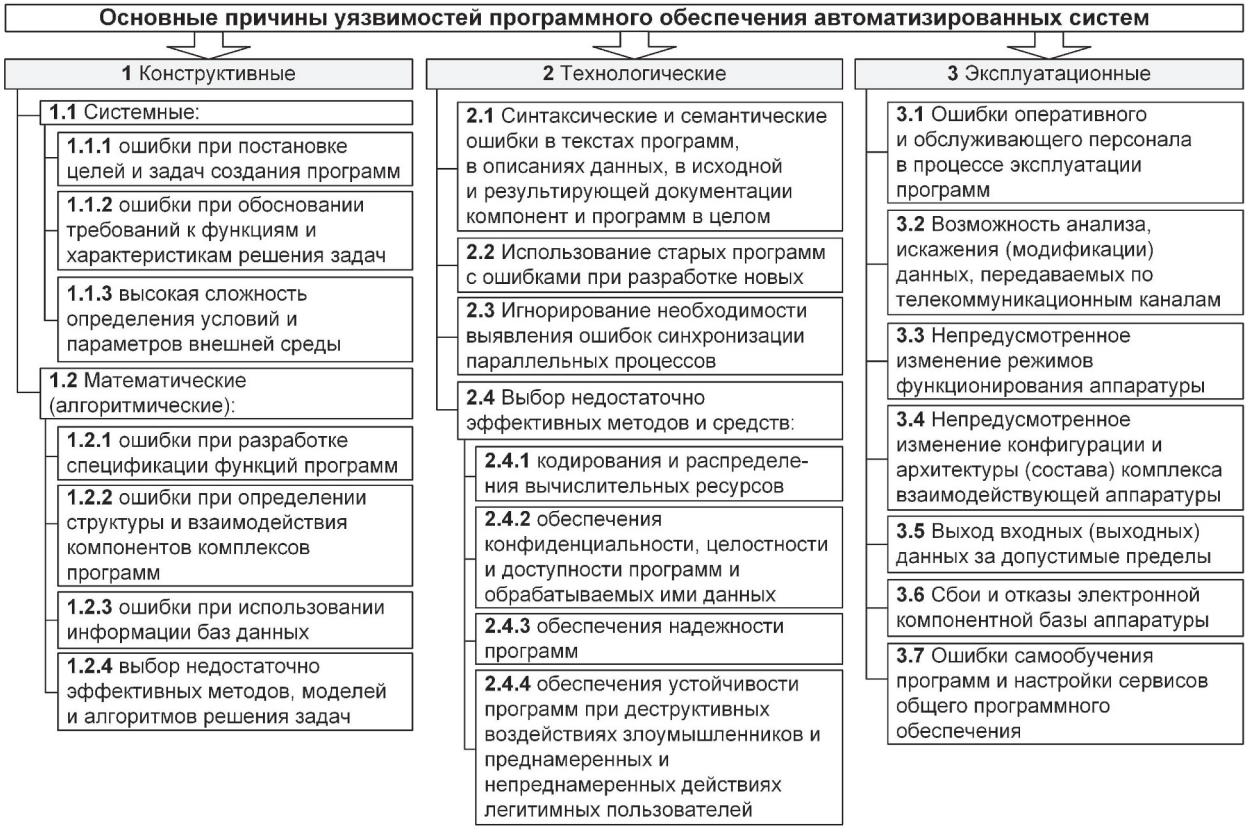


Рис. 3. Основные причины уязвимостей программного обеспечения

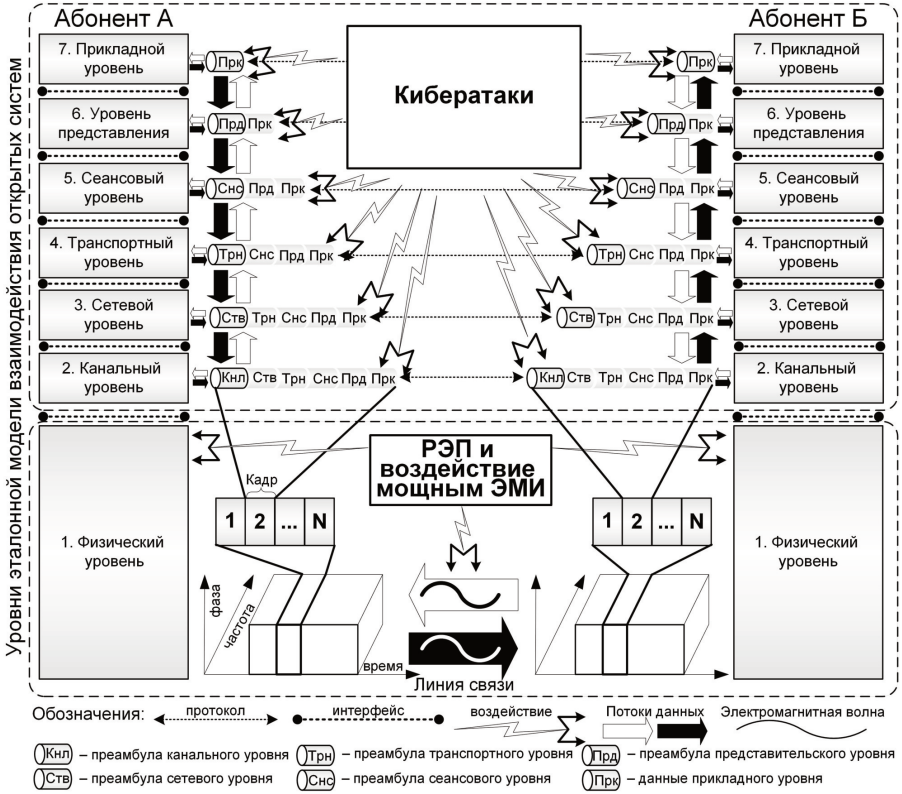


Рис. 4. Виды информационно-технических воздействий
с позиции эталонной модели взаимодействия открытых систем

Иными словами, в отличие от РЭП и воздействия мощным ЭМИ, которые нацелены на радиоприемный тракт ИТС, цель КА состоит в том, чтобы манипулировать данными, содержащими информацию, используемую целевым объектом, после аналого-цифрового преобразования принятой электромагнитной волны (принятых импульсов электрического тока) и устранения в этих данных избыточности, нужной для обеспечения устойчивости в условиях помех, создаваемых средствами РЭП и воздействия мощным ЭМИ. То есть КА не воздействуют на модем (модулятор-демодулятор) в классическом понимании этого термина. Именно в этом состоит ключевое отличие КА от активных имитирующих помех. КА формируют условия для проявления уязвимостей в ПО АС и одновременно являются деструктивным фактором.

Следует пояснить, что в монографии для определения совокупности процессов РЭП, воздействия мощным ЭМИ и КА не используется классический для РЭБ термин «радиоэлектронное поражение». Вместо него используется термин «информационно-техническое воздействие» по следующим причинам.

Во-первых, указанные воздействия являются не только радиоэлектронными. Ведь оптико-электронное подавление (ОЭП), гидроакустическое и акустическое подавление в *радио*электронной борьбе не осуществляются в диапазоне *радио*волн. Здесь уместно напомнить, что радиоэлектроника – это собирательное название ряда областей науки и техники, связанных с передачей и преобразованием информации на основе использования *радио*частотных электромагнитных колебаний и волн; основные из них – *радио*техника *и* электроника [45]. В то же время *радио*техника – это наука об электромагнитных колебаниях и волнах *радио*диапазона (от 0,03 Гц до 3 ТГц), методах их генерации, усиления, излучения, приема.

Во-вторых, широко известно, что поражение – это воздействие на объект, нарушающее его работоспособное состояние, которое может быть восстановлено только после проведения ремонта. Здесь ключевое значение имеет слово «ремонт» (от франц. *remonte* – поправить, пополнить, снова собрать). В то же время результатом РЭП является не пораженное, а подавленное состояние объекта воздействия. Подавление – это воздействие на объект, нарушающее его работоспособное состояние, которое восстанавливается без проведения ремонта после завершения воздействия или в процессе воздействия в результате применения мер помехозащиты. Аналогично результатом воздействия мощным ЭМИ не обязательно является поражение элементов электронной компонентной базы. При таком воздействии может иметь место и подавление. Именно по этой причине в настоящей монографии вместо термина «поражение электромагнитным излучением» используется термин «воздействие мощным ЭМИ». Качественная характеристика «мощное» поясняет потенциальную способность такого ЭМИ при определенных условиях перевести объект воздействия в пораженное состояние.

Учитывая указанные причины использования в монографии терминологии, несколько отличающейся от общепринятой, внимательный читатель заметит, что даже сам термин «радиоэлектронная борьба» по своей сути уже давно «разросся» до термина «информационно-техническая борьба». Конечно же в военной сфере архаизмы нередки. Например, в СВ США в легких, тяжелых бригадах и бригадах «Страйкер» до сих пор существуют «кавалерийские эскадроны» (от англ. *cavalry squadron*), хотя кони в их организационно-штатной структуре не используются [279]. Но все же, как известно, терминология – это важная часть науки, от которой во многом зависит успешность ее развития и практического применения. Тем не менее, поскольку фундаментальное совершенствование терминологии не является целью настоящей монографии, этот термин, основополагающий для столь важной в современной военной науке области, используется в ней в неизмененном виде.

Основными точками входа для КА в боевых условиях являются интерфейсы ИТС, отвечающие за процессы информационного взаимодействия. Объект КА – это любой образец АС (система таких образцов), в котором присутствует канал обмена данными с внешними субъектами. Как уже отмечено выше, на физическом уровне ЭМВОС КА представляет собой активную имитирующую помеху. Однако характеристика КА не исчерпывается классической способностью таких помех блокировать работу РЭС сетей радиосвязи на физическом уровне ЭМВОС или изменять ложными радиосигналами поведение АС, использующих

РЭС локации и/или навигационно-временного обеспечения. Применение на канальном и вышестоящих уровнях ЭМВОС дополнительно придает КА следующие свойства, позволяющие рассматривать их в качестве самостоятельного вида помех функционированию АС – **программных помех** [28]:

1) *поражающая способность* – КА способны не только подавлять, но и поражать ИТС АС. То есть после завершения КА для восстановления работоспособности ИТС АС может потребоваться ремонт (в зависимости от функций СПС);
2) *транслируемость* – КА воздействуют не только на цифровые РЭС радиосвязи, но и на СВТ, использующие РЭС в качестве модема;
3) *авторегенерируемость* – КА способны обеспечивать многократное нарушение штатного режима функционирования целевых ИТС даже после завершения процесса боевого применения техники КА за счет того, что СПС могут оставаться в программной среде целевого ИТС и самомодифицироваться;
4) *прозрачность* – КА имеют возможность за счет наличия обратной связи с целевыми ИТС обеспечивать достоверный контроль своей эффективности, получая от целей ответные сообщения, которые могут содержать сведения о местоположении ИТС, данные с их машинных носителей информации, а также сведения о сетевой структуре АС, в рамках которой работают целевые ИТС;
5) *транзитивность* – КА на отдельный элемент информационно-управляющей сети может вывести из строя другие ее элементы, сегменты АС или даже всю сеть в целом;
6) *телеоперационность* – КА на одно ИТС, подключенное к единому информационному пространству, состоящему из множества локальных информационно-управляющих сетей, может нарушить или исказить логику и алгоритмы функционирования любого ИТС в этом пространстве;
7) *низкая энергоемкость* – КА по каналам цифровой радиосвязи могут не требовать превышения уровня помехового сигнала над полезным, являясь эффективными даже при приеме сигнала с СПС на уровне чувствительности радиоприемника, что значительно повышает живучесть техники реализации КА в сравнении с традиционной («силовой») техникой РЭП;
8) *высокая избирательность* – КА воздействуют на заданные ИТС без ухудшения качества функционирования других аналогичных средств.

Таксономия киберзащиты весьма развита. В ГОСТ [94] приводится подробная классификация уязвимостей, актуальных и для АС ВФ. Федеральная служба по техническому и экспортному контролю (ФСТЭК) России постоянно пополняет перечень угроз безопасности информации и уязвимостей, часть которых эксплуатируются в КА [17]. Известны и другие отечественные и зарубежные базы данных с уязвимостями. Классификаций способов реализации КА известно множество (см., например, [116, 137, 173]), но ни одна из них не является общепринятой. Анализ работ в этой области позволил выделить ряд общих классификационных признаков способов реализации КА, которые представлены в таблице 1.

Таблица 1 — Классификационные признаки способов реализации кибератак

Признак	Характеристика	Описание
1 По характеру воздействия	1.1 Пассивное	Реализует цели КА без изменения обрабатываемых в целевом ИТС данных.
	1.2 Активное	Реализует цели КА путем изменения обрабатываемых в целевом ИТС данных.
2 По ожидаемому эффекту	2.1 Диверсионное	Приводит к изменению алгоритмов обработки данных в подсистеме обработки данных и в подсистеме управления целевого ИТС в соответствии с целями противника.
	2.2 Дезинформирующее	Приводит к извлечению подсистемой обработки данных целевого ИТС из принимаемых сигналов ложных данных, содержание которых определяется противником.
	2.3 Подавляющее	Приводит к разрушению полезных данных до их поступления в целевое ИТС.
3 По цели воздействия на информацию	3.1 Конфиденциальность	Приводит к перехвату и расшифровке информации, обрабатываемой целевым ИТС.
	3.2 Целостность	Приводит к искажению информации, обрабатываемой целевым ИТС.
	3.3 Доступность	Приводит к отказу в доступе к обрабатываемой целевым ИТС информации.
4 По условию начала воздействия	4.1 После запроса от ИТС	Условие начала – передача от целевого ИТС запроса определенного типа.
	4.2 После события в ИТС	Условие начала – возникновение определенного (ожидаемого) события в целевом ИТС.
	4.3 Безусловное	Условие начала – безотносительно к состоянию целевого ИТС.
5 По наличию обратной связи	5.1 С обратной связью	Воздействие, предполагающее получение ответов от целевого элемента ИТС.
	5.2 Без обратной связи	Воздействие, осуществляемое без реакции на поведение ИТС.
6 По месту применения	6.1 В глобальной сети	Воздействие из любой точки земной поверхности, в которой есть доступ к целевому ИТС.
	6.2 В тактическом районе	Воздействие на целевой ИТС в тактическом районе.
7 По уровню ЭМВОС	7.1 На канальном уровне	Воздействие на уровне звена сигнализации, выполняющего задачи по контролю, адресации и безошибочной передаче сообщений в рамках одной среды передачи данных.
	7.2 На сетевом уровне	Воздействие на уровне определения маршрута сообщений (пакетов) и логической адресации между различными сетями с различными средами передачи данных.
	7.3 На транспортном уровне	Воздействие на уровне установления прямой связи между конечными пунктами маршрута и обеспечения надежности этой связи.
	7.4 На сеансовом уровне	Воздействие на уровне организации сеансов связи между абонентами.
	7.5 На представительном уровне	Воздействие на уровне, преобразующем информацию из вида, удобного для приложений, в вид, удобный для передачи по каналам сигнализации.
	7.6 На прикладном уровне	Воздействие на уровне, обеспечивающем доступ к сети прикладных процессов абонентов.
8 По источнику воздействия	8.1 Одиночное	Воздействие, проводимое от одного источника и строящееся по схеме 1:1 или 1:М.
	8.2 Распределенное	Воздействие, проводимое одновременно несколькими источниками по схеме М:М или М:1.
9 По времени	9.1 Краткосрочное	Воздействие, время проведения которого не превышает одного цикла работы целевого ИТС.
	9.2 Долгосрочное	Воздействие, время проведения которого превышает один цикл работы целевого ИТС.

В боевых условиях типовыми целевыми объектами для КА являются телекоммуникационное оборудование, вычислительные компоненты АС ВФ, дистанционно управляемые образцы вооружения, системы навигационно-временного обеспечения, средства реализации КА противника и его системы противодействия КА, информационные системы, базы и банки данных, используемые для обеспечения боевых действий, системы радиочастотной идентификации и системы опознавания типа «замок-ключ». Перечень целевых объектов постоянно пополняется по мере внедрения цифровых информационных технологий в военное дело.

В ведущих странах разработка средств реализации КА, очевидно, является одним из приоритетных направлений развития образцов вооружения. Возможности по КА на АС противостоящей стороны конфликта есть, например, у кибернетического командования и подразделений разведки и РЭБ США, других стран НАТО и Китая [175, 272]. Ведь общеизвестно, что в области цифровых информационных технологий научно-технический потенциал ведущих стран мира весьма высок. Примером тому, как уже отмечено во введении к настоящей монографии, является многодоменная оперативная группа сухопутных войск США (англ. *Multi-Domain Task Force*, MDTF), в состав которой входит батальон разведки, информации, РЭБ, кибер- и космических операций (англ. *Intelligence*, *Information*, *Cyber/Electronic Warfare & Space*, I2CEWS) [189].

Сведения о названиях и возможностях средств реализации КА в открытых источниках отсутствуют. Тем не менее такие средства во всем мире применяются уже более 30 лет. Первым в истории (из доступных для научной общественности) примером применения КА в бою, доказавшим их высокую эффективность, стал начальный этап наступательной операции коалиции многонациональных сил «Буря в пустыне» в Ираке в январе 1991 г., когда СПС «AF/91», внедренное агентурным методом на этапе подготовки операции в оргтехнику информационно-управляющей сети иракской системы противовоздушной обороны (ПВО), частично парализовало ее работу [116]. Другим типовым примером являются перехваты управления боевыми беспилотными летательными аппаратами (БПЛА). О таких перехватах, например, БПЛА RQ-170 Sentinel (рус. *дозорный*) над Ираном в 2011, 2012 гг., ScanEagle (рус. *сканирующий орел*), MQ-9 Reaper (рус. *жнец*) над Сирией и Ираком в 2019 г., известно из официальных средств массовой информации [13, 298]. И это, по всей видимости, только «вершина айсберга». Ведь, как отмечено выше, информация о средствах реализации КА и результатах их применения тщательно скрывается.

Эффективные способы реализации КА имеют высокий уровень конфиденциальности, а производители АС ВФ даже после выявления уязвимостей скрывают их ввиду критической важности такой информации. Мировой опыт поиска уязвимостей показывает, что даже если уязвимости сложной системы неизвестны, то это означает, что они просто еще не найдены.

Таким образом, результаты проведенного анализа свидетельствуют о том, что в долгосрочной перспективе КА на АС ВФ будут весьма актуальными.

1.1.2 Актуальность повышения эффективности функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований, в условиях кибератак

Во многом процесс обеспечения защищенности ПО АС ВФ от КА (в монографии этот процесс, как уже отмечено выше, называется киберзащитой) должен иметь упреждающий характер. Соответствующие требования должны указываться в тактико-технических заданиях на опытно-конструкторские работы по созданию (модернизации) АС и обеспечиваться в процессе выполнения этих работ. Однако сегодня этому препятствуют следующие обстоятельства.

Во-первых, современные нормативно-технические документы (НТД) в области защиты информации (например, ГОСТы [85, 89, 91, 92, 95]) предусматривают широкий спектр организационных, технических и программных мер по предотвращению ошибочных и преднамеренных несанкционированных действий пользователей с АС и защите от известных способов реализации КА. Но сегодня уделяется недостаточно внимания защите АС от КА по каналам цифровой радиосвязи. Это обусловлено следующим.

Сложность обеспечения защиты ПО от КА по каналам цифровой радиосвязи состоит в том, что в этих каналах используется случайный доступ заранее неизвестного множества абонентов. Поэтому в них процедуры канального уровня ЭМВОС, предшествующие идентификации и аутентификации, могут инициироваться противником. Доля таких каналов в активных периодах боевых действий, как следует из анализа организационно-штатных структур бригад СВ США [279], составляет около 90…95 %. Поэтому взаимодополняющими факторами высокой эффективности применения КА в современных высокоманевренных боевых условиях являются принципиальная невозможность организации полноценной энергетической и физической защиты каналов передачи данных и АС от несанкционированного (в первую очередь, удаленного) доступа и знание уязвимостей ПО.

Во-вторых, уязвимости во многом должны устраняться на этапе разработки АС, что должно контролироваться в процессе их испытаний. Но на практике ПО таких систем является очень сложным. Например, в ПО американской Боевой системы будущего (англ. *Future Combat System*), являющейся аналогом отечественной ЕСУ ТЗ «Созвездие-М», 63 млн строк программного кода, в ПО самолета F-35 24 млн строк, в ПО самолета F-22 Raptor (рус. *хищник*) 1,7 млн строк, а ядро операционной системы Linux версии 2.6 содержит 5,7 млн строк кода [284]. Даже если программы АС ВФ соизмеримы, например, с тремя-четырьмя взаимодействующими между собой средними приложениями для iPhone (по 40 тыс. строк [284]), то полноценно исследовать на испытаниях и такой объем программного кода согласно требованиям ГОСТов [87, 89, 90] невозможно. Ошибки в ПО проявляются, например, при обращении некоторой управляющей программы к функции динамической библиотеки, уже содержащей ошибку. Как следствие, при выполнении этой функции в ходе КА возможен отказ в работе одной, нескольких или всех программ, от нее зависимых. Поэтому не выявленные

на этапе создания (модернизации) ошибки в ПО АС, принятых на снабжение или вооружение, могут приводить к срывам выполнения боевых задач.

По этой причине оценка защищенности ПО АС от КА на испытаниях сегодня состоит только в применении известных способов реализации КА и проверке наличия в составе АС сертифицированной подсистемы защиты информации (ПЗИ), функции которой соответствуют категории объекта информатизации, а реализуемые в ПЗИ известные адаптивные, ситуационные и рефлексивные методы обеспечения защиты АС от КА, регламентируемые, например, ГОСТами [98, 99], ориентированы в основном на известный перечень способов КА и малопригодны для новых, еще неизвестных ПЗИ ИТС способов КА, которые, несомненно, должны приберегаться противником для решающих моментов боевых действий. Существующие подходы, ориентированные на неизвестные способы реализации КА, представляют эти способы абстрактно в качестве «потенциальных угроз», что позволяет оперировать только имеющимися фрагментарными знаниями об изученных эффектах применения КА в боевых условиях. Однако темпы получения таких знаний на сегодняшний день значительно отстают от темпов информатизации и развития практики применения КА. Для парирования этого отставания защиту АС от КА необходимо рассматривать не с позиции устранения «потенциальных угроз», а с позиции разработки и эксплуатации при создании этих систем новых действительных способов реализации КА, использующих уязвимости в конкретных образцах ПО. То есть способов, в наибольшей степени соответствующих тем способам, которые потенциально способен применять противник в реальных боевых условиях.

В-третьих, известные подходы к созданию безопасного ПО не позволяют разрабатывать необходимое и достаточное множество тестовых способов реализации КА [27]. Это обусловлено следующими причинами.

1. Подход к синтезу активных имитирующих помех [224], который широко применяется для разработки способов РЭП, оперирует статистическими характеристиками частотных, амплитудных, фазовых, пространственных и временных параметров помеховых и полезных сигналов на физическом уровне ЭМВОС. Для разработки тестовых способов реализации КА такой подход не применим, поскольку на канальном и вышестоящих уровнях ЭМВОС, где применяются КА, значение имеют не усредненные статистические характеристики сигналов, а параметры точности содержания (синтаксические и семантические), кратности отправки и своевременности доставки конкретных разнотипных сообщений, регламентируемых телекоммуникационными протоколами и применяющихся в различном сочетании в разных процедурах этих протоколов.

2. Сегодня во всем мире активно применяются средства тестирования программных реализаций телекоммуникационных протоколов. К примерам наиболее развитых коммерческих средств тестирования телекоммуникационного оборудования на канальном и вышестоящих уровнях ЭМВОС следует отнести: «MaxPatrol» российской компании «Positive Technologies; «Сканер-ВС» российской компании «Эшелон»;

«RedCheck» российской компании «Алтекс-софт»; «Test Advisor» американской компании «Synopsys»; «Metasploit Framework» американской компании «Rapid7»; «Nessus» американской компании «Tenable Network Security»; «Drozer» финской компании «MWR Infosecurity» («F-Secure»); «Canvas» канадской компании «Immunity»; «Core Impact» американской компании «Core Security»; «CMW500» немецкой компании «Rohde&Schwarz». Несмотря на высокий уровень практичности известных средств, их критическими недостатками являются:

- невозможность учета своевременности доставки сообщений в тестовых способах реализации КА. Используется только выборочное тестирование неправильными, неожиданными или случайными данными (так называемый «фаззинг», от англ. *fuzzing* – размывание, затуманивание);
- невозможность разработки новых и редактирования существующих моделей для синтеза тестовых способов реализации КА. Модели телекоммуникационных протоколов разрабатывает только производитель средства тестирования.

Кроме того, известен широкий спектр академических проектов, к которым, в первую очередь, следует отнести проекты «UniTESK» и «BLAST» от Института системного программирования (ИСП) Российской академии наук (РАН), «Java Pathfinder» от NASA (США), «TLA+» от «Microsoft» (США), «Spin» от Bell Labs» (США), «Uppaal» от университетов Уппсалы (Швеция) и Ольборга (Дания). Область применимости, ограничения и особенности методов, применяемых в этих и аналогичных проектах, не позволяющие им полноценно выйти на коммерческий уровень и составить конкуренцию вышеуказанным средствам тестирования телекоммуникационных протоколов, приведены далее в параграфе 1.2.

В-четвертых, известные средства моделирования боевых действий (например, расчетно-моделирующий комплекс (РМК) СВ ВС РФ [82], изделие «Спектр» компании «РусБИТех» (г. Москва) [221]) не учитывают влияние КА на временные и вероятностные характеристики процессов разведки, связи, управления, ИТВ и ОП, взаимосвязанных в рамках боевых циклов ВФ. Это не позволяет количественно определять меру ущерба, который наносят КА данным процессам.

Таким образом, изложенные обстоятельства свидетельствуют об актуальном противоречии между потребностью в выявлении и устранении уязвимостей ПО АС, применяемых в боевых циклах ВФ, в процессе их создания (модернизации) и ограниченными возможностями существующих средств обеспечения защищенности ПО таких систем от КА противника.

1.2 Анализ существующего состояния научно-методического аппарата обеспечения защищенности программного обеспечения автоматизированных систем, применяемых в боевых циклах воинских формирований, от кибератак противника

1.2.1 Анализ сферы проектирования информационно-телекоммуникационных систем

Для разрешения вышеуказанного противоречия согласно основным принципам системного анализа [163, 229] процесс функционирования АС, применяемых в боевых циклах ВФ, в условиях КА противника следует рассматривать в двух аспектах:

- **во-первых**, как систему процессов функционирования отдельных ИТС, информационное взаимодействие которых осуществляется по телекоммуникационным протоколам. Вероятностно-временные характеристики этих процессов должны учитывать состояния конфликта средств реализации КА и ПЗИ ИТС, а в рамках КА должна рассматриваться эксплуатация не только известных, но и новых уязвимостей, выявленных в процессе создания (модернизации) АС на основе анализа телекоммуникационных протоколов ИТС, входящих в их состав;
- **во-вторых**, как неотъемлемый компонент боя противостоящих ВФ, в котором применяется наиболее полный перечень известных воздействий, включая КА.

Такому взгляду препятствует недостаточная разработанность трех последовательно пересекающихся научных сфер: проектирования информационно-телекоммуникационных систем, исследования информационного конфликта и исследования боевых действий. Эти сферы показаны в виде диаграммы Эйлера на рис. 5. Область исследования киберзащиты АС ВФ, которая рассматривается в монографии (**область *A***), объединяет пять отдельных областей в этих сферах.

Сфера проектирования информационно-телекоммуникационных систем, в которой в качестве самостоятельного направления с 60-х годов XX века развивается тематика проектирования телекоммуникационных протоколов. Она базируется в основном на применении теоретико-множественного подхода, математического аппарата марковских процессов и теории автоматов (см., например, работы В.М. Вишневского [70, 69], Ж. Теля [321]). С 70-х годов прошлого века по мере увеличения компьютерных сетей увеличивалось и количество желающих наносить вред их пользователям. Это привело к появлению протоколов сетевой безопасности и пересечению тем самым сферы проектирования информационно-телекоммуникационных систем (**I**) со сферой исследования информационного конфликта (**II**). В результате появилась область исследования безопасности телекоммуникационных протоколов (**область *B***).

В **области *B*** сформировались два направления. Первое образовали разработчики протоколов, а второе – злоумышленники и коммерческие организации, предоставляющие услуги по защите информации.

Рис. 5. Области научных направлений по тематике исследования

***B*$_1$. Направление защиты протоколов**. Суть процесса защиты состоит в верификации протоколов, то есть в доказательстве того, что программная (программно-техническая) реализация протокола [132, 155]:

- удовлетворяет сформулированным требованиям, спецификациям и стандартам;
- реализована без непредусмотренных функций;
- имеет надежные криптографические примитивы;
- является стойкой к атакам в предположении надежности криптографических примитивов.

То есть верификация не требует доказательства того, что в протоколе нет уязвимостей, а фактически служит средством оправдания разработчика перед заказчиком и потребителем в случае получения ими ущерба вследствие КА. На сегодняшний день для верификации применяются восемь основных методов.

***B*$_{1,1}$ – метод выборочного тестирования** (англ. *fuzzing*). Основан на работах В.В. Липаева [168], Б. Бейзера [20], С. Канера [131], G.J. Myers [310] и др. Базируется на разработке возможных тестовых воздействий (способов реализации КА), использующих неправильные, неожиданные или случайные входные данные, сформированные по установленным правилам в целях обнаружения ошибок в реализации ИТС. Этот метод применялся с момента зарождения отрасли разработки ПО и базируется на применении теории графов и теории автоматов. Сегодня он активно развивается научными школами В.П. Иванникова [57-59, 195] в ИСП РАН, Н.В. Евтушенко [102, 103, 254], В.Т. Еременко [121, 122] и др. Этот метод достаточно глубоко проработан для алгоритмов функционирования ИТС с одним или несколькими потоками управления, а также для случая синхронного информационного взаимодействия нескольких пространственно распределенных ИТС. Поддержку синхронизации обеспечивает математический аппарат теории автоматов. Однако в случае асинхронного информационного взаимодействия ИТС известные результаты, как показано в [58], позволяют рассматривать каждый компонент композиции взаимодействующих автоматов по отдельности, не учитывая временные параметры передачи сообщений между компонентами в рамках единого распределенного процесса, регламентируемого телекоммуникационным протоколом.

***B*$_{1,2}$ – метод аксиоматического доказательства корректности реализации протокола (дедуктивный анализ)** [160, 258]. Достоинством этого метода является то, что он дает возможность работы с бесконечными пространствами состояний, а также позволяет глубоко понять систему. Но он очень трудоемок, требует высокого уровня квалификации и не позволяет построить полную систему аксиом и правил вывода из-за того, что использует исчисление предикатов первого порядка (см. теорему Геделя о неполноте [229]). Поэтому данный метод применим в основном при верификации отдельных свойств телекоммуникационных протоколов сетевой безопасности и авионики. Переход на исчисление предикатов высшего порядка привел к появлению **метода *B*$_{1,3}$**.

***B*$_{1,3}$ – метод проверки модели** (англ. *model checking*) [132, 282] (см. рис. 6). Состоит в представлении процесса функционирования ИТС в виде дискретно-событийной модели (структуры Крипке), представлении каждого требо-

вания к этому процессу в виде формулы темпоральной (временной) логики (*Linear Temporal Logic*, *Computational Tree Logic* и др.), преобразовании структуры Крипке и формулы темпоральной логики в автомат Бюхи, выполнении операции синхронной композиции этих двух автоматов и попытке доказательства того, что полученное в результате такой композиции подмножество нештатных состояний ИТС не является пустым. Если это подмножество непустое, то *эмпирически* предлагаются тестовые способы реализации КА, переводящие ИТС в нештатные состояния. В противном случае считается, что верификация требования выполнена успешно. Достоинством метода является то, что он гипотетически позволяет сформировать полное множество способов реализации КА для заданной модели системы и спецификации ее свойств и имеет развитую инструментальную поддержку (например, «Java Pathfinder» от NASA, «BLAST» от ИСП РАН, «TLA+» от Microsoft и академические проекты «Spin», «Uppaal»).

Рис. 6. Схема реализации метода проверки модели

Однако данный метод имеет следующие ключевые недостатки:

- его применение связано со сложностью определения состояний и формализации требований. Данные действия осуществляются эмпирически. Однако даже квалифицированный аналитик при работе с некоторым элементом алгоритма функционирования ИТС способен пропустить целый класс состояний или важное требование

к корректности этого элемента. Ведь число состояний системы, в которой параллельно выполняются несколько процессов, зависит от числа ее компонентов экспоненциально. Это приводит к известной в системном анализе проблеме «взрыва пространства состояний». По этой причине проверка на модели не гарантирует разработку необходимого и достаточного множества способов реализации КА;

- проверяется не реальная система, а ее абстрактная модель, которая может быть недостаточно адекватна исследуемым процессам;
- язык спецификации свойств системы может быть неполным [155];
- требует очень высокой квалификации исследователя.

Сочетание **методов** $B_{1,1}$ и $B_{1,3}$ в рамках единого **комбинированного метода** $B_{1,4}$ позволило исключить ряд недостатков методов-прототипов. Например, комбинированный метод используется в технологии UniTESK (англ. *Unified TEsting & Specification tool Kit* – унифицированный инструментарий тестирования и спецификаций) [104, 164], предложенной в ИСП РАН (см. рис. 7). Несмотря на значительные успехи применения этой технологии для верификации широко распространенных протоколов сетевой безопасности (например, TLS, IPsec v2) и развитую инструментальную поддержку (например, средства «CTESK» и «JavaTESK»), комбинированный метод не позволяет парировать еще большую сложность, требующую высокой квалификации, а также ключевой недостаток **метода** $B_{1,3}$, связанный с проблемой «взрыва пространства состояний». Также этот метод характеризуется высокой стоимостью применения, поскольку затраты на его внедрение и создание математической модели ПО или ИТС соизмеримы с затратами на их разработку без модели. При этом в смете расходов на разработку АС сегодня практически невозможно обосновать непредусмотренные действующими НТД затраты на получение высокого качества реализации ПО. Последнее способствовало трансформации **метода** $B_{1,4}$ в $B_{1,5}$.

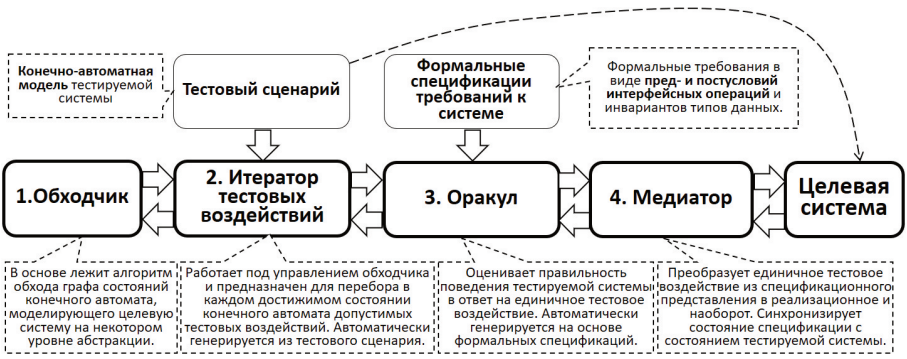


Рис. 7. Схема реализации технологии UniTESK

$B_{1,5}$ **– метод разработки ПО на основе модели** (англ. *model-driven development*), базирующийся на таком стиле разработки, когда итерационно создается математическая модель разрабатываемого объекта, на основе этой модели автоматически генерируются программный код и тестовые воздействия для

проверки корректности кода [104, 164, 258]. То есть это синтетический метод. Он объединяет концепцию разработки на базе моделей и все вышеуказанные методы. Этот метод ориентирован на цифровые устройства, не взаимодействующие с мобильными пространственно распределенными объектами внешней среды с использованием цифровых сообщений. На сегодняшний день он активно применяется во всем мире для исследования контроллеров автомобильной техники, авионики и имеет развитую инструментальную поддержку (например, средства «Abstract State Machine Language» и «Spec Explorer» компании «Microsoft», средства «T-VEC», «Stateflow» и «Simulink» компании «MathWorks», средство «Rational Sofrware Architect» компании «IBM»). Достоинствами метода являются значительная теоретическая проработка и относительно высокая скорость получения результата. Однако его недостатки – это низкая активность компаний-разработчиков ПО в обеспечении совместимости (интероперабельности) моделей согласно международным стандартам, а также указанные выше недостатки **метода** $B_{1,4}$ в случае исследования цифровых устройств, которые взаимодействуют с мобильными объектами внешней среды.

$B_{1,6}$ **– метод статического анализа**. Используется для поиска часто встречающихся ошибок по шаблонам [191]. Такой анализ хорошо автоматизируется. Однако основными недостатками этого метода являются:

- использование строгих базисных методов анализа, не допускающих пропуска ошибок, но приводящих к большому количеству сообщений о возможных ошибках, которые таковыми не являются;
- невозможность обеспечить полноту множества шаблонов.

$B_{1,7}$ **– метод имитационного моделирования** (в том числе аналитико-имитационного) [229]. Состоит в разработке стохастической модели процессов функционирования каждого элемента исследуемой системы согласно заданному телекоммуникационному протоколу, в многократном воспроизведении процессов информационного взаимодействия этих элементов с различной (удобной для исследователя) скоростью и в обработке полученных статистических данных. Традиционным способом формализации процессов функционирования (в том числе информационного взаимодействия) ИТС в данном методе являются различные вариации сетей Петри. Достоинством этого метода является возможность детально учесть логические и временные условия указанных процессов, а недостатком – невозможность получения решения в общем виде и, как следствие, существенная трудоемкость определения первичной причины уязвимости.

$B_{1,8}$ **– метод экспертизы** [191]. В качестве видов экспертиз выделяют организационные, технические экспертизы, сквозной контроль, инспекции и проверки. Экспертиза применима к любым свойствам ПО, позволяет выявить любые виды ошибок, но не может быть автоматизирована и требует участия экспертов. Эффективность экспертиз по количеству обнаруживаемых ошибок и затрачиваемым ресурсам выше, чем эффективность других методов верификации. Но продолжительность этого процесса с повышением сложности ПО экспоненциально возрастает.

B_2**. Направление компрометации протоколов**. Это направление отражает диаметрально противоположный от используемого в направлении B_1

взгляд на безопасность протоколов – взгляд злоумышленника. Составляющие его методы имеют ключевое достоинство – они сравнительно просты в понимании и использовании, поскольку перед злоумышленниками не стоит задача снять с себя ответственность за уязвимости, которые могут проявиться в будущем. При этом данные методы весьма эффективны из-за несовершенства методов направления $\boldsymbol{B_1}$. Рассмотрим далее методы направления $\boldsymbol{B_2}$ подробно.

$\boldsymbol{B_{2,1}}$ – **эмпирический метод.** Основан на предположениях аналитиков об уязвимостях в ИТС и проверке этих предположений путем формирования и эксплуатации соответствующих тестовых способов реализации КА [27]. Несмотря на продуктивность этого метода, он не гарантирует положительного результата в течение длительного периода исследований, а ориентация на него предприятий промышленности может привести к неоправданно высокой стоимости создания и модернизации АС.

$\boldsymbol{B_{2,2}}$ – **феноменологический метод**. Основан на накоплении фактов проявления уязвимостей в процессе функционирования ИТС и разработке соответствующих способов реализации КА, эксплуатирующих эти уязвимости [27]. Этот метод сегодня во всем мире успешно применяется при бета-тестировании крупных программных продуктов, когда большое количество пользователей бесплатно работает с незавершенными версиями этих продуктов и сообщает разработчику о выявленных ошибках. Однако недостатками метода являются:

- большая продолжительность процесса накопления фактов проявления уязвимостей ИТС и невозможность установления момента его завершения, гарантирующего отсутствие уязвимостей;
- сложность точного определения условий и факторов, способствующих проявлению уязвимостей ИТС;
- невозможность автоматизации разработки способов реализации КА.

$\boldsymbol{B_{2,3}}$ – **метод поиска аналогий** в известных базах данных уязвимостей [219, 220]. Основан на анализе доступных баз данных с разнородными уязвимостями ИТС и эксплуатирующими их способами реализации КА и выборе в этих базах данных подходящих тестовых способов для исследуемой АС. Например, такие базы данных содержатся в Банке данных угроз безопасности информации ФСТЭК России [17], Common Vulnerabilities and Exposures компании «MITRE» [286], National Vulnerabilities Database Национального института стандартов и технологий США [311], Open Source Vulnerabilities Data Base [326], Vulnerability Nodes Database группы чрезвычайного компьютерного реагирования США [327], базе данных эксплоитов компании «Offensive Security» [313]. Этот метод используют широко известные коммерческие системы тестирования сетевой безопасности «Canvas» [280], «Core Impact» [287], «Drozer» [288], «Metasploit Framework» [308], «Nessus» [324], «Router Exploitation Framework» [318], «Test Advisor» [322], «XSpider» [329] и др. Однако, поскольку метод ориентирован на поиск в ИТС известных уязвимых компонентов, изначально найденных с использованием преимущественно **методов** $\boldsymbol{B_{2,1}}$ и $\boldsymbol{B_{2,2}}$, решить с его применением задачу разработки необходимого и достаточного множества тестовых способов реализации КА на ИТС возможно только в случае, если ИТС состоит только из известных и детально изученных компонентов, что для АС ВФ маловероятно.

Следует отметить, что в рамках **направления B_2** также может активно использоваться **метод $B_{1,1}$** в контексте классических работ [20, 131, 310].

Результаты анализа показали, что какая-либо комбинация методов **области B** не обеспечивает возможность разработки необходимого (в смысле полноты учитываемых параметров передачи сообщений) и достаточного (в смысле безызбыточной проверки сочетаний параметров передачи сообщений) множества тестовых способов реализации КА для известной процедуры телекоммуникационного протокола с учетом своевременности доставки сообщений. Наиболее пригодным для развития в этом направлении является **метод $B_{1,1}$.**

1.2.2 Анализ сферы исследования информационного конфликта

Прежде, чем рассматривать методы других областей, показанных на рис. 5, следует отметить, что в [176] приведен обзор около 400 работ отечественных авторов по тематике конфликта. В том числе предложена классификация предметных областей сферы исследования информационного конфликта. С позиции контекста, рассматриваемого в настоящей монографии, в работе [176] наиболее полно рассмотрена **область D** (радиолокация, радио- и радиотехнический мониторинг, радионавигация, техническая и компьютерная разведка, радиосвязь, оптическое наблюдение), которую учитывают, но не развивают результаты настоящего исследования. Анализ остальных областей рассмотрим далее в такой проекции, которая уточняет приводимую в [176] классификацию в целях отражения существа противоречия в теории, ставшего для автора побудительным мотивом для проведения научных изысканий.

***C*. Область исследования конфликта средств реализации КА и средств защиты информации.** В этой области сформировались три направления.

***C*$_1$. Направление обеспечения защиты АС от КА**.

Раннему обнаружению и предупреждению КА посвящены работы научной школы А.Г. Ломако и С.А. Петренко [25, 26, 213]. С позиции уровня абстракции теоретико-множественного подхода метод, предложенный в этих работах, позволяет «предвидеть будущее» и дает возможность защищаемому объекту осуществлять действия для достижения поставленных целей в условиях противостояния в киберпространстве без ущерба от КА. Вопрос ранней идентификации КА исследуется также в работах научных школ Н.Н. Толстых и А.Г. Остапенко [257, 270], в которых применяется аппарат теории случайных блужданий, теории катастроф и теории хаоса.

Адаптивному обеспечению устойчивости функционирования АС специального назначения, взаимодействующих через информационно-телекоммуникационные сети общего пользования, в условиях ИТВ посвящены работы научной школы И.Б. Саенко [3, 126, 232, 233]. В этих работах применяются теоретико-множественный подход, теория вероятностей и нечеткая логика.

Тематике построения системы защиты АС от КА также посвящены работы Е.Б. Дроботуна [114-116], базирующиеся на применении теоретико-

множественного подхода. В них формируется перечень способов реализации КА с использованием **метода $B_{2,3}$** с присущими ему недостатками, а также функциональные требования к системе защиты АС от КА, основанные на процедурах моделирования угроз и оценки рисков их реализации. Показателем эффективности защиты АС является риск невыполнения системой целевых функций, равный произведению вероятности реализации угрозы КА на величину наносимого ущерба/потерь. Вопросу определения количественного значения ущерба/потерь внимание не уделяется. Данный метод по своей теоретической проработке уступает методам вышеуказанных научных школ, но выигрывает у них с позиции практичности.

Разработке научно-методического аппарата, предназначенного для построения и функционирования ситуационных систем управления инцидентами безопасности критически важных объектов, реализующих свойства проактивности, динамичности и многоаспектности, посвящены работы научной школы И.В. Котенко [152, 155, 156]. Этот научно-методический аппарат базируется на применении логического вывода, основанного на экспертных знаниях, и принципе апостериорной защиты, допускающей, что у нарушителя уже имеются необходимые средства реализации КА.

Методы обеспечения устойчивости информационно-телекоммуникационных систем в условиях информационного конфликта на основе адаптивного, рефлексивного и ситуационного управления их безопасностью и защитой посвящены работы научной школы Н.Н. Толстых [68, 127, 196, 257]. Они базируются на применении математического аппарата сетей Петри и теории динамических систем. Конфликт рассматривается на сигнальном (физический уровень ЭМВОС) и информационном уровне, включающем семантический и прагматический подуровни. В этих работах рассматривается информационный конфликт компонентов информационно-телекоммуникационных систем со средствами ИТВ, включая КА. Наивысший по иерархии показатель эффективности исследуемой системы – вероятность реализации ее целевой функции, которой является мера способности выполнять задачу доведения информации с требуемыми показателями эффективности в условиях противодействия. Эти методы развиваются в исследовании Е.А. Жидко [124] с использованием математического аппарата теории борьбы за существование (популяционной динамики).

В работах научной школы М.А. Коцыняка [151, 157, 158] разработаны методики, позволяющие прогнозировать распределение КА по элементам информационно-телекоммуникационных сетей с учетом их роли и места, а также определять показатели, характеризующие устойчивость сети в условиях воздействия КА и требования к системе защиты. Полученные в этих работах результаты позволяют обосновать топологию информационно-телекоммуникационной сети, нейтрализующую КА, систему защиты, предотвращающую (затрудняющую) реализацию КА. В этих работах процесс реализации КА воспроизводится с применением метода топологического преобразования стохастических сетей, а опасность КА оценивается с применением метода анализа иерархий. В данных работах рассматриваются

известные классы уязвимостей КА, а эффективность функционирования информационно-телекоммуникационной сети в условиях КА определяется оперативностью технологических циклов управления.

Также это направление исследуется в работах научных школ:

- А.В. Душкина [119, 159, 200], развивающих с применением тензорного анализа и теории популяционной динамики научно-методический аппарат моделирования системы конфликтных взаимодействий в АС;
- А.И. Костогрызова [149, 150], применяющих аппарат теории массового обслуживания и теории вероятностей для оценки качества функционирования АС по показателям надежности и своевременности предоставления запрашиваемой или принудительно выдаваемой информации, конфиденциальности, полноты и актуальности используемой информации, безошибочности информации после контроля, корректности обработки информации, безошибочности действий должностных лиц и защищенности АС от КА;
- Л.Е. Мистрова [182-184], развивающих с применением теории множеств, теории игр и исследования операций научно-методический аппарат обеспечения конфликтной устойчивости иерархических многоуровневых организационно-технических систем в условиях конкуренции в контексте информационной безопасности;
- А.Г. Остапенко [204-206], развивающих с применением теории вероятностей научно-методический аппарат оценки рисков ущербности, шансов полезности и жизнестойкости компонентов АС в условиях КА;
- А.А. Сироты [77, 240, 241], развивающих с применением теории полумарковских случайных процессов и теории автоматов научно-методический аппарат оценки уязвимости АС на основе ситуационной модели динамики конфликта в интересах определения времени нарушения информационной безопасности при несвоевременном закрытии обнаруживаемых уязвимостей;
- Ю.И. Стародубцева [248, 249], развивающих с применением теории марковских процессов и теории вероятностей научно-методический аппарат мониторинга безопасности информации в информационно-телекоммуникационных системах;
- Ю.К. Язова [255, 275, 276], применяющих аппарат сетей Петри-Маркова для оценки эффективности защиты АС от КА по показателю относительного времени реализации угроз с применением мер защиты и без них.

Несмотря на существенную развитость научно-методического аппарата в этом направлении, он не позволяет обеспечить полноценную защиту от КА, поскольку не уделяет внимания заблаговременному выявлению новых, ранее неизвестных, уязвимостей ИТС, которые следует устранять в процессе разработки АС, а не стараться парировать в процессе их эксплуатации. В данном контексте уместна известная метафора – «дыры в лодке лучше латать до ее выхода в море». Кроме того, результаты работ в данном направлении не позволяют дифференцированно рассматривать КА по каналам передачи

данных АС на различных уровнях ЭМВОС, а также учесть характерные для боевых условий возможности средств реализации КА по выводу из строя, захвату управления и применения в своих целях ИТС, а также ответные меры ПЗИ на эти действия.

***C_2*. Направление исследования эффективности КА**.

Методы оценки и обеспечения функциональной устойчивости комплексов средств автоматизации военного назначения в условиях КА рассматриваются в работах научной школы С.М. Климова [10, 24, 135, 136]. Они базируются на применении математического аппарата теории игр и сетей Петри. Работы этой школы внесли существенный вклад в теорию и практику обеспечения защиты современных АС критически важных объектов от КА. Однако применение результатов этих работ ограничивается тем, что они рассматривают эффективность функционирования АС только в контексте своевременности и качества решения ИРЗ, не затрагивая вопросы ЗО и ЗУ этих систем. Также эта школа применяет для создания новых, ранее неизвестных, способов реализации КА **метод $B_{2,1}$** с присущими ему ограничениями.

Вопросам информационного конфликта сетей связи и средств ИТВ посвящены работы научных школ Ю.И. Стародубцева [19, 247], Е.В. Гречишникова [18, 21, 101], П.А. Будко [49]. Для этого применяется математический аппарат теории вероятностей и теории графов. Применимость этих работ также ограничена задачами связи, обеспечиваемыми ИТС АС.

Методы обеспечения устойчивости транспортной телекоммуникационной сети специального назначения в условиях динамического многоуровневого информационного конфликта рассматриваются в работах научной школы С.И. Макаренко [170, 171, 173, 175, 186-188]. Они базируются на применении математического аппарата теории борьбы за существование (популяционной динамики). В них детализируется информационный конфликт в части воспроизведения процессов совместного влияния способов ИТВ на динамические процессы функционирования протоколов на физическом, канальном и сетевом уровнях ЭМВОС. Однако в этих работах наивысшим по иерархии показателем является среднесетевая вероятность устойчивости информационного направления связи, что ограничивает применимость результатов этой школы только к задачам связи, не затрагивая ИРЗ и ЗУ, выполнение которых также обеспечивается АС ВФ.

В работах П.П. Крутских [161, 252] рассмотрена иерархическая модель взаимодействия систем добывания, обработки и передачи информации с учетом деструктивных воздействий, позволяющая воспроизводить конфликт как по схеме противодействия, так и по схеме содействия в интересах оценки целевой функции таких систем по показателю информационного превосходства, рассчитываемого на основе анализа возможностей стороны конфликта по использованию информации для управления сложными объектами. Результаты этих пионерских в рассматриваемой предметной области работ не утратили своей актуальности и сегодня. В частности, в них впервые предлагается воспроизводить в модели АС в условиях деструктивных воздействий (в том числе КА) не только процессы передачи-приема, но и процессы обработки

информации. Тем не менее, данные работы не предусматривают возможности оценки влияния КА на боевые циклы ВФ, обеспечиваемые АС.

Несмотря на значительную теоретическую проработку работ в этом направлении, разрозненность применяемых в них подходов не позволяет учитывать возможность одновременного обеспечения ИТС процессов выполнения информационно-расчетных, управляющих и обеспечивающих задач в условиях информационного конфликта. Интеграция существующих подходов к оценке эффективности влияния КА на ИТС приводит к известной в системном анализе проблеме «взрыва пространства состояний», для разрешения которой автором предлагается применять метод стратификации, рассмотренный в параграфе 3.2 настоящей монографии.

***C_3*. Направление исследования распространения СПС** в сетях базируется на имитационных и аналитических моделях [169, 173].

Имитационные модели (основываются на применении метода Монте-Карло) наиболее развиты в работах научной школы И.В. Котенко [156, 154]. Они обеспечивают высокую точность моделирования при большом количестве сетевых узлов, но требуют детального знания алгоритмов информационного взаимодействия узлов. Однако для наиболее вероятных на практике исходных данных только о структуре сетей ВФ и среднестатистических временных характеристиках функционирования СПС и ПЗИ их узлов приоритет имеют аналитические модели, отличающиеся высокой скоростью моделирования и возможностью получения решения «в общем виде» [153]. Аналитические модели этого направления делятся на две группы:

- модели, основанные на применении аппарата популяционной динамики. Они предоставляют возможность для анализа важных состояний совокупности узлов с учетом времени, но не учитывают структуру сетей [146, 293, 309];
- модели, основанные на применении теории графов, теории марковских процессов, теории массового обслуживания и тензорного исчисления. Они учитывают структуру сетей, но либо ограничены использованием заведомо недостаточного количества состояний узлов из-за высокой вычислительной сложности применяемых методов [105, 199], либо не дают информации о состоянии защищенности каждого конкретного узла сети в заданный момент времени [259].

Несмотря на высокий уровень теоретической проработки, в целом работы аналитического направления не позволяют определять вероятностно-временные характеристики состояний каждого узлового ИТС сети с одновременным учетом:

- архитектуры сети;
- характеристик функционирования ПЗИ узловых ИТС;
- поведенческих характеристик «скрытных» и «нескрытных» СПС;
- возможности заражения сети множеством СПС различных типов в любые моменты времени.

Эти обстоятельства свидетельствуют об актуальности развития аналитических моделей научного направления исследования распространения СПС.

1.2.3 Анализ сферы исследования боевых действий

Пересечение сфер исследований информационного конфликта и боевых действий образовало **область исследования процессов разведки, управления, связи, навигационно-временного обеспечения в боевых условиях с применением информационного оружия (область *E*** на рис. 5). В этой области используются следующие подходы.

***E*$_1$. Экспертные подходы**.

В [148] предлагается учитывать возможности КА в так называемом «полном» боевом потенциале (БП) ВФ наряду с ОП, РЭП, управлением и разведкой в качестве слагаемого. В [125, 147, 166] предполагается присвоение средствам реализации КА весового коэффициента. Такой подход **не учитывает** реальные возможности средств реализации КА, динамику применения образцов вооружения и ВФ, противодействие противника и влияние техники РЭБ на его огневую мощь.

***E*$_2$. Вероятностные подходы**. К таким подходам относятся:

- подход, предложенный научной школой В.И. Владимирова [71, 250]. Этот подход полезен при экспресс-оценке РЭП радиосвязи, но не учитывает возможности КА. Сегодня этот подход развивается в работах Р.Л. Михайлова [186-188] в части детализации информационного конфликта информационно-телекоммуникационных систем на основе системного учета взаимного влияния процессов функционирования трех подсистем каждого из противоборствующих ВФ: разведки, связи и РЭП. Но в этих работах также не учитываются возможности КА по влиянию на вероятностные и временные характеристики подсистем разведки и ОП противника и на временные характеристики его подсистемы управления;
- методология оценки эффективности РЭБ в операциях (боевых действиях), которой посвящен ряд глубоко проработанных с теоретической точки зрения трудов Ю.С. Сухорукова [2, 117, 178, 251], С.Н. Меркулова [178], Ю.Е. Донскова [110-112] и Г.Д. Высторобского [76]. Однако в них также не учитываются КА.

***E*$_3$. Подходы на основе теории марковских процессов**. Наиболее известным подходом в этом классе является подход научной школы Ю.Л. Козирацкого [51, 52, 141, 142], методологическая основа которого состоит в применении математического аппарата полумарковских процессов для анализа переходных процессов в боевых ситуациях с применением средств РЭП. Эти работы адаптированы для исследования сложных дуэльных ситуаций, возникающих в бою. Однако применяемый в них математический аппарат не ориентирован на моделирование боя ВФ.

***E*$_4$. Имитационное моделирование**. Такой подход развивается научной школой А.П. Богомолова [235, 236] и базируется на методе Монте-Карло, широко поддерживаемом многочисленными программными и программно-аппаратными средствами. Достоинством имитационных моделей является возможность адекватного отражения различных свойств исследуемого процесса,

а их недостатками являются необходимость проведения многократных статистических экспериментов и ориентация на процессы с относительно небольшим количеством потенциально возможных сценариев развития. Также имеет место важная особенность имитационных моделей, существенно ограничивающая их применение. Дело в том, что в них используется один или комбинация двух следующих способов учета модельного времени [239, 244, 269]: способ постоянных приращений и способ существенных состояний. Ни один из этих способов не позволяет решать в ходе одной реализации сценария боя оптимизационные задачи (в первую очередь, целераспределение) в рамках ВФ в целом или в рамках его относительно самостоятельных крупных составных частей. Эта особенность обусловлена неопределенностью в том, какие именно события в процессе боя брать за точки отсчета временных интервалов боевых циклов, в интересах которых проводится оптимизация. Подробно это рассмотрено в главе 4.

Указанные работы отличаются глубокой теоретической проработкой, но не позволяют учесть одновременное влияние КА на временные и вероятностные (в том числе вероятностно-временные) характеристики функционирования подсистем, задействованных в боевых циклах ВФ.

Область *F* на рис. 5 является **областью исследования боя с применением средств ОП, разведки, имитации обстановки, аэрозольного противодействия и воздействия на личный состав**. К наиболее проработанным трудам в этой области относятся работы В.Г. Анисимова и Е.Г. Анисимова [5, 6], А.И. Буравлева [53-56], В.М. Буренок [61-63], П.А. Дульнева [120], Н.В. Митюкова [185], Д.А. Новикова [198], Г.Б. Петухова [214, 215], В.И. Поленина [217], О.В. Саяпина [234], А.И. Черноскутова [264, 265] и др. Однако работы в этой области не затрагивают тематику информационного конфликта и, следовательно, тематику КА.

Таким образом, недостаточная степень разработанности направлений рассмотренных научных областей свидетельствует о противоречии в науке *между* потребностью в оценке защищенности ПО АС, применяемых в боевых циклах ВФ, в процессе их создания *и* недостаточной развитостью существующего научно-методического аппарата обеспечения защищенности ПО этих систем от КА противника.

1.3 Постановка проблемы киберзащиты автоматизированных систем воинских формирований

Целью настоящей работы является повышение эффективности функционирования АС, применяемых в боевых циклах ВФ, на основе обеспечения защищенности их ПО от КА противника. Для достижения этой цели требуется разработать совокупность методов, моделей и методик обеспечения защищенности от ранее неизвестных способов реализации КА противника ПО АС, применяемых в боевых циклах ВФ, в процессе их создания. Совокупность элементов решения проблемы киберзащиты АС ВФ представлена на рис. 8.

Формализованный вид процесса разработки указанных методов, моделей и методик согласно [130, 174] состоит в следующем.

Рис. 8. Совокупность элементов решения проблемы киберзащиты автоматизированных систем воинских формирований

Необходимо разработать совокупность методов, моделей и методик M_0, обеспечивающую на основе анализа объекта исследования с использованием совокупности моделей, отображающей множество X исходных параметров способов реализации КА, эксплуатирующих уязвимости АС, во множество Y выходных параметров эффективности, определение такого подмножества $X_{кр} \subset X$ способов реализации КА, при парировании которого в процессе создания (модернизации) АС ее эффективность на уровне выходных параметров информационных $Y_{ИНФ} \subset Y$ и информационно-боевых $Y_{ИНФБ} \subset Y$ показателей достигает значений, при которых боевой показатель ВФ, оснащенного защищаемой АС, $Y_{БОЕВ} \subset Y$ максимален при недостижимости порогового значения ε или достигает это значение с минимальной затратой доступных ресурсов при заданных:

- множествах внутренних параметров: состава, структуры, местоположения, процессов функционирования, воздействия, обеспеченности ресурсами с детализацией ЭБП ВФ до устройств, ИТС АС и людей – O_C (могут также учитываться критически важные объекты гражданской инфраструктуры); связей устройств, ИТС и людей – O_R; стоимость работ по устранению уязвимостей ИТС – $O_\$$;
- множестве параметров среды – $\mathbb{R}$: метео-, географических и временных условий, местности, диверсионной деятельности сторон конфликта;
- множествах ограничений: физической реализуемости компонентов АС и ЭБП ВФ в целом – Θ_C (могут учитываться критически важные объекты гражданской инфраструктуры); связей устройств, ИТС и людей – Θ_R; параметров среды – $\Theta_{\mathbb{R}}$; максимально допустимой стоимости работ по устранению уязвимостей – $\Theta_\$$.

Пороговое значение эффективности функционирования АС в боевых условиях ε обосновывается следующим образом. Орган управления наступающего ВФ в процессе принятия решения на бой (операцию) всегда рассчитывает долю остаточной численности своих сил и средств после выполнения задачи. Здесь под численностью понимается численность ЭБП ВФ, взвешенная по их коэффициентам боевой соизмеримости (КБС). Существует остаточная доля численности ВФ, по достижении которой даже выполнение задачи «любой ценой» прекращается. Для ВФ США и других стран НАТО в наступлении в таком случае ε = 25 % [325]. В общем случае допускается потеря не более 25 % в одном бою [113]. То есть для ВФ уровня мотострелкового батальона (мсб) в наступлении при выполнении первой из трех задач дня ε = 75 %, при выполнении второй из трех задач дня ε = 56 %, а при выполнении главной задачи дня ε = 42 %. Это связано с необходимостью сохранения более 40 % численности ВФ после третьего боя за день. Иначе ВФ считается небоеспособным [113].

Если в результате мероприятий по обеспечению киберзащиты АС, применяемых в обороняющемся ВФ, значение остаточной доли численности наступающего противника, рассчитывающего на эффективное применение средств реализации КА, будет ниже планируемого уровня, то это может способствовать отказу наступающего ВФ от своих планов. Однако на практике для сохранения инициативы наступающее ВФ может допустить и большие потери. Рационально полагать, что наступающее ВФ в реальных условиях прекратит атаку в случае, если в одном бою достигнет уровня потерь, допустимого для двух боев и более. То есть для первого боя остаточная доля численности должна составлять не 75 %, а 56 % (на 19 % меньше), для второго боя не 56 %, а 42 % (на 14 % меньше), а для третьего боя не 42 %, а менее 40 % (на 2 % меньше). Поэтому в общем случае при обеспечении киберзащиты АС обороняющегося ВФ рационально стремиться к снижению остаточной доли численности наступающего ВФ, рассчитывающего на эффективность КА, не менее чем на 19 %, а в критически важном бою – не менее чем на 50 %. В случае недостижимости указанных значений по причине принципиальной невозможности или отсутствия ресурсов приемлемым может считаться любое дополнительное снижение остаточной доли численности наступающего ВФ за счет киберзащиты, а в случае достижения этих значений с затратой некоторой доли выделенных на киберзащиту ресурсов будет иметь место экономия.

С учетом изложенного формализованная постановка проблемы киберзащиты заданного (защищаемого) образца АС ВФ с позиции теоретико-множественного подхода имеет следующий вид:

$$
\begin{gathered}
M_0: \ \langle X, O, \mathbb{R} \rangle \to \begin{cases} Y_{\max} \subset Y, \text{ если } \forall \left(y_{\text{БОЕВ}} \in Y_{\text{БОЕВ}} \right) < \varepsilon; \\ Y_{+} \subset Y, \text{ если } \exists \left(y_{\text{БОЕВ}} \in Y_{\text{БОЕВ}} \right) \geq \varepsilon; \end{cases} \\
O = O_{\text{С}} \cup O_{\text{R}} \cup O_{\$}, Y = Y_{\text{БОЕВ}} \left(Y_{\text{ИНФБ}} \left(Y_{\text{ИНФ}} \right) \right), \\
\forall \left(y_{\text{БОЕВ}} \in Y_{+} \right) = \varepsilon, \forall \left(y_{\text{БОЕВ}} \in Y_{\max} \right) = \max_{O_{\text{С}} \subseteq \Theta_{\text{С}}, O_{\text{R}} \subseteq \Theta_{\text{R}}, O_{\$} \subseteq \Theta_{\$}, \mathbb{R} \subseteq \Theta_{\mathbb{R}}} M_0 \left(X, O, \mathbb{R} \right).
\end{gathered}
\tag{1}
$$

Для отражения сущности требуемых методов следует воспользоваться методом декомпозиции [129].

Метод генерации КА на телекоммуникационное оборудование M_1 предусматривает множество $O_{\text{C}}^{*} \subset O_{\text{C}}$ процессов функционирования образцов ИТС АС, связанных множеством $O_{\text{R}}^{*} \subset O_{\text{R}}$. Эти множества вкладываются в процесс частного антагонистического конфликта, в котором выбирается подмножество $X_{\text{кр}} \subset X$ критичных входных параметров способов реализации КА, приводящих ИТС АС во множество $\Psi_{\text{кр}} \subset \sum$ нештатных состояний потери работоспособности α_1, сниженной эффективности функционирования α_2, управляемости α_3 или доступности для углубленного анализа α_4 противником:

$$M_1 : < \left(X_{\text{кр}} \subset X\right), O_{\text{C}}^{*}, O_{\text{R}}^{*} > \rightarrow \Psi_{\text{кр}} \subset \sum, \ \forall\left(\psi_{\text{кр}} \in \Psi_{\text{кр}}\right) = \alpha_1 \vee \alpha_2 \vee \alpha_3 \vee \alpha_4 . \qquad (2)$$

В формуле (2) используются следующие обозначения.

1. $O_{\text{C}}^{*} = < I_{\text{AC}}, J = \bigcup_{\forall i} J_i, S = \bigcup_{\forall i,j} S_{i,j} \subseteq S^{\sim}, M = \{m_{i,j,\mu,r}\} >$,

где I_{AC} – множество образцов АС в ВФ, включающее заданный защищаемый образец АС и все образцы АС, с которыми он взаимодействует;

J_i – множество образцов ИТС в защищаемом i-м образце АС ($i = 1\ldots|I_{\text{AC}}|$);

$S_{i,j} = \{s_{i,j,\mu}\}$, $j = 1\ldots|J_i|$, $\mu = 1\ldots|S_{i,j}|$ – множество процессов функционирования ПО в j-м ИТС i-го образца АС, шаги которых могут включать прием/передачу сообщений;

$S^{\sim}$ – множество корректных процессов;

M – множество типов сообщений, которыми обмениваются ИТС заданного защищаемого образца АС;

$m_{i,j,\mu,r}$ – r-й тип сообщения, используемый в μ-м процессе j-го ИТС заданного защищаемого i-го образца АС, $r = 1\ldots|M|$.

2. $X = \bigcup_{\forall i,j,\mu,r} \mathbb{Q}_{i,j,\mu,r} : \mathbb{Q}_{i,j,\mu,r} = \left\{W_{i,j,\mu,r,k} \times \Omega_{i,j,\mu,r,k}\right\}$,

где $\mathbb{Q}_{i,j,\mu,r}$ – множество пар «сообщение-время», образуемое множествами $W_{i,j,\mu,r,k} = W_{i,j,\mu,r,k}^{+} \cup W_{i,j,\mu,r,k}^{-} \subseteq W_{i,j,\mu,r,k}^{\sim}$ и $\Omega_{i,j,\mu,r,k} = \Omega_{i,j,\mu,r,k}^{+} \cup \Omega_{i,j,\mu,r,k}^{-} \subseteq \Omega_{i,j,\mu,r,k}^{\sim}$;

$k = 1\ldots|\mathbb{Q}_{i,j,\mu,r}|$ (здесь и далее неиндексированное множество с некоторым именем – это объединение всех индексированных множеств с этим именем);

$W_{i,j,\mu,r,k}^{+}$ и $W_{i,j,\mu,r,k}^{-}$ – k-е элементы множеств, соответственно, предусмотренных и непредусмотренных протоколом вариантов содержания сообщения r-го типа μ-го процесса j-го ИТС защищаемого i-го образца АС;

$W_{i,j,\mu,r,k}^{\sim}$ – k-й элемент множества допустимых протоколом вариантов содержания сообщения r-го типа в μ-м процессе j-го ИТС i-го образца АС;

$\Omega_{i,j,\mu,r,k}^{\sim}$ – k-й элемент множества моментов времени передачи сообщения r-го типа в μ-м процессе j-го ИТС защищаемого i-го образца АС, длительность интервалов между которыми синхронизирована с каналом связи, обеспечивающим этот процесс;

$\Omega_{i,j,\mu,r,k}^{+}$ и $\Omega_{i,j,\mu,r,k}^{-}$ – k-е элементы множеств, соответственно, предусмотренных и непредусмотренных моментов времени передачи сообщения r-го типа в μ-м процессе j-го ИТС защищаемого i-го образца АС;

3. O_{R}^{*} – множество параметров связей ИТС защищаемой АС.

4. $\sum=\{\psi_{i,j}\}$ – множество индикаторов работоспособности ИТС в защищаемом i-м образце АС,

$$\psi_{i,j}=\begin{cases}1, & \text{если } j\text{-е ИТС работает штатно после получения}\\ & \text{одного или более однотипных сообщений;}\\ 0 & \text{в противном случае.}\end{cases}$$

С учетом этого для метода M_1 требуется разработать детерминированную модель совокупности процессов функционирования заданного образца АС, устанавливающую закономерность изменения множества $\sum$ выходных параметров от множеств W^{+}, Ω^{+} входных параметров, множеств $I_{\text{АС}}$, J, S, M, O_{R}^{*} внутренних параметров и множеств W^{-}, Ω^{-} параметров тестовых конфликтных условий функционирования. На множество S процессов функционирования ИТС, входящих в состав АС, накладывается ограничение корректности $S\subseteq S^{\tilde{}}$, а на значения параметров множеств W^{+}, Ω^{+}, W^{-}, Ω^{-} накладываются ограничения физической реализуемости: $W^{+}\cup W^{-}\subseteq W^{\tilde{}}$, $\Omega^{+}\cup\Omega^{-}\subseteq\Omega^{\tilde{}}$. При этом требуется выявить множество пар $<w\in W_{\text{кр}},\ \omega\in\Omega_{\text{кр}}>$ критических значений параметров функционирования образца АС при их варьировании на всем диапазоне допустимых значений: $w\in W^{+}\cup W^{-}$, $\omega\in\Omega^{+}\cup\Omega^{-}$. Значение пары параметров $<w,\ \omega>$ является критичным, если при этих значениях любое ИТС заданного i-го образца АС переводится в нештатный режим функционирования, то есть $\exists j$: $\psi_{i,j}=0$. С учетом этого формализованная постановка задачи на разработку метода M_1 имеет следующий вид:

$$\begin{gathered}M_1:<\left\{\left(W^{+}\cup W^{-}\right)\times\left(\Omega^{+}\cup\Omega^{-}\right)\right\},O_{\text{C}}^{*},O_{\text{R}}^{*}>\to\Psi_{\text{кр}}\subset\sum;\\ \forall\left(\psi_{\text{кр}}\in\Psi_{\text{кр}}\right)=\alpha_1\vee\alpha_2\vee\alpha_3\vee\alpha_4;\ \forall\, w,\omega\left(w\in W^{+}\cup W^{-}\subseteq W^{\tilde{}},\omega\in\Omega^{+}\cup\Omega^{-}\subseteq\Omega^{\tilde{}}\right):\\ w\in W_{\text{кр}},\omega\in\Omega_{\text{кр}},\ \text{если}\ \exists j:\ \ \psi_{i,j}\left(<w,\omega>,I_{\text{АС}},J,S,M,O_{\text{R}}^{*}\right)=0;\\ O_{\text{C}}^{*}=<I_{\text{АС}},J,S,M>\subseteq O_{\text{C}}\subseteq\Theta_{\text{C}};\ O_{\text{R}}^{*}\subseteq O_{\text{R}}\subset\Theta_{\text{R}}.\end{gathered}\qquad(3)$$

Метод оценки эффективности КА в боевых действиях M_2 предусматривает вложение конфликта, учитываемого в методе M_1, в процесс боя ВФ, в котором, в свою очередь, используются реализации подмножества нештатных состояний ИТС $\Psi_{\text{кр}}$ для выбора при заданных ограничениях **либо** подмножества $Y_{+}\subset Y$ выходных параметров информационной и информационно-боевой эффективности функционирования защищаемой АС и параметра боевой эффективности ВФ, оснащенного защищаемой АС, при которых достигается заданное пороговое значение боевой эффективности ВФ с минимальной затратой доступных ресурсов, **либо** подмножества $Y_{\max}\subset Y$ этих параметров, в котором пороговое значение ε недостижимо, а значение параметра боевой эффективности ВФ максимально:

$$\begin{gathered}M_2:<IDP_i\times<W_{\text{кр}\,i},\Omega_{\text{кр}\,i}>,O^{*},\mathbb{R}>\to\begin{cases}Y_{\max}\subset Y,\ \text{если}\ \forall\left(y_{\text{БОЕВ}}\in Y_{\text{БОЕВ}}\right)<\varepsilon;\\ Y_{+}\subset Y,\ \text{если}\ \exists\left(y_{\text{БОЕВ}}\in Y_{\text{БОЕВ}}\right)\geq\varepsilon;\end{cases}\\ O^{*}=O_{\text{C}}\cup O_{\text{R}}\cup O_{\$}-IDP_i\times<W_{\text{кр}\,i},\Omega_{\text{кр}\,i}>;\ Y=Y_{\text{БОЕВ}}\left(Y_{\text{ИНФБ}}\left(Y_{\text{ИНФ}}\right)\right);\end{gathered}\qquad(4)$$

$$\forall\left(y_{\text{БОЕВ}}\in Y_{+}\right)=\varepsilon;\ \forall\left(y_{\text{БОЕВ}}\in Y_{\max}\right)=\max_{O_{\text{C}}\subseteq\Theta_{\text{C}},O_{\text{R}}\subseteq\Theta_{\text{R}},O_{\$}\subseteq\Theta_{\$},\mathbb{R}\subseteq\Theta_{\mathbb{R}}}M_2\left(\left(X_{\text{кр}}\subset X\right),O,\mathbb{R}\right);$$

$$O_{\text{C}}=\left\langle PM,\aleph,\Re,\mathbb{H},VP,\mathcal{M},PE,TS,\left\langle IT,IR,IV,<IPZ,IPT>,<IDF,IDE,IDR,IDP,IDI>\right\rangle\right\rangle.$$

В формуле (4) используются следующие обозначения.

1. O_{C} – кортеж внутренних параметров каждого ЭБП ВФ, включающий множества параметров:

PM – параметры местоположения;

$\aleph$ – параметры управления;

$\Re$ – параметры защиты от воздействий противника;

$\mathbb{H}$ – параметры подверженности диверсии;

VP – параметры времени подготовки к работе;

$\mathcal{M}$ – параметры ущерба для вывода из строя;

PE, *TS*, *RA* – параметры функционирования людей, устройств и ИТС.

Кортеж *RA* (в формуле (4) показан в виде своих элементов) состоит из следующих множеств параметров ИТС:

IT – параметры времени подготовки ИТС к работе;

IR – параметры обеспечивающих ресурсов, необходимых для работы ИТС;

IV – параметры возможностей по влиянию ИТС на противника;

IP – параметры процессов функционирования ИТС (кортеж *IP* в формуле (4) показан в виде своих составляющих кортежей: *IPZ* – параметры выполняемых задач; *IPT* – параметры качества электронной компонентной базы);

ID – параметры защищенности от воздействия противника, в формуле (4) кортеж показан в виде составляющих его кортежей: *IDF* – параметры защиты от ОП; *IDE* – параметры защиты от воздействия мощным ЭМИ; *IDR* – параметры защиты от РЭП; *IDP* – параметры защиты от КА (период и время смены параметров протоколов, период и время регламентного поиска СПС, время обнаружения активных СПС); *IDI* – параметры защиты от разведки.

2. $O_{\text{R}}=\left\{R_{\eta}\right\},\ \eta=1...\left|PE\times TS\times RA\times PE\times TS\times RA\right|$ – множество внутренних параметров, характеризующих иерархически упорядоченное информационное взаимодействие и взаимное влияние ИТС, устройств и людей. В R_{η} входят множества:

TY_{η} – типов связей в η-й паре ИТС, устройств и людей воюющих сторон;

CH_{η} – параметров связи в η-й паре.

3. $O_{\$}=\{\rho_{i,j}\}$, $\rho_{i,j}$ – стоимость *j*-го ИТС или устройства в *i*-м ЭБП.

4. O^{*} – вспомогательное множество, состав которого раскрыт в формуле (4).

Границы настоящего исследования исключают вопросы криптозащиты ПО. С одной стороны, это обусловлено закрытостью данной тематики для АС ВФ, а с другой – широко известным наличием значительных результатов в данной предметной области. Они свидетельствуют о том, что сегодня вскрытие криптозащиты в подавляющем большинстве случаев при доступных вычислительных ресурсах является не проблемой, а задачей. Качество ПО в границах исследования учитывается в части защищенности от КА, а также в части надежности ОПО и функциональной пригодности, производительности и надежности СПО.

Выводы по первой главе

Результаты анализа автоматизированных систем, применяемых в боевых циклах воинских формирований, процесса их функционирования в современных боевых действиях и вооруженных конфликтах показывают, что при создании таких систем не реализуемыми в полном объеме являются требования обеспечения защищенности их программного обеспечения от кибератак противника.

Факторами высокой эффективности применения в современном бою кибератак на автоматизированные системы являются невозможность организовать полноценную энергетическую и физическую защиту каналов передачи данных этих систем от удаленного доступа, а также наличие информации об уязвимостях программного обеспечения их информационно-технических средств. Эти уязвимости обусловлены неизбежно допускаемыми в процессе разработки ошибками в многообразных, многопоточных и вариативных программах, объем которых составляет от десятков тысяч до миллионов строк программного кода.

Средства реализации кибератак формируют условия для проявления уязвимостей программного обеспечения автоматизированных систем. При этом основными точками входа кибератак являются интерфейсы автоматизированных систем, отвечающие за процессы информационного взаимодействия. Объектом кибератак являются информационно-технические средства автоматизированных систем, в которых присутствует канал обмена данными с внешними субъектами. Поражающим фактором кибератак являются электромагнитные колебания (электрические токи), переносящие последовательности цифровых символов, воспринимаемых в автоматизированной системе как деструктивная программа. В сравнении с классической техникой радиоэлектронного подавления отличительными характеристиками кибератак являются: поражающая способность, транслируемость, авторегенерируемость, прозрачность, транзитивность, телеоперационность, низкая энергоемкость и высокая избирательность.

Результаты анализа показывают, что сегодня имеет место очевидная потребность в выявлении и устранении уязвимостей программного обеспечения автоматизированных систем, предназначенных для применения в боевых циклах воинских формирований, в процессе их создания. В то же время налицо ограниченные возможности существующих средств обеспечения защищенности программного обеспечения таких систем от кибератак противника. Это противоречие обусловлено недостаточной развитостью существующего научно-методического аппарата киберзащиты автоматизированных систем воинских формирований, что свидетельствует об актуальности нового теоретического направления исследования, объединяющего методы в трех пересекающихся научных сферах: проектирования информационно-телекоммуникационных систем, исследования информационного конфликта и исследования боевых действий.

В следующих главах настоящей монографии рассматриваются результаты разработки и применения недостающих и весьма потребных сегодня элементов научно-методического аппарата киберзащиты автоматизированных систем воинских формирований.

2 Модель процесса информационного взаимодействия информационно-технических средств автоматизированных систем по известной процедуре телекоммуникационного протокола и метод генерации кибератак на телекоммуникационное оборудование

«Простота – это высшая сложность».

Народная мудрость

2.1 Модель процесса информационного взаимодействия информационно-технических средств автоматизированных систем по известной процедуре телекоммуникационного протокола

Анализ предметной области. В наиболее общем случае моделирование процесса информационного взаимодействия ИТС АС проводится на основе анализа спецификаций телекоммуникационных протоколов, регламентированных международными или отраслевыми НТД. Например, тома спецификации протоколов стандарта IEEE-802.11 Wi-Fi, используемого в том числе в ИТС АС ВФ ведущих стран мира, включают несколько тысяч страниц. При этом в спецификациях используются преимущественно текстовые описания процедур информационного взаимодействия ИТС.

Телекоммуникационный протокол – это совокупность взаимосвязанных процедур, каждая из которых реализуется в конкретных условиях функционирования ИТС. Известные подходы к моделированию таких процедур, изложенные, например, в работах [69, 321], представляют их в виде дискретно-событийных моделей, в которых каждое состояние – это отдельный шаг процесса функционирования одного ИТС, совокупность выполняемых одновременно шагов нескольких ИТС или результат редукции (упрощения) последовательности шагов в одном ИТС, а переход между состояниями – это связь между шагами процесса(ов) функционирования одного или нескольких ИТС. Однако, как отмечено в параграфе 1.2, такие модели не позволяют учитывать временные параметры информационного взаимодействия ИТС (распределенных в пространстве и одновременно функционирующих), необходимые для разработки тестовых способов реализации КА. Рассмотрим сущность этих временных параметров.

В ИТС могут приходить сообщения от легитимных абонентов или злоумышленников в течение так называемого «интервала своевременности», раньше или позже него (см. рис. 9). Этот интервал начинается в момент начала ожидания поступления сообщения программной реализацией соответствующего алгоритма функционирования ИТС. Заканчивается этот интервал в момент завершения так называемого «интервала одновременности», в течение которого принимается сообщение. При этом неважно, от кого это сообщение поступило, от легитимного абонента или от злоумышленника. Главное, чтобы структура

и содержание принятого сообщения соответствовали структуре и содержанию сообщения, которое ожидает программная реализация алгоритма функционирования ИТС. Следует отметить, что один алгоритм функционирования ИТС одновременно может быть готов принять разные типы сообщений, и для каждого типа сообщения в этом алгоритме предусматривается отдельная ветвь его обработки. В то же время в ИТС алгоритмов, одновременно ожидающих сообщение, может быть несколько. В интервале одновременности приемное устройство ИТС рассматривает все принятые сообщения как одно. Этот интервал в спецификациях телекоммуникационных протоколов обычно называют временным слотом или «таймслотом». Например, его длительность в сетях цифровой радиосвязи (СЦР) стандарта DMR (англ. *Digital Mobile Radio* – цифровое мобильное радио) равна 30 мс [291].

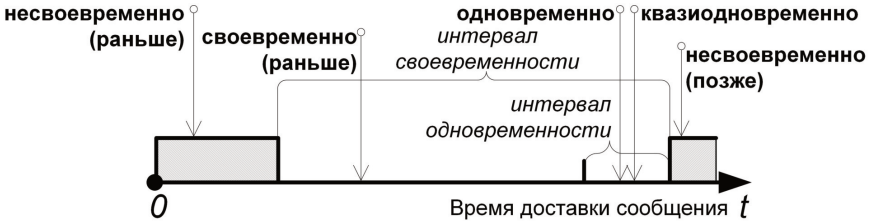


Рис. 9. Своевременность доставки сообщения

При приеме сообщения возможны следующие реакции ИТС.

1. При **раннем** приеме *ожидаемого* сообщения, отправленного средством реализации КА, (то есть до начала или в течение интервала своевременности) ИТС преждевременно переходит к последующим шагам своего алгоритма функционирования, на которых оно отправит сообщение или будет ожидать поступления уже других сообщений. Поэтому при отправке легитимным абонентом сообщения, которое уже было отправлено злоумышленником, оно не будет принято. Ведь ИТС, для которого предназначено сообщение, уже не будет его ждать. Это ИТС будет работать с учетом данных, заданных средством реализации КА. Ранний прием может быть инициирован многократно, в том числе в целях непредусмотренного расходования ресурсов ИТС.

2. **Поздний** прием сообщения, равно как и невозможность приема, ожидающее его ИТС воспримет как сбой. Этот сбой может обрабатываться программной реализацией алгоритма функционирования ИТС корректно, игнорироваться или приводить к ошибке.

3. **Одновременный** прием легитимного и нелегитимного сообщений может обрабатываться двумя способами. При несущественном различии на входе радиоприемного тракта мощности радиосигналов, несущих легитимное и нелегитимное сообщения, ИТС воспринимает это как ошибку на физическом уровне ЭМВОС, то есть как шум. При превышении мощности одного из принимаемых сигналов более некоторого порогового значения радиоприемный тракт воспринимает этот сигнал как полезный, а другой сигнал воспринимает как шум. Каждому виду сигнала соответствует собственное пороговое значение «сигнал/шум».

Рассмотрим далее модель, учитывающую временные параметры информационного взаимодействия ИТС в интересах разработки необходимого и достаточного множества тестовых способов реализации КА.

Исходные данные: спецификации протоколов ИТС АС.

Постановка задачи: разработка модели процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола, учитывающей временные параметры этого процесса.

Идея решения этой задачи состоит в следующем [27, 41]. В теории графов известна задача поиска Эйлерова пути через семь кёнигсбергских мостов (ныне г. Кёнигсберг называется Калининградом), когда нужно последовательно пройти все мосты, но нельзя пройти любой из мостов дважды. Известно, что в силу особенностей протекания реки Преголя в Калининграде эта задача на плоскости решения не имеет. Решение возникает, если перемещаться между мостами не в двухмерном, а в трехмерном пространстве.

По аналогии с решением задачи о кёнигсбергских мостах для учета временных параметров передачи сообщений между ИТС в рамках единого распределенного процесса, регламентируемого телекоммуникационным протоколом, следует выйти за рамки «плоского» восприятия процесса информационного взаимодействия распределенных в пространстве ИТС и сформировать третье измерение, которое отражает требуемые временные параметры. В рамках декомпозиционно-агрегативного (интегративного) подхода в системном анализе такая операция называется операцией образования второго уровня агрегирования [229]. В результате этой операции получается результирующий системный граф второго уровня, который включает вершины, образуемые комплексами из множеств вершин первого уровня.

Рассмотрим, каким образом граф второго уровня агрегирования позволяет учесть временные параметры асинхронной передачи сообщений между ИТС, что являлось невозможным при представлении системы в виде «плоскостной» схемы синхронной композиции детерминированных и полностью определенных автоматов в [58].

Формализация модели. Предлагаемая модель процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола базируется на следующих положениях [27]:

- функционирование ИТС представляется в виде комплекса локальных процессов (ЛП), взаимосвязанных единым распределенным процессом (РП) функционирования АС, включающей эти ИТС. Модель изначально ориентирована не только на программные, но и на электромагнитные воздействия, так как в виде алгоритма представляется функционирование ИТС на любом уровне ЭМВОС;
- взаимодействие ИТС рассматривается с позиции обмена сообщениями, под которыми понимается как совокупность цифровых данных, так и электромагнитный (в том числе отраженный) или электрический сигнал. Передача сообщений между ИТС является асинхронной. Синхронный обмен сообщениями в общем случае является частным случаем асинхронного обмена [321].

Результаты анализа показывают, что наиболее полные определения ЛП и РП изложены в работе [321]. Однако для решения рассматриваемой задачи определение ЛП требует дополнительного учета потоков управления и данных [20], а определение РП требует следующих уточнений:

- каждый ЛП в некотором состоянии РП может находиться только в одном состоянии;
- в структуре множества переходов РП рассматриваются только те переходы ЛП, которые связанны с событиями передачи и приема сообщений и тем самым способны оказать влияние на другие ЛП.

Исходя из этого, предлагаются следующие определения ЛП и РП.

Определение 1. **Локальным процессом** будем называть семерку вида

$$al = < Z, I, \vdash_{\mathrm{i}}, \vdash_{\mathrm{s}}, \vdash_{\mathrm{r}}, AP, L >, \qquad (5)$$

где Z – конечное непустое множество состояний;

I – множество начальных состояний;

$\vdash_{\mathrm{i}}$ – отношение на множестве $Z \times Z$;

$\vdash_{\mathrm{s}}$ и $\vdash_{\mathrm{r}}$ – отношения на множестве $Z \times \Xi \times Z$;

$\Xi = \{m_\xi\}$ – конечное непустое множество сообщений с уникальной семантикой, $\xi = 1...|\Xi|$;

AP – конечное непустое множество информационных элементов сообщений, используемых ЛП;

L: $Z \to 2^{AP}$ – функция меток состояний (сообщений), сопоставляющая каждому состоянию (сообщению) ЛП множество информационных элементов, используемых (обрабатываемых, передаваемых или ожидающих обработки) в этом состоянии (сообщении).

Отношения $\vdash_{\mathrm{i}}$, $\vdash_{\mathrm{s}}$ и $\vdash_{\mathrm{r}}$ представляют переходы между состояниями, связанные с внутренними событиями, с передачей и приемом сообщений, соответственно. Отношение $\vdash$ на Z определяется соотношением

$$\forall z \in Z \left(\begin{array}{c} \left(z \vdash z' \Leftrightarrow < z, z' > \in \vdash_{\mathrm{i}} \right) \vee \left(\exists m_\xi \in \Xi \right) \\ \left(< z, m_\xi, z' > \in \vdash_{\mathrm{s}} \cup \vdash_{\mathrm{r}} \right) \end{array} \right), \qquad (6)$$

где $<\ldots>$ – упорядоченное множество (кортеж);

$\Leftrightarrow$ – логическая эквивалентность.

Сообщение ЛП описывается следующим образом:

$$L(m_\xi) = \{\varphi_{\xi,v}\} : \varphi_{\xi,v} \in AP_\xi;\ AP_\xi \subseteq AP; v \in 1...\left|AP_\xi\right|, \qquad (7)$$

где $\varphi_{\xi,v}$ – v-й информационный элемент, передаваемый в ξ-м сообщении;

AP_ξ – множество информационных элементов, передаваемых в ξ-м сообщении;

$|\ldots|$ – число элементов множества.

Распределенный процесс R функционирования системы ИТС описывает взаимодействие ЛП, которые выполняются на S ИТС, входящих в рассматриваемую АС, и S' ИТС других АС, с которыми может взаимодействовать рассматриваемая система по схеме 1 : s, (j=1...$|AL_s|$, $AL_s \subseteq AL$, s =1...$|S|+|S'|$).

Определение 2. **Распределенным процессом** будем называть четверку следующего вида:

$$R = (C_{\text{сост}}, C_{\text{пер}}, C_{\text{нач}}, \Xi), \tag{8}$$

где $C_{\text{сост}} = \{c_r\}$: $r=1...|C|$ – конечное непустое множество состояний в R;

$C_{\text{пер}} = \{<C_g, C_{g'}>_l\} \cup \{<C_v, C_{v'}>_f\}$, g, g', v, $v' \le r$, $g \ne g'$, $v \ne v'$ – конечное непустое множество **прямых** $\{<C_g, C_{g'}>_l\}$ и **опосредованных** $\{<C_v, C_{v'}>_f\}$ **переходов** между состояниями R;

$C_{\text{нач}} = \{c_{g''}\}$: $g'' < r$ – конечное множество начальных состояний R, в которые нет переходов;

Ξ – конечное непустое множество сообщений с уникальной семантикой.

Каждое состояние в R является совокупностью таких состояний всех ЛП всех ИТС, для которых одному состоянию, предшествующему некоторому исходящему сообщению одного ЛП одного ИТС с некоторой семантикой, соответствует множество состояний множества ЛП множества ИТС, получающих сообщение с этой же семантикой. При этом один и тот же ЛП в некотором ИТС не может передавать сообщение сам себе. Элементы множества C предлагается описывать следующим образом:

$$\begin{gathered} c_r = < z_{s,j,k}, m_\xi, \{z_{s',j',k'}\} >: \\ \forall s, s' = 1...|S| + |S'|, \forall j, j', h = 1...|AL_s|, \forall k, k' = 1...|Z_{s,j}|, \forall m_\xi \in \Xi \\ \left(< z_{s,j,k}, m_\xi, z'_{s,j,k} > \in \vdash_{\text{s}} \wedge < z_{s',j',k'}, m_\xi, z'_{s',j',k'} > \in \vdash_{\text{r}} \right), \\ \left((al_{s,j} \ne al_{s,h}) \wedge (j \ne h) \right), \\ \left((z_{s,j,k} \in Z_{s,j}), (z_{s,j,k} \ne z_{s',j',k'}) \wedge (s = s') \wedge (j = j') \right). \end{gathered} \tag{9}$$

Из некоторого состояния R существует **прямой переход** во все состояния R, у которых состояния ЛП, порождающие исходящие сообщения, без промежуточных входящих сообщений следуют за состоянием, порождающим исходящие сообщения в данном состоянии R, или состояниями, получающими входящее сообщение в данном состоянии R. Прямой переход предлагается описывать следующим образом:

$$\begin{gathered} < C_g, C_{g'} >_l = \left\langle < z_{s,j,k}, m_\xi, \{z_{s',j',k'}\} >, < \hat{z}_{\hat{s},\hat{j},\hat{k}}, m_{\hat{\xi}}, \{\hat{z}_{\hat{s}',\hat{j}',\hat{k}'}\} > \right\rangle: \\ \forall s, \hat{s}, s' = 1...|S| + |S'|, \forall j, \hat{j}, j' = 1...|AL_s|, \forall k, \hat{k}, k' = 1...|Z_{s,j}|, \forall \xi, \hat{\xi} = 1...|\Xi| \\ \left((s = \hat{s}) \wedge (j = \hat{j}) \wedge \left(< z_{s,j,k}, m_\xi, \hat{z}_{\hat{s},\hat{j},\hat{k}} > \in \vdash_{\text{s}} \right) \right) \vee \\ \vee \left((s' = \hat{s}) \wedge (j' = \hat{j}) \wedge \left(< z_{s',j',k'}, m_{\hat{\xi}}, \hat{z}_{\hat{s},\hat{j},\hat{k}} > \in \vdash_{\text{r}} \right) \right). \end{gathered} \tag{10}$$

Из некоторого состояния R существует **опосредованный переход** во все состояния R, у которых состояния ЛП, порождающие исходящие сообщения, через одно входящее сообщение следуют за состоянием, порождающим исходящие сообщения в данном состоянии R, или состояниями, получающими входящее сообщение в данном состоянии R. Опосредованный переход предлагается описывать следующим образом:

$$\begin{gathered} < C_v, C_{v'} >_f = \left\langle < z_{s,j,k}, m_\xi, \{z_{s',j',k'}\} >, < \hat{z}_{\hat{s},\hat{j},\hat{k}}, m_{\hat{\xi}}, \{\hat{z}_{\hat{s}',\hat{j}',\hat{k}'}\} > \right\rangle: \\ \forall s, \dot{s}, \hat{s} = 1...|S| + |S'|, \forall j, \dot{j}, \hat{j} = 1...|AL_s|, \forall k, \dot{k}, \hat{k} = 1...|Z_{s,j}|, \forall \xi, \xi' = 1...|\Xi| \end{gathered} \tag{11}$$

$$\Big((s=\dot{s}=\hat{s})\wedge(j=\dot{j}=\hat{j})\wedge(<z_{s,j,k},m_{\xi},\dot{z}_{\dot{s},\dot{j},\dot{k}}>\in\vdash_{s})\wedge(<\dot{z}_{\dot{s},\dot{j},\dot{k}},m_{\xi'},\hat{z}_{\hat{s},\hat{j},\hat{k}}>\in\vdash_{r})\Big)\vee$$
$$\vee\Big((s=\hat{s})\wedge(j=\hat{j})\wedge(<z_{s',j',k'},m_{\xi'},\hat{z}_{\hat{s},\hat{j},\hat{k}}>\in\vdash_{r})\Big).$$

Для определения элементов состояний РП предлагается представлять ЛП в редуцированной форме. Редукцию предлагается проводить по следующему правилу: каждая последовательность элементов ЛП, начинающаяся после приема (передачи) сообщения и заканчивающаяся перед приемом (передачей) сообщения, заменяется соответствующим этой последовательности состоянием.

Рассмотрим пример фрагмента структуры ВФ в условиях КА на ИТС, показанный на рис. 10. В нем два ЛП выполняются в ИТС № 1 и по одному в ИТС № 2 и ИТС № 3. Редукция ЛП для информационного взаимодействия ИТС в этом фрагменте показана на рис. 11. Взаимодействие ЛП в рассматриваемой АС и соответствующий этой системе РП показаны на рис. 12. В блоках и узлах схем и полученных из них графов на рис. 11 показаны идентификаторы состояний ЛП ИТС (например, $z_{1,1,1}$) и в фигурных скобках приведены перечни соответствующих этим состояниям информационных элементов (для $z_{1,1,1}$ это $\{p, c, v, a\}$).

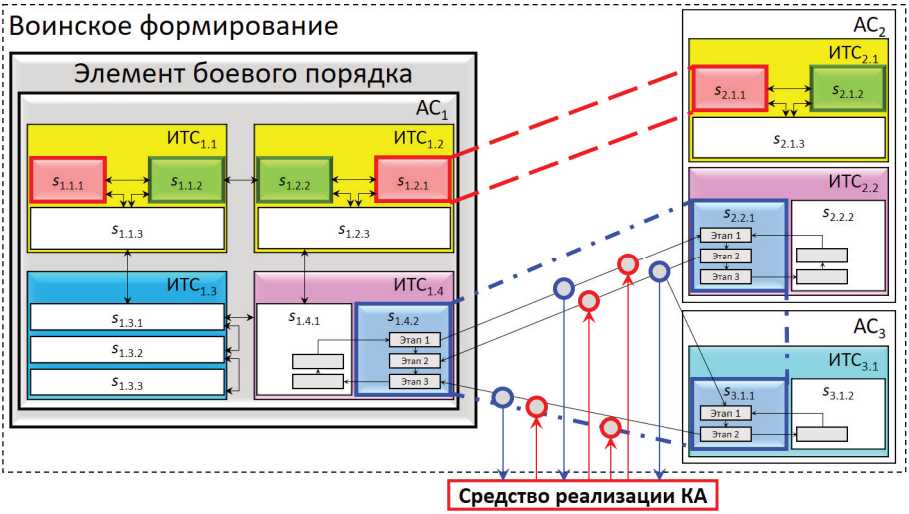


Рис. 10. Фрагмент структуры воинского формирования в условиях кибератак на информационно-технические средства его автоматизированных систем

Такое представление процесса информационного взаимодействия ИТС АС позволяет установить границы интервалов своевременности доставки каждого сообщения (**рассматриваемого сообщения**) в каждом ЛП следующим образом:

- «своевременно» ($\Delta t_{\text{св}} = [t(m_{\xi}), t(m_{\xi}) + \Delta t_{\min}]$) – с момента $t(m_{\xi})$ фиксации средством объективного контроля (далее по тексту – фиксации) передачи сообщения в одном из состояний РП, из которого существует *прямой переход* в состояние РП с передачей **рассматриваемого сообщения**, до момента окончания временного интервала отправки сообщения $\Delta t_{\min}$;

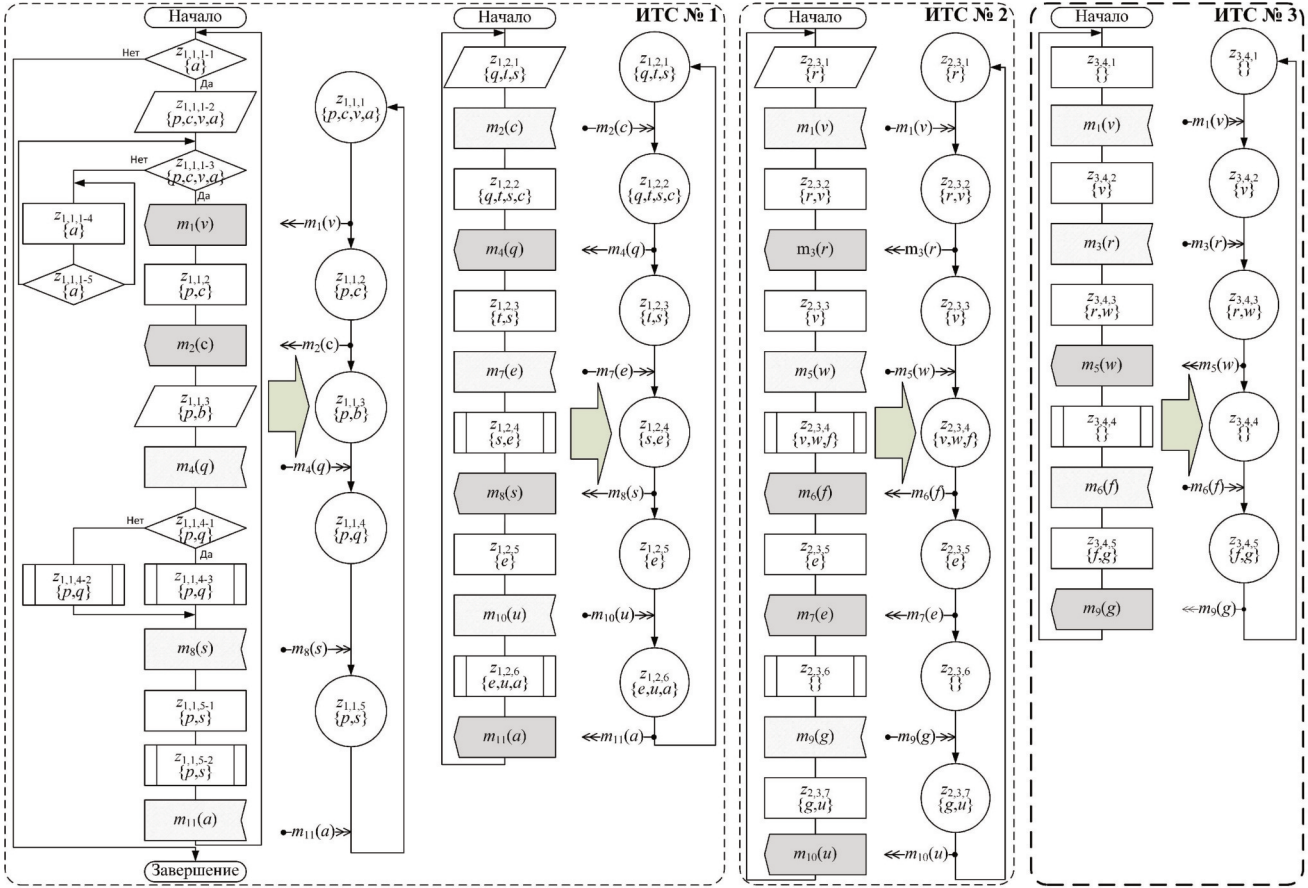


Рис. 11. Редукция локальных процессов в информационно-технических средствах автоматизированных систем (пример)

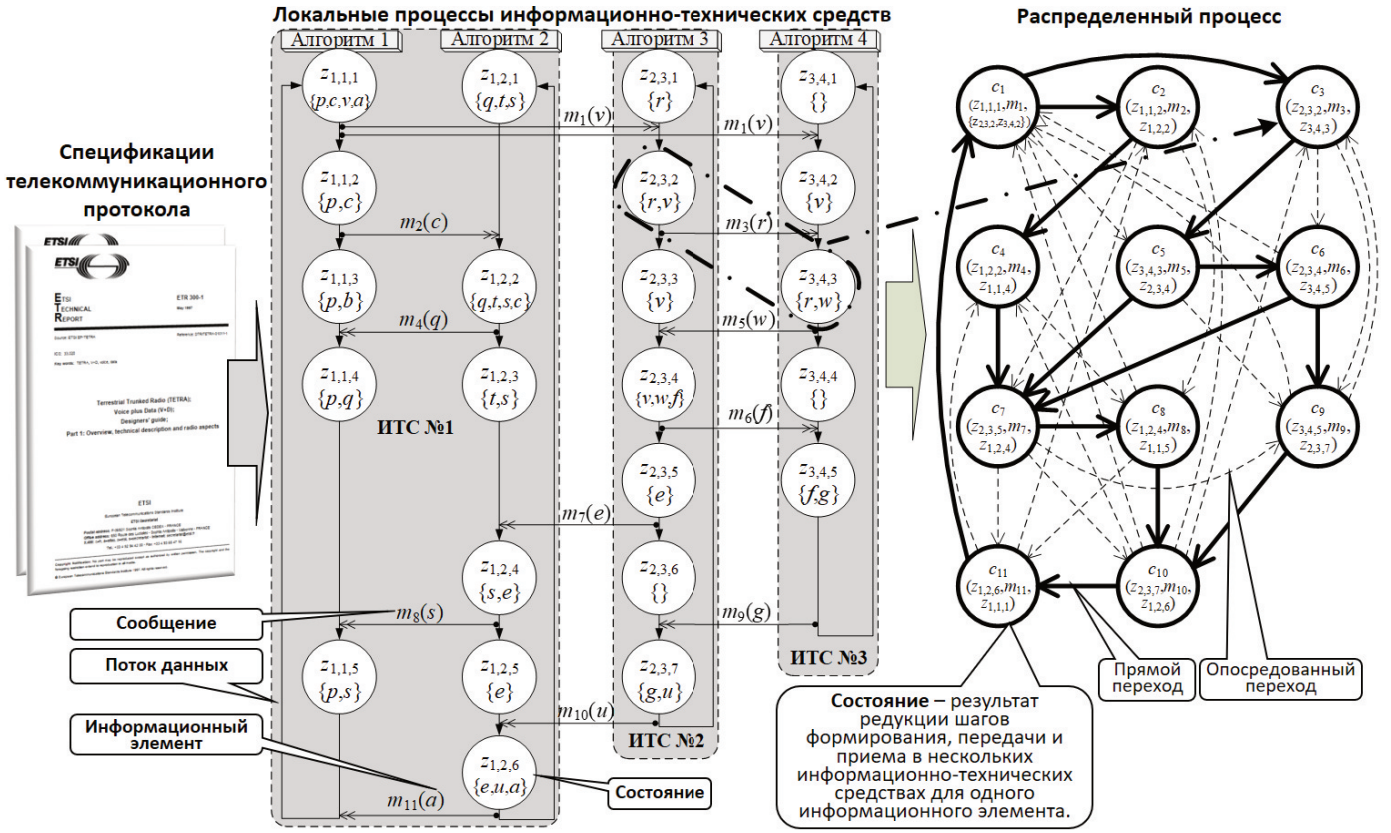


Рис. 12. Общая последовательность преобразования локальных процессов информационно-технических средств в распределенный процесс

- «раньше» ($\Delta t_{\succ} = [t(m_{\xi'}), t(m_{\xi''})]$) – с момента $t(m_{\xi'})$ фиксации передачи сообщения в состоянии РП, из которого существует *опосредованный переход* в состояние РП, в котором передается **рассматриваемое сообщение**, до момента $t(m_{\xi''})$ фиксации передачи сообщения в состоянии РП, из которого существует *прямой переход* в состояние РП с передачей этого сообщения;
- «позже» ($\Delta t_{\prec} = [t(m_{\xi'''}), t(m_{\xi'''}) + \Delta t_{\text{wait}}]$) – с момента $t(m_{\xi'''})$ фиксации передачи сообщения в одном из состояний РП, из которого существует *прямой переход* в состояние РП с передачей **рассматриваемого сообщения**, до момента окончания интервала Δt_{wait}, в течение которого сообщение в ИТС ожидается.

Практические аспекты создания таких моделей приведены в параграфе 2.3.

Таким образом, предложенная модель процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола в отличие от моделей, изложенных в [69, 282, 321], в которых воспроизводится процесс условного синхронного информационного взаимодействия нескольких пространственно распределенных ИТС, учитывает асинхронность передачи сообщений между ИТС. Это достигается за счет воспроизведения данного процесса в виде двух взаимодействующих страт, одна из которых воспроизводит теоретико-множественное представление ориентированных графов частных локальных процессов функционирования ИТС, учитывающих прием и отправку сообщений, и инициализирует на второй страте процесс информационного взаимодействия этих средств в дискретно-событийном виде, в котором каждое состояние – это результат редукции в нескольких ИТС этапов формирования, передачи и приема одного информационного элемента, актуального для рассматриваемой процедуры протокола, а переход между состояниями – это результат редукции последовательности шагов процесса функционирования ИТС, являющегося общим для связываемых этим переходом состояний, начиная с отправки/получения сообщения до отправки этим средством другого сообщения без промежуточных входящих сообщений или через одно входящее сообщение. В результате предлагаемая модель позволяет определить границы временных интервалов легитимной и реализуемой в КА отправки сообщений между ИТС в соответствии с известной процедурой телекоммуникационного протокола.

Роль модели, предлагаемой в настоящем параграфе, в настоящем исследовании состоит в том, что она формализует процедуры телекоммуникационных протоколов на канальном и вышестоящих уровнях ЭМВОС в наиболее общем виде с учетом временных параметров процессов функционирования взаимодействующих ИТС и информационных элементов сообщений, которыми эти ИТС обмениваются.

Эта модель необходима для разработки способов реализации КА, которые учитываются в моделях СЦР более высоких уровней абстракции (обычно на уровне марковских процессов), позволяющих оценить эффективность КА или мер защиты от них на уровне показателей эффективности таких сетей. Например, в [208, 210] таким показателем является вероятность установления

соединения абонентским терминалом (АТ). Способы реализации КА в таких моделях задаются эмпирически высококвалифицированными специалистами. Предлагаемая модель дает возможность систематизировать и существенно упростить процесс разработки новых способов.

2.2 Основные положения метода генерации кибератак на телекоммуникационное оборудование

Анализ предметной области. Процесс оценки защищенности ПО АС от КА в научно-методическом аппарате, рассматриваемом в настоящей монографии, состоит из двух фаз:

- фаза проверки соответствия ОПО и СПО требованиям действующих НТД по защите информации, предусматривающая проверку наличия сертифицированных средств защиты информации. Эта фаза регламентирована существующими НТД и в монографии не детализируется;
- фаза проведения практических мероприятий по выявлению уязвимостей ПО, способных привести к нарушению конфиденциальности, целостности и доступности самого ПО и данных, с применением тестовых способов реализации КА. Эта фаза состоит из двух этапов. На первом этапе с применением известных методик (см., например, [138, 169, 170]) исследуются ОПО и СПО ЗУ, ИРЗ и ЗО в части задач разведки и ИТВ, а на втором этапе исследуется СПО ЗО в части задач связи. Задача навигационно-временного обеспечения в этом контексте рассматривается как задача связи, осуществляемой в симплексном режиме.

В настоящей монографии детализируется второй этап второй фазы процесса оценки защищенности ПО АС от КА, поскольку актуальной с научной и практической точек зрения является на сегодняшний день именно его проработка.

Несмотря на очевидную актуальность задачи оценки защищенности ПО АС, а также на наличие отечественных и международных НТД, описывающих уязвимости ИТС (например, ГОСТ [93]), существование ежедневно пополняемых баз данных уязвимостей (например, [17]), многочисленных учебных пособий по информационной безопасности (например, [65, 78, 106, 135, 171, 194]) и научных трудов по тематике КА на ИТС (например, [190, 192, 197, 275]) вопросу непосредственной разработки тестовых способов реализации КА на ИТС в литературе уделяется мало внимания по следующим причинам:

- высокой опасности придания огласке механизмов дестабилизации АС;
- относительной молодости современных компьютерных технологий, научное обоснование комплексного применения которых значительно отстает от темпов развития и совершенствования инструментария КА;
- значительной сложности современных АС как объектов системного анализа на предмет выявления максимально возможного числа уязвимостей.

Как отмечено в параграфе 1.2, основным методом выявления уязвимостей телекоммуникационных протоколов традиционно являлся **эмпирический**,

основанный на предположении аналитиками уязвимостей в ИТС и проверке этих предположений путем формирования и реализации соответствующих тестовых способов реализации КА. Однако этот метод не гарантирует положительного результата в течение длительного периода исследований. Для парирования такой ситуации автором совместно с М.А. Перегудовым проработан вопрос систематизации разрабатываемых в рамках эмпирического подхода способов реализации КА на основе моделей процесса функционирования СЦР, позволяющих оценить эффективность этих способов. В результате на базе классических моделей процесса функционирования СЦР Л. Клейнрока [134], A.B. Carleial [281], Y. Onozato [314], N. Abramson [277], H. Kobayashi [303] разработан комплекс взаимоувязанных моделей процесса функционирования процедур случайного множественного доступа к среде типа S-ALOHA [208, 210], процедур синхронизации АТ со средством контроля и управления сети, хэндовера, управления мощностью [209] и зарезервированного доступа к среде [207], характерных для канального уровня современных СЦР. Однако, несмотря на возможность значительно расширить номенклатуру действительно эффективных способов реализации КА на ИТС, оказалось, что этот научно-методический аппарат имеет следующие недостатки:

- требует очень высокого уровня квалификации эксперта-аналитика;
- не позволяет разрабатывать новые способы реализации КА, поскольку модель СЦР формируется и уточняется только с учетом способов, уже полученных ранее с применением **эмпирического** метода.

Следует также отметить, что, как уже было ранее указано в параграфе 1.1, применить методологию **синтеза активных имитирующих помех** [224], которая широко применяется в РЭБ, для разработки тестовых способов реализации КА оказалось невозможно. Причина этого состоит в следующем.

Данная методология оперирует статистическими характеристиками частотных, амплитудных, фазовых, пространственных и временных параметров помеховых и полезных сигналов на физическом уровне ЭМВОС, которые в соответствии со стандартом связи должны приниматься одинаково всеми приемниками РЭС этого стандарта, разрабатываемыми различными производителями. Это дает возможность применять для синтеза помех метод максимального правдоподобия, оперирующий усредненными параметрами сигналов. В то же время на канальном и вышестоящих уровнях ЭМВОС, на которых применяются КА, значение имеют не усредненные статистические характеристики сигналов, а параметры точности (синтаксические и семантические), кратности и своевременности доставки конкретных разнотипных сообщений, регламентированных используемыми в АС телекоммуникационными протоколами и применяющихся в различном сочетании в разных процедурах этих протоколов. При этом программы обработки одинаковых сообщений одного и того же протокола в образцах АС отдельных разработчиков реализуются по-разному и, соответственно, содержат свои уникальные уязвимости, которые используются в КА. Это обусловлено высоким уровнем конкуренции организаций-разработчиков ПО, из-за которого сформировать единую базу данных безопасного ПО пока

невозможно не только в мировом масштабе, но даже на уровне министерства обороны отдельной страны. Поэтому метод максимального правдоподобия для разработки тестовых способов реализации КА не применим.

Как следствие, изложенные в п. 1.2.1 результаты анализа известных методов исследования телекоммуникационных протоколов, а также указанные выше недостатки свидетельствуют о том, что создание на основе базового **метода выборочного тестирования** узкоспециализированного метода генерации КА на телекоммуникационное оборудование является актуальной научной задачей.

Ключевая идея метода: сформировать необходимое (в смысле полноты учитываемых параметров передачи сообщений) и достаточное (в смысле безызбыточной проверки сочетаний параметров передачи сообщений, позволяющей реализовать их при проведении предварительных или государственных испытаний) множество тестовых способов реализации КА на телекоммуникационное оборудование на основе доступной информации об их алгоритмах функционирования возможно путем комбинаторного сочетания параметров своевременности доставки, кратности передачи и точности содержания сообщений, регламентируемых телекоммуникационным протоколом. Содержание метода показано на рис. 13.

В основе базового **метода выборочного тестирования** лежит рассмотрение любой величины (например, размер буферной памяти, значение переменной программы) в поле ее ожидаемых значений, когда рассматриваются пять основных вариантов: точное среднестатистическое значение, точные значения на нижней и верхней границах, неточное значение меньше нижней и больше верхней границы, а также вне поля ожидаемых значений (например, буквы вместо цифр) (см. рис. 14) [20, 131]. Значения вне поля ожидаемых значений в ряде источников приравниваются к неточным.

За основу при разработке тестовых способов реализации КА целесообразно брать не только точность используемых величин, как это показано на рис. 14, но и кратность передачи сообщений, а также их своевременность, определяемую с применением модели процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола, предложенной в параграфе 2.1.

Существуют три варианта наборов исходных данных для создания тестовых способов реализации КА [41]:

- **полевой набор**, когда доступны образцы ИТС. Позволяет вскрыть уязвимости отдельных образцов ИТС. При этом алгоритмы информационного взаимодействия ИТС выявляются на основе эксплуатации этих средств;
- **фолиантный набор**, когда доступна спецификация целевого ИТС. Этот набор позволяет определить потенциальные уязвимости целого класса ИТС;
- **лабораторный набор** – представляет собой комбинацию фолиантного и полевого наборов, значительно расширяющую возможности по выявлению уязвимостей ИТС.

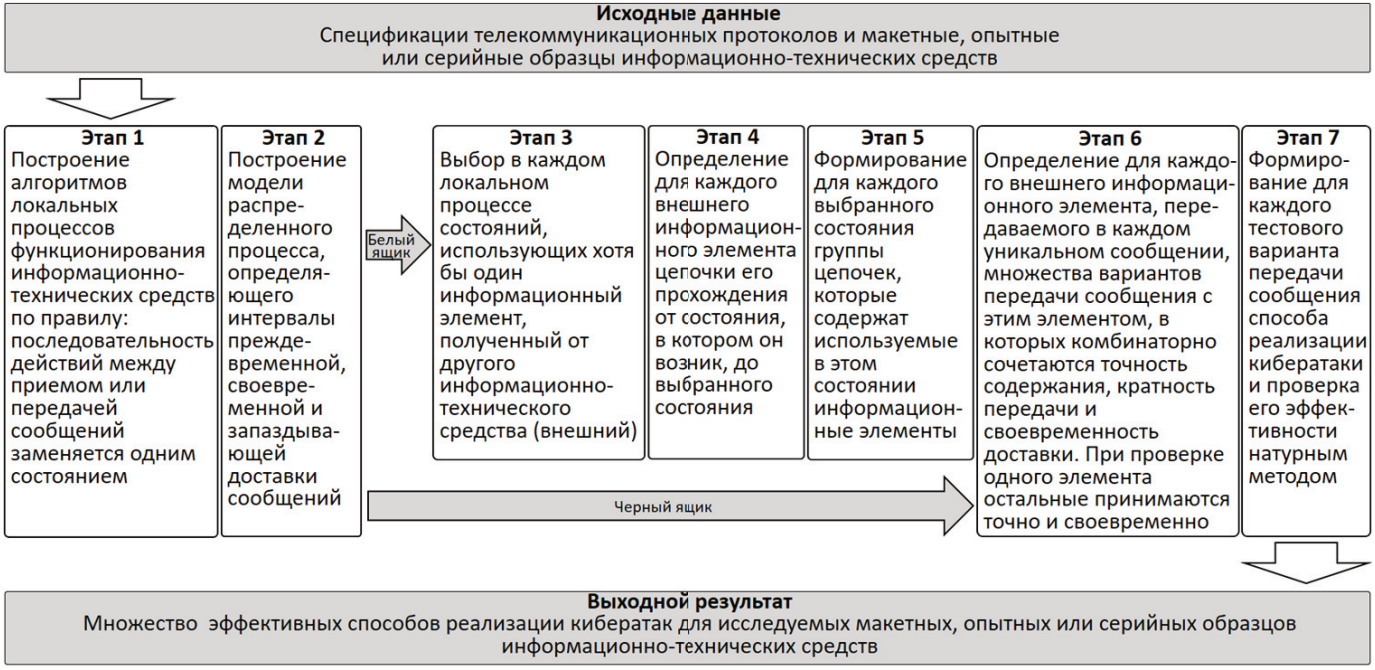


Рис. 13. Содержание метода генерации кибератак на телекоммуникационное оборудование

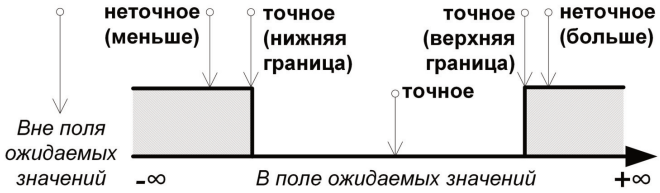


Рис. 14. Варианты рассмотрения величин в тестировании

Рассматриваемый метод использует лабораторный набор исходных данных. В методе предлагается использовать следующие базисные параметры сообщений, на которые оказывают влияние КА, показанные на рис. 15.

1. **Точность содержания** данных, передаваемых в сообщениях, которые могут соответствовать, быть больше или меньше граничных значений, равны им и могут быть согласно ГОСТу [97] *прецизионными* (входить в интервал прецизионности) и *правильными* (не в интервале прецизионности, но входить в интервал правильности). Этот базисный параметр, исходя из специфики процедуры телекоммуникационного протокола, может быть определен на любой шкале измерений: наименований, порядка, интервалов или отношений.

Например, в информационном элементе сообщения предусмотрено использование множества строго определенных битовых последовательностей, то есть используется шкала наименований (наиболее распространенный в практике случай). В этом примере правильным будет любое значение из этого множества кроме прецизионных, а прецизионным (но не точным!) будет значение, которое в рассматриваемой процедуре телекоммуникационного протокола является равноправной альтернативой точному значению. То есть точное и прецизионное значения обрабатываются одной веткой программной реализации соответствующего алгоритма функционирования ИТС.

В случае использования шкалы интервалов, например, при передаче температуры контролируемого объекта, правильным может быть любое непрецизионное значение из установленного спецификацией протокола диапазона, а прецизионным может быть значение, которое в текущий момент времени не воспринимается алгоритмом в качестве некорректного. То есть значения границ интервала прецизионности должны в явном виде присутствовать в спецификации протокола. Их отсутствие в спецификации, очевидно, является критической уязвимостью защищаемой автоматизированной системы. Стоит отметить, что известный вирус «Win32/Stuxnet», поразивший объекты ядерной энергетики Ирана в 2010 году [172, 230], по всей видимости, именно за счет незначительного изменения в пределах интервала прецизионности параметров работы центрифуг для обогащения уранового топлива за несколько месяцев привел эти центрифуги к критическому состоянию.

Также базисный параметр точности содержания данных включает позицию «вне поля ожидаемых значений». Необходимость учета этой позиции обусловлена тем, что в ряде случаев информационные элементы сообщений, отправляемых в процессе КА, могут содержать, например, строковые значения вместо числовых и т.д. Такая особенность актуальна в основном для исследова-

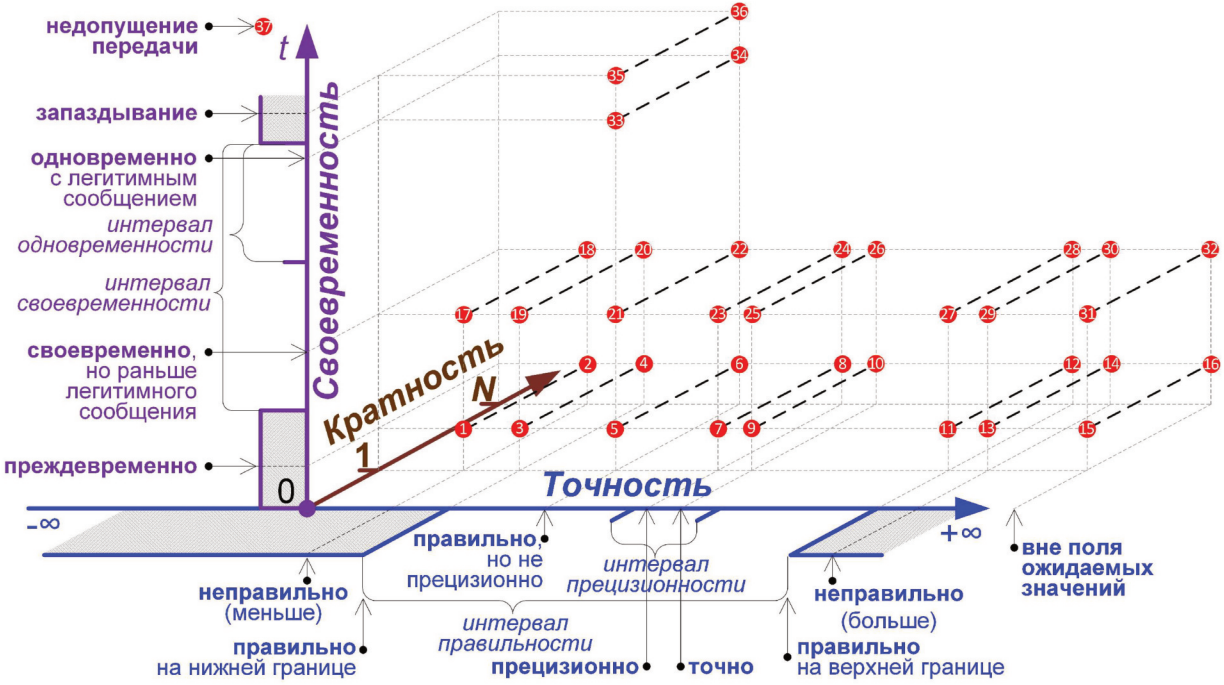


Рис. 15. Пространство вариантов передачи сообщения в тестовых способах реализации кибератак

ния защищенности протоколов представительского уровня ЭМВОС (например, от атак типа «SQL-injection»). Для низших уровней ЭМВОС она избыточна, так как они оперируют единым бинарным типом данных.

2. **Своевременность доставки**. В ЛП функционирования ИТС согласно модели, рассмотренной в параграфе 2.1, сообщения принимаются «своевременно», «раньше» и «позже».

3. **Кратность передачи**. Эффекты от единичной и *N*-кратной реализации тестовых способов реализации КА на практике существенно различаются. Значение *N* определяется на основе результатов анализа спецификации телекоммуникационного протокола и по умолчанию принимается равным ∞, то есть осуществляется так называемое «зацикливание способа».

Для разработки тестовых способов реализации КА на ИТС в методике сначала разрабатываются модели ЛП и РП исследуемого ИТС согласно правилам, изложенным в параграфе 2.1. Далее выполняются следующие действия.

Шаг 1. Фиксировать в каждом ЛП всех ИТС множество состояний $\Psi_{s,j}=\{z_{s,j,q}\}$, непосредственно использующих информационные элементы из ЛП других ИТС:

$$\begin{gathered}\forall s' \neq s : s, s' = 1...|S| + |S'|, \forall m_\xi \in \Xi, \forall j, j' = 1...|AL_s|, \forall q, k, k', l, l' = 1...|Z_{s,j}| \\ \exists z_{s,j,q} \in Z_{s,j} : \begin{pmatrix} (L(z_{s,j,q}) \cap L(m_\xi) \neq \varnothing) \wedge (< z_{s',j',k'}, m_\xi, z_{s,j,k} > \in \vdash_{\mathrm{r}}) \wedge \\ \wedge (< z_{s,j,k}, z_{s,j,l} >, ..., < z_{s,j,l'}, z_{s,j,q} > \in \vdash_{\mathrm{i}}) \end{pmatrix}.\end{gathered} \tag{12}$$

Шаг 2. Определить для каждого зафиксированного состояния множество цепочек из состояний ЛП, описывающих путь информационного элемента от состояния, в котором он возник, до состояния, в котором использован:

$$\begin{gathered}\forall s, s' = 1...|S| + |S'| \wedge (s' \neq s), \forall j, j' = 1...|AL_s|, \\ \forall m_\xi \in \Xi, \forall k, k', l, l' = 1...|Z_{s,j}|, \forall q \leq |Z_{s,j}| \\ \sigma_{s,j,q} = z_{s',j',k'} \# ... \# z_{s,j,k} \# ... \# z_{s,j,q} : \\ (< z_{s,j,k}, z_{s,j,l} >, ..., < z_{s,j,l'}, z_{s,j,q} > \in \vdash_{\mathrm{i}}) \wedge \\ \wedge (L(z_{s',j',k'}) \cap ... \cap L(z_{s,j,k}) \cap L(z_{s,j,q}) \cap L(m_\xi) \neq \varnothing) \wedge \\ \wedge (< z_{s',j',k'}, m_\xi, z_{s,j,k} > \in \vdash^{\mathrm{r}}),\end{gathered} \tag{13}$$

где # – знак конкатенации (лат. *concatenatio* – сцепление) элементов в цепочке.

Шаг 3. Выделить для каждого зафиксированного на **шаге 2** состояния множество цепочек, содержащих используемые в нем информационные элементы:

$$\begin{gathered}\forall \psi, \psi' = 1...|\pi_{s,j,q}| \wedge (\psi \neq \psi'), \forall s = 1...|S| + |S'|, \forall j = 1...|AL_s|, \forall q \leq |Z_{s,j}| \\ \pi_{s,j,q} = \{\sigma_{s,j,q,\psi}\} : \sigma_{s,j,q,\psi} \neq \sigma_{s,j,q,\psi'}.\end{gathered} \tag{14}$$

Шаг 4. Определить для каждого выделенного на **шаге 3** множества цепочек по одной группе тестовых способов реализации КА $sp_{s,j,q}$, включающей для каждой цепочки из множества $\pi_{s,j,q}$ все варианты $\theta_{s,j,q,\psi,\gamma}$ передачи сообщений.

Оценка защищенности СПО от КА состоит в определении разности единицы и частного от деления количества способов, натурный эксперимент реализации которых доказал их эффективность, к общему количеству разработанных тестовых способов. Варианты передачи сообщения в каждом тестовом способе реализации КА представлены в таблице 2.

Таблица 2 — Варианты тестовых способов реализации кибератак

Параметры сообщений		Номер тестового способа γ
Своевременность	Точность	
Своевременно	Точно	1
	Прецизионно	2
	Правильно, но не прецизионно	3
	На нижней границе интервала своевременности	4
	На верхней границе интервала своевременности	5
	Выше верхней границы интервала своевременности	6
	Ниже нижней границы интервала своевременности	7
	Вне поля ожидаемых значений	8
Раньше	Точно	9
	Прецизионно	10
	Правильно, но не прецизионно	11
	На нижней границе интервала своевременности	12
	На верхней границе интервала своевременности	13
	Выше верхней границы интервала своевременности	14
	Ниже нижней границы интервала своевременности	15
	Вне поля ожидаемых значений	16
Одновременно	Правильно, но не прецизионно	17
Позже	—	18
Недопущение передачи	—	19

В таблице 2 для вариантов, соответствующих значениям γ = 1…18 и предполагающих однократную реализацию, дополнительно рассматриваются варианты, предполагающие *N*-кратную реализацию. Количество способов, ориентированных на один информационный элемент, равно 37.

Группа тестовых способов реализации КА определяется по формуле:

$$\forall s = 1...|S| + |S'|, \forall j = 1...|AL_s|, \forall q \le |Z_{s,j}|, \forall \psi = 1...|\Delta_{s,j,q}|, \forall \gamma = 1...37$$

$$sp_{s,j,q} = \bigcup \left(\begin{array}{l} \bigcup_{\gamma} <\theta_{s,j,q,1,\gamma}, \theta_{s,j,q,2,1}, ..., \theta_{s,j,q,\psi,1}> \\ \qquad \text{при } \Delta t_{\circ}(\sigma_{s,j,q,1}), \Delta t_{>}(\sigma_{s,j,q,1}), \Delta t_{<}(\sigma_{s,j,q,1}), \\ \bigcup_{\gamma} <\theta_{s,j,q,1,1}, \theta_{s,j,q,2,\gamma}, ..., \theta_{s,j,q,\psi,1}> \\ \qquad \text{при } \Delta t_{\circ}(\sigma_{s,j,q,2}), \Delta t_{>}(\sigma_{s,j,q,2}), \Delta t_{<}(\sigma_{s,j,q,2}), \\ \qquad ... \\ \bigcup_{\gamma} <\theta_{s,j,q,1,1}, \theta_{s,j,q,2,1}, ..., \theta_{s,j,q,\psi,\gamma}> \\ \qquad \text{при } \Delta t_{\circ}(\sigma_{s,j,q,\psi}), \Delta t_{>}(\sigma_{s,j,q,\psi}), \Delta t_{<}(\sigma_{s,j,q,\psi}) \end{array} \right). \quad (15)$$

На **шаге 4** по аналогии с подходом NASA к тестированию авионики, изложенным в [294], для недопущения «взрыва» пространства тестируемых состояний при проверке одной цепочки в остальных цепочках принимаются точные и своевременные сообщения. На рис. 15 варианты 1...32 относятся

к информационным элементам в сообщении, а варианты 33…37 относятся к сообщениям как таковым.

Последовательная реализация каждой полученной таким образом совокупности наборов взаимосвязанных параметров сообщений, определяющей содержание группы тестовых способов реализации КА, позволит осуществить поиск ошибок в каждом состоянии ЛП, связанном с обработкой сообщений от всех ЛП других ИТС, и в результате проверить натурным экспериментом возможность приведения ИТС или АС в целом в состояние потери работоспособности, сниженной эффективности функционирования, управляемости или доступности для более глубокого анализа источником КА. В примере, рассмотренном на рис. 11, 12, таким образом представляется возможным получить шесть групп тестовых способов реализации КА. В частности, для состояния $z_{2,3,4}$ имеет место следующая группа способов:

$$
\begin{gathered}
sp_{2,3,1} = (\bigcup\nolimits_{\gamma=1\ldots37} < \theta_{2,3,1,1,\gamma}, \theta_{2,3,1,2,1} >) \cup (\bigcup\nolimits_{\gamma=1\ldots37} < \theta_{2,3,1,1,1}, \theta_{2,3,1,2,\gamma} >) \\
\text{для } \pi_{2,3,1} = (\sigma_{2,3,1,1}, \sigma_{2,3,1,2}) : \sigma_{2,3,1,1} = z_{1,1,1-2} \# z_{1,1,1-3} \# z_{2,3,2} \# z_{2,3,3} \# z_{2,3,4}, \\
\sigma_{2,3,1,2} = z_{3,4,3} \# z_{2,3,4} \text{ при } \Delta t_{\circ}(\sigma_{2,3,1,1}) = [t(m_{11}), t(m_{11}) + \Delta t_{\min}]; \\
\Delta t_{>}(\sigma_{2,3,1,1}) = [t(m_6) \vee t(m_8) \vee t(m_9) \vee t(m_{10}), t(m_{11})]; \\
\Delta t_{<}(\sigma_{2,3,1,1}) = [t(m_{11}), t(m_{11}) + \Delta t_{\text{wait}}]; \\
\Delta t_{\circ}(\sigma_{2,3,1,2}) = [t(m_3), t(m_3) + \Delta t_{\min}]; \\
\Delta t_{>}(\sigma_{2,3,1,2}) = [t(m_1), t(m_3)]; \\
\Delta t_{<}(\sigma_{2,3,1,2}) = [t(m_3), t(m_3) + \Delta t_{\text{wait}}].
\end{gathered}
\tag{16}
$$

Эта группа содержит наборы факторов для информационных элементов «*v*» и «*w*», используемых в состоянии $z_{2,3,4}$. Информационный элемент «*f*», присутствующий в состоянии $z_{2,3,4}$, используется только в состоянии $z_{3,4,5}$ и поэтому в группе $sp_{2,3,1}$ не задействован. В зависимости от исходных данных защищаемую АС можно рассматривать с позиции «белого» или «черного ящика». Фрагменты модели системы для обоих случаев показаны на рис. 16.

Для системы, представляемой в виде «белого ящика», возможен анализ всех состояний ЛП каждого ИТС и передаваемых в системе сообщений, а система, представляемая в виде «черного ящика», дает возможность анализировать только передаваемые ИТС сообщения. С учетом этого в виде схемы на рис. 17 показаны этапы разработки необходимого и достаточного множества тестовых способов реализации КА для различных наборов исходных данных.

Важно заметить, что предложенный метод генерации КА на телекоммуникационное оборудование не обязательно должен учитывать параметр своевременности доставки сообщений. Например, в стеке протоколов TCP/IP в протоколе UDP (англ. *User Datagram Protocol* – протокол передачи пользовательских блоков данных) не требуется подтверждение полученного сообщения. Потому проверки своевременности доставки сообщений для этого протокола не требуется. Метод применим к этому протоколу только в части проверки точности содержания и кратности передачи сообщений.

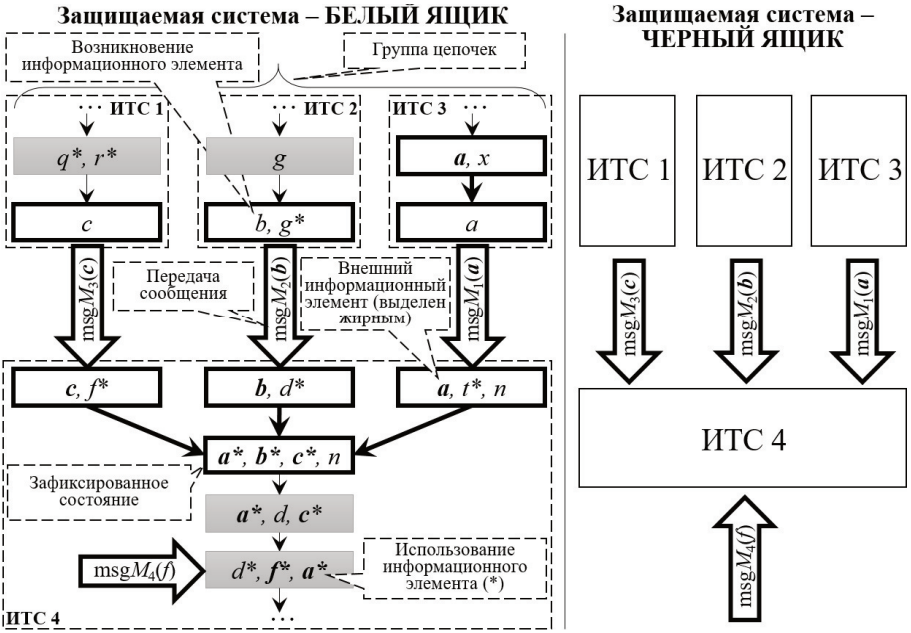


Рис. 16. Фрагмент модели системы

Этап 1. Выполняют построение моделей для всех **локальных процессов** ИТС АС.

Этап 2. Выполняют **редукцию** моделей локальных процессов.

Этап 3. Выполняют построение модели **распределенного процесса**.

Белый ящик

Этап 4. Фиксируют в каждом локальном процессе каждого ИТС состояния, использующие хотя бы один внешний (то есть полученный от другого ИТС) **информационный элемент**.

Этап 5. Определяют для каждого внешнего информационного элемента **цепочку** его прохождения от состояния, в котором он возник (получен, введен), до зафиксированного на **этапе 4** состояния, соответствующего этому элементу.

Этап 6. Формируют для каждого зафиксированного на **этапе 4** состояния **группу цепочек**, которые содержат используемые в этом состоянии информационные элементы.

Этап 7. Определяют для каждого внешнего информационного элемента каждого зафиксированного на **этапе 4** состояния **набор тестовых способов реализации КА**, включающий необходимое и достаточное множество вариантов передачи этого элемента в сообщении. При проверке одной цепочки в остальных цепочках группы принимаются точные и своевременные сообщения.

Черный ящик

Этап 4. Определяют для каждого информационного элемента, передаваемого в каждом уникальном сообщении, **набор тестовых способов реализации КА**, включающий необходимое и достаточное множество вариантов передачи этого информационного элемента в сообщении.

Параметры своевременности сообщений определяют по модели **распределенного процесса**.

Рис. 17. Этапы разработки тестовых способов реализации кибератак

Таким образом, в предлагаемом в настоящем параграфе методе генерации КА на телекоммуникационное оборудование в отличие от методов, изложенных в [20, 131, 310], заключающихся в выборочном тестировании неправильными, неожиданными или случайными данными, дополнительно в тестовых способах

реализации КА учтен фактор своевременности доставки сообщений. Это достигается за счет выбора в алгоритме функционирования каждого из взаимодействующих ИТС таких этапов, на которых происходит прием информации от других ИТС, и генерировании уникальных для этих этапов множеств тестовых наборов сообщений, в каждом из которых (наборе сообщений) только у одного сообщения искажена кратность передачи, точность содержания или своевременность доставки одного информационного элемента.

Метод позволяет осуществить генерацию и экспериментальную проверку множества тестовых способов реализации КА для известных телекоммуникационных протоколов ИТС АС и оценить защищенность СПО задачи связи от КА как долю безуспешно реализованных тестовых способов. Роль метода, рассмотренного в настоящем параграфе, в данном исследовании состоит в том, что на его основе возможно разработать множество ранее неизвестных способов реализации КА, которое является необходимым, так как учитывает все параметры сообщений в телекоммуникационных протоколах (точность, кратность и своевременность), и достаточным, так как исключает избыточность проверки сочетаний параметров передачи сообщений.

2.3 Практические аспекты разработки способов реализации кибератак на телекоммуникационное оборудование

В качестве примера исходных данных для создания способов реализации КА рассмотрим следующие процедуры СЦР:

- процедура инициирования АТ сеанса связи в стандарте DMR в режиме работы с ретранслятором (см. рис. 18) [291]. Форматы сообщений CSBK (англ. *Control Signaling BlocK* – управляющий блок сигнализации) и IDLE (англ. *idle* – свободный), используемых в этой процедуре, и РП этой процедуры показаны на рис. 19;
- процедура установления соединения точки доступа и АТ для передачи данных в стандарте IEEE 802.11 Wi-Fi (см. рис. 20) [297]. Формат сообщения RTS (англ. *Request To Send* – запрос передачи) и РП этой процедуры показаны на рис. 21, где полужирным шрифтом выделены поля, непосредственно задействованные в процедуре.

Учитывая, что в стандартах СЦР двойного назначения используются десятки различных взаимосвязанных процедур, а их описание занимает тысячи страниц преимущественно текстовой информации, в интересах повышения практичности предлагаемого в настоящей главе метода в ходе исследования разработан алгоритм разработки модели процесса информационного взаимодействия ИТС АС с применением процедур, описываемых в спецификации любого стандарта (блок-схема алгоритма показана на рис. 22). Этот алгоритм предусматривает разработку обобщенного графа функционирования анализируемой системы, в котором узлы – выявленные уникальные процедуры, а дуги – возможные переходы между ними. В алгоритме ЛП функционирования ИТС формируются отдельно для каждой уникальной процедуры и отдельно для каждого перехода между процедурами

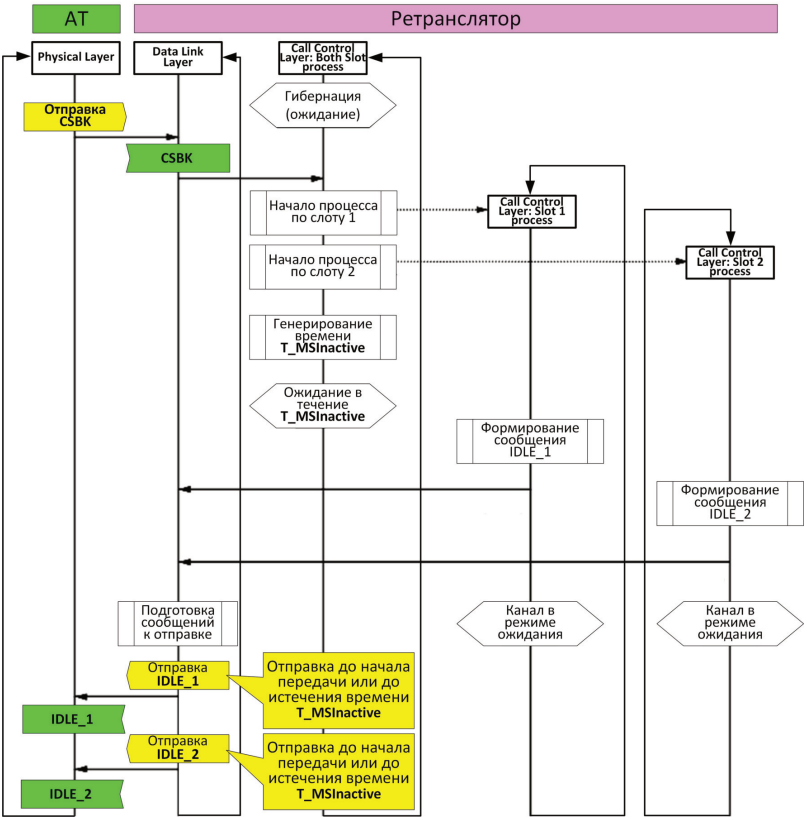
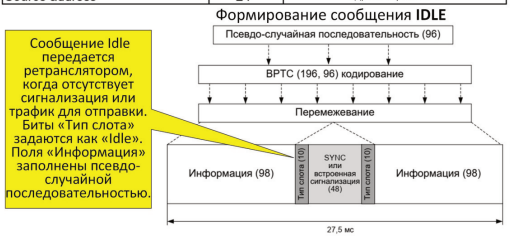


Рис. 18. Процедура инициирования абонентским терминалом сеанса связи в стандарте DMR

Формат сообщения **CSBK**

Информационный элемент	Размер, бит	Описание
Message dependent elements		
Last block (LB)	1	Индикатор последнего блока (должен быть равен 1)
Protect Flag (PF)	1	Флаг защиты (в процедуре не актуален)
Feature elements		
CSBK Opcode (CSBKO)	6	Код операции, содержащийся в сообщении CSBK
Feature set ID (FID)	8	Идентификатор запрашиваемой функции
Reserved	16	Зарезервировано (все нули)
BS address	24	Адрес базовой станции (ретранслятора)
Source address	24	Адрес отправителя



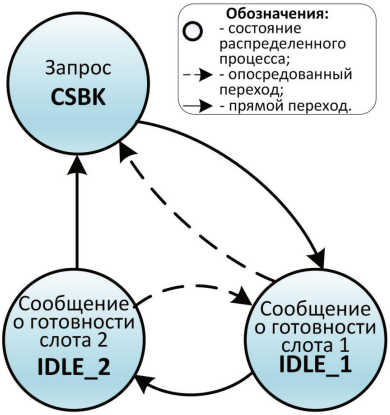


Рис. 19. Формат сообщения CSBK и распределенный процесс инициирования абонентским терминалом сеанса связи в стандарте DMR

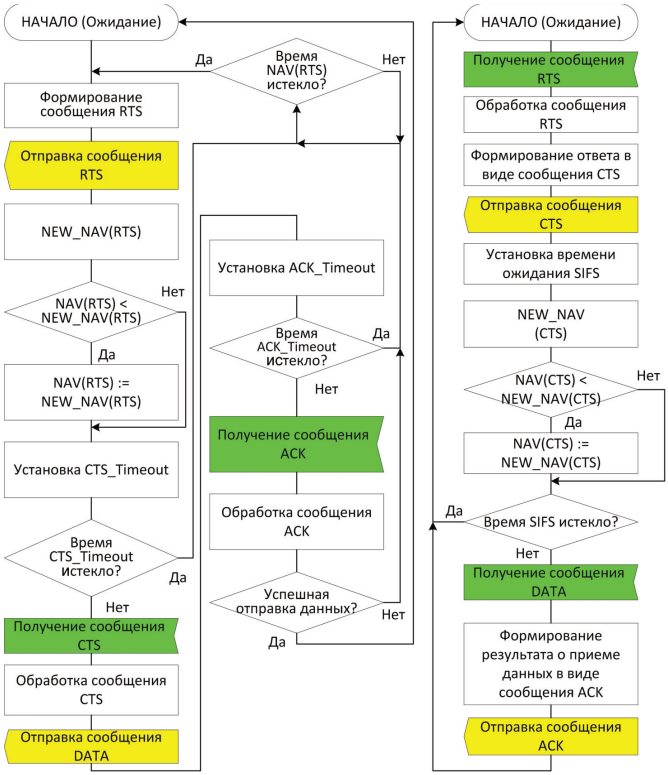


Рис. 20. Процедура установления соединения абонентским терминалом (слева) с точкой доступа (справа) в стандарте IEEE 802.11 Wi-Fi

Формат сообщения **RTS**

Информационный элемент	**Размер, бит**	**Значение**	**Описание**
Protocol Version	2	00_2	Версия протокола 802.11 MAC
Type	**2**	**01_2**	**Тип фрейма MAC**
Subtype	**4**	**1011_2**	**Указывает подтип фрейма**
To/From DS	2	00_2	Кадры между STA
		10_2	Кадр данных, предназначенных для DS
		01_2	Кадр данных от DS к точке доступа
		11_2	Кадр данных, использующий формат заголовка MAC с четырехзначным адресом
More Fragments	1	1_2	Служебный фрейм или фрейм данных
		0_2	Управляющий фрейм
Retry	1	1_2	Повторная передача служебных фреймов и данных
		0_2	В остальных случаях
Power management	1	1_2	STA в режиме PS
		0_2	STA в активном режиме
More data	1	1_2	Данные буферизированы в AP или точке доступа
		0_2	Данные не буферизированы
Protected Frame	1	-	-
Order	1	-	-
Duration	16	-	Время передачи фрейма RTS
Receiver address	48	-	Адрес получателя
Transmitter address	**48**	**-**	**Адрес отправителя**
FSC	32	-	32-битный циклически избыточный код CRC

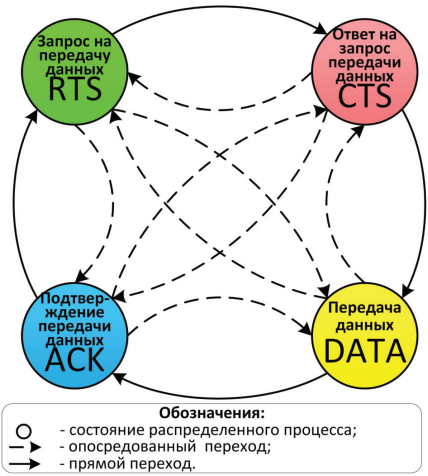


Рис. 21. Формат сообщения RTS и распределенный процесс установления соединения абонентского терминала с точкой доступа в стандарте IEEE 802.11

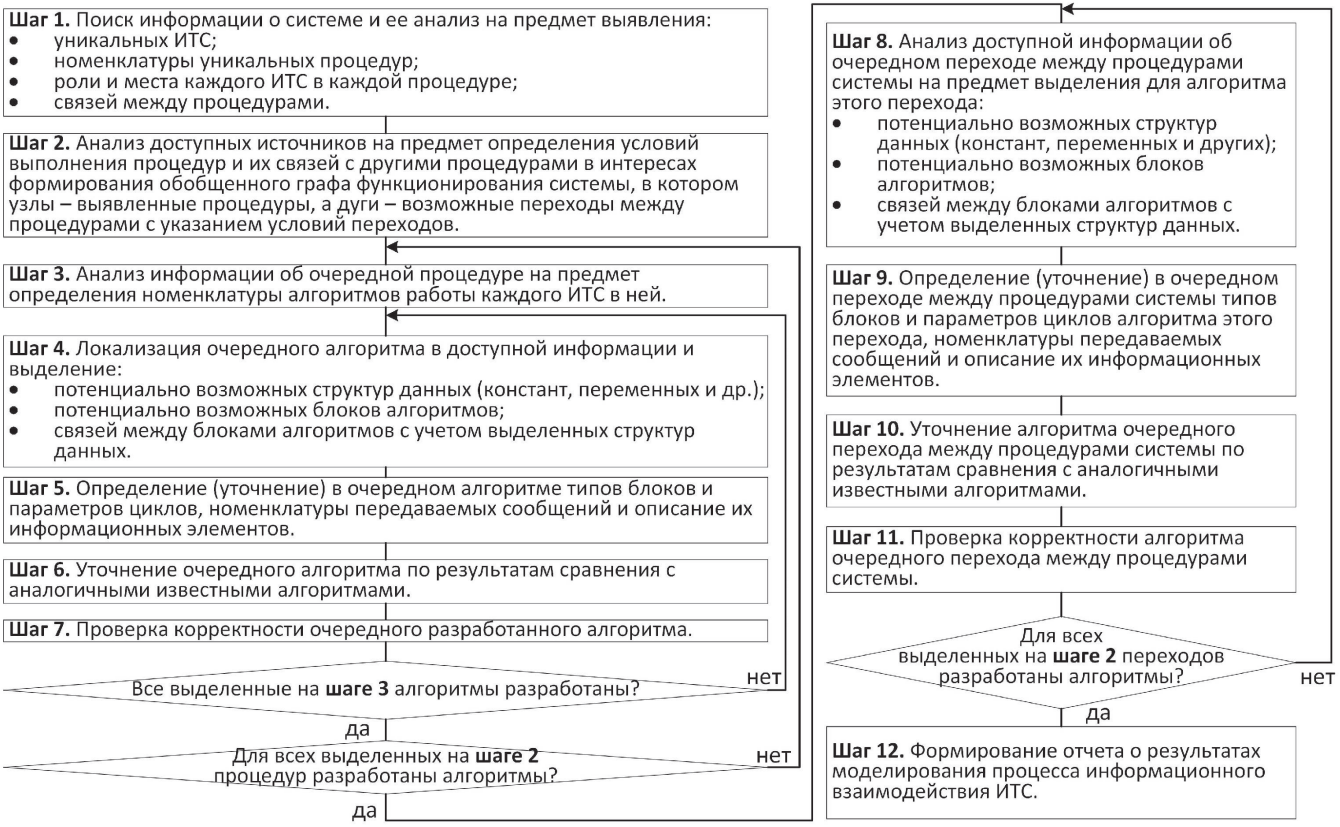


Рис. 22. Блок-схема алгоритма разработки модели процесса информационного взаимодействия информационно-технических средств

с учетом номенклатуры передаваемых сообщений и информационных элементов. Генерацию тестовых способов реализации КА следует проводить для каждой уникальной процедуры и для каждого перехода между процедурами.

Важно отметить, что в спецификациях телекоммуникационных протоколов нередко в явном виде отсутствуют исходные данные для построения блок-схем ЛП функционирования ИТС, которые требуются для создания модели процесса их информационного взаимодействия. Возникает вопрос, могут ли разные аналитики разработать разные блок-схемы? И может ли впоследствии это привести к разным результирующим множествам сгенерированных тестовых способов реализации КА? Ответ состоит в следующем. Дело в том, что своего рода мерой адекватности построения блок-схем ЛП является учет всех сообщений, которыми обмениваются ИТС. Именно последовательность приема и передачи сообщений имеет ключевое значение для генерации тестовых способов реализации КА. Спецификации телекоммуникационных протоколов в обязательном порядке исключают двоякое толкование таких последовательностей. Имеющийся у автора и его коллег опыт анализа подтверждает это правило. Поэтому разные аналитики действительно могут разработать разные блок-схемы, но частные интерпретации элементов блок-схем, не относящихся к приему и передаче сообщений, на набор тестовых способов реализации КА не влияют. Практика также показала, что каждый сформированный ЛП целесообразно проверять на корректность не только по требованиями ГОСТа [83], но и с использованием следующих основных критериев:

- каждому входящему сообщению в любом ЛП должно соответствовать исходящее сообщение в другом ЛП;
- передача сообщений в рамках одного ЛП недопустима;
- каждый переход между блоками ЛП должен начинаться в блоке и заканчиваться в блоке;
- начало и конец перехода в одном блоке недопустимы;
- циклы формируются только с использованием логического блока;
- ЛП должен иметь один начальный блок;
- в случае отсутствия блока завершения (когда исследуемая система является реактивной) ЛП должен быть зацикленным;
- на пути от возникновения информационного элемента до его использования может быть передача сообщений только между различными ЛП;
- возникновение и/или (использование и/или уничтожение) информационного элемента не должно осуществляться в процессе его передачи в сообщении;
- в каждом блоке может быть только один вход и один или несколько (условный блок) выходов. Исключение составляют начальный блок, из которого существует только один выход, и конечный блок, в который может быть более одного входа.

Также особенностью реализации метода генерации КА на телекоммуникационное оборудование является крайне затратная по времени процедура анализа и преобразования спецификаций телекоммуникационных протоколов

в модели процессов информационного взаимодействия ИТС. Парировать данное обстоятельство на сегодняшний день с использованием существующих средств моделирования текста не представляется возможным по причине их недостаточной развитости. Это перспективное направление исследования.

В ходе апробации установлено, что даже квалифицированный специалист при применении предлагаемого метода допускает до 20 % ошибок при определении опосредованных переходов в РП. Для устранения этого недостатка разработано программное средство [237], автоматически выполняющее все следующие за первым этапы разработки тестовых способов реализации КА, изложенные на рис. 17, для вводимых пользователем ЛП функционирования ИТС. Интерфейс данного программного средства выполнен в стиле программного продукта Microsoft Visio. Оно позволяет наносить на лист формата А4 блоки ЛП, указывать связи между ними и названия сообщений и их информационных элементов (см. рис. 23 для примера в части Wi-Fi).

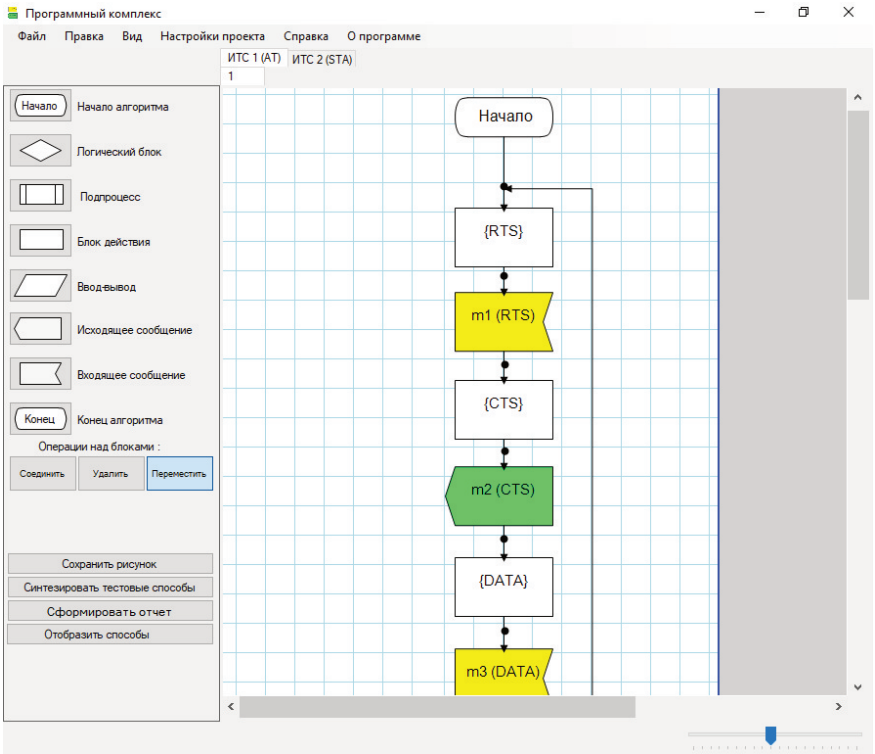


Рис. 23. Элемент интерфейса программы разработки тестовых способов

После ввода ЛП системы пользователь генерирует тестовые способы, которые представляются в виде HTML-файла. Фрагмент сгенерированного HTML-файла для рассмотренной выше процедуры стандарта Wi-Fi приведен на рис. 24.

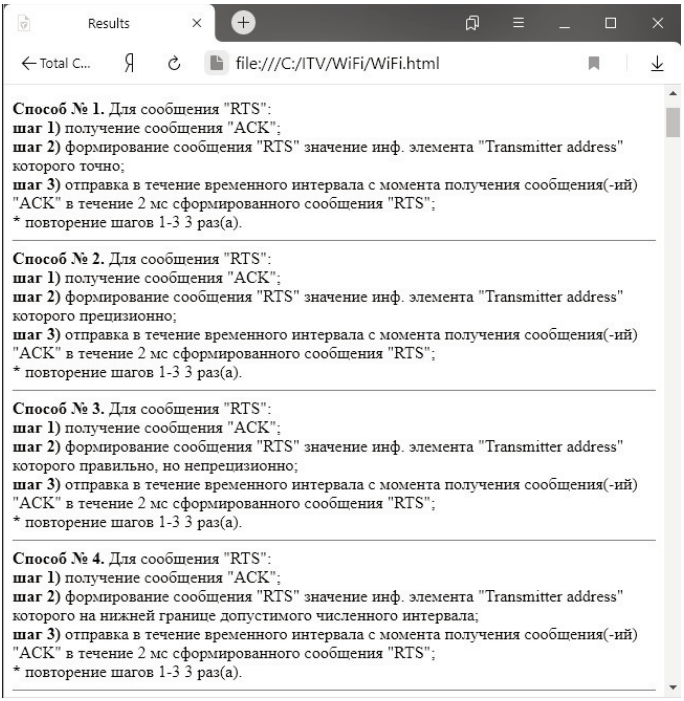


Рис. 24. Фрагмент HTML-файла с описанием тестовых способов

Программное средство представляет тестовые способы в виде, удобном для последующей оценки их эффективности натурным методом. Для этого кроме HTML-файла для каждого сгенерированного способа создается файл «Способ_X.txt» (где X – номер способа), содержащий последовательность действий, аналогичную представленной на рис. 24, но записанную на разработанном в ходе исследования языке описания тестовых способов реализации КА BOSL (англ. *Basic Online Synthesis Language* – базовый язык интерактивного синтеза). Синтаксические конструкции BOSL, описанные с использованием формы Бэкуса-Наура [302] показаны в таблице 3. Пример файла с тестовым способом КА на BOSL показан на рис. 25. Команды разработанных способов на BOSL предназначены для трансляции в команды программно-аппаратного модуля технического анализа и КА, реализующего натурный метод оценки эффективности этих способов (см. рис. 26). В монографии технические вопросы исполнения этого модуля не рассматриваются. Следует лишь отметить, что он базируется на SDR-технологии (англ. *Software-Defined Radio* – программно определяемое радио) и по сути выполняет комбинацию функций модема, параметры которого в полном объеме согласованы с исследуемыми образцами ИТС, и ретранслятора BOSL в низкоуровневый код. Подобный функционал имеется у широкой номенклатуры современных SDR-устройств (см., например, устройство «USRP» от компании «Ettus Research» [289]).

Таблица 3 — Синтаксические конструкции BOSL

Форма Бэкуса-Наура	Описание исполняемой команды
<frame>::=FRAMEδ <int>δ<bit>[(+δAND|ORδ <int>δ<bit>)$^{0-n}$]	Ожидает получение из канала связи сообщения, для которого удовлетворяется до n+1 условий вида: в сообщении, начиная с бита <int>, содержится битовая последовательность <bit>. Возможны конъюнкция и/или дизъюнкция условий.
<delay>::= DELAYδ<int>	Обеспечивает временную задержку перед выполнением следующей синтаксической конструкции на <int> мкс.
<repeat>::=REPEATδ<оператор>δUNTILδ<условие>	Обеспечивает выполнение команды <оператор> до тех пор, пока не будет выполнено <условие>.
<message>::= MESSAGEδ<int1> [δ<int2>|<+1>]	Если используется как <оператор>, то накапливает сообщения длиной <int1> бит в массив, увеличивая его размер на единицу <+1>. Если используется как <условие>, то выдает логическое значение наполненности массива размером <int2> сообщениями длиной <int1>.
<bit>::= BITδ<int1>δ<int2> [(+δ<int1>δ<int2>)$^{0-n}$]	Формирует битовую строку BIT путем сравнения во всех сообщениях массива <message> до n+1 последовательностей бит, начиная с бита <int1>, до бита <int1>+<int2> и записи в строку BIT наиболее часто встречающихся в массиве <message> таких последовательностей. Возможна конъюнкция последовательностей.
<modif>::= MODIFδ<int>δ<bit> [(+δANDδ<int>δ <bit>)$^{0-n}$]	Модифицирует битовую строку BIT по n+1 правилу: в сообщении биты, начиная с бита <int>, заменяются на битовую последовательность <bit>. Возможна конъюнкция правил.
<generate>::= GENEATEδ<signal>	Создает файл <signal>, содержащий битовую строку BIT передаваемого сообщения.
<radiation>::= RADIATIONδ <signal>δ<int>	Излучает сообщение из файла <signal> с мощностью <int> в dBm. Конструкция учитывает параметры передачи сообщения в физической среде передачи сообщений.

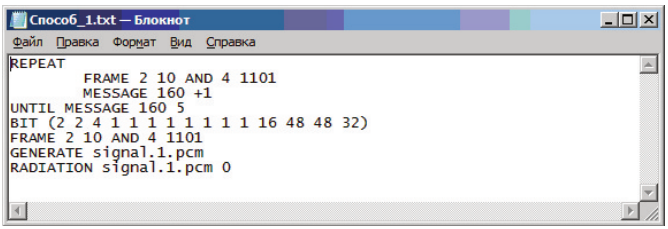


Рис. 25. Пример файла с описанием тестового способа реализации кибератак на специализированном языке BOSL

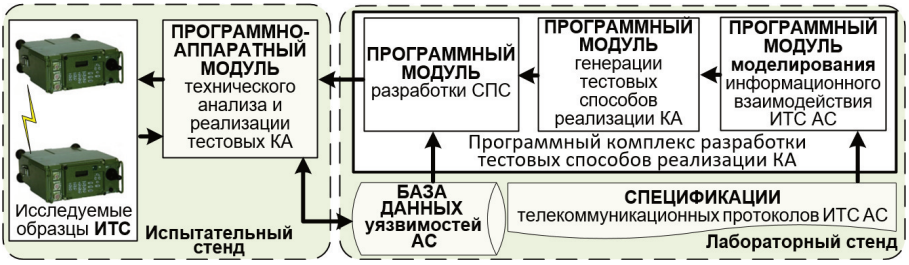


Рис. 26. Технологическая платформа выявления уязвимостей телекоммуникационного оборудования

Алгоритм применения технологической платформы выявления уязвимостей телекоммуникационного оборудования, в состав которой входит программно-аппаратный модуль технического анализа и КА, показан на рис. 27.

В результате анализа спецификаций протоколов различных стандартов СЦР установлено, что приведенных в таблице 3 конструкций вполне достаточно для описания любого тестового способа реализации КА. Поэтому BOSL может рассматриваться в качестве претендента на роль унифицированного языка описания тестовых способов реализации КА для перспективных программно-аппаратных платформ сертификации защищенности ИТС от КА. С применением BOSL любая сложная КА, например, типа «человек посередине» (англ. *man-in-the-middle*), разработанная в ходе исследования модели процесса информационного взаимодействия ИТС АС (см. рис. 22), может быть представлена в виде сценария применения совокупности разнородных и элементарных способов реализации КА, аналогичных показанному на рис. 25.

В частности, для вышеуказанных процедур стандартов DMR (см. рис. 18) и Wi-Fi (см. рис. 20) с применением предложенных модели и метода получены, тестовые способы реализации КА. Разработанные способы проверены на предмет дублирования с уже разработанными и апробированными способами реализации КА. При этом установлено, что полученные тестовые способы реализации КА включают в том числе способы, разработанные с применением эмпирического метода (см. параграф 2.2). Приведем два примера.

Пример № 1. Сгенерированный на основе РП, показанного на рис. 19, тестовый способ реализации КА на СЦР стандарта DMR, соответствующий прямому переходу из состояния «CSBK» в состояние «IDLE_1». Этот способ опубликован в [211].

Пример № 2. Сгенерированный на основе РП, показанного на рис. 21, тестовый способ реализации КА на сети широкополосного доступа семейства стандартов IEEE 802.11 Wi-Fi, соответствующий прямому переходу из состояния «ACK» в состояние «RTS», опубликован в [301]. Этот способ основан на уязвимости процедуры случайного множественного доступа к среде с предварительным резервированием канала передачи данных посредством

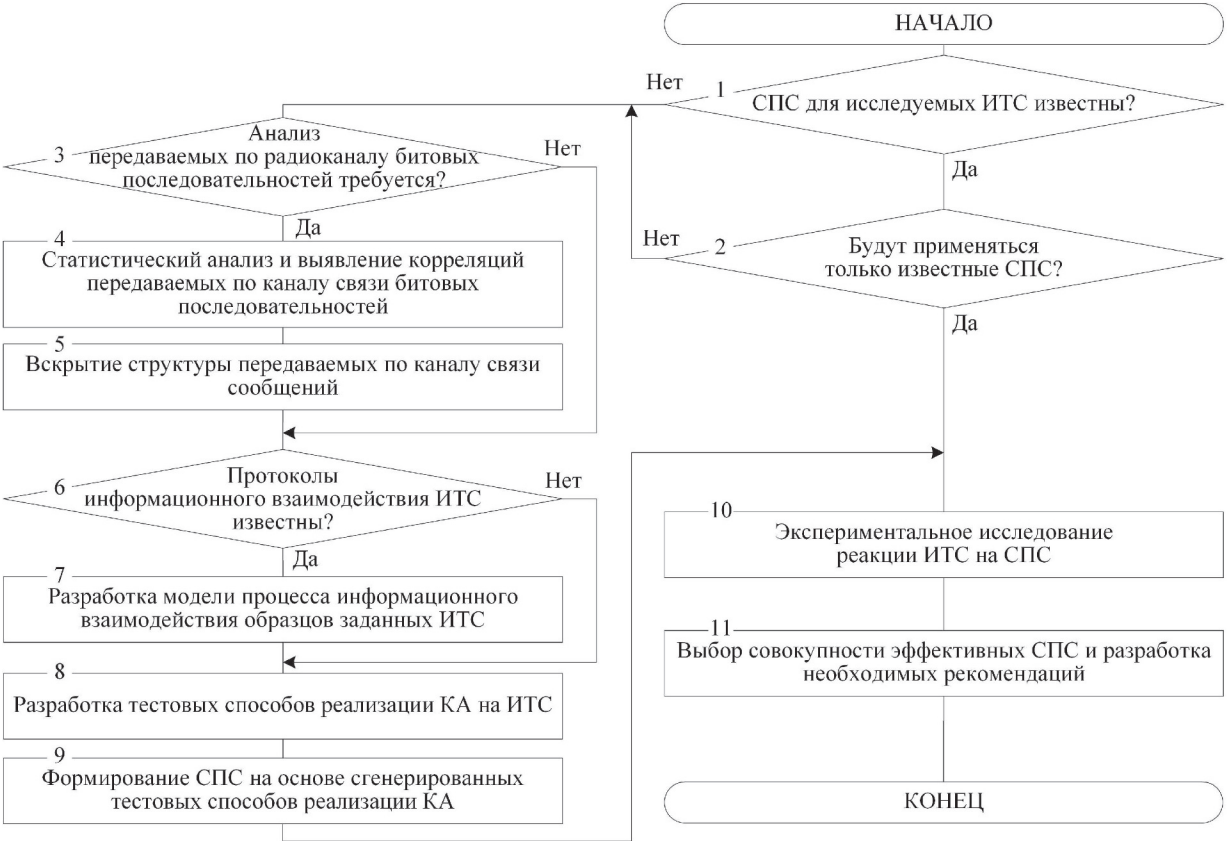


Рис. 27. Алгоритм применения технологической платформы выявления уязвимостей телекоммуникационного оборудования

служебных сообщений «RTS». Способ состоит в передаче от имени легитимного АТ на адрес точки доступа или от имени точки доступа на адрес АТ сообщения с запросом резервирования канала передачи данных «RTS» с указанием максимального значения времени резервирования канала передачи данных. Этапы реализации этого способа показаны на рис. 28 [301].

Рис. 28. Этапы эксплуатации уязвимости процедуры случайного множественного доступа к среде с предварительным резервированием канала передачи данных посредством служебных сообщений «RTS» в сетях стандарта IEEE 802.11 Wi-Fi

Таким образом, применение модели процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола и метода генерации КА на телекоммуникационное оборудование позволяет определить временные границы отправки/получения любого выбранного сообщения в процедуре протокола и разработать необходимое (в смысле полноты учитываемых параметров передачи сообщений) и достаточное (в смысле безызбыточной проверки сочетаний параметров передачи сообщений) множество тестовых способов КА для доступной информации об алгоритмах функционирования ИТС и при этом:

- увеличить количество эффективных способов реализации КА;
- определить уровень защищенности СПО от разработанных тестовых способов реализации КА. Учитывая, что для разработки способов с применением предлагаемого подхода не требуется высокая квалификация специалистов, такой результат позволяет рассматривать этот подход к поиску уязвимостей ПО в сравнении с известными подходами как наиболее рациональный.

Рассмотренные в настоящей главе модель и метод возможно использовать в интересах выявления уязвимостей и сертификации на предмет защищенности от КА. Также потенциально они могут использоваться при интеграционном тестировании сложных программных проектов, когда используемая категория «информационно-техническое средство» отождествляется с программным модулем или блоком ИТС, и в процессе тестирования программных модулей, разработанных с применением объектно-ориентированного подхода, когда категория «информационно-техническое средство» отождествляется с объектом.

Выводы по второй главе

Во второй главе представлены модель процесса информационного взаимодействия информационно-технических средств автоматизированных систем по известной процедуре телекоммуникационного протокола и метод генерации кибератак на телекоммуникационное оборудование. Для их реализации на практике предложены алгоритм разработки модели процесса информационного взаимодействия информационно-технических средств, формализующей взаимосвязанную совокупность процедур телекоммуникационного протокола, язык описания тестовых способов реализации кибератак Basic Online Synthesis Language, технологическая платформа выявления уязвимостей телекоммуникационного оборудования, основным элементом которой является разработанный в ходе исследования программный комплекс разработки тестовых способов реализации кибератак, а также алгоритм применения этой платформы.

Применение этих результатов позволяет определить временные границы отправки/получения любого сообщения в процедуре телекоммуникационного протокола и разработать необходимое (в смысле полноты учитываемых параметров передачи сообщений) и достаточное (в смысле безызбыточной проверки сочетаний параметров передачи сообщений) множество тестовых способов кибератак для доступной информации об алгоритмах функционирования информационно-технических средств и при этом увеличить количество эффективных способов реализации кибератак, а также определить уровень защищенности специального программного обеспечения, функционирующего на основе исследованных процедур стандартов цифровой радиосвязи. Учитывая, что для разработки способов реализации кибератак с применением предлагаемых модели и метода не требуется высокая квалификация специалистов, такой результат позволяет рассматривать предлагаемый подход к поиску уязвимостей программного обеспечения в сравнении с известными подходами как наиболее рациональный.

В следующей главе рассматриваются вопросы моделирования процессов функционирования компонентов автоматизированных систем, которые будут использоваться при оценке эффективности способов реализации кибератак в условиях боевой обстановки.

3 Модели процессов функционирования компонентов автоматизированных систем воинских формирований

«Не может быть системного мышления без ясного понимания процесса».

Станфорд Л. Оптнер

3.1 Методические аспекты аналитического описания процессов с дискретным множеством состояний и непоказательным распределением времен переходов

Известные из практики законы распределения временных характеристик процессов функционирования АС ВФ не позволяют применять для их анализа методы теории марковских процессов, ориентированные на распределение времен по показательному закону [36, 266]. Причина состоит в следующем. Во-первых, суть этого закона: чем меньше время, тем больше вероятность реализации перехода. На практике такое встречается крайне редко. Во-вторых, коэффициент вариации (отношение среднеквадратического отклонения (СКО) к математическому ожиданию) у этого закона равен единице [7]. Точность численных значений показателей, оцениваемых с использованием такой модели, очевидно, вряд ли может быть приемлемой. Для процессов функционирования АС ВФ наиболее вероятны значения в окрестности среднего. Поэтому на испытаниях образцов вооружения за счет увеличения количества экспериментов СКО доводится до нескольких процентов от математического ожидания. Парировать эти ограничения позволяет использование полумарковских процессов.

К числу наиболее практичных следует отнести два метода описания полумарковских процессов. Первый метод предложен Ю.Л. Козирацким [143] и позволяет решить задачу определения вероятности нахождения исследуемой системы в каждом состоянии в любой момент времени путем агрегирования групп состояний, не прибегая к численным методам, но требуя кропотливой работы по прямому и обратному преобразованию Лапласа близких к нормальному распределению функций, характеризующих время переходов между состояниями исходной модели. Второй метод, предложенный М.Г. Чикиным в [266], позволяет решить такую задачу в полностью автоматическом режиме, но требует применения численных методов. Поскольку вычислительные мощности современных электронных вычислительных машин (ЭВМ) позволяют обеспечить приемлемую точность решений, полученных численными методами, за основу в настоящей работе взят метод М.Г. Чикина.

Существо второго метода состоит в развитии метода М.Д. Кендалла на основе преобразования структуры дискретного процесса с распределенным по обобщенному закону Эрланга ***n***-го порядка временем переходов в марковский процесс путем введения псевдосостояний и описании полученного процесса в виде системы линейных однородных дифференциальных уравнений. Модифицированный метод М.Д. Кендалла оперирует тем фактом [144], что произвольная плотность распределения времени нахождения системы

в некотором состоянии с достаточной степенью точности аппроксимируется с помощью обобщенного закона Эрланга ***n***-го порядка. Данная плотность распределения описывается с использованием следующей формулы:

$$T_{s,v}(t) = (-1)^{n-1} \prod_{i=0}^{n-1} \lambda_{s,v,i} \sum_{j=0}^{n-1} \frac{e^{-\lambda_{s,v,j} t}}{\prod_{k=0,k\neq j}^{n-1} \left(\lambda_{s,v,j} - \lambda_{s,v,k}\right)}, \quad (17)$$

где $T_{s,v}(t)$ – плотность распределения времени нахождения системы в s-м состоянии до перехода в v-е состояние;

$\lambda_{s,v,i}$, $\lambda_{s,v,j}$, $\lambda_{s,v,k}$ – параметры обобщенного закона Эрланга ***n***-го порядка.

Коэффициент вариации этого закона равен $\boldsymbol{n}^{-0,5}$ [7]. Например, при $\boldsymbol{n}$ = 100 СКО равно 10 % от математического ожидания. Для $\boldsymbol{n}$ = 2 выражение (17) принимает вид:

$$T_{s,v}(t) = -\lambda_{s,v,0}\lambda_{s,v,1}\left(\frac{e^{-\lambda_{s,v,0}t}}{\lambda_{s,v,0} - \lambda_{s,v,1}} + \frac{e^{-\lambda_{s,v,1}t}}{\lambda_{s,v,1} - \lambda_{s,v,0}}\right). \quad (18)$$

Из (18) видно, что случайная величина, распределенная по обобщенному закону Эрланга 2-го порядка, может быть представлена как сумма двух случайных величин, распределенных по показательным законам с параметрами $\lambda_{s,v,0}$ и $\lambda_{s,v,1}$. Это свойство дает возможность представить переходы на графе состояний в виде последовательности переходов с временами, распределенными по показательным законам, с учетом дополнительного введения псевдосостояний. Если из некоторого состояния S_0 имеется k альтернативных переходов в состояния $S_1, S_2, \ldots, S_k$, то безусловное распределение времени перехода каждого из них распределено по обобщенному закону Эрланга ***n***-го порядка с параметрами $\lambda_{r,s,v,0}, \lambda_{r,s,v,1}, \ldots, \lambda_{r,s,v,n-1}$, $r = 1 \ldots k$. При этом вводятся состояния $S_{j_1, j_2, \ldots, j_k}$, $j_i = 0 \ldots \boldsymbol{n} - 1$. Состояние $S_{0,0,\ldots,0}$ является эквивалентным состоянию S_0, а остальные являются псевдосостояниями. Суть проводимого в рамках метода преобразования моделей показана на рис. 29. Полученный процесс является марковским, так как времена всех переходов распределены по показательным законам.

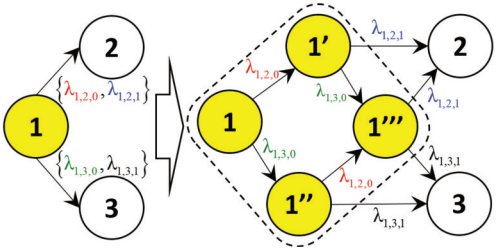


Рис. 29. Суть преобразования моделей

Из содержания данного метода, на первый взгляд, может показаться, что распределение времени работы системы зависит от числа ее «псевдосостояний», которое априори неизвестно и фактически задается исследователем, что создает неопределенность в выборе исходной модели. Однако это не так. Исходные модели, как будет показано в следующих параграфах настоящей главы,

являются строго определенными. Времена переходов в них в части оценки надежности задаются на основе результатов статистической оценки, доступных из протоколов предварительных или государственных испытаний ИТС или АС, а в части времени до ОП каждого ЭБП противоборствующих ВФ определяются текущим состоянием боевой обстановки. В то же время выбираемое количество псевдосостояний в результирующих моделях определяется тем, какой порядок обобщенного закона Эрланга используется. Чем выше порядок этого закона, тем больше вычислений, но и тем выше точность получаемого результата.

Приведенные правила преобразования применимы вручную для систем с небольшим числом состояний (до 5…7) и переходов между ними (до 10…15). ИТС, как будет показано далее, к таким системам не относятся. Поэтому в [36] предложен алгоритм, автоматизирующий процесс преобразования аналитического описания немарковского процесса с дискретными состояниями и распределенным по обобщенному закону Эрланга n-го порядка временем переходов в марковский процесс. Блок-схема этого алгоритма приведена на рис. 30. Реализация в виде программы для ЭВМ этого алгоритма требует весьма значительных вычислительных ресурсов, объем которых экспоненциально зависит от числа состояний и переходов в исходной модели. Тем не менее она позволила на персональной ЭВМ с процессором Intel Core i3 с 4 Гб оперативной памяти исследовать рассматриваемые далее в настоящей главе модели процесса функционирования ИТС, учитывающие весь спектр выполняемых этими средствами задач в условиях комплексного влияния деструктивных факторов, возникающих в боевых условиях.

Важно заметить, что используемый в настоящей работе математический аппарат полумарковских процессов основывается на решении системы значительного количества линейных однородных дифференциальных уравнений, для чего используются численные методы, требующие больших вычислительных затрат. На первый взгляд, более выгодной альтернативой, с точки зрения сложности проводимых вычислений, является имитационное моделирование. Однако, как будет показано далее в параграфе 4.1, имитационное моделирование имеет ряд фундаментальных ограничений, которые не позволяют воспроизводить боевые циклы воинских формирований в динамике боя и влияние на них ИТВ (в том числе КА). По этой причине достичь цели настоящего исследования представляется возможным только с применением комбинации численных и аналитических методов.

3.2 Модель процесса функционирования информационно-технического средства автоматизированной системы

Анализ предметной области. ИТС АС, как уже отмечено выше в п. 1.1.1, могут решать ИРЗ, ЗО и ЗУ. В современном бою ИТС имеют двойственную роль [43]. С одной стороны, они обеспечивают повышение производительности своего ВФ, а с другой – подвержены влиянию деструктивных факторов, характерных для СВТ: КА и мощного ЭМИ, приводящих к нарушению конфиденциальности, целостности и доступности обрабатываемой информации и алгоритмов ее обработки, физическому износу и уничтожению [27].

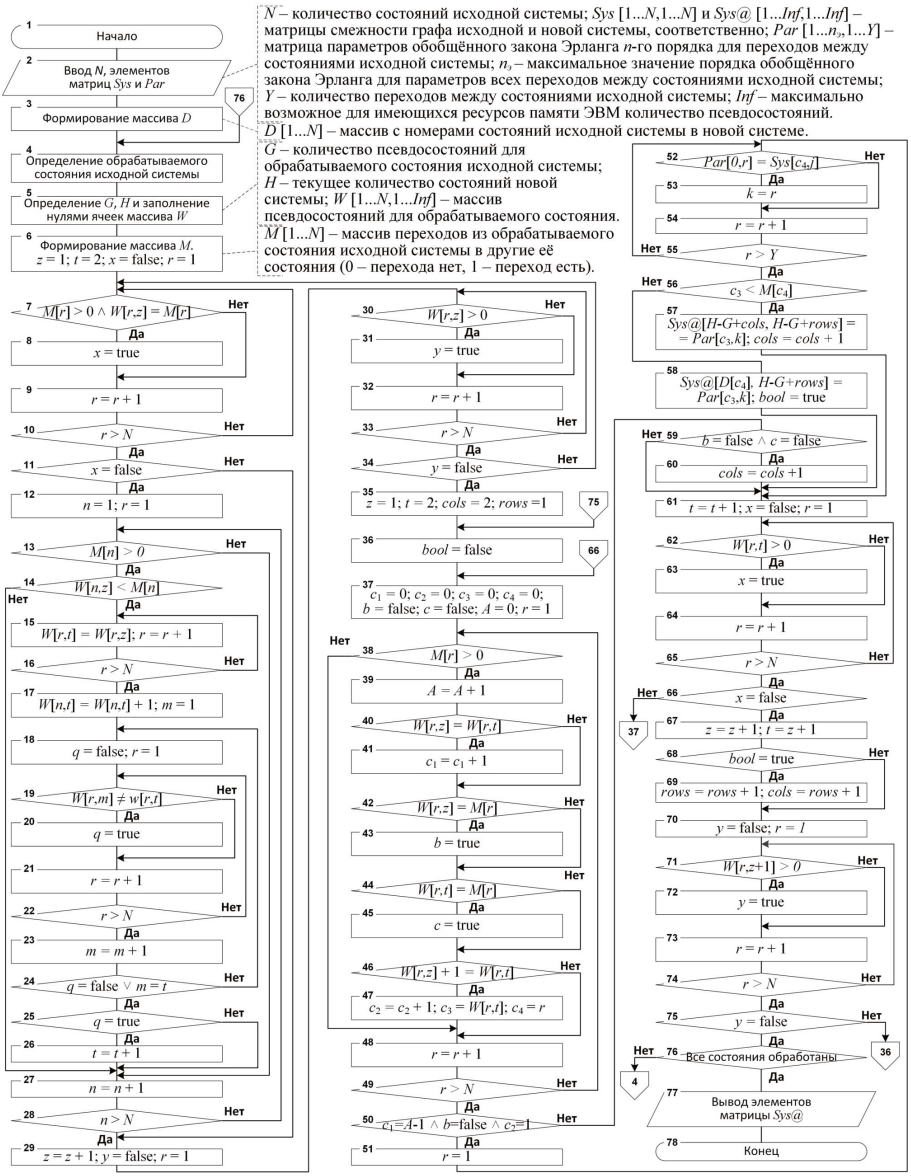


Рис. 30. Алгоритм автоматизированного преобразования аналитического описания немарковского процесса с распределенным по обобщенному закону Эрланга ***n***-го порядка временем переходов в марковский процесс

С практической точки зрения известные модели процесса функционирования ИТС [47, 51, 71, 145] и аналогичные им либо не учитывают специфику выполняемых ИТС задач, либо представляют эти задачи однотипными. В этих моделях не принимаются во внимание особенности функционирования ТК, ОПО (операционной системы, систем управления базами данных, базовой системы ввода-вывода и др.), а из деструктивных факторов учитывается только РЭП, характерное для РЭС и приводящее к нарушению доступности информации. В результате осуществить адекватную оценку практически значимой номенклатуры показателей функционирования ИТС с учетом всего спектра выполняемых этими средствами задач, качества входящих в них компонентов и комплексного влияния деструктивных факторов с применением известных моделей невозможно.

С методической точки зрения ИТС относятся к таким сложным системам, многообразие ключевых процессов в которых, с одной стороны, не представляется возможным аналитически описать в виде причинно-следственных моделей параллельных действий, а с другой стороны, недостаточно рассматривать только в статике или в установившихся режимах с использованием графо-сигнальных моделей [229]. Для аналитического описания функционирования систем такого класса в наибольшей степени применим математический аппарат полумарковских процессов [51, 81, 229]. Однако количество ключевых процессов функционирования в типовом ИТС настолько велико, что разработка для него аналитического описания в виде единой детальной полумарковской модели неизбежно приводит к «взрыву» пространства состояний.

Постановка задачи: разработать модель совокупности процессов функционирования ИТС АС, базирующуюся на применении аппарата полумарковских процессов и парирующую «взрыв» пространства состояний при учете всего спектра выполняемых этими средствами задач, качества входящих в их состав компонентов и комплексного влияния деструктивных факторов в бою.

Решение. Модель базируется на изложенном в [163] методе стратификации, заключающемся в рассмотрении сложной системы в различных слоях ее функционального пространства, называемых стратами, и анализе каждой страты без учета влияния остальных страт. Построение модели состоит в выполнении следующего алгоритма [35].

Шаг 1. Выделяют множество страт функционирования ИТС. При этом одна из страт может характеризовать суперпроцесс, координирующий некоторое подмножество страт. Наличие суперпроцесса не является обязательным.

Шаг 2. Разрабатывают аналитическое описание страт. Страты описывают в виде полумарковских процессов, а суперпроцесс – в виде системы с очередями. Ввиду того, что произвольная плотность распределения неотрицательной случайной величины с достаточной степенью точности аппроксимируется с помощью обобщенного закона Эрланга ***n***-го порядка, плотность распределения времени нахождения полумарковского процесса в каждом состоянии описывают с использованием этого закона (см. формулу (17)).

Шаг 3. Формируют группы состояний. Количество групп равно количеству исследуемых характеристик ИТС. Состояние включают в группу, если оно влияет на соответствующую характеристику исследуемого ИТС.

Каждая группа может включать состояния разных страт и учитывать влияние суперпроцесса.

Шаг 4. Определяют вероятностно-временные характеристики страт. За основу на данном шаге берется модифицированный метод Кендалла, изложенный выше в параграфе 3.1 [266].

Шаг 5. Вычисляют значения показателей групп состояний. Для этого в каждый момент времени применяют следующие правила:

- значения учитываемых в показателе вероятностно-временных характеристик состояний, принадлежащих одному процессу, складываются;
- суммарные значения вероятностно-временных характеристик разных полумарковских процессов перемножаются;
- значения характеристик суперпроцесса учитываются в множителях, описывающих состояния зависящих от него полумарковских процессов.

Эти правила обусловлены тем, что в каждом полумарковском процессе совокупность его состояний образует полную группу событий, а частные процессы считаются независимыми. Поэтому применимы правила сложения и умножения вероятностей.

Рассмотрим результаты моделирования на примере ИТС АС, которое может одновременно выполнять ИРЗ, ЗО и ЗУ. Относительно самостоятельные частные процессы функционирования такого ИТС имеют стратифицированную структуру, показанную на рис. 31.

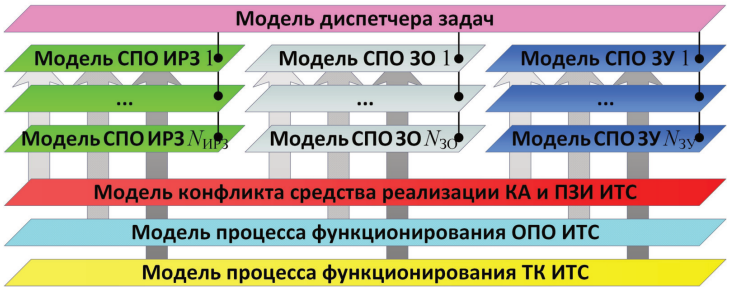


Рис. 31. Стратифицированная структура процесса функционирования информационно-технического средства

Такая структура напоминает «слоеный пирог». Она включает модели процесса функционирования СПО, реализующего ИРЗ, ЗО и ЗУ, модель диспетчера, являющегося суперпроцессом и координирующего выполнение задач, а также модели процессов функционирования ТК, ОПО и информационного конфликта между СПС, используемыми в КА, и ПЗИ ИТС. В данной структуре отсутствует диспетчеризация процесса функционирования ОПО. Такое упрощение обусловлено тем, что при разработке АС ВФ производительность каждого ИТС выбирается таким образом, чтобы исключить влияние диспетчеризации на согласованное выполнение прикладных задач, обеспечиваемых этим средством.

Далее рассматривается описание моделей процессов функционирования компонентов ИТС АС, показанных на рис. 31.

3.3 Модель процесса функционирования технического компонента информационно-технического средства в боевых условиях

Модели процесса функционирования технических средств рассматриваются в теории надежности (см., например, [1, 144, 218]). Однако такие модели не учитывают возможность уничтожения в бою ТК ИТС (или устройства, входящего в состав ЭБП) и воздействия мощным ЭМИ на электронную компонентную базу. В [35] предложена модель функционирования устройства или ТК ее ИТС, в которой воспроизводится процесс функционирования с позиции надежности и особенностей реализации потенциально возможных воздействий в боевых условиях. Граф состояний модели показан на рис. 32.

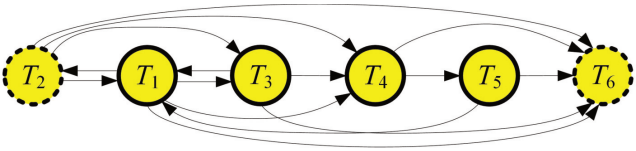


Рис. 32. Граф состояний, отражающий динамику функционирования технического компонента информационно-технического средства (или устройства) в боевых условиях

Граф динамики функционирования ТК включает шесть состояний:

- T_1 – нормальное функционирование;
- T_2 – ТК функционирует с нулевой производительностью (например, в течение воздействия на элементы его электронной компонентной базы мощным ЭМИ с обратимым эффектом);
- T_3 – произошел сбой (самовосстанавливающийся частичный отказ, обусловленный, например, некачественной пайкой или внутренними дефектами электронной компонентной базы);
- T_4 – произошел отказ ТК (например, по причине перегорания элемента электронной компонентной базы в результате ее износа или воздействия на нее мощным ЭМИ с необратимым эффектом);
- T_5 – проводится ремонт;
- T_6 – ТК уничтожен.

В этом графе в сравнении с известными моделями процесса функционирования технических средств дополнительно введены состояния «уничтожено» и «зависание». На рис. 32 эти состояния показаны прерывистой линией.

Исходные данные для этой модели в части времен переходов, характеризующих надежность, приводятся в соответствующих протоколах испытаний ИТС или АС, а в части времени до уничтожения ТК и воздействия мощным ЭМИ определяются моделью боевой обстановки, в которой применяется АС. Параметры защищенности ТК конкретных образцов ИТС от воздействия мощным ЭМИ содержатся в соответствующих протоколах испытаний ИТС или АС.

Следует отметить, что для технических средств времена перехода из состояний T_3, T_4 и T_5 в состояние T_6 характеризуют надежность этих средств и потому

многократно превосходят длительность современных боев. Поэтому математическое ожидание этих времен можно считать равным математическому ожиданию времени перехода «$T_1 \rightarrow T_6$». Если техническое средство переходит в бою в состояние T_2 раньше, чем в состояние T_6, то математическое ожидание времени перехода «$T_2 \rightarrow T_6$» равно разности математического ожидания времени перехода «$T_1 \rightarrow T_6$» и математического ожидания времени перехода «$T_1 \rightarrow T_2$». В противном случае оно равно математическому ожиданию времени перехода «$T_1 \rightarrow T_6$».

Таким образом, в модели процесса функционирования ТК ИТС в боевых условиях в отличие от моделей, изложенных в [1, 144, 218], в которых воспроизводится процесс функционирования технических средств с позиции надежности, дополнительно учитываются возможности противника по уничтожению ТК и воздействию мощным ЭМИ на электронную компонентную базу. Это достигается за счет введения дополнительных конфликтно обусловленных транзитивного состояния «зависание» и терминального состояния «уничтожено», а также преобразования полученного полумарковского процесса, в котором плотности распределения времен переходов определяются обобщенным законом Эрланга ***n***-го порядка, в марковский процесс модифицированным методом Кендалла. Модель позволяет исследовать влияние средств ОП и воздействия мощным ЭМИ на работоспособность ТК ИТС.

Роль предлагаемой модели в данном исследовании состоит в обеспечении взаимосвязи процессов функционирования ИТС с моделью процессов функционирования АС в боевом эпизоде. Суть этой взаимосвязи будет показана в главе 4.

3.4 Модель конфликта средства реализации кибератак и подсистемы защиты информации информационно-технического средства

Модели информационного конфликта средства реализации КА и ПЗИ ИТС известны из работ [77, 140]. Эти модели воспроизводят процесс КА на средства обработки информации АС. Однако известные из практики особенности КА требуют дополнительного учета в таких моделях воздействий СПС на каналы передачи данных АС на канальном и вышестоящих уровнях ЭМВОС и возможностей СПС по выводу из строя, захвату управления и применения в своих целях ИТС, а также ответных мер ПЗИ на эти действия.

Рассмотрим модель, учитывающую эти особенности [35, 36]. Граф состояний модели показан на рис. 33 (дополнительно введенные состояния показаны прерывистой линией). Состояния имеют следующие описания:

- S_1 – исходное работоспособное состояние;
- *группа состояний внедрения СПС в программную среду ИТС* (S_2 – у средства реализации КА есть физический доступ; S_4 – у средства реализации КА есть технический доступ; S_6 – инициатор КА анализирует управляющую информацию протоколов канального уровня; S_8 – инициатором КА получен доступ к протоколам сетевого, транспортного и сеансового уровней; S_{10} – СПС внедрилось в ИТС);
- *группа состояний поддержания работоспособности ИТС* (S_3 – ПЗИ нейтрализует физический доступ; S_5 – ПЗИ нейтрализует технический

доступ; S_7 – ПЗИ нейтрализует возможность доступа к протоколам сетевого, транспортного и сеансового уровней; S_{18} – ПЗИ проводит принудительный поиск СПС; S_{21} – восстановление работоспособности ИТС; S_{22} – подготовка ИТС к работе);

- *группа состояний блокирования коммуникационных возможностей ИТС* (S_9 – средство реализации КА нарушает доступность информации на канальном уровне; S_{11} – средство реализации КА нарушает доступность информации на сетевом, транспортном и/или сеансовом уровне);
- *группа состояний скрытного применения СПС* (S_{16} – СПС дезинформирует ИТС; S_{17} – СПС проводит разведку в ИТС);
- *группа состояний открытого применения СПС* (S_{12} – СПС проводит отказ в обслуживании ИТС; S_{13} – СПС применяет ИТС в своих целях; S_{14} – СПС осуществляет вывод ИТС из строя);
- *группа состояний обеспечения выживаемости СПС* (S_{15} – СПС размножается; S_{19} – СПС самомодифицируется; S_{20} – СПС ожидает).

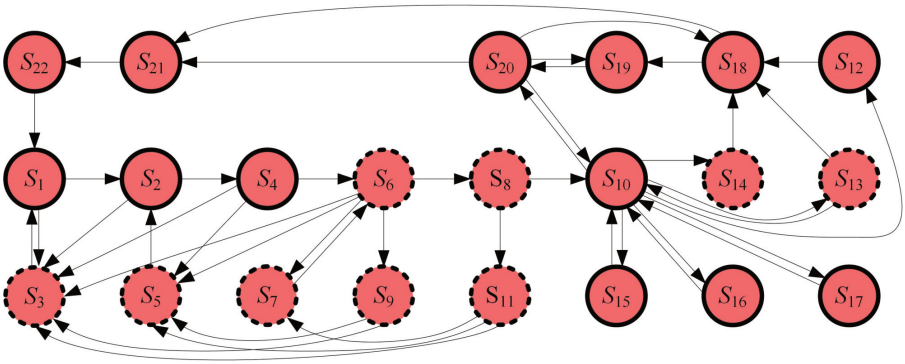


Рис. 33. Граф состояний, отражающий динамику конфликта средства реализации кибератак и подсистемы защиты информации информационно-технического средства

Набор состояний и переходов в модели, несмотря на стремление учесть как можно больше состояний конфликта, оптимизирован с учетом возможностей программной реализации рассмотренного в параграфе 3.1 алгоритма преобразования немарковского в марковский. Тем не менее, следует сделать ряд дополнительных пояснений.

Во-первых, в модели, на первый взгляд, не учитывается важная и весьма вероятная на практике возможность одновременного выполнения СПС нескольких деструктивных функций. Такая ситуация парируется применением теоремы сложения вероятностей для совместных событий, которые получаются в результате решения системы линейных однородных дифференциальных уравнений.

Во-вторых, в модели выделяются две группы протоколов: протоколы канального уровня и протоколы сетевого, транспортного и сеансового уровней. Однако каждый из протоколов второй группы выполняет уникальные задачи, и программная реализация каждого протокола может иметь собственные

уязвимости. Такое разделение протоколов в модели реализовано ввиду того, что в ней в качестве основных классов уязвимостей рассматриваются:

- уязвимости СПО телекоммуникационных задач в локальной информационно-управляющей сети, которая в боевых условиях, как отмечено в главе 1, в наиболее общем случае является беспроводной. На выявление этих уязвимостей ориентирован метод генерации КА на телекоммуникационное оборудование, предложенный в главе 2;
- уязвимости типового ОПО межсетевого взаимодействия (это преимущественно стек протоколов TCP/IP), которые на сегодняшний день являются широко известными и в монографии детально не рассматриваются. В настоящей модели конфликта учитывается эффект от их эксплуатации;
- уязвимости программной среды, с которой непосредственно взаимодействует пользователь (то есть с позиции ЭМВОС эта среда затрагивает программные реализации протоколов представительского и прикладного уровней). Эти уязвимости эксплуатируются в состояниях S_{12}-S_{17} и играют ключевую роль в процессе воздействия КА на АС, обеспечивающие боевые циклы ВФ.

В-третьих, в модели из состояния S_8 (инициатором КА получен доступ к протоколам сетевого, транспортного и сеансового уровней) нет переходов в состояния S_3, S_5 и S_7 (подсистема защиты информации нейтрализует, соответственно, физический, технический доступ и доступ к протоколам сетевого уровня и выше), в то время как на практике такие переходы вероятны. Такая структура модели полагается допустимой потому, что применительно к продолжительности боя (от десятков минут до нескольких часов) время переходов из состояния S_8 в состояния S_{10} и S_{11} (доли секунд) и времена переходов в состояния S_3, S_5 и S_7 (от десятков минут до нескольких месяцев) настолько различны, что последними переходами предлагается пренебречь.

Исходные данные для модели могут быть получены на основе анализа поведенческих характеристик конкретных образцов СПС, а также по результатам применения промежуточных моделей. Промежуточные модели позволяют оценить вероятностно-временные характеристики функционирования СЦР в условиях КА на уровнях ЭМВОС от канального до представительского в условиях деструктивных воздействий, параметры которых определяются в модели процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола, предложенной в параграфе 2.1. Параметры перехода из состояния S_8 в состояние S_{11} позволяют получить промежуточные модели, рассмотренные, например, в работе [173], а параметры перехода из состояния S_6 в состояние S_9 позволяет получить модель одного из следующих классов:

- обобщенная модель процесса функционирования направления радиосвязи, если информация об используемых в ИТС телекоммуникационных протоколах существенно ограничена. В качестве такой модели может использоваться модель, предложенная М.Г. Чикиным в [267] и базирующаяся на использовании метода [266], взятого за основу в настоящей монографии. Граф состояний модели показан на рис. 34;

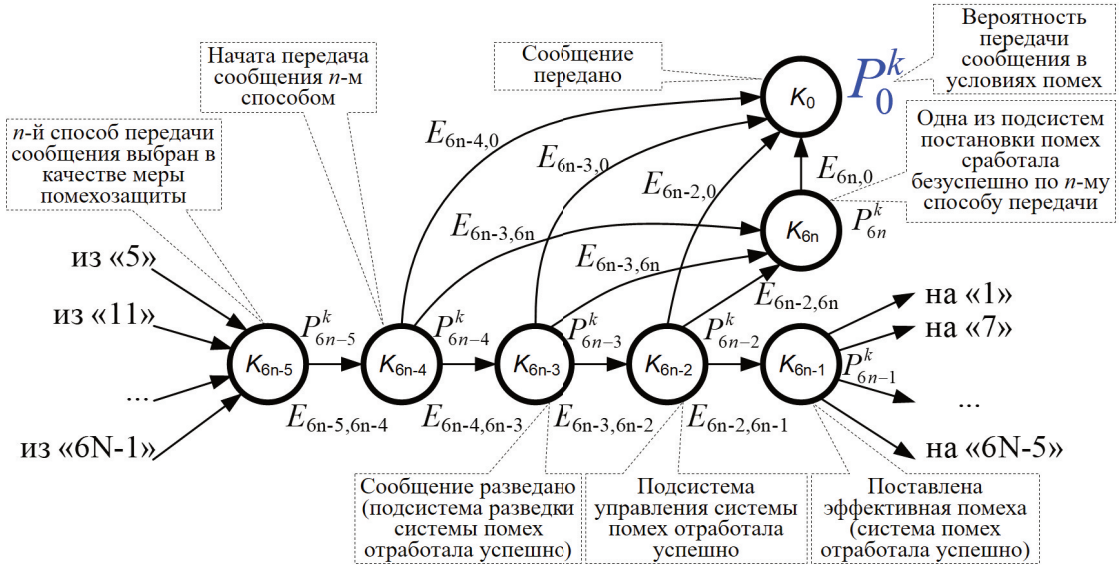


Рис. 34. Граф состояний функционирования направления радиосвязи

- специализированная модель, ориентированная на конкретные процедуры телекоммуникационных протоколов, в случае наличия информации об используемом в ИТС телекоммуникационном протоколе. Примеры таких моделей приведены в работах [207-212].

Рассмотрим в качестве примера специализированную промежуточную модель процедуры случайного множественного доступа к среде типа S-ALOHA, изложенную в работе [208]. Следует подчеркнуть, что данная процедура применяется на канальном уровне ЭМВОС, а не на физическом, где используются технологии множественного доступа к физическому каналу типа частотного FDMA (Frequency-Division Multiple Access), временного TDMA (Time-Division Multiple Access), пространственного SDMA (Space-Division Multiple Access), кодового CDMA (Code-Division Multiple Access) разделения, их разновидности и сочетания. Основные виды таких процедур, используемых на канальном уровне ЭМВОС, показаны на рис. 35.

Функциональная схема специализированной промежуточной модели процедуры случайного множественного доступа к среде типа S-ALOHA показана на рис. 36. Рассмотрим описание этой схемы.

Схема на рис. 36 включает АТ, средство коммутации и управления СЦР и злоумышленника. Процедура затрагивает два канала СЦР: канал от АТ к средству коммутации и управления (линия «вверх») и обратно (линия «вниз»). Каждый из N АТ, входящих в СЦР и конкурирующих между собой за использование канала, может функционировать в режиме первичной или вторичной передачи сообщений с запросом на доступ к среде по линии «вверх».

В первом режиме АТ генерирует и передает сообщение с вероятностью p_0 в любой дискретный временной интервал t (t =1,2,…) продолжительностью τ (далее – временной слот).

Во втором режиме АТ вторично передает сообщение с вероятностью p_r в течение одного временного слота. Одновременно в режиме вторичной передачи находятся $Y(t)$ АТ, а в режиме первичной передачи $N_{AT} - Y(t)$ АТ.

Вне зависимости от режима каждый АТ за один временной слот не может передать больше одного первичного или вторичного сообщения. Передача считается успешной, если только один из N АТ осуществляет передачу в течение временного слота. В противном случае АТ создают коллизии в канале и через некоторое время ожидания при неполучении сообщения подтверждения успешной доставки переходят в режим вторичной передачи. АТ, находящиеся в режиме вторичной передачи, не генерируют сообщения и называются самоблокированными. Средство коммутации и управления СЦР определяет количество отправленных всеми АТ в каждом временном слоте первичных и вторичных сообщений с запросом на доступ и формирует поток управления по линии «вниз», в котором широковещательно рассылает параметры p_0^* и p_r^*. Эти параметры равны вероятностям, с которыми абонентским терминалам рекомендуется передавать сообщения в режимах первичной и вторичной передачи, соответственно.

Рис. 35. Основные виды процедур случайного множественного доступа к среде на канальном уровне эталонной модели взаимодействия открытых систем

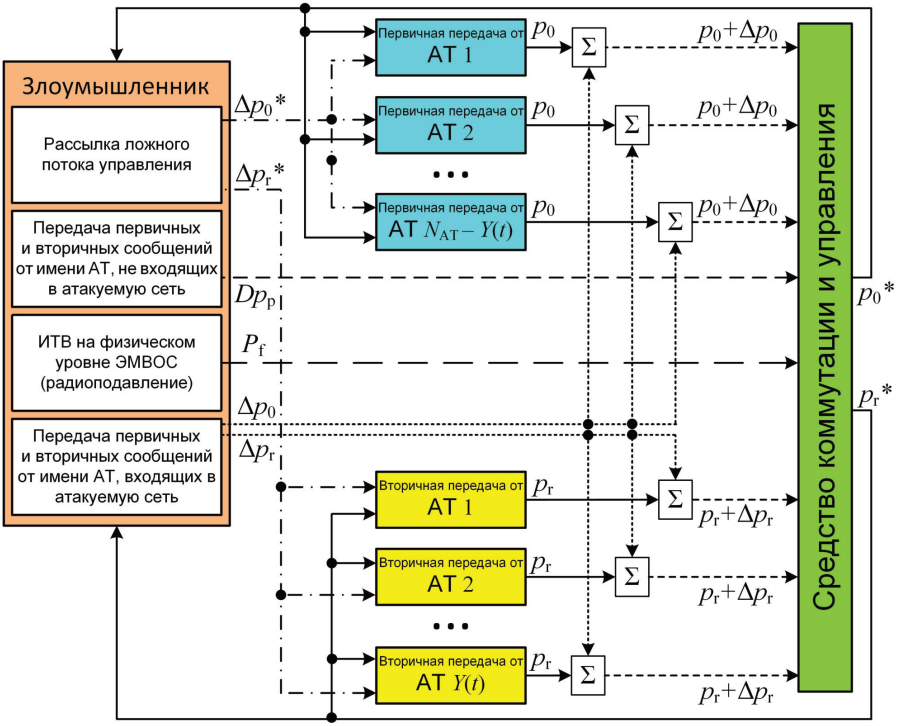


Рис. 36. Функциональная схема процедуры случайного множественного доступа к среде типа S-ALOHA

Злоумышленник в интересах создания коллизий в каждом временном слоте реализует следующие ИТВ:

- радиоподавление путем формирования с вероятностью P_f радиопомехи на физическом уровне ЭМВОС по линиям «вверх» (по линии «вниз» формирование такой помехи в наиболее общем случае нецелесообразно по причине высокой продолжительности ожидания эффекта);
- КА путем широковещательной рассылки по линии «вниз» ложного потока управления с параметрами Δp_0^* и Δp_r^*;
- КА путем передачи по линии «вверх» с вероятностью Dp_p первичных и вторичных сообщений от имени D АТ, не входящих в атакуемую сеть;
- КА путем передачи по линии «вверх» с вероятностями Δp_0 и Δp_r, соответственно, первичных и вторичных сообщений от имени N_{AT} АТ, входящих в атакуемую сеть.

Следует подчеркнуть, что указанные способы реализации КА разработаны эмпирическим методом. Рассматриваемая процедура представляется в виде марковской цепи с дискретным временем и дискретными состояниями (см. рис. 37).

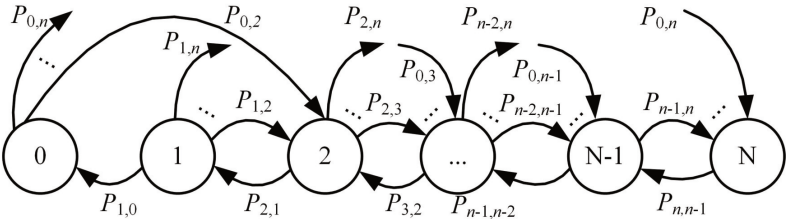


Рис. 37. Граф состояний марковской цепи процедуры случайного множественного доступа к среде типа S-ALOHA

Модель имеет $N_{\text{AT}}+1$ состояние, каждому из которых во временной слот t соответствует $Y(t)$ самоблокированных легитимных АТ, находящихся в режиме вторичной передачи. Если во временной слот t АТ одновременно передали $Y(t)$ сообщений, то в канале случайного множественного доступа к среде возникает коллизия и переданные сообщения буферизуются в $Y(t)$ АТ.

Рассматриваемая марковская цепь описывается матрицей $P = [p_{i,j}]$, где $i = Y(t)$, $j = Y(t+1)$. За один временной слот сеть может переместиться на одно состояние назад (успешная вторичная передача), остаться в том же состоянии (передача сообщений не осуществляется, или одна успешная первичная передача, или произошла коллизия, вызванная только вторичными сообщениями) или перейти на одно или несколько состояний вперед (произошла коллизия, вызванная только первичными сообщениями или одновременно первичными и вторичными сообщениями).

Пусть в текущем временном слоте $S_{\text{пер}}$ – количество первичных сообщений, одновременно переданных N_{AT} – $Y(t)$ АТ; $Q_{\text{втор}}$ – количество вторичных сообщений, одновременно переданных $Y(t)$ АТ; $U_{\text{зл}}$ – количество переданных злоумышленником сообщений от имени D АТ и (или) наличие радиопомехи на физическом уровне ЭМВОС. Тогда вероятность перехода $p_{i,j}$ примет следующий вид:

$$p_{i,j} = \begin{cases} 0, \text{ если } j \le i-2; \\ P_{S_{\text{пер}}=0} P_{Q_{\text{втор}}=1} P_{U_{\text{зл}}=0}, \text{ если } j = i-1; \\ P_{S_{\text{пер}}=1} P_{Q_{\text{втор}}=0} P_{U_{\text{зл}}=0} + P_{S_{\text{пер}}=0} P_{Q_{\text{втор}}\ge 1} + P_{S_{\text{пер}}=0} P_{Q_{\text{втор}}=1} P_{U_{\text{зл}}=1}, \text{ если } j = i; \\ P_{S_{\text{пер}}=1} P_{Q_{\text{втор}}\ge 1}, \text{ если } j = i+1; \\ P_{S_{\text{пер}}=j-i}, \text{ если } j \ge i+2; \end{cases}$$

$$\text{при } P_{S_{\text{пер}}=0} = \left(1-(p_0+\Delta p_0)\right)^{N_{\text{AT}}-i};$$

$$P_{Q_{\text{втор}}=0} = \left(1-(p_{\text{r}}+\Delta p_{\text{r}})\right)^{i}; \; P_{U_{\text{зл}}=0} = (1-Dp_{\text{p}})(1-P_{\text{f}}); \tag{19}$$

$$P_{S_{\text{пер}}=1} = (N_{\text{AT}}-i)(p_0+\Delta p_0)\left(1-(p_0+\Delta p_0)\right)^{N_{\text{AT}}-i-1};$$

$$P_{Q_{\text{втор}}=1} = i(p_{\text{r}}+\Delta p_{\text{r}})\left(1-(p_{\text{r}}+\Delta p_{\text{r}})\right)^{i-1}; \; P_{U_{\text{зл}}=1} = (1-Dp_{\text{p}})P_{\text{f}} + Dp_{\text{p}}(1-P_{\text{f}});$$

$$P_{S_{\text{пер}}=j-i} = \mathbf{C}_{j-i}^{N_{\text{AT}}-i}(p_0+\Delta p_0)^{j-i}\left(1-(p_0+\Delta p_0)\right)^{N_{\text{AT}}-j};$$

$$P_{Q_{\text{втор}}\ge 1} = 1-\left(1-(p_{\text{r}}+\Delta p_{\text{r}})\right)^{i}; \; \sum_{i=0}^{N_{\text{AT}}} P_i = 1.$$

Для нахождения предельных вероятностей моделируемых состояний такой цепи традиционно решается система из $N_{АТ}$ линейных однородных алгебраических уравнений. На основе полученных вероятностей в [208] вычисляется система показателей эффективности функционирования процедуры случайного множественного доступа к среде типа S-ALOHA в условиях ИТВ (см. рис. 38).

Для полученного значения вероятности $P_{св}$ успешного выполнения последовательности отдельных процедур канального уровня (для специализированных моделей) или передачи сообщения (для обобщенной модели), задавшись вероятностью гарантированного установления соединения $P_{гар}$, с учетом доступных статистических данных согласно ГОСТ [97] представляется возможным оценить параметры перехода из состояния S_6 в состояние S_9 и из состояния S_8 в состояние S_{11} на рис. 33. При этом отдельные значения математического ожидания времени перехода T вычисляются для наиболее пессимистичного случая по следующей формуле:

$$T = \tau_{мин} \frac{\ln P_{гар}}{\ln P_{св}}, \qquad (20)$$

где $\tau_{мин}$ – продолжительность минимального значимого для СЦР интервала времени (обычно это временной слот или так называемый «таймслот»).

Таким образом, в модели конфликта средства реализации КА и ПЗИ ИТС в отличие от моделей, изложенных в работах [135, 140, 190], в которых воспроизводятся КА на средства обработки информации АС, учтены возможности проведения КА на канальном и вышестоящих уровнях ЭМВОС, включая возможности средств реализации КА по выводу из строя, захвату управления и применения в своих целях ИТС, а также ответные меры ПЗИ на эти действия.

Это достигается за счет введения дополнительных конфликтно обусловленных транзитивных состояний:

- средство реализации КА анализирует управляющую информацию протоколов канального уровня;
- инициатором КА получен доступ к протоколам сетевого, транспортного и сеансового уровней;
- ПЗИ нейтрализует физический доступ;
- ПЗИ нейтрализует технический доступ;
- ПЗИ нейтрализует возможность доступа к протоколам сетевого транспортного и сеансового уровней;
- средство реализации КА нарушает доступность информации на канальном уровне;
- средство реализации КА нарушает доступность информации на сетевом, транспортное и/или сеансовом уровне;
- СПС применяет ИТС в своих целях;
- СПС осуществляет вывод ИТС из строя,

а также преобразования полученного полумарковского процесса, в котором плотности распределения времен переходов определяются обобщенным законом Эрланга ***n***-го порядка, в марковский процесс модифицированным методом Кендалла.

Рис. 38. Система показателей эффективности функционирования процедуры случайного множественного доступа к среде типа S-ALOHA в условиях информационно-технических воздействий

Модель позволяет исследовать влияние поражающей способности КА на работоспособность ИТС. Ее роль в данном исследовании состоит в том, что она:

- связывает модель процесса функционирования ИТС с моделью процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола (см. параграф 2.1);
- учитывает все известные поведенческие характеристики СПС.

3.5 Модель процесса функционирования специального программного обеспечения задачи управления устройством в боевых условиях

Модель процесса функционирования ОПО ИТС на рис. 31 с учетом процессов, характеризующих надежность информационных систем, в наиболее часто встречающихся на практике условиях, когда устранение ошибок в нем невозможно, и специальные требования к функционированию в режиме реального времени не предъявляются, представим в виде графа со следующими состояниями:

- C_1 – нормальное функционирование;
- C_2 – зависание (самовосстанавливающийся частичный отказ, перезагрузка не требуется);
- C_3 – сбой (самовосстанавливающийся частичный отказ, требуется перезагрузка);
- C_4 – отказ (например, по причине ошибки в программном коде);
- C_5 – восстановление.

Данная модель в полном объеме заимствована из [218]. Граф для нее показан на рис. 39.

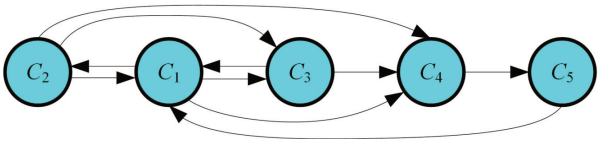


Рис. 39. Граф состояний динамики функционирования общего программного обеспечения информационно-технического средства

Модель процесса функционирования СПО, реализующего ИРЗ ИТС, аналогична модели ОПО. Но, исходя из практики, надежность ОПО может быть существенно выше надежности СПО, реализующего ИРЗ.

Модель процесса функционирования СПО, реализующего ЗО ИТС, в полном объеме может быть заимствована из известных источников. Эта модель рассматривается в связке с известными моделями процессов разведки, РЭП, воздействия мощным ЭМИ или связи (например, см. [51, 165, 267]). В частности, модель передачи сообщений другим ИТС по различным доступным линиям связи в условиях воздействий техники РЭБ, изложенная в [267] и рассмотренная выше в параграфе 3.4, позволяет оценить вероятность передачи сообщения в любой момент времени с учетом адаптивного применения различных мер помехозащиты.

Модель процесса функционирования СПО, реализующего ЗУ ИТС, должна учитывать, что при выполнении ЗУ задействуются как СПО, так и управляемые ИТС устройства. Модель, по сути, должна интегрировать в себе состояния модели ОПО (или ИРЗ), показанные на рис. 39, и состояния модели ТК ИТС, показанные на рис. 32. Однако известные модели, изложенные, например, в [133, 218], такой характер функционирования СПО не учитывают.

Для парирования этого обстоятельства предлагается модель, в которой с позиции теории надежности воспроизводится процесс функционирования СПО, реализующего ЗУ ИТС, и дополнительно формализуются неотъемлемые от него процессы функционирования устройства и возможности противника по уничтожению устройства и воздействию мощным ЭМИ на его электронную компонентную базу [35]. Граф этой модели показан на рис. 40.

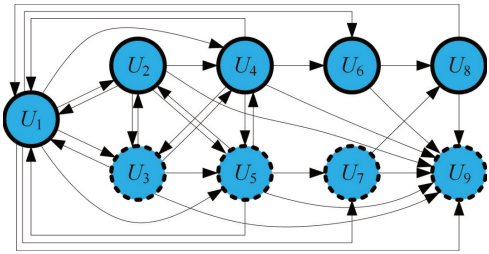


Рис. 40. Граф состояний, отражающий динамику функционирования специального программного обеспечения задачи управления информационно-технического средства

Состояния графа на рис. 40 имеют следующее описание:

- U_1 – нормальное выполнение;
- U_2 – зависание СПО;
- U_3 – зависание устройства;
- U_4 – сбой СПО;
- U_5 – сбой устройства;
- U_6 – отказ СПО;
- U_7 – отказ устройства;
- U_8 – восстановление работоспособности;
- U_9 – устройство уничтожено.

Дополнительно введенными состояниями в этом графе являются состояния «уничтожено», «зависание устройства», «сбой устройства», «отказ устройства» и «ремонт». Они показаны на рис. 40 прерывистой линией.

Таким образом модель процесса функционирования СПО ЗУ в боевых условиях в отличие от моделей, изложенных в работах [14, 133, 218], в которых процесс функционирования воспроизводится с позиции надежности, учитывает изменения процесса функционирования управляемого устройства при уничтожении или воздействии мощным ЭМИ на его электронную компонентную базу противником. Это достигается за счет введения дополнительных конфликтно обусловленных транзитивных состояний «зависание устройства», «сбой

устройства», «отказ устройства» и «ремонт» и терминального состояния «уничтожено», а также преобразования полученного полумарковского процесса, в котором плотности распределения времен переходов определяются обобщенным законом Эрланга ***n***-го порядка, в марковский процесс модифицированным методом Кендалла. Данная модель позволяет исследовать влияние ОП и воздействия мощным ЭМИ на работоспособность устройств, управление которыми осуществляется с применением СПО.

Модель процесса-диспетчера, определяющего дисциплину обслуживания ИРЗ, ЗО и ЗУ, может быть заимствована из теории массового обслуживания (например, см. [134]). Пример такой модели в виде простейшей одноканальной системы типа M/M/1 с множественным доступом и дисциплиной FIFO показан на рис. 41. Обозначения на рис. 41 приведены ниже в описании формулы (21).

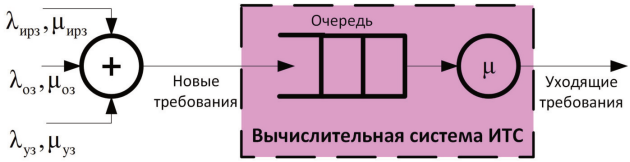


Рис. 41. Модель диспетчера задач информационно-технического средства

Совместное применение заимствованных и предложенных усовершенствованных моделей позволит далее выявить закономерности влияния средств ОП и воздействия мощным ЭМИ на работоспособность ТК ИТС, устройств и СПО ЗУ, влияния КА на работоспособность ИТС, а также рационально распределить параметры ПЗИ ИТС в боевых условиях за счет учета эффекта от способов реализации КА.

3.6 Показатели эффективности функционирования информационно-технического средства

Совокупность рассмотренных в настоящей главе моделей позволяет с использованием правил, изложенных при описании шага 5 алгоритма моделирования процесса функционирования ИТС АС в параграфе 3.2, определить следующие важные для применения АС в бою относительно самостоятельные показатели эффективности функционирования ИТС [35].

1. **Работоспособность** $E(t)$, определяемая как вероятность успешного выполнения ИРЗ, ЗО и ЗУ в момент времени t с использованием следующего выражения:

$$E(t)=\begin{cases}\dfrac{\rho P_{тк}(t)P_{опо}(t)\Omega_{Е}}{\lambda_{ирз}+\lambda_{зо}+\lambda_{зу}}\left(\begin{matrix}\lambda_{ирз}P_{ирз}(t)Q_{ирз}+\lambda_{зу}P_{зу}(t)Q_{зу}+\\ +\lambda_{зо}P_{зо}(t)Q_{зо}P_{РЭП}(t)\end{matrix}\right) \text{ для ИТС;}\\ P_{тк}(t) \text{ для устройства}\end{cases} \tag{21}$$

$$\text{при } \rho=\begin{cases}1, \text{ если } \mu_{ирз}+\mu_{зо}+\mu_{зу}\le\mu;\\ \dfrac{\mu}{\mu_{ирз}+\mu_{зо}+\mu_{зу}} \text{ в противном случае;}\end{cases}$$

$$\Omega_{\text{E}} = \begin{cases} P(\sum_{k=1}^{|\mathbb{C}|} \Xi_k)_{\text{совм}}, \text{ если } \mathbb{C} \neq \varnothing; \\ 0 \text{ в противном случае;} \end{cases}$$

$$P(\Xi_k) = \sum_{j=1\ldots8,10,13,15\ldots20} P_{k,S_j}(t),$$

где $Q_{\text{ирз}}$, $Q_{\text{зо}}$ и $Q_{\text{зу}}$ – показатели функциональной пригодности СПО ИРЗ, ЗО и ЗУ ИТС, соответственно, определяемые в интервале [0,1] (методику оценки см. в [42]);

$\lambda_{\text{ирз}}$, $\lambda_{\text{зо}}$ и $\lambda_{\text{зу}}$ – интенсивности поступления заявок на выполнение ИРЗ, ЗО и ЗУ в ИТС, соответственно;

$P_{\text{тк}}(t)$, $P_{\text{опо}}(t)$, $P_{\text{ирз}}(t)$, $P_{\text{зу}}(t)$, $P_{\text{зо}}(t)$ – вероятностно-временные характеристики нахождения в работоспособном состоянии ТК ИТС, ОПО, СПО ИРЗ, СПО ЗУ и СПО ЗО, соответственно;

$P_{\text{РЭП}}(t)$ – вероятностно-временная характеристика выполнения ЗО на физическом уровне ЭМВОС в условиях РЭП (см., например, модели в [72, 267]);

μ – максимальная производительность ИТС;

$\mu_{\text{ирз}}$, $\mu_{\text{зо}}$ и $\mu_{\text{зу}}$ – ресурсоемкости ИРЗ, ЗО и ЗУ в ИТС, соответственно;

$P(\ldots)_{\text{совм}}$ – вероятность суммы совместных событий;

$\mathbb{C}$ – множество СПС в ИТС;

Ξ_k – событие воздействия СПС k-го типа на ИТС;

j – индекс состояния конфликта средства реализации КА и ПЗИ ИТС на рис. 33, в котором ИТС работоспособно (j = 1…8, 10, 13, 15…20).

2. **Заразность** ИТС для СПС k-го типа $Z_k(t)$, определяемая как вероятность нахождения конфликта СПС k-го типа и ПЗИ ИТС в состоянии S_{15} на рис. 33 с учетом работоспособности ТК, ОПО, ЗО связи и функциональной пригодности СПО ЗО связи в момент времени t с использованием следующего выражения:

$$Z_k(t) = P_{\text{тк}}(t) P_{\text{опо}}(t) P_{\text{зо}}(t) Q_{\text{зо}} \Omega_{\text{Z}}$$

$$\text{при } \Omega_{\text{Z}} = \begin{cases} P(\sum_{k=1}^{|\mathbb{C}|} \Xi_k)_{\text{совм}}, \text{ если } \mathbb{C} \neq \varnothing; \\ 0 \text{ в противном случае;} \end{cases} \quad (22)$$

$$P(\Xi_k) = P_{k,S_{15}}(t).$$

Этот показатель позволяет учесть результаты моделирования процесса распространения СПС в информационно-управляющей сети АС (такая модель рассмотрена далее в параграфе 3.7) и тем самым предоставляет возможность для анализа процессов функционирования ИТС, которые изначально могут быть физически недоступны для техники реализации КА в боевых условиях.

3. **Подверженность дезинформации** с применением СПС $D(t)$, определяемая как вероятность нахождения конфликта средства реализации КА и ПЗИ ИТС в состоянии S_{16} на рис. 33 с учетом работоспособности ТК, ОПО, ЗО связи и функциональной пригодности СПО ЗО связи в момент времени t с использованием следующего выражения:

$$D(t) = P_{\text{тк}}(t) P_{\text{опо}}(t) P_{\text{зо}}(t) Q_{\text{зо}} \Omega_{\text{D}} \quad (23)$$

$$\text{при } \Omega_{\text{D}} = \begin{cases} P(\sum_{k=1}^{|\mathbb{C}|} \Xi_k)_{\text{совм}}, \text{ если } \mathbb{C} \neq \varnothing; \\ 0 \text{ в противном случае;} \end{cases}$$
$$P(\Xi_k) = P_{k,S_{16}}(t).$$

4. **Подверженность разведке** с применением СПС $V(t)$, определяемая как вероятность нахождения конфликта средства реализации КА и ПЗИ ИТС в состоянии S_{17} на рис. 33 с учетом работоспособности ТК, ОПО, СПО ЗО связи и функциональной пригодности СПО ЗО связи в момент времени t с использованием следующего выражения:

$$V(t) = P_{\text{тк}}(t) P_{\text{опо}}(t) P_{\text{зо}}(t) Q_{\text{зо}} \Omega_{\text{V}}$$
$$\text{при } \Omega_{\text{V}} = \begin{cases} P(\sum_{k=1}^{|\mathbb{C}|} \Xi_k)_{\text{совм}}, \text{ если } \mathbb{C} \neq \varnothing; \\ 0 \text{ в противном случае;} \end{cases} \quad (24)$$
$$P(\Xi_k) = P_{k,S_{17}}(t).$$

5. **Подверженность перехвату управления** с применением СПС $A(t)$, определяемая как вероятность нахождения конфликта средства реализации КА и ПЗИ ИТС в состоянии S_{13} на рис. 33 с учетом работоспособности ТК, ОПО, СПО ЗО связи, ЗУ и функциональной пригодности СПО ЗО связи и ЗУ в момент времени t с использованием следующего выражения:

$$A(t) = P_{\text{тк}}(t) P_{\text{опо}}(t) P_{\text{зо}}(t) Q_{\text{зо}} P_{\text{зу}}(t) Q_{\text{зу}} \Omega_{\text{A}}$$
$$\text{при } \Omega_{\text{A}} = \begin{cases} P(\sum_{k=1}^{|\mathbb{C}|} \Xi_k)_{\text{совм}}, \text{ если } \mathbb{C} \neq \varnothing; \\ 0 \text{ в противном случае;} \end{cases} \quad (25)$$
$$P(\Xi_k) = P_{k,S_{13}}(t).$$

Таким образом, в модели процесса функционирования ИТС АС в отличие известных моделей системной стратификации сложных процессов, изложенных в [163, 179, 229], при оценке показателей эффективности функционирования ИТС одновременно учтены вероятностно-временные характеристики состояний полумарковских процессов функционирования его ТК, ОПО, СПО ИРЗ, ЗУ и ЗО, конфликта средства реализации КА и ПЗИ ИТС. Это достигается за счет:

1) *преобразования* полумарковских процессов, в которых плотности распределения времен переходов определяются обобщенным законом Эрланга ***n***-го порядка, в марковские модифицированным методом Кендалла;
2) согласованного по времени *воспроизведения* иерархической совокупности этих процессов, достигаемого путем решения в каждом эпизоде применения АС задачи Коши для каждого процесса в едином масштабе времени с начальными условиями, соответствующими результирующему состоянию функционирования ИТС в предыдущем эпизоде;
3) *координирования* процессов функционирования СПО процессом-диспетчером в виде системы массового обслуживания типа M/M/1, неоднородный поток заявок которой характеризуется интенсивностями выполнения и ресурсоемкостью задач, а обслуживание заявок характеризуется максимальной производительностью ИТС.

Модель позволяет исследовать влияние ОП, КА и воздействия мощным ЭМИ на работоспособность, заразность, подверженность ИТС дезинформации, разведке и перехвату управления им. Роль модели состоит во взаимной увязке известных аспектов функционирования ИТС АС в боевых условиях.

В качестве примера для определения вероятностно-временных характеристик частных процессов функционирования ИТС рассмотрим СВТ из состава комплекта Р-175 [80]. Это СВТ по своим характеристикам может рассматриваться как аналогичное изделию AN/UYK-128, применяемому в АС FBCB2 и размещаемому, например, в автомобиле M1167A1 разведывательного взвода разведывательной роты ВС США [279]. СВТ из состава комплекта Р-175 работает под управлением ОПО и взаимодействует с аналогичными СВТ, образующими информационно-управляющую сеть ВФ. Рассмотрим вариант СПО СВТ из состава комплекта Р-175, обеспечивающий выполнение следующих задач:

- одну ЗУ (управление противотанковыми управляемыми ракетами);
- две ЗО (передача данных; навигационно-временное обеспечение посредством приема сигналов GPS и ГЛОНАСС);
- две ИРЗ (отображение местоположения ЭБП своего ВФ и ВФ противника на электронной карте местности; расчет данных для запроса артиллерийской и авиационной поддержки, боеприпасов и материально-технического обеспечения).

Пусть рассматриваемое СВТ из состава комплекта Р-175 применяется в условиях ОП и РЭБ. Значение показателя $P_{\text{РЭП}}(t)$ является константой и равно 0,85. Это ИТС кроме РЭП подвергается воздействию мощного ЭМИ, эффектом которого являются периодические зависания ТК ИТС. Условие $\mu \geq \mu_{\text{ирз}} + \mu_{\text{зо}} + \mu_{\text{зу}}$ для данного ИТС выполняется. Функциональная пригодность СПО $Q_{\text{ирз}} = Q_{\text{зо}} = Q_{\text{зу}} = 0{,}99$. Интенсивности поступления задач в примере равны [с^{-1}]: $\lambda_{\text{ирз}} = 1/30$, $\lambda_{\text{зо}} = 1/120$ и $\lambda_{\text{зу}} = 1/600$. Через информационно-управляющую сеть в ОПО СВТ из состава комплекта Р-175 в начале боя противник внедряет СПС. Вероятные математические ожидания времен переходов частных моделей процессов функционирования компонентов ИТС приведены в таблице 4. Рассматривается обобщенный закон Эрланга 2-го порядка (СКО равно 70 % от математического ожидания). Полученные для указанных исходных данных зависимости показаны на рис. 42-48.

Из рис. 42 видно, что в течение боя вероятность нормального функционирования ТК ИТС снижается на 65 %. Воздействие мощным ЭМИ почти не оказывает влияния на работу ТК (находится на уровне 1…1,5 %) по причине экранирования корпуса ИТС. В то же время зависание СПО ЗУ, как показано на рис. 43, снижает на 10 % работоспособность ИТС при выполнении этой задачи, которая с учетом уничтожения управляемого устройства снижается на 38 %. Динамика работоспособности ОПО и СПО ИРЗ/ЗО сравнивается на рис. 44 и 45. Из-за меньшей надежности программ работоспособность СПО ИРЗ в течение боя в среднем составляет 88 %, в то время как работоспособность ОПО находится на уровне 94 %.

Таблица 4 — Вариант исходных данных для СВТ из состава комплекта Р-175

Модель	s	v	τ	s	v	τ	s	v	τ	s	v	τ	s	v	τ
ТК	1	2	10 мин	1	6	30 мин	2	4	–	3	4	–	4	6	–
	1	3	–	2	1	10 с	2	6	30 мин	3	6	–	5	1	–
	1	4	–	2	3	–	3	1	–	4	5	–	5	6	–
ОПО	1	2	5 мин	1	4	–	2	3	60 мин	3	1	1 мин	4	5	–
	1	3	60 мин	2	1	20 с	2	4	–	3	4	–	5	1	–
Конфликт средства реализации КА и ПЗИ ИТС	1	2	60 с	6	3	–	9	5	–	11	5	–	18	19	15 мин
	1	3	–	6	5	–	10	12	15 с	11	7	–	18	21	5 мин
	2	3	–	6	7	–	10	13	15 с	12	18	5 мин	19	20	1 с
	2	4	30 с	6	8	30 с	10	14	15 с	13	10	10 мин	20	10	10 мин
	3	1	–	6	9	–	10	15	15 с	13	18	5 мин	20	18	5 мин
	4	3	–	7	6	–	10	16	15 с	14	18	5 мин	20	19	15 мин
	4	5	–	8	10	1 с	10	17	15 с	15	10	15 с	20	21	5 мин
	4	6	1 с	8	11	–	10	20	30 мин	16	10	60 с	21	22	120 с
	5	2	–	9	3	–	11	3	–	17	10	30 с	22	1	30 с
ИРЗ/ЗО	1	2	150 с	1	4	60 мин	2	3	30 мин	3	1	30 с	4	5	30 с
	1	3	30 мин	2	1	20 с	2	4	60 мин	3	4	60 мин	5	1	2 мин
ЗУ	1	2	150 с	2	1	20 с	3	4	30 мин	4	9	30 мин	6	9	30 мин
	1	3	10 мин	2	3	10 мин	3	5	–	5	1	–	7	8	–
	1	4	30 мин	2	4	30 мин	3	9	30 мин	5	2	–	7	9	–
	1	5	–	2	5	–	4	1	30 с	5	4	–	8	1	2 мин
	1	6	60 мин	2	9	30 мин	4	3	10 мин	5	7	–	8	9	30 мин
	1	7	–	3	1	10 с	4	5	–	5	9	–	–		
	1	9	30 мин	3	2	150 с	4	6	60 мин	6	8	30 с			

Примечания: τ – математическое ожидание продолжительности перехода из s-го в v-е состояние; «–» – время, большее длительности боя.

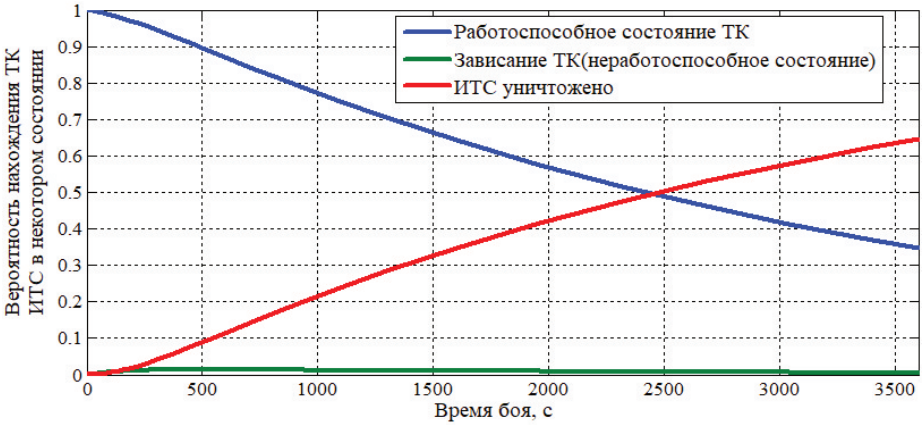


Рис. 42. Динамика состояний технического компонента информационно-технического средства

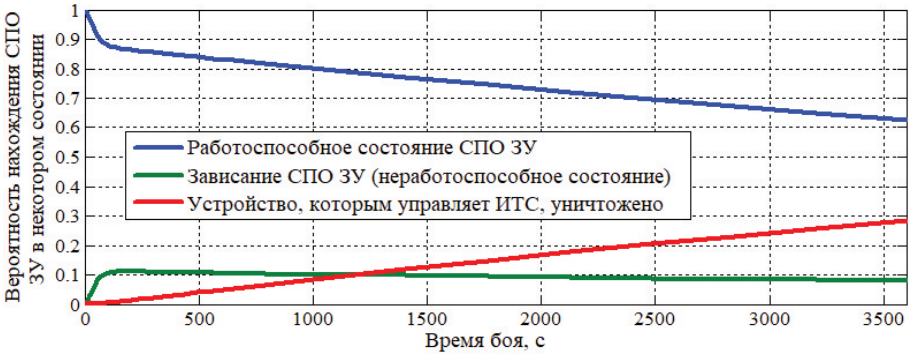


Рис. 43. Динамика состояний для специального программного обеспечения задачи управления устройством, выполняемой информационно-техническим средством

Рис. 44. Динамика состояний для общего программного обеспечения информационно-технического средства

Рис. 45. Динамика состояний для специального программного обеспечения информационно-расчетных задач и задач обеспечения, выполняемых информационно-техническим средством

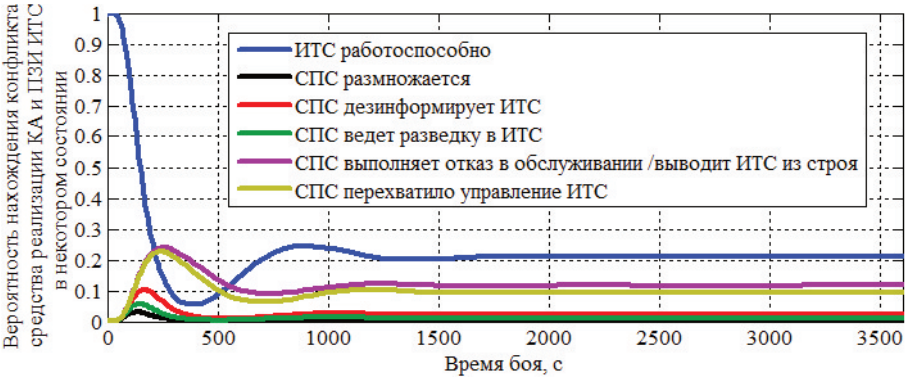


Рис. 46. Динамика состояний в конфликте средства реализации кибератак и подсистемы защиты информации информационно-технического средства

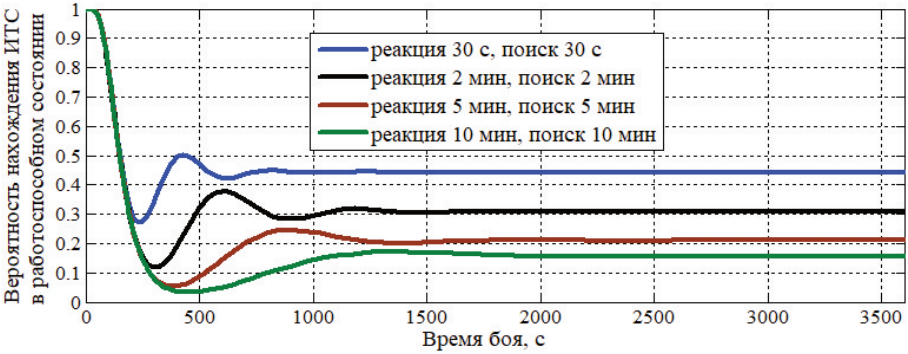


Рис. 47. Динамика работоспособности информационно-технического средства при различном времени реакции подсистемы защиты информации и поиска специальных программных средств

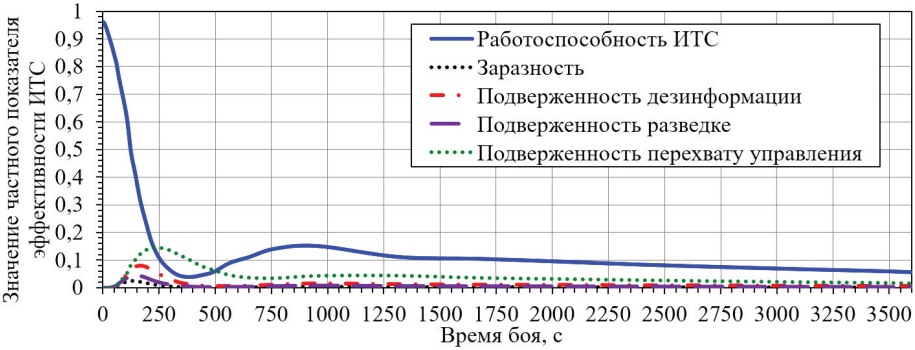


Рис. 48. Динамика показателей функционирования информационно-технического средства

Зависимости на рис. 46 показывают, что для указанных в таблице 4 характеристик информационного конфликта средства реализации КА и ПЗИ ИТС в течение боя с применением СПС ИТС подвержено дезинформации с вероятностью 0,02, разведке с вероятностью 0,01, перехвату управления с вероятностью 0,1 и выводу из строя с вероятностью 0,12. При этом СПС размножается с вероятностью 0,006. Результатом этого конфликта является снижение работоспособности ИТС на 78 %. Такой уровень работоспособности во многом обусловлен параметрами функционирования ПЗИ ИТС в условиях КА.

Динамика работоспособности ИТС при различном времени реакции ПЗИ ИТС и поиска СПС в рассматриваемом случае показана на рис. 47. На нем видно, что увеличение оперативности ПЗИ (в таблице 4 это времена переходов 12-18, 13-18, 14-18 и 18-21, равные 5 минутам) в 2,5 раза приводит к росту работоспособности ИТС на 52 %, а ее увеличение в 10 раз повышает работоспособность ИТС в 2,1 раза (рассматривается установившийся режим после 15…20 минут боя). В ходе исследования установлено, что зависимость работоспособности ИТС от оперативности ПЗИ в установившемся режиме является логарифмической и определяется по формуле

$$P(t) = -\boldsymbol{\alpha} \ln T_{\text{ПЗИ}} + \boldsymbol{\beta}, \tag{26}$$

где $P(t)$ – вероятностно-временная характеристика нахождения ИТС в работоспособном состоянии в конфликте СПС и ПЗИ ИТС;

$1 \geq \boldsymbol{\alpha} > P(t)$ и $1 \geq \boldsymbol{\beta} > 0$ – параметры, зависящие от исходных данных (в рассматриваемом случае $\boldsymbol{\alpha} = 0{,}1$, $\boldsymbol{\beta} = 0{,}79$);

$T_{\text{ПЗИ}}$ – оперативность ПЗИ ИТС [с].

С учетом формулы (26) имеет место следующая аналитическая зависимость, полезная для обоснования требований к оперативности ПЗИ ИТС:

$$T_{\text{ПЗИ}} = e^{\frac{\boldsymbol{\beta} - P(t)}{\boldsymbol{\alpha}}}. \tag{27}$$

Аналогично представляется возможным обосновать параметры оперативности ПЗИ на канальном уровне, а также параметры СПС при фиксированных значениях иных параметров модели.

На рис. 48 показана динамика показателей функционирования ИТС. Из него видно, что в заданных условиях работоспособность ИТС в течение первых 4…5 минут боя снижается на 90 %. Этот эффект обусловлен, во-первых, уничтожением ИТС в бою, и, во-вторых, внедрением и деструктивным действием СПС. При этом значение имеют не только функции СПС, которые могут отличаться от указанных в таблице 4, но и сам факт применения СПС, требующий ресурсов на его устранение и восстановление работоспособности ИТС.

Следует отметить, что исходные данные для модели конфликта средства реализации КА и ПЗИ ИТС на уровнях ЭМВОС от *прикладного* до *сетевого* определяются по результатам применения моделей, изложенных, например, в работах [135, 173, 275], а на *канальном* уровне ЭМВОС – по результатам применения моделей, изложенных, например, в работах [207-212]. Модели в данных работах могут учитывать способы реализации КА, разработанные с применением метода, ранее рассмотренного в параграфе 2.2. Исходные данные для модели процесса функционирования ИТС в части выполнения

ЗО на *физическом* уровне ЭМВОС в условиях РЭП могут быть получены, например, на основе использования моделей, изложенных в [2, 72, 143, 267].

Выводы. Таким образом, применение совокупности взаимосвязанных моделей процессов функционирования элементов АС в боевых условиях впервые позволило выявить закономерности влияния средств ОП и воздействия мощным ЭМИ на работоспособность ТК ИТС, устройств и СПО ЗУ, влияния КА на работоспособность ИТС и обосновать следующие, согласующиеся с практикой, закономерности:

- в части модели конфликта средства реализации КА и ПЗИ ИТС – закономерность влияния КА на работоспособность ИТС в интересах обоснования требований к оперативности ПЗИ ИТС, а также к параметрам КА, способы реализации которых разработаны в том числе на основе предложенной в параграфе 2.1 модели процесса информационного взаимодействия ИТС АС по известной процедуре телекоммуникационного протокола. Установлена аналитическая зависимость оперативности ПЗИ при обнаружении и поиске СПС от параметров СПС и требуемой работоспособности ИТС;
- в части моделей процессов функционирования ТК ИТС (или устройства) и СПО ЗУ в боевых условиях – закономерности влияния средств ОП и воздействия мощным ЭМИ на работоспособность ТК ИТС, устройств и СПО ЗУ в интересах оценки влияния этих средств на процесс функционирования ИТС;
- в части модели процесса функционирования ИТС АС – закономерности влияния конфликтно обусловленных факторов боя, включая в том числе КА противостоящего ВФ, на работоспособность ИТС, его заразность для других ИТС, объединяемых с ним единой информационно-управляющей сетью своего ВФ, и подверженность дезинформации, разведке и перехвату управления в интересах взаимосвязи совокупности моделей процессов функционирования компонентов АС и модели процессов функционирования АС в боевом эпизоде, рассмотренной далее в главе 4.

3.7 Модель процесса распространения специальных программных средств в информационно-управляющей сети, образуемой информационно-техническими средствами автоматизированных систем

Анализ предметной области. Основными характерными чертами информационно-управляющих сетей АС, применяемых в боевых циклах ВФ, с позиции распространения в них СПС (в литературе СПС, способные распространяться по сети, часто называются «вирусами») являются [33]:

- априорная ограниченность информации о составе программ и ТК узловых ИТС сетей;
- фиксированная структура сетей, коррелирующаяся с иерархической структурой ВФ и включающая от десятков до тысяч узлов;

- существование среднестатистических временных характеристик функционирования конкретных СПС в узлах сетей ВФ, соответствующих вектору целей и возможностям этих средств;
- существование среднестатистических временных характеристик функционирования ПЗИ сетевых узлов.

Очевидно, что оценка защищенности сетей АС от воздействия СПС с применением натурных методов моделирования в подавляющем большинстве случаев является крайне дорогостоящей. Известен широкий спектр результатов отечественных и зарубежных исследований в области моделирования процесса распространения СПС. Эти результаты делятся на два основных направления [146, 153]: аналитическое и имитационное.

Модели аналитического направления, в свою очередь, можно разделить на две группы. Модели первой группы (например, [146, 293, 309]) не учитывают структуру сетей, но предоставляют возможность для анализа важных с точки зрения вирусной угрозы состояний узлов с учетом времени. Исторически сложилось, что такие модели явились пионерскими в рассматриваемой области и были заимствованы из математических основ эпидемиологии. В этих моделях все множество объектов в зоне риска разделялось на несколько подмножеств «инфицированных», «уязвимых к заражению», «излеченных» и т.д., а динамика численности этих подмножеств описывалась дифференциальными уравнениями. Модели второй группы учитывают структуру сетей. Но они либо ограничены использованием заведомо недостаточного количества состояний узлов по причине высокой вычислительной сложности применяемых методов (например, [105, 199]), либо не дают информации о состоянии защищенности каждого конкретного узла сети в заданный момент времени (например, [259]).

Классификация моделей и систем имитационного направления процесса распространения СПС представлена, например, в [154]. Эти модели получили широкое применение в условиях появления высокопроизводительных систем имитационного моделирования, в том числе объектно-ориентированных. Пример такой системы показан в [156]. Они обеспечивают высокую точность моделирования при большом количестве сетевых узлов. Но такие модели требуют детального знания алгоритмов информационного взаимодействия узлов сети, которые зачастую недоступны для исследователя.

Для наиболее вероятных на практике исходных данных только о структуре сетей ВФ и среднестатистических временных характеристиках функционирования СПС и ПЗИ их узлов приоритет имеют аналитические модели. Они отличаются высокой скоростью моделирования и возможностью получения решения «в общем виде» [153]. Однако попытки применения известных аналитических моделей процесса распространения СПС или их комбинаций для потенциально доступного набора исходных данных о сетях ВФ оказались безуспешными, поскольку преимущества этих моделей с лихвой перекрывались их недостатками.

Постановка задачи: разработать модель процесса распространения СПС в сетях различной структуры, позволяющую в различные моменты времени

оценить вероятность заражения несколькими СПС каждого узла с учетом характеристик СПС и ПЗИ.

Формирование исходных данных. Предлагаемый подход к решению указанной задачи требует следующих исходных данных:

- количество узлов сети и структура связей;
- интервалы с момента инициирования узлами соединений до момента окончания этих соединений;
- количество типов СПС;
- количество экземпляров СПС каждого типа;
- вероятности изначального заражения сети различными экземплярами СПС;
- интервалы внедрения нескрытных СПС;
- поведенческие характеристики СПС и ПЗИ в каждом узле сети;
- интервал моделирования;
- точность метода решения задачи Коши.

Формализация модели. Пусть сеть представляет собой ориентированный граф, состоящий из N узлов. Каждая дуга характеризуется среднестатистическим временным интервалом между штатными сеансами связи i-го узла с j-м узлом $\tau_{i,j}$ (по инициативе i-го узла). В различные моменты времени сеть заражается V типами СПС по q_v экземпляров с различными вероятностями изначального заражения μ_g ($g = 1 \ldots q_v$). СПС могут обеспечивать или не обеспечивать скрытность своего распространения (далее – скрытные и нескрытные СПС, соответственно). Скрытному СПС, находящемуся в i-м узле, для заражения j-го узла необходимо дождаться штатного сеанса связи между i-м и j-м узлами. Нескрытное СПС, попав в i-й узел, приступает к инициированию сеанса связи с j-м узлом независимо от штатных сеансов связи. Временная диаграмма заражения j-го узла СПС v-го типа, находящимся в i-м узле, показана на рис. 49.

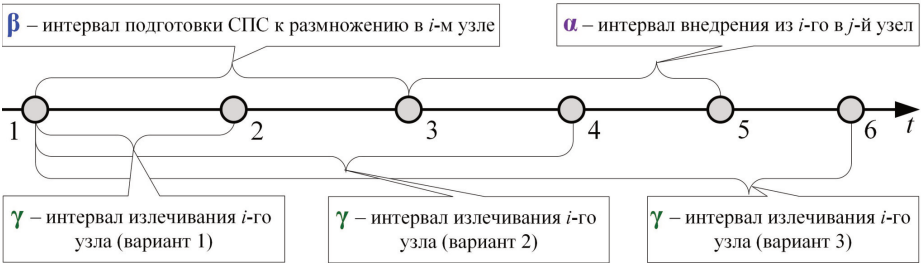


Рис. 49. Временная диаграмма заражения специальным программным средством узла сети

На нем в точке 1 на временной оси СПС внедрилось в i-й узел и начинает подготовку к размножению. СПС готово к размножению из i-го узла в точке 3. От точки 3 до точки 5 СПС внедряется из i-го в j-й узел. ПЗИ i-го узла стремится удалить или нейтрализовать СПС. Излечивание начинается с точки

1 и, в зависимости от возможностей ПЗИ, заканчивается либо в точках 2 (вариант 1) или 4 (вариант 2) и тогда СПС не сможет размножиться, либо в точке 6 (вариант 3) и тогда СПС размножится. СПС не внедряется в узел по причине информационной несовместимости, то есть когда оно «не знает» протоколы узла или их уязвимости. Значение интервала передачи СПС *v*-го типа между связанными *i*-м и *j*-м узлами предлагается вычислять по формуле

$$m_{v,i,j} = \begin{cases} \alpha_{v,i,j} + \beta_{v,i}, \text{ если } \gamma_{v,i} > \alpha_{v,i,j} + \beta_{v,i}; \\ \infty, \text{ если} \left(\begin{matrix} \text{СПС информационно} \\ \text{несовместимо с узлом} \end{matrix} \right) \vee \left(\gamma_{v,i} \le \alpha_{v,i,j} + \beta_{v,i} \right), \end{cases} \quad (28)$$

где $\alpha_{v,i,j}$ – интервал с момента готовности СПС *v*-го типа к размножению в *i*-м узле до момента его внедрения в *j*-й узел;

$\beta_{v,i}$ – интервал с момента внедрения СПС *v*-го типа в *i*-й узел до момента, когда это СПС будет готово к размножению;

$\gamma_{v,i}$ – интервал с момента внедрения СПС *v*-го типа в *i*-й узел до момента, когда данный узел от этого СПС будет излечен.

Сеансы связи между парой связанных узлов сети могут устанавливаться либо по инициативе только одного из них (например, в большинстве пар «клиент-сервер» сеансы связи инициируются только клиентами), либо по инициативе любого узла из этой пары (например, в паре связанных сетевых абонентских терминалов сеанс связи может инициировать любой из них).

Поскольку скрытное СПС может передаваться независимо от того, какой из двух связанных узлов является инициатором сеанса связи, **значение показателя $\alpha_{v,i,j}$** предлагается вычислять с использованием формулы

$$\alpha_{v,i,j} = \begin{cases} \dfrac{\tau_{i,j}\tau_{j,i}}{\tau_{i,j} + \tau_{j,i}}, \text{если} \left(\begin{matrix} \text{связь инициируется} \\ \text{обоими узлами} \end{matrix} \right) \wedge (\text{СПС скрытное}); \\ \tau_{i,j}, \text{ если} \left(\begin{matrix} \text{связь инициируется} \\ \text{только одним узлом} \end{matrix} \right) \wedge (\text{СПС скрытное}); \\ \tau_v, \text{ если СПС нескрытное}, \end{cases} \quad (29)$$

где τ_v – интервал внедрения нескрытного СПС *v*-го типа. Значение этого показателя является одинаковым для всех узлов сети и является исходной характеристикой поведения СПС этого типа.

Поведенческие характеристики СПС рассмотрены в работах [35, 36] и изложены в параграфе 3.4, где анализируется конфликт средства реализации КА и ПЗИ ИТС. В таком конфликте СПС находится в трех основных режимах функционирования: подготовка к применению, скрытное и открытое применение, а ПЗИ выполняет типовые задачи по предупреждению, обнаружению и устранению последствий воздействия СПС. Полагая отлаженными процессы сопряжения узлов в сети друг с другом, этот конфликт с позиции распространения СПС в сетях сводится к частному конфликту СПС и ПЗИ узла, граф состояний которого представлен на рис. 50.

Состояния в графе на рис. 50 имеют следующее описание:

- A_1 – СПС внедрилось в программную среду узла и анализирует его текущее состояние;

- A_2 – СПС проводит отказ в обслуживании узла, приводящий к невозможности выполнения любых задач;
- A_3 – СПС использует функции узла в своих целях;
- A_4 – СПС осуществляет вывод узла из строя;
- A_5 – СПС размножается;
- A_6 – СПС дезинформирует узел;
- A_7 – СПС проводит разведку;
- A_8 – ПЗИ проводит принудительный поиск СПС;
- A_9 – СПС осуществляет самомодификацию;
- A_{10} – СПС перешло в режим ожидания;
- A_{11} – СПС излечено.

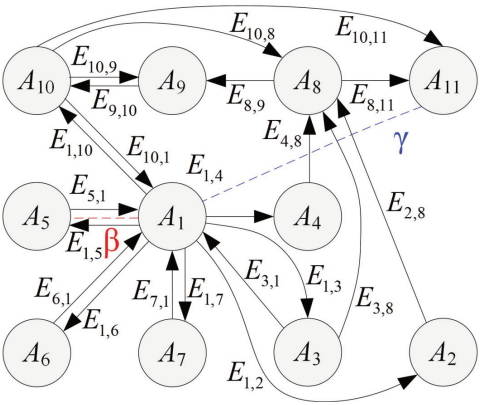


Рис. 50. Граф состояний динамики конфликта специального программного средства и подсистемы защиты информации узлового информационно-технического средства информационно-управляющей сети

Значение показателя $\beta_{v,i}$ в формуле (28) равно значению интервала $E_{1,5}$ перехода i-го узла из состояния A_1 в состояние A_5 и является исходной поведенческой характеристикой СПС v-го типа.

Значение показателя $\gamma_{v,i}$ в формуле (28) равно интервалу перехода рассматриваемого конфликта i-го узла из состояния A_1 в состояние A_{11} при воздействии СПС v-го типа. Это значение вычисляется следующим образом.

Интервалы переходов конфликта СПС и ПЗИ узла из одного состояния в другое не имеют экспоненциальный характер, а коррелируют с некоторой средней величиной. Для анализа такого конфликта применим метод аналитического описания процессов, изложенный в [266] и рассмотренный в параграфе 3.1. Полученный с применением этого метода граф марковского процесса для показанного на рис. 50 конфликта СПС и ПЗИ узла при $\boldsymbol{n}$ = 2 содержит 165 псевдосостояний и 1 319 переходов, а при $\boldsymbol{n}$ = 3 данный граф содержит уже 2 305 псевдосостояний и 20 298 переходов. С учетом изложенного **значение показателя $\gamma_{v,i}$** может быть получено с применением следующего алгоритма.

Шаг 1. Решение задачи Коши для марковского процесса конфликта СПС v-го типа и ПЗИ в j-м узле численным методом с начальным условием равенства единице вероятности нахождения процесса в состоянии A_1 и нулевых вероятностей – для других состояний.

Шаг 2. Вычисление значения показателя $\gamma_{v,i}$ как интервала времени с момента, когда конфликт СПС и ПЗИ вышел из состояния A_1, до момента, когда этот конфликт перешел в состояние A_{11}, с учетом того, что изображенный на рис. 50 процесс не является стационарным:

$$\gamma_{v,i} = t\,(P_{i11} = \xi_{i11} - \upsilon) - t\,(P_{i1} = \xi_{i1} - \upsilon), \qquad (30)$$

где $t\,(P_{i11} = \xi_{i11} - \upsilon)$ – момент времени установления в i-м узле процесса конфликта СПС и ПЗИ в состоянии A_{11} с вероятностью $\xi_{i11} - \upsilon$;

$t\,(P_{i1} = \xi_{i1} - \upsilon)$ – момент времени, после которого процесс конфликта СПС и ПЗИ для i-го узла находится в состоянии A_1 с вероятностью меньше $\xi_{i1} - \upsilon$;

υ – погрешность численного метода решения задачи Коши;

ξ_{i1} и ξ_{i11} – достаточные вероятности нахождения процесса конфликта СПС и ПЗИ i-го узла в состояниях A_1 и A_{11}, соответственно.

Поскольку рассматриваемая математическая модель оперирует среднестатистическими временными интервалами, то показатели ξ_{i1} и ξ_{i11} в формуле (30) предлагается определять как вероятности нахождения процесса конфликта СПС и ПЗИ в состояниях A_1 и A_{11} в так называемый «медианный» момент времени. «Медианным» называется момент времени, в котором площадь, ограниченная кривой распределения вероятности соответствующего состояния, делится пополам.

Полученные значения интервалов передачи СПС между связанными узлами предлагается использовать для анализа процесса распространения СПС в сетях различной структуры с применением указанного выше метода [266]. Для этого состояния процесса распространения СПС отождествляются с узлами сети, а переходы между состояниями – со связями между этими узлами. Такое отождествление уместно для наиболее часто встречающегося на практике случая, когда ПЗИ узлов запоминают излеченные ими СПС, приобретая тем самым иммунитет к ним. Поэтому разработка модели предполагает выполнение алгоритма, состоящего из следующих этапов.

Этап 1. Вычисление $\gamma_{v,i}$ с применением вышеуказанного алгоритма для каждого узла сети и каждого типа СПС.

Этап 2. Представление сети в виде ориентированного графа, в котором переходы характеризуются интервалами $m_{v,i,j}$, вычисляемыми по формуле (28).

Этап 3. Преобразование построенного на этапе 2 графа в марковский процесс с использованием метода, предложенного в [266].

Этап 4. Вычисление вероятностно-временных характеристик заражения всех узлов сети всеми экземплярами СПС всех типов. Для этого для полученного на этапе 3 марковского процесса решается задача Коши для каждого экземпляра каждого СПС. Начальные условия для решения задачи Коши: вероятность нахождения экземпляра СПС в том узле, который этим СПС заражен изначально, равна единице (в остальных узлах равна нулю); начальное время соответствует времени начала действия экземпляра СПС.

Этап 5. Проверка заражения каждого *i*-го узла СПС *v*-го типа по формуле

$$P_{v,i}(t)=\begin{cases}0, \text{ если } \max\limits_{g=1\ldots q_v}\{P_{g,i}(t)\mu_g\}<\dfrac{1}{N\sqrt{n}};\\ 1 \text{ в противном случае,}\end{cases} \quad (31)$$

где $P_{g,i}(t)$ – вероятностно-временная характеристика заражения *i*-го узла *g*-м экземпляром СПС *v*-го типа;

μ_g – вероятность исходного заражения сети *g*-м экземпляром СПС *v*-го типа;

N – количество уязвимых и доступных для СПС узлов сети;

n – используемый порядок обобщенного закона Эрланга ($\boldsymbol{n}^{-0,5}$ – коэффициент вариации [7], характеризующий СКО времени сеансов связи).

Рассмотрим пример информационно-управляющей сети ВФ, подверженной СПС. В качестве примера ВФ рассмотрим мотострелковый батальон (далее – мсб), усиленный танковой ротой. Структура этого ВФ повторяет структуру мотопехотного батальона (далее – мпб) механизированной бригады «Страйкер» (далее – мбр). Отличие состоит только во взводе мобильных орудий в каждой роте мпб. Это отличие компенсируется приданием мсб танковой роты для выполнения конкретной боевой задачи, предусматривающей придание каждой роте мсб по одному танковому взводу. Такой состав ВФ обусловлен стремлением получить относительно универсальные результаты исследования.

Согласно [279] в мпб используется 103 ед. ИТС AN/UYK-128 (аналог СВТ из состава комплекта Р-175), размещаемых на мобильной базе различного класса. Непосредственно в боевых циклах мпб применяются 73 ед. таких ИТС. Сеть мпб через сеть WIN-T с использованием спутниковый аппаратуры Ku/Ka-диапазона частот AN/MRC-150, находящейся в штабе этого ВФ, связана с штабом мбр. Для выхода в сеть WIN-T используется аппаратура OL-701A/TYQ со средством засекречивания связи KOI-18/TSEC [279]. Аналогичная по характеристикам аппаратура используется и в мсб. Учитывая, что для реализации КА дешифрация информации за время оперативной ценности в тактическом звене между штабами мсб (мпб) и мсбр (мбр) является весьма ресурсоемкой задачей, рассмотрим рациональную ситуацию внедрения СПС только в сеть мсб (мпб). Граф такой сети показан на рис. 51.

По интенсивности сеансы связи в сети делятся на три категории. Для категории I $\tau_{i,j} = 300$ с, для категории II $\tau_{i,j} = 120$ с и для категории III $\tau_{i,j} = 60$ с. Сеть поражается СПС двух типов: скрытным и нескрытным, у которого $\tau = 10$ с. Продолжительность боя задается равной одному часу. Деструктивные функции СПС не рассматриваются. Оперативность ПЗИ не позволяет выявить СПС в течение боя (то есть в формуле (28) $\gamma_{v,i} > \alpha_{v,i,j} + \beta_{v,i}$). Для всех СПС интервал с момента внедрения в узел до готовности к размножению β равен 1 с. Во всех каналах $\tau_{i,j} = \tau_{j,i}$. В результате применения алгоритма автоматизированного преобразования аналитического описания немарковского процесса в марковский, рассмотренного в параграфе 3.1, для обобщенного закона Эрланга при $n = 2$ сеть включает 1 356 псевдосостояний и 11 905 переходов.

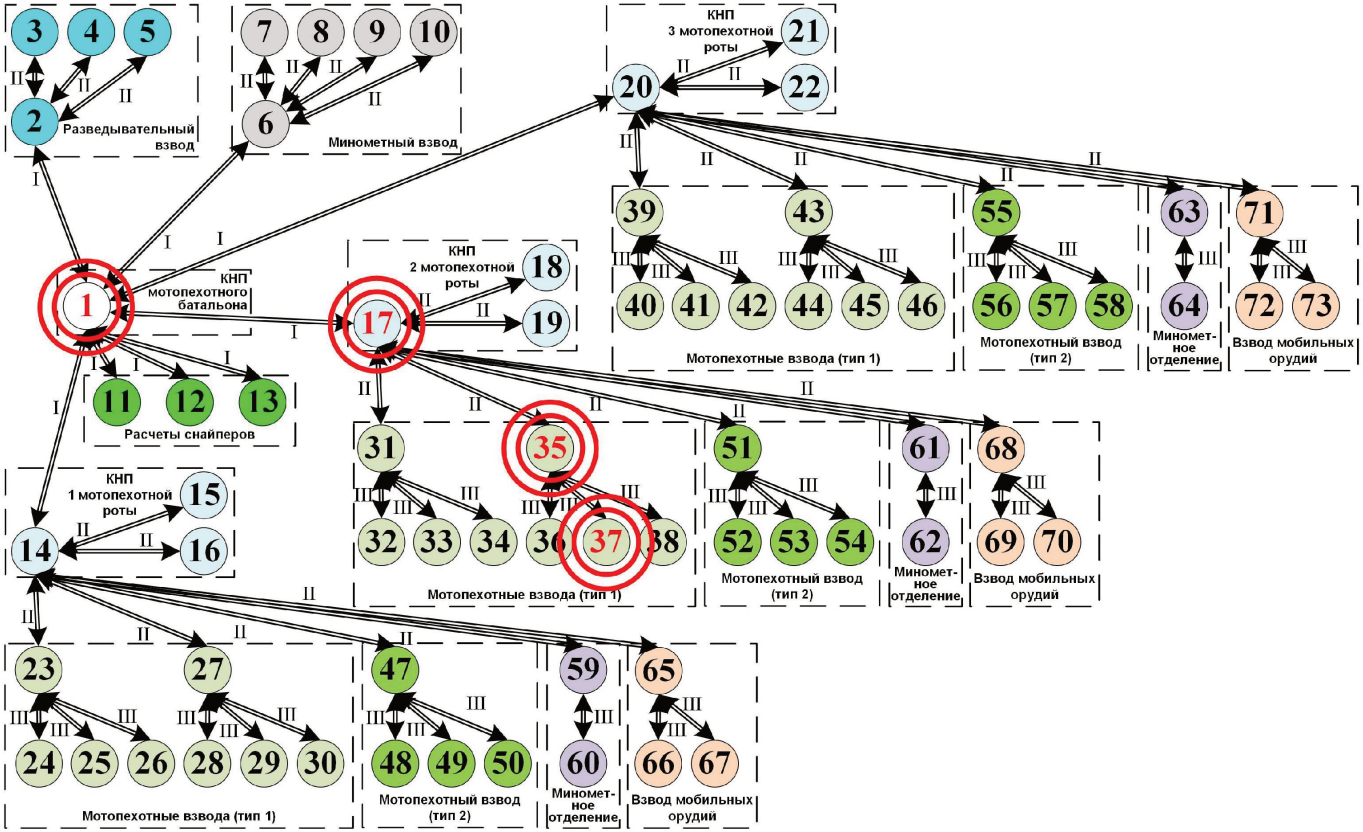


Рис. 51. Граф сети, обеспечивающей боевые циклы мотострелкового батальона, усиленного танковой ротой, или мотопехотного батальона

Вариант 1. Заражение в начале боя одного узла сети (№ 1, № 17, № 35, № 37) одним СПС. Результаты моделирования показаны на рис. 52 и 53.

Результаты, отраженные на этих рисунках, подтверждают широко известный из практики факт, состоящий в том, что нескрытные СПС размножаются быстрее, чем скрытные. При этом рациональным является заражение КНП батальона. На рис. 52 показано, что при заражении командно-наблюдательного пункта (КНП) батальона нескрытным СПС сеть полностью заражается через две минуты.

При невозможности заражения центрального узла целесообразно выбирать наиболее доступный узел, поскольку различие в эффективности СПС при заражении узлов 2…4 уровней нивелируется в течение 1…2 минут. Нескрытные СПС имеют непродолжительный период актуальности ввиду относительно быстрого приобретения ПЗИ целевых ИТС иммунитета к ним, но обновление ПЗИ в боевых условиях может быть затруднительным. В боевой обстановке рациональными с точки зрения сохранения актуальности для будущего применения являются скрытные СПС. Из рис. 53 следует, что при применении скрытных СПС в качестве эпицентра размножения допустимо использовать любой доступный узел, что значительно упрощает процесс применения техники реализации КА. Однако в течение боя скрытное СПС заражает в два раза меньше узлов мсб(мпб), чем нескрытное.

Вариант 2. Одновременное заражение двух узлов в начале боя. Результаты моделирования, когда узел № 1 заражается скрытным СПС и узел № 37 нескрытным, показаны на рис. 54. Они свидетельствуют о нецелесообразности в случае применения нескрытного СПС дополнительно применять скрытное СПС на любом уровне иерархии узлов сети, поскольку выигрыш в 7 узлов достигается только с 25 секунды по третью минуту боя. Результаты моделирования для случая заражения тех же узлов скрытными СПС показаны на рис. 55. Из него следует, что при таких исходных данных со второй минуты до конца боя прирост числа зараженных узлов составляет 8…16 ед. (то есть 36…64 %).

Вариант 3. Заражение скрытными СПС в течение боя. На рис. 56 показаны результаты при заражении на пятой минуте узла № 57, на восьмой минуте узла № 25 и на десятой минуте боя узла № 37. Результаты моделирования последовательного заражения этих трех узлов в течение боя показаны на рис. 57. Из них следует, что в бою рационально заражать один узел одного взвода каждой из трех рот мпб.

Выводы. Таким образом, в модели процесса распространения СПС в информационно-управляющей сети, образуемой ИТС АС, в отличие от моделей, позволяющих либо анализировать множество потенциально возможных состояний узлов сети во времени без учета ее структуры [146, 293, 309], либо учитывать структуру сети и отдельные состояния узлов во времени [105, 199, 259], учтены одновременно потенциально возможные состояния узлов сети во времени и ее структура. Это достигается за счет представления сети в виде графа полумарковской модели, в которой переходы – это каналы связи между ИТС сети, плотности распределения времен которых описываются

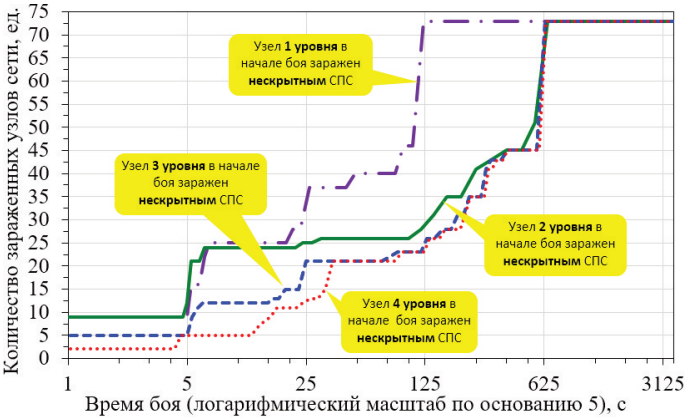


Рис. 52. Заражение сети нескрытным специальным программным средством

Рис. 53. Заражение сети скрытным специальным программным средством

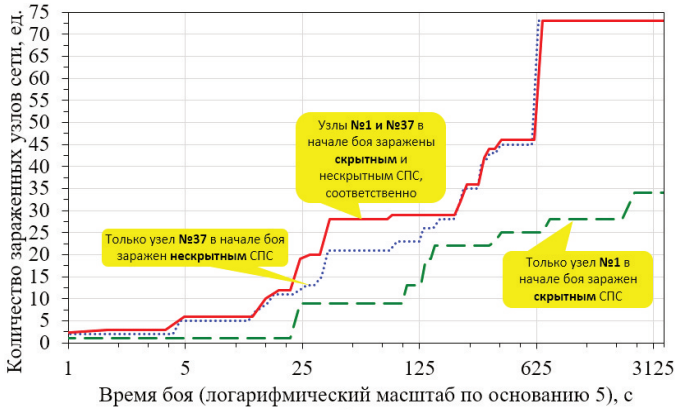


Рис. 54. Одновременное заражение сети *двумя* специальными программными средствами – скрытным и нескрытным

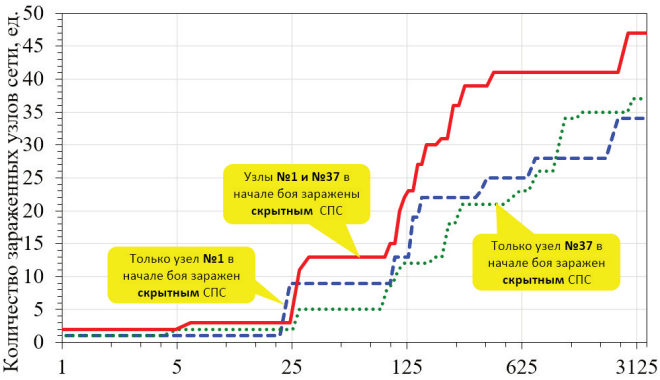


Рис. 55. Одновременное заражение сети *двумя* скрытными специальными программными средствами

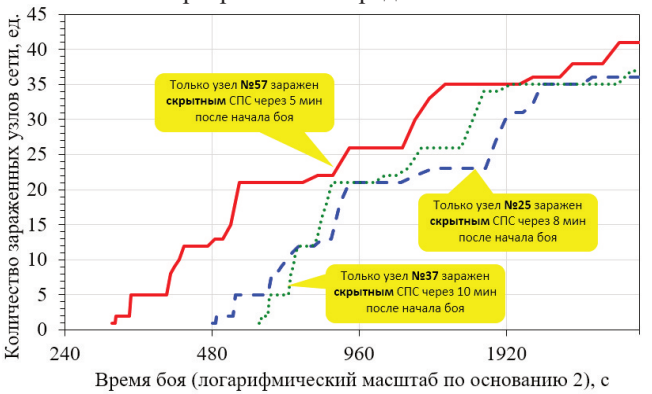


Рис. 56. Заражение сети *одним* скрытным специальным программным средством в течение боя

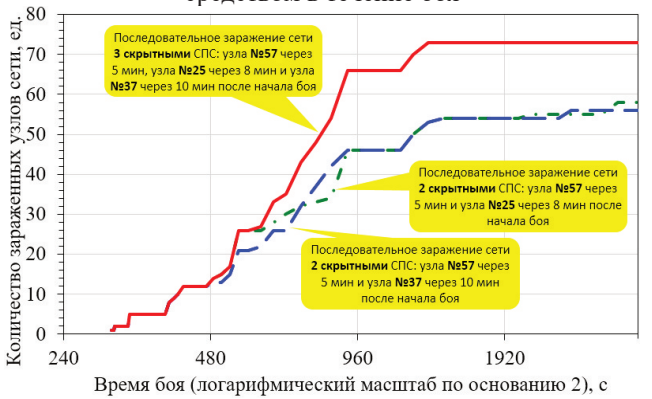


Рис. 57. Последовательное заражение сети *тремя* скрытными специальными программными средствами

обобщенным законом Эрланга ***n***-го порядка, параметры которого определяются для нескрытных СПС интенсивностью их размножения, для скрытных СПС – интенсивностью легитимного обмена информацией между узлами сети согласно протоколам установления сеанса связи, а состояния – это узловые ИТС сети, состояния которых определяются по результатам конфликта средства реализации КА и ПЗИ ИТС при условии внедрения СПС в программную среду ИТС, а также преобразования полученного полумарковского процесса в марковский модифицированным методом Кендалла.

Применение модели впервые без применения метода статистических испытаний позволяет определить вероятностно-временные характеристики состояний каждого узлового ИТС сети с учетом ее архитектуры, характеристик ПЗИ узловых ИТС, поведения СПС и возможности одновременного заражения каждого узлового ИТС сети различными типами СПС, а также обосновать следующие закономерности применения СПС в сети ВФ на примере мсб, усиленного танковой ротой, и мпб бригады «Страйкер»:

- наиболее эффективными являются нескрытные СПС, способные заразить все узлы сети в начале боя. Скрытное СПС заражает в два раза меньше узлов мсб, усиленного танковой ротой, или мпб, чем нескрытное;
- рациональным эпицентром заражения является КНП батальона. При его недоступности принадлежность узла не имеет значения;
- совместно применять нескрытное и скрытное СПС нерационально. Скрытными СПС рационально заражать узел одного взвода каждой роты.

Роль модели в настоящем исследовании состоит в учете свойств авторегенерируемости, транслируемости, транзитивности, прозрачности и телеоперационности КА, которые обусловлены возможностями СПС самомодифицироваться и распространяться по информационно-управляющим сетям противостоящего ВФ.

Выводы по третьей главе

В третьей главе рассмотрены пять взаимосвязанных моделей процессов функционирования компонентов автоматизированных систем воинских формирований:

- процесса функционирования информационно-технического средства автоматизированной системы;
- процесса функционирования технического компонента информационно-технического средства в боевых условиях;
- конфликта средства реализации кибератак и подсистемы защиты информации информационно-технического средства;
- процесса функционирования специального программного обеспечения задачи управления устройством в боевых условиях;
- процесса распространения специальных программных средств в информационно-управляющей сети, образуемой информационно-техническими средствами автоматизированных систем.

Эти модели предоставляют возможность для оценки следующих пяти информационных показателей эффективности информационно-технических средств, используемых в автоматизированных системах военного назначения:

- работоспособность;
- заразность;
- подверженность дезинформации с применением специальных программных средств;
- подверженность разведке с применением специальных программных средств;
- подверженность перехвату управления с применением специальных программных средств.

В качестве методологической базы представленных моделей используется математический аппарат полумарковских процессов. В частности, используется метод М.Д. Кендалла, усовершенствованный М.Г. Чикиным, для практического применения которого разработан алгоритм автоматизированного преобразования аналитического описания немарковских процессов с распределенным по обобщенному закону Эрланга n-го порядка временем переходов в марковский процесс, а также предложена его программная реализация.

Полученные аналитические выражения для расчета численных значений вышеуказанных показателей отображают совокупность известных из практики возможностей средств реализации кибератак по влиянию на процессы функционирования автоматизированных систем воинских формирований в боевых условиях.

В следующей главе рассматривается модель процессов функционирования автоматизированных систем в боевом эпизоде, использующая рассмотренные информационные показатели эффективности информационно-технических средств.

4 Модель процессов функционирования автоматизированных систем в боевом эпизоде

«Не было гвоздя – подкова пропала.
Не было подковы – лошадь захромала.
Лошадь захромала – командир убит.
Конница разбита – армия бежит.
Враг вступает в город, пленных не щадя, –
Оттого, что в кузнице не было гвоздя!»

Английский фольклор.
Перевод Самуила Яковлевича Маршака

4.1 Постановка задачи на моделирование

Традиционно сферами применения математических моделей в военном деле являлись строительство и боевое применение войск (сил) [62].

В сфере боевого применения войск (сил) на оперативном уровне и выше, а также в сфере военного строительства математические модели позволили достичь значительных успехов. Накопленный опыт моделирования в этих сферах удалось воплотить даже в семейство международных стандартов IEEE 1516 [296]. На основе этих стандартов сегодня успешно функционируют АС ВС США и других стран НАТО. С высоким темпом процесс создания таких систем идет и в России.

Однако в сфере боевого применения войск (сил) в тактическом звене результаты применения математических моделей и у нас, и за рубежом гораздо скромнее. Ведь современный бой весьма сложен не только по причине его высокой маневренности, скоротечности, большой дальности и точности средств ОП, применения широкой номенклатуры роботизированных образцов вооружения, но и вследствие применения в нем разнородных средств реализации ИТВ, которые оказывают воздействие на информацию в боевых циклах ВФ. Синергетическое использование совокупности этих аспектов в динамике боя является актуальной проблемой военной науки на текущем этапе ее развития. Мировой опыт системного анализа показывает, что без автоматизированной поддержки принятия решения, базирующейся на развитом математическом аппарате, здесь не обойтись. Тем не менее, в среде военных специалистов до сих пор ведутся дискуссии о том, какой из базовых методов моделирования следует взять за основу для тактического звена [128]. Мнения расходятся до диаметрально противоположных, вплоть до отвержения самой необходимости использования математических моделей или полного доминирования в таких моделях мнения эксперта. В связи с этим даже высказываются мнения о необходимости применения вместо математических моделей номограмм на «электронных планшетах» (по примерам, изложенным в классическом труде А.Я. Вайнера [66]). Но часто не принимается во внимание, что номограммы являются полномасштабно и широко апробированным результатом применения математических моделей, по сути, их квинтэссенцией, но никак не заменой.

Причина успеха математических моделей в одной сфере применения и одновременно низкого уровня доверия к ним в другой сфере объясняется сущностью базовых методов моделирования боевых действий.

До последнего времени основным в данной научной области являлся **эмпирический метод**. Он состоит в обобщении боевого опыта, его сопоставлении с основными тенденциями развития потенциального противника и в выработке рекомендаций по использованию этого опыта. При этом процесс боевых действий разбивается на совокупность частных процессов (боевых задач), которые, в свою очередь, делятся на подпроцессы и т.д. Каждый процесс рассматривается на своем уровне иерархии как самостоятельный и представляет собой дуэльную схему антагонистического конфликта своих сил и средств с противником. Этот метод прост и логичен (на первый взгляд!). Однако ему присущи следующие недостатки:

- конкретные условия и ход минувшей войны уже никогда не повторятся. Как говорил Гераклит Эфесский, «нельзя войти в одну и ту же реку дважды». Именно поэтому на страницах военно-теоретических журналов эмпирический метод нередко подвергается критике, состоящей в том, что «военным свойственно готовиться к войне прошлого»;
- тенденции развития вероятного противника, часто провозглашаемые самим же вероятным противником, почти всегда носят идеализированный, рекламный характер;
- в одном дуэльном конфликте крайне сложно учесть влияние других одновременно происходящих конфликтов. В частности, конфликты, ориентированные на материальный аспект боевой обстановки, крайне редко учитывают конфликты, ориентированные на ее информационный аспект. Например, боевые задачи мотострелковым подразделениям или частям обычно не учитывают возможности своих сил и средств РЭБ, и тем более возможности сил и средств РЭБ противника;
- множество самостоятельных дуэльных конфликтов на каждом уровне иерархии формируется эмпирически, что провоцирует возможность упустить на тактическом и даже на оперативном уровне какой-либо важный процесс боевых действий, обусловленный применением новых образцов вооружения;
- не учитывает синергетический эффект от комбинации разных процессов.

Понимая вышеизложенную ситуацию, военные специалисты стали искать пути ее разрешения. Как результат, с конца XX века ключевой тенденцией в этом направлении является попытка применить для прогнозирования боевых действий **теоретико-игровые методы и метод имитационного моделирования** с использованием последних достижений компьютерных технологий. Однако область применения этих методов имеет следующие ограничения.

Во-первых, в основе имитационного моделирования боевых действий всегда лежит некоторый сценарий, задаваемый экспертами. Ключевым признаком причисления математических моделей к имитационным является применение метода статистических испытаний (метода Монте-Карло) [129]. Он предусматривает выполнение следующих этапов: описание модели

исследуемой системы в виде последовательности элементарных или агрегированных операций в соответствии с логикой структурных взаимосвязей, повторение статистически значимого количества «прогонов» имитационных экспериментов и анализ результатов совокупности этих «прогонов». Достоинством имитационных моделей является возможность адекватного отражения различных свойств элементов системы, а их недостатком – необходимость проведения многократных статистических экспериментов. Этот метод моделирования ориентирован на процессы с относительно небольшим количеством потенциально возможных сценариев развития (например, подбрасывание монеты, прохождение корабля через минные заграждения). Здесь следует понимать, что сценариев развития вооруженного конфликта ВФ даже уровня мотострелковой роты очень много (условно – «миллион»).

Во-вторых, оценка точности результатов имитационного моделирования имеет смысл только применительно к одному выбранному сценарию боя из «миллиона». Но в практике имитационного моделирования боевых действий нередки случаи, когда из «миллиона» возможных сценариев берется лишь один. Этот сценарий повторяют «миллион» раз и делают на основе статистических данных по результатам этих «прогонов» выводы о вероятностях хода и исхода боя в целом, забывая, что эти выводы справедливы только для одного сценария из «миллиона».

В-третьих, если бы имитационное моделирование сложных конфликтных процессов было эффективным, то были бы известны имитационные модели, позволяющие, например, достоверно оценить исход любого футбольного матча. Однако даже для таких относительно простых условий с полностью известными правилами получить достоверные результаты посредством имитационного моделирования принципиально невозможно.

В-четвертых, сценарий боевых действий в имитационном моделировании и «стратегия» поведения противника в теории игр всегда известны. Однако в том-то и состоит суть реальной войны, что в ней «все средства хороши». Знание того, как поведет себя противник, уже является одним из ключевых преимуществ. Ведь, как отмечал известный китайский полководец Сунь-Цзы, «война – это путь обмана». Реальные замыслы тщательно скрываются каждой стороной конфликта, в том числе путем дезинформации.

Во многом эти ограничения обусловлены весьма важной фундаментальной особенностью имитационных моделей. Дело в том, что в них используется один или комбинация двух следующих способов учета модельного времени [239, 244, 269]:

- **способ постоянных приращений** (или способ «Δt», принцип «Δt»), состоящий в разбиении времени боя на заданные равные приращения времени, величина которых во избежание пропуска значимых событий выбирается с учетом минимальной продолжительности цикла работы моделируемых объектов;
- **способ существенных состояний** (способ «Δz», способ «по событиям», принцип «δz»), при котором приращение времени проводится в момент наступления очередного события в модели.

Ни один из этих способов (в том числе их комбинация) не позволяет решать в ходе одной реализации сценария боя оптимизационные задачи (в первую очередь, целераспределение) в рамках ВФ в целом или в рамках его относительно самостоятельных крупных составных частей. Эта особенность обусловлена неопределенностью в том, какие именно события в процессе боя брать за точки отсчета временных интервалов боевых циклов, в интересах которых проводится оптимизация.

В таких обстоятельствах очевидна потребность в поиске подхода к прогнозированию боевых действий, лишенного указанных недостатков. Этот подход может базироваться только на аналитическом моделировании. Кстати, именно с аналитической модели боя, предложенной еще в 1915 году в работе М.П. Осипова, начался расцвет теоретических основ моделирования боевых действий, впоследствии подхваченный английским инженером Ф.У. Ланчестером и другими военными теоретиками по всему миру [185]. Как известно, все развивается по спирали. Но обновленный аналитический метод на очередном витке «спирали времени» должен обеспечивать такую степень детализации аналитических моделей боевых действий, которая позволяет адекватно учесть в боевой обстановке наиболее полное множество функций образцов вооружения, воздействующих одновременно и на «материю», и на «информацию». Рассмотрим потенциальные возможности такого подхода.

Аналитические модели описывают определенный процесс в моделируемой системе посредством математических конструкций (функций или функционалов, алгебраических или дифференциальных уравнений и т.д.). Они позволяют либо получить конечные результаты исследования в виде формализованных соотношений, либо использовать для получения результатов исследования численные методы. Возможность получения результатов с высокой скоростью является неоспоримым достоинством аналитических моделей. Но, как известно, «даже самый мощный аппарат современной математики позволяет адекватно описать поведение только относительно простых систем» [239]. Как следствие, недостаток аналитического моделирования состоит в существенной идеализации сложной системы и ее элементов. По этой причине в известных аналитических моделях боевых действий отсутствует детальный учет траекторий одновременного перемещения множества разнородных ЭБП. Это значительно «загрубляет» результаты исследования и делает их малопригодными для практики.

Рациональным путем использования аналитических и имитационных моделей является интеграция их лучших свойств. Для этого за основу следует взять аналитическое моделирование, обеспечивающее высокую скорость расчетов, а от имитационного моделирования следует взять гибкость модельного времени и возможность учета траекторий движения ЭБП. Требуемые модели по классификации в [180] должны относиться к операционным структурно-функциональным моделям. Известные модели функционирования АС в боевых условиях можно разделить на два класса:

- **класс А** – модели, ориентированные на учет материального аспекта боевой обстановки (в первую очередь, на возможности

противоборствующих сторон по ОП). Это направление существенно развили М.П. Осипов [203] и Ф.У. Ланчерстер [306]. В дальнейшем оно было развито в работах [1, 5, 6, 47, 53, 54, 125, 178, 181, 185, 198, 217, 245, 253, 256, 261, 262, 264, 265, 268, 299, 300, 304, 320, 328] и др.;

- **класс В** – модели, ориентированные на учет информационного аспекта боевой обстановки (в первую очередь, на функции разведки, управления, связи, РЭП и имитации), предложенные, например, в работах [2, 50-52, 67, 68, 71-73, 111, 112, 117, 127, 139-143, 147, 161, 162, 165, 178, 216, 224, 250, 267, 271, 278] и др. Эти модели часто называются моделями информационного конфликта.

При анализе этой классификации становится очевидной потребность в формировании моделей нового класса (**класс С**) – моделей, ориентированных на системный учет в боевой обстановке «материи» и «информации». Но подходы к разработке таких полнофункциональных моделей сегодня отсутствуют. С одной стороны, сложившаяся ситуация обусловлена тем, что научные школы, разрабатывающие модели **классов А** и **В,** традиционно развивались обособленно. Превосходство моделей **класса А** всегда считалось неоспоримым, так как исторически они начали развиваться раньше, а результаты их применения с некоторой погрешностью всегда можно было проверить на практике [262]. Ведь если эффектом от применения, например, гаубицы является разрушенное здание или уничтоженная техника, то эффект от применения станции радиопомех не всегда очевиден. Ситуация изменилась только в последние годы, когда во всем мире ВФ стали оснащаться ИТС до солдата включительно. В таких условиях эффект от сил и средств, ориентированных на информационный аспект боевой обстановки (в первую очередь, сил и средств РЭБ), приобрел существенно большую наглядность. С другой стороны, препятствие к системному учету в моделях боя «материи» и «информации» заложено в недостаточно глубокой исследованности сущности факторов, влияющих на успех в бою. Рассмотрим их детально.

Существуют три классических фактора успеха в бою [253]: соотношение сил, пространство и время (см. рис. 58).

Требуемый подход к аналитическому моделированию боя заведомо не может адекватно учесть потенциально возможные перемещения разнородных сил и средств во времени. Современный уровень развития математической отрасли наук этого не позволяет. В моделях боя учет этих факторов представляет наибольший интерес при одновременном изменении каждого из них и при изменении двух с постоянным третьим. Однако одновременное изменение пространства и времени, проявляемое в маневрах и ударах, на практике обычно описывается алгебраическими и геометрическими выражениями (см., например, [253, 268]), в основе которых лежат нормативы, базирующиеся на боевом опыте и объективных возможностях сил и средств по перемещению в различных условиях боевой обстановки.

Такое положение дел обусловлено тем, что результаты математического моделирования одновременного изменения пространства и времени, полученные, как правило, на имитационных моделях (см., например, [47, 217]),

имеют низкую адекватность, поскольку предугадать поведение противника в реальном бою ВФ уровня роты и выше с разнородным вооружением крайне сложно. Поэтому, учитывая, что зависимость соотношения сил от местоположения ЭБП противоборствующих ВФ без учета времени не представляет значительного интереса для практики, в моделях боя целесообразно анализировать изменение соотношения сил (то есть боевых потенциалов, от лат. *potentia* – сила) во времени при фиксированных позициях ЭБП (разноприоритетные альтернативные варианты позиций задает эксперт).

Рис. 58. Классические факторы успеха в бою

То есть для оценки возможностей сил и средств по перемещению в пространстве все же применим только эмпирический метод прогнозирования боевых действий. Зато аналитическая модель дает возможность командиру понять, как во времени будет изменяться соотношение БП противоборствующих ВФ при фиксированных позициях их ЭБП. Но как именно командир будет распоряжаться своими силами и средствами? – это зависит только от его интеллекта, уровня подготовки, творческого потенциала и воли.

При моделировании боя во внимание традиционно принимались четыре субфактора, влияющих на соотношение БП:

- *энергетический*, характеризующий совокупность средств вооруженной борьбы и защиты от них, включая средства боевого обеспечения;
- *ресурсный*, характеризующий тыловое обеспечение;
- *психологический*, характеризующий индивидуальную и коллективную психическую деятельность личного состава;
- *телекоммуникационный*, характеризующий совокупность проводных и беспроводных (в том числе акустических) каналов связи и разведки, образуемых устройствами, ИТС и людьми.

Следует отметить, что появление во второй половине XX века моделей **класса В** связано с осознанием существования телекоммуникационного субфактора (см. рис. 59). Однако попытки полноценной интеграции моделей **клас-**

сов А и **В** к успеху не привели. Этому, например, в области РЭБ способствует использование таких показателей, как «относительный объем эффективно выполняемых задач» [147]. Подобного рода показатели моделей **класса В**, очевидно, приводят к недостаточно полному пониманию разработчиками моделей **класса А** того, какой именно вклад в соотношение БП дает ресурс средств и личного состава, обеспечивающий выполнение некоторого объема задач.

Рис. 59. Субфакторы фактора соотношения сил

Проблема концентрации внимания информационного аспекта боевой обстановки только на телекоммуникационном факторе состоит в том, что само по себе отсутствие/наличие каналов связи и разведки еще не обеспечивает полноту картины боя. Для этого нужно уметь анализировать еще и то, что по этим каналам передается, то есть информацию в ее когнитивном (от лат. *cognitio* – узнавать) контексте, опирающемся на смысл (семантику) и ценность (прагматику). Но телекоммуникационный субфактор рассматривает информацию, как максимум, в синтаксическом контексте.

Данные обстоятельства свидетельствуют о необходимости выделения нового субфактора, влияющего на соотношение БП, – *когнитивного*.

Когнитивный субфактор характеризует информацию в *боевых циклах*, каждый из которых согласно классическим канонам военной науки, как уже отмечено ранее в п. 1.1.1, состоит из пяти этапов [175]: сбор информации, ее анализ и осознание, планирование, принятие решения и его исполнение. Очевидно, что боевой цикл эффективен, если информационные потоки, создаваемые, обрабатываемые или передаваемые на каждом его этапе, останутся неизвестными противнику, не будут искажены и будут успешно получены/переданы и обработаны. Пользуясь терминологией теории защиты информации (см. ГОСТ [86]), в боевых циклах информационные потоки должны сохранить:

- *конфиденциальность* – состояние информации, когда она принадлежит только тем субъектам, которые имеют на ее использование соответствующие полномочия. Нарушение конфиденциальности

информации является не чем иным, как разведкой. До тех пор, пока информация не разведана, она конфиденциальна;

- *целостность* – состояние информации, при котором обеспечивается неизменность ее формы представления и содержания в условиях деструктивного воздействия. Фактически нарушение целостности информации есть ее подмена, в том числе дезинформация;
- *доступность* – состояние информации, при котором к ней обеспечивается беспрепятственный доступ субъектов, имеющих на это полномочия. Нарушить доступность можно путем уничтожения, полного или частичного блокирования в течение заданного периода времени носителя, источника или потребителя информации.

Эти свойства информации боевых циклов являются тремя «китами» информационной безопасности, которых каждая из противоборствующих сторон стремится разрушить у противника и сохранить у себя. Иные свойства информации (актуальность, полнота и пр.), а также свойства процессов управления (устойчивость, непрерывность, оперативность, скрытность) в бою являются производными от этих свойств [31, 43]. В общем случае для нарушения конфиденциальности информации используются средства разведки, для нарушения доступности – средства ОП, РЭП, воздействия мощным ЭМИ и КА, а для нарушения целостности – средства имитации боевой (в том числе радиоэлектронной) обстановки и КА. С учетом этого структурная схема информационного конфликта ВФ в современных боевых условиях имеет вид, представленный на рис. 60 [43].

Таким образом, актуальной является задача разработки модели, позволяющей воспроизвести обеспечиваемые АС процессы разведки, управления, связи, ОП, имитации обстановки, РЭП, воздействия мощным ЭМИ и КА при их одновременном применении в рамках боевых циклов ВФ с учетом когнитивного субфактора.

Внимательный читатель конечно же обратил внимание на то, что в приведенном обзоре не рассмотрена активно развивающаяся сегодня область «искусственного интеллекта». Это сделано умышленно. Дело в том, что методология данной области, как известно, базируется на трех «китах»: 1) методах формирования и актуализации банка данных об «окружающем мире»; 2) методах формализации данных об «окружающем мире»; 3) методах производства знаний об «окружающем мире». Применительно к военному делу наиболее развиты на сегодняшний день методы первой группы, поскольку они являются универсальными и потому могут быть заимствованы из гражданского коммерческого сектора. Методы третьей группы сегодня в принципе находятся в «зачаточном» состоянии. Именно по этой причине сам термин «искусственный интеллект» пока еще вызывает значительный скепсис у многих ученых во всем мире. Перспективы методов третьей группы являются весьма неопределенными. Без новых научных открытий здесь, по всей видимости, не обойтись. А вот к методам второй группы в военном деле сегодня относятся все указанные выше недостатки существующих моделей боевых действий. Поэтому разработка требуемой модели будет являться вкладом в том числе в развитие методологии военного «искусственного интеллекта».

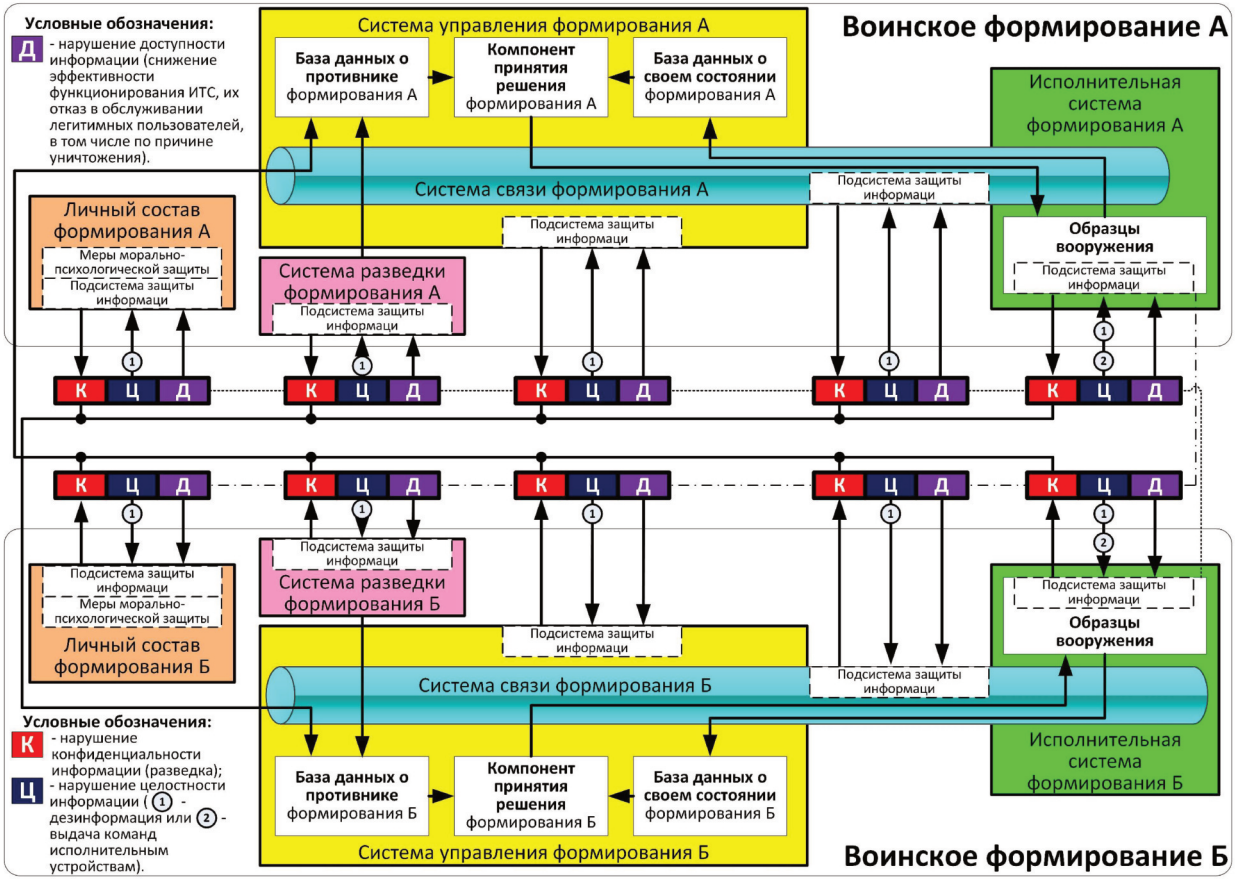


Рис. 60. Структурная схема информационного конфликта воинских формирований в современных боевых условиях

4.2 Формализация модели

4.2.1 Концепция моделирования

Для системного учета в модели боя указанных выше субфакторов применим подход, предложенный Д.А. Новиковым [198]. В этом подходе вооруженный конфликт представляется в виде совокупности взаимосвязанных моделей, упорядоченных по пяти уровням иерархии:

1) взаимодействие отдельных боевых единиц;
2) «локальное» взаимодействие подразделений;
3) динамика численности;
4) распределение сил и средств во времени;
5) распределение сил и средств в пространстве.

Однако особенностью этого подхода, затрудняющей его использование на практике, по указанным выше причинам является ориентация на имитационное моделирование и теорию игр на первом, четвертом и пятом уровнях.

С учетом этого предлагается следующий подход к аналитическому моделированию боя, опубликованный в [30, 32]. Сначала разрабатывается древовидный граф боя. Согласно подходу, предложенному С.Н. Меркуловым [178], бой представляют древовидным графом, в котором боевые эпизоды между смежными узловыми точками характеризуются относительно постоянными напряжением сил и интенсивностью работы средств (см. рис. 61). Далее по тексту этот граф называется «деревом» боя или графом позиционной динамики ЭБП ВФ. Узловые точки «дерева» боя, кроме начальной, характеризуют моменты времени, в которых ход боя может измениться в нескольких «направлениях», например, соответствующих вариантам маневров (перегруппировки) сил и средств или завершиться по достижении заданного условия.

В начале каждого боевого эпизода ЭБП противоборствующих сторон статично размещают на электронной карте местности. ЭБП детализируют до людей и образцов вооружения, которые включают отдельные ИТС (в том числе нештатные) и устройства (например, автомобиль, орудие). В ЭБП и между ними определяют каналы связи, организуемые с использованием ИТС и людей (в том числе вербально, знаками).

На электронной карте определяются возможности устройств и ИТС на основе их тактико-технических характеристик (ТТХ). ЭБП с функциями управления осуществляют эти функции по каналам связи и могут применять ИТС, в том числе нештатные. Средства имитации обстановки также наносятся на электронную карту и имитируют функционирование реальных образцов вооружения на различных фонах наблюдения. ИТС и устройства представляются указанным в параграфе 3.3 образом. Дополнительно на карту района наносят силы и средства вышестоящих уровней (в том числе спутники) согласно двум правилам (см. рис. 62):

1) если они оказывают влияние на ЭБП в этом районе;
2) если они оказывают влияние на ЭБП, нанесенные на карту согласно правилу № 1.

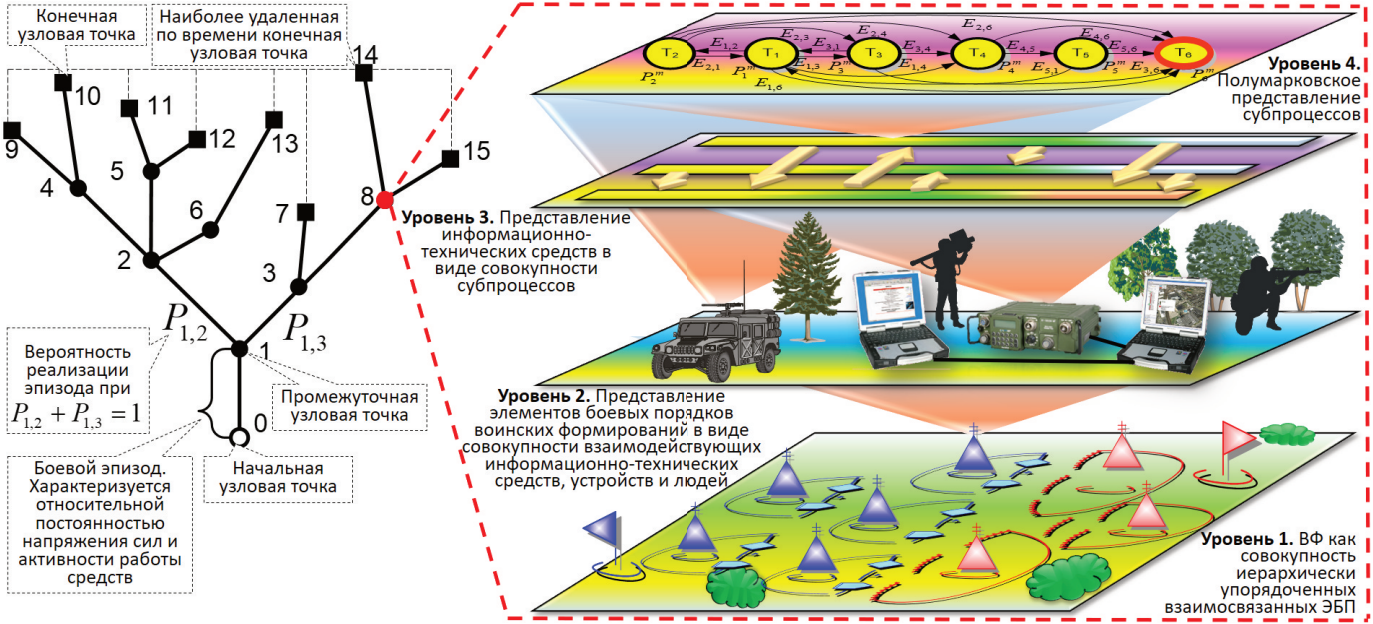


Рис. 61. Древовидный граф боя (вариант)

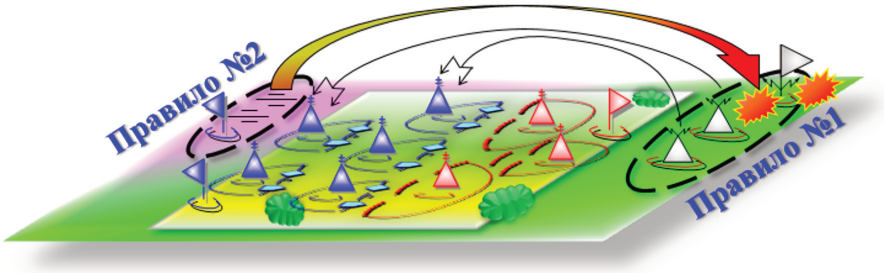


Рис. 62. Правила нанесения сил и средств вышестоящих уровней

Рассмотрим далее аналитические выражения, используемые для оценки наивысшего по иерархии показателя боевой эффективности ВФ.

4.2.2 Остаточная доля численности воинского формирования

Ключевым показателем в рассматриваемой модели процессов функционирования АС в боевом эпизоде является *остаточная доля численности* каждого из противоборствующих ВФ. Этот показатель характеризует для каждого ВФ совокупный удельный вес его ЭБП с учетом того, что в бою эти элементы могут быть разведаны и уничтожены, захвачены в результате диверсии или КА, выведены из строя мощным ЭМИ, их личный состав подвергается радиационному, химическому, биологическому (РХБВ), психологическому (ПсВ) и нелетальному (НелВ) воздействию. При этом ЭБП противника могут подвергаться аналогичному воздействию.

Значение этого показателя в момент времени t вычисляется по формуле

$$N^{\text{А}}(t)=\sum_{n=1}^{|C^{\text{А}}|}\left(\psi_n^{\text{А}}(t)\chi_n^{\text{А}}(t)W_n^{\text{А}}P_{\text{нф}_n}^{\text{А}}\right)+\sum_{m=1}^{|C^{\text{Б}}|}\left(\psi_m^{\text{Б}}(t)\left(1-\chi_m^{\text{Б}}(t)\right)W_m^{\text{Б}}\left(1-P_{\text{нф}_m}^{\text{Б}}\right)\right),$$
$$\sum_{n=1}^{|C^{\text{А}}|}W_n^{\text{А}}+\sum_{m=1}^{|C^{\text{Б}}|}W_m^{\text{Б}}=1, \qquad (32)$$

где $C^{\text{А(Б)}}$ – множество ЭБП ВФ А(Б) (выражение А(Б) означает ВФ А или Б);

$\chi_{n(m)}^{\text{А(Б)}}(t)\in[0,1]$ – устойчивость к диверсии ЭБП ВФ А(Б);

$\psi_{n(m)}^{\text{А(Б)}}(t)\in[0,1]$ – работоспособность ЭБП ВФ А(Б);

$P_{\text{нф}_{n(m)}}^{\text{А(Б)}}\in[0,1]$ – вероятность выполнения личным составом ЭБП ВФ А(Б) неавтоматизированных функций;

$W_{n(m)}^{\text{А(Б)}}$ – КБС ЭБП ВФ А(Б) (методику оценки см. далее в параграфе 5.4).

При этом *боеспособность* $n(m)$-го ЭБП в момент времени t равна

$$БС_{n(m)}(t)=\psi_{n(m)}(t)\,\chi_{n(m)}(t)\,P_{\text{нф}_{n(m)}}. \qquad (33)$$

Значение показателя $\psi_{n(m)}(t)$ в формулах (32) и (33) вычисляется с использованием следующей формулы:

$$\psi_{n(m)}(t)=\sum_{s=1}^{N_{n(m)}}E_{n(m),s}(t)\varphi_{n(m),s},\ \sum_{s=1}^{N_{n(m)}}\varphi_{n(m),s}=1, \qquad (34)$$

где $N_{n(m)}$ – количество образцов ИТС и устройств в $n(m)$-м ЭБП;

$\varphi_{n(m),s}$ – КБС s-го образца ИТС/устройства в $n(m)$-м ЭБП;

$E_{n(m),s}(t)$ – работоспособность s-го образца ИТС/устройства в $n(m)$-м ЭБП в момент времени t (вычисляется по формуле (21), приведенной в параграфе 3.6).

Значение показателя $\chi_{n(m)}^{\text{А(Б)}}(t)$ в формулах (32) и (33) вычисляется по следующей формуле:

$$\chi_{n(m)}(t)=\left(1-\alpha_{n(m)}\right)\left(1-\Delta_{n(m)}\left(1-\sum_{s=1}^{N_{\text{упр}_{n(m)}}}\left(\left(1-A_{n(m),s}(t)\right)\beta_{n(m),s}\right)\right)\right), \tag{35}$$

где $A_{n(m),s}(t)$ – подверженность перехвату управления с применением СПС s-м ИТС, обеспечивающим решение задач управления оружием $n(m)$-го ЭБП, в момент времени t (вычисляется по формуле (25), приведенной в параграфе 3.6);

$\beta_{n(m),s}$ – доля задач управления оружием, решаемых s-м ИТС $n(m)$-го ЭБП;

$N_{\text{упр}_{n(m)}}$ – количество ИТС в $n(m)$-м ЭБП, обеспечивающих решение ЗУ;

$\alpha_{n(m)}$ – вероятность использования $n(m)$-го ЭБП диверсионно-разведывательными подразделениями противника;

$\Delta_{n(m)}\in[0,1]$ – уровень информатизации $n(m)$-го ЭБП (методика оценки рассматривается далее в параграфе 5.3).

Значение показателя вероятности выполнения личным составом ЭБП неавтоматизированных функций $P_{\text{нф}_{n(m)}}^{\text{А(Б)}}$ в (32) и (33) вычисляется по формуле

$$P_{\text{нф}_{n(m)}}=1-\Delta_{n(m)}\prod_{j=1}^{3}\left(1-\Omega_j\right)\left(1-\xi_{\text{бп}}K_{\text{бп}_{n(m)}}-\xi_{\text{боп}}K_{\text{боп}_{n(m)}}\right) \text{ при}$$

$$\Omega_1=\begin{cases}P_{\text{ПсВ}_{n(m)}}(d), \text{ если } n(m)\text{-й ЭБП } \left(\text{в зоне действия боеприпаса ПсВ}\right)\vee\\ \vee\left(\begin{array}{c}\text{является целью хотя бы одного не уничтоженного до момента}\\ \text{воздействия ЭБП противника со средством/боеприпасом ПсВ}\end{array}\right);\\ 0 \text{ в противном случае;}\end{cases}$$

$$\Omega_2=\begin{cases}P_{\text{НелВ}_{n(m)}}(d), \text{ если } \left(\begin{array}{c}n(m)\text{-й ЭБП является целью хотя бы одного ЭБП}\\ \text{противника со средством/боеприпасом НелВ,}\\ \text{не уничтоженного до момента воздействия}\end{array}\right)\\ 0 \text{ в противном случае;}\end{cases} \tag{36}$$

$$\Omega_3=\begin{cases}P_{\text{РХБВ}_{n(m)}}(d)\mathcal{B}, \text{ если } n(m)\text{-й ЭБП } \left(\text{в зоне действия боеприпаса РХБВ}\right)\vee\\ \vee\left(\begin{array}{c}\text{является целью хотя бы одного не уничтоженного до}\\ \text{момента воздействия ЭБП противника с боеприпасом РХБВ}\end{array}\right);\\ 0 \text{ в противном случае;}\end{cases}$$

$$\mathcal{B}=\begin{cases}1-N_{\text{л}_{n(m)}}^{-1}\sum_{i=1}^{N_{\text{л}_{n(m)}}}P_{\text{РХБЗ}_{n(m),i}}, \text{ если в } n(m)\text{-м ЭБП отсутствует средство}\\ \qquad\text{радиационной, химической и биологической защиты}\\ \qquad\text{коллективного пользования;}\\ 1-P_{\text{РХБЗкол}_{n(m)}} \text{ в противном случае,}\end{cases}$$

где $P_{\text{РХБВ}_{n(m)}}(d)$, $P_{\text{НелВ}_{n(m)}}(d)$, $P_{\text{ПсВ}_{n(m)}}(d)$ – вероятность вывода из строя личного состава в $n(m)$-м ЭБП на расстоянии d ЭБП противника со средством/боеприпасом РХБВ, НелВ и ПсВ, соответственно;

$N_{\text{Л}_{n(m)}}$ – количество людей в $n(m)$-м ЭБП;

$P_{\text{РХБЗкол}_{n(m)}}$ – максимальная вероятность защиты от РХБВ средства радиационной, химической и биологической защиты (РХБЗ) коллективного пользования в $n(m)$-м ЭБП;

$P_{\text{РХБЗ}_{n(m),i}}$ – вероятность защиты от РХБВ индивидуального средства РХБЗ i-го человека в $n(m)$-м ЭБП (при отсутствии средства РХБЗ у i-го человека $P_{\text{РХБЗ}_{n(m),i}} = 0$);

$K_{\text{бп}_{n(m)}} \in (0,1]$, $K_{\text{боп}_{n(m)}} \in [0,1]$ – коэффициенты боевой подготовки и боевого опыта личного состава в $n(m)$-м ЭБП, соответственно;

$\xi_{\text{бп}}$, $\xi_{\text{боп}}$ – весовые коэффициенты боевой подготовки и боевого опыта, соответственно ($\xi_{\text{бп}}+\xi_{\text{боп}}=1$). Например, в [79] они задаются так: $\xi_{\text{бп}}=⅔$ и $\xi_{\text{боп}}=⅓$).

4.2.3 Взаимное влияние элементов боевых порядков

В рассматриваемой модели взаимное влияние ЭБП ВФ учитывается на уровне времен переходов полумарковских процессов функционирования устройств и ИТС (эти процессы описаны в параграфе 3.3), исходя из местоположения, особенностей целераспределения и ТТХ этих образцов в условиях противодействия противника, а также возможностей по его опережению в скорости боевых циклов и при совершении маневров в начале каждого боевого эпизода. Живучесть ЭБП определяется живучестью входящих в их состав устройств и/или ИТС. При этом учитывается, что инженерное оборудование ЭБП дополнительно защищает от ОП и снижает заметность. Экипаж (орган управления, расчет) ЭБП в результате ОП теряет боеспособность аналогично устройствам и ИТС.

Модель рассматривает конфликт ВФ, в котором действие одного ВФ сопровождается противодействием другого. Она учитывает взаимное влияние ЭБП противоборствующих ВФ со следующими основными функциями:

- управления (пример: КНП, далее – *элемент У*);
- разведки (пример: средство технической разведки, далее – *элемент Р*);
- ОП (пример: танк, гранатомет, гаубица, далее – *элемент ОП*);
- РЭП (пример: средство РЭП радиосвязи, далее – *элемент РЭП*);
- воздействия мощным ЭМИ (пример: радиочастотное оружие, далее – *элемент ЭМИ*);
- КА (пример: блокиратор сотовой связи, далее – *элемент КА*);
- связи (пример: подвижный узел связи, далее – *элемент С*);
- воздействия на личный состав (пример: станция звуковещания, далее – *элемент ЛС*);

- аэрозольного противодействия (примеры: мобильные и стационарные постановки аэрозольных заграждений).

Один ЭБП может выполнять несколько указанных функций. В отдельных случаях ЭБП, осуществляющие какой-либо вид воздействия, далее по тексту будут обозначаться *элементами В*.

Модель включает совокупность частных взаимосвязанных аналитических моделей процессов функционирования различных ЭБП. В качестве примера рассмотрим частную модель совместного применения ЭБП с функциями разведки и ОП. Демонстрация этой частной модели позволяет увидеть наиболее общий процесс конфликта ЭБП в бою, поскольку передача информации от *элемента Р элементу ОП* возможна напрямую, через промежуточные ЭБП, а также непосредственно в ЭБП, если он комбинирует функции разведки и ОП. Частные модели *элементов РЭП*, *ЭМИ* и *КА* могут быть получены из этой частной модели, поскольку такие ЭБП имеют функцию разведки и в процессе боевого применения в наиболее общем случае могут обойтись без внешнего целеуказания.

В процессе применения *элемент Р* ВФ А(Б) осуществляет разведку в заданном районе и передает разведданные о целевом ЭБП ВФ Б(А) одному или нескольким *элементам ОП* своего ВФ. Эти *элементы ОП*, в свою очередь, осуществляют ОП целевого ЭБП ВФ Б(А). Процесс применения рассматриваемых элементов (элемента) ВФ А(Б) осуществляется в условиях деструктивных воздействий различной природы со стороны ЭБП ВФ Б(А), показанных на рис. 63.

Например, *элементы КА* осуществляют воздействие на ПО внутреннего управления ЭБП, каналы навигации, каналы связи, а также на ИТС промежуточных ЭБП, *элементы РЭП* воздействуют на каналы разведки ЭБП с функцией разведки (осуществляют постановку классических радиопомех и имитацию радиоэлектронной обстановки), каналы навигации ЭБП, а также на их каналы связи и ИТС промежуточных элементов, *элементы ОП* воздействуют на устройства и ТК ИТС рассматриваемых и промежуточных ЭБП, *элементы Р* осуществляют разведку местоположения и каналов связи рассматриваемых и промежуточных ЭБП, *элементы ЭМИ* осуществляют комплексное воздействие на электронную компонентную базу рассматриваемых и промежуточных ЭБП.

Каждый ЭБП ВФ Б(А), противодействующий рассматриваемым ЭБП ВФ А(Б), характеризуется собственными временами перемещения на требуемые позиции, развертывания, подготовки к работе и реализации своих воздействий. Рассматриваемая частная модель обеспечивает вычисление показателя «время до ОП» *i*-го ЭБП ВФ Б(А) $T_i^{Б(А)}$. Этот показатель используется в качестве исходных данных в модели процесса функционирования ТК ИТС в боевых условиях, рассмотренной в параграфе 3.3. Он зависит от конкретных условий боевой обстановки, в которых находится ЭБП. Продолжительность этого времени при допущении, что при ОП любого ЭБП все ИТС и устройства этого ЭБП поражаются одинаково, и при вскрытии средствами разведки хотя бы одного ИТС ЭБП вскрывается весь ЭБП, предлагается вычислять с использованием следующей формулы:

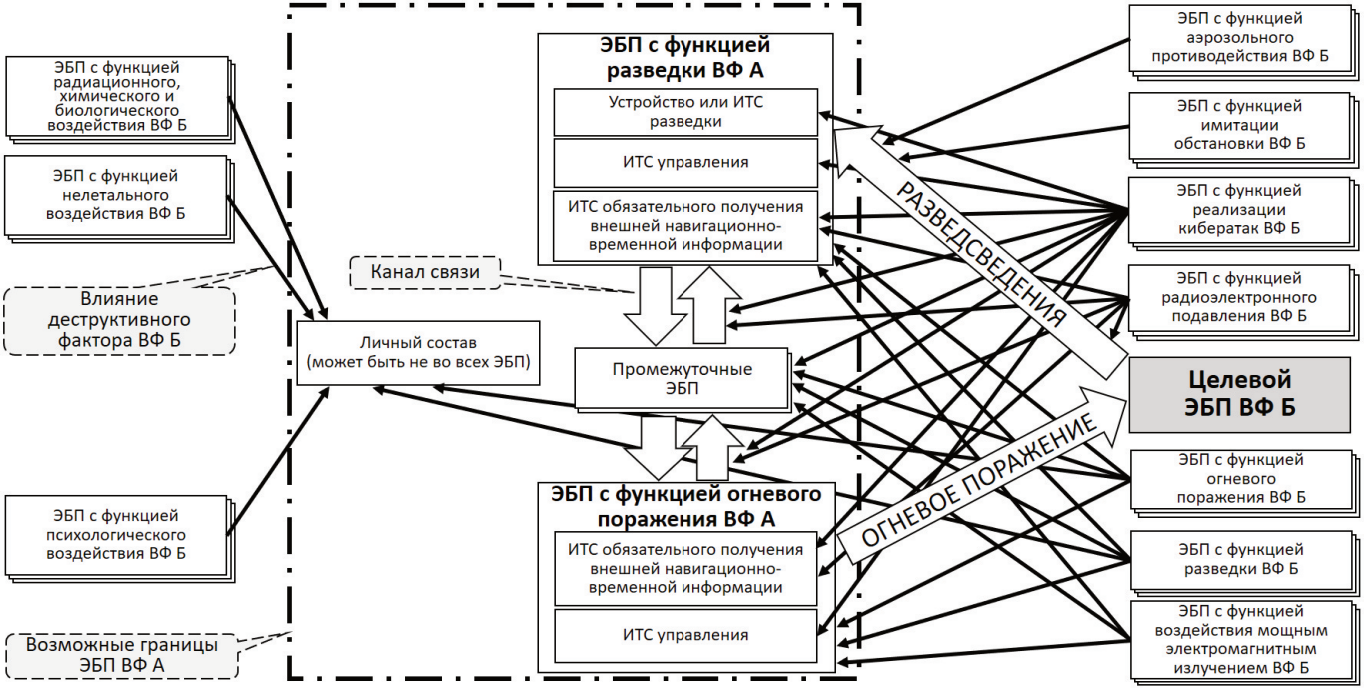


Рис. 63. Взаимное влияние элементов боевых порядков (в части боевого цикла, образуемого элементами боевого порядка с функциями разведки и огневого поражения)

$$T_i^{\text{Б}} = \begin{cases} \min\limits_{\forall f \in 1...N_{\text{ОП}}^{\text{А}}} \left(\max\limits_{\forall f \in 1...N_{\text{ОП}}^{\text{А}},\ \forall n \in 1...N_{\text{Р}}^{\text{А}}} \begin{pmatrix} T_{\text{ОПпер}_f}^{\text{А}} + T_{\text{ОППод}_f}^{\text{А}}, \\ \phi^{\text{А}}(f,n), \\ T_{\text{Рпер}_n}^{\text{А}} + T_{\text{Рпод}_n}^{\text{А}} + T_{\text{Ррез}_n}^{\text{А}} \end{pmatrix} + T_{\text{ОПупр}_f}^{\text{А}} \eta_f^{\text{А}} \right), \\ \quad \text{если } \exists h \in 1...H: \ \left(u_{\text{замет}_i}^{\text{Б}}(h) - u_{\text{маск}_i}^{\text{Б}}(h) \geq U_{\text{Рдал}_n}^{\text{А}}(d,h) \right) \wedge \left(K_i^{\text{Б}} \in \Theta_f^{\text{А}} \right) \\ \quad \text{при } \eta_f^{\text{А}} = \begin{cases} \infty, \text{ если } u_{\text{доп}_i}^{\text{Б}} + u_{\text{баз}_i}^{\text{Б}} \geq U_{\text{ОПдал}_f}^{\text{А}}(d); \\ 1 \text{ в противном случае;} \end{cases} \\ \infty \text{ в противном случае,} \end{cases} \quad (37)$$

где $N_{\text{ОП}}^{\text{А}}$, $N_{\text{Р}}^{\text{А}}$ – множества ЭБП с функцией ОП (далее – *элементов ОП*) и разведки (далее – *элементов Р*), соответственно;

$T_{\sim\text{пер}}^{\text{А}}$ и $T_{\sim\text{под}}^{\text{А}}$ – время передвижения ЭБП на требуемую позицию и его подготовки к работе, соответственно (здесь и далее в нижнем индексе символы «~», «#» и «*» обозначают любую функцию или номер ЭБП);

H – множество видов заметности;

$T_{\text{Ррез}}^{\text{А}}$ – время получения результатов разведки;

$T_{\text{ОПупр}}^{\text{А}}$ – время получения, подготовки, ретрансляции, обработки, анализа информации и принятия решения на применение ЭБП;

$u_{\text{баз}}^{\text{Б}}$, $u_{\text{доп}}^{\text{Б}}$ – уровни базовой и дополнительной защищенности ЭБП от ОП;

$U_{\sim\text{дал}}^{\text{А}}(d)$ – дальностная характеристика применения ЭБП на расстоянии d;

$u_{\text{замет}}^{\text{Б}}(h)$ – уровень h-го вида заметности ЭБП;

$u_{\text{маск}}^{\text{Б}}(h)$ – уровень маскировки ЭБП для h-го вида заметности, учитывающий в том числе аэрозольное противодействие;

$K^{\text{Б}}$ – координаты ЭБП;

$\Theta^{\text{А}}$ – множество доступных для ЭБП координат;

$\phi^{\text{А(Б)}}(f, n)$ – коэффициент противодействия выполнению боевого цикла n-м *элементом Р* и f-м *элементом ОП* стороны А, учитывающий влияние стороны Б на ЭБП стороны А, задействованные в боевом цикле.

В формуле (37) использованы следующие допущения:

- ИТС, люди и устройства ЭБП в элементарном объеме поля боя поражаются огнем с учетом принципа инкапсуляции ИТС и людей в устройства и/или сооружения;
- при вскрытии средствами видовой и/или параметрической разведки хотя бы одного ИТС/устройства вскрывается весь ЭБП;
- используется двухтактная схема рефлексии конфликта, то есть на боевые циклы ВФ А(Б), элементы ОП которых могут уничтожить ЭБП ВФ Б(А), оказывают влияние все способные к этому ЭБП ВФ Б(А).

Коэффициент $\phi^{\text{А(Б)}}(f, n)$ в формуле (37) учитывает влияние ВФ Б(А) на все ЭБП ВФ А(Б), задействованные в боевом цикле. Возможны три варианта реализации этого цикла, когда функции разведки и ОП выполняются:

1) одним комбинированным *элементом Р* и *ОП*;
2) *элементами Р* и *ОП*, связанными напрямую;

3) *элементами Р* и *ОП*, связанными через один или несколько ЭБП.

Для первого варианта коэффициент $\phi^{\text{А}}(f, n) = \infty$, если

$$\exists h \in 1...H\ ,\ \exists g \in 1...N_{\text{ОП}}^{\text{Б(А)}}\ ,\ \exists m \in 1...N_{\text{РЭП}}^{\text{Б(А)}}\ ,\ \exists v \in 1...N_{\text{ЭМИ}}^{\text{Б(А)}}\ ,$$

$$\exists b \in 1...N_{\text{КА}}^{\text{Б(А)}}\ ,\ \exists z \in 1...N_{\text{Р}}^{\text{Б(А)}}\ ,\ \forall q \in 1...N_{\text{Р беспр}_{\#}}^{\text{А(Б)}}$$

$$\min_{\{n\}}\left(T_{\text{Р пер}_n}^{\text{А}} + T_{\text{Р разв}_n}^{\text{А}} + T_{\text{Р эфф}_n}^{\text{А}}\right) \geq \min\begin{pmatrix} T_{\text{ОП}}^{\text{Б}}(g,z), \text{ если } \xi(n,z) \wedge \alpha(n,g), \\ T_{\text{РЭП}}^{\text{Б}}(m), \text{ если } \xi(n,m) \wedge \beta(n,m), \\ T_{\text{ЭМИ}}^{\text{Б}}(v), \text{ если } \xi(n,v) \wedge \gamma(n,v), \\ T_{\text{КА}}(b), \text{ если } \xi(n,b) \wedge \delta(n,b), \\ \infty \text{ в противном случае} \end{pmatrix} \text{ при}$$

$$T_{\text{ОП}}^{\text{Б}}(g,z) = \min_{\{g\}}\left(\max_{\{g\},\{z\}}\left(T_{\text{ОП пер}_g}^{\text{Б}} + T_{\text{ОП разв}_g}^{\text{Б}}, T_{\text{Р пер}_z}^{\text{Б}} + T_{\text{Р разв}_z}^{\text{Б}} + T_{P\text{рез}_z}^{\text{Б}}\right) + T_{\text{ОП упр}_g}^{\text{Б}}\right);$$

$$T_{\text{РЭП}}^{\text{Б}}(m) = \min_{\{m\}}\left(T_{\text{РЭП пер}_m}^{\text{Б}} + T_{\text{РЭП разв}_m}^{\text{Б}} + T_{\text{РЭП рез}_m}^{\text{Б}} + T_{\text{РЭП упр}_m}^{\text{Б}}\right);$$

$$T_{\text{ЭМИ}}^{\text{Б}}(v) = \min_{\{v\}}\left(T_{\text{ЭМИ пер}_v}^{\text{Б}} + T_{\text{ЭМИ разв}_v}^{\text{Б}} + T_{\text{ЭМИ рез}_v}^{\text{Б}} + T_{\text{ЭМИ упр}_v}^{\text{Б}}\right);$$

$$T_{\text{КА}}^{\text{Б}}(b) = \min_{\{b\}}\left(T_{\text{КА пер}_b}^{\text{Б}} + T_{\text{КА разв}_b}^{\text{Б}} + T_{\text{КА рез}_b}^{\text{Б}} + T_{\text{КА физ}_b}^{\text{Б}} + T_{\text{КА техн}_b}^{\text{Б}} + T_{\text{КА упр}_b}^{\text{Б}} + \min\left(T_{\text{КА сет}_b}^{\text{Б}}, T_{\text{КА кан}_b}^{\text{Б}}\right)\right); \quad (38)$$

$$\xi(\#,\sim) = \left(K_{\text{Р}_{\#}}^{\text{А}} \in \Theta_{\text{Р}_{\sim}}^{\text{Б}}\right) \wedge \left(u_{\text{Р замет}_{\#}}^{\text{А}}(h) - u_{\text{Р маск}_{\#}}^{\text{А}}(h) \leq \min_{\{\sim\}}\left(U_{\text{Р дал}_{\sim}}^{\text{Б}}(d,h)\right)\right);$$

$$\alpha(\#,\sim) = \left(K_{\text{Р}_{\#}}^{\text{А}} \in \Theta_{\text{ОП}_{\sim}}^{\text{Б}}\right) \wedge \left(u_{\text{Р доп}_{\#}}^{\text{А}} + u_{\text{Р баз}_{\#}}^{\text{А}} \leq \max_{\{\sim\}}\left(U_{\text{ОП дал}_{\sim}}^{\text{Б}}(d)\right)\right);$$

$$\gamma(\#,\sim) = \left(K_{\text{Р}_{\#}}^{\text{А}} \in \Theta_{\text{ЭМИ}_{\sim}}^{\text{Б}}\right) \wedge \left(u_{\text{Р завис}_{\#}}^{\text{А}} \leq \max_{\{\sim\}}\left(U_{\text{ЭМИ дал}_{\sim}}^{\text{Б}}(d)\right)\right);$$

$$\beta(\#,\sim) = \left(K_{\text{Р}_{\#}}^{\text{А}} \in \Theta_{\text{РЭП}_{\sim}}^{\text{Б}}\right) \wedge \left(\left(u_{\text{Р п/с}_{\#}}^{\text{А}}(q) \leq \max_{\{\sim\},\{q\}}\left(U_{\text{РЭП дал}_{\sim}}^{\text{Б}}(d,q)\right)\right) \wedge \right.$$

$$\left. \wedge \left(\left(N_{\text{Р развИТС}_{\#}}^{\text{А}} \subseteq N_{\text{РЭП достИТС}_{\sim}}^{\text{Б}}\right) \vee \left(\left(N_{\text{Р нав}_{\#}}^{\text{А}} \subseteq N_{\text{РЭП достИТС}_{\sim}}^{\text{Б}}\right) \wedge \left(N_{\text{Р нав}_{\#}}^{\text{А}} \neq \varnothing\right)\right)\right)\right);$$

$$\delta(\#,\sim) = \left(K_{\text{Р}_{\#}}^{\text{А}} \in \Theta_{\text{КА}_{\sim}}^{\text{Б}}\right) \wedge \left(\left(u_{\text{Р с/ш}_{\#}}^{\text{А}}(q) \leq \max_{\{\sim\},\{q\}}\left(U_{\text{КА дал}_{\sim}}^{\text{Б}}(d,q)\right)\right) \wedge \right.$$

$$\left. \wedge \left(\left(\left(N_{\text{Р нав}_{\#}}^{\text{А}} \subseteq N_{\text{КА достИТС}_{\sim}}^{\text{Б}}\right) \wedge \left(N_{\text{Р нав}_{\#}}^{\text{А}} \neq \varnothing\right)\right) \vee \left(N_{\text{Р беспр}_{\#}}^{\text{А}} \subseteq N_{\text{КА достИТС}_{\sim}}^{\text{Б}}\right)\right)\right),$$

где $N_{\text{РЭП}}^{\text{Б(А)}}$, $N_{\text{ЭМИ}}^{\text{Б(А)}}$ и $N_{\text{КА}}^{\text{Б(А)}}$ – множество *элементов РЭП*, *ЭМИ* и *КА* в ВФ Б(А), соответственно;

$T_{\text{КА физ}_{\#}}^{\text{Б(А)}}$ – время получения физического доступа *элемента КА* к ИТС целевого для него элемента (то есть время достижения электромагнитной доступности);

$T_{\text{КА техн}_{\#}}^{\text{Б(А)}}$ – время получения технического доступа *элемента КА* к ИТС целевого для него элемента (то есть время подбора параметров радиосигналов);

$T_{\text{КА сет}_{\#}}^{\text{Б(А)}}$ – время до начала нарушения *элементом КА* доступности информации ИТС целевого для него ЭБП на сетевом, транспортном и сеансовом уровнях ЭМВОС;

$T_{\text{КА кан}_{\#}}^{\text{Б(А)}}$ – время до начала нарушения *элементом КА* доступности информации ИТС целевого для него ЭБП на канальном уровне ЭМВОС;

$N^{\text{А(Б)}}_{*\text{беспр}_{\#}}$ – множество ИТС для беспроводной связи в некотором ЭБП;

$U^{\text{Б(А)}}_{\text{РЭП дал}_{\#}}(d,q)$ – дальностная характеристика применения некоторого *элемента РЭП*, характеризующая его способность нарушить работу q-го ИТС, обеспечивающего беспроводной связью целевой ЭБП, путем достижения или превышения порогового уровня отношения мощностей помехи и сигнала на входе приемника этого ИТС на расстоянии d (рассчитывается согласно [109, 165] с учетом энергопотенциалов, чувствительностей и высот *элемента РЭП* и q-го ИТС, а также дистанции подавления и дистанций связи q-го ИТС с другими ИТС);

$u^{\text{А(Б)}}_{*\text{п/с}_{\#}}(q)$ – пороговый уровень отношения помеха/сигнал для нарушения работы q-го ИТС, обеспечивающего беспроводной связью некоторый ЭБП;

$U^{\text{Б(А)}}_{\text{ЭМИ дал}_{\#}}(d)$ – дальностная характеристика применения *элемента ЭМИ*, характеризующая плотность потока энергии электромагнитного поля, формируемого этим элементом на расстоянии d (рассчитывается согласно [109, 165] с учетом энергопотенциала и высоты *элемента ЭМИ*);

$N^{\text{А(Б)}}_{\text{Р развИТС}_{\#}}$ – множество разведывательных ИТС *элемента Р*;

$N^{\text{Б(А)}}_{*\text{достИТС}_{\#}}$ – множество ИТС, доступных для *элемента РЭП* или *КА*;

$N^{\text{А(Б)}}_{*\text{нав}_{\#}}$ – множество ИТС некоторого ЭБП для получения внешней навигационной информации, без которой этот ЭБП неработоспособен;

$u^{\text{А(Б)}}_{*\text{с/ш}_{\#}}(q)$ – минимальный уровень приема сигнала q-м ИТС, обеспечивающим беспроводной связью ЭБП;

$u^{\text{А(Б)}}_{*\text{завис}_{\#}}$ – пороговая плотность потока энергии электромагнитного поля, формируемая *элементами ЭМИ*, достаточная для подавления ИТС ЭБП;

$U^{\text{Б(А)}}_{\text{КА дал}_{-}}(d,q)$ – дальностная характеристика применения *элемента КА*, характеризующая его способность установить информационное взаимодействие с q-м ИТС, обеспечивающим беспроводной связью и/или навигационной информацией целевой ЭБП, на уровне чувствительности приемника этого ИТС на расстоянии d (рассчитывается согласно [109, 165] с учетом энергопотенциалов, чувствительностей и высот *элемента КА* и q-го ИТС, а также дистанции воздействия на q-й ИТС).

При невыполнении условия (38) коэффициент $\phi^{\text{А(Б)}}(f, n) = 0$ для первого варианта реализации боевого цикла. Для второго варианта $\phi^{\text{А(Б)}}(f, n) = \infty$, если

$$\max\begin{pmatrix} \min\limits_{\{n\}}\left(T^{\text{А(Б)}}_{\text{Р пер}_n} + T^{\text{А(Б)}}_{\text{Р разв}_n} + T^{\text{А(Б)}}_{\text{Р эфф}_n}\right), \\ \min\limits_{\{f\}}\left(T^{\text{А(Б)}}_{\text{ОП пер}_f} + T^{\text{А(Б)}}_{\text{ОП разв}_f} + T^{\text{А(Б)}}_{\text{ОП эфф}_f}\right) \end{pmatrix} \geq$$

$$\geq \min\begin{pmatrix} T_{\text{ОП}}(g,z), \text{если } \left(\xi(n,z)\wedge\alpha(n,g)\right)\vee\left(\xi(f,z)\wedge\alpha(f,g)\right), \\ T_{\text{РЭП}}(m), \text{ если } \left(\xi(n,m)\wedge\beta(n,m)\right)\vee\left(\xi(f,m)\wedge\beta(f,m)\right), \\ T_{\text{ЭМИ}}(v), \text{ если } \left(\xi(n,v)\wedge\gamma(n,v)\right)\vee\left(\xi(f,v)\wedge\gamma(f,v)\right), \\ T_{\text{КА}}(b), \quad \text{если } \left(\xi(n,b)\wedge\delta(n,b)\right)\vee\left(\xi(f,b)\wedge\delta(f,b)\right), \\ \infty \text{ в противном случае} \end{pmatrix}. \tag{39}$$

При невыполнении условия (39) коэффициент $\phi^{\text{А(Б)}}(f, n) = 0$ для второго варианта реализации. Для третьего варианта $\phi^{\text{А(Б)}}(f, n) = \infty$, если

$$\max\begin{pmatrix} \min\limits_{\{n\}}\left(T^{\text{А(Б)}}_{\text{Р пер}_n} + T^{\text{А(Б)}}_{\text{Р разв}_n} + T^{\text{А(Б)}}_{\text{Р эфф}_n}\right), \\ \min\limits_{\{f\}}\left(T^{\text{А(Б)}}_{\text{ОП пер}_f} + T^{\text{А(Б)}}_{\text{ОП разв}_f} + T^{\text{А(Б)}}_{\text{ОП эфф}_f}\right), \\ \max\left(\min\limits_{\{s\}}\left(T^{\text{А(Б)}}_{*\text{пер}_s} + T^{\text{А(Б)}}_{*\text{разв}_s} + T^{\text{А(Б)}}_{*\text{эфф}_s}\right)\right) \end{pmatrix} \geq$$

$$\geq \min\begin{pmatrix} T_{\text{ОП}}(g,z), \text{если } \left(\xi(n,z)\wedge\alpha(n,g)\right)\vee \\ \qquad \vee\left(\xi(f,z)\wedge\alpha(f,g)\right)\vee\left(\bigvee\limits_{\{s\}}\left(\xi_s(s,z)\wedge\alpha_s(s,g)\right)\right), \\ T_{\text{РЭП}}(m), \text{если } \left(\xi(n,m)\wedge\beta(n,m)\right)\vee \\ \qquad \vee\left(\xi(f,m)\wedge\beta(f,m)\right)\vee\left(\bigvee\limits_{\{s\}}\left(\xi_s(s,m)\wedge\beta_s(s,m)\right)\right), \\ T_{\text{ЭМИ}}(v), \text{если } \left(\xi(n,v)\wedge\gamma(n,v)\right)\vee \\ \qquad \vee\left(\xi(f,v)\wedge\gamma(f,v)\right)\vee\left(\bigvee\limits_{\{s\}}\left(\xi_s(s,v)\wedge\gamma_s(s,v)\right)\right), \\ T_{\text{КА}}(b), \text{если } \left(\xi(n,b)\wedge\delta(n,b)\right)\vee \\ \qquad \vee\left(\xi(f,b)\wedge\delta(f,b)\right)\vee\left(\bigvee\limits_{\{s\}}\left(\xi_s(s,b)\wedge\delta_s(s,b)\right)\right), \\ \infty \text{ в противном случае} \end{pmatrix}, \quad (40)$$

где $\{s\}$ – множество промежуточных ЭБП, обеспечивающих передачу разведданных от n-го *элемента Р* f-му *элементу ОП* формирования А(Б).

При невыполнении условия (40) коэффициент $\phi^{\text{А(Б)}}(f, n) = 0$ для третьего варианта реализации боевого цикла.

Формулы (38)-(40) имеют следующий физический смысл. Время до ОП каждого ЭБП ВФ (далее – целевого ЭБП) есть минимальное время, за которое хотя бы одна пара связанных друг с другом ЭБП с функцией разведки и ОП (или один ЭБП с функциями разведки и ОП) противника переместится на требуемую позицию на поле боя, развернется, подготовится к работе, проведет разведку и нанесет удар по целевому ЭБП. При этом ЭБП противника с функцией разведки должен в заданных метеоусловиях заметить целевой ЭБП, и ЭБП с функцией ОП противника должен попасть в этот целевой ЭБП в условиях противодействия противника. Приведенные в этих формулах аспекты взаимного влияния ЭБП учитывают только функции разведки (включая возможность имитации боевой обстановки), управления, связи, ОП, РЭП, воздействия мощным ЭМИ и КА. Следует напомнить, что возможности сторон по нелетальному, психологическому, радиационному, химическому и биологическому воздействию на личный состав учитываются в формуле (36).

С использованием рассмотренной модели представляется возможным оценивать изменение во времени численности ВФ до первой смены позиции любым ЭБП. После смены позиции вышеуказанные показатели рассчитываются снова. То есть модель применима для одного боевого эпизода.

Следует также отметить, что формула (37) приведена в настоящей монографии в обобщенном виде. В ней имеются следующие недостатки:

- не отражены возможности сторон по организации ОП, в то время как избранный способ ОП, безусловно, играет ключевую роль при выполнении боевой задачи ВФ;
- не детализирован перечень приводимых ТТХ средств, входящих в состав ЭБП. Этот перечень всего лишь ограничен указанием так называемых «дальностных» характеристик применения ЭБП;
- не учтена совместимость (интероперабельность) современных и перспективных АС, имеющая существенное влияние на боевую эффективность использующих их ВФ.

Все эти аспекты учитываются в перспективном РМК [39], задачи, состав и общий алгоритм функционирования которого приводятся далее в параграфе 6.2 настоящей монографии. Этот комплекс по сути является ядром компьютерной игры жанра «стратегия». Он может использоваться для исследовательских целей, а также для планирования боевых действий и оценки текущего соотношения БП противоборствующих ВФ в боевых условиях на основе информации о местоположении своих сил и средств и противника, поступающей в режиме реального времени.

Этот РМК в полном объеме базируется на методе, моделях, алгоритмах и методиках, приводимых в главах 3-5 настоящей монографии, но также дополнительно использует широкую номенклатуру алгоритмов ведения разведки, целераспределения, поведения ЭБП в бою и систему методик оценки боевой обстановки для органов управления различных уровней, взаимодействующих посредством обмена неформализованными сообщениями и формализованными боевыми документами. Следует отметить, что такой РМК объединяет в себе три типа программ («Sketch in the decision» (рус. *набросок в решение*), «Blitzkrieg» (рус. *блицкриг*) и «Crystal sphere» (рус. *кристальная сфера*)), наличие которых по классификации НАТО позволяет относить АС ВФ к классам C4I и C4ISR [8].

В РМК используется высоко детализированная база исходных данных. На момент написания этих строк она состоит из 70 сущностей с более чем 500 атрибутами и более чем 120 связями между сущностями. Как и любая сложная система, ядро этого РМК постоянно развивается и совершенствуется. Изложение частных технических аспектов функционирования такого комплекса выходит за рамки настоящей монографии. Ведь ее цель – показать читателю концепцию решения проблемы киберзащиты АС ВФ и существо необходимого для этого научно-методического аппарата. Для этого сделаем акцент на важном аспекте вычислений, проводимых РМК в одном боевом эпизоде. А именно рассмотрим далее, каким образом оценивается время до уничтожения каждого ЭБП, если такие времена являются взаимно влияющими.

4.2.4 Алгоритм расчета времен до уничтожения элементов боевых порядков

Реальная возможность выполнения процессов ведения разведки и целераспределения, а также использования результатов этих процессов при воздействии на противника у каждой из сторон определяется тем, успеют ли ЭБП, объединенные в боевой цикл, выполнить свои функции в условиях противодействия противника. При расчете времен до уничтожения ЭБП используется двухтактная схема рефлексии конфликта ВФ, показанная на рис. 64.

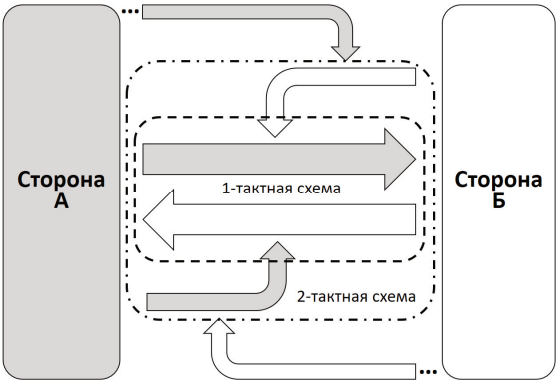


Рис. 64. Рефлексия конфликта воинских формирований при расчете времен до уничтожения их элементов боевых порядков

При двухтактной схеме расчет времени до уничтожения некоторого элемента ВФ Б(А) проводится с учетом того, что на боевые циклы ВФ А(Б), элементы ОП которых могут уничтожить этот элемент, оказывают влияние все способные к этому элементы ВФ Б(А). Выбор в пользу двухтактной схемы обусловлен тем, что однотактная схема не учитывает противодействие, а выигрыш в адекватности детализации отдельного боевого эпизода при использовании даже трехтактной схемы нивелируется лавинообразным ростом сложности математических конструкций и необходимых вычислений.

Состав и структура боевых циклов ВФ зависят от применения в них АС управления следующим образом:

- с применением АС управления боевой цикл связывает по кратчайшему пути *элементы Р* и *В* в их информационно-управляющей сети;
- без применения АС управления боевой цикл связывает *элементы Р* и *В* через ЭБП, которые обеспечивают ретрансляцию разведсведений от *элемента Р* до ближайшего *элемента У*, являющегося начальником для *элемента В*, и управляющей информации от этого *элемента У* до *элемента В* (это задается в исходных данных).

Состав ЭБП, образующих боевые циклы, однозначно определяется **списками информационных и материальных целей** противоборствующих сторон, в которых каждый боевой цикл начинается со средства разведки

в момент обнаружения цели и заканчивается соответствующим средством или боеприпасом в момент окончания их применения (эти моменты фиксируются в списках целей). Промежуточные элементы в боевом цикле определяются вышеуказанными особенностями применения АС управления в ВФ.

Формат **Списка информационных целей** показан на рис. 65.

№	Идентификатор средства разведки	Идентификатор целевого элемента	Местоположение цели	Точность определения местоположения	Идентификатор целевого ИТС	Время обнаружения цели	Стандарт связи/ разведки/ вещания	Литера	Уровень иерархии цели	Признак РЭБ	Время РЭБ

Рис. 65. Формат Списка информационных целей

Список информационных целей содержит следующие поля:

- «№» (автоинкрементное поле);
- «Идентификатор средства разведки» – идентификатор ИТС, которое разведало цель;
- «Идентификатор целевого элемента» – принимает значение идентификатора элемента, если он установлен в процессе разведки, или «NONE» в противном случае;
- «Местоположение цели» – координаты позиции, на которой находится целевое ИТС, если местоположение определено;
- «Точность определения местоположения» – точность определения местоположения цели средством разведки;
- «Идентификатор целевого ИТС» – значение идентификатора разведанного ИТС;
- «Время обнаружения цели» – содержит момент времени, в который цель стала доступной для воздействия;
- «Стандарт связи/разведки/вещания» – значение стандарта, в котором работает цель;
- «Литера» – значение литеры стандарта, на которой работает цель;
- «Уровень иерархии цели» – принимает значение уровня иерархии цели, если он определен в процессе разведки, или «NONE» в противном случае. По мере наполнения Список информационных целей автоматически упорядочивается по значению этого поля;
- «Признак РЭБ» – содержит момент времени, с которого цель считается подверженной ИТВ, если она назначена в процессе целераспределения соответствующих средств и боеприпасов, или «NULL» в противном случае;
- «Время РЭБ» – содержит длительность нахождения цели в условиях ИТВ, определяется в процессе целераспределения соответствующих средств и боеприпасов (забрасываемых передатчиков помех).

Формат **Списка материальных целей** показан на рис. 66.

№	Идентификатор средства разведки	Идентификатор целевого элемента	Местоположение цели	Точность определения местоположения	Время обнаружения цели	Признак сопровождения	Ранг цели	Признак ОП	Время ОП	Признак РХБВ	Время РХБВ	Признак ПсВ	Время ПсВ	Признак НелВ	Время НелВ	Признак ОЭП	Время ОЭП

Рис. 66. Формат Списка материальных целей

Список материальных целей содержит следующие отличные от Списка информационных целей поля:

- «Признак сопровождения» – полю присваивается единица в случае разведки цели средством локационной (например, гидроакустической локации, радиолокации), оптико-визуальной или оптико-электронной разведки. Для таких целей координаты их местоположения всегда актуальны. Если цель разведало другое средство разведки (разведка может вестись во всех известных физических полях), то этому полю присваивается ноль;
- «Признак ОП» – определяется в процессе целераспределения;
- «Время ОП» – содержит одно из трех значений: момент времени, с которого цель считается подверженной воздействию боеприпасов ОП, если она назначена в процессе целераспределения; «NONE» – если цель не уязвима; «NULL» – если цель уязвима, но не назначена;
- «Признак РХБВ» – определяется в процессе целераспределения боеприпасов РХБВ;
- «Время РХБВ» – содержит одно из трех значений: момент времени, с которого цель считается подверженной РХБВ, если она назначена в процессе целераспределения соответствующих боеприпасов; «NONE» – если цель не уязвима к РХБВ (то есть в ЭБП нет людей); «NULL» – если цель уязвима к РХБВ, но не назначена;
- «Признак ПсВ» – определяется в процессе целераспределения средств и боеприпасов ПсВ;
- «Время ПсВ» – содержит одно из трех значений: момент времени, с которого цель считается подверженной ПсВ, если она назначена в процессе целераспределения соответствующих средств и боеприпасов; «NONE» – если цель не уязвима к ПсВ (то есть в ЭБП нет людей); «NULL» – если цель уязвима к ПсВ, но не назначена;
- «Признак НелВ» – определяется в процессе целераспределения средств и боеприпасов НелВ;
- «Время НелВ» – содержит одно из трех значений: момент времени, с которого цель считается подверженной НелВ, если она назначена в процессе целераспределения соответствующих средств и боеприпасов; «NONE» – если цель не уязвима к НелВ (то есть в ЭБП нет людей); «NULL» – если цель уязвима к НелВ, но не назначена;
- «Признак ОЭП» – определяется в процессе целераспределения соответствующих средств и боеприпасов РЭБ;
- «Время ОЭП» – содержит одно из трех значений: момент времени, с которого цель считается подверженной воздействию соответствующих средств или боеприпасов РЭБ, если она назначена в процессе их целераспределения; «NONE» – если цель не уязвима к ОЭП (нет соответствующих средств разведки); «NULL» – если цель уязвима к ОЭП, но не назначена.

С учетом изложенного алгоритм расчета времен до уничтожения ЭБП представлен в виде блок-схемы на рис. 67. Рассмотрим блоки этого алгоритма.

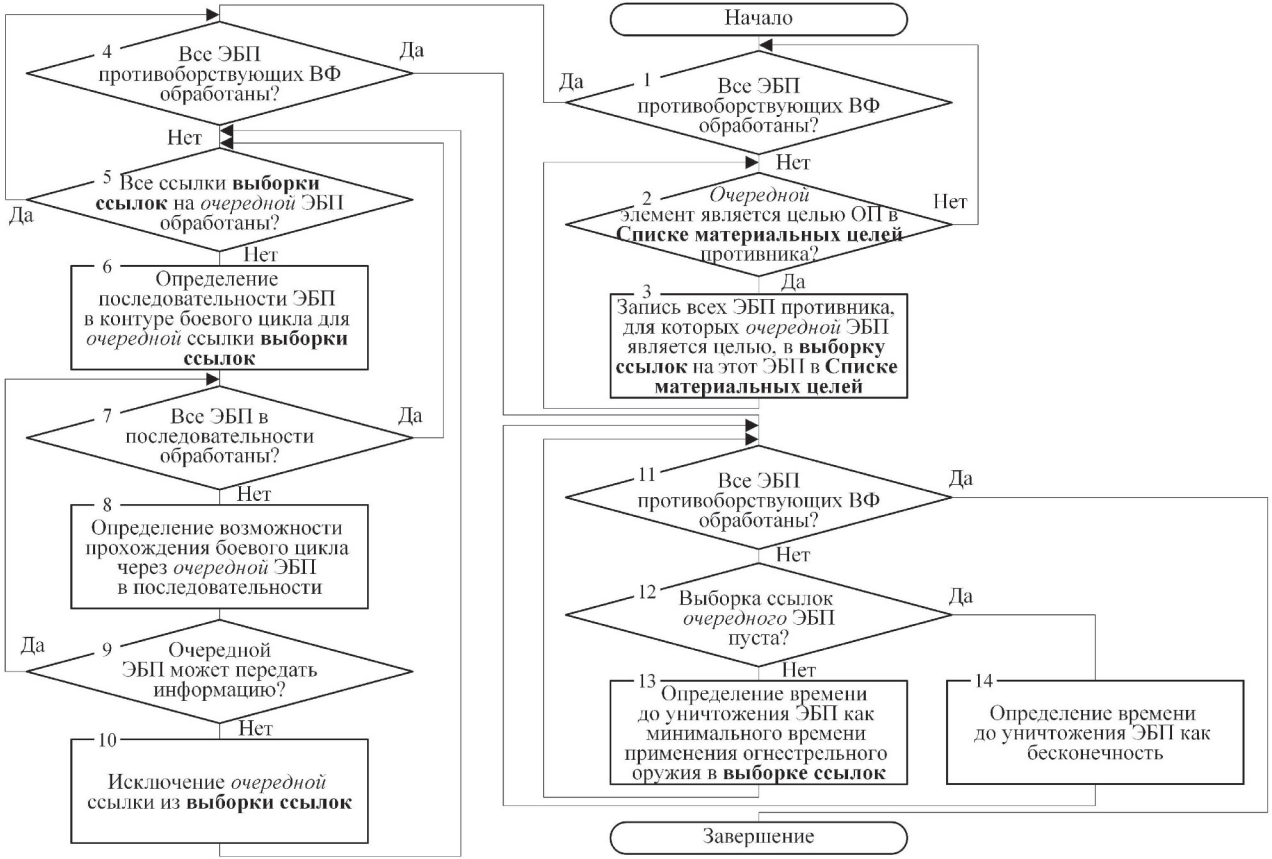


Рис. 67. Блок-схема алгоритма расчета времен до уничтожения элементов боевых порядков

Шаг 1. Проводится проверка, все ли ЭБП противоборствующих ВФ обработаны (выполняется цикл). Если нет, то осуществляется переход к шагу 2. В противном случае осуществляется переход к шагу 4.

Шаг 2. Проводится проверка, является ли очередной ЭБП целью ОП в Списке материальных целей противника. Если нет, то осуществляется переход к шагу 1. В противном случае осуществляется переход к шагу 3.

Шаг 3. Проводится запись ЭБП противника, для которых очередной ЭБП является целью, в выборку ссылок на очередной элемент в Списке материальных целей. Выборка ссылок содержит все строки Списка материальных целей противника, в которых боеприпасы ОП назначены для уничтожения очередного ЭБП. Она упорядочивается по значению параметра «Время ОП» Списка материальных целей. После этого осуществляется переход к шагу 2.

Шаг 4. Проводится проверка, все ли ЭБП противоборствующих ВФ обработаны (выполняется цикл). Если нет, то осуществляется переход к шагу 5. Иначе осуществляется переход к шагу 11. ЭБП, обрабатываемые на этом шаге, называются **рассчитываемыми**.

Шаг 5. Проводится проверка, все ли ссылки выборки ссылок на очередной рассчитываемый ЭБП обработаны (выполняется цикл). Если нет, то осуществляется переход к шагу 6. В противном случае осуществляется переход к шагу 4.

Шаг 6. Проводится определение последовательности ЭБП в боевом цикле уничтожения очередного рассчитываемого ЭБП для очередной ссылки выборки ссылок. Эта процедура осуществляется указанным выше способом, то есть с применением АС управления по кратчайшему пути в информационно-управляющей сети или без применения АС управления.

Шаг 7. Проводится проверка, все ли ЭБП последовательности обработаны (выполняется цикл). Если нет, то осуществляется переход к шагу 8. В противном случае осуществляется переход к шагу 5.

Шаг 8. Проводится определение возможности прохождения боевого цикла через очередной ЭБП последовательности (далее – прохождение фазы боевого цикла, обеспечиваемой ЭБП). Возможность прохождения фазы существует, если момент уничтожения очередного ЭБП последовательности позднее момента передачи им информации в фазе боевого цикла. Момент уничтожения очередного ЭБП последовательности определяется из его выборки ссылок как минимальное время в поле «Время ОП». Момент передачи информации ЭБП в фазе боевого цикла зависит от способа передачи разведсведений и влияния техники РЭБ. Этот момент рассчитывается с использованием следующей формулы:

$$T_{\text{сРЭБ}} = T_{\text{безРЭБ}} \cdot n_{\text{п}}, \qquad (41)$$

где $T_{\text{безРЭБ}}$ – время прохождения фазы боевого цикла через ЭБП без учета влияния техники РЭБ;

$n_{\text{п}}$ – количество попыток прохождения этой фазы в условиях влияния техники РЭБ.

Значение показателя $n_{\text{п}} = 1$ вне зависимости от влияния техники РЭБ в следующих случаях:

- в очередном ЭБП последовательности существует хотя бы одно средство беспроводной связи со следующим ЭБП последовательности, которое в течение всего периода воздействия не назначено ни одному средству или боеприпасу РЭБ в Списке информационных целей противника (см. поля «Признак РЭБ» и «Время РЭБ»),

ИЛИ

- в очередном ЭБП последовательности существует хотя бы один проводной канал передачи информации следующему ЭБП последовательности,

ИЛИ

- между очередным и следующим ЭБП последовательности существует оптическая видимость.

В остальных случаях целое значение показателя $n_{\text{п}}$ определяется по следующей известной из теории вероятностей формуле, предполагающей наиболее пессимистичный случай:

$$n_{\text{п}} = \left\lceil \frac{\ln\left(1 - P_{\text{гпи}}\right)}{\ln\left(P_{\text{ИТВ}} \cdot P_{\text{дост}}\right)} \right\rceil, \tag{42}$$

где $P_{\text{гпи}}$ – вероятность гарантированной передачи информации;

$P_{\text{ИТВ}}$ – вероятность реализации ИТВ;

$P_{\text{дост}}$ – вероятность нахождения забрасываемого передатчика помех в работоспособном состоянии после приземления. Для средства РЭБ $P_{\text{дост}} = 1$.

Рассмотрим пример. Пусть $P_{\text{ИТВ}} = 0{,}5$, а время ретрансляции информации в ЭБП равно $T_{\text{безРЭБ}} = 5$ с. Тогда с учетом классического критерия $P_{\text{гпи}} = 0{,}9$ получаем $n_{\text{п}} = 4$. То есть в условиях влияния техники РЭБ время ретрансляции информации в ЭБП увеличится с 5 до 20 с.

С учетом этого момент передачи информации ЭБП в фазе боевого цикла определяется одним из следующих вариантов.

Вариант 1. Если ЭБП комбинирует функции разведки, управления и воздействия – сумма:

- момента обнаружения ЭБП, по которому применяется боевой цикл;
- времени принятия решения.

Вариант 2. Если ЭБП первый и не последний в последовательности и не имеет функции управления – сумма:

- момента обнаружения ЭБП, по которому применяется боевой цикл;
- времени подготовки и отправки документа с информацией о цели следующему ЭБП в последовательности.

Вариант 3. Если ЭБП первый и не последний в последовательности и имеет функцию управления – сумма:

- момента обнаружения ЭБП, по которому применяется боевой цикл;
- суммы времен принятия решения, подготовки и отправки документа с информацией о цели следующему ЭБП в последовательности.

Вариант 4. Если ЭБП не первый и не последний в последовательности и не имеет функции управления – сумма:

- момента отправки документа предыдущим ЭБП последовательности;
- времени ретрансляции документа в ЭБП.

Вариант 5. Если ЭБП не первый и не последний в последовательности и имеет функцию управления – сумма:

- момента отправки документа предыдущим ЭБП последовательности;
- суммы времен получения и обработки документа, принятия решения, подготовки и отправки документа с информацией о цели следующему ЭБП в последовательности.

Вариант 6. Если ЭБП последний в последовательности и не имеет функции управления – сумма:

- момента отправки документа предыдущим ЭБП последовательности;
- времени получения и обработки документа.

Вариант 7. Если ЭБП последний в последовательности и имеет функцию управления – сумма:

- момента отправки документа предыдущим ЭБП последовательности;
- суммы времен получения и обработки документа и принятия решения.

Шаг 9. Проводится проверка, может ли очередной ЭБП передать информацию боевого цикла. Если нет, то осуществляется переход к шагу 10. В противном случае осуществляется переход к шагу 7.

Шаг 10. Проводится исключение очередной ссылки из текущей выборки ссылок. После этого осуществляется переход к шагу 5.

Шаг 11. Проводится проверка, все ли ЭБП противоборствующих ВФ обработаны (выполняется цикл). Если нет, то осуществляется переход к шагу 12. В противном случае алгоритм завершается.

Шаг 12. Проводится проверка, пуста ли выборка ссылок очередного ЭБП. Если нет, то осуществляется переход к шагу 13. В противном случае осуществляется переход к шагу 14.

Шаг 13. Проводится определение времени до уничтожения ЭБП как минимального времени применения огнестрельного оружия в выборке ссылок. После этого осуществляется переход к шагу 11.

Шаг 14. Проводится определение времени до уничтожения ЭБП как бесконечность. После этого осуществляется переход к шагу 11.

Таким образом, рассмотренный алгоритм позволяет рассчитать времена до уничтожения ЭБП ВФ с учетом их взаимного влияния в ходе одного боевого эпизода.

Рассмотрим далее результаты верификации модели процессов функционирования АС в боевом эпизоде, предлагаемой в настоящей главе.

4.3 Верификация модели

4.3.1 Эталонная модель боя

Для подтверждения корректности модели процессов функционирования АС в боевом эпизоде предлагается использовать ее следующий эталонный вариант, воспроизводящий динамику численности ВФ в бою при средних скоростях потерь, что позволяет свести бой к одному боевому эпизоду [28].

На рис. 68 показаны возможные варианты геометрической интерпретации динамики численности ВФ в таком бою при победе Синих, когда их численность больше или меньше численности Красных.

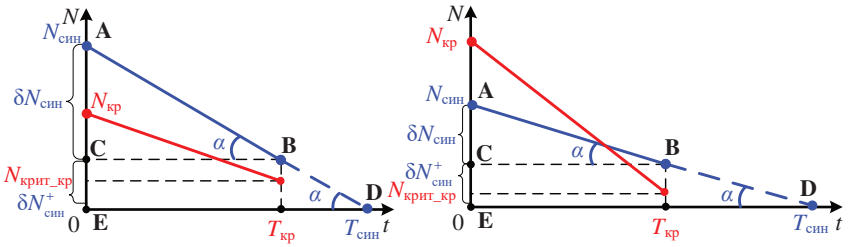


Рис. 68. Геометрические интерпретации динамики численности воинского формирования в бою

Красные прекратили сопротивление в момент времени $T_{кр}$, дойдя до критического значения $N_{крит\_кр}$. Синие были бы уничтожены в момент времени $T_{син}$, если бы Красные продолжили сопротивление. В момент $T_{кр}$ численность Синих снизилась на $\delta N_{син}$. На рис. 68 прямоугольные треугольники $\triangle$**ABC** и $\triangle$**ADE** подобны. Это следует из равенства их углов. Из этого следует соотношение:

$$\frac{\delta N_{син}}{N_{син}} = \frac{T_{кр}}{T_{син}}. \tag{43}$$

То есть боевые потери победивших Синих равны

$$\delta N_{син} = \frac{T_{кр} N_{син}}{T_{син}}. \tag{44}$$

Согласно основным положениям теории боевой эффективности образцов вооружения и ВФ БП определяется величиной наносимого противнику среднего ущерба за время его существования [56]. В рассматриваемом примере Синие потеряли $\delta N_{син}/N_{син}$ своих сил, а Красные потеряли все свои силы. Поэтому положим, что у победившей стороны БП равен 1 (или 100 %), так как она полностью уничтожила противника, а у проигравшей стороны БП меньше единицы. Тогда соотношение БП сторон рассчитывается по формуле

$$f = \left(\frac{\delta N_{син}}{N_{син}} \right)^{-1} = \frac{N_{син}}{\delta N_{син}}. \tag{45}$$

Формула (45) приводится к следующему виду:

$$f = \frac{N_{\text{син}}}{N_{\text{син}} - \delta N^{+}_{\text{син}}} = \left(1 - \frac{\delta N^{+}_{\text{син}}}{N_{\text{син}}}\right)^{-1} = \frac{1}{1 - \delta N^{*}_{\text{син}}}, \quad (46)$$

где $\delta N^{+}_{\text{син}}$ и $\delta N^{*}_{\text{син}}$ – соответственно, остаточная численность и доля численности победившей стороны, то есть Синих. Показатель $\delta N^{*}_{\text{син}}$ в качестве альтернативы показателя, характеризующего соотношение БП, будет использоваться далее.

Подставляя (44) в (45), получаем формулу для оценки соотношения БП, выраженную через времена до уничтожения сторон:

$$f = \frac{T_{\text{син}}}{T_{\text{кр}}}. \quad (47)$$

Для определения значений времен $T_{\text{кр}}$ и $T_{\text{син}}$ рассмотрим эталонную модель боя с применением ИТВ. Структурная схема боя показана на рис. 69.

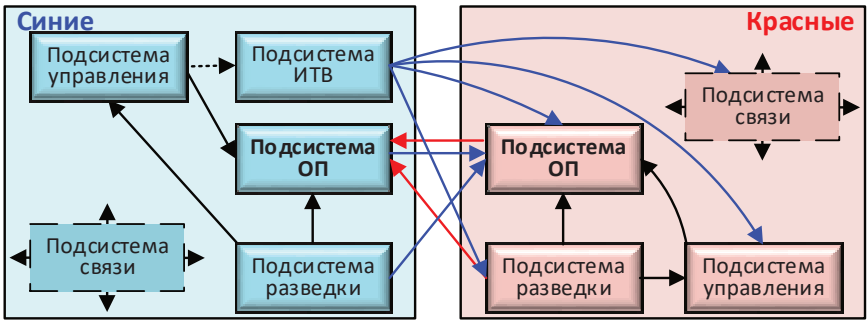


Рис. 69. Структурная схема боя с применением информационно-технического воздействия

Состав сторон включает подсистемы разведки, связи, управления и ОП. Наступающим Синим дополнительно придана подсистема ИТВ, включающая средство ИТВ. Перечень показателей подсистем приведен в таблице 5.

В бою подсистемы разведки, управления, связи и ИТВ (в части КА) являются скрытными, и средства ОП сторон поражают только друг друга. То есть, «в рассматриваемую группу средств ближнего боя взята численность средств ОП с условно включенными в нее другими важными объектами, влияние которых на исход боя проявляется через эффективность средств ОП» [223]. Восстановление средств ОП не происходит, дополнительные резервы не придаются. Подсистема управления может работать в режиме сетецентрического управления, когда средства подсистемы ОП получают целеуказания из подсистемы разведки, минуя подсистему управления. После уничтожения средства ОП огонь автоматически переводится на еще не уничтоженные средства ОП противника. При применении Синими РЭП Красные обнаруживают местоположение источника помех своей подсистемой разведки (заметность техники РЭП в модели учитывается на качественном уровне). Средства ОП применяются в одном из режимов: «ОП $\succ$ РЭП» или «РЭП $\succ$ ОП» ($\succ$ – знак отношения предпочтения).

Таблица 5 — Обозначения и физический смысл показателей в модели боя

Обозначение	Физический смысл	Ед. измерен.
U	ослабление ущерба обороняемым позициям (для наступающих Синих значение этого показателя равно единице)	раз
$P_{\text{гар}}$	требуемая вероятность гарантированного ОП цели	–
Δ	уровень информатизации Красных	–
$N_{\text{кр}}$, $N_{\text{син}}$	количество средств ОП Красных и Синих	ед.
$P_{1\text{бп\_кр}}$, $P_{1\text{бп\_син}}$	вероятность поражения цели одним боеприпасом средства ОП Красных и Синих	–
$T_{\text{оп\_кр}}$, $T_{\text{оп\_син}}$	время подготовки подсистемы ОП Красных и Синих, включающее время обработки управляющей информации (подразумевается, что в каналах нет очереди)	с
$T_{1\text{бп\_кр}}$, $T_{1\text{бп\_син}}$	время воздействия одним боеприпасом в подсистеме ОП Красных и Синих	–
$K_{\text{бп\_кр}}$, $K_{\text{бп\_син}}$	количество боеприпасов в боекомплекте одного средства ОП Красных и Синих	ед.
$N_{\text{им\_кр}}$, $N_{\text{им\_син}}$	количество имитируемых средств ОП Красных и Синих	ед.
$T_{\text{р\_кр}}$, $T_{\text{р\_син}}$	время работы подсистемы разведки (обнаружение цели, анализ данных, подготовка информации; очереди нет)	с
$P_{\text{р\_кр}}$, $P_{\text{р\_син}}$	вероятность вскрытия и распознавания цели подсистемой разведки Красных и Синих	–
$T_{\text{упр\_кр}}$, $T_{\text{упр\_син}}$	время работы подсистемы управления Красных и Синих, (время оценки обстановки, принятия решения и подготовки управляющей информации; очереди нет)	с
$T_{\text{св\_кр}}$, $T_{\text{св\_син}}$	время передачи информации по каналу связи	с
$P_{\text{св\_кр}}$, $P_{\text{св\_син}}$	вероятность гарантированной передачи информации	–
$P_{\text{ИТВ}}$	вероятность реализации ИТВ Синими	–

Рассмотрим режим «ОП≻РЭП». Время уничтожения Красных в этом режиме вычисляется с использованием следующей формулы:

$$T_{\text{кр(ОП)}} = \begin{cases} T_{1\text{бп\_кр}} + \Omega, \text{ если наступают Красные;} \\ \Omega, \text{ если наступают Синие} \end{cases}$$
$$\text{при } \Omega = \frac{N_{\text{кр}} + N_{\text{им\_кр}}}{N_{\text{син}}} K_{1\text{кр}} T_{\text{бц\_син}}, \tag{48}$$

где $K_{1\text{кр}}$ – количество боеприпасов, необходимое средству ОП Синих для уничтожения одного средства ОП Красных;

$T_{\text{бц\_син}}$ – время боевого цикла Синих.

Значение показателя $K_{1\text{кр}}$ для случая, когда боеприпасы не расходуются на цель без гарантии ее поражения, вычисляется по классической формуле [12]:

$$K_{1\text{кр}} = \begin{cases} \Theta, \text{ если } \Theta \geq K_{\text{бп\_кр}}; \\ \infty \text{ в противном случае} \end{cases} \tag{49}$$

$$\text{при } \Theta = \left\lceil \frac{\ln\left(1 - P_{\text{гар}}\right)}{\ln\left(1 - P_{\text{1бп\_син}} P_{\text{р\_син}} U\right)} \right\rceil,$$

где $\lceil ... \rceil$ – операция округления до ближайшего целого в большую сторону.

Значение показателя $T_{\text{бц\_син}}$ в формуле (48) равно

$$T_{\text{бц\_син}} = \begin{cases} T_{\text{1бп\_син}}, \text{ если } (\text{позиции статичны}) \vee (\text{наступают Синие}); \\ T_{\text{р\_син}} + T_{\text{св\_син}} + T_{\text{оп\_син}} + T_{\text{1бп\_син}}, \text{ если } (\text{наступают Красные}) \wedge \\ \wedge (\text{позиции динамичны}) \wedge \begin{pmatrix} \text{есть сетецентрическое} \\ \text{управление у Синих} \end{pmatrix}; \\ T_{\text{р\_син}} + T_{\text{упр\_син}} + 2T_{\text{св\_син}} + T_{\text{оп\_син}} + T_{\text{1бп\_син}}, \text{ если } (\text{наступают Красные}) \wedge \\ \wedge (\text{позиции динамичны}) \wedge \begin{pmatrix} \text{нет сетецентрического} \\ \text{управления у Синих} \end{pmatrix}. \end{cases} \quad (50)$$

Время уничтожения Синих в режиме «ОП $\succ$ РЭП» при условии, что их подсистема ИТВ не является целью, вычисляется по формуле (48), в которой инвертированы индексы сторон конфликта, то есть:

$$T_{\text{син(ОП)}} = \begin{cases} T_{\text{1бп\_син}} + \Omega, \text{ если наступают Синие;} \\ \Omega, \text{ если наступают Красные} \end{cases}$$
$$\text{при } \Omega = \frac{N_{\text{син}} + N_{\text{им\_син}}}{N_{\text{кр}}} K_{\text{1син}} T_{\text{бц\_кр}}, \quad (51)$$

где $K_{\text{1син}}$ – количество боеприпасов, необходимое средству ОП Красных для уничтожения одного средства ОП Синих;

$T_{\text{бц\_кр}}$ – время боевого цикла Красных.

Формулы (48) и (51) предполагают одинаковую тактику применения средств ОП сторон. Например, в работах [55, 265] показано, что наиболее рациональной является тактика «все на одного» с последовательным переводом огня на менее приоритетные цели.

Значение показателя $K_{\text{1син}}$ в формуле (51) для случая, когда боеприпасы не расходуются на цель без гарантии ее поражения, вычисляется по формуле

$$K_{\text{1син}} = \begin{cases} \Theta, \text{ если } \Theta \geq K_{\text{бп\_син}}; \\ \infty \text{ в противном случае} \end{cases}$$
$$\text{при } \Theta = \left\lceil \frac{\ln\left(1 - P_{\text{гар}}\right)}{\ln\left(1 - \left(P_{\text{1бп\_кр}} L_{\text{ИТВ\_оп}}\right)\left(P_{\text{р\_кр}} L_{\text{ИТВ\_р}}\right) U\right)} \right\rceil, \quad (52)$$

где $L_{\text{ИТВ\_оп}}$ и $L_{\text{ИТВ\_р}}$ – показатели снижения вероятности выполнения процессов в подсистемах ОП и разведки Красных за счет КА, РЭП или воздействия мощным ЭМИ. Значения этих показателей предлагается рассчитывать с использованием следующего выражения:

$$L_{\text{ИТВ\_*}} = \begin{cases} 1 - P_{\text{ИТВ}}\Delta, \text{ если подсистема * (то есть ОП или разведки)} \\ \qquad \text{подвержена КА, РЭП или воздействию мощным ЭМИ;} \\ 1 \text{ в противном случае.} \end{cases} \quad (53)$$

Значение показателя $T_{\text{бц\_кр}}$ в формуле (51) предлагается вычислять следующим образом:

$$T_{\text{бц\_кр}}=\begin{cases} T_{\text{1бп\_кр}},\ \text{если}\ (\text{позиции статичны})\vee(\text{наступают Красные});\\ T_{\text{р\_кр}}K_{\text{ИТВ\_р}}+T_{\text{св\_кр}}K_{\text{ИТВ\_св}}+\left(T_{\text{оп\_кр}}+T_{\text{1бп\_кр}}\right)K_{\text{ИТВ\_оп}},\ \text{если}\\ \quad(\text{наступают Синие})\wedge(\text{позиции динамичны})\wedge\\ \quad\wedge(\text{у Красных сетецентрическое управление});\\ T_{\text{р\_кр}}K_{\text{ИТВ\_р}}+T_{\text{упр\_кр}}K_{\text{ИТВ\_упр}}+2T_{\text{св\_кр}}K_{\text{ИТВ\_св}}+\left(T_{\text{оп\_кр}}+T_{\text{1бп\_кр}}\right)K_{\text{ИТВ\_оп}},\\ \quad\text{если}\ (\text{наступают Синие})\wedge(\text{позиции динамичны})\wedge\\ \quad\wedge(\text{у Красных нет сетецентрического управления}). \end{cases} \tag{54}$$

Показатели $K_{\text{ИТВ\_р}}$, $K_{\text{ИТВ\_оп}}$ и $K_{\text{ИТВ\_упр}}$ в формуле (54) характеризуют влияние КА Синих на время выполнения операций, соответственно, в подсистеме разведки, ОП и управления Красных. Учитывая вероятностный характер КА или воздействия мощным ЭМИ и обязательность выполнения операций в подсистемах, эти показатели характеризуют количество попыток выполнить одну операцию в условиях таких воздействий. Для оценки значений этих показателей предлагается применять известную в теории вероятностей формулу определения гарантированного количества независимых повторений одного эксперимента в наиболее пессимистичном случае, когда успешное выполнение операции осуществляется при ее последнем повторении:

$$K_{\text{ИТВ\_р}}=K_{\text{ИТВ\_оп}}=K_{\text{ИТВ\_упр}}=\begin{cases} \dfrac{1}{1-P_{\text{ИТВ}}\Delta},\ \text{если подсистема подвержена}\\ \qquad\qquad\text{КА или воздействию мощного ЭМИ;}\\ 1\ \text{в противном случае.} \end{cases} \tag{55}$$

Количество попыток для различных Δ и $P_{\text{ИТВ}}$ показано на рис. 70.

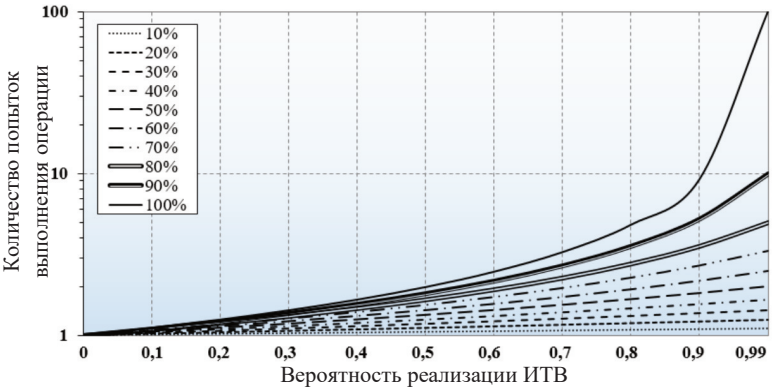


Рис. 70. Зависимость количества попыток выполнения одной операции от вероятности ИТВ при различных Δ (в логарифмическом масштабе)

Оценивать значение $K_{\text{ИТВ\_св}}$ предлагается по следующей формуле [71]:

$$K_{\text{ИТВ\_св}}=\begin{cases} \dfrac{\ln P_{\text{св\_кр}}}{\ln\left(1-P_{\text{ИТВ}}\Delta\right)},\ \text{если на подсистему связи}\\ \qquad\text{производится РЭП, воздействие мощным ЭМИ или КА;}\\ 1\ \text{в противном случае.} \end{cases} \tag{56}$$

Формула (56) используется для учета КА, РЭП или воздействия мощным ЭМИ. Из формулы следует критерий эффективности ИТВ на подсистему связи:

$$P_{\text{ИТВ}} > \frac{1 - P_{\text{св\_кр}}}{\Delta}. \tag{57}$$

Методика расчета значения показателя Δ для отдельного образца вооружения и ВФ в целом предложена в [34] и будет рассмотрена далее в параграфе 5.3. Под уровнем информатизации подсистемы связи ВФ в формуле (57) понимается доля в нем ЭБП, связь которых с остальными ЭБП этого ВФ осуществляется с применением ИТС связи (за исключением средств проводной аналоговой связи).

В режиме работы средств ОП с приоритетом «РЭП $\succ$ ОП» подсистема ОП Красных до обнаружения средства РЭП Синих воздействует на их подсистему ОП, после обнаружения средства РЭП уничтожает его и продолжает воздействовать на подсистему ОП Синих. Время уничтожения Красных в режиме «РЭП$\succ$ОП» вычисляется по формуле (48), то есть $T_{\text{кр(РЭП)}} = T_{\text{кр(ОП)}}$. Время до уничтожения подсистемы ИТВ Синих ($T_{\text{ун\_ИТВ}}$) при условии одновременного начала РЭП и ОП, что часто практикуется, вычисляется следующим образом:

$$T_{\text{ун\_ИТВ}} = \begin{cases} T_{\text{вскр\_ИТВ}} + \dfrac{K_{\text{1син}} T_{\text{1бп\_кр}}}{N_{\text{кр}} P_{\text{оп\_кр}}\left(T_{\text{вскр\_ИТВ}}\right)}, \text{ если позиции динамичны;} \\ \dfrac{K_{\text{1син}} T_{\text{1бп\_кр}}}{N_{\text{кр}}} \text{ в противном случае,} \end{cases} \tag{58}$$

где $T_{\text{вскр\_ИТВ}}$ – время вскрытия Красными местонахождения подсистемы ИТВ Синих;

$P_{\text{оп\_кр}}(T_{\text{вскр\_ИТВ}})$ – вероятность работоспособного состояния подсистемы ОП Красных в момент $T_{\text{вскр\_ИТВ}}$.

Значение показателя $T_{\text{вскр\_ИТВ}}$ в формуле (58) предлагается вычислять следующим образом:

$$T_{\text{вскр\_ИТВ}} = \begin{cases} T_{\text{р\_кр}} K_{\text{ИТВ\_р}} + T_{\text{св\_кр}} K_{\text{ИТВ\_св}} + \left(T_{\text{оп\_кр}} + T_{\text{1бп\_кр}}\right) K_{\text{ИТВ\_оп}}, \\ \quad \text{если у Красных сетецентрическое управление;} \\ T_{\text{р\_кр}} K_{\text{ИТВ\_р}} + T_{\text{упр\_кр}} K_{\text{ИТВ\_упр}} + 2T_{\text{св\_кр}} K_{\text{ИТВ\_св}} + \\ + \left(T_{\text{оп\_кр}} + T_{\text{1бп\_кр}}\right) K_{\text{ИТВ\_оп}}, \text{ в противном случае.} \end{cases} \tag{59}$$

Для вычисления значения показателя $P_{\text{оп\_кр}}(T_{\text{вскр\_ИТВ}})$ в формуле (58) предлагается воспользоваться моделью функционирования ТК ИТС в боевых условиях, рассмотренной в параграфе 3.3. Для повышения скорости расчетов динамики $P_{\text{оп\_кр}}$ может использоваться упрощенная модель функционирования сложной технической системы, граф которой включает состояния 1 и 6 этой модели. Это позволяет свести получаемую с использованием метода, изложенного в [266], полумарковскую модель к последовательности из n+1 состояний с однонаправленными переходами из 1-го в (n+1)-е состояние и интенсивностью переходов между состояниями λ, равной частному от деления времени до уничтожения на n. Полученная система из n линейных однородных дифференциальных уравнений решается известным численным методом.

Время до уничтожения подсистемы ОП Синих в режиме «РЭП $\succ$ ОП» вычисляется по следующей формуле:

$$T_{\text{син(РЭП)}} = T_{\text{ун\_ИТВ}} + T_{\text{ост}}, \tag{60}$$

где $T_{\text{ун\_ИТВ}}$ – время до уничтожения подсистемы ИТВ Синих, см. формулу (58);

$T_{\text{ост}}$ – время уничтожения Красными оставшейся доли подсистемы ОП Синих после уничтожения подсистемы ИТВ (без влияния РЭП).

Положим, что сумма долей средств ОП Синих, уничтоженных Красными до ($Z_{\text{до}}$) и после ($Z_{\text{после}}$) уничтожения подсистемы ИТВ Синих, равна единице ($Z_{\text{до}}+Z_{\text{после}}=1$). При неизменной интенсивности ОП в бою в течение времени $T_{\text{ун\_ИТВ}}$ Красными будет уничтожена доля подсистемы ОП Синих $Z_{\text{до}}$, вычисляемая по формуле

$$Z_{\text{до}} = \frac{T_{\text{ун\_ИТВ}}}{T^{\bullet}_{\text{син(ОП)}}}, \tag{61}$$

где $T^{\bullet}_{\text{син(ОП)}}$ – время уничтожения Синих в режиме «ОП $\succ$ РЭП» при условии, что их подсистема ИТВ не уничтожена, но является целью. Это значение равно

$$T^{\bullet}_{\text{син(ОП)}} = \begin{cases} T_{\text{1бп\_син}} + \Omega, & \text{если наступают Синие;} \\ \Omega, & \text{если наступают Красные} \end{cases}$$
$$\text{при } \Omega = \frac{N_{\text{син}} + N_{\text{им\_син}} + 1}{N_{\text{кр}}} K_{\text{1син}} T_{\text{бц\_кр}}. \tag{62}$$

Оставшаяся доля подсистемы ОП Синих $Z_{\text{после}}$, которая будет уничтожаться по истечении времени $T_{\text{ун\_ИТВ}}$, определяется по формуле

$$Z_{\text{после}} = 1 - Z_{\text{до}} = 1 - \frac{T_{\text{ун\_ИТВ}}}{T^{\bullet}_{\text{син(ОП)}}}. \tag{63}$$

Тогда время $T_{\text{ост}}$ в формуле (60) будет вычисляться следующим образом:

$$T_{\text{ост}} = \left(1 - Z_{\text{до}}\right) \cdot T_{\text{син(ОП)}} = \left(1 - \frac{T_{\text{ун\_ИТВ}}}{T^{\bullet}_{\text{син(ОП)}}}\right) T_{\text{син(ОП)}}, \tag{64}$$

где значение показателя $T_{\text{син(ОП)}}$ вычисляется по указанной выше формуле (51).

Подставляя (64) в (60), получаем следующее выражение:

$$T_{\text{син(РЭП)}} = T_{\text{ун\_ИТВ}} + \left(1 - \frac{T_{\text{ун\_ИТВ}}}{T^{\bullet}_{\text{син(ОП)}}}\right) T_{\text{син(ОП)}}. \tag{65}$$

Исходные параметры модели могут детализироваться (например, вводиться несколько типов средств, входящих в состав каждой подсистемы, учитываться особенности работы средств каждого типа по различным типам целей). Общности модели это не нарушит, поскольку в предлагаемом подходе к аналитическому моделированию боя важна не численность сторон, а время, которое необходимо сторонам для уничтожения противника. При перемещении ЭБП в трехмерном пространстве в рамках заданного сценария боя время до уничтожения этих элементов вычисляется в отдельных боевых эпизодах для остаточной после предыдущего эпизода численности ВФ с учетом дальностных характеристик средств, входящих в его подсистемы.

4.3.2 Исходные данные для верификации

Задача верификации модели боя может решаться только частично, так как подтвердить натурным экспериментом результаты математического моделирования в этом случае нельзя. Представляется возможным только применять математические модели к уже имеющимся статистическим данным. Но статистика уязвимостей образцов вооружения ВФ не публикуется, поскольку такая информация имеет важное значение для обороноспособности любой страны. К тому же известные аналитические модели боя строятся на существенно отличающихся принципах, используют сокращенный набор параметров ИТВ и ВФ, на которые влияет ИТВ, а приводимые авторами этих моделей результаты в большинстве случаев не содержат полного описания исходных данных. Тем не менее, частичная верификация предлагаемой модели проведена путем сравнения результатов ее применения с результатами применения известных аналитических моделей-прототипов [71, 300] для динамичного боя с параметрами:

- ВФ – самоходный артиллерийский дивизион, то есть $N_{кр} = N_{син} = 18$;
- $N_{им\_кр} = N_{им\_син} = 0$;
- $U = 1$;
- $P_{гар} = 0{,}94$. Например, при выполнении упражнения ПМ-1 (стрельба из пистолета Макарова на 25 м) это соответствует оценке «удовлетворительно», когда нужно набрать 18 из 30 баллов при трех выстрелах;
- $T_{р\_кр} = T_{р\_син} = 30$ с – время определения координат цели при первичном ее обнаружении или места разрыва снаряда при корректировке огня;
- $P_{р\_кр} = P_{р\_син} = 0{,}99$ – соответствует оптико-визуальной разведке цели;
- $T_{упр\_кр} = T_{упр\_син} = 20$ с – время оценки обстановки и распределения координат средствам ОП;
- $T_{оп\_кр} = T_{оп\_син} = 30$ с – время анализа координат, полученных от подсистемы разведки, и производства расчетов;
- $T_{1бп\_кр} = T_{1бп\_син} = 8$ с;
- $K_{бп\_кр} = K_{бп\_син} = \infty$;
- $P_{1бп\_кр} = P_{1бп\_син} = 0{,}3$ – соответствует классическим для артиллерии восьми снарядам для поражения точечной цели при стрельбе с закрытой огневой позиции;
- $P_{св\_кр} = 0{,}9$;
- $T_{св\_кр} = T_{св\_син} = 30$ с;
- СКО для времен равно 10 %;
- подсистема ИТВ состоит из одного наземного средства.

4.3.3 Результаты верификации

Первая модель-прототип [71, 250] имеет следующий вид:

$$f_{рез} = f_{нач}\, e^{-(1-C_{защ})v}, \qquad (66)$$

где $f_{рез}$ и $f_{нач}$ – результирующее и начальное соотношения БП, соответственно;

$C_{защ}$ – защищенность подсистемы управления от РЭП;

v – доля подавленных каналов передачи информации, то есть $v = P_{итв}$.

Для заданных условий в формуле (66) $f_{нач}$ = 1. Экспоненциальный множитель в (66) характеризует ослабление стороны, подвергшейся РЭП (в заданных условиях Красных). С учетом этого выигрыш Синих оценивается по формуле

$$\delta N^{*}_{син} = 1 - e^{-(1-C_{защ})v}. \qquad (67)$$

На рис. 71 показаны результаты верификации для первой модели-прототипа в случае, когда защищенность подсистемы управления Красных от РЭП $C_{защ}$ и уровень информатизации Δ связаны зависимостью $C_{защ}$ =1 – Δ.

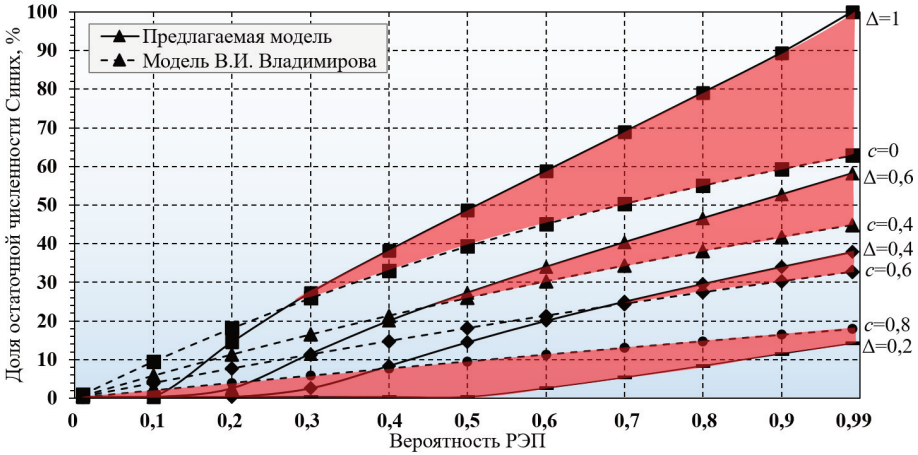


Рис. 71. Верификация для первой модели-прототипа (моделируется радиоэлектронное подавление подсистемы связи)

Из анализа результатов сравнения моделей следует, что их оценки в целом сопоставимы, но максимальное отклонение результатов превышает 10 % при Δ > 0,7. Такое различие обусловлено тем, что модель-прототип изначально ориентирована на оперативное звено, а предлагаемая модель ориентирована на тактическое звено.

Вторая модель-прототип – это уравнения Осипова-Ланчестера 2-го рода (линейный закон Ланчестера) [300], которые используются для оценки эффективности стрельбы по площадям и в том числе взяты за основу в работе [223]:

$$\begin{cases} B(t) = B_0 \dfrac{\beta R_0 - \gamma B_0}{\beta R_0 e^{(\beta R_0 - \gamma B_0)t} - \gamma B_0}; \\ R(t) = R_0 \dfrac{\gamma B_0 - \beta R_0}{\gamma B_0 e^{(\gamma B_0 - \beta R_0)t} - \beta R_0}, \end{cases} \qquad (68)$$

где B_0, R_0 и $B(t)$, $R(t)$ – численность Синих (*Blue*) и Красных (*Red*) в начале боя и в момент времени t, соответственно;

γ и β – скорострельности (интенсивности выполнения задач поражения) одной боевой единицы Синих и Красных, соответственно, определяемые через среднее время выполнения задачи ОП одной боевой единицы T ($\gamma = 1/T$).

Эта модель изначально ориентирована на тактическое звено. Для заданных условий боя (то есть $B_0 = R_0$) система (68) приобретает следующий вид:

$$\begin{cases} B(t)[\%] = 100\dfrac{\left(\beta - \delta\beta_р\right) - \gamma}{\left(\beta - \delta\beta_р\right)e^{\left((\beta-\delta\beta_р)-\gamma\right)t} - \gamma}; \\ R(t)[\%] = 100\dfrac{\gamma - \left(\beta - \delta\beta_р\right)}{\gamma e^{\left(\gamma-(\beta-\delta\beta_р)\right)t} - \left(\beta - \delta\beta_р\right)}, \end{cases} \tag{69}$$

где $\delta\beta_р$ – ослабление скорострельности Красных за счет тотального РЭП их подсистем разведки, связи и ОП.

Для рассматриваемых условий боя существует аналитическое решение задачи оценки боевых потерь победивших Синих [300]:

$$\delta B[\%] = 100\left(1 - \frac{\beta - \delta\beta_р}{\gamma}\left(1 - N_{крит\_кр}\right)\right), \tag{70}$$

где $N_{крит\_кр}$ – критическое значение численности Красных, по достижении которого в бою они сдаются.

Пусть $N_{крит\_кр} = 0$. Для рассматриваемых условий боя $\gamma = \beta$. Тогда

$$\delta B[\%] = 100\frac{\delta\beta_р}{\beta}. \tag{71}$$

Поскольку показатель ослабления скорострельности за счет РЭП $\delta\beta_р$ может принимать значение в диапазоне $[0, \beta]$, будем считать, что при $\delta\beta_р = \beta$ вероятность РЭП подсистемы разведки Красных равна единице, а при $\delta\beta_р = 0$ она равна нулю.

Допустим, значения $\delta\beta_р$ и вероятности РЭП связаны зависимостью

$$\delta\beta_р = \beta \cdot P_{ИТВ} \cdot \Delta. \tag{72}$$

Для нее на рис. 72 показаны результаты применения предлагаемой модели и второй модели-прототипа.

Максимальное абсолютное отклонение результатов моделей для заданных условий боя в этом случае составляет не более 4,7 %. При увеличении $P_{1бп\_кр} = P_{1бп\_син}$ до уровня высокоточного оружия или уровня стрельбы с открытой огневой позиции результаты оценок предлагаемой эталонной модели и модели-прототипа существенно различаются. Это связано с тем, что вторая модель-прототип изначально разрабатывалась и верифицировалась для оценки эффективности стрельбы с закрытых огневых позиций с применением обычного огнестрельного оружия.

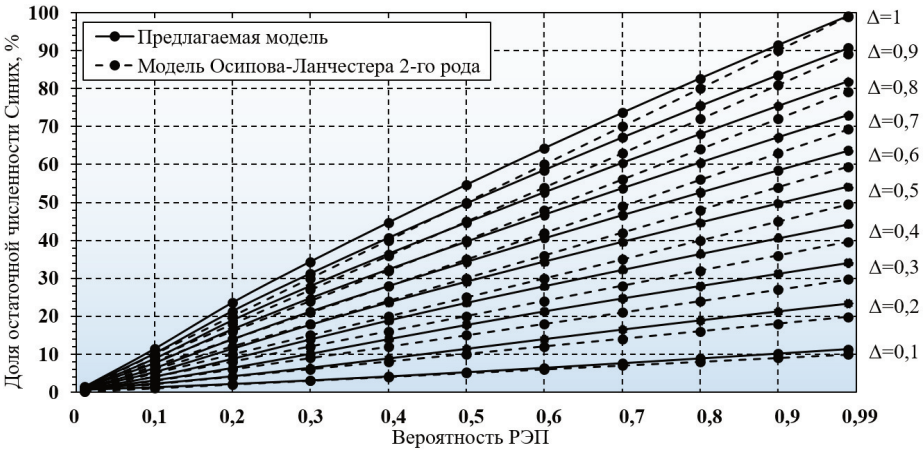


Рис. 72. Верификация для второй модели-прототипа (моделируется радиоэлектронное подавление подсистемы разведки)

Третья модель-прототип – это уравнения Осипова-Ланчестера 1-го рода (квадратичный закон Ланчестера) [300], которые используются для оценки БП ВФ при стрельбе с открытых огневых позиций:

$$\begin{cases} B(t) = B_0 \cosh\left(t\sqrt{\beta\gamma}\right) - \sqrt{\dfrac{\beta}{\gamma}} R_0 \sinh\left(t\sqrt{\beta\gamma}\right); \\ R(t) = R_0 \cosh\left(t\sqrt{\beta\gamma}\right) - \sqrt{\dfrac{\gamma}{\beta}} B_0 \sinh\left(t\sqrt{\beta\gamma}\right). \end{cases} \tag{73}$$

Для заданных условий боя система (73) приобретает следующий вид:

$$\begin{cases} B(t)[\%] = \cosh\left(t\sqrt{(\beta - \delta\beta_р)\gamma}\right) - \sqrt{\dfrac{\beta - \delta\beta_р}{\gamma}} \sinh\left(t\sqrt{(\beta - \delta\beta_р)\gamma}\right); \\ R(t)[\%] = \cosh\left(t\sqrt{(\beta - \delta\beta_р)\gamma}\right) - \sqrt{\dfrac{\gamma}{\beta - \delta\beta_р}} \sinh\left(t\sqrt{(\beta - \delta\beta_р)\gamma}\right). \end{cases} \tag{74}$$

Для этой системы уравнений также существует аналитическое решение задачи оценки боевых потерь победивших Синих [300]:

$$\delta B[\%] = 100\sqrt{1 - \frac{\beta - \delta\beta_р}{\gamma}\left(1 - N_{крит\_кр}\right)}. \tag{75}$$

Пусть $N_{крит\_кр} = 0$. Для рассматриваемых условий боя $\gamma = \beta$. Тогда

$$\delta B[\%] = 100\sqrt{\frac{\delta\beta_р}{\beta}}. \tag{76}$$

По аналогии с предыдущим прототипом предположим, что $\delta\beta_р$ и вероятность РЭП связаны зависимостью (72). На рис. 73 для такой

зависимости показано сравнение результатов применения сравниваемых моделей при РЭП подсистем разведки и ОП. Максимальное абсолютное отклонение составило 15 %.

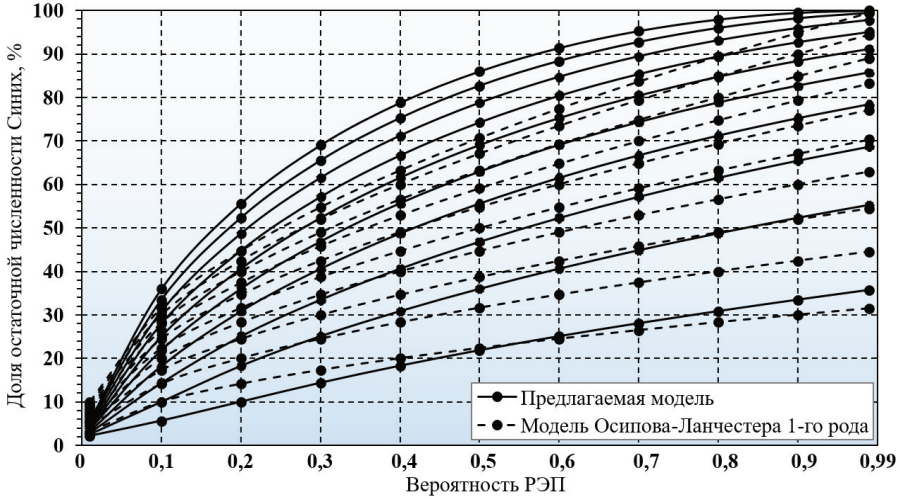


Рис. 73. Верификация для третьей модели-прототипа (моделируется радиоэлектронное подавление подсистем разведки и огневого поражения)

Следует заметить, что решения (70) и (75) применимы к так называемому «А-правилу» боя (превосходство в абсолютных величинах) [300], предполагающему выход стороны из боя в случае достижения ее численности заданного порогового значения. Тем не менее, эти решения, адаптированные к условиям верификации в выражениях (71) и (76), полностью соответствуют адаптированным аналогичным образом решениям для так называемого «Р-правила», предполагающего выход стороны из боя в случае достижения заданного порогового соотношения численности сторон.

Результаты верификации на рис. 72, 73 показывают, что имеет место более сложная зависимость между исследуемыми параметрами. Она имеет вид

$$\delta\beta_p = \beta y\,(P_{ИТВ}, \Delta), \qquad (77)$$

где y – показательная функция.

Из изложенного следует вывод, что линейный и квадратичный законы Ланчестера характерны только для боев от античности и до середины XX века. Сегодня эти зависимости имеют более высокую степень, подчеркивающую существенно возросшие возможности современных средств разнохарактерного воздействия в бою. Это перспективное направление исследований.

Таким образом, можно констатировать, что результаты проведенной верификации могут быть признаны удовлетворительными. Они свидетельствуют о том, что при различных наборах исходных данных результаты эталонной модели с приемлемой точностью повторяют результаты известных моделей

боя. По сути, это означает, что предлагаемый подход к аналитическому моделированию боя дает возможность разрабатывать такие модели, которые можно считать обобщающими известные аналитические модели боя.

4.3.4 Аналитическая зависимость остаточной доли численности воинского формирования от вероятности реализации информационно-технического воздействия во встречном бою

Для повышения оперативности применения эталонной модели боя при различных вариантах применения ИТВ в ходе проведенного исследования выявлена универсальная аналитическая зависимость остаточной доли численности ВФ от вероятности реализации ИТВ во встречном бою одинаковых ВФ, одно из которых дополнено подсистемой ИТВ:

$$\delta N^{*}_{\text{син}} = \mathbf{a}\Delta^{\mathbf{b}}\left(1-\left(P_{\text{ИТВ}}\mathbf{d}\right)^{\mathbf{c}}\right), \tag{78}$$

где **a** – коэффициент, характеризующий оперативность функционирования подсистем ВФ в условиях ИТВ;

b и **c** – коэффициенты, характеризующие вероятностные и временные параметры функционирования подсистем в условиях ИТВ;

d – коэффициент, учитываемый при ИТВ на подсистему связи ВФ;

Δ – уровень информатизации.

Формула (78) может быть использована для экспресс-оценки эталонной меры эффективности ИТВ или *коэффициента полезного действия* заданного комплекта техники ИТВ против ВФ с заданными параметрами. По мнению автора, развитие этого аналитического выражения является весьма перспективным и может принести существенную пользу для практики.

В ходе исследования также проведен регрессионный анализ результатов применения рассмотренной эталонной модели, и с использованием метода наименьших квадратов получены формулы для расчета значений коэффициентов в формуле (78). Эти формулы приведены в таблице 6 для вариантов тотального ИТВ на все подсистемы и выборочной реализации ИТВ на подсистему связи, управления, разведки или ОП.

В таблице 6 используется единая формула для вычисления количества боеприпасов для уничтожения цели:

$$\mathbb{N} = \left\lceil \frac{\ln(1-P_{\text{гар}})}{\text{n}(1-P_{\text{р}}P_{\text{1бп}})} \right\rceil, \tag{79}$$

где $P_{\text{р}}$ – вероятность разведки;

$P_{\text{гар}}$ – требуемая вероятность гарантированного ОП цели;

$P_{\text{1бп}}$ – вероятность ОП цели одним боеприпасом.

Точность формул в таблице 6 характеризуется диаграммами максимальных абсолютных отклонений численных значений, полученных с применением формулы (78), от результатов вычислений, полученных для различных условий боя с применением рассматриваемой в настоящем параграфе эталонной аналитической модели боя. Эти диаграммы показаны на рис. 74-78 [29].

Таблица 6 — Коэффициенты в формуле (78)

Условия боя	Выражения для расчета коэффициентов	Примечание
1. Тотальные КА или скрытное воздействие мощным ЭМИ	$\mathbf{a} = 1$ $\mathbf{b} = \dfrac{1}{\Delta^{1,88}\left(3,55 - 0,02\ln\mathbb{N}\right)^{2,05} + k^{2,04}}$, где $k = 1,21 + 0,84T_{\text{бц}}^{-0,06}\mathbb{N}^{-1}$ $\mathbf{c} = \Delta^{2,34}k^{2,56} + k^{1,29}$ $\mathbf{d} = 1$	$T_{\text{бц}}$ – время от обнаружения цели до первого выстрела по ней
2. КА, скрытное воздействие мощным ЭМИ или РЭП применительно к подсистеме связи	$\mathbf{a} = 1,04 - \left(8\cdot10^{-4}T_{\text{св}} + 0,03\right)\ln T_{\text{бц}} + 6\cdot10^{-3}T_{\text{св}}$ $\mathbf{b} = 0,0147e^{-0,027T_{\text{св}}}T_{\text{бц}} + 2\cdot10^{-4}T_{\text{св}}^2 - 0,015T_{\text{св}} + 1,144 + 1,1T_{\text{св}}^{-1,04}\ln\mathbb{N}$ $\mathbf{c} = 63,1T_{\text{бц}}^{-1,19}T_{\text{св}}^{1-4,43T_{\text{бц}}^{-0,4}} - 5\cdot10^{-5}T_{\text{бц}} + 0,014$ $\mathbf{d} = P_{\text{гар}}^{-1}$	$T_{\text{бц}}$ – аналогично условиям тотальных КА
3. КА или скрытное воздействие мощным ЭМИ применительно к подсистеме управления	$\mathbf{a} = 1 + 0,64e^{0,0366T_{\text{бц}}}T_{\text{упр}}^{-1,2313e^{0,0022T_{\text{бц}}}} + 0,0626e^{0,0357T_{\text{бц}}}T_{\text{упр}}^{-0,782e^{0,0044T_{\text{бц}}}}$ $\mathbf{b} = 1,283 + 0,2358T_{\text{упр}}^{-0,842}T_{\text{бц}} - 0,0013T_{\text{упр}} - 0,018\ln T_{\text{упр}}$ $\mathbf{c} = 1,39 + \left(0,0386\ln T_{\text{бц}} + 0,059\right)\ln T_{\text{упр}} - 0,4093\ln T_{\text{бц}} + 0,0175e^{-0,003T_{\text{бц}}}$ $\mathbf{d} = 1$	$T_{\text{бц}}$ не включает $T_{\text{св}}$
4. КА или скрытное воздействие мощным ЭМИ применительно к подсистеме разведки / огневого поражения	$\mathbf{a} = 1 + 0,045T_{\text{бц}}^{-0,228}T_{\text{р}}^{k}$, где $k = 0,24 - 10^{-6}T_{\text{бц}}^2 + 5\cdot10^{-4}T_{\text{бц}}$ $\mathbf{b} = 0,555 + \left(0,0744 - 2\cdot10^{-4}T_{\text{р}}\right)\ln T_{\text{бц}} - 5,59T_{\text{р}}^{-0,665}\mathbb{N}^{-8,98T_{\text{р}}^{-0,628}}$ $\mathbf{c} = 0,7784 + \left(0,012 - 0,0274\ln T_{\text{р}}\right)\ln T_{\text{бц}} + 0,2176\ln T_{\text{р}} + 2\mathbb{N}^{-1,66}$ $\mathbf{d} = 1$	$T_{\text{бц}}$ не включает $T_{\text{р}}$.

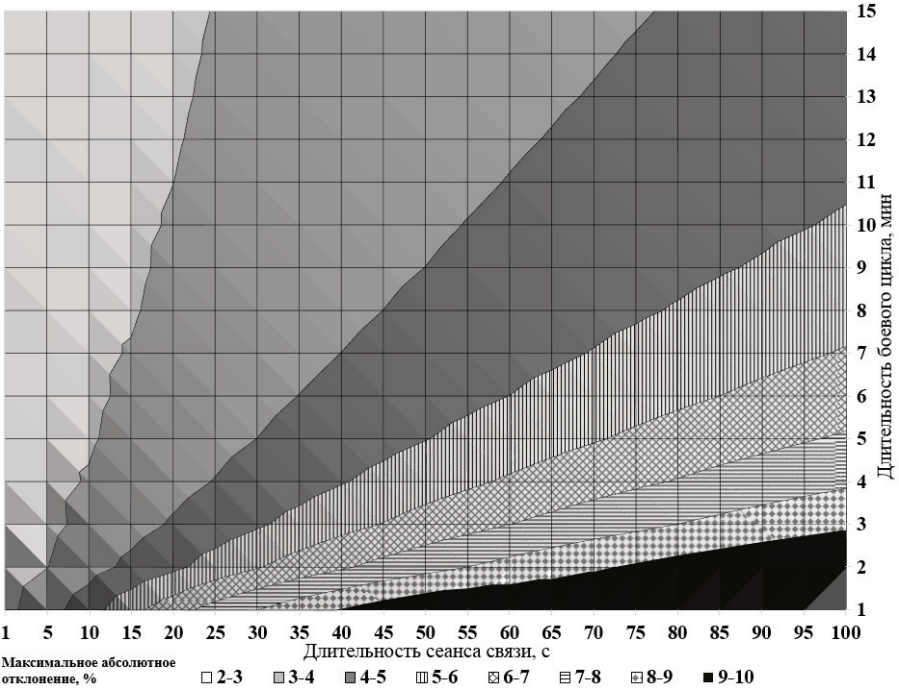


Рис. 74. Диаграмма максимальных абсолютных отклонений для тотальных кибератак или скрытного воздействия мощным электромагнитным излучением

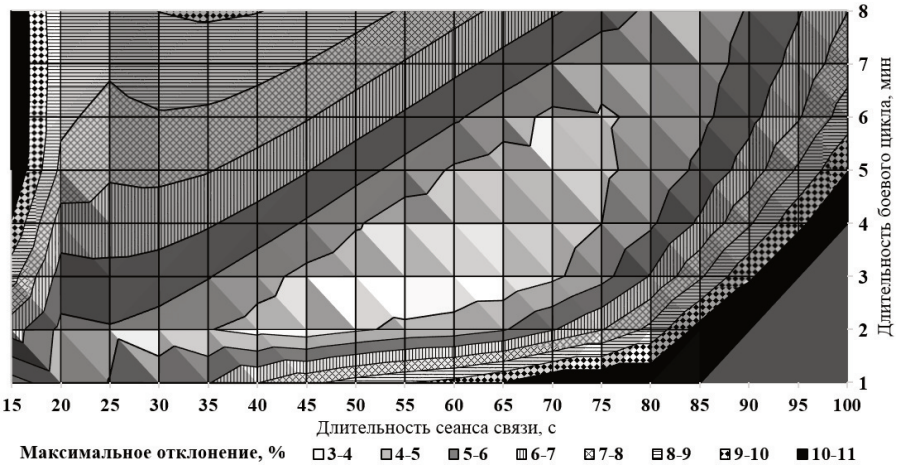


Рис. 75. Диаграмма максимальных абсолютных отклонений для кибератак, скрытного воздействия мощным электромагнитным излучением или радиоэлектронного подавления применительно к подсистеме связи

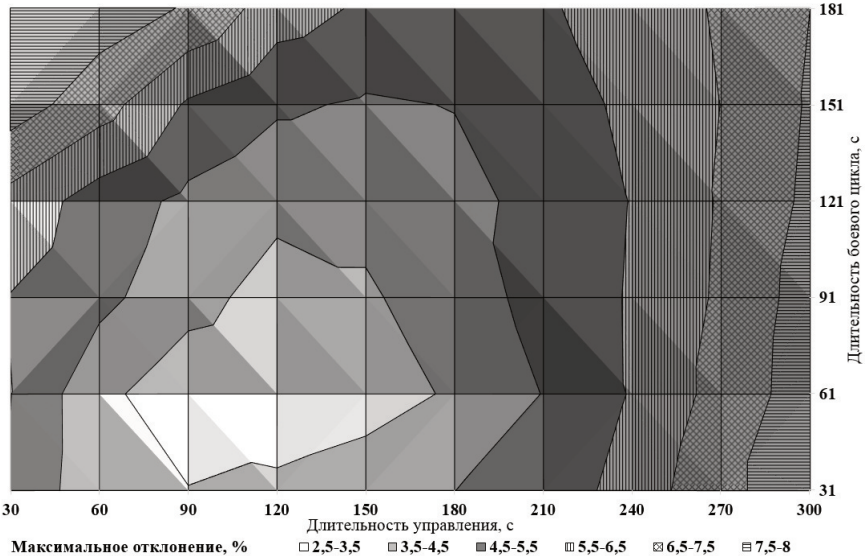


Рис. 76. Диаграмма максимальных абсолютных отклонений для кибератак или скрытного воздействия мощным электромагнитным излучением на подсистему управления при стрельбе с закрытых огневых позиций с применением обычных средств огневого поражения ($P_{оп} = 0{,}1 \ldots 0{,}6$)

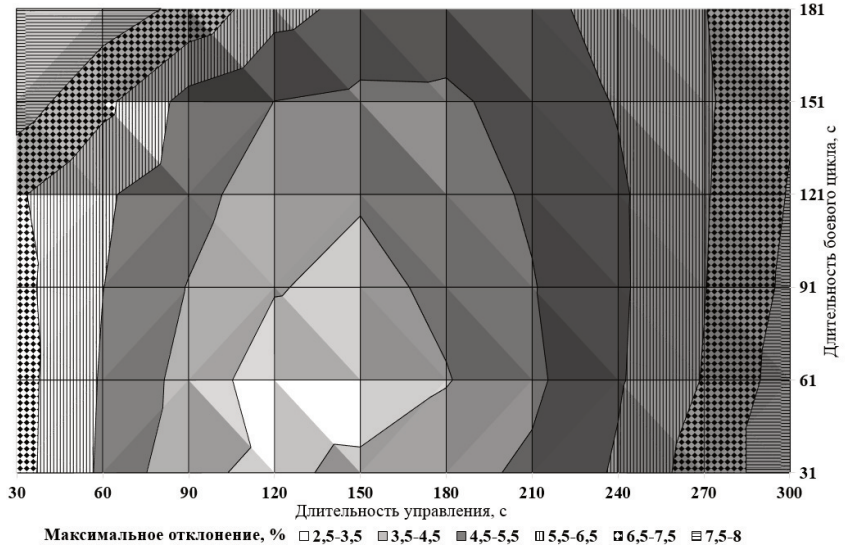


Рис. 77. Диаграмма максимальных абсолютных отклонений для кибератак или скрытного воздействия мощным электромагнитным излучением на подсистему управления при стрельбе прямой наводкой и с закрытых огневых позиций с применением высокоточных средств огневого поражения ($P_{оп} = 0{,}6 \ldots 0{,}9$)

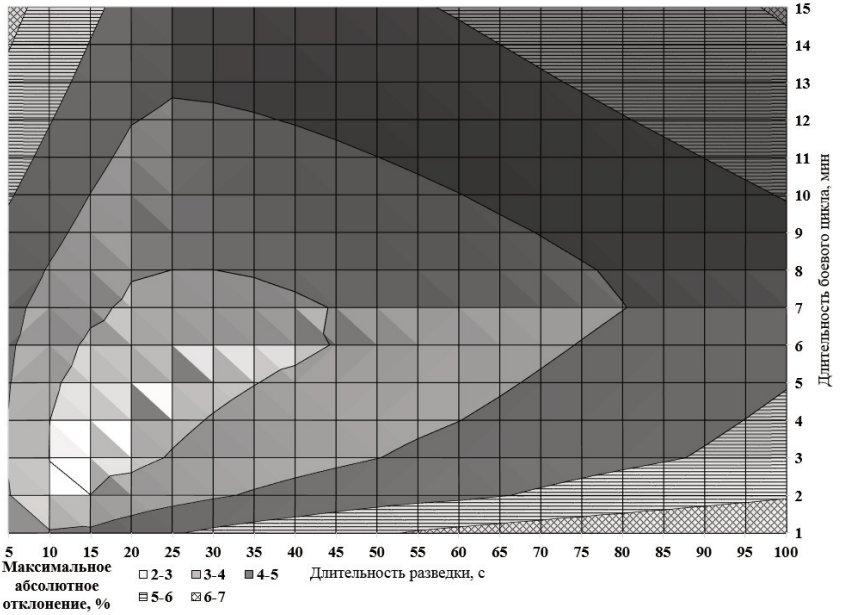


Рис. 78. Диаграмма максимальных абсолютных отклонений для кибератак или скрытного воздействия мощным электромагнитным излучением на подсистему разведки или огневого поражения

Максимальные абсолютные отклонения значений, вычисленных с применением предложенных формул, от результатов моделирования для указанных на рис. 74-78 актуальных диапазонов вероятностных и временных характеристик функционирования подсистем разведки, управления, связи и ОП ВФ составляют 2…5 % [29].

4.4 Результаты моделирования боя

4.4.1 Исходные данные для моделирования

Основным фактором высокой эффективности КА, как отмечено в п. 1.1.1, является наличие информации об уязвимостях ПО АС. Такая информация является весьма ценной и потому тщательно скрывается. Особенностью уязвимостей ПО АС ВН является то, что они имеют сравнительно короткий период актуальности. Поэтому демонстрировать применение предлагаемого в монографии научно-методического аппарата в части разработки способов реализации КА возможно для уже выявленных и, несомненно, устраненных уязвимостей ПО, информация о которых получена из открытых источников.

К числу отечественных элементов АС, применяемых в боевых циклах ВФ, можно отнести, например, следующие образцы SDR-радиоаппаратуры:

- УКВ-радиосвязи Р-187-П1 «Азарт», в том числе применяющие телекоммуникационные протоколы международного стандарта TETRA

(англ. *TErrestrial Trunked RAdio* – наземное транковое радио) [228]. Этот стандарт согласно [290] также является совместимым с базовыми военными стандартами HAVE QUICK II ВС США и SATURN ВС стран НАТО в Евросоюзе (например, AN/PRC-150 [226], AN/PRC-117 [225] в ВС США, M3TR в ВС Германии [317]). Особенностью таких SDR-радиостанций является подключение в бою к единой информационно-управляющей сети для обмена данными и получения сетецентрического доступа к развединформации. Упрощенной версией стандарта TETRA является стандарт DMR, в котором отсутствует ряд дорогостоящих функций и на физическом уровне ЭМВОС во временном слоте стандарта DMR используется два канала (слота) обслуживания абонентов, а во временном слоте стандарта TETRA используется четыре канала. Поэтому недорогие радиостанции стандарта DMR, имеющие высокую помехоустойчивость, сегодня могут широко применяться во всем мире не только государственными и коммерческими службами безопасности и экстренными службами, но и незаконными вооруженными формированиями. Уязвимости TETRA, характерные и для DMR, исследованы в [207, 209, 210];

- УКВ-радиосвязи ЕСУ ТЗ Р-168-МР [227], применяющие телекоммуникационные протоколы международного стандарта IEEE 802.11 Wi-Fi. Уязвимости этого стандарта, не зависящие от использования режима засекречивания передаваемых данных, исследованы, например, в [212];
- внутренней связи ЕСУ ТЗ [64] и переносного комплекта военнослужащих Р-175 [80], применяющие уязвимые телекоммуникационные протоколы международного стандарта IEEE 802.11 Wi-Fi. В США стандарт Wi-Fi используется в персональных модулях из состава АС FBCB2 (США), которыми оснащается каждый солдат [242].

Из описания указанных образцов SDR-радиоаппаратуры следует, что одни и те же международные стандарты цифровой радиосвязи применяются и в ВС РФ, и в ВС НАТО. Это подтверждает известный факт, что с конца XX века во всем мире при разработке военной продукции стала применяться концепция COTS-технологий (от англ. *Commercial Off-The-Shelf* – «коммерческое с полки» [285]), в результате чего наиболее качественные коммерческие технологии стали активно применяться в военной сфере, получив название технологий двойного назначения. К числу таких технологий, кстати, относятся и технологии разработки элементов СЦР и СВТ, проблема импортозамещения которых в РФ пока в полном объеме не решена.

Рассмотрим виды боя перспективных ВФ, в которых КА могут быть подвержены все или некоторые подсистемы при варьируемом уровне их информатизации. Приводимые результаты получены для эталонной модели боя с исходными данными, предполагающими неизменность во времени местоположения и интенсивности воздействий сторон и позволяющими представить бой в виде одного боевого эпизода.

Сначала рассмотрим бой, в котором участвуют два одинаковых ВФ – Красные и Синие. Тип ВФ – самоходный артиллерийский дивизион. Состав сторон включает подсистемы разведки, связи, управления и ОП. Начинающим бой Синим дополнительно придана подсистема ИТВ, включающая наземное средство ИТВ. Подсистемы разведки, управления, связи и ИТВ являются скрытными, средства ОП сторон поражают друг друга, а средства ОП Красных дополнительно могут поражать подсистему ИТВ Синих, если она осуществляет РЭП. То есть при применении Синими РЭП Красные обнаруживают местоположение источника помех своей подсистемой разведки и в связи с высокой заметностью средств РЭП применяют средства ОП в одном из режимов: с приоритетом «ОП≻РЭП» или «РЭП≻ОП». Средства в бою не восстанавливаются. «По умолчанию» управление не сетецентрическое. После уничтожения средства ОП огонь автоматически переводится на еще не уничтоженные средства ОП противника. Обобщенная структурная схема боя показана ранее в параграфе 4.3 на рис. 69. Исходные значения параметров боя приведены в таблице 7.

Таблица 7 — Параметры моделируемого боя

Обозначение	Физический смысл	Значение
U	ослабление ущерба обороняемым позициям	1
$P_{гар}$	требуемая вероятность гарантированного ОП цели	0,94
Δ	уровень информатизации Красных	0…1
$N_{кр}$, $N_{син}$	количество средств ОП Красных и Синих	18
$P_{1бп\_кр}$, $P_{1бп\_син}$	вероятность поражения цели одним боеприпасом средства ОП	0,3
$T_{оп\_кр}$, $T_{оп\_син}$	время подготовки подсистемы ОП Красных и Синих	30 с
$T_{1бп\_кр}$, $T_{1бп\_син}$	время воздействия одним боеприпасом в подсистеме ОП	8 с
$K_{бп\_кр}$, $K_{бп\_син}$	количество боеприпасов в боекомплекте одного средства ОП	∞
$N_{им\_кр}$, $N_{им\_син}$	количество имитируемых средств ОП Красных и Синих	0
$T_{р\_кр}$, $T_{р\_син}$	время работы подсистемы разведки Красных и Синих	30 с
$P_{р\_кр}$, $P_{р\_син}$	вероятность вскрытия и распознавания цели подсистемой разведки	0,99
$T_{упр\_кр}$, $T_{упр\_син}$	время работы подсистемы управления Красных и Синих	20 с
$T_{св\_кр}$, $T_{св\_син}$	время передачи информации по каналу связи Красных и Синих	30 с
$P_{св\_кр}$, $P_{св\_син}$	вероятность гарантированной передачи информации по каналу связи	0,9
$P_{ИТВ}$	вероятность реализации ИТВ Синими	0,01…0,99
Примечания: 1. СКО для времен равно 10 % от математического ожидания. 2. Дублирование подсистем отсутствует.		

В рассматриваемом бою, по мнению органа управления Синих, техника ИТВ должна обеспечить увеличение БП, достаточное для победы. То есть, зная

заранее уязвимости образцов вооружения Красных, орган управления Синих полагает, что его техника ИТВ способна увеличить остаточную долю численности Синих до такого уровня, который достигается при исходном соотношении 1,5:1 (критерий для успешного наступления во встречном бою) без применения техники ИТВ. При заданных исходных данных и соотношении $N_{син} : N_{кр} = 27:18$ (без применения техники ИТВ) остаточная доля численности Синих составляет 58 %. Это значит, что ИТВ при $N_{син} = N_{кр} = 18$ должны обеспечить остаточную долю численности Синих, равную 58 %.

Возникает два вопроса:

1) «При каких параметрах Красных орган управления Синих ошибается?»;
2) «Как защитить Красных от КА, чтобы не допустить их поражения?».

Для ответа на эти вопросы рассмотрим различные варианты этого боя.

4.4.2 Результаты моделирования для различных вариантов боя

Вариант боя № 1. Сравнение эффективности КА и РЭП на подсистему связи. Схема этого варианта показана на рис. 79.

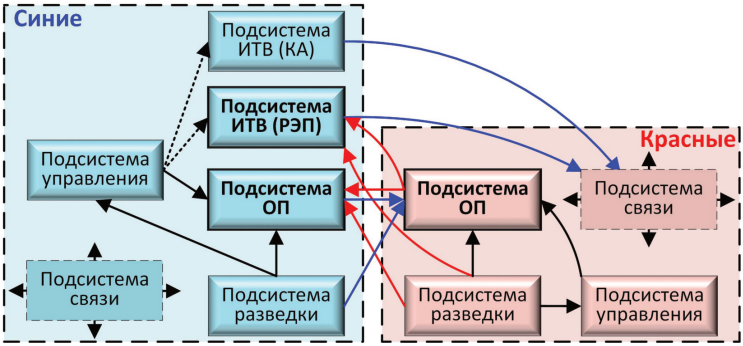


Рис. 79. Схема влияния кибератак и радиоэлектронного подавления применительно к подсистеме связи

Зависимость $\delta N^*_{син}(P_{ИТВ})$ при реализации КА (или в этом варианте боя скрытного РЭП, поскольку оба вида воздействия оказывают влияние только на время связи) для различных значений Δ показана на рис. 80. Примечание: здесь и далее для удобства отображения на графиках БП ВФ соответствует остаточной доле численности победившего ВФ $\delta N^*_{син}$ (см. формулу (46)).

Сравнение эффективности КА (скрытного РЭП) и нескрытного РЭП для рассматриваемого варианта показана на рис. 81 для Δ = 100 % (далее Δ может выражаться процентами). На рис. 81 показан «мнимый парадокс», когда КА или скрытное РЭП оказывается в основном менее эффективно, чем нескрытное РЭП, высокий энергопотенциал электромагнитного излучения которого хорошо заметен для средств разведки Красных. Дело в том, что, сберегая численность средств ОП, в случае применения нескрытного РЭП Синие жертвуют своей

подсистемой ИТВ. Следует отметить, что длительность такого боя составляет около 20 мин, а **время жизни нескрытного средства РЭП в нем около 5 мин** (при $P_{ИТВ} = 0{,}5$ и $\Delta = 100\ \%$), что делает нескрытное РЭП в этом бою нецелесообразным.

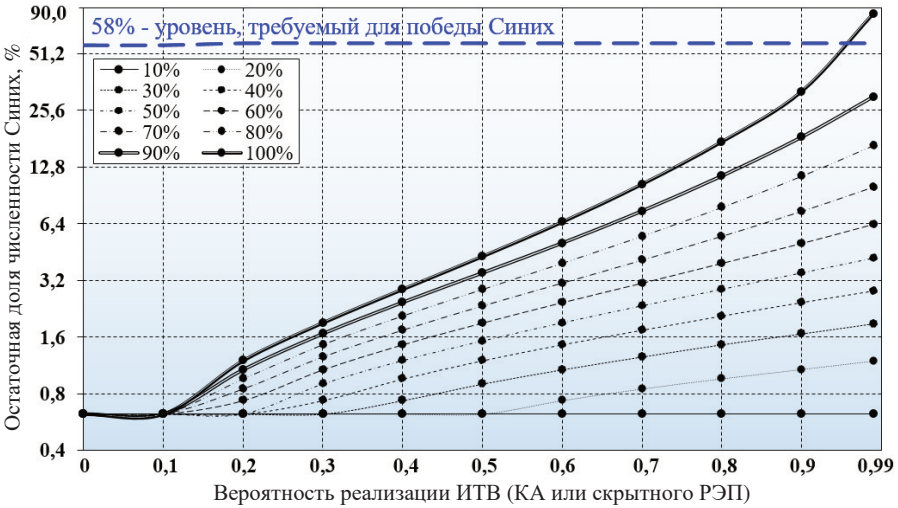


Рис. 80. Эффективность кибератак или скрытного радиоэлектронного подавления применительно к подсистеме связи при различных уровнях информатизации Δ (в логарифмическом масштабе по основанию 2)

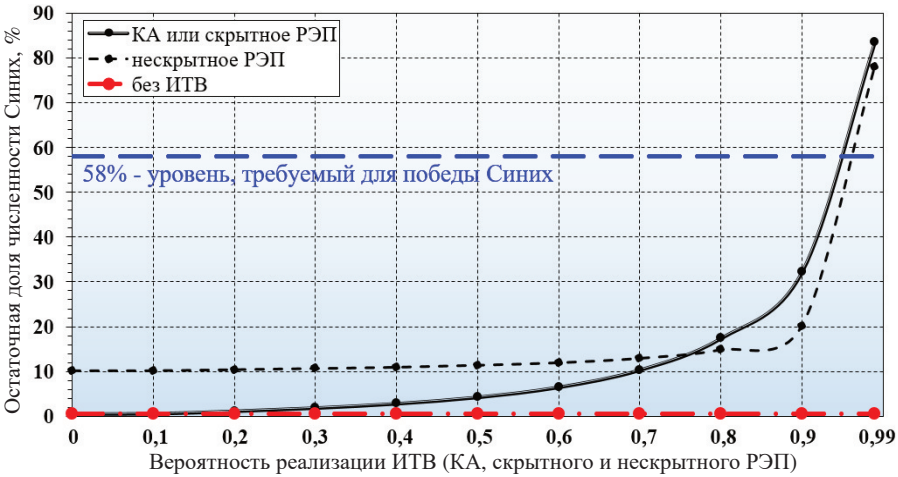


Рис. 81. Сравнение эффективности кибератак, скрытного и нескрытного радиоэлектронного подавления применительно к подсистеме связи

Здесь следует пояснить, что понимается под скрытностью РЭП. Как известно, сам по себе этот вид воздействия не может являться скрытным ввиду необходимости обеспечения определенного превышения сигнала помехи над полезным сигналом на входе радиоприемного тракта цели. Скрытным РЭП в данном контексте является в том случае, если местоположение средства РЭП невозможно, крайне трудно или нецелесообразно определять. Например, когда средство РЭП является целевой нагрузкой БПЛА, низкие параметры заметности которого не позволяют поразить его имеющимися у Красных средствами ОП, либо когда применяются забрасываемые передатчики помех, которые из-за их большого количества и малых габаритов делают применение по ним средств ОП бесполезным. Из-за указанной выше низкой живучести нескрытных средств РЭП в боевых условиях далее рассматривается только скрытное РЭП.

Выводы по варианту боя № 1:

- орган управления Синих ошибается, если уровень информатизации Красных менее 100 %, но даже в таком случае вероятность успешного КА или скрытного РЭП должна составлять более 0,95;
- для недопущения поражения Красных им достаточно либо, не прибегая к устранению уязвимостей, обеспечить свой уровень информатизации менее 90 %, либо использовать хотя бы 5 % неуязвимых средств связи.

В контексте варианта боя № 1 представляют интерес результаты оценки эффективности КА или скрытного РЭП на подсистему связи для различных времен сеанса связи при наиболее часто встречающемся на практике случае, когда $\Delta = 100$ %. Они показаны на рис. 82, где наглядно прослеживается известный из практики факт, что **в бою лучше передавать сообщения по каналам передачи данных, чем использовать голосовые средства радиосвязи, в том числе цифровые**.

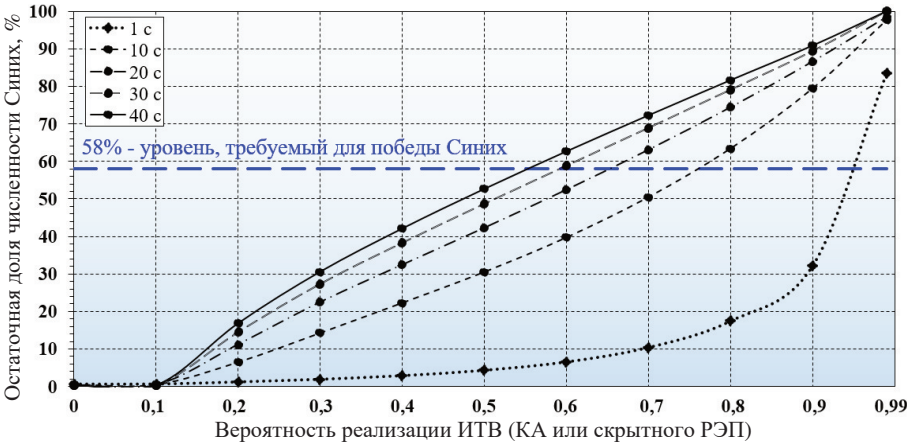


Рис. 82. Эффективность кибератак или скрытного радиоэлектронного подавления применительно к подсистеме связи для различных времен сеанса связи при $\Delta = 100$ %

В данном контексте также представляют интерес результаты оценки КБС подсистем Синих в этом варианте боя (см. рис. 83, сумма КБС для каждой стороны равна 100 %). Из анализа рис. 83 следует, что вес средства ИТВ Синих превышает вес их средства ОП в 3,7 (при $P_{ИТВ} = 0{,}15$) … 10,7 (при $P_{ИТВ} = 0{,}75$) раз. Снижение КБС средства ИТВ после достижения максимума обусловлено тем, что блокирование связи на уровне $P_{ИТВ} = 0{,}75$ приводит к такой задержке боевого цикла Красных, после которой дальнейшее увеличение КБС подсистемы ИТВ Синих сдерживается возрастанием КБС их других подсистем. Тем не менее, это увеличение необходимо для снижения боевых потерь. На рис. 84 показано, как отличаются КБС компонентов Синих при $P_{ИТВ} = 0{,}75$ и $P_{ИТВ} = 0{,}99$.

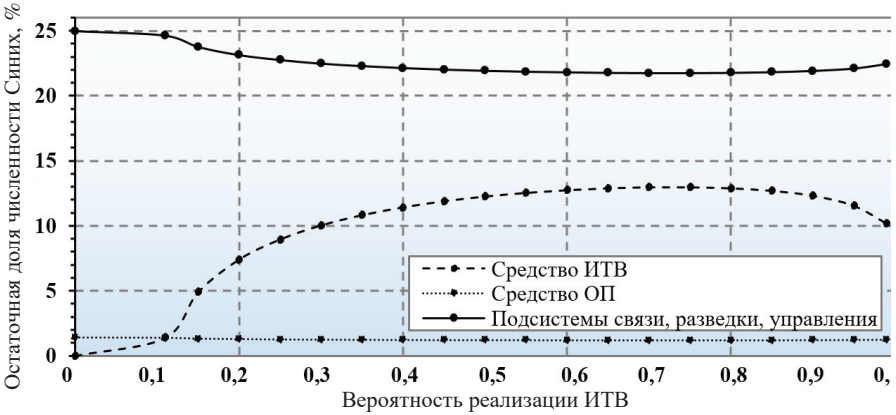


Рис. 83. Коэффициенты боевой соизмеримости компонентов Синих в варианте боя № 1

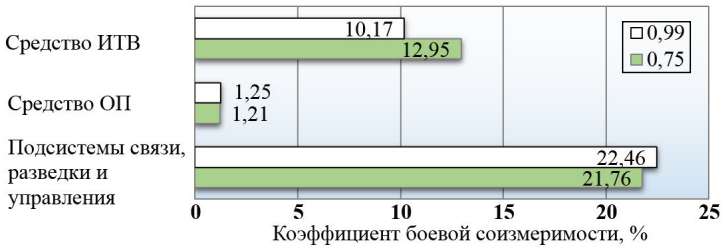


Рис. 84. Коэффициенты боевой соизмеримости компонентов Синих при $P_{ИТВ} = 0{,}75$ и $P_{ИТВ} = 0{,}99$

Вариант боя № 2. Сравнение эффективности КА и скрытного РЭП подсистемы разведки. Схема этого варианта показана на рис. 85.

Эффективность КА и скрытного РЭП для различных уровней информатизации Δ показана на рис. 86 и 87, соответственно. Сравнение

эффективности этих видов ИТВ в данном варианте боя приведено на рис. 88 для Δ = 100 %. На рис. 88 видно, что эффективность КА выше эффективности скрытного РЭП. Это обусловлено тем, что КА влияют на вероятность разведки и на время выполнения задач (операций) в подсистеме разведки, а РЭП – только на вероятность разведки.

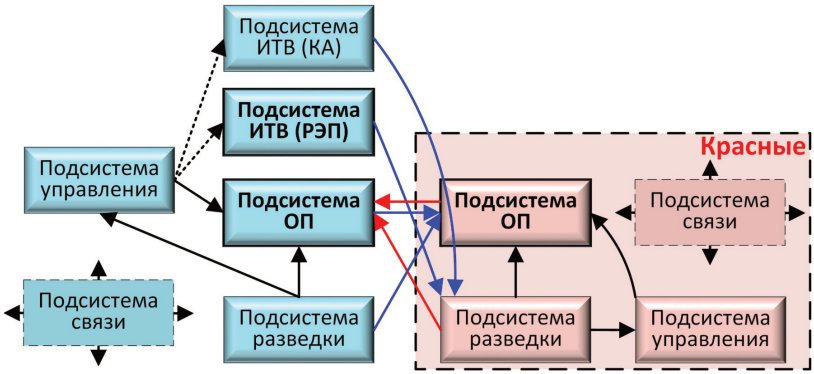


Рис. 85. Схема влияния кибератак и скрытного радиоэлектронного подавления применительно к подсистеме разведки

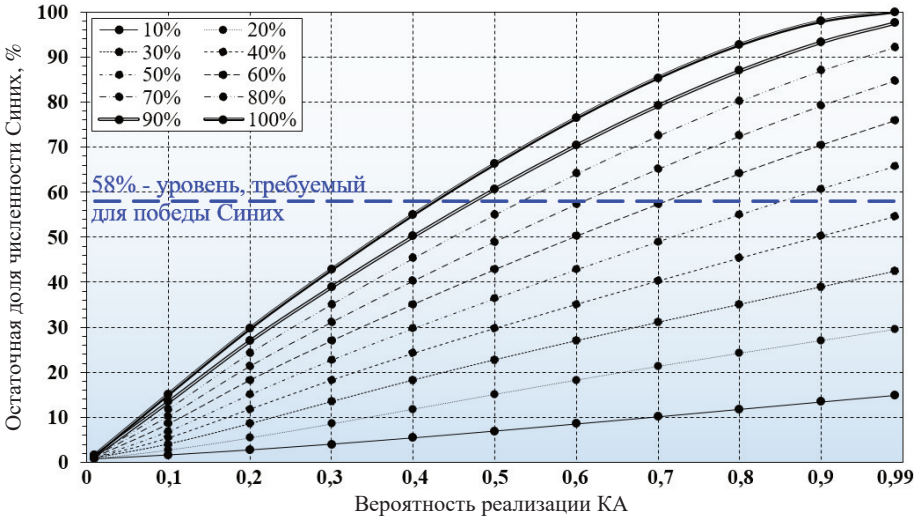


Рис. 86. Эффективность кибератак на подсистему разведки при различных уровнях информатизации Δ

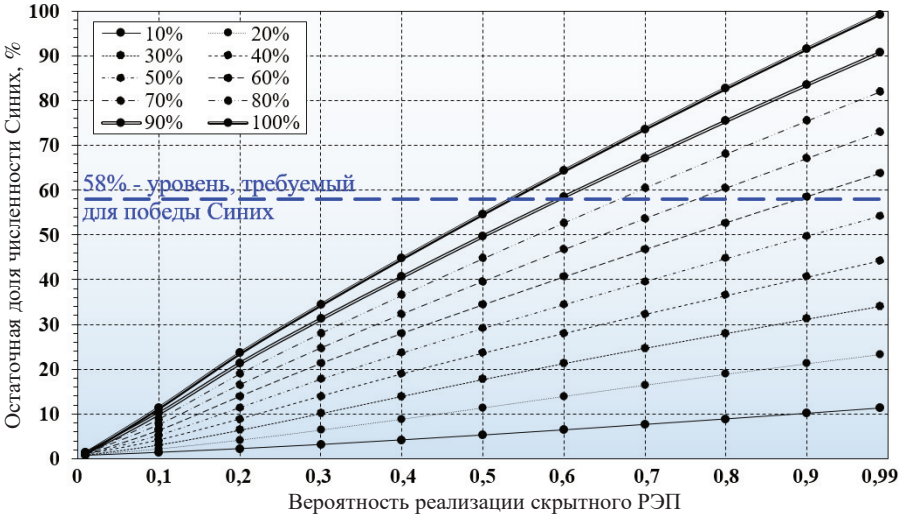


Рис. 87. Эффективность скрытного радиоэлектронного подавления подсистемы разведки при различных уровнях информатизации Δ

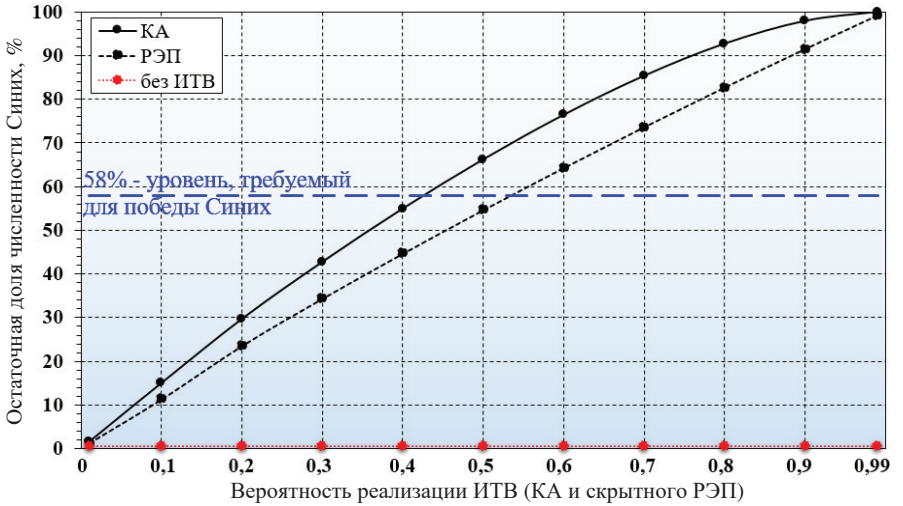


Рис. 88. Эффективность кибератак и скрытного радиоэлектронного подавления применительно к подсистеме разведки при Δ = 100 %

Выводы по варианту боя № 2:

1) орган управления Синих ошибается при выполнении критериев: $P_{ИТВ} < 0{,}42 / \Delta$ – для КА; $P_{ИТВ} < 0{,}53 / \Delta$ – для скрытного РЭП;

2) если уровень информатизации подсистемы разведки Красных более 50 %, то она требует значительных мер для обеспечения защиты от КА.

Вариант боя № 3. Эффективность ИТВ (КА и РЭП) на подсистему ОП. Схема этого варианта показана на рис. 89.

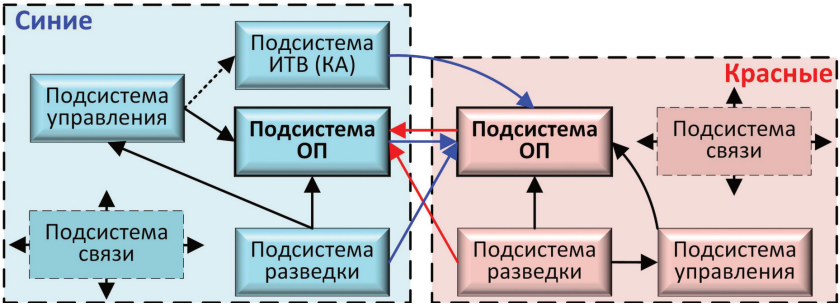


Рис. 89. Схема влияния информационно-технического воздействия на подсистему огневого поражения

Влияние КА и скрытного РЭП на подсистему ОП с позиции математических конструкций аналогично их влиянию на подсистему разведки. Однако на практике РЭП и КА на подсистему ОП отличаются от РЭП и КА на подсистему разведки. Под РЭП на подсистему ОП понимается подавление приемных устройств навигационно-временного обеспечения средств ОП, позволяющих осуществить геопривязку своего местоположения и цели по сигналам радионавигационных систем (в первую очередь, спутниковых), а под КА на подсистему ОП понимается нарушение работы ИТС управления средством ОП. При эффективном нарушении работы средств ОП более некоторого порога (на практике около 10…20 %) Красные по низкой эффективности стрельбы, которую обнаружит их подсистема разведки, поймут, что подверглись ИТВ и перейдут на ручной режим управления. Исключение составляют дистанционно-управляемые роботизированные средства ОП. То есть для нероботизированных средств ОП справедливыми будут только части графиков на рис. 86, 87 в диапазоне вероятности ИТВ от 0 до 0,2. Тем не менее, ввиду того, что в рассматриваемом бою вероятность ОП значительно ниже вероятности разведки, показанная на рис. 90 эффективность КА на подсистему ОП может считаться вполне соответствующей реальному положению дел на практике.

Выводы по варианту боя № 3:

- орган управления Синих ошибается при выполнении критерия $P_{\text{ИТВ}} < 0{,}44 / \Delta$;
- если уровень информатизации для средств разведки Красных более 50 %, то их подсистема ОП требует значительных мер для обеспечения защиты от КА.

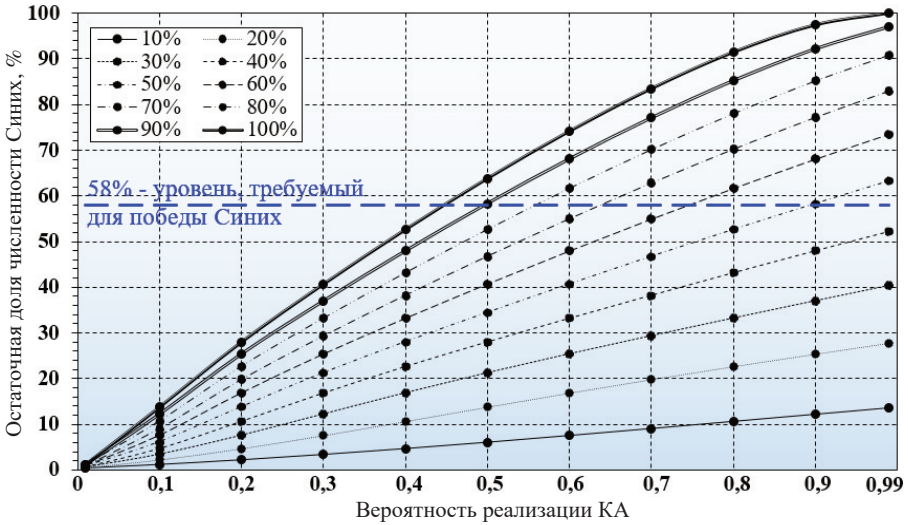


Рис. 90. Эффективность кибератак на подсистему огневого поражения при различных уровнях информатизации Δ

Вариант боя № 4. Эффективность КА на подсистему управления. Схема этого варианта показана на рис. 91. Эффективность КА для различных значений уровня информатизации Δ показана на рис. 92. Очевидно, при наличии сетецентрического доступа средств ОП Красных к развединформации КА на подсистему их управления не являются эффективными.

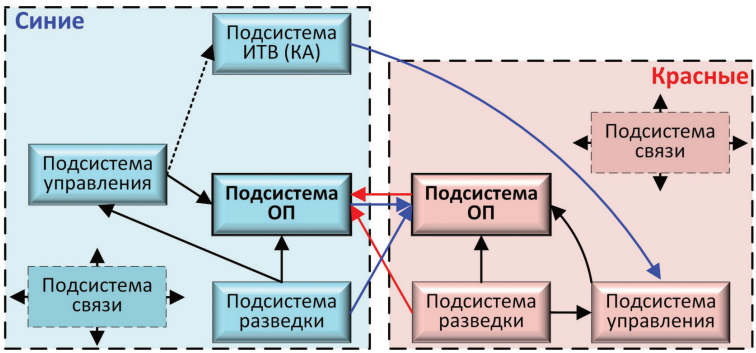


Рис. 91. Схема влияния кибератак на подсистему управления

В этом контексте следует обратить внимание на обоснование целесообразности сетецентрического доступа средств ОП к развединформации. На рис. 93 показаны времена до уничтожения Красных при различных схемах доступа сторон к развединформации без применения КА. На нем видно, что Синие, наступая, тем не менее, терпят поражение при схеме № 2, когда они

сетецентрический доступ не применяют, а Красные применяют. Условия, при которых Синие побеждают при схеме № 2, показаны на рис. 94.

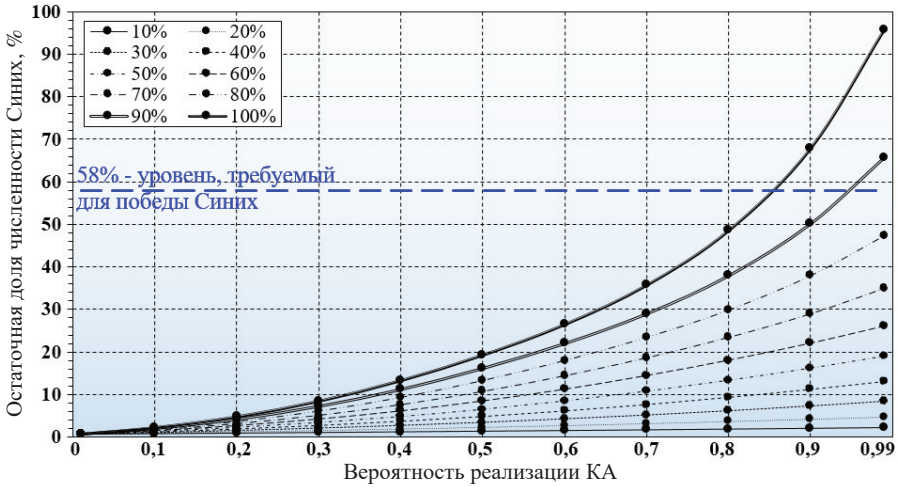
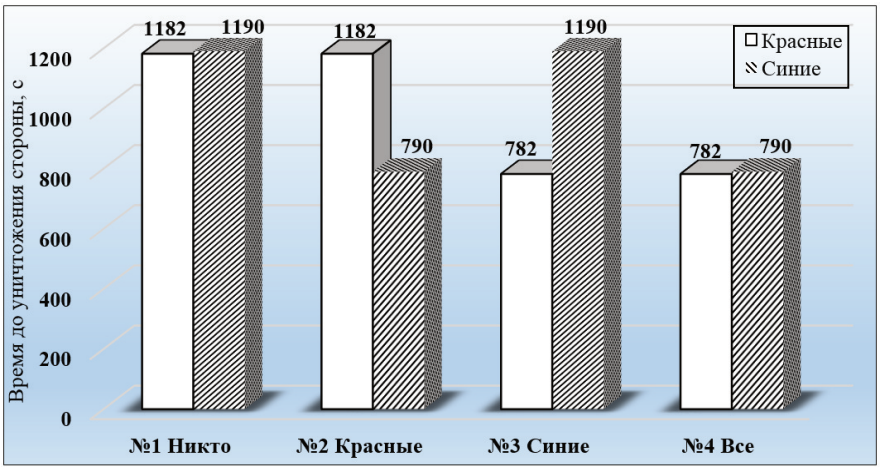


Рис. 92. Эффективность кибератак на подсистему управления при различных уровнях информатизации Δ



Схемы применения сетецентрического доступа к развединформации

Рис. 93. Времена до уничтожения сторон при различных схемах доступа к развединформации без применения кибератак

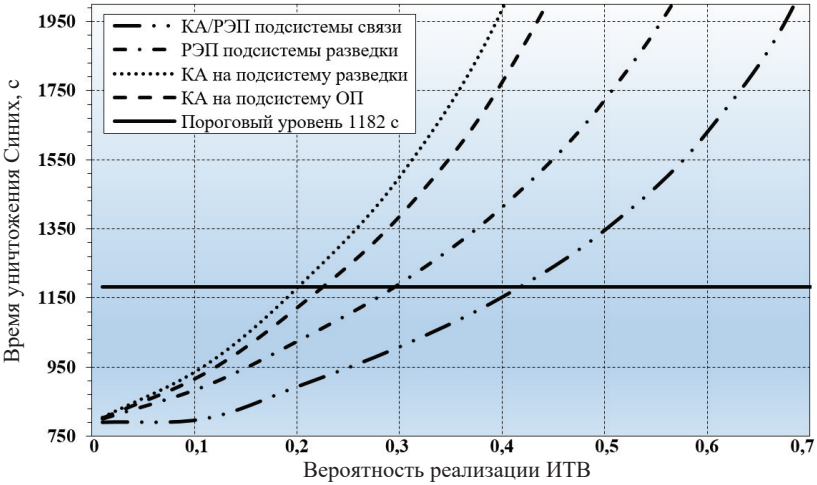


Рис. 94. Времена до уничтожения Красных для различных вариантов информационно-технического воздействия при Δ = 100 %

Выводы по варианту боя № 4:

- орган управления Синих ошибается, если уровень информатизации Красных менее 90 %, но даже в таком случае вероятность успешного КА или скрытного РЭП должна составлять более 0,95;
- для недопущения поражения Красных им достаточно либо, не прибегая к устранению уязвимостей, обеспечить свой уровень информатизации менее 90 %, либо использовать хотя бы 5 % неуязвимых средств связи.

Вариант боя № 5. Эффективность тотального воздействия КА, РЭП и воздействия мощным ЭМИ. Схема варианта показана на рис. 95. Здесь под тотальным воздействием понимается одновременное воздействие на все подсистемы, которые потенциально доступны для соответствующего вида ИТВ.

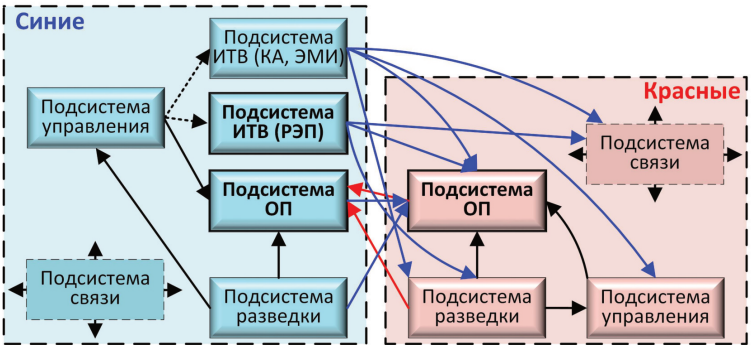


Рис. 95. Схема тотального воздействия кибератаками, радиоэлектронным подавлением и мощным электромагнитным излучением

Эффективность КА и скрытного РЭП для различных значений Δ показана на рис. 96 и 97, соответственно. Сравнение эффективности КА и скрытного РЭП для этого варианта показано на рис. 98 для Δ = 100 %.

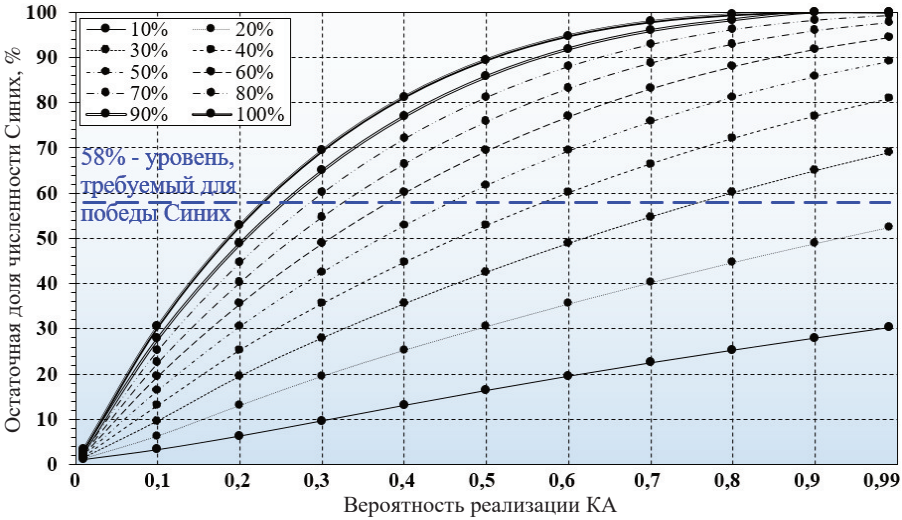


Рис. 96. Эффективность тотального воздействия кибератаками при различных уровнях информатизации Δ

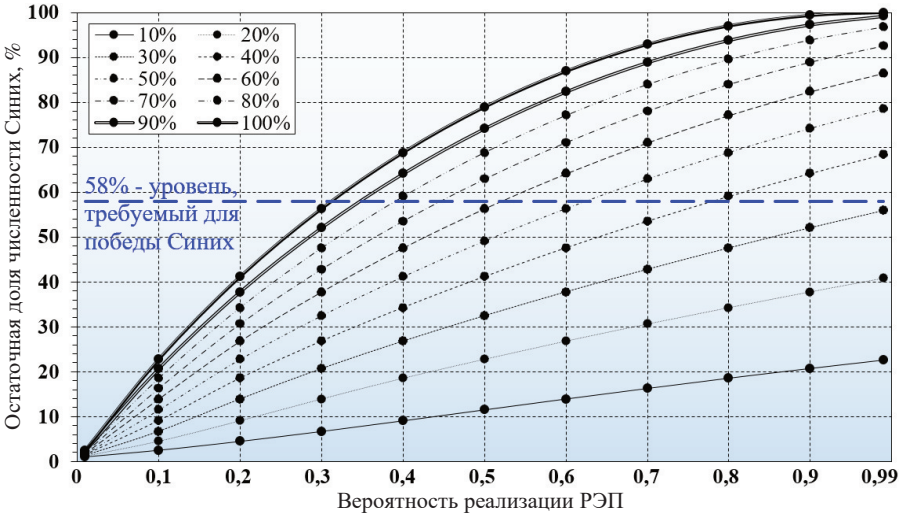


Рис. 97. Эффективность тотального скрытного радиоэлектронного подавления при различных уровнях информатизации Δ

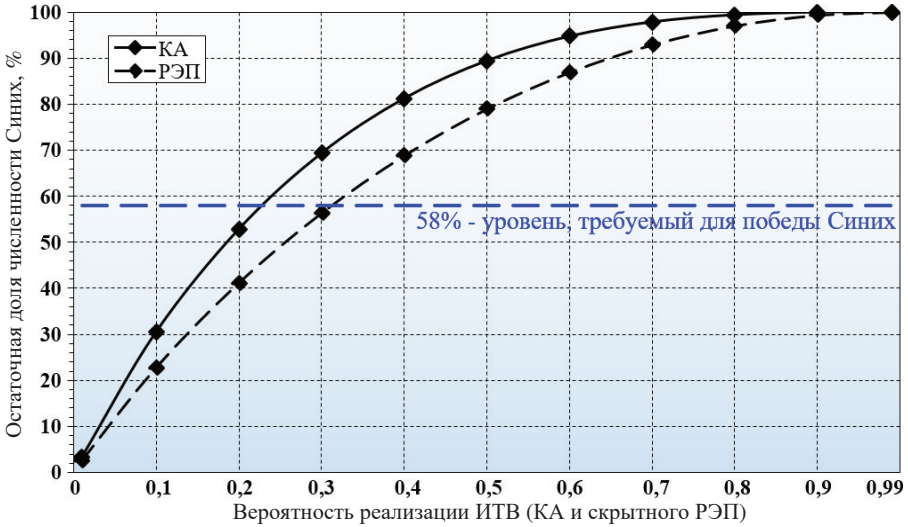


Рис. 98. Эффективность тотальных кибератак и скрытного радиоэлектронного подавления при Δ = 100 %

Выводы по варианту боя № 5:

- орган управления Синих ошибается, если выполняются критерии: $P_{ИТВ} < 0{,}225 / \Delta$ – для КА; $P_{ИТВ} < 0{,}31 / \Delta$ – для скрытного РЭП;
- в интересах недопущения поражения Красных их образцы вооружения требуют значительных мер для обеспечения защиты от ИТВ.

Вариант боя № 6. Эффективность КА, тотального воздействия мощным ЭМИ, имитации боевой обстановки и занятия Красными оборудованных позиций. Схема варианта показана на рис. 99.

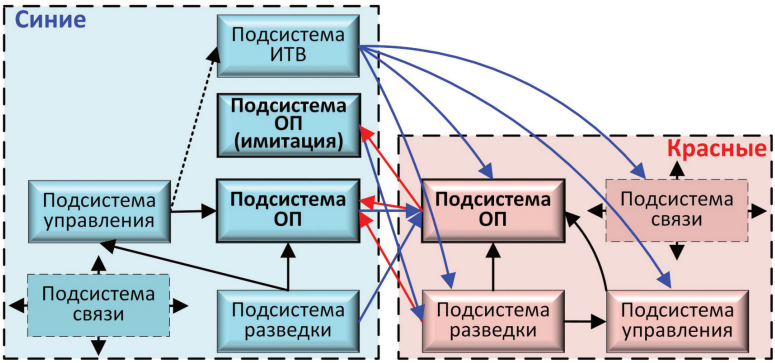


Рис. 99. Схема применения кибератак и имитации боевой обстановки

Под имитацией боевой обстановки здесь понимается применение Синими ложных средств ОП, создаваемых любыми способами (в том числе постановкой активных и пассивных имитирующих помех, развертыванием муляжей), на которые Красные расходуют часть своего боекомплекта и ресурс скорострельности. На рис. 100 показана эффективность КА на различные подсистемы для $\Delta = 100$ %, тотального воздействия мощным ЭМИ для $\Delta = 100$ % и имитации боевой обстановки Синими без дополнительной защиты Красных и с защитой, предполагающей занятие ими обороны на оборудованных позициях.

Выводы по варианту боя № 6:

- орган управления Синих ошибается, если количество имитируемых средств ОП составляет менее 10;
- в интересах недопущения поражения Красных их подсистема разведки должна распознавать не менее 50 % ложных целей;
- при применении Синими средств имитации боевой обстановки или ИТВ Красным следует как можно скорее занять оборону.

Следует отметить, что в ходе исследования установлен общий вид критерия эффективности скрытных ИТВ в боевых условиях

$$P_{\text{ИТВ}} < \frac{\eta}{\Delta}, \tag{80}$$

где η – коэффициент, характеризующий целевую для ИТВ подсистему.

Таким образом, в рассмотренных вариантах применения ИТВ в современном бою вместо КА или РЭП может использоваться воздействие мощным ЭМИ. Если воздействие мощным ЭМИ является скрытным (например, если массогабаритные характеристики средства позволяют поместить его на БПЛА), то его эффективность аналогична таковой для КА. Иначе эффект от применения мощного ЭМИ будет несколько выше эффекта тотального воздействия КА, как показано на рис. 100, но за этот незначительный эффект, наблюдаемый при $\Delta = 0…30$ %, Синим придется пожертвовать средством воздействия мощным ЭМИ.

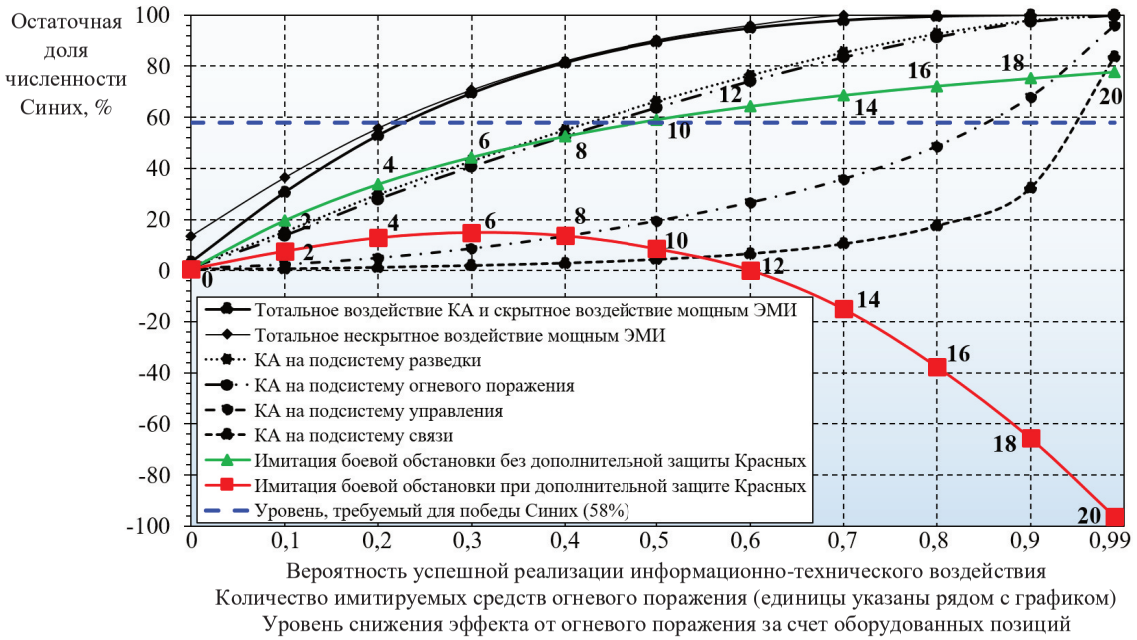


Рис. 100. Сравнение эффективности информационно-технического воздействия и имитации боевой обстановки

Выводы по четвертой главе

В четвертой главе рассмотрена модель процессов функционирования автоматизированных систем в боевом эпизоде, в которой, в отличие от моделей, изложенных в [256, 268, 300, 320, 328], дополнительно учтены оснащение воинских формирований средствами реализации кибератак, состав, функции, параметры и характеристики функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований. Это достигается за счет воспроизведения процессов боевого применения противоборствующих воинских формирований в виде иерархически упорядоченной четырехуровневой полимодельной системы, в которой:

- **на первом уровне** с позиции теории вероятностей воспроизводится функционирование множества элементов боевых порядков, каждый из которых в течение боевого эпизода статично размещается на местности и характеризуется показателем информатизации и боеспособностью, определяемой как произведение его работоспособности, коэффициента боевой соизмеримости, устойчивости к диверсии, вероятности выполнения личным составом неавтоматизированных функций;
- **на втором уровне** в каждом элементе боевого порядка с позиции теории вероятностей воспроизводится функционирование множества информационно-технических средств, которые характеризуются показателями работоспособности, заразности, подверженности дезинформации, разведке и перехвату управления и учитывают распространение специальных программных средств по информационно-управляющим сетям автоматизированных систем, а также воспроизводится функционирование множества устройств, которые характеризуются показателем работоспособности;
- **на третьем уровне** используются стратифицированные модели каждого информационно-технического средства автоматизированных систем;
- **на четвертом уровне** с использованием полумарковских моделей воспроизводятся процессы функционирования информационно-технических средств и устройств, конфликтно обусловленные плотности распределения времен переходов которых определяются на основе воспроизведения взаимного влияния структурных единиц своего воинского формирования и противника по правилу: элемент воздействует на цель, если он назначен на нее, его ресурс и характеристики обеспечивают такую возможность с учетом местоположения, не поражен в момент получения целеуказания, не прерван боевой цикл.

Модель позволяет воспроизвести в виде единой системы комплекс процессов огневого поражения, разведки, связи, управления, имитации обстановки, радиоэлектронного подавления, воздействия мощным электромагнитным излучением и кибератак на информацию в ее источнике, при

передаче и в потребителе в боевых циклах воинских формирований и получить численное значение показателя боевого потенциала воинского формирования в виде суммы взвешенных по коэффициентам боевой соизмеримости аддитивных сверток боеспособностей элементов боевого порядка своего воинского формирования и взвешенных по коэффициентам боевой соизмеримости аддитивных сверток боеспособностей элементов боевого порядка противостоящего воинского формирования, управление которыми перехвачено в результате диверсионно-разведывательной деятельности и применения специальных программных средств с функцией перехвата управления. Роль модели в настоящем исследовании состоит в агрегировании моделей, приведенных в предыдущей главе 3.

Совокупность предложенных в предыдущей и настоящей главах моделей позволяет выявлять закономерности влияния кибератак на процесс взаимного уничтожения элементов боевых порядков противоборствующих воинских формирований в боевом эпизоде. Учет эффектов кибератак удалось формализовать и исследовать в виде процесса динамического многоуровневого антагонистического конфликта. В частности, показано, что в боевых условиях техника реализации кибератак способна обеспечивать существенное преимущество использующему ее воинскому формированию пропорционально уровню информатизации подсистем разведки, связи и управления войсками (силами) и оружием противостоящей стороны.

В целом в предлагаемых моделях процессов функционирования автоматизированных систем воинских формирований учтены все отличительные свойства кибератак. Поражающая способность, транслируемость, авторегенерируемость, транзитивность, телеоперационность и прозрачность учтены в модели процесса распространения специальных программных средств в информационно-управляющей сети, образуемой информационно-техническими средствами автоматизированных систем, и в модели конфликта средства реализации кибератак и подсистемы защиты информации информационно-технического средства. Низкая энергоемкость и высокая избирательность учтены в модели процессов функционирования автоматизированных систем в боевом эпизоде.

В следующей главе рассматриваются вопросы оценки эффективности способов реализации кибератак в условиях боевой обстановки.

5 Метод оценки эффективности кибератак в боевых действиях и методики, реализующие его этапы

«Всякое решение плодит новые проблемы.»
Закон Мерфи

5.1 Основные положения метода оценки эффективности кибератак в боевых действиях

Анализ предметной области приведен в параграфе 1.2, где показано, что на сегодняшний день отсутствуют методы оценки эффективности КА в боевых действиях, которые можно было бы использовать в процессе создания (модернизации) АС, применяемых в боевых циклах ВФ, в интересах обеспечения защищенности этих систем от КА противника. В настоящем параграфе предлагается метод, предназначенный для парирования проблемной ситуации в рассматриваемой предметной области.

Ключевая идея метода состоит в следующем. Предлагается оценивать влияние КА на ход и исход боевых действий на основе определения структуры контуров управления в боевых циклах противоборствующих ВФ, обеспечиваемых подверженными КА АС, и последовательного расчета в каждом боевом эпизоде системы информационных показателей эффективности функционирования ИТС АС, информационно-боевых показателей эффективности боевых циклов и боевого показателя соотношения БП сторон [37]. Содержание метода показано на рис. 101.

Метод отличается от своих методов-прототипов, изложенных в работах [2, 51, 52, 71, 76, 110-112, 117, 141, 142, 148, 178, 250, 251] по оценке эффективности техники ИТВ, учитывающих влияние на ход и исход боя ресурса средств разведки, связи, управления, ОП и радиоэлектронного поражения, тем, что учитывает совокупность боевых циклов ВФ, одновременно обеспечиваемых средствами разведки, управления и связи и подверженных на каждой фазе каждого цикла влиянию совокупности средств ОП, имитации обстановки, РЭП, воздействия мощным ЭМИ и реализации КА. Это достигается за счет формирования графа позиционной динамики ЭБП на основе безызбыточной комбинации траекторно-временных матриц сценариев боя и оценки в каждом боевом эпизоде, формализуемом вершиной этого графа, информационных показателей эффективности функционирования ИТС АС, применяемых в боевых циклах ВФ, информационно-боевых показателей эффективности боевых циклов и боевого показателя соотношения боевых потенциалов противоборствующих сторон.

Рассматриваемый метод позволяет оценивать ущерб, наносимый с применением разработанных и ранее известных способов реализации КА на БП ВФ в ходе боевых действий.

Этапы предлагаемого метода реализуются совокупностью взаимосвязанных методик, представленных в следующих параграфах настоящей главы.

Рис. 101. Содержание метода оценки эффективности кибератак в боевых действиях

5.2 Методика разработки графа позиционной динамики элементов боевых порядков воинских формирований

Рассмотренная в главе 4 модель процессов функционирования АС в боевом эпизоде согласно классификации, приведенной в [180], относится к классу операционных структурно-функциональных моделей. Она учитывает боевые циклы сторон с детализацией до солдата, устройства и ИТС. Эта модель в рамках рассматриваемого в монографии научно-методического аппарата является элементом модели современного боя, который представляется в виде «дерева» [30, 32], показанного на рис. 61. Граф представляет собой совокупность различных альтернативных последовательностей боевых эпизодов. Каждая последовательность боевых эпизодов формируется на основе задаваемых или автоматически генерируемых альтернативных разноранговых траекторий движения ЭБП сторон, которые имеют остановки с разной продолжительностью и различную скорость на различных участках пути.

Анализ предметной области. Тематика группового управления подвижными объектами активно рассматривается с середины прошлого века в рамках исследования операций. Сегодня зарубежные (например, [307, 316, 319]) и отечественные (например, [22, 193, 201, 274, 305]) работы в области исследования проблем группового управления подвижными объектами ориентированы на синтез множества синхронизированных во времени и пространстве процессов в сложных организационно-технических системах и, в первую очередь, на синтез оптимальных траекторий движения для групп автономных роботов. Ряд работ (например, [305, 319]) посвящен исследованию процессов боевого применения сил и средств в рамках концепции сетецентрических войн. Но вопросам анализа траекторий, параметры которых известны и которые являются асинхронными в силу своей природы, с целью их последующей синхронизации в рамках единого суперпроцесса, как того требует древовидное представление боя, в известных работах внимание не уделялось.

При разработке «дерева» боя требуется учет следующих исходных данных.

1. Λ – пространство боя, которое образуется множеством кубических элементарных объемов со стороной, равной ζ (далее по тексту эти элементарные объемы будут называться *элемобами*). То есть $\Lambda = \{\lambda_{x,y,z}\}$: $x = 1\ldots N_x$, $y = 1\ldots N_y$, $z = 1\ldots N_z$. Размеры пространства боя равны $N_x\zeta \times N_y\zeta \times N_z\zeta$.

2. $\Gamma=\{\gamma_f\}$ – множество типов элемобов. Например, γ_1 = «шоссе», γ_2 = «грунтовая дорога», γ_3 = «пересеченная местность», γ_4 = «труднопроходимая местность, преодолеваемая только человеком», γ_5 = «непреодолеваемое заграждение», γ_6 = «воздух», γ_7 = «вода».

3. $C^{\text{А}}$ и $C^{\text{Б}}$ – множество ЭБП противоборствующих ВФ А и Б, соответственно (или отдельных ВФ, которые приравниваются к ЭБП). $C = C^{\text{А}} \cup C^{\text{Б}}$; $C=\{c_i\}$: $i = 1\ldots|C|$. Здесь и далее знаком $|\ldots|$ обозначается мощность множества, то есть количество его элементов. ЭБП – это кортеж вида

$$c_i = < a_i, < v_i(\gamma) >>, \tag{81}$$

где a_i – тип i-го ЭБП (например, человек, сухопутное средство, морское средство, воздушное средство, стационарный объект);

$v_i(\gamma)$ – скорость i-го ЭБП при движении по элемобу γ-го типа.

4. τ – шаг дискретизации времени боя.

5. $S = \{s_i\}$ – множество траекторий движения ЭБП, задаваемых или генерируемых с использованием известных методов, изложенных, например, в работе [305]. Совокупность траекторий движения i-го ЭБП – это кортеж вида

$$s_i = < O_i, < R_{i,m}, H_{i,m}, W_{i,m} > > : m = 1 \ldots M_i, \quad (82)$$

где $O_i = \{o_{i,k}\} \subset \Lambda$: $o_{i,k} = \lambda_{x,y,z}$, $k = 1 \ldots |O_i|$ – множество попарно смежных через грани или ребра элемобов, которые занимает i-й ЭБП. Множество O_i в процессе боя не меняется;

$R_{i,m} = <r_{i,m,q}>$: $r_{i,m,q} = \lambda_{x,y,z}$, $q = 1 \ldots Q_{i,m}$ – кортеж последовательно расположенных и попарно смежных через грани или ребра элемобов, через которые проходит m-я траектория движения i-го ЭБП; $Q_{i,m}$ – количество элемобов, через которые перемещается i-й ЭБП на m-й траектории движения;

M_i – количество альтернативных траекторий движения i-го ЭБП;

$W_{i,m}$ – ранг важности m-й траектории движения i-го ЭБП на единой для всех ЭБП θ-бальной шкале ($\theta \in Z^+$). Ранг наиболее предпочтительной траектории движения равен θ, а ранги остальных траекторий с ней сравниваются;

$H_{i,m} = \{h_{i,m,j}\}$: $j = 1 \ldots |H_{i,m}|$, $H_{i,m} \subset R_{i,m}$ – множество точек действия на m-й траектории движения i-го ЭБП. Точка действия – это кортеж вида

$$h_{i,m,j} = < \lambda_{x,y,z}, T_{i,m,j} >, \quad (83)$$

где $\lambda_{x,y,z}$ – элемоб, в котором осуществляется какое-либо действие (например, воздействие на противника средствами огневого поражения);

$T_{i,m,j}$ – время нахождения i-го ЭБП в j-й точке действия m-й траектории движения. Для ЭБП, которые не останавливаются в бою, траектория движения может разбиваться на этапы (например, этапы «полет летательного аппарата в заданный район» $\Rightarrow$ «разведка» $\Rightarrow$ «воздействие» $\Rightarrow$ «возвращение»). На границах этапов создаются «виртуальные» точки действия, у которых $T_{i,m,j} = \tau$.

6. $T_{\text{эп}}$ – время расчета одного боевого эпизода.

7. $T_{\text{доп}}$ – максимальное время, отводимое на расчеты.

8. ς – шаг дискретизации параметра масштабирования боя $T_{\text{м}}$.

Параметр масштабирования боя $T_{\text{м}}$ равен целому числу τ и характеризует минимальное время, в течение которого ЭБП считается неподвижным, а интенсивность его работы считается неизменной. Этот параметр не задается, а вычисляется для заданных значений показателей $T_{\text{эп}}$ и $T_{\text{доп}}$.

Постановка задачи: сформировать граф позиционной динамики ЭБП ВФ в бою, представляющий собой множество узлов, соответствующих боевым эпизодам, синхронизированным по времени движения отдельных ЭБП противоборствующих ВФ на поле боя, и множество взвешенных по вероятностям реализаций боевых эпизодов дуг между узлами, соответствующих причинно-следственным связям боевых эпизодов, для такого наибольшего количества боевых эпизодов, суммарное время проведения расчетов которых не больше заданного, при фиксированных шаге дискретизации времени боя, шаге дискретизации параметра масштабирования боя и времени расчета одного боевого эпизода.

Методика решения задачи состоит из следующих этапов [40] (см. рис. 102).

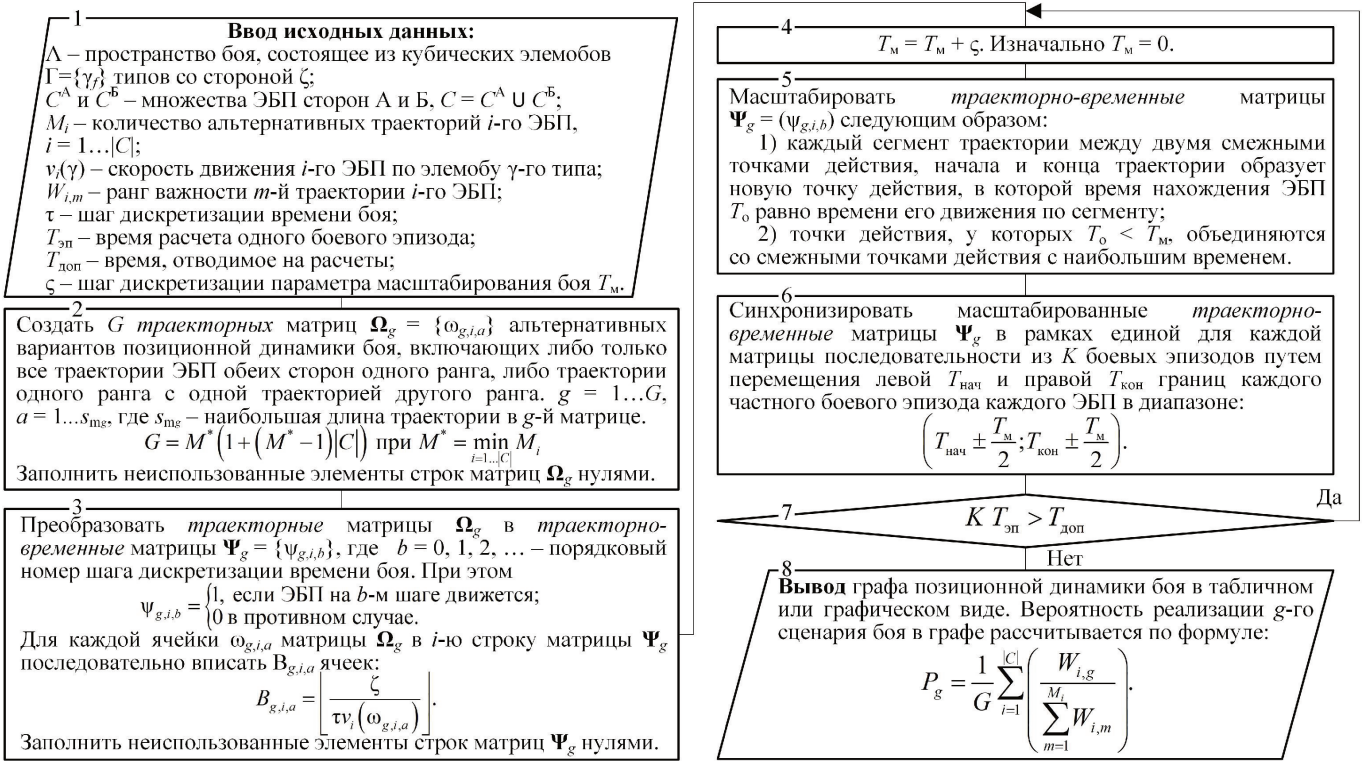


Рис. 102. Блок-схема формирования графа позиционной динамики элементов боевых порядков воинских формирований

На **этапе 1** проводится ввод исходных данных.

На **этапе 2** проводится создание G *траекторных* матриц $\mathbf{\Omega}_g = \{\omega_{g,i,a}\}$ альтернативных вариантов позиционной динамики боя, где i – порядковый номер ЭБП, $g = 1\ldots G$, $i = 1\ldots|C|$, $a = 1\ldots s_{m_g}$, s_{m_g} – наибольшая из всех заданных длин траекторий пути ЭБП противоборствующих ВФ в g-й матрице. Каждая *траекторная* матрица содержит траектории движения всех ЭБП противоборствующих сторон. Каждая траектория имеет заданный ранг.

В реальных боевых условиях множество C может включать до тысяч ЭБП. Даже для боя двух мотострелковых рот с 10 ЭБП (по числу бронетехники) в каждой при количестве альтернативных траекторий для одного ЭБП $M = 3$ количество траекторных матриц при использовании подхода полного перебора составляет $G = 3^{20} \approx 3{,}5 \cdot 10^9$. Поэтому полный перебор всех сочетаний траекторий движения ЭБП реализовать крайне сложно. Разрешить данную ситуацию позволяет задание приоритетов этих траекторий.

Это дает возможность группировать траектории по приоритету и рассматривать каждую группу как множество траекторий с одинаковым приоритетом. Будем называть такие группы базовыми. Количество базовых групп равно наименьшему количеству заданных альтернативных траекторий. Например, если, количество заданных альтернативных траекторий для всех ЭБП сторон от 2 до 3, то базовых групп две, а если от 1 до 10, то базовая группа одна. Альтернативные траектории с одинаковыми рангами к базовым группам относят произвольно. Например, пусть трем траекториям движения одного из ЭБП присвоены ранги 10, 8 и 8. Тогда при трех базовых группах одну из двух траекторий с рангом 8 произвольно относят ко второй группе, а другую к третьей. При двух базовых группах в этом примере только одну из двух траекторий с рангом 8, выбранную произвольно, относят ко второй группе, а третья траектория в базовые группы не попадает.

Каждая полученная таким образом базовая группа не учитывает траектории движения ЭБП в остальных базовых группах и траектории, не попавшие ни в одну базовую группу. Для учета этого аспекта для каждой базовой группы создаются ее дубликаты таким образом, что в каждой такой группе одна и только одна траектория движения некоторого ЭБП заменяется на другую альтернативную траекторию этого элемента. Получившееся множество групп обеспечивает *квазиполный перебор* всех возможных вариантов траекторий движения ЭБП в бою. Такой подход используется в NASA при тестировании авионики [294]. Он парирует проблему взрыва пространства тестируемых состояний сложных критически важных систем и, в отличие от весьма ресурсоемкого подхода *полного перебора* сочетаний всех вариантов наборов тестируемых переменных, предполагает создание только таких наборов, в которых правильными являются либо все переменные, либо все, кроме одной переменной. Данный подход не позволяет исследовать все возможные варианты поведения системы. Для сложных систем это практически невозможно. Тем не менее, он дает возможность в условиях ресурсных ограничений максимально приблизиться к этой цели, оставляя без внимания

редкие для практики случаи. Поэтому в методике полагается, что правильные тестируемые переменные в подходе, изложенном в [294], – это базовые группы траекторий движения ЭБП с одинаковым уровнем важности, а неправильные переменные – это все остальные траектории с другими рангами. Такая интерпретация, в частности, позволяет наглядно показать несостоятельность подхода, учитывающего только базовые группы, то есть, когда $G = M$. При тестировании состояний сложных систем это означало бы, что проверка проводится только с правильными исходными данными, а ошибочным данным внимание не уделяется.

Для создания *траекторных* матриц $\mathbf{\Omega}_g$ используют следующие правила.

Правило 1Т. Создается M^* *траекторных* матриц сценариев боя $\mathbf{\Omega}_g$, каждая из которых соответствует базовой группе траекторий. При этом M^* равно наименьшему заданному количеству альтернативных траекторий движения среди всех ЭБП, участвующих в бою. То есть $M^* = \min M_i \big|_{i=1\ldots|C|}$.

Траекторные матрицы $\mathbf{\Omega}_g$ определяются следующим образом:

$$\mathbf{\Omega}_g = \{\omega_{g,i,a}\}: \omega_{g,i,a} = r_{i,\,g,a},\ g = 1\ldots M^*. \tag{84}$$

Неиспользованные части строк матрицы $\mathbf{\Omega}_g$ заполняются нулями.

Правило 2Т. Для каждой матрицы, созданной по правилу 1Т, формируется множество ее дубликатов (новых матриц), в каждом из которых одна траектория движения каждого ЭБП заменяется на другую его траекторию.

Матрицы, построенные с применением правил 1Т-2Т, составляют множество искомых *траекторных* матриц $\mathbf{\Omega}_g = \{\omega_{g,i,a}\}$.

Как уже отмечено выше, преимущество подхода, изложенного в [294], в сравнении с использованием подхода *полного перебора* состоит в сокращении объема проводимых вычислений. Покажем это на примере. Пусть для каждого ЭБП в обязательном порядке задаются M^* альтернативных траекторий движения. Тогда с учетом приведенных выше правил имеем следующее выражение для оценки количества *траекторных* матриц:

$$G = M^*(1 + (M^* - 1)|C|). \tag{85}$$

И если для указанного выше примера боя двух мотострелковых рот $G \approx 3{,}5 \cdot 10^9$, то для подхода, изложенного в [294], G = 123. Если будет задано меньше, чем M^* альтернативных траекторий движения для одного ЭБП, то значение G будет меньше.

На **этапе 3** проводится преобразование *траекторных* матриц $\mathbf{\Omega}_g$ в *траекторно-временные* матрицы $\mathbf{\Psi}_g$. Они определяются следующим образом:

$$\mathbf{\Psi}_g = \{\psi_{g,i,b}\}, \tag{86}$$

где b = 0, 1, 2, …– порядковый номер шага дискретизации времени боя.

Такое преобразование необходимо для синхронизации во времени процессов движения всех ЭБП на поле боя следующим образом.

Для каждой ячейки $\omega_{g,i,a}$ i-й строки *траекторной* матрицы $\mathbf{\Omega}_g$ в i-ю строку *траекторно-временной* матрицы $\mathbf{\Psi}_g$ последовательно записываются $B_{g,i,a}$ ячеек, каждая из которых принимает одно из двух значений:

$$\psi_{g,i,b} = \begin{cases} 1, & \text{если } i\text{-й ЭБП на } b\text{-м шаге движется;} \\ 0 & \text{в противном случае.} \end{cases} \tag{87}$$

Определение численного значения $B_{g,i,a}$ осуществляется с использованием общеизвестной физической формулы следующим образом:

$$B_{g,i,a} = \left\lfloor \frac{\zeta}{\tau v_i(\omega_{g,i,a})} \right\rfloor, \quad (88)$$

где $v_i(\omega_{g,i,a})$ – скорость движения i-го элемента в a-м элемобе *траекторной* матрицы $\mathbf{\Omega}_g$, находящемся на g-й траектории движения этого ЭБП;

ζ – размер стороны элемоба;

τ – шаг дискретизации времени боя;

$\lfloor ... \rfloor$ – знак округления до ближайшего целого в меньшую сторону.

Конечные моменты последних боевых эпизодов всех ЭБП в *траекторно-временных* матрицах выравниваются по конечному моменту боевого эпизода, завершающегося последним. Этот момент характеризует продолжительность боя. В позициях строк, добавленных в процессе выравнивания, ЭБП считаются находящимися в неподвижном состоянии.

На **этапе 4** проводится обновление значения параметра масштабирования боя по формуле $T_м = T_м + \varsigma$. При этом изначально $T_м = 0$.

На **этапе 5** проводится масштабирование *траекторно-временных* матриц $\mathbf{\Psi}_g$. Для этого каждая строка матрицы $\mathbf{\Psi}_g$ подвергается процедуре, регламентированной следующими правилами.

Правило 1М. Каждый сегмент траектории между смежными точками действия, начала и конца траектории образует новую точку действия, время остановки в которой равно времени движения по сегменту. Местоположение вновь создаваемой точки – это позиция, в которой ЭБП находится в средний момент времени прохождения сегмента.

Правило 2М. Каждая точка действия, время остановки в которой меньше $T_м$, объединяется со смежной точкой действия с наибольшим временем остановки. При равенстве времен остановки смежных точек выбирается ближайшая к противнику точка.

На **этапе 6** проводится синхронизация масштабированных *траекторно-временных* матриц $\mathbf{\Psi}_g^*$ в рамках единой для каждой отдельной матрицы последовательности боевых эпизодов. Процедура синхронизации состоит в том, что левую и правую границы частного боевого эпизода каждого ЭБП перемещают в рамках допустимого диапазона значений в целях сведения количества единой для матрицы последовательности боевых эпизодов к минимуму. В этой процедуре $T_м$ выступает в качестве меры погрешности определения временных границ единых для матрицы боевых эпизодов следующим образом. Применение правил 1М и 2М позволяет получить в масштабированных *траекторно-временных* матрицах продолжительность каждого частного боевого эпизода не менее $T_м$. Поэтому для того, чтобы боевой эпизод в каждой точке действия в результате синхронизации не перестал существовать, необходимо, чтобы варьирование его границ проводилось в диапазоне

$$(T_{нач} \pm ½T_м;\ T_{кон} \pm ½T_м), \quad (89)$$

где $T_{нач}$ и $T_{кон}$ – времена начала и завершения боевого эпизода, соответственно.

С учетом изложенного для синхронизации масштабированных *траекторно-временных* матриц $\mathbf{\Psi}_g^*$ выполняются следующие действия.

Шаг 1. Фиксируется начало очередного единого для матрицы эпизода.

Шаг 2. Проводится копирование ячеек *n*-го столбца очередного единого боевого эпизода на место предшествующих столбцов этого эпизода. Столбцы в едином боевом эпизоде нумеруются, начиная с единицы. Порядковый номер в едином боевом эпизоде для копируемого столбца вычисляется по формуле

$$n = \left\lceil \frac{T_{\text{м}}}{2\tau} \right\rceil, \tag{90}$$

где $\lceil ... \rceil$ – знак округления до ближайшего целого в большую сторону.

Шаг 3. Проводится переход к *n*-му столбцу единого боевого эпизода, и в каждой строке *траекторно-временной* матрицы $\mathbf{\Psi}_g^*$ значению счетчика несовпадений Σ присваивается ноль.

Шаг 4. Сравнивается очередной столбец масштабированной *траекторно-временной* матрицы $\mathbf{\Psi}_g^*$ с последующим столбцом.

Если содержание ячеек одной строки в очередном и последующем столбцах одинаковое, то осуществляется переход к следующему столбцу, и шаг 4 повторяется. Если последующий столбец последний, то алгоритм завершается.

Если содержание ячеек одной строки в очередном и последующем столбцах различается, то для нее $\Sigma = \Sigma + \tau$ и проверяется выполнение условия:

- если $\Sigma < T_{\text{м}} / 2$, то значения ячеек в очередном и последующем столбцах меняются на «*», осуществляется переход к следующему столбцу, и шаг 4 повторяется;
- если $\Sigma \geq T_{\text{м}} / 2$, то очередной столбец считается конечным для очередного единого боевого эпизода, счетчики Σ у всех строк обнуляются, осуществляется переход к следующему столбцу, и выполняется шаг 1.

На **этапе 7** проводится проверка условия

$$K \cdot T_{\text{эп}} > T_{\text{доп}}, \tag{91}$$

где *K* – максимальное количество полученных в результате выполнения этапа 6 единых боевых эпизодов для всех *траекторно-временных* матриц $\mathbf{\Psi}_g^*$.

Если условие (91) выполняется, то осуществляется переход к этапу 4. Иначе осуществляется переход к этапу 8.

На **этапе 8** проводится построение графа позиционной динамики с учетом вероятностей реализации его ветвей. Целью этой процедуры является определение вероятности реализации каждого сценария боя, характеризующегося своей собственной последовательностью единых боевых эпизодов. Для нахождения вероятности реализации *g*-го сценария боя используется формула

$$P_g = \frac{1}{G} \sum_{i=1}^{|C|} \frac{W_{i,g}}{\sum_{m=1}^{M_i} W_{i,m}}, \tag{92}$$

где $W_{i,g}$ – ранг важности траектории пути i-го ЭБП в g-м сценарии;

$W_{i,m}$ – ранг важности m-й траектории движения i-го ЭБП;

G – количество траекторных матриц;

M_i – количество траекторий движения i-го ЭБП.

После нахождения вероятности реализации каждого сценария боя строится граф позиционной динамики боя.

Каждый самостоятельный остов графа позиционной динамики является последовательностью общих для всех ЭБП противоборствующих сторон боевых эпизодов, реализуемых с одинаковой вероятностью. В зависимости от исходных данных этот граф может иметь вид «куста», «дерева», «леса», «кустистого леса» или «леса деревьев». Остов графа будет древовидным в случае равенства одного или большего количества начальных боевых эпизодов у двух или большего количества сценариев боя или кустовидным в случае одинаковых исходных позиций ЭБП в двух различных сценариях боя и более.

Рассмотрим пример создания *траекторных* матриц альтернативных вариантов позиционной динамики боя (этап 2 методики). Пусть в бою участвуют по три ЭБП с каждой стороны А и Б. Траекториям ЭБП назначены ранги:

- для ЭБП А.1 – А.1.1 (ранг 10), А.1.2 (ранг 7) и А.1.3 (ранг 3);
- для ЭБП А.2 – А.2.1 (ранг 10) и А.2.2 (ранг 5);
- для ЭБП А.3 – А.3.1 (ранг 10), А.3.2 (ранг 8) и А.3.3 (ранг 3);
- для ЭБП Б.1 – Б.1.1 (ранг 10), Б.1.2 (ранг 5) и Б.1.3 (ранг 2);
- для ЭБП Б.2 – Б.2.1 (ранг 10), Б.2.2 (ранг 9) и Б.2.3 (ранг 9);
- для ЭБП Б.3 – Б.3.1 (ранг 10), Б.3.2 (ранг 10) и Б.3.3 (ранг 10).

При таких исходных данных создаются 24 *траекторные* матрицы (см. таблицу 8).

Рассмотрим пример масштабирования *траекторно-временных* матриц (этап 5 методики). Пусть один ЭБП (например, пехотинец) перемещается в соответствии с особенностями местности по некоторой траектории из точки «Начало траектории» в точку «Конец траектории» и ведет огонь в движении и в точках остановки. Вариант траектории движения такого ЭБП в бою показан на рис. 103. На нем кругами с малым диаметром показаны точки действия без остановки, в которых пехотинец движется и одновременно ведет огонь, а кругами с большим диаметром показаны точки действия с остановкой, в которых пехотинец ведет огонь по противнику, находясь в неподвижном состоянии. При этом точки действия с остановкой, в которых пехотинец находится в неподвижном состоянии, являются защищенными от огня противника, что для практики естественно. Времена преодоления участков местности и нахождения пехотинца в неподвижном состоянии также показаны на рис. 103. Общее время движения пехотинца составляет 14 мин 15 с.

На рис. 104 показана траектория движения рассматриваемого пехотинца при начальных условиях (траектория А) и при $T_м$ =30 с (траектория Б). На нем видно, что траектория А состоит из 10 точек действия с остановками. При ограничении, вводимом параметром $T_м$, траектория Б включает восемь точек действия с остановками. Траектории, получаемые при дискретном увеличении значения параметра $T_м$, показаны на рис. 105-107.

Таблица 8 — Варианты траекторных матриц

Строки	Столбцы		
	Матрица Ω_1	Матрица Ω_2	Матрица Ω_3
А.1	траектория А.1.1, ранг 10	траектория А.1.2, ранг 7	**траектория А.1.2, ранг 7**
А.2	траектория А.2.1, ранг 10	траектория А.2.2, ранг 5	траектория А.2.1, ранг 10
А.3	траектория А.3.1, ранг 10	траектория А.3.2, ранг 8	траектория А.3.1, ранг 10
Б.1	траектория Б.1.1, ранг 10	траектория Б.1.2, ранг 5	траектория Б.1.1, ранг 10
Б.2	траектория Б.2.1, ранг 10	траектория Б.2.2, ранг 9	траектория Б.2.1, ранг 10
Б.3	траектория Б.3.1, ранг 10	траектория Б.3.2, ранг 10	траектория Б.3.1, ранг 10
	Матрица Ω_4	Матрица Ω_5	Матрица Ω_6
А.1	**траектория А.1.3, ранг 3**	траектория А.1.1, ранг 10	траектория А.1.1, ранг 10
А.2	траектория А.2.1, ранг 10	**траектория А.2.2, ранг 5**	траектория А.2.1, ранг 10
А.3	траектория А.3.1, ранг 10	траектория А.3.1, ранг 10	**траектория А.3.2, ранг 8**
Б.1	траектория Б.1.1, ранг 10	траектория Б.1.1, ранг 10	траектория Б.1.1, ранг 10
Б.2	траектория Б.2.1, ранг 10	траектория Б.2.1, ранг 10	траектория Б.2.1, ранг 10
Б.3	траектория Б.3.1, ранг 10	траектория Б.3.1, ранг 10	траектория Б.3.1, ранг 10
	Матрица Ω_7	Матрица Ω_8	Матрица Ω_9
А.1	траектория А.1.1, ранг 10	траектория А.1.1, ранг 10	траектория А.1.1, ранг 10
А.2	траектория А.2.1, ранг 10	траектория А.2.1, ранг 10	траектория А.2.1, ранг 10
А.3	**траектория А.3.3, ранг 3**	траектория А.3.1, ранг 10	траектория А.3.1, ранг 10
Б.1	траектория Б.1.1, ранг 10	**траектория Б.1.2, ранг 5**	**траектория Б.1.3, ранг 2**
Б.2	траектория Б.2.1, ранг 10	траектория Б.2.1, ранг 10	траектория Б.2.1, ранг 10
Б.3	траектория Б.3.1, ранг 10	траектория Б.3.1, ранг 10	траектория Б.3.1, ранг 10
	Матрица Ω_{10}	Матрица Ω_{11}	Матрица Ω_{12}
А.1	траектория А.1.1, ранг 10	траектория А.1.1, ранг 10	траектория А.1.1, ранг 10
А.2	траектория А.2.1, ранг 10	траектория А.2.1, ранг 10	траектория А.2.1, ранг 10
А.3	траектория А.3.1, ранг 10	траектория А.3.1, ранг 10	траектория А.3.1, ранг 10
Б.1	траектория Б.1.1, ранг 10	траектория Б.1.1, ранг 10	траектория Б.1.1, ранг 10
Б.2	**траектория Б.2.2, ранг 9**	**траектория Б.2.3, ранг 9**	траектория Б.2.1, ранг 10
Б.3	траектория Б.3.1, ранг 10	траектория Б.3.1, ранг 10	**траектория Б.3.2, ранг 10**
	Матрица Ω_{13}	Матрица Ω_{14}	Матрица Ω_{15}
А.1	траектория А.1.1, ранг 10	**траектория А.1.1, ранг 10**	**траектория А.1.3, ранг 3**
А.2	траектория А.2.1, ранг 10	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5
А.3	траектория А.3.1, ранг 10	траектория А.3.2, ранг 8	траектория А.3.2, ранг 8
Б.1	траектория Б.1.1, ранг 10	траектория Б.1.2, ранг 5	траектория Б.1.2, ранг 5
Б.2	траектория Б.1.1, ранг 10	траектория Б.2.2, ранг 9	траектория Б.2.2, ранг 9
Б.3	**траектория Б.3.3, ранг 10**	траектория Б.3.2, ранг 10	траектория Б.3.2, ранг 10
	Матрица Ω_{16}	Матрица Ω_{17}	Матрица Ω_{18}
А.1	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7
А.2	**траектория А.2.1, ранг 10**	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5
А.3	траектория А.3.2, ранг 8	**траектория А.3.1, ранг 10**	**траектория А.3.3, ранг 3**
Б.1	траектория Б.1.2, ранг 5	траектория Б.1.2, ранг 5	траектория Б.1.2, ранг 5
Б.2	траектория Б.2.2, ранг 9	траектория Б.2.2, ранг 9	траектория Б.2.2, ранг 9
Б.3	траектория Б.3.2, ранг 10	траектория Б.3.2, ранг 10	траектория Б.3.2, ранг 10
	Матрица Ω_{19}	Матрица Ω_{20}	Матрица Ω_{21}
А.1	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7
А.2	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5
А.3	траектория А.3.2, ранг 8	траектория А.3.2, ранг 8	траектория А.3.2, ранг 8
Б.1	**траектория Б.1.1, ранг 10**	**траектория Б.1.3, ранг 2**	траектория Б.1.2, ранг 5
Б.2	траектория Б.2.2, ранг 9	траектория Б.2.2, ранг 9	**траектория Б.2.1, ранг 10**
Б.3	траектория Б.3.2, ранг 10	траектория Б.3.2, ранг 10	траектория Б.3.2, ранг 10
	Матрица Ω_{22}	Матрица Ω_{23}	Матрица Ω_{24}
А.1	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7	траектория А.1.2, ранг 7
А.2	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5	траектория А.2.2, ранг 5
А.3	траектория А.3.2, ранг 8	траектория А.3.2, ранг 8	траектория А.3.2, ранг 8
Б.1	траектория Б.1.2, ранг 5	траектория Б.1.2, ранг 5	траектория Б.1.2, ранг 5
Б.2	**траектория Б.2.3, ранг 9**	траектория Б.2.2, ранг 9	траектория Б.2.2, ранг 9
Б.3	траектория Б.3.2, ранг 10	**траектория Б.3.1, ранг 10**	**траектория Б.3.3, ранг 10**

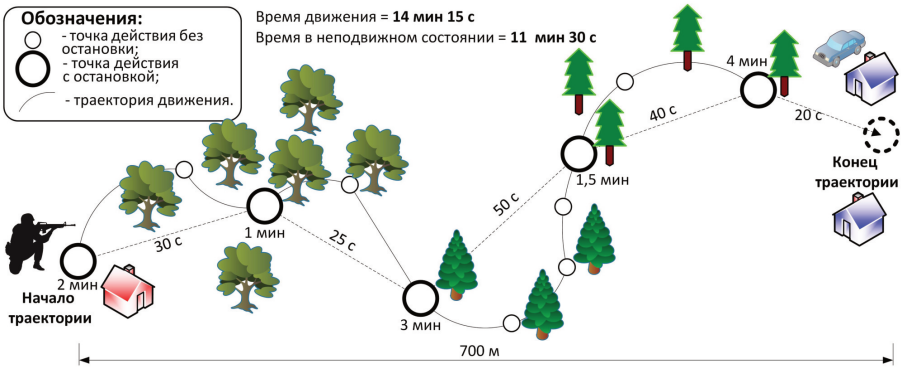


Рис. 103. Траектория движения элемента боевого порядка (вариант)

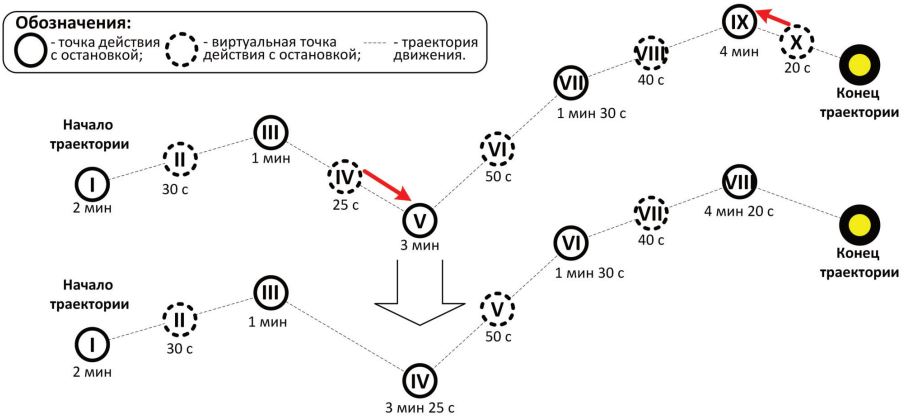


Рис. 104. Траектории движения при $T_м$ =30 с

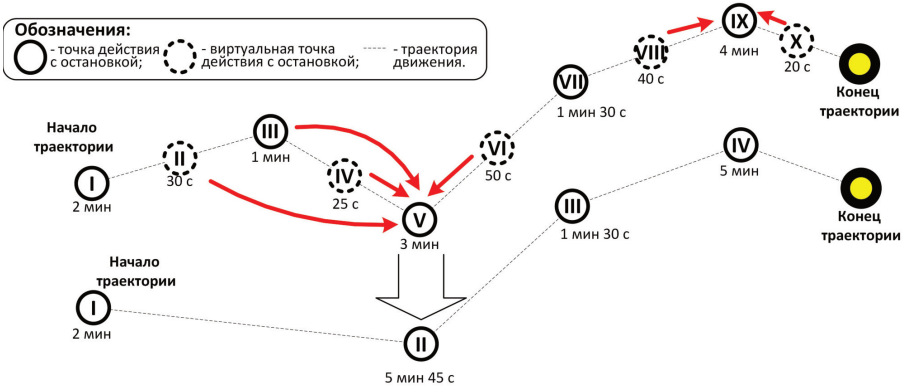


Рис. 105. Траектории движения при $T_м$ = 1 мин 30 с, $T_м$ = 2 мин

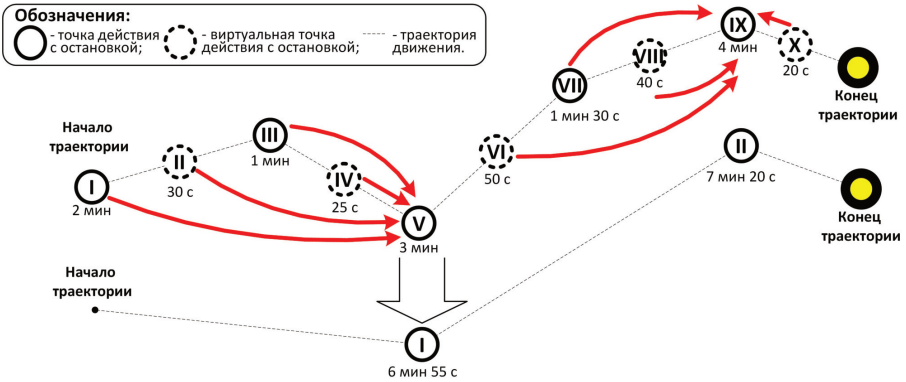


Рис. 106. Траектории движения при $T_м$ = 2 мин 30 с, $T_м$ = 3 мин

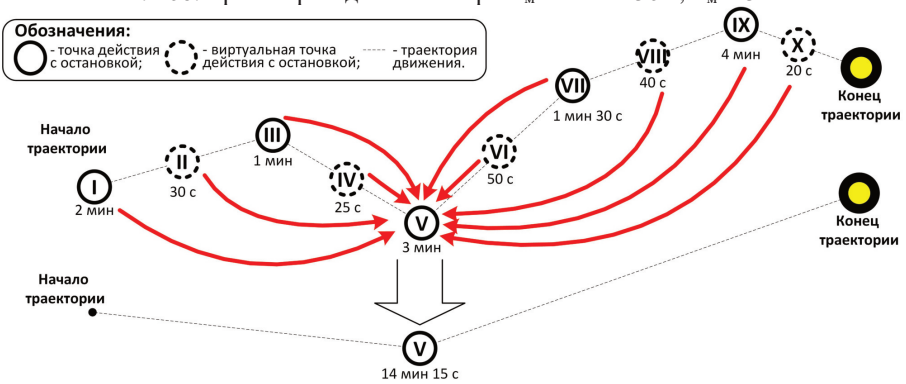


Рис. 107. Траектории движения при $T_м$ = 4 мин 30 с и более

На рис. 105-107 видно, что при $T_м$ = 1 мин количество точек действия с остановками равно пяти, при $T_м$ = 1 мин 30 с и $T_м$ = 2 мин оно равно четырем, при $T_м$ = 2 мин 30 с и $T_м$ = 3 мин равно двум, а при $T_м$ = 3 мин 30 с и выше оно равно единице. При увеличении значения $T_м$ снижается детализация траекторий движения ЭБП. Как следствие, снижается точность результатов моделирования. Эта особенность позволяет за счет гибкого изменения значения $T_м$ настраивать такую детализацию траекторий движения ЭБП, которая позволяет проводить расчеты, не выходя за рамки временных ограничений в боевой обстановке.

Рассмотрим далее пример синхронизации масштабированных *траекторно-временных* матриц в рамках единой для каждой отдельной матрицы последовательности боевых эпизодов (этап 6 методики). Для *траекторно-временной* матрицы боя, показанной на рис. 108, результат синхронизации приведен на рис. 109. Для наглядности вместо координат элемобов в ячейках матрицы показаны порядковые номера частных боевых эпизодов. В этом примере каждая из сторон (А и Б) имеет по три ЭБП, каждый из которых имеет одну траекторию движения. Бой разбит на интервалы с τ = 20 с. Общая продолжительность боя составляет 20 мин, $T_м$ = 1 мин. Общее количество частных боевых эпизодов равно 43. После синхронизации количество глобальных боевых эпизодов

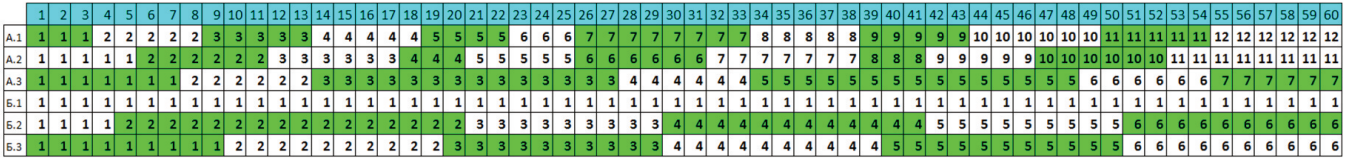


Рис. 108. Пример масштабированной траекторно-временной матрицы

Рис. 109. Пример результата процедуры синхронизации масштабированной траекторно-временной матрицы

составило 14. Поэтому для такого примера граф позиционной динамики боя будет состоять из 14 узлов, связанных в хронологической последовательности.

Выводы. Таким образом, в методике разработки графа позиционной динамики ЭБП ВФ («дерева» боя) в отличие от методики [253] при определении узловых точек боя и статичного размещения в них ЭБП учтены разноранговые варианты траекторий маршрутов движения в бою каждого ЭБП с разной скоростью на участках пути и остановками разной продолжительности. Это достигается за счет создания и комбинаторного использования базовой группы траекторных матриц сценариев боя, количество которых равно наименьшему заданному количеству альтернативных траекторий движения среди всех ЭБП, и формирования для каждой матрицы из базовой группы множества ее дубликатов, в каждом из которых одна траектория движения каждого ЭБП заменяется на другую его траекторию, а также использования вычисляемого для заданного времени анализа боя параметра масштабирования, значение которого определяет, во-первых, минимальную длительность частных эпизодов ЭБП и, во-вторых, величину диапазона допустимого отклонения моментов начала и завершения частных эпизодов при их синхронизации в рамках единого эпизода.

Методика позволяет воспроизвести необходимую и достаточную (безызбыточную) вариативность позиционной динамики ЭБП в бою с учетом вероятностного характера множества альтернативных последовательностей частных боевых эпизодов каждого ЭБП и синтезировать такое наибольшее множество единых для противоборствующих ВФ последовательностей боевых эпизодов, синхронизированных по времени движения отдельных ЭБП на поле боя, суммарное время проведения расчетов которых не превосходит выделенного времени при фиксированном шаге дискретизации времени боя, шаге дискретизации параметра масштабирования боя и времени расчета одного эпизода.

Роль методики в настоящем исследовании состоит в подготовке сценария боя, в котором воспроизводится влияние КА на обеспечиваемые АС процессы разведки, связи, управления и ОП в боевых циклах ВФ.

В ходе применения методики установлено, что она позволяет сократить время разработки графа позиционной динамики в 4…5 раз в сравнении с эмпирическим подходом даже для боя двух рот, а также увеличить не менее чем в 2 раза точность учета в графе траекторий движения ЭБП. При увеличении численности ВФ зависимость показателя сокращения времени разработки графа от числа ЭБП имеет экспоненциальный характер.

5.3 Методика оценки уровня информатизации элемента боевого порядка воинского формирования

Анализ предметной области. Сегодня в военное дело активно внедряются новые цифровые информационные (в том числе телекоммуникационные) технологии. Этот процесс имеет устоявшееся название – «информатизация», хотя существуют и альтернативные его названия

(например, «технологизация» [263], «цифровизация» или «диджитализация»). Учитывая, пожалуй, наиболее общее содержание термина «информатизация», изложенное в работе [243], следует отметить, что в ВС любой страны цель информатизации, как явления, двойственна. С одной стороны, информатизация позволяет *повысить скорость процессов в боевых циклах* ВФ за счет внедрения ИТС в сложные образцы вооружения, что, по определению в ГОСТ [84], делает их образцами АС. С другой стороны, информатизация повышает производительность и улучшает качество труда личного состава, оптимизирует управление и в ряде случаев *освобождает человека* от участия в процессах получения, преобразования, передачи и использования информации. При этом снижение вклада человека в технологические процессы образца вооружения, очевидно, способствует сокращению потерь личного состава.

Однако не следует отождествлять процессы информатизации и автоматизации. Цели этих процессов пересекаются, но у автоматизации согласно [45] цель одна, и более содержательная. Она состоит в *освобождении человека* от участия в процессах получения, преобразования, передачи и использования не только информации, но также энергии и материалов. Анализ тенденций развития общества в XXI веке показывает [243], что в настоящее время всеобщая автоматизация постепенно сменяется всеобщей информатизацией, которая в результате наполнения всех сфер деятельности ИТС начинает угасать и дает начало переходу общества на очередной эволюционный этап его развития. Поэтому уровень информатизации является одной из ключевых ТТХ образцов вооружения.

Известен ряд публикаций, посвященных вопросам исследования процессов информатизации ВС [48, 177, 263]. Однако подходы к численной оценке уровня информатизации образцов вооружения в этих работах не рассматриваются. Тем не менее, на практике этот уровень оценивается двумя способами: экспертным опросом или как выраженный в процентах результат отношения количества задач, выполняемых в образце вооружения с применением ИТС, к общему количеству задач в этом образце (традиционный способ). При этом под задачей образца вооружения понимается совокупность работ некоторого процесса в технологии его применения по назначению, проводимых с использованием входящих в его состав ИТС и/или устройств.

В гражданской сфере вопросам оценки уровня информатизации в научных публикациях уделяется внимание не только в части отдельных отраслей деятельности государства [4, 238], но и на международном уровне.

Так, например, широко известен индекс развития информационно-коммуникационных технологий (так называемый «ICT – Development Index»), ежегодно вычисляемый для 190 стран мира Международным союзом электросвязи [323]. Для этого используется единая методика оценки уровня информатизации. Она заключается в формировании набора частных показателей, вычисляемых по статистическим данным, определении на их основе общих показателей, характеризующих отдельные качественные характеристики информатизации, и агрегировании общих показателей в индекс

информатизации с применением формулы взвешенной аддитивной свертки, веса которой оцениваются по результатам экспертного опроса.

Такие методики оценки ключевой для образцов вооружения ТТХ не учитывают особенности организации технологических процессов и способны привести к противоречию между нередко заявляемым разработчиками высоким приростом «технологичности» и сравнительно низким приростом эффективности их применения по назначению. Поэтому разработка методики оценки уровня информатизации образцов вооружения, учитывающего особенности реализованных в этих образцах технологических процессов, является актуальной научной задачей. Поскольку многие сложные образцы вооружения в бою представляют собой отдельные ЭБП ВФ, далее в методике вместо термина «образец вооружения» применяется термин «ЭБП».

Для анализа совокупности технологических процессов в ЭБП целесообразно использовать комбинацию методов теории вероятностных процессов, теории надежности и теории массового обслуживания, поскольку такая комбинация обеспечивает наиболее адекватную степень детализации рассматриваемых процессов и имеет достаточно развитый математический аппарат. Рассмотрим обобщенную модель ЭБП в виде смешанной системы массового обслуживания со следующими характеристиками [34]:

- *поток заявок* – неограниченный, неординарный. То есть несколько заявок на выполнение различных процессов могут прийти в ЭБП одновременно, но очередная заявка в каждом процессе придет не ранее окончания обработки предыдущей;
- *емкость накопителя* – неограниченная;
- *режим работы системы* – стационарный, без перегрузок. То есть интенсивность поступления заявок не больше интенсивности их обслуживания. Такой режим в ЭБП регулируется автоматически, с одной стороны, вышестоящим органом управления, знающим сформированную им же загрузку, а с другой стороны – повышенной производительностью труда органа управления (расчета, экипажа) ЭБП в боевых условиях. Процессы в образце выполняются поэтапно (этап – это часть процесса, в котором выполняется одна или параллельно несколько задач);
- *дисциплина обслуживания* – с абсолютным приоритетом (с продолжением прерванного обслуживания). Данная дисциплина предусматривает естественное для ЭБП наличие разных приоритетов у реализуемых ими процессов. Если человек в ЭБП занят выполнением некоторой задачи, то он прерывается, когда ему поступает более приоритетная задача, и продолжает ее выполнение по окончании выполнения всех поступивших более приоритетных задач.

Согласно классическим положениям теории вероятностных процессов, теории надежности и теории массового обслуживания среднее время выполнения процессов в такой системе предлагается рассчитывать по следующей формуле [34]:

$$t_{пр} = \frac{\sum\limits_{i=1}^{I_{\text{проц}}} \lambda_i \tau_i}{\sum\limits_{i=1}^{I_{\text{проц}}} \lambda_i} \text{ при } \tau_i = \sum_{j=1}^{\Im_i} t_{i,j} + \rho_i;$$

$$t_{i,j} = \begin{cases} \max\limits_{k=1..K_{i,j}} (t_{i,j,k}), \text{ если задачи на } j\text{-м этапе} \\ \text{могут выполняться параллельно;} \\ t_{i,j,1} \text{ в противном случае;} \end{cases} \quad (93)$$

$$\rho_i = \begin{cases} \sum\limits_{e=1...I_{\text{проц}}, h=1...\mathscr{B}_e, l=1...\mathscr{L}_{e,h}} t_{e,h,l}, \text{ если } \forall e \neq i, \forall h, \exists l : \left(pr(i) < pr(e) \right) \wedge \\ \wedge \left(\begin{array}{c} l\text{-я задача } h\text{-го этапа } e\text{-го процесса выполняется} \\ \text{человеком-оператором, реализующим } i\text{-й процесс} \end{array} \right); \\ 0 \text{ в противном случае,} \end{cases}$$

где $I_{\text{проц}}$ – количество процессов в технологии применения ЭБП;

λ_i – интенсивность поступления заявок на обработку в i-м процессе;

$\Im_i$ – количество этапов в i-м процессе;

$K_{i,j}$ – количество задач в j-м этапе i-го процесса;

$t_{i,j,k}$ – время выполнения k-й задачи в j-м этапе i-го процесса;

$pr(\ldots)$ – приоритет соответствующего процесса;

$\mathscr{B}_e$ – количество этапов в e-м процессе;

$\mathscr{L}_{e,h}$ – количество задач h-го этапа в e-м процессе.

С учетом этого методика состоит в выполнении следующих этапов.

Этап 1. Представление совокупности технологических процессов ЭБП в виде системы массового обслуживания с вышеуказанными характеристиками.

Этап 2. Вычисление по формуле (93) среднего времени выполнения технологических процессов ЭБП для двух вариантов их реализации: без использования ИТС (то есть «вручную») и с их использованием. На этом этапе также оценивается количество личного состава, которое необходимо для применения образца с использованием и без использования ИТС.

Этап 3. Вычисление значения показателя уровня информатизации ЭБП Δ как доли необходимых для его применения человеческих и временных ресурсов, обеспечиваемых ИТС, по следующей формуле [34]:

$$\Delta[\%] = 100(1 - \mathbb{P}\mathbb{Q}) \text{ при } \mathbb{P} = \frac{t^*_{\text{пр}}}{t_{\text{пр}}};$$

$$\mathbb{Q} = \begin{cases} 1, \text{ если ЭБП эксплуатируется без личного состава;} \\ \dfrac{k^*_{\text{пр}}}{k_{\text{пр}}} \text{ в противном случае,} \end{cases} \quad (94)$$

где $\mathbb{P}$ – доля сбереженного времени на применение ЭБП за счет информатизации;

$\mathbb{Q}$ – доля сбереженного личного состава ЭБП за счет информатизации;

$t_{пр}$ и $t^*_{пр}$ – среднее время выполнения процессов в ЭБП без применения и с применением ИТС, соответственно, вычисляемое по формуле (93);

$k_{пр}$ и $k^*_{пр}$ – количество личного состава, необходимое для выполнения процессов в ЭБП без применения и с применением ИТС, соответственно.

Примечание: в модели, исходя из базовых целей процесса информатизации ЭБП, полагается, что $t_{пр} > t^*_{пр}$ и $k_{пр} > k^*_{пр}$.

Предлагаемая методика может найти применение при оценке уровня информатизации ВФ в целом. В таком случае уровень информатизации ВФ оценивается с применением классической формулы взвешенной аддитивной свертки:

$$\Delta = \sum_{n=1}^{|C|} \Delta_n W_n \text{ при } \sum_{n=1}^{|C|} W_n = 1, \tag{95}$$

где Δ – уровень информатизации ВФ;

C – множество ЭБП в рассматриваемом ВФ;

Δ_n – уровень информатизации n-го ЭБП, см. формулу (94);

W_n – КБС n-го ЭБП в ВФ (методику оценки см. далее в параграфе 5.4).

Предлагаемая методика может применяться как при определении реального уровня информатизации, так и при обосновании требований к нему.

Формула (94) при известных стоимости внедрения ИТС для решения отдельных задач и допустимых затратах на информатизацию ЭБП предоставляет возможность для осуществления параметрического синтеза. Для этого следует использовать методы теории выбора и решить комбинированную задачу так называемого «O-оптимального» выбора на множестве эффективных альтернатив, полученном в результате решения задачи так называемого «γ-эффективного» выбора [130]:

$$\exists\left(x^* \in \mathbb{k}^*\right)\left(x^* = \arg\max_{\mathfrak{A} \in \mathbb{k}^*} \Delta(x)\right) \text{ при } \left(\mathfrak{A} \in \mathbb{k}^*\right) = \left\{x \in \mathbb{k} \mid \mathbb{S}(x) \le \mathbb{S}_{\max}\right\}, \tag{96}$$

где x – набор задач, обеспечиваемых ИТС;

$\mathbb{S}_{\max}$ – максимально допустимая стоимость информатизации ЭБП;

$\mathbb{S}(x)$ – функция стоимости ЭБП для набора задач x, обеспечиваемых ИТС;

$\mathbb{k}$ – множество альтернативных наборов задач, удовлетворяющих ограничениям на время выполнения задач, структуру процессов в ЭБП и используемую модель системы массового обслуживания;

$\mathfrak{A}$ – набор задач, обеспечиваемых ИТС, при котором стоимость ЭБП не больше максимальной и удовлетворяются ограничения на время выполнения задач, структуру процессов в ЭБП и используемую модель системы массового обслуживания;

$\mathbb{k}^*$ – множество наборов задач, обеспечиваемых ИТС, при котором стоимость ЭБП не больше максимальной и удовлетворяются ограничения на время выполнения задач, структуру процессов в ЭБП и используемую модель системы массового обслуживания;

x^* – набор задач, обеспечиваемых ИТС, стоимость которого не превосходит заданную и при котором уровень информатизации максимален;

$\Delta(x)$ – уровень информатизации ЭБП для набора задач x, обеспечиваемых ИТС (рассчитывается по формуле (94)).

Применение методики можно продемонстрировать на примере ЭБП, в котором три технологических процесса, одновременно обеспечиваемых людьми и ИТС. Схематично эти процессы показаны на рис. 110.

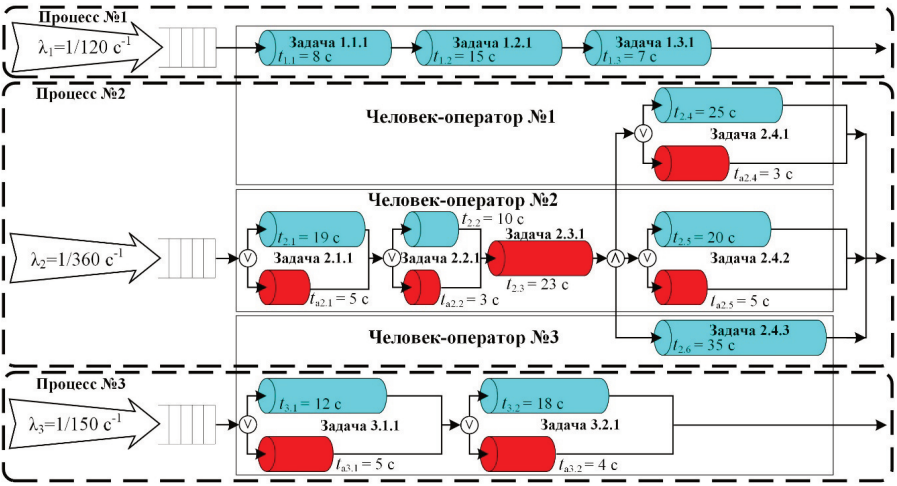


Рис. 110. Технологические процессы в элементе боевого порядка (вариант)

В примере личный состав ЭБП включает три человека-оператора, один из которых выполняет все задачи процесса № 1 и одну задачу процесса № 2, второй – четыре из шести задач процесса № 2, а третий – все задачи процесса № 3 и одну задачу процесса № 2. Задачи № 2.1.1, № 2.2.1, № 2.4.1, № 2.4.2, № 3.1.2 и № 3.2.1 могут выполняться «вручную» или с применением ИТС, сокращающих время выполнения процессов, а остальные задачи – только «вручную». Высший приоритет имеет процесс № 2, то есть при выполнении задач процессов № 1 и № 3 люди-операторы прерываются на выполнение своих работ в процессе № 2.

По формуле (93) для этого примера имеем следующие выражения:

$$t_{\text{пр}} = \frac{\tau_1\lambda_1+\tau_2\lambda_2+\tau_3\lambda_3}{\lambda_1+\lambda_2+\lambda_3}$$

$$\text{при } \tau_1 = t_{1.1.1} + t_{1.2.1} + t_{1.3.1} + t_{\text{a}2.4.1}; \quad (97)$$

$$\tau_2 = t_{\text{a}2.1.1} + t_{\text{a}2.2.1} + t_{2.3.1} + t_{2.4.3};$$

$$\tau_3 = t_{\text{a}3.1.1} + t_{\text{a}3.2.1} + t_{2.4.3}.$$

При использовании традиционной методики оценки в примере уровень информатизации для ЭБП равен 54,5 %, поскольку ИТС обеспечивают шесть из 11 задач. Однако реальное ускорение процессов за счет информатизации в рассматриваемом ЭБП, рассчитанное с использованием предлагаемой методики, значительно ниже. Оно для процесса № 1 составляет 40 %

(сокращение от 55 до 33 с), № 2 – 24,1 % (сокращение от 87 до 66 с), № 3 – 32,3 % (сокращение от 65 до 44 с), а в целом для ЭБП согласно формуле (97) – 33,7 %. То есть при использовании традиционной методики уровень информатизации завышается не менее чем в 1,8 раза.

Для приведенного примера уровень информатизации ЭБП Δ, рассчитываемый по формуле (94), также равен 33,7 %, поскольку информатизация не привела к сокращению боевого расчета этого ЭБП. Однако в случае реализации решения задачи № 2.4.3 с использованием ИТС, сокращающего время ее выполнения от 35 до 7 с и позволяющего сделать процесс № 2 полностью автоматическим, среднее время выполнения процессов ЭБП сократится в 2,3 раза – от 63,8 до 27,4 с, а Δ увеличится более чем в 2,1 раза – до 71,3 %. При традиционной методике расчета уровень информатизации в таком случае составляет 63,6 %.

Из указанных численных результатов следует, что задача повышения уровня информатизации ЭБП должна решаться не только ускорением технологических процессов и заменой человека машиной там, где это возможно, но и оптимизацией ролей личного состава в этих процессах.

Пусть для рассмотренного примера допустимая стоимость ЭБП составляет 30 условных единиц, а цены на внедрение ИТС для решения задач составляют: № 2.1.1 – 5 у.е.; № 2.2.1 – 7 у.е.; № 2.4.1 – 12 у.е.; № 2.4.2 – 3 у.е.; № 3.1.2 – 4 у.е.; № 3.2.1 – 6 у.е. Количество вариантов информатизации ЭБП в таком случае равно $2^6 = 64$.

Варианты набора задач, суммарная стоимость информатизации которых *равна* допустимой, приведены в таблице 9. В примере оптимальным (см. формулу (96)) является первый из указанных в таблице 9 вариантов набора задач, то есть набор с задачами № 2.1.1, № 2.4.1, № 2.4.2, № 3.1.2 и № 3.2.1.

Таблица 9 — Варианты информатизации элемента боевого порядка

№ варианта	Задачи, обеспечиваемые ИТС	Время решения задачи $t_{пр}$, с	Цена информатизации, у.е.	Уровень информатизации Δ, %
1	2.1.1; 2.4.1; 2.4.2; 3.1.2; 3.2.1	43,4	30	32,0
2	2.1.1; 2.2.1; 2.4.1; 3.2.1	44,9	30	29,6

Таким образом, в методике оценки уровня информатизации ЭБП ВФ в отличие от методик, изложенных в [4, 238, 263, 323] и базирующихся на попарном сравнении отдельных характеристик ИТС ЭБП, уровень информатизации ЭБП вычисляется как доля необходимых для его применения людских и временных ресурсов, обеспечиваемых ИТС. Это достигается за счет воспроизведения совокупности процессов этого элемента в виде системы массового обслуживания типа M/M/N, структура, нагрузка и функциональные параметры которой определяются его технологической картой при заданных технической и штатной комплектациях, а времена выполнения процессов определяются с использованием и без использования ИТС.

Методика позволяет учесть при оценке показателя уровня информатизации одновременно среднее время выполнения процессов информационной технологии, реализованной в ЭБП, и количество привлекаемых для этого людей.

Роль методики в настоящем исследовании состоит в получении численного значения одного из ключевых показателей ЭБП ВФ – уровня информатизации, характеризующего меру использования ИТС в АС, обеспечивающих процессы разведки, связи, управления и ОП, взаимосвязанные в рамках боевых циклов ВФ. Этот показатель необходим для оценки соотношения БП противоборствующих ВФ в бою с применением КА.

5.4 Методика оценки коэффициентов боевой соизмеримости элементов боевых порядков воинских формирований

Анализ предметной области. КБС применяются в аналитических свертках различного вида для оценки показателей эффективности ЭБП и ВФ в целом. При оценке КБС на практике приходится сталкиваться с необходимостью учета разнородных факторов и процессов, оказывающих влияние на эффективность ЭБП и ВФ в целом. Результаты анализа известных работ в области оценки КБС или весовых коэффициентов сложных организационно-технических систем, к которым относятся, например, крупные организации, пространственно распределенные телекоммуникационные системы, показали, что эта задача решается тремя основными методами [38]:

- **эмпирический метод** [125, 147, 245, 253, 295, 312] предусматривает ранжирование, парные сравнения и шкальные оценки исходной информации об организационно-технических системах с последующим определением экспертами весов на основе личного опыта и без учета результатов ее реального функционирования. Практика показывает, что этот метод является основным в подавляющем большинстве систем поддержки принятия решений. Но общеизвестно, что даже группе квалифицированных экспертов трудно преодолеть проблему «взрыва» пространства факторов и состояний анализируемых процессов, тем более, если эти процессы нестационарные;
- **натурный метод** [217, 315] предполагает определение весовых коэффициентов элементов организационно-технической системы по результатам анализа процесса ее функционирования в реальных или имитируемых условиях. Этот метод требует часто недоступных значительных ресурсных затрат и большого количества статистических результатов функционирования организационно-технических систем для различных условий. В имитационных, в том числе мультиагентных, моделях боя (то есть базирующихся на применении метода Монте-Карло) КБС обычно находят применение опосредованно на основе результатов исхода боя, поскольку в таких моделях показатели эффективности могут быть получены напрямую,

без КБС. Но общеизвестно, что результаты статистического моделирования боя (не отдельного эпизода) даже при неизменных начальных условиях могут существенно различаться. Это может привести к дорогостоящим ошибкам в принятии решений;

- **аналитический метод** [129, 214] предполагает определение в каждом элементе системы количества одинаковых компонентов, выполняющих ее основную функцию и входящих в состав каждого ее элемента, и вычислении веса элемента как отношения количества этих компонентов в элементе к их числу в системе. При отсутствии в элементе таких компонентов этот элемент в расчетах не учитывается. Однако этот метод учитывает только отдельные эффекты применения ЭБП ВФ. Обобщение нескольких эффектов одного ЭБП в рамках этого метода осуществляется эмпирическим или натурным методами, имеющими указанные выше недостатки.

Поэтому актуальной является разработка методики, развивающей аналитический метод и позволяющей оценить КБС ЭБП ВФ с учетом комплекса эффектов их применения на уровне показателя эффективности ВФ без применения экспертного и натурного методов. Предлагаемая методика предполагает наличие аналитической модели боя, обеспечивающей возможность вычисления боевого показателя ВФ с использованием КБС его ЭБП и учитывающей комплекс эффектов от применения этих ЭБП. Такая модель была рассмотрена ранее в главе 4.

Идея методики состоит в следующем. Полагается, что каждое ВФ выполняет некоторую работу для достижения своей цели. Каждый ЭБП выполняет долю работы ВФ, соответствующую своему КБС. Сумма КБС для всех ЭБП ВФ полагается равной единице. Каждому ЭБП назначается одинаковое для всех ЭБП ВФ усредненное значение их КБС, соответствующее случаю, когда все ЭБП в ВФ выполняют одинаковый объем работ. Далее вычисляется значение показателя эффективности ВФ при одинаковом для всех ЭБП усредненном значении КБС. После этого вычисляются значения показателя эффективности ВФ поочередно без каждого из его ЭБП. Нормированная величина разницы между этим значением показателя эффективности ВФ с исключением некоторого ЭБП и ее значением, рассчитанным с усредненным КБС, является весом исключенного ЭБП. То есть в методике полагается, что именно отсутствие эффекта от применения исключенного ЭБП наносит урон ВФ, в состав которого этот элемент входит. Такая «методика последовательных исключений» состоит в выполнении следующих шагов [38].

Шаг 1. Устанавливают для КБС ЭБП ВФ единое усредненное значение и вычисляют значение показателя эффективности ВФ f_0 с одинаковым для всех элементов усредненным КБС w. То есть полагается, что изначально все ЭБП равнозначны. Поскольку сумма весовых коэффициентов ЭБП равна единице, то значение их КБС равно $w = |C|^{-1}$, где C – множество ЭБП в ВФ.

Шаг 2. Вычисляют значение показателя эффективности ВФ поочередно с исключением каждого из ЭБП и пропорциональным перераспределением веса исключенного ЭБП по оставшимся ЭБП ВФ. То есть КБС оставшихся ЭБП равен

$$w' = \frac{1}{|C|-1}. \tag{98}$$

Кортеж полученных значений эффективности ВФ имеет вид:

$$F = \langle f_1 \dots f_n \dots f_{|C|} \rangle, \tag{99}$$

где f_n – значение показателя эффективности ВФ при исключенном n-м ЭБП.

Необходимость перераспределения веса доказывается примером боя одинаковых ВФ, одному из которых дополнительно придан уникальный ЭБП. Для таких исходных данных исключение дополнительного ЭБП без перераспределения КБС приведет к ситуации, когда два одинаковых ВФ будут выполнять разный совокупный объем работ, что противоречит логике. При необходимости проводят перенормировку КБС в группах ЭБП, подгруппах и т.п., предусматриваемых функцией эффективности ВФ.

Шаг 3. Вычисляют действительный КБС каждого ЭБП по относительной разности соотношения значений показателей эффективности ВФ со всеми ЭБП и без этого ЭБП следующим образом:

$$W_n = \frac{f_0 - f_n}{\sum_{i=1}^{|C|}(f_0 - f_i)} \text{ при } \sum_{i=1}^{|C|}(f_0 - f_i) > 0. \tag{100}$$

Полученные с использованием формулы (100) КБС могут иметь положительные, нулевые или отрицательные значения. Отрицательные значения КБС могут быть у ЭБП, наносящих урон своему ВФ (например, ЭБП ведет «дружественный огонь» вследствие дезинформации или перехвата управления ИТС АС).

Методика предполагает возможность исключения нескольких ЭБП из состава ВФ. В таком случае ущерб от их исключения будет соответствовать весу совокупности исключенных ЭБП. Следует учитывать, что суммарный ущерб от исключения двух и т.д. ЭБП по отдельности меньше ущерба от их одновременного исключения по причине объективного существования «синергетического» эффекта от их совместного применения.

Для демонстрации результатов применения методики рассмотрим гипотетический боевой эпизод, в котором ЭБП двух мотострелковых (мотопехотных) рот размещаются на расстоянии до 5 км друг от друга (см. рис. 111). Состав, ТТХ образцов вооружения в ЭБП и информационные потоки рот А и Б одинаковые. Состав ЭБП роты: КНП роты, средство разведки (СР), по три средства огневого поражения (СОП) в каждом из трех взводов. КНП взвода размещается на одном из его СОП. КНП каждой роты размещается на отдельном СОП. Всеми ЭБП используются ИТС УКВ-радиосвязи, местоположение и информацию которых вскрывает СР противника. Уровень информатизации ЭБП – 33 %, что соответствует обеспечению ИТС только средств радиосвязи в боевом цикле каждого ЭБП. Вероятность попадания СОП в цель – 0,3. Вероятность разведки ЭБП противника нетехническими средствами – 0,5. Длительность боевого эпизода – 20 мин. Такая редкая для практики длительность боевого эпизода взята для того, чтобы наглядно отразить эффект от взаимного влияния сторон.

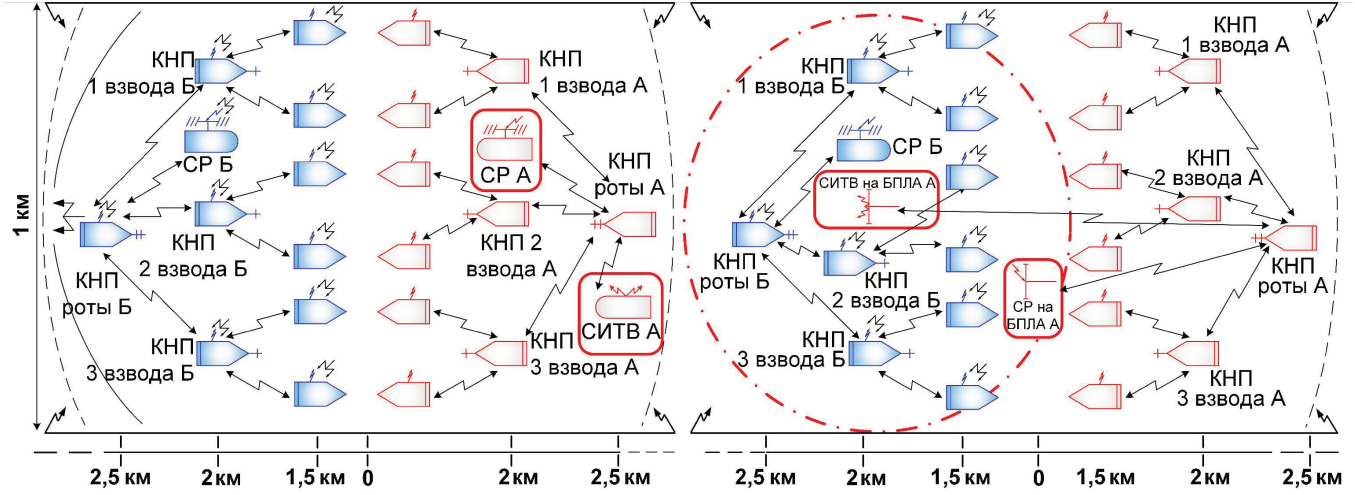


Рис. 111. Варианты размещения элементов боевых порядков двух рот с применением одной из них средства информационно-технического воздействия

Пусть в роте А дополнительно присутствует средство ИТВ (СИТВ), способное осуществлять РЭП средств радиосвязи противника или КА на эти средства. При этом моделируются три варианта выполнения боевой задачи средством ИТВ. Первый вариант предусматривает его мобильное исполнение и наземное размещение вблизи КНП роты (см. рис. 111 слева). При этом осуществляется нескрытное РЭП. Второй вариант, когда наземное средство ИТВ реализует КА. Этот вариант аналогичен ситуации, когда средство ИТВ, реализующее РЭП, размещается на БПЛА, поскольку скрытность средства РЭП в таком случае позволяет достичь аналогичного с КА эффекта применительно к средствам связи. Третий вариант, когда СР и средство ИТВ, реализующее РЭП или КА, исполнены в виде целевых нагрузок БПЛА, барражирующих над боевым порядком противника (см. рис. 111 справа).

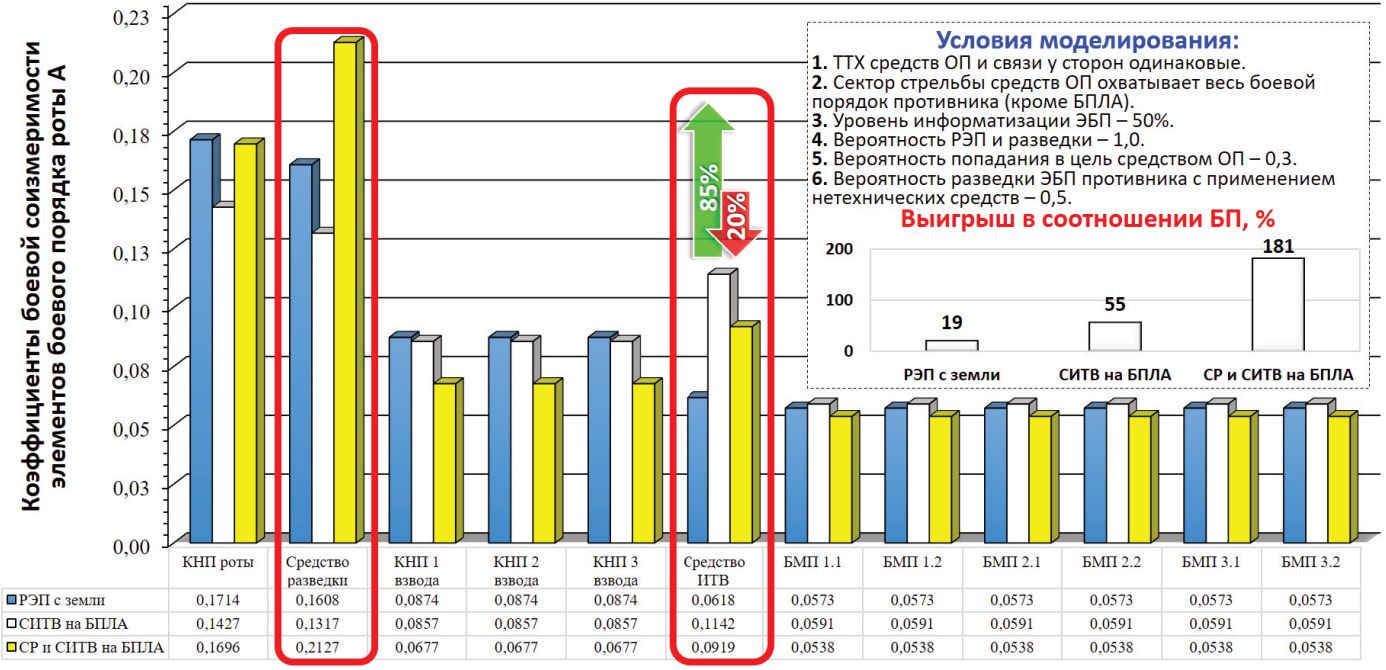
Сектор стрельбы каждого СОП охватывает весь боевой порядок противника. Исключение составляют БПЛА роты А в третьем варианте. Вероятность как РЭП, так и разведки равна единице. СР на земле подвержено ОП, а БПЛА для СОП недосягаем. Применение методики позволяет получить КБС для каждого из указанных вариантов применения средств ИТВ и разведки, показанные на рис. 112.

Разница эффектов от размещения средства ИТВ состоит в том, что с земли при осуществлении РЭП ввиду ограниченной дальности реализуемого им воздействия оно способно блокировать радиосвязь только тех СОП, которые находятся на передовых позициях боевого порядка (не являются КНП). Средство ИТВ, осуществляющее КА, способно блокировать радиосвязь всех СОП, поскольку эффект от такого воздействия достигается даже в том случае, когда радиосигнал с СПС принимается на пороге чувствительности приемного тракта средств радиосвязи. На рис. 112 также показаны результаты оценки выигрыша в соотношении БП, достигаемого в каждом из вариантов.

Таким образом, в методике оценки КБС ЭБП ВФ в отличие от методик, изложенных в [125, 147, 245, 217] и базирующихся на экспертных методах или попарном сравнении одинаковых параметров ЭБП, учтен комплекс эффектов применения ЭБП в бою на уровне показателя БП ВФ. Это достигается за счет определения значения показателя БП ВФ в бою с равными весами всех ЭБП, а затем поочередно с исключением каждого из ЭБП с перераспределением его веса по оставшимся ЭБП своего ВФ в равных пропорциях и вычисления КБС каждого ЭБП по относительной разности БП его ВФ со всеми ЭБП и без него. Это позволяет количественно оценить КБС ЭБП без парного сравнения множеств параметров возможностей их функционирования, которые у ЭБП разнородных ВФ могут не пересекаться.

В частности, анализ результатов применения рассмотренной выше методики позволил сделать следующие выводы:

- установлено, что размещение на БПЛА средств разведки и ИТВ дает прирост в соотношении БП в бою мотострелковых/мотопехотных рот в 2,3 раза;
- подтверждена известная из практики эмпирически установленная закономерность, что при ОП средства разведки должны иметь



	КНП роты	Средство разведки	КНП 1 взвода	КНП 2 взвода	КНП 3 взвода	Средство ИТВ	БМП 1.1	БМП 1.2	БМП 2.1	БМП 2.2	БМП 3.1	БМП 3.2
РЭП с земли	0,1714	0,1608	0,0874	0,0874	0,0874	0,0618	0,0573	0,0573	0,0573	0,0573	0,0573	0,0573
СИТВ на БПЛА	0,1427	0,1317	0,0857	0,0857	0,0857	0,1142	0,0591	0,0591	0,0591	0,0591	0,0591	0,0591
СР и СИТВ на БПЛА	0,1696	0,2127	0,0677	0,0677	0,0677	0,0919	0,0538	0,0538	0,0538	0,0538	0,0538	0,0538

Рис. 112. Результаты оценки коэффициентов боевой соизмеримости

приоритет перед средствами ИТВ. Данная закономерность уточнена в части того, что при планировании применения средств ОП, разведки и ИТВ в тактическом звене необходимо учитывать следующее отношение предпочтения ЭБП противника: «элементы с функцией разведки $\succ$ элементы с функцией ИТВ $\succ$ элементы с функцией управления $\succ$ элементы с функцией ОП». Поэтому в боевых условиях, когда средства разведки и командные пункты (КП) и КНП эффективно маскируются, средства ИТВ, демаскирующие себя электромагнитным излучением с высоким энергетическим потенциалом, являются наиболее приоритетными для уничтожения целями.

Роль рассмотренной методики в настоящем исследовании состоит в получении численного значения одного из ключевых показателей ЭБП ВФ – КБС, позволяющего на единой шкале измерить вклад в соотношение БП противоборствующих ВФ как средств, воздействующих на «материю», так и средств, воздействующих на «информацию», в том числе КА. Этот показатель используется при оценке соотношения БП противоборствующих ВФ в бою с применением КА.

5.5 Методика оценки соотношения боевых потенциалов противоборствующих воинских формирований, оснащенных автоматизированными системами

Анализ предметной области. Анализ свойств КА на АС показывает, что эффективность этих систем наиболее полно может быть оценена наивысшим по иерархии в теории боевой эффективности образцов вооружения и ВФ боевым показателем – соотношением БП ВФ. Использование информационно-боевых и информационных показателей, часто применяемых для оценки эффективности радиоэлектронных воздействий (см., например, [15, 165]), не может быть удовлетворительным, поскольку КА способны системно влиять на весь боевой цикл или совокупность частных боевых циклов атакуемого ВФ, нарушая конфиденциальность, целостность и доступность информации в этих циклах. То есть КА влияют на каждый этап боевого цикла с момента начала процесса получения разведданных о целях до момента применения средств ОП по этим целям, а не только на частные процессы разведки, связи и навигационно-временного обеспечения. Оценка влияния КА на уровне информационно-боевых и тем более информационных показателей эффективности не позволяет системно взглянуть на защищенность АС от КА и учесть эффект, достигаемый ими во всех подсистемах атакуемого ВФ.

Для того, чтобы оценить эффективность функционирования АС на уровне БП ВФ, рассмотрим сначала сущность самого понятия «боевой потенциал». Под БП ВФ понимается интегральный показатель, характеризующий объем заданий (операций), которые может выполнить ВФ по целевому предназначению в расчетных условиях при нормативных уровнях возможностей систем управления, тылового обеспечения и подготовки личного состава [46]. Военный энциклопедический словарь определяет

потенциал как средства, запасы, источники, возможности, которые имеются в наличии и могут быть использованы для достижения определенных целей, решения каких-либо задач [74]. Известные методологические подходы к оценке БП образцов вооружения и ВФ условно делятся на две группы [56]:

- **детальной оценки**, когда применяются средства имитационного моделирования, требующие значительных трудозатрат на подготовку исходных данных и получение результатов;
- **экспресс-оценки**, ориентированные на оперативное получение результатов расчетов, но обеспечивающие меньшую детализацию боя.

В предыдущей главе уже детально рассмотрены особенности подходов первой группы, способствующие их применению при решении частных исследовательских задач с редким достижением теоретической общности результатов. Подходы второй группы, очевидно, представляют наибольший интерес, поскольку позволяют получить общие решения и используются в качестве базиса в подходах первой группы. Краткая характеристика этих подходов приведена выше в п. 1.2.3 при анализе сферы исследования боевых действий. Рассмотрим их детально.

Подходы второй группы условно можно разделить на следующие классы.

1. **Экспертные подходы**. Такие подходы содержатся, например, в [125, 147, 148, 166]. В работе [148] предлагается учитывать возможности КА в так называемом «полном» БП ВФ наряду с ОП, РЭП, управлением и разведкой в качестве слагаемого. Подходы [125, 147, 166] предполагают присвоение КА весового коэффициента, определяемого на основе экспертных оценок. Такой подход к анализу и прогнозированию боевых действий наряду с очевидным преимуществом простоты расчетов имеет следующие недостатки:

- метод экспертных оценок в теории принятия решений характеризуется крайне низкой точностью;
- отсутствует возможность учета таких современных и актуальных компонентов РЭБ, как КА и воздействие мощным ЭМИ. В то же время применение средств реализации КА может привести к отказу от наступления противника ввиду блокирования его системы управления;
- отсутствует учет противодействия противника;
- отсутствует учет динамики применения образцов вооружения и ВФ, оказывающей первостепенное влияние на ход и исход боя;
- отсутствует учет возможность внесения сторонами конфликта дезинформации в сети связи противника и перехвата управления роботизированными образцами вооружения (например, БПЛА с различными целевыми нагрузками).

Кроме того, такие подходы не позволяют с точностью, необходимой для обоснования требований к защищенности АС ВФ от КА, проводить сравнительный анализ различных средств реализации КА и защиты от них образцов вооружения ВФ в условиях боевой обстановки.

2. **Вероятностные подходы**. К таким подходам, в первую очередь, следует отнести подход, предложенный научной школой В.И. Владимирова (см., например, [71, 250]). В нем БП ВФ определяется как произведение БП без

РЭП и экспоненты, отрицательная степень которой установлена эмпирически и представляет собой произведение доли подавленных каналов передачи информации ВФ и уровня уязвимости подсистемы управления ВФ (см. формулу (66)). Этот подход полезен в экспресс-оценке РЭП радиосвязи, но не учитывает указанные возможности КА. Он развивается в работах Р.Л. Михайлова (см., например, [186-188]) в части детализации информационного конфликта информационно-телекоммуникационных систем на основе системного учета взаимного влияния процессов функционирования трех подсистем каждого из противоборствующих ВФ: разведки, связи и РЭП. Однако в этих работах не рассматривается боевой цикл ВФ как единое целое. Это не позволяет учесть в условиях применения сторонами средств ОП возможности КА по влиянию на вероятностные и временные характеристики подсистем разведки и ОП противника, а также на временные характеристики его подсистемы управления.

3. **Подходы на основе теории марковских процессов**. Наиболее известными подходами в этом классе являются подходы на основе метода динамики средних или уравнений Осипова-Ланчестера. Рассмотрим их.

3.1. Работы научной школы А.И. Буравлева (например, [53, 55, 56]). В этих работах потенциал образца вооружения определяется величиной наносимого противнику среднего ущерба за время его существования при реализации ключевых ТТХ, а соотношение БП ВФ определяется классическими уравнениями Осипова-Ланчестера 1-го рода (для высокоорганизованного боя), в которых интенсивности поражающего действия сторон рассчитываются на основе аддитивной свертки БП его образцов вооружения. При этом полагается, что аддитивная свертка дает нижнюю оценку, а ошибка в результатах применения подхода в сравнении с результатами, которые дают подходы детальной оценки с теми же исходными данными, характеризует коэффициент синергизма, которым обладает ВФ по сравнению с простой совокупностью образцов вооружения. Этот подход, несомненно, имеет большую ценность для оценки БП отдельных образцов вооружения, но его применение для оценки БП ВФ ограничивается следующим.

Во-первых, для боя многочисленных ВФ в ограниченном дальностью прямой видимости пространстве он может дать эффект, когда сумма пораженных целей противника, складывающаяся из целей, пораженных отдельными средствами ОП, больше их реального числа. Например, когда уничтоженную воздушную цель расчет каждого из стрелявших по ней зенитных орудий записывает на свой счет.

Во-вторых, он не учитывает возможности сторон по активному противодействию боевым циклам как отдельных образцов вооружения, так и ВФ противника в целом (в том числе средствами РЭБ и, в частности, КА), что особенно актуально для современного боя. Поэтому с применением этого подхода вероятна не нижняя оценка, предполагающая синергизм, а завышенная оценка, когда «2 + 2 < 4».

3.2. Работы отечественных (например, [5, 6, 23, 43, 118, 185, 223, 264, 265]) и зарубежных (например, [300, 320, 328]) авторов, в которых детально

исследуются различные вариации уравнений Осипова-Ланчестера. В частности, в работах [185, 300] приведены весьма ценные результаты теоретического обобщения моделей динамики средних для различных вариантов боя, а работа [300], кроме того, содержит детальный обзор зарубежных исследований в рассматриваемой предметной области. В работах научной школы А.И. Черноскутова [264, 265] с использованием уравнений динамики средних анализируется бой, в котором участвуют более двух сторон, а точнее одна из сторон рассматривается как совокупность нескольких относительно самостоятельных сторон. В работе [43] предложена базирующаяся на уравнениях Осипова-Ланчестера 1-го рода модель боя с применением всей номенклатуры ИТВ. Однако, несмотря на возможность оценки влияния КА на все подсистемы ВФ, в [43] рассматриваются только вероятностные параметры этапов боевых циклов противоборствующих ВФ, а временным параметрам этих циклов внимание не уделяется.

В рамках данного класса подходов также представляет интерес работа [223], где решается задача аналитического моделирования боя с применением РЭП на основе так называемых «уравнений Динера» [107]. Следует отметить, что изложенные в [223] эти уравнения являются упрощенными уравнениями Осипова-Ланчестера 2-го рода (см., например, [300]). В этом подходе используется одновременное приращение интенсивности выполнения задач поражения одной стороны за счет наступательных действий по РЭБ и снижение интенсивности выполнения задач поражения второй стороны за счет защитных действий по РЭБ. Иными словами, в модели [223] считается, что вдобавок к тому, что сторона подверглась РЭП, и скорость противника по ее уничтожению возросла, она еще и снижает свою скорость уничтожения противника, защищаясь от РЭП. Очевидно, такая ситуация крайне нежелательна в реальном бою. Ведь действия противника каждая сторона должна стремиться своим противодействием ослабить, а не усилить.

В целом указанные работы отличаются глубокой теоретической проработкой, но в полном объеме актуальные для КА на АС вопросы организации боевых циклов ВФ в них также не учитываются.

3.3. Работы научной школы Ю.Л. Козирацкого (например, [51, 52, 141, 142]), которые ввиду их первоначальной ориентации на РЭП заслуживают отдельного рассмотрения. Методологическая основа этих работ состоит в применении математического аппарата полумарковских процессов для анализа переходных процессов в боевых ситуациях с применением средств РЭП. Эта основа базируется на методах теории автоматического управления, в которой процессы моделируются в форме передаточных функций, и, пожалуй, наилучшим образом адаптирована для исследования сложных дуэльных ситуаций, возникающих в бою. Но недостаток этого подхода для моделирования боя ВФ лучше всего отмечают его авторы [142]: «возрастание численности каждой из сторон приводит к значительному увеличению мощности множества состояний динамической модели, что, несмотря на экспоненциальные законы распределения времени ожидания при переходах, приведет к существенной громоздкости полученных аналитических

соотношений и возникновению определенных сложностей при обратном преобразовании Лапласа». Поэтому в работе [142] уже для ВФ с пятью ЭБП используется имитационное моделирование, относящееся к рассмотренной выше первой группе подходов к оценке БП.

В данном контексте следует обратить пристальное внимание на показательный и, в частности, на экспоненциальный закон плотности распределения времени переходов между состояниями в моделях рассматриваемого класса. Этот закон имеет существенное значение в теории марковских процессов. Однако следует учитывать два его ключевых недостатка, отмеченных в параграфе 3.1, которые во многом ограничивают применение этого закона в исследовательской практике: уменьшение вероятности с увеличением времени перехода и равенство единице коэффициента вариации.

Кроме того, понимая важность работ М.П. Осипова [203], Ф.У. Ланчестера [306] и их последователей и неоценимость сделанного ими вклада в дело моделирования боевых действий, следует обратить внимание на вид зависимости численности сторон от времени, получаемый с применением предложенных в этих работах уравнений динамики боя. Она имеет экспоненциальный характер. Возникает вопрос: при каких условиях на практике при неизменных во времени скоростях уничтожения сторонами друг друга их численности могут убывать по экспоненте? На практике в таком случае может иметь место только очевидная линейная зависимость. Ведь если человек идет из пункта А в пункт Б с неизменной скоростью, то почему в начале пути он будет проходить за единицу времени гораздо больше пути, чем в конце. Это противоречит классическим постулатам кинематики. Зависимости в уравнениях Осипова-Ланчестера имеют экспоненциальный характер потому, что используемый в их основе метод динамики средних предполагает экспоненциальный закон распределения времени переходов между двумя метасостояниями противоборствующих сторон.

Проведенный обзор подходов к экспресс-оценке БП ВФ не претендует на исчерпывающую полноту. Тем не менее, он показывает, что подходы, которые позволили бы полноценно учесть особенности КА на АС в бою, связанные с их одновременным влиянием на временные и вероятностные характеристики функционирования всех подсистем противника, сегодня отсутствуют.

Предлагаемая методика базируется на совокупности моделей процессов функционирования АС в условиях КА, рассмотренной в главах 3 и 4. Она предусматривает иерархическую вложенность ВФ. При этом ВФ уровня бригады или дивизии, применяемые в отдельном тактическом районе, называются *управляемыми*, а вышестоящие ВФ называются *управляющими*. Рассмотрим шаги методики [39].

Шаг 1. Формирование графа позиционной динамики боя для каждого тактического района как совокупности альтернативных последовательностей боевых эпизодов. Каждая последовательность формируется на основе задаваемых многоальтернативных разноранговых траекторий движения ЭБП сторон с изменяющейся скоростью и остановками разной продолжительности.

Эпизоды в каждой последовательности являются общими для всех ЭБП сторон. Методика формирования этого графа рассмотрена в параграфе 5.2. В графе эпизоды являются синхронизированными по вероятностным и временным параметрам движения отдельных ЭБП сторон на поле боя. Синхронизация осуществляется с применением вычисляемого параметра масштабирования боя, определяющего степень детализации траектории движения ЭБП и диапазон изменения границ синхронизируемых эпизодов без их потери.

Шаг 2. Моделирование боевой обстановки в боевых эпизодах каждого тактического района. Для этого используется иерархическая аналитическая модель процессов функционирования АС в боевом эпизоде, рассмотренная в главе 4. В каждом эпизоде ЭБП статично размещают на электронной карте местности с детализацией до людей и образцов вооружения, включающих ИТС и устройства. Возможности устройств и ИТС задают на основе ТТХ образцов вооружения, в состав которых они входят. В ЭБП и между ними определяют каналы связи, организуемые с использованием ИТС и людей. В этой модели в качестве составляющих используются модели процессов функционирования компонентов АС, рассмотренные в параграфах 3.2-3.5, а также модель процесса распространения СПС в информационно-управляющей сети, образуемой ИТС АС, рассмотренная в параграфе 3.7.

Шаг 3. Оценка соотношения БП управляемых ВФ. Для этого граф позиционной динамики боя в каждом тактическом районе свертывается в отрезок между начальной и наиболее отдаленной по времени точками [30, 32]. Соотношение БП на этом отрезке в каждый момент времени оценивается как сумма значений соотношения БП всех боевых эпизодов, предусмотренных графом в этот момент, взвешенных по вероятности реализации этих эпизодов с учетом предшествующих ветвлений до этого момента. Завершившиеся к рассматриваемому моменту альтернативные варианты боя продлеваются до завершения самого длительного варианта с сохранением достигнутого соотношения БП неизменным. Пример свертывания графа позиционной динамики показан на рис. 113.

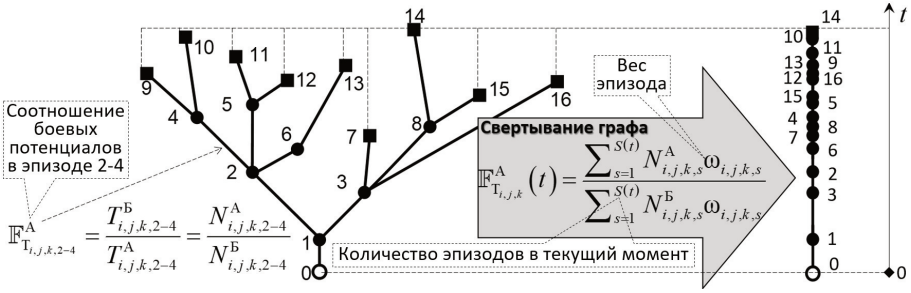


Рис. 113. Пример свертывания графа позиционной динамики боя

В боевом эпизоде соотношение БП в тактическом районе оценивается с использованием выражения

$$\mathbb{F}^{\text{А}}_{\text{Т}_{i,j,k}}(t)=\frac{\sum\limits_{s=1}^{S(t)}T^{\text{Б}}_{i,j,k,s}\omega_{i,j,k,s}}{\sum\limits_{s=1}^{S(t)}T^{\text{А}}_{i,j,k,s}\omega_{i,j,k,s}}, \qquad (101)$$

где $T^{\text{А(Б)}}_{i,j,k,s}$ – время уничтожения ВФ в *s*-м боевом эпизоде графа позиционной динамики ЭБП ВФ;

$S(t)$ – количество альтернативных боевых эпизодов в районе в текущий момент времени t;

$\omega_{i,j,k,s}$ – вес эпизода (определяется рангами используемых в эпизоде траекторий движения ЭБП, задаваемых при разработке графа позиционной динамики).

Шаг 4. Оценка эффективности управления боевыми циклами управляющих ВФ. На этом шаге сначала осуществляется построение структурных моделей ВФ с учетом особенностей их информационных потоков. Структурная модель ВФ представляет собой ориентированный граф, узлы и дуги которого имеют следующее описание.

Узлами графа могут являться следующие структурные элементы ВФ:

- *управляющий элемент* (УЭ). Примеры: КП, КНП;
- *разведывательный элемент* (РЭ). Пример: часть разведки;
- *исполнительный элемент* (ИЭ). Примеры: танковая, самоходно-артиллерийская часть;
- *элемент связи* (ЭС). Примеры: подвижный узел связи, стационарный узел связи;
- *комбинированный элемент*, объединяющий в себе функции вышеуказанных элементов. Комбинированным элементом может являться, например, разведывательно-исполнительный элемент (РИЭ). Пример: часть РЭБ.

То есть в зависимости от избранной степени детализации элементом на данном шаге может быть либо ЭБП, либо отдельное ВФ, входящее в состав дивизии или бригады.

Дуги графа ориентированы по направлениям информационных потоков ВФ и характеризуются интенсивностью передачи сообщений. Информационные потоки делятся по целевому признаку на четыре вида:

- **разведывательный** поток – поток с информацией о противнике от элемента с функцией разведки непосредственно к элементам с функцией управления своего ВФ;
- **управляющий** поток – поток с директивной информацией от элемента с функцией управления к непосредственно подчиненным ему элементам;
- **исполнительный** поток – поток с информацией о результатах деятельности и собственном состоянии от подчиненного к управляющему им элементу;
- **нештатный** поток – поток, способный заместить любой из вышеуказанных потоков.

Потоки организуются с применением ИТС и без них. Нештатные потоки образуются с использованием нештатных ИТС (например, сотовых телефонов, ноутбуков). Нештатные ИТС обеспечивают информационные потребности личного состава и, как показывает практика, активно используются для замены штатных ИТС. Информационные потоки подвергаются деструктивному воздействию в источнике, при передаче и в потребителе информации. Воздействие может быть силовым (например, ОП элементов, по которым проходит поток) и информационно-техническим.

На рис. 114 показан вариант структурной модели ВФ уровня армии, учитывающий основные информационные потоки.

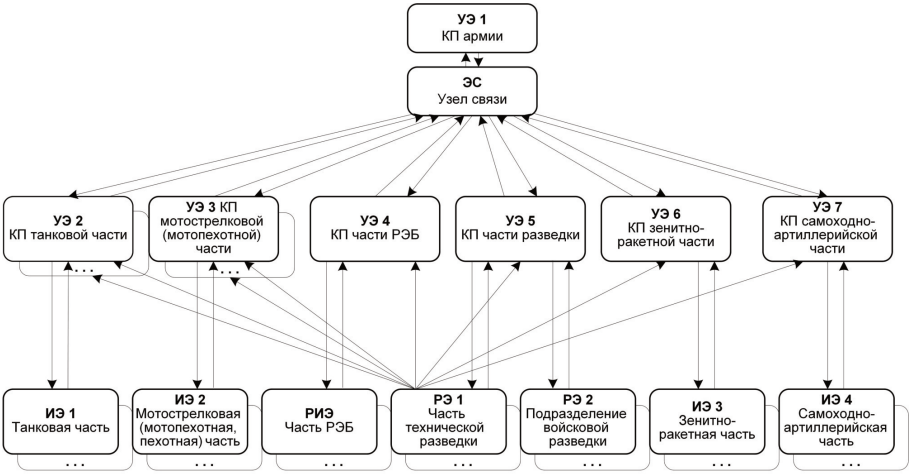


Рис. 114. Структурная модель воинского формирования, учитывающая информационные потоки (вариант)

В этой модели, в частности, части технической разведки обладают возможностью передачи разведанной информации не только своему КП, но и всем заинтересованным в этой информации частям. Тем самым в модели учитывается «сетецентричность» современного боя, в основе которой лежит возможность формирования единой картины происходящих событий в цифровом формате и предоставления доступа к этой картине всем заинтересованным. Функции элемента в ВФ могут обеспечиваться одним, несколькими ИТС или могут решаться вообще без ИТС. Вариант детализации структурной модели УЭ, соответствующего КП мотострелковой части из указанного примера, показан на рис. 115. На этом КП установлена локальная вычислительная сеть, три ИТС являются автоматизированными рабочими местами (АРМ), одно ИТС является коммутатором, одно ИТС – радиостанцией, и личный состав имеет возможность осуществлять обмен информацией с использованием двух нештатных ИТС (ноутбука со встроенным адаптером беспроводной связи и АТ сотовой связи).

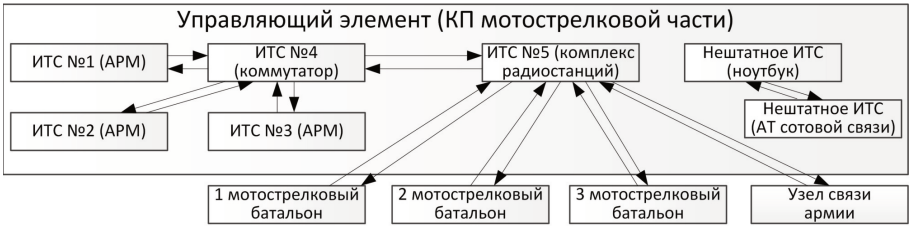


Рис. 115. Структурная модель командного пункта, учитывающая информационные потоки (вариант)

Дополнительно в предлагаемом подходе к построению структурных моделей ВФ вводятся категории «сеть» и «сегмент сети».

Сетью ВФ называется совокупность потоков определенного вида (см. рис. 116).

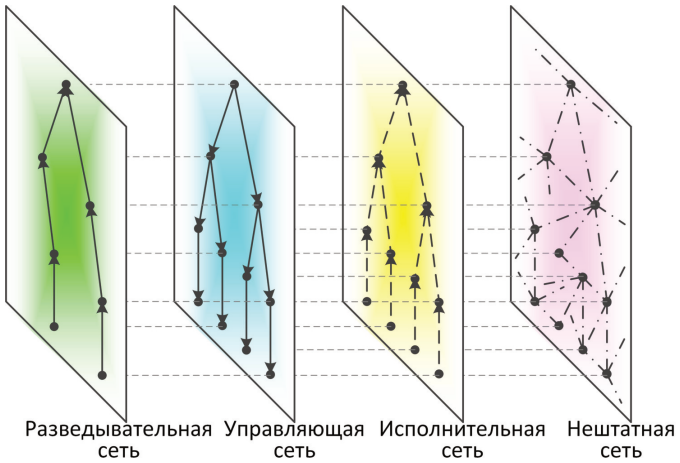


Рис. 116. Сети воинских формирований (вариант)

Потоки в исполнительной сети являются восходящими по иерархии, в управляющей сети – нисходящими по иерархии, а в разведывательной сети с учетом «сетецентричности» потоки могут быть восходящими, нисходящими или связывать элементы ВФ одного уровня иерархии.

Сегментом сети называется ее самостоятельная единица, порождающая потоки и обеспечивающая их передачу потребителям. Элементы, использующие потоки сегмента, в этот сегмент не включаются. Из сегментов состоят разведывательная, управляющая и исполнительная сети.

Образующим в сегменте называется элемент, порождающий потоки. В сегменте один образующий элемент. Сети для рассматриваемого примера структурной модели армии показаны на рис. 117.

Рассмотрим далее особенности построения этих сетей.

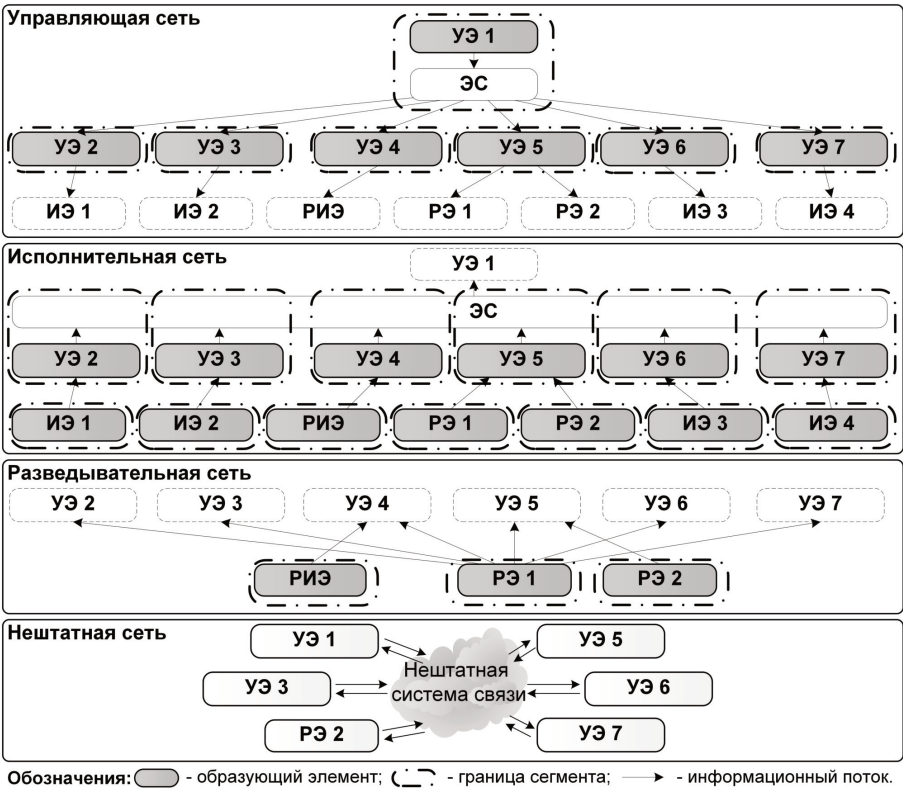


Рис. 117. Сети информационных потоков воинского формирования (вариант)

Разведывательная сеть состоит из $C_р$ сегментов ($C_р$ – количество элементов ВФ с функцией разведки). Пример фрагмента схемы обеспечения элементов ВФ развединформацией показан на рис. 118.

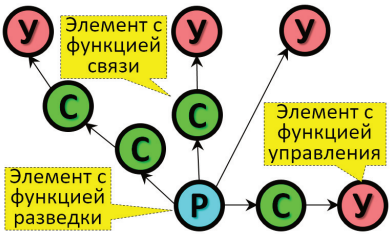


Рис. 118. Вариант фрагмента схемы обеспечения элементов развединформацией

Показатель **конфиденциальности информации разведывательной сети** в момент времени t определяется как взвешенная сумма значений показателей конфиденциальности информации входящих в нее сегментов:

$$\kappa_{\text{р}}(t)=\sum_{c=1}^{C_{\text{р}}}\frac{\kappa_{\text{р}_c}(t)\sum_{g=1}^{C_{\text{у}_c}}W_{\text{у}_{c,g}}}{\sum_{j=1}^{C_{\text{у}}}\left(W_{\text{у}_j}n_{\text{р}_j}\right)}, \tag{102}$$

где $C_{\text{у}}$ – количество элементов с функцией управления в ВФ;

$C_{\text{у}_c}$ – количество элементов с функцией управления, обеспечиваемых разведданными из c-го сегмента разведывательной сети;

$n_{\text{р}_j}$ – количество элементов с функцией разведки, информация от которых поступает в j-й элемент с функцией управления;

$W_{\text{у}_{c,g}}$ – КБС g-го элемента с функцией управления, обеспечиваемого разведданными из c-го сегмента разведывательной сети (здесь и далее КБС определяются по методике, рассмотренной ранее в параграфе 5.4);

$W_{\text{у}_j}$ – КБС j-го элемента с функцией управления в ВФ;

$$\kappa_{\text{р}_c}(t)=\begin{cases}\kappa_{c,h}(t), \text{ если в } c\text{-м сегменте нет промежуточных}\\ \qquad\text{элементов с функцией связи;}\\ \kappa_{c,h}(t)\sum_{g=1}^{C_{\text{у}_c}}\left(W_{\text{у}_{c,g}}\prod_{q=1}^{C_{\text{св\_р}_{c,g}}}\kappa_{\text{св\_р}_{c,g,q}}(t)\right) \text{ в противном случае;}\end{cases} \tag{103}$$

$\kappa_{c,h}(t)$ – конфиденциальность информации образующего элемента в c-м сегменте разведывательной сети в момент времени t, см. формулу (108);

$\kappa_{\text{св\_р}_{c,g,q}}(t)$ – конфиденциальность информации q-го промежуточного элемента с функцией связи, обеспечивающего передачу разведданных g-му элементу с функцией управления в c-м сегменте разведывательной сети в момент времени t, см. формулу (108);

$C_{\text{св\_р}_{c,g}}$ – количество промежуточных элементов с функцией связи в c-м сегменте разведывательной сети, обеспечивающих передачу разведданных g-му элементу с функцией управления в этом сегменте.

Приведенные в формулах (102) и (103) зависимости аналогичны для **показателей целостности** $\gamma_{\text{р}}(t)$ **и доступности** $\delta_{\text{р}}(t)$ **информации разведывательной сети** в момент времени t с учетом соответствующей замены показателей конфиденциальности информации.

Управляющая сеть состоит из $C_{\text{у}}$ сегментов, в которых элементам с функцией управления могут быть подчинены элементы с исполнительной, разведывательной или управляющей функцией. Значение **показателя конфиденциальности информации управляющей сети** в момент времени t предлагается оценивать как взвешенную сумму значений показателей конфиденциальности информации ее сегментов:

$$\kappa_{\text{у}}(t)=\sum_{c=1}^{C_{\text{у}}}\kappa_{\text{у}_c}(t)W_{\text{у}_c}, \tag{104}$$

где $W_{\text{у}_c}$ – КБС элемента, образующего c-й сегмент управляющей сети;

$$\kappa_{\text{у}_c}(t)=\begin{cases}\kappa_{c,h}(t), \text{ если в } c\text{-м сегменте нет промежуточных} \\ \qquad \text{элементов с функцией связи;} \\ \kappa_{c,h}(t)\left(\sum\limits_{s=1}^{C_{\text{и\_у}_c}}\left(W_{\text{и\_у}_{c,s}}\prod\limits_{q=1}^{C_{\text{св\_и\_у}_{c,s}}}\kappa_{\text{св\_и\_у}_{c,s,q}}(t)\right)+\sum\limits_{s=1}^{C_{\text{у\_у}_c}}\left(W_{\text{у\_у}_{c,s}}\prod\limits_{q=1}^{C_{\text{св\_у\_у}_{c,s}}}\kappa_{\text{св\_у\_у}_{c,s,q}}(t)\right)+\right. \\ \qquad \left.+\sum\limits_{s=1}^{C_{\text{р\_у}_c}}\left(W_{\text{р\_у}_{c,s}}\prod\limits_{q=1}^{C_{\text{св\_р\_у}_{c,s}}}\kappa_{\text{св\_р\_у}_{c,s,q}}(t)\right)\right)/ \\ \qquad /\left(\sum\limits_{s=1}^{C_{\text{и\_у}_c}}W_{\text{и\_у}_{c,s}}+\sum\limits_{s=1}^{C_{\text{у\_у}_c}}W_{\text{у\_у}_{c,s}}+\sum\limits_{s=1}^{C_{\text{р\_у}_c}}W_{\text{р\_у}_{c,s}}\right) \text{в противном случае;}\end{cases} \quad (105)$$

$\kappa_{c,h}(t)$ – конфиденциальность информации образующего элемента в *c*-м сегменте управляющей сети в момент времени *t*, см. формулу (108);

$\kappa_{\text{св\_у\_у}_{c,s,q}}(t)$, $\kappa_{\text{св\_р\_у}_{c,s,q}}(t)$ и $\kappa_{\text{св\_и\_у}_{c,s,q}}(t)$ – конфиденциальность информации *q*-го промежуточного элемента с функцией связи *c*-го сегмента управляющей сети, обеспечивающего передачу информации от образующего элемента данного сегмента *s*-му непосредственно подчиненному элементу с функцией управления, разведки и с исполнительной функцией, соответственно, в момент времени *t*, см. формулу (108);

$C_{\text{у\_у}_c}, C_{\text{р\_у}_c}$ и $C_{\text{и\_у}_c}$ – количество в *c*-м сегменте управляющей сети непосредственно подчиненных образующему элементу сегмента элементов с функцией управления, разведки и с исполнительной функцией, соответственно;

$W_{\text{у\_у}_{c,s}}$, $W_{\text{р\_у}_{c,s}}$ и $W_{\text{и\_у}_{c,s}}$ – КБС *s*-го непосредственно подчиненного образующему элементу *c*-го сегмента управляющей сети элементов с функцией управления, разведки и с исполнительной функцией, соответственно;

$C_{\text{св\_у\_у}_{c,s}}$, $C_{\text{св\_р\_у}_{c,s}}$ и $C_{\text{св\_и\_у}_{c,s}}$ – количество промежуточных элементов с функцией связи, обеспечивающих передачу информации от образующего элемента в *c*-м сегменте управляющей сети к *s*-му непосредственно подчиненному элементу с функцией управления, разведки и с исполнительной функцией, соответственно.

Приведенные в формулах (104) и (105) зависимости аналогичны для **показателей целостности** $\gamma_{\text{у}}(t)$ **и доступности** $\delta_{\text{у}}(t)$ **информации управляющей сети** в момент времени *t* с учетом соответствующей замены в этих формулах показателей конфиденциальности информации.

Исполнительную сеть могут образовывать элементы с исполнительной функцией, функцией управления и функцией разведки, сообщая непосредственно вышестоящим по иерархии элементам с функцией управления о результатах своей деятельности и собственном состоянии. Не образует сегмента исполнительной сети только элемент, стоящий головным в ВФ. Значение **показателя конфиденциальности информации исполнительной сети** в момент времени *t* оценивается как взвешенная сумма показателей конфиденциальности информации ее сегментов:

$$\kappa_{\text{и}}(t)=\frac{\sum_{c=1}^{C'_{\text{у\_и}}+C_{\text{и\_и}}+C_{\text{р\_и}}}\left(\kappa_{\text{и\_и}_c}(t)W_{\text{и(у,р)\_и}_c}\right)}{\sum_{s=1}^{C'_{\text{у\_и}}}W_{\text{у\_и}_s}+\sum_{s=1}^{C_{\text{и\_и}}}W_{\text{и\_и}_s}+\sum_{s=1}^{C_{\text{р\_и}}}W_{\text{р\_и}_s}};\ C'_{\text{у\_и}}=C_{\text{у}}-1, \tag{106}$$

где $W_{\text{и(у,р)\_и}_c}$ – КБС элемента, образующего c-й сегмент исполнительной сети;

$C'_{\text{у\_и}}$, $C_{\text{и\_и}}$ и $C_{\text{р\_и}}$ – количество элементов, соответственно, с функцией управления, исполнительной функцией и функцией разведки, образующих сегменты исполнительной сети;

$W_{\text{у\_и}_s}$, $W_{\text{р\_и}_s}$ и $W_{\text{и\_и}_s}$ – КБС, соответственно, s-го элемента с функцией управления, разведки, исполнительной функцией, образующих сегменты исполнительной сети;

$$\kappa_{\text{и}_c}(t)=\begin{cases}\kappa_{c,h}(t), \text{ если в } c\text{-м сегменте нет промежуточных элементов с функцией связи;}\\ \kappa_{c,h}(t)\prod_{q=1}^{C_{\text{св\_и}_c}}\kappa_{\text{св\_и}_{c,q}}(t), \text{ иначе;}\end{cases} \tag{107}$$

$\kappa_{c,h}(t)$ – показатель конфиденциальности информации образующего элемента в c-м сегменте исполнительной сети в момент времени t, см. формулу (108);

$\kappa_{\text{св\_и}_{c,q}}(t)$ – показатель конфиденциальности информации q-го промежуточного элемента связи c-го сегмента исполнительной сети, обеспечивающего передачу информации от образующего сегмент элемента, в момент времени t;

$C_{\text{св\_и}_c}$ – количество элементов связи в c-м сегменте исполнительной сети, через которые идет информационный поток от образующего элемента.

Приведенные в формулах (106) и (107) аналитические зависимости аналогичны для **показателей целостности** $\gamma_{\text{и}}(t)$ **и доступности** $\delta_{\text{и}}(t)$ **информации исполнительной сети** в момент времени t с учетом соответствующей замены в этих формулах показателей конфиденциальности информации.

Если значение показателя доступности информации элемента меньше значения показателя доступности информации нештатного ИТС в нем, и потребитель его информации имеет нештатное ИТС, то передача информации будет выполнена с использованием нештатных ИТС. При этом значение показателя доступности информации этого элемента равно наименьшему из значений показателей доступности информации нештатных ИТС этого элемента и потребителя.

Рассмотрим далее подход к оценке защищенности информации элементов, составляющих узлы сетей противоборствующих ВФ, предложенный в [31].

Пусть в состав i-го элемента входит $\mathscr{E}_i$ ИТС, каждое из которых обеспечивает решение некоторой доли *не*связных задач i-го элемента (то есть ИРЗ, ЗУ, разведка, РЭБ), и $\mathscr{F}_i$ ИТС с задачей связи i-го элемента с другими элементами ВФ. Если одно ИТС в элементе обеспечивает решение связных и других задач (например, АРМ в виде ноутбука с СПО поддержки принятия решения и встроенным Wi-Fi-адаптером), то это ИТС одновременно учитывается в $\mathscr{E}_i$ и $\mathscr{F}_i$.

Значение показателя **конфиденциальности информации** *i*-го **элемента** в момент времени *t* предлагается вычислять следующим образом. Положим, что изначально информация в *i*-м элементе полностью конфиденциальна и содержит в том числе сведения о местоположении этого элемента. Некоторая ее часть обрабатывается с использованием ИТС. Тогда значение рассматриваемого показателя будем считать равным суммарной конфиденциальности необрабатываемой ИТС информации с учетом возможности ее разведки нетехническими методами и конфиденциальности информации, обрабатываемой ИТС в условиях деструктивного воздействия противника.

То есть значение показателя конфиденциальности информации *i*-го элемента в момент времени *t* равно произведению суммарной конфиденциальности, взвешенной по доле решаемых задач, тех ИТС, которые обеспечивают решение несвязных задач, и минимальной конфиденциальности тех ИТС, которые обеспечивают связь этого элемента с другими элементами:

$$\kappa_i(t) = \left(1 - \vartheta_i^{\text{р}}\right)\left(\left(1-\Delta_i\right)Q_{\text{у}_i} + \Delta_i\left(\sum_{s=1}^{|\mathcal{E}_i|}\left(1 - V_{i,s}(t)\right)\varphi_{i,s}\right)\min_{v=1\ldots|\mathcal{E}_i|}\left(1 - V_{i,v}(t)\right)\right), \qquad (108)$$

где $V_{i,s}(t)$ и $V_{i,v}(t)$ – подверженность разведке с применением СПС *s*-го (*v*-го) ИТС в *i*-м элементе в момент времени *t*, см. формулу (24);

Δ_i – уровень информатизации *i*-го элемента, см. формулу (94);

$\varphi_{i,s}$ – КБС *s*-го ИТС, см. формулу (100);

$\vartheta_i^{\text{р}}$ – вероятность разведки информации *i*-го элемента диверсионно-разведывательными подразделениями противника (задается);

$Q_{\text{у}_i}$ – уровень качественного состояния органа управления (расчета, экипажа) *i*-го элемента (методика расчета приведена в [222]);

$|...|$ – количество элементов множества.

Значение показателя *целостности информации i-го элемента* в момент времени *t* равно

$$\gamma_i(t) = \left(1 - \xi_i\right)\left(\left(1-\Delta_i\right)Q_{\text{у}_i} + \Delta_i\left(\sum_{s=1}^{|\mathcal{E}_i|}\left(1 - D_{i,s}(t)\right)\varphi_{i,s}\right)\min_{v=1\ldots|\mathcal{E}_i|}\left(1 - D_{i,v}(t)\right)\right), \qquad (109)$$

где ξ_i – вероятность подмены информации в *i*-м элементе диверсионно-разведывательными подразделениями противника (задается);

$D_{i,s}(t)$ и $D_{i,v}(t)$ – показатели подверженности элемента дезинформации с применением СПС в момент времени *t*, см. формулу (23).

Значение показателя *доступности информации i-го элемента* в момент времени *t* равно

$$\delta_i(t) = \left(1 - \eta_i\right)\left(\left(1-\Delta_i\right)Q_{\text{у}_i} + \Delta_i\left(\sum_{s=1}^{|\mathcal{E}_i|}E_{i,s}(t)\varphi_{i,s}\right)\min_{v=1\ldots|\mathcal{E}_i|}E_{i,v}(t)\right), \qquad (110)$$

где η_i – вероятность уничтожения *i*-го элемента диверсионно-разведывательными подразделениями противника (задается);

$E_{i,s}(t)$ и $E_{i,v}(t)$ – показатели работоспособности *s*-го (*v*-го) ИТС в *i*-м элементе в момент времени *t*, см. формулу (21).

С учетом изложенного эффективность управления боевыми циклами управляющего ВФ в момент времени *t* определяется его возможностями по нарушению целостности, доступности и конфиденциальности информационных потоков в боевых циклах противника (в том числе в результате применения технических средств перехвата информации и СПС средств реализации КА) и защите своих боевых циклов от такого воздействия с использованием следующей формулы [31]:

$$\mathbb{k}_{\text{у}}^{\text{А}}(t)=\gamma_{\text{у}}^{\text{А}}(t)\delta_{\text{у}}^{\text{А}}(t)\left(\begin{array}{c}\left(1-\wp_{\text{р}}\right)\gamma_{\text{и}}^{\text{А}}(t)\delta_{\text{и}}^{\text{А}}(t)+\wp_{\text{р}}\gamma_{\text{р}}^{\text{А}}(t)\delta_{\text{р}}^{\text{А}}(t)\times\\ \times\left(1-\left(\wp_{\text{р}}\kappa_{\text{р}}^{\text{Б}}(t)+\left(1-\wp_{\text{р}}\right)\left(\wp_{\text{и}}\kappa_{\text{и}}^{\text{Б}}(t)+\wp_{\text{у}}\kappa_{\text{у}}^{\text{Б}}(t)\right)\right)\right)\end{array}\right), \qquad (111)$$

где $\kappa_{\text{у}}^{\text{Б}}(t)$ – показатель конфиденциальности информации совокупности управляющих потоков ВФ Б в момент времени *t*;

$\kappa_{\text{и}}^{\text{Б}}(t)$ – показатель конфиденциальности информации совокупности исполнительных потоков ВФ Б в момент времени *t*;

$\kappa_{\text{р}}^{\text{Б}}(t)$ – показатель конфиденциальности информации совокупности разведывательных потоков ВФ Б в момент времени *t*;

$\gamma_{\text{у}}^{\text{А}}(t)$ – показатель целостности информации совокупности управляющих потоков ВФ А в момент времени *t*;

$\gamma_{\text{и}}^{\text{А}}(t)$ – показатель целостности информации совокупности исполнительных потоков ВФ А в момент времени *t*;

$\gamma_{\text{р}}^{\text{А}}(t)$ – показатель целостности информации совокупности разведывательных потоков ВФ А в момент времени *t*;

$\delta_{\text{у}}^{\text{А}}(t)$ – показатель доступности информации совокупности управляющих потоков ВФ А в момент времени *t*;

$\delta_{\text{и}}^{\text{А}}(t)$ – показатель доступности информации совокупности исполнительных потоков ВФ А в момент времени *t*;

$\delta_{\text{р}}^{\text{А}}(t)$ – показатель доступности информации совокупности разведывательных потоков ВФ А в момент времени *t*;

$\wp_{\text{у}}$ – вес совокупности управляющих потоков;

$\wp_{\text{и}}$ – вес совокупности исполнительных потоков;

$\wp_{\text{р}}$ – вес совокупности разведывательных потоков.

Примечания:

1) показатели в формуле (111) определены в интервале [0,1];

2) $\wp_{\text{у}} + \wp_{\text{и}} = 1$, $\wp_{\text{р}} < 1$;

3) в наиболее общем случае имеет место равенство $\wp_{\text{у}} = \wp_{\text{и}} = \wp_{\text{р}} = 0{,}5$.

Пример зависимостей эффективности управления боевыми циклами управляющего ВФ от неизменной во времени вероятности нарушения

целостности или доступности информационных потоков его сетей в результате КА показан на рис. 119.

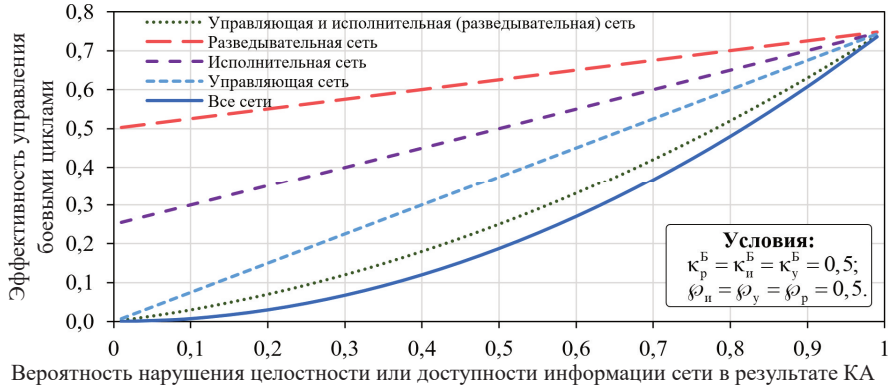


Рис. 119. Эффективность управления боевыми циклами управляющего воинского формирования от неизменной во времени вероятности нарушения целостности или доступности сети в результате кибератак

Шаг 5. Оценка соотношения боевых потенциалов управляющих ВФ. Для оценки соотношения БП управляющих ВФ на оперативном уровне и выше используются модифицированные уравнения Осипова-Ланчестера, в которых численность ВФ заменена на их БП, а интенсивность изменения численности заменена произведением уровня ресурсного обеспечения и эффективности боевых циклов, в которых потоки с развединформацией и донесениями трансформируются в потоки с командами. Формула обобщенной оценки соотношения БП ВФ в момент времени t имеет следующий вид [32]:

$$\mathbb{F}_{С}^{А(Б)}(t) = \sum_{i=1}^{I_{ОС}} \left(W_{ОС_i} \sum_{j=1}^{I_{О_i}} \left(W_{О_{i,j}} \sum_{k=1}^{I_{Т_{i,j}}} \left(W_{Т_{i,j,k}} \mathbb{F}_{Ti,j,k}^{А(Б)}(t) \right) \sqrt{\frac{\mathbb{k}_{рО_{i,j}}^{А(Б)} \mathbb{k}_{уО_{i,j}}^{А(Б)}(t)}{\mathbb{k}_{рО_{i,j}}^{Б(А)} \mathbb{k}_{уО_{i,j}}^{Б(А)}(t)}} \right) \sqrt{\frac{\mathbb{k}_{рОС_i}^{А(Б)} \mathbb{k}_{уОС_i}^{А(Б)}(t)}{\mathbb{k}_{рОС_i}^{Б(А)} \mathbb{k}_{уОС_i}^{А(Б)}(t)}} \right), \quad (112)$$

где $W_{ОС_i} \in (0,1]$, $W_{О_{i,j}} \in (0,1]$ и $W_{Т_{i,j,k}} \in (0,1]$ – показатели важности i-го оперативно-стратегического, j-го оперативного и k-го тактического района, соответственно. Эти показатели задаются. Их сумма на одном уровне иерархии при одном непосредственном начальнике равна единице;

$\mathbb{F}_{Ti,j,k}(t)$ – соотношение БП в k-м тактическом районе j-го оперативного района i-го оперативно-стратегического района в момент времени t;

$\mathbb{k}_{рОС_i}^{А(Б)}$ и $\mathbb{k}_{рО_{i,j}}^{А(Б)}$ – показатели ресурсного обеспечения i-го оперативно-стратегического района, соответственно (методика оценки приведена в [9]);

$\mathbb{k}_{уОС_i}^{А(Б)}(t)$ и $\mathbb{k}_{уО_{i,j}}^{А(Б)}(t)$ – показатели эффективности управления боевыми циклами в районах в момент времени t.

Первая из вышеуказанных замен вполне очевидна, поскольку даже на тактическом уровне под численностью ВФ в настоящем исследовании понимается его эффективная численность, то есть БП, учитывающий КБС ЭБП. Однако замена интенсивности изменения численности произведением уровня ресурсного обеспечения и эффективности боевых циклов у внимательного читателя, на первый взгляд, может вызвать некоторое сомнение. Тем не менее, для оперативного и вышестоящих уровней иерархии такая замена вполне оправдана. Дело в том, что в современном высокоманевренном бою применяется широкая номенклатура высокоточных средств ОП, а полнота и точность единой картины боевой обстановки в режиме реального времени обеспечиваются почти неуязвимыми БПЛА ближнего действия и малой дальности с поддержкой средств космической разведки, недоступных для обычных средств ОП. В таких условиях ключевую роль в обеспечении классической для уравнений Осипова-Ланчестера «скорострельности» (то есть интенсивности изменения численности) играют доступные для воздействия ресурсы и состояние совокупности боевых циклов, в которых обнаруживаются и уничтожаются цели противника.

Также следует отметить, что произведенная замена не противоречит сделанному в п. 4.3.3 выводу о том, что линейный и квадратичный законы Ланчестера характерны только для боев от античности и до середины XX века. Замена касается ВФ, которые непосредственно в бою не участвуют, а управляют ведущими бой подчиненными ВФ, для соотношения БП которых используется модель, предлагаемая в главе 4 настоящей монографии.

С учетом изложенных аналитических выражений схема влияния КА на БП ВФ в контексте вычисляемых информационных, информационно-боевых и боевых показателей показана на рис. 120. В частности, из этой схемы видна взаимосвязь модели процесса распространения СПС и модели конфликта средства реализации КА и ПЗИ ИТС, которые, на первый взгляд, получают исходные данные друг от друга. Особенность такой взаимосвязи состоит в том, что выходные данные модели процесса распространения СПС в одном боевом эпизоде являются исходными данными для модели конфликта средства реализации КА и ПЗИ ИТС в последующем боевом эпизоде. При этом выходные данные модели конфликта средства реализации КА и ПЗИ ИТС в боевом эпизоде являются входными данными для модели процесса распространения СПС в этом же эпизоде.

Таким образом, в рассмотренной в настоящем параграфе методике оценки соотношения БП противоборствующих ВФ, оснащенных АС, в отличие от методик, изложенных в работах [5, 56, 71, 118, 148, 166, 264], учтены КА на АС, применяемые в боевых циклах непосредственно конфликтующих (управляемых) ВФ и в боевых циклах управляющих ими ВФ. Это достигается за счет использования:

- **в тактическом звене** – взвешенной по вероятности реализации последовательности боевых эпизодов в графе позиционной динамики ЭБП ВФ аддитивной свертки показателей соотношения БП управляемых ВФ во всех альтернативных последовательностях

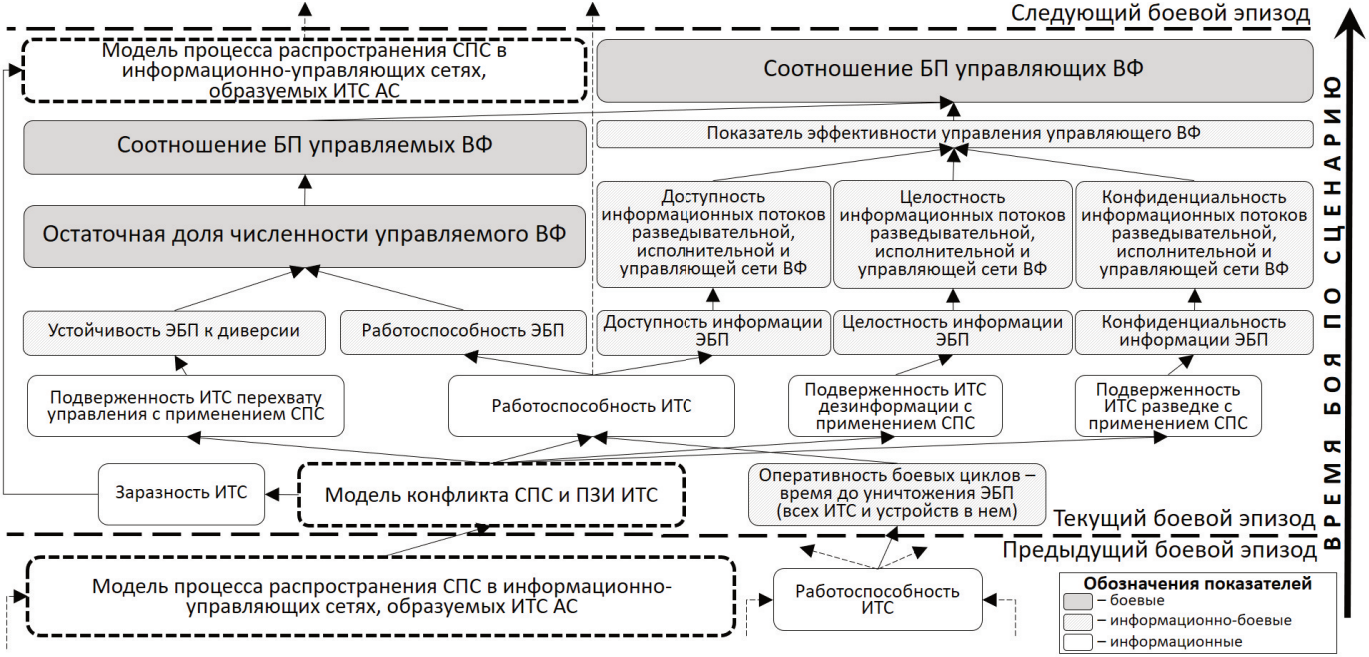


Рис. 120. Схема влияния кибератак на боевой потенциал воинского формирования

боевых эпизодов графа, определяемых в каждом боевом эпизоде как отношение времени уничтожения выигрывающего бой ВФ ко времени уничтожения проигрывающего бой ВФ при неизменных интенсивностях поражающих воздействий сторон, соответствующих этому боевому эпизоду;

- **на высших уровнях** – выводимой из уравнений Осипова-Ланчестера 2-го рода модифицированной формулы оценки соотношения БП противоборствующих ВФ, в которой отношение показателей численности ВФ заменено на аддитивную свертку показателей соотношения БП управляемых ВФ, взвешенную по доле используемых в этих ВФ линейных ЭБП, а показатель интенсивности воздействия заменен на произведение показателей уровня ресурсного обеспечения и эффективности управления боевыми циклами управляющего ВФ, которая рассчитывается с использованием ориентированного мультиграфа каналов информационного взаимодействия структурных компонентов ЭБП ВФ, образуемых в том числе нештатными ИТС, с циркулирующими по этим каналам исполнительными (с донесениями о результатах деятельности и собственном состоянии), разведывательными (с развединформацией) и управляющими (с командами) потоками информации с различной интенсивностью передачи сообщений.

Методика позволяет оценивать влияние ИТВ, включающих РЭП, воздействие мощным ЭМИ и КА, на соотношение БП ВФ в динамике боя.

Роль этой методики в настоящем исследовании состоит в том, что она непосредственно позволяет осуществить анализ влияния эффектов от реализации КА на обеспечиваемые АС в боевых условиях процессы разведки, связи, управления и ОП, взаимосвязанные в рамках боевых циклов ВФ.

Выводы по пятой главе

В пятой главе предложен метод и реализующие его этапы методики оценки эффективности кибератак в боевых действиях. Метод отличается от ранее известных методов, учитывающих влияние на ход и исход боя ресурса средств разведки, связи, управления, огневого поражения и радиоэлектронного подавления, тем, что учитывает совокупность боевых циклов воинских формирований, одновременно обеспечиваемых средствами разведки, управления и связи и подверженных на каждой фазе каждого цикла влиянию совокупности средств огневого поражения, имитации обстановки, радиоэлектронного подавления, поражения электромагнитным излучением и реализации кибератак. Это достигается за счет формирования графа позиционной динамики элементов боевых порядков на основе безызбыточной комбинации траекторно-временных матриц сценариев боя и оценки в каждом боевом эпизоде, формализуемом вершиной этого графа, информационных показателей эффективности функционирования информационно-технических средств автоматизированных систем, применяемых в боевых циклах воинских формирований, информационно-боевых показателей эффективности боевых циклов и боевого показателя соотношения боевых потенциалов противоборствующих сторон. Предложенный метод позволяет оценивать ущерб, наносимый с применением разработанных и ранее известных способов реализации кибератак на боевой потенциал воинского формирования в ходе боевых действий.

Эпиграфом к данной главе является знаменитый закон Мерфи, гласящий, что всякое решение проблемы плодит новые проблемы. Предложенное в монографии решение проблемы разработки методов, моделей и методик обеспечения защищенности от возможных способов реализации кибератак противника программного обеспечения автоматизированных систем, предназначенных для применения в боевых циклах воинских формирований, в процессе их создания, безусловно подтверждает этот закон. Оно порождает следующие проблемы, в первую очередь, практического характера, связанные с переводом со старого на новый уклад следующих процессов:

- прогнозирования эффективности образцов вооружения в условиях современного боя, в котором в том числе применяются кибератаки, и проведения исследований по защите этих образцов от кибератак;
- обоснования требований к защищенности перспективных образцов автоматизированных систем воинских формирований от кибератак противника и проведения испытаний этих образцов на предмет защищенности от кибератак противника;
- проведения исследований по оценке эффективности кибератак в современных боевых условиях.

В следующей главе рассматриваются вопросы методической организации и практической реализации киберзащиты автоматизированных систем воинских формирований, которые, по мнению автора, будут во многом способствовать решению этих проблем.

6 Методика киберзащиты автоматизированных систем воинских формирований и предложения по повышению эффективности функционирования этих систем в условиях кибератак противника

«Если Вы хотите построить корабль, то не собирайте людей рубить деревья, не давайте им заданий и не поручайте никакой работы… Просто заразите их всех своей любовью к морю – и тогда они сами построят корабль».

Антуан де Сент-Экзюпери

6.1 Методика киберзащиты автоматизированных систем воинских формирований

Анализ предметной области приведен в параграфе 1.2, где показано, что сегодня отсутствуют методики, позволяющие обеспечить киберзащиту АС ВФ. В предыдущих главах монографии получены результаты, которые по сути образуют методологический базис такой киберзащиты. Требуемая методика киберзащиты АС ВФ является обобщающей последовательностью применения этого базиса (см. рис. 8).

Ключевая идея, лежащая в основе методики, состоит в том, что обеспечить защищенность АС, применяемых в боевых циклах ВФ, от КА противника, эксплуатирующих уязвимости программных реализаций телекоммуникационных протоколов, в процессе создания этих систем возможно на основе разработки ранее неизвестных способов реализации таких атак и устранения уязвимостей, которые максимизируют БП своего ВФ при заданных ограничениях. Содержание методики показано на рис. 121.

Основные отличия предлагаемой методики от известных методик адаптивного, ситуационного и рефлексивного управления АС в условиях КА [116, 135, 158, 257] состоят в следующем.

Во-первых, в рассмотрении не только известных способов реализации КА, но и в выявлении неизвестных ранее уязвимостей.

Во-вторых, в ориентации на защиту не только информационно-телекоммуникационных систем, но и АС разведки, связи и управления войсками (силами) и оружием, применяемых в боевых циклах ВФ.

В-третьих, в ориентации не на процесс эксплуатации АС, а на процесс их создания.

В-четвертых, в учете не только «конфликтного компонента» в системах обмена данными, но и условий конфликта ВФ, оснащенных АС, эффективность которых кроме качественных параметров систем обмена данными зависит, в первую очередь, от возможностей сторон по взаимному уничтожению.

Рис. 121. Содержание методики киберзащиты автоматизированных систем воинских формирований

При задании неизменными значений наборов варьируемых параметров и учете ограничений методика обеспечивает обоснование параметров защищенности ПО АС, применяемых в боевых циклах ВФ, от КА противника.

Схема обоснования таких параметров, описывающая выполнение этапов 2-3 методики, показана на рис. 122. Обоснование параметров предполагает определение таких параметров защиты АС от КА, при которых выполняется критерий, указанный в выражении (4). Методика позволяет выявлять закономерности влияния конфликтно обусловленных параметров ПО АС (уязвимость для известных ранее и синтезированных эффективных способов реализации КА, периодичность смены настроек протоколов на канальном уровне ЭМВОС и выше, периодичность регламентного поиска и оперативность обнаружения СПС) на эффективность этих систем и выбрать оптимальные значения этих параметров в заданных или достижимых границах боевой эффективности ВФ.

Для оценки влияния способов реализации КА на БП ВФ, в состав которого входит защищаемая АС (этап 2 методики), может использоваться одна из двух моделей боя, представленных в главе 4:

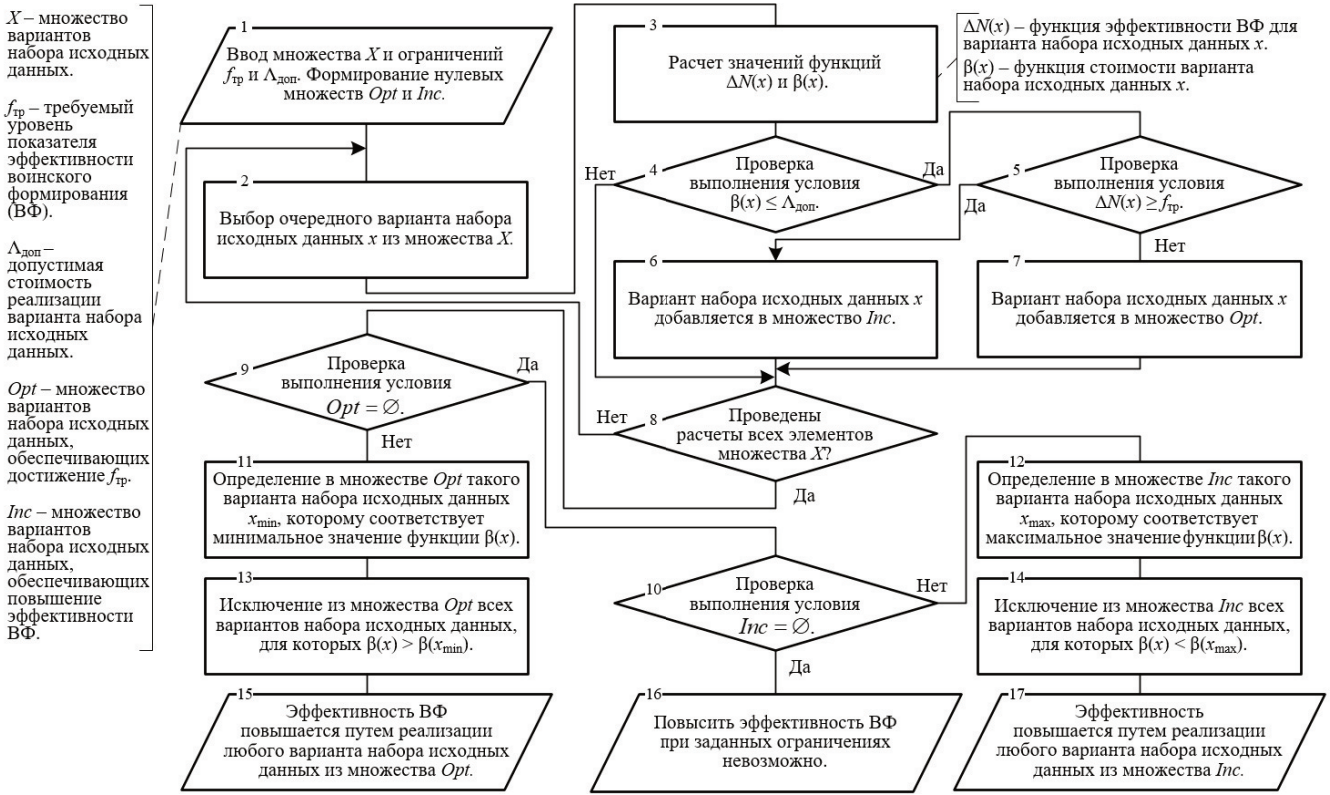


Рис. 122. Схема обоснования параметров защищенности автоматизированных систем, применяемых в боевых циклах воинских формирований, от кибератак противника (этапы 2-3 методики киберзащиты автоматизированных систем воинских формирований)

- модель боя, учитывающая размещение ЭБП ВФ в трехмерном пространстве (см. параграф 4.2) [32];
- эталонная модель боя, не учитывающая размещение ВФ на электронной карте местности (см. параграф 4.3) [28].

При использовании эталонной модели боя оценку следует проводить с учетом показателя ослабления ущерба обороняемым позициям *U*, который используется в формулах (49) и (52) в параграфе 4.3. Вычислять значение этого показателя предлагается следующим способом, впервые изложенным в [29].

Известны классические критерии исходного соотношения численностей ВФ, по которым в наиболее общем случае принимается решение для типовых видов боя [113]:

- для встречного боя – 1,5:1;
- для неподготовленных позиций обороны – 3:1;
- для подготовленных позиций обороны – 6:1.

Следует помнить, что под численностью ВФ в настоящей монографии понимается его эффективная численность, то есть БП, учитывающий КБС ЭБП.

Если органом управления наступающего ВФ принято решение атаковать в заданных условиях, то это означает, что указанный критерий согласно проведенным расчетам выполнен. Неизменная для практики ограниченность ресурсов в наиболее общем случае способствует тому, чтобы расчетные соотношения исходных численностей ВФ не отклонялись от классических критериев. При этом реальное значение соотношения численностей сторон на момент начала боя может варьироваться в соответствии с возможностями сторон и состоянием обороняемых позиций. Например, исходное соотношение, рассчитываемое только по средствам ОП, составляет 2:1, и превосходящее по численности ВФ наступает на неподготовленные позиции обороны, для которых должно выполняться классическое соотношение 3:1. Это может означать, что возможности наступающего ВФ по расчетам его органа управления обеспечивают соотношение 3:1, например, за счет применения КА. В случае скрытного оборудования обороняемых позиций обороняющееся ВФ может увеличить свой БП, приведя тем самым соотношение БП, например, с 3:1 до 2:1, что, по всей видимости, приведет к невозможности выполнения боевой задачи наступающим ВФ.

С учетом этого для определения значения показателя ослабления ущерба обороняемым позициям *U* выполняется следующий алгоритм.

Шаг 1. Значение *U* для наступающего и обороняющегося ВФ задается равным единице.

Шаг 2. Проводится моделирование боя с заданными исходными данными ВФ без применения КА при типовом соотношении численностей для заданных боевых условий (например, для неподготовленных позиций обороны 3:1) и определяется остаточная доля численности наступающего ВФ.

Шаг 3. Значение показателя *U* снижается до такого значения, при котором остаточная доля численности наступающего ВФ равна 75 %, если иное не обосновано.

Ущерб от реализации КА в методике рассчитывается как разность δN остаточной доли численности ВФ, оснащенного защищаемой АС, без применения мероприятий по защите от КА N_0 и с применением этих мероприятий $N_{КА}$ по тривиальной формуле

$$\delta N = N_0 - N_{КА}. \quad (113)$$

Следует помнить, что БП ВФ определяется в диапазоне от минус 100 до 100 %. Он положителен при победе ВФ и отрицателен при его поражении. Отрицательное значение БП ВФ равно остаточной доле численности победившего противника.

В [29] предложен вариант оценки ущерба от КА с использованием эталонной модели как разности единицы и остаточной доли численности ВФ, применяющего АС, во встречном бою с аналогичным ВФ, эксплуатирующим выявленные уязвимости АС.

Таким образом, методика киберзащиты АС ВФ отличается от методик, изложенных в работах [116, 135, 158, 257], ориентированных на защиту информационного ресурса АС в процессе их эксплуатации и ранее известные способы реализации КА без учета боевой обстановки, тем, что ориентирована на процесс создания (модернизации) АС, применяемых в боевых циклах ВФ, ранее неизвестные способы реализации КА и боевую обстановку, в которой эти системы обеспечивают процессы разведки, связи, управления и ОП. Это достигается за счет определения условий функционирования защищаемой АС при использовании противником КА, разработки и осуществления множества тестовых способов реализации КА на ее телекоммуникационное оборудование на основе спецификаций телекоммуникационных протоколов, оценки влияния эффектов от новых и ранее известных способов реализации КА на уровне информационных, информационно-боевых и боевых показателей в совокупности условий и факторов боевой обстановки с детализацией до полумарковских процессов функционирования ИТС и устройств в ЭБП противоборствующих сторон, и выбора множества устраняемых уязвимостей АС в соответствии с заданными ограничениями. Методика позволяет повысить БП ВФ, оснащенного АС, до требуемого уровня или максимально приблизиться к нему в заданных условиях.

6.2 Предложения по повышению эффективности функционирования автоматизированных систем воинских формирований в условиях кибератак противника

Предложенный в монографии научно-методический аппарат ориентирован, в первую очередь, на применение в ходе создания (модернизации) АС ВФ на этапе «Тестирование комплексов программ» стадии «Рабочая документация» фазы «Разработка» (по ГОСТу [87]). При проведении работы «Оценка качества комплексов программ» предлагается проводить следующую дополнительную последовательность действий по повышению эффективности функционирования АС, применяемых в боевых циклах ВФ, в условиях КА противника:

1) *разработка* моделей ЛП процедур телекоммуникационных протоколов, используемых в ИТС АС, на основе их спецификации;

2) *формирование* на основе этих моделей модели РП каждой процедуры и *генерирование* тестовых способов реализации КА;
3) *проведение* натурного эксперимента по реализации КА на такие количество и номенклатуру ИТС, которые могут считаться достаточными для проверки всех тестовых способов реализации КА;
4) *выявление* фактов нештатного функционирования ИТС в течение и в результате каждого тестового способа реализации КА и *определение* эффекта от каждого способа на уровне эффективности функционирования АС ВФ;
5) *оценка* ущерба от каждого способа реализации КА на АС, применяемые в боевых циклах ВФ, и определение множества уязвимостей, подлежащих устранению при заданных ограничениях.

Схема технологического процесса киберзащиты АС ВФ в нотации IDEF0 метода функционального моделирования Structured Analysis and Design Technique [202] представлена на рис. 123. В этой нотации процессы системы и потоки данных представляются как блоки и дуги (стрелки), соответственно. Управляющая информация входит в блок сверху, входная информация, подвергающаяся обработке, – с левой стороны блока, результаты (выход) показываются с правой стороны, а субъект, осуществляющий процесс, представляется дугой, входящей в блок снизу. В состав входных данных для процесса входят спецификации телекоммуникационных протоколов АС ВФ, описательные модели типовых боевых эпизодов с применением защищаемых или целевых ИТС, а также образцы ИТС защищаемой АС. На выходе кроме эффективных способов реализации КА возможно получить ряд рекомендаций, учет которых при создании (модернизации) АС способен повысить эффективность их функционирования в условиях КА.

Для обеспечения процесса оценки эффективности способов реализации КА, показанного на рис. 123, предлагается создать перспективный РМК, реализующий метод, модели и методики, изложенные в главах 3-5 монографии. Краткое описание РМК приведено в п. 4.2.3. Он может применяться не только в исследовательских, но и в штабных целях. Задачами РМК в штабных целях являются [39]:

1) нанесение боевой обстановки на электронную карту местности и обновление в режиме реального времени по данным от сопряженных средств видовой и параметрической разведки и датчиков на своих ЭБП с применением искусственного интеллекта и полномасштабной технологии виртуальной реальности;
2) автоматическое целераспределение собственных и придаваемых комплектов вооружения и военной техники с функциями разведки, связи, ОП, управления, РЭП, КА, воздействия мощным ЭМИ, имитации обстановки, НелВ, ПсВ, РХБВ и аэрозольного противодействия;
3) оптимизация траекторий маневра и позиций ЭБП своего ВФ;
4) расчет потребности в боеприпасах и горюче-смазочных материалах при выполнении боевых задач;

Рис. 123. Схема технологического процесса киберзащиты автоматизированных систем воинских формирований

5) расчет соотношения БП ВФ с детализацией до процессов работы отдельных ИТС с учетом свойств информации в боевых циклах, ТТХ комплектов вооружения и военной техники и их позиций на местности, а также прогнозирование хода и исхода боя и оценка ущерба, наносимого противостоящему ВФ, по этапам выполнения задач;
6) расчет потребности в придаваемых и поддерживающих силах и средствах при выполнении боевых задач (в том числе в авиационном ресурсе, ресурсе средств береговой охраны, ресурсе сил флота);
7) расчет потребности в мероприятиях инженерного обеспечения, в медицинской помощи, ремонтно-восстановительных работах и восполнении потерь личного состава и образцов вооружения (по видам ремонта);
8) расчет вклада формирований родов войск и образцов вооружения с различными функциями (в том числе роботизированных средств) в ущерб, наносимый противнику, включая оценку эффективности информационного противоборства;
9) расчет темпа продвижения и устойчивости позиций в обороне;
10) доведение задач и обобщение результатов расчетов с использованием формализованных боевых документов.

В исследовательских целях кроме обеспечения технологического процесса киберзащиты АС ВФ предлагаемый РМК в полном объеме сможет решать уже реализованные и перспективные задачи РМК СВ [82]. Структурная схема перспективного РМК показана на рис. 124.

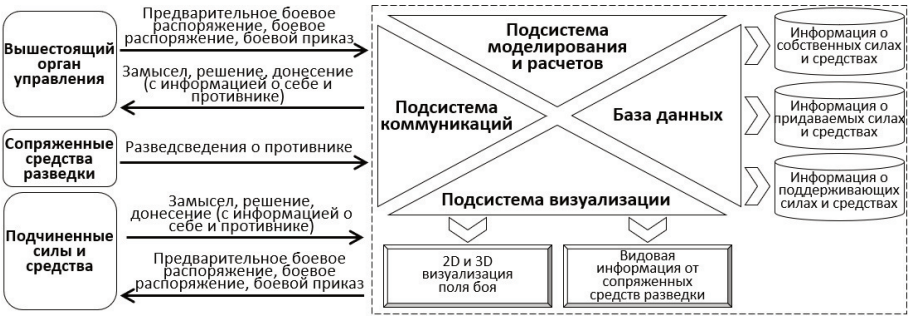


Рис. 124. Структурная схема перспективного расчетно-моделирующего комплекса

Результаты расчетов, выполненные перспективным РМК на уровне штаба батальона/полка/бригады, могут обобщаться и ретранслироваться вышестоящим штабам до оперативно-стратегического командования (ОСК) и центра управления обороной (ЦУО) включительно. Варианты размещения перспективного РМК показаны в таблице 10.

Исходя из особенностей размещения, перспективный РМК обеспечивает возможность работы в одном из трех основных режимов: «Обобщение», «Обобщение и ретрансляция» и «Расчет». Диаграмма потоков данных в различных режимах работы перспективного РМК показана на рис. 125.

Таблица 10 — Варианты размещения расчетно-моделирующего комплекса

Вариант размещения	Центр управления обороной	Штаб ОСК	Штаб армии/ корпуса	Штаб дивизии/ бригады	Штаб полка/ батальона
1	–	–	–	–	+
2	–	–	–	+	+/–
3	–	–	+	+	+/–
4	–	+	+	+	+/–
5	+	+	+	+	+/–

Обозначения:
+ обязательное размещение; +/– необязательное размещение; – не размещается.

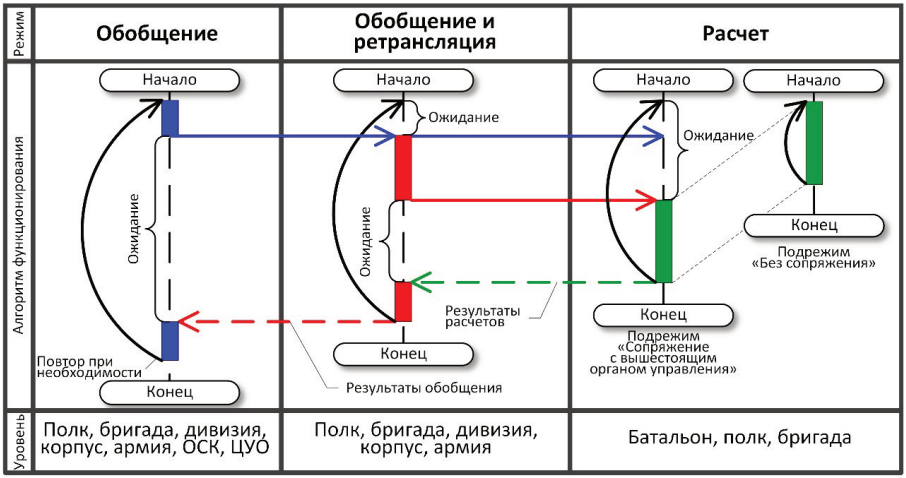


Рис. 125. Диаграмма потоков данных в различных режимах работы расчетно-моделирующего комплекса

В режиме «Расчет» для исходных данных о противнике и своих силах и средствах формируется граф позиционной динамики боя, для каждого боевого эпизода которого последовательно выполняются следующие этапы.

Этап 1 – создание в ЭБП списков материальных и информационных целей ВФ, которые доступны средствам разведки. Список материальных целей включает цели противника, которые подвергаются ОП, РХБВ, ПсВ, НелВ и ОЭП. Список информационных целей включает ИТС противника, работу которых необходимо блокировать средствами и боеприпасами РЭБ (забрасываемыми передатчиками помех). В зависимости от наличия АС управления списки целей могут формироваться в отдельных ЭБП, их группах или в ВФ в целом.

Этап 2 – целераспределение средств и боеприпасов в ЭБП. Для целераспределения боеприпасов огнестрельного оружия с различными целевыми нагрузками проводится разделение текущего боевого эпизода на субэпизоды так, что продолжительность каждого субэпизода равна периоду между моментами приведения в готовность ЭБП в текущем боевом эпизоде.

Пример разделения на пять субэпизодов боевого эпизода, в котором применяются 15 ЭБП с различными временами готовности, показан на рис. 126. На этом рисунке показано, что боевой эпизод разделяется моментами готовности различных ЭБП. Каждому субэпизоду в списке материальных целей соответствует некоторое количество целей, которое обнаружено средствами разведки до завершения этого субэпизода. То есть обнаруженные в течение субэпизода цели распределяются по средствам воздействия в текущем и последующих субэпизодах.

Этап 3 – расчет времен до уничтожения ЭБП. Каждый контур, в котором добываются и анализируются разведсведения, принимается решение и осуществляется воздействие, образует боевой цикл. Возможность выполнения этапов каждого боевого цикла определяется тем, успеют ли участвующие в этом цикле ЭБП выполнить свои функции в условиях противодействия противника.

Этап 4 – расчет системы показателей эффективности ВФ. При расчете учитывается наличие критически важных элементов гражданской инфраструктуры и ЭБП в составе противоборствующих сторон, уничтожение которых автоматически приводит к поражению, несмотря на текущее соотношение БП.

Этап 5 – автоматическая корректировка графа позиционной динамики боя в случаях отступления или полного уничтожения ЭБП, обнаружения ими минного поля, исчерпания боеприпасов или горюче-смазочных материалов, срабатывания датчиков присутствия противника, уничтожения мобильной базы ЭБП, завершения аэрозольного противодействия и др.

Возможности предлагаемого РМК позволят применять его при подготовке к бою для задания альтернативных вариантов поведения противоборствующих сторон и оценки динамики соотношения БП сторон для этих вариантов, а также в ходе боя для оценки соотношения БП сторон в складывающихся условиях. Используемая в нем аналитическая модель боя в каждом боевом эпизоде учитывает типовые алгоритмы функционирования ВФ в бою, которые пользователь РМК может корректировать. Однако даже при самых совершенных алгоритмах этот комплекс не имеет цели заменить командира. РМК нацелен на то, чтобы помочь командиру в складывающихся всегда крайне сложных условиях боевой обстановки быстро получить ответ на вопрос: каким будет соотношение БП в бою, если обе стороны действуют «некоторым задаваемым способом», комплексно применяя самые современные образцы вооружения. И именно предполагаемый при планировании боя или реально складывающийся в бою «способ» действий представляет собой наиболее критичный фактор, влияющий на адекватность результатов, получаемых с использованием реализуемого в РМК метода.

В процессе планирования боя источником данных для определения начальных позиций ЭБП и построения альтернативных траекторий их движения даже при поддержке самых совершенных математических методов группового управления подвижными объектами является орган управления ВФ, то есть командир и его штаб. Степень достоверности этих данных всецело

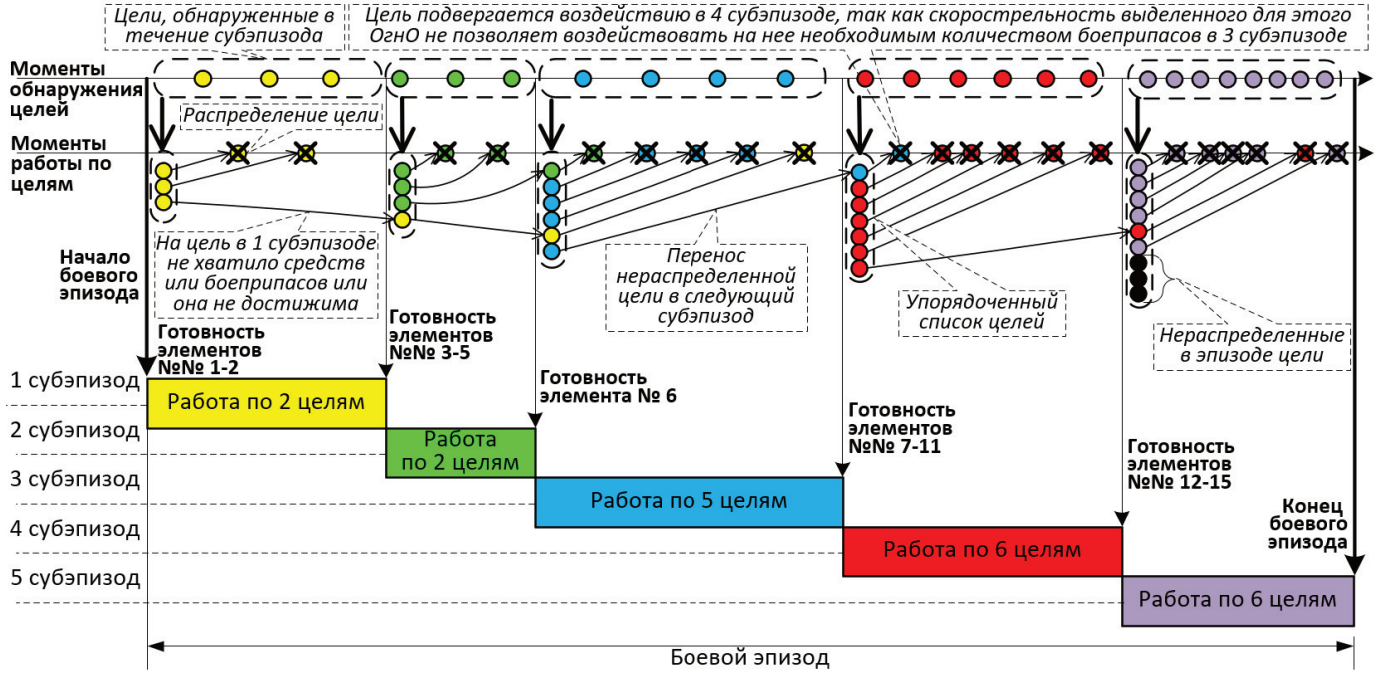


Рис. 126. Пример разделения боевого эпизода на субэпизоды в перспективном расчетно-моделирующем комплексе

определяется достоверностью имеющейся информации о предстоящем бое, а также уровнем боевой подготовки и боевого опыта личного состава органа управления. Очевидно, что при низкой достоверности исходных данных ценность результатов моделирования будет ничтожной. Гораздо менее весомым, но все-таки значимым для используемого метода является время, доступное для принятия решения. При минимальном времени на проведение расчетов за счет трансформации траекторий движения ЭБП бой «сжимается» в один боевой эпизод, расчеты для которого будут весьма грубыми. Однако даже в таком случае полученное соотношение БП поможет командиру получить ответ на ключевой вопрос: обороняться или наступать.

Следует отметить, что способы в вооруженной борьбе имеют строго выраженную иерархию, показанную на рис. 127 [32].

Рис. 127. Иерархия способов в вооруженной борьбе

На *первом уровне* (низшем), то есть в основе эффективности ВФ в боевых действиях, лежат способы воздействия. Способы этого уровня характеризуют физические процессы (факторы и условия) воздействия без привязки к пространственным характеристикам образцов вооружения и объектов воздействия. Эффективность этих способов доказывается теоретически или натурным методом в лабораторных условиях.

На *втором уровне* находятся способы применения образцов вооружения. Эти способы отличаются от способов первого уровня следующим:

- включают один или несколько способов воздействия, но рассматривают их с позиции «черного ящика»;
- характеризуют технические особенности образцов вооружения, включая их носители;
- характеризуют особенности размещения в пространстве образцов вооружения и объектов воздействия;
- характеризуют особенности процессов разведки и управления, необходимых для эффективного применения образцов вооружения;

- не привязаны к конкретным условиям боевой обстановки;
- эффективность этих способов доказывается при проведении испытаний или военно-технических экспериментов.

На *третьем уровне* (наивысшем) находятся способы применения сил (подразделений, частей, соединений, объединений). Общеизвестно, что способ применения сил включает избранный порядок воздействия на объекты противника, сосредоточения усилий, построения боевого порядка, а также маневра и управления силами и средствами.

Эти способы отличаются от способов второго уровня следующим:

- включают один или несколько способов применения образцов вооружения, но рассматривают их с позиции «черного ящика»;
- характеризуют организационные особенности сил и порядок их взаимодействия с другими силами;
- учитывают конкретные условия боевой обстановки;
- характеризуют особенности процессов разведки, координации и управления различными образцами техники, необходимых для эффективного применения сил;
- эффективность этих способов доказывается на учениях, при выполнении специальных задач или в боевых условиях.

Предлагаемый в настоящей монографии научно-методический аппарат ориентирован на разработку способов первого уровня и на оценку эффективности способов второго и третьего уровней иерархии.

Таким образом, в предложениях по повышению эффективности функционирования АС ВФ в условиях КА противника в отличие от применяемой в настоящее время проверки защищенности от известного перечня способов реализации КА, регламентируемой руководящими документами [219, 220], предлагается учесть ранее неизвестные способы. Это достигается за счет выполнения на этапе «Тестирование комплекса программ» фазы «Разработка» при проведении работы «Оценка качества комплексов программ» дополнительной последовательности действий по разработке моделей ЛП процедур используемых телекоммуникационных протоколов на основе их спецификации, формированию на основе этих моделей РП каждой процедуры и генерированию тестовых способов реализации КА, проведению полунатурного эксперимента по реализации КА на ИТС с установленным на них СПО в количестве и номенклатуре, достаточными для проверки всех тестовых способов, и выявлении фактов нештатного функционирования ИТС в течение и в результате реализации каждой КА, определению эффекта от реализации каждой КА на уровне эффективности функционирования АС и оценке ущерба от каждого способа реализации КА на АС, применяемых в боевых циклах ВФ, в интересах определения множества уязвимостей, подлежащих устранению при заданных ограничениях. Это позволяет еще в процессе разработки выявлять и устранять новые критически важные уязвимости программных реализаций процедур телекоммуникационных протоколов АС ВФ.

6.3 Результаты применения методики киберзащиты автоматизированных систем воинских формирований

Рассмотрим пару примеров боевых ситуаций, при анализе которых наглядно просматривается польза от применения методики киберзащиты АС ВФ и в целом научно-методического аппарата, предлагаемого в монографии.

Первая ситуация – это известный в военной истории боевой эпизод преодоления средствами воздушного нападения коалиции западных стран ПВО Ирака во время начальной стадии операции «Буря в пустыне» в 1991 году. Тогда коалицией было заблаговременно внедрено СПС «AF/91» в драйвер принтера, подключенного к информационно-управляющей сети иракской системы ПВО [116]. Учитывая недостаток достоверных исходных данных, можно предположить, что уровень информатизации сторон в том бою был не менее 80 %.

Общеизвестно, что соотношение численностей сторон в этой операции в целом оценивается на уровне 2,7:1. Весьма вероятно, силы коалиции в рассматриваемой боевом эпизоде имели и большее преимущество, но будем исходить из наихудшего для них варианта, когда в этом эпизоде соотношение было таким же, как и во всей операции. Оборонявшаяся сторона имела оборудованные позиции. Обеими сторонами применялось высокоточное оружие ($P_{1бп\_кр} = P_{1бп\_син} = 0{,}8$), а оперативность боевых циклов (включая сетецентрический доступ к развединформации) и вероятность разведки средств воздушного нападения коалиции были не выше значений таких же параметров иракских средств ПВО советского производства (среднее время боевого цикла сторон равно 15 с, вероятность разведки сторон равна $P_{р\_кр} = P_{р\_син} = 0{,}99$).

Коэффициент снижения ущерба обороняемым позициям у иракских средств ПВО при предполагаемой потере 25 % численности сил коалиции составил $U = 0{,}2$. Полученные с применением эталонной модели (см. главу 4, [28]) зависимости остаточной доли численности коалиции при различных вероятностях КА на все подсистемы (разведки, связи, управления и ОП) иракской ПВО для указанных исходных данных приведены на рис. 128.

На этом рисунке показано, что без применения КА иракская система ПВО должна была отразить авианалет с остаточной численностью 16 %. КА обеспечивают успех авианалета даже в том случае, если СПС поразит от 5 до 40 % иракской системы ПВО, а при поражении более 40 % победа коалиции будет уверенной. Наиболее вероятная эффективность КА в этом бою по экспертным оценкам составляла от 20 до 50 %. Тем не менее даже при 20 %, судя по рис. 128, имеет место существенное изменение БП сторон с 16 % остаточной численности иракской системы ПВО до 46 % остаточной численности коалиции (то есть $\delta N \geq 62$ %) [28].

Безусловно, приведенные результаты расчетов следует рассматривать только в качестве демонстрации возможностей предлагаемого научно-методического аппарата в части оценки эффективности КА, поскольку достоверные исходные данные об указанном боевом эпизоде у автора

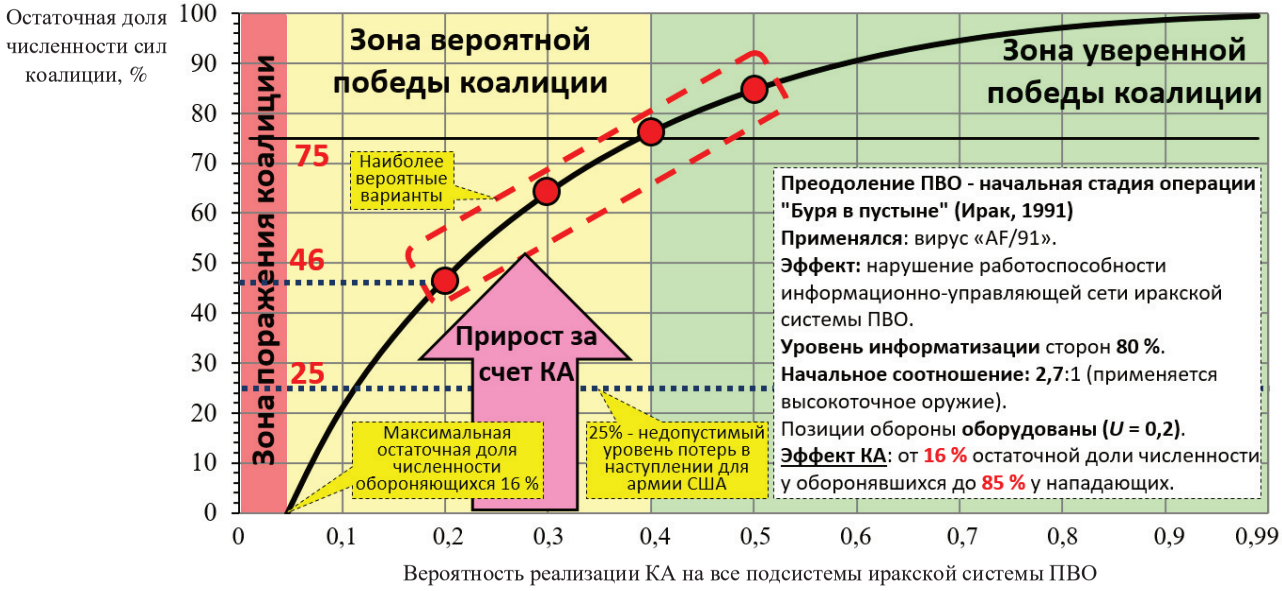


Рис. 128. Эффективность КА на начальной стадии операции «Буря в пустыне»

отсутствуют. Тем не менее, эти результаты наглядно показывают, что пренебрегать эффектом от реализации КА в боевых действиях не стоит.

Конечно же, редко можно внедрить СПС в АС ВФ противника до начала боя. Весьма вероятной представляется другая боевая ситуация, в которой средства ОП применяются в основном прямой наводкой, а радиосвязь обеспечивает некоторую долю боевых циклов ВФ. Рассмотрим эту ситуацию для следующих гипотетических исходных данных.

Вторая ситуация. Оборонительный бой мотострелкового батальона ВС РФ, оснащенного перспективными радиостанциями Р-187-П1 и Р-168МР, который усилен танковой ротой. Такой состав обороняющегося ВФ обоснован ранее в параграфе 3.7. Оборона является маневренной, что обусловливает необходимость использования радиосвязи для координации ЭБП всех уровней иерархии до солдата включительно в районе ответственности до 10 км по фронту и в глубину согласно уставам СВ.

Противник наступает силами мбр «Страйкер» ВС США и применяет комплексы разведки и РЭБ AN/MLQ-40(V) «Prophet» батальона разведки, которые используют аппаратуру станций помех AN/JSQ-146(V) только для реализации КА, скрытно блокирующих 99 % радиостанций Р-187-П1 и Р-168МР. Такая эффективность КА объясняется тем, что средства реализации КА не требуют превышения уровня помехового сигнала над полезным сигналом, являясь эффективными даже при приеме их сигнала на пороге чувствительности радиоприемника. Противник не использует станции помех AN/JSQ-146(V) для радиоподавления в целях обеспечения собственной живучести [29]. Других радиостанций у обороняющихся нет.

ЭБП обороняющегося ВФ до начала боя частично обеспечены средствами проводной связи. После предшествующего атаке массированного ракетно-артиллерийского удара, который нанесен силами артиллерийского дивизиона мбр «Страйкер», по экспертным оценкам доля линий радиосвязи в системе связи обороняющегося ВФ составляет от 70 до 90 %. Наиболее вероятные значения доли боевых циклов обороняющегося ВФ, обеспечиваемых радиосвязью, составляют от 50 до 80 %. Это обусловлено отсутствием радиостанций Р-187-П1 и Р-168МР в боевых циклах подразделений танковой роты и возможностью использовать для обмена информацией между ЭБП мсб акустические и визуальные каналы связи. Вероятность поражения цели одним боеприпасом равна $P_{1бп\_кр} = P_{1бп\_син} = 0{,}8$. Среднее время боевого цикла сторон равно 15 с (время обнаружения – 5 с, время передачи информации – 5 с, время обработки управляющей информации – 4 с, время воздействия одним боеприпасом – 1 с). Средства разведки обеспечивают сторонам полную ситуационную осведомленность, то есть $P_{р\_кр} = P_{р\_син} = 0{,}99$. Коэффициент ослабления ущерба обороняемым позициям для данных условий боя равен 0,51.

Противник планирует бой, исходя из классического критерия 3:1. Исключая обеспечивающие силы и средства, соотношение численности ЭБП сторон составляет 180:60. В качестве ЭБП рассматривается отделение (боевой расчет). В конце боя противник планирует иметь остаточную численность своего ВФ, равную не менее 75 % от исходной численности (см. [113]). Для

сбережения своих сил и средств он дополнительно сокращает свою численность, полагаясь на высокую эффективность КА. То есть, например, в случае, если доля линий радиосвязи в системе связи обороняющегося ВФ равна 70 %, а доля боевых циклов этого ВФ, обеспечиваемых системой связи, равна 80 %, то противник применяет не 180 ЭБП, а 129 ЭБП.

Однако до начала рассматриваемого боя в радиостанциях Р-187-П1 и Р-168МР уязвимости устранены в ходе мероприятий по киберзащите, выполненных в соответствии с предложениями в параграфе 6.2.

Результаты моделирования для таких исходных данных показаны на рис. 129. Из этого рисунка видно, что устранение уязвимостей радиостанций при наиболее вероятных диапазонах значений исходных данных снижают время боевого цикла обороняющегося ВФ с 44…20,9 с до 15 с, приводя к снижению остаточной доли численности противника на 10…48 %. И даже если доля боевых циклов обороняющегося ВФ, обеспечиваемых системой связи, составляет 20 %, противнику наносится урон в 1,48 %, что равно потере им, как минимум, двух ЭБП.

Как следствие, следует констатировать, что за счет заблаговременного устранения уязвимостей ПО АС в маневренном оборонительном бою мотострелкового батальона, усиленного танковой ротой, длительность боевых циклов этого ВФ сокращается более чем в 1,4 раза, что приводит к снижению остаточной доли численности противника не менее чем на 10 %.

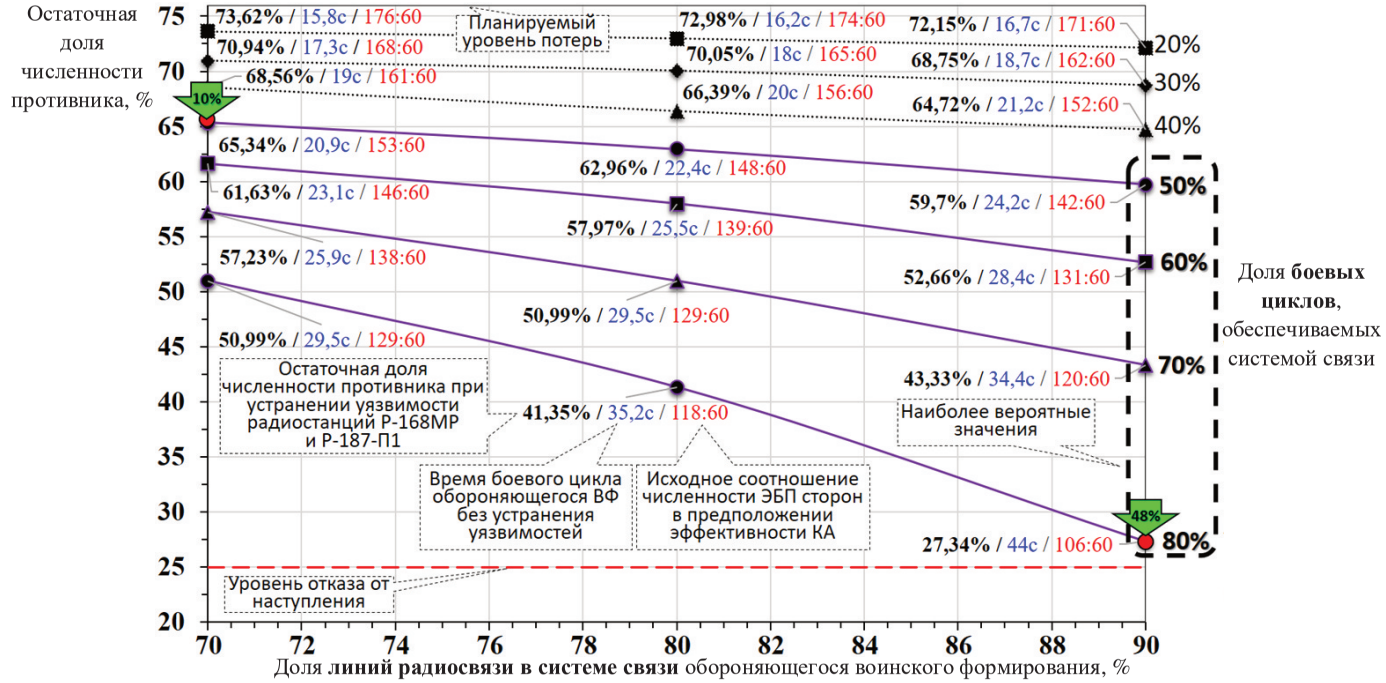


Рис. 129. Эффективность киберзащиты на примере автоматизированной системы связи оборонительного маневренного боя мотострелкового батальона, усиленного танковой ротой, или мотопехотного батальона бригады «Страйкер»

Выводы по шестой главе

В шестой главе представлены методика киберзащиты автоматизированных систем воинских формирований и предложения по повышению эффективности функционирования этих систем в условиях кибератак противника.

Обеспечение защищенности от кибератак программного обеспечения автоматизированных систем, применяемых в боевых циклах воинских формирований, может быть достигнуто заблаговременно в процессе их создания (модернизации) на основе генерирования необходимого и достаточного множества тестовых способов реализации кибератак для используемых в этих системах телекоммуникационных протоколов, оценки влияния вновь разработанных и ранее известных способов на боевой потенциал воинского формирования, применяющего защищаемые системы, и выбора таких подлежащих устранению уязвимых мест программного обеспечения, которые наносят наибольший суммарный ущерб воинскому формированию при заданных ограничениях.

Предложения, разработанные на основе полученных в монографии научных результатов, при их применении в процессе создания (модернизации) автоматизированных систем позволяют сократить длительность боевых циклов применяющего их воинского формирования более чем в 1,4 раза, чем способствуют снижению боевого потенциала противника не менее чем на 10 %.

Полученные результаты свидетельствуют о достижении заявленной в параграфе 1.3 цели настоящего исследования, состоящей в повышении эффективности функционирования автоматизированных систем, применяемых в боевых циклах воинского формирования, на основе обеспечения защищенности их программного обеспечения от кибератак противника.

Заключение

«Даже если ваше объяснение настолько ясно, что исключает всякое ложное толкование, все равно найдется человек, который поймет вас неправильно!»

Закон Мерфи

В монографии изложено решение проблемы разработки методов, моделей и методик обеспечения защищенности от ранее неизвестных способов реализации кибератак противника программного обеспечения автоматизированных систем, применяемых в боевых циклах воинских формирований, в процессе создания этих систем. Это решение состоит в применении следующих вновь разработанных компонентов научно-методического аппарата киберзащиты автоматизированных систем воинских формирований.

1. Модель процесса информационного взаимодействия информационно-технических средств автоматизированных систем по известной процедуре телекоммуникационного протокола и метод генерации кибератак на телекоммуникационное оборудование. Они позволяют определять границы интервалов преждевременной, своевременной и запаздывающей доставки сообщений, которые используются в ходе кибератак, и разрабатывать необходимое и достаточное множество способов реализации таких атак на программное обеспечение телекоммуникационных протоколов, используемых в автоматизированных системах воинских формирований.

2. Совокупность взаимосвязанных моделей процессов функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований, и компонентов этих систем в условиях кибератак противника. Данные модели позволяют выявлять закономерности влияния кибератак на процесс взаимного уничтожения элементов боевых порядков противоборствующих сторон в рамках одного боевого эпизода, предусматривающего статичное положение этих элементов на поле боя и неизменную интенсивность воздействий на «материю» и «информацию».

3. Метод и реализующие его этапы методики оценки эффективности кибератак в боевых действиях, которые позволяют оценивать ущерб, наносимый с применением вновь разработанных и ранее известных способов реализации кибератак на боевой потенциал воинского формирования в ходе боевых действий.

4. Методика киберзащиты автоматизированных систем воинских формирований и предложения по повышению эффективности функционирования этих систем в условиях кибератак противника,

позволяющие выявлять уязвимости программной реализации телекоммуникационных протоколов, устранение которых при заданных ограничениях максимизирует боевой потенциал своего воинского формирования.

В монографии при моделировании процесса функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований, впервые учтен новый фактор деструктивного воздействия противника, состоящий в реализации кибератак. Предложены новые методы генерации кибератак на телекоммуникационное оборудование, оценки эффективности кибератак в боевых действиях и методика киберзащиты автоматизированных систем воинских формирований. Также выявлены новые закономерности влияния кибератак на эффективность функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований.

Элементом новизны настоящей работы также является то, что в ней впервые применен математический аппарат теории полумарковских процессов для моделирования процесса взаимного влияния пространственно распределенных элементов боевых порядков воинских формирований, оснащенных автоматизированными системами и применяющих в бою средства разведки, связи, управления, огневого поражения, радиоэлектронного подавления, воздействия мощным электромагнитным излучением, имитации обстановки и реализации кибератак.

С практической точки зрения польза монографии состоит в обосновании технических путей повышения эффективности функционирования автоматизированных систем разведки, связи и управления войсками (силами) и оружием, применяемых в боевых циклах воинских формирований, в условиях кибератак противника за счет совершенствования процесса создания (модернизации) программного обеспечения этих систем. Сформулированные на основе выявленных закономерностей предложения могут использоваться в процессе сертификации защищенности программного обеспечения критически важных автоматизированных систем информационной инфраструктуры от кибератак, а также при разработке перспективных средств защиты сетей цифровой радиосвязи критически важных объектов от кибератак. Выполнение этих предложений позволяет превратить процесс выявления новых уязвимостей, ранее считавшийся эмпирической деятельностью специалистов высшей квалификации с непрогнозируемым временем завершения, в технологию, применимую в условиях жестких временных ограничений.

Полученные в работе результаты в дальнейшем могут быть полезны:

- при обосновании требований к перспективным образцам автоматизированных систем воинских формирований в части их защищенности от кибератак противника;
- при проведении предварительных и государственных испытаний образцов автоматизированных систем воинских формирований в части их защищенности от кибератак противника;

- при проведении исследований, связанных с оценкой эффективности кибератак в боевых условиях и защитой от них автоматизированных систем воинских формирований.

Приоритетными направлениями дальнейшего развития результатов настоящего исследования являются:

- синтез тестовых сценариев реализации кибератак на автоматизированные системы в боевых условиях. Для этого целесообразно применять предложенный метод генерации кибератак на телекоммуникационное оборудование и метод оценки эффективности кибератак в боевых действиях в сочетании с известными методами комбинаторного анализа и динамического программирования;
- адаптивный синтез траекторий движения элементов боевых порядков воинских формирований при меняющихся условиях боевой обстановки. Это направление может быть разработано на основе предложенной в монографии совокупности взаимосвязанных моделей процессов функционирования автоматизированных систем, применяемых в боевых циклах воинских формирований, с применением методов теории выбора, математического аппарата темпоральной логики, используемого для верификации процессов функционирования сложных технических систем, и группового управления подвижными объектами;
- адаптивная оптимизация целераспределения элементов боевых порядков воинских формирований в динамике боя. В этом направлении целесообразно применение методов искусственного интеллекта и теории игр в сочетании с предложенной в монографии моделью процессов функционирования автоматизированных систем в боевом эпизоде.

Настоящая монография по существу содержит ответ на вопрос: как влияют новые цифровые информационные (в том числе телекоммуникационные) технологии, внедряемые в образцы вооружения, на ход и исход современного боя? В целом можно констатировать, что эффект от этого влияния пропорционален уровню информатизации этих образцов. Изложенные результаты свидетельствуют о том, что киберпространство не только в перспективных, но уже и в современных вооруженных конфликтах может являться сферой ведения боевых действий. И военные эксперты ведущих стран мира, закрепивших эту сферу в доктринальных документах, не ошибались. Место кибератакам есть и в тактическом звене, а эффект от гаубицы в бою может быть значительно меньше, чем эффект от кибератаки. Нескрытное средство радиоэлектронной борьбы в бою будет жить недолго и действительно может значительно уступать тяжелой огнеметной системе. В то же время скрытное средство реализации кибератак, недоступное для средств огневого поражения противостоящей стороны, может нанести противнику такой ущерб, который будет соизмерим с ущербом от батареи тяжелых огнеметных систем. Только для этого нужно, чтобы разработчики средств реализации кибератак

обладали как можно большими знаниями об уязвимостях автоматизированных систем своего противника.

Подводя черту, можно с уверенностью сказать, что в различных боевых условиях эффект от кибератак будет отличаться. И во многом он зависит от способности сторон выявлять новые, ранее неизвестные уязвимости в своих автоматизированных системах и аналогичных системах противника. Научно-методический аппарат для выявления таких уязвимостей и оценки эффективности использующих их кибератак в бою как раз и предложен в настоящей монографии. Этот аппарат является очередным кирпичиком в научном здании теоретических основ для получения единой меры взаимного влияния «материи» и «информации» в новых реалиях вооруженной борьбы.

11 июля 2021 года

Список используемых сокращений

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
АТ	–	абонентский терминал
БП	–	боевой потенциал
БПЛА	–	беспилотный летательный аппарат
ВС	–	Вооруженные Силы
ВФ	–	воинское формирование
ГОСТ	–	государственный стандарт
ЕСУ	–	Единая система управления
ЗО	–	задачи обеспечения разведки, связи, информационно-технического воздействия и навигационно-временного обеспечения
ЗУ	–	задача управления устройством
ИРЗ	–	информационно-расчетная задача
ИСП	–	Институт системного программирования
ИТВ	–	информационно-техническое воздействие
ИТС	–	информационно-техническое средство
ИЭ	–	исполнительный элемент
КА	–	кибератака (компьютерная атака)
КБС	–	коэффициент боевой соизмеримости
КНП	–	командно-наблюдательный пункт
КП	–	командный пункт
ЛП	–	локальный процесс
мбр	–	механизированная бригада
МО	–	Министерство обороны
мпб	–	мотопехотный батальон
мсб	–	мотострелковый батальон
НелВ	–	нелетальное воздействие
НТД	–	нормативно-технический документ
ОП	–	огневое поражение
ОПО	–	общее программное обеспечение
ОСК	–	оперативно-стратегическое командование
ОЭП	–	оптико-электронное подавление
ПВО	–	противовоздушная оборона
ПЗИ	–	подсистема защиты информации
ПО	–	программное обеспечение
ПсВ	–	психологическое воздействие
РАН	–	Российская академия наук
РИЭ	–	разведывательно-исполнительный элемент
РМК	–	расчетно-моделирующий комплекс
РП	–	распределенный процесс
РФ	–	Российская Федерация
РХБВ	–	радиационное, химическое и биологическое воздействие
РХБЗ	–	радиационная, химическая и биологическая защита
РЭ	–	разведывательный элемент

РЭБ – радиоэлектронная борьба
РЭП – радиоэлектронное подавление
РЭС – радиоэлектронное средство
СВ – сухопутные войска
СВТ – средство вычислительной техники
СИТВ – средство информационно-технического воздействия
СКО – среднеквадратическое отклонение
СОП – средство огневого поражения
СПО – специальное программное обеспечение
СПС – специальное программное средство
СР – средство разведки
СЦР – сеть цифровой радиосвязи
ТЗ – тактическое звено
ТК – технический компонент
ТТХ – тактико-техническая характеристика
УКВ – ультракороткие волны
УЭ – управляющий элемент
ФСТЭК – Федеральная служба по техническому и экспортному контролю
ЦУО – центр управления обороной
ЭБП – элемент боевого порядка
ЭВМ – электронно-вычислительная машина
ЭМВОС – эталонная модель взаимодействия открытых систем
ЭМИ – электромагнитное излучение
ЭС – элемент связи
ATCCS – Army Tactical Command and Control System (тактическая система командования и контроля армии)
BOSL – Basic Online Synthesis Language (базовый язык интерактивного синтеза)
C6ISR – Command, Control, Communications, Computers, Cyber-Defense and Combat Systems, Intelligence, Surveillance, Reconnaissance (командование, контроль, связь, компьютеры, системы киберзащиты и борьбы, разведка, наблюдение, распознавание)
COTS – Commercial Off-The-Shelf (коммерческое с полки)
DMR – Digital Mobile Radio (цифровое мобильное радио)
FBCB2 – Force XXI Battle Command Brigade-and-Bellow (силы XXI века боевого командования бригады и ниже)
HTML – Hyper-Text Markup Language (язык гипертекстовой разметки)
I2CEWS – Intelligence, Information, Cyber/Electronic Warfare & Space (разведка, информация, радиоэлектронная борьба, кибер- и космические операции)
IEEE – Institute of Electrical and Electronics Engineers (Институт инженеров электротехники и электроники)
MDTF – Multi-Domain Task Force (многодоменная оперативная группа)
OODA – Observe-Orient-Decide-Act (наблюдение, ориентация, решение, действие)
SDR – Software-Defined Radio (программно определяемое радио)
TETRA – TErrestrial Trunked Radio (наземное транковое радио)
UniTESK – Unified TEsting & Specification tool Kit (унифицированный инструментарий тестирования и спецификаций)

Список используемых обозначений

A	–	набор задач, обеспечиваемых информационно-техническими средствами, при котором стоимость элемента боевого порядка не больше максимальной
$A(t)$	–	подверженность информационно-технического средства перехвату управления с применением специальных программных средств в момент времени t
a	–	коэффициент, характеризующий оперативность функционирования подсистем воинского формирования в условиях информационно-технического воздействия
a_i	–	тип i-го элемента боевого порядка
al	–	локальный процесс
AP	–	конечное непустое множество информационных элементов сообщений, используемых локальным процессом
AP_ξ	–	множество информационных элементов, передаваемых в ξ-м сообщении
$БС_{n(m)}(t)$	–	боеспособность $n(m)$-го элемента боевого порядка в момент времени t
B_0	–	численность Синих в начале боя
$B(t)$	–	численность Синих в момент времени t
$\mathscr{B}_e$	–	количество этапов в e-м процессе технологии применения элемента боевого порядка
b	–	коэффициент, характеризующий вероятностные и временные параметры функционирования подсистем воинского формирования в условиях информационно-технического воздействия
C	–	множество элементов боевых порядков противоборствующих воинских формирований
$\mathbb{C}$	–	множество специальных программных средств в информационно-техническом средстве
$C'_{\text{у\_и}}$	–	количество элементов с функцией управления, образующих сегменты исполнительной сети
CH_η	–	множество параметров связи в η-й паре информационно-технических средств
$C_\text{р}$	–	количество элементов боевого порядка воинского формирования с функцией разведки
$C_\text{у}$	–	количество элементов боевого порядка воинского формирования с функцией управления
$C_{\text{у}_c}$	–	количество элементов боевого порядка с функцией управления, обеспечиваемых разведданными из c-го сегмента разведывательной сети
$C^{\text{А(Б)}}$	–	количество элементов боевых порядков в воинском формировании А(Б)
$C_{\text{и\_и}}$	–	количество элементов с исполнительной функцией, образующих сегменты исполнительной сети
$C_{\text{р\_и}}$	–	количество элементов с функцией разведки, образующих сегменты исполнительной сети
$C_{\text{св\_и}_c}$	–	количество элементов связи в c-м сегменте исполнительной сети, через которые идет информационный поток от образующего элемента
$C_{\text{св\_р}_{c,g}}$	–	количество промежуточных элементов с функцией связи в c-м сегменте разведывательной сети, обеспечивающих передачу разведданных g-му элементу с функцией управления в этом сегменте

$C_{\text{св\_у\_у}_{c,s}}$ – количество промежуточных элементов с функцией связи, обеспечивающих передачу информации от образующего элемента в *c*-м сегменте управляющей сети к *s*-му непосредственно подчиненному элементу с функцией управления

$C_{\text{св\_р\_у}_{c,s}}$ – количество промежуточных элементов с функцией связи, обеспечивающих передачу информации от образующего элемента в *c*-м сегменте управляющей сети к *s*-му непосредственно подчиненному элементу с функцией разведки

$C_{\text{св\_и\_у}_{c,s}}$ – количество промежуточных элементов с функцией связи, обеспечивающих передачу информации от образующего элемента в *c*-м сегменте управляющей сети к *s*-му непосредственно подчиненному элементу с исполнительной функцией

$C_{\text{у\_у}_c}$ – количество в *c*-м сегменте управляющей сети непосредственно подчиненных образующему элементу сегмента элементов с функцией управления

$C_{\text{р\_у}_c}$ – количество в *c*-м сегменте управляющей сети непосредственно подчиненных образующему элементу сегмента элементов с функцией разведки

$C_{\text{и\_у}_c}$ – количество в *c*-м сегменте управляющей сети непосредственно подчиненных образующему элементу сегмента элементов с исполнительной функцией

$C_{\text{защ}}$ – защищенность подсистемы управления от радиоэлектронного подавления

$C_{\text{нач}}$ – конечное множество начальных состояний распределенного процесса, в которые нет переходов

$C_{\text{пер}}$ – конечное непустое множество прямых и опосредованных переходов между состояниями распределенного процесса

$C_{\text{сост}}$ – конечное непустое множество состояний в распределенном процессе

c – коэффициент, характеризующий вероятностные и временные параметры функционирования подсистем воинского формирования в условиях информационно-технического воздействия

c_i – *i*-й элемент боевого порядка

D – количество абонентских терминалов, не входящих в атакуемую сеть

$D(t)$ – подверженность информационно-технического средства дезинформации с применением специальных программных средств в момент времени t

d – коэффициент, учитываемый при информационно-техническом воздействии на подсистему связи воинского формирования

d – расстояние

$Dp_{\text{р}}$ – вероятность передачи первичных и вторичных сообщений от имени абонентских терминалов, не входящих в атакуемую сеть

$E(t)$ – работоспособность информационно-технического средства в момент времени t

$\mathscr{E}_i$ – множество информационно-технических средств, каждое из которых обеспечивает решение некоторой доли несвязных задач (то есть информационных задач, задач управления, разведки и информационно-технического воздействия) *i*-го элемента боевого порядка

f – соотношение боевых потенциалов сторон в бою

f_0 – значение показателя эффективности воинского формирования с одинаковым для всех элементов его боевого порядка усредненным коэффициентом боевой соизмеримости

$f_{\text{нач}}$ – начальное соотношение боевых потенциалов

$f_{\text{рез}}$ – результирующее соотношение боевых потенциалов

f_c – значение показателя эффективности воинского формирования при исключенном c-м элементе боевого порядка

$f_{\text{тр}}$ – требуемый уровень показателя эффективности воинского формирования

$\mathscr{F}_i$ – множество информационно-технических средств с задачей обеспечения связи i-го элемента боевого порядка с другими элементами воинского формирования

$\mathbb{F}^{\text{А}}_{\text{Т}_{i,j,k}}(t)$ – соотношение боевых потенциалов в k-м тактическом районе j-го оперативного района i-го оптативно-стратегического района в момент времени t (формирование А относительно формирования Б)

G – количество траекторных матриц альтернативных вариантов позиционной динамики боя

$H_{i,m}$ – множество точек действия на m-й траектории движения i-го элемента боевого порядка

H – множество видов заметности

$\mathbb{H}$ – множество параметров подверженности элемента боевого порядка воинского формирования диверсии

I – множество начальных состояний локального процесса

$I_{\text{проц}}$ – количество процессов в технологии применения элемента боевого порядка

$I_{\text{АС}}$ – множество образцов автоматизированных систем в воинском формировании

ID – множество параметров защищенности от воздействия противника

IDE – множество параметров защиты от поражения электромагнитным излучением

IDF – множество параметров защиты от огневого поражения

IDI – множество параметров защиты от разведки

IDP – множество параметров защиты от кибератак

IDR – множество параметров защиты от радиоэлектронного подавления

Inc – множество вариантов набора исходных данных, обеспечивающих повышение эффективности воинского формирования

IP – множество параметров процессов функционирования информационно-технического средства

IPT – множество параметров качества электронной компонентной базы

IPZ – множество параметров выполняемых задач

IR – множество параметров обеспечивающих ресурсов, необходимых для работы информационно-технического средства

IT – множество параметров времени подготовки информационно-технического средства к работе

IV – множество параметров возможностей по влиянию информационно-технических средств на противника

$\Im_i$ – количество этапов в i-м процессе технологии применения элемента боевого порядка

J_i – множество образцов информационно-технических средств в i-м образце автоматизированной системы

K – максимальное количество единых боевых эпизодов для всех траекторно-временных матриц

$K_{1кр}$ – количество боеприпасов, необходимое средству огневого поражения Синих для уничтожения одного средства огневого поражения Красных

$K_{1син}$ – количество боеприпасов, необходимое средству огневого поражения Красных для уничтожения одного средства огневого поражения Синих

$K_{i,j}$ – количество задач в j-м этапе i-го процесса технологии применения элемента боевого порядка

$K^{Б}$ – координаты элемента боевого порядка

$K_{бп\_кр}$ – количество боеприпасов в боекомплекте одного средства огневого поражения Красных

$K_{бп\_син}$ – количество боеприпасов в боекомплекте одного средства огневого поражения Синих

$K_{ИТВ\_оп}$ – коэффициент влияния кибератак Синих на время выполнения операций в подсистеме огневого поражения Красных

$K_{ИТВ\_р}$ – коэффициент влияния кибератак Синих на время выполнения операций в подсистеме разведки Красных

$K_{ИТВ\_св}$ – коэффициент влияния кибератак Синих на время передачи информации в подсистеме связи Красных

$K_{ИТВ\_упр}$ – коэффициент влияния кибератак Синих на время выполнения операций в подсистеме управления Красных

$K_{бп_{n(m)}}$ – коэффициент боевой подготовки личного состава в $n(m)$-м элементе боевого порядка

$K_{боп_{n(m)}}$ – коэффициент боевого опыта личного состава в $n(m)$-м элементе боевого порядка

$k_{пр}$ – количество личного состава, необходимое для выполнения процессов в элементе боевого порядка без применения информационно-технических средств

$k^{*}_{пр}$ – количество личного состава, необходимое для выполнения процессов в элементе боевого порядка с применением информационно-технических средств

$\mathbb{k}$ – множество альтернативных наборов задач, удовлетворяющих ограничениям на время выполнения задач, структуру процессов в элементе боевого порядка, а также ограничениям на используемую модель системы массового обслуживания

$\mathbb{k}^{*}$ – множество наборов задач, обеспечиваемых информационно-техническими средствами, при котором стоимость элемента боевого порядка не больше максимальной и удовлетворяются ограничения на время выполнения задач, структуру процессов в элементе боевого порядка и используемую модель системы массового обслуживания

$\mathbb{k}^{А(Б)}_{рОС_i}$ – показатель ресурсного обеспечения i-го оперативно-стратегического района

$\mathbb{k}^{А(Б)}_{рО_{i,j}}$ – показатель ресурсного обеспечения j-го оперативного района i-го оперативно-стратегического района

$\mathbb{k}^{А(Б)}_{уОС_i}(t)$ – показатель эффективности управления боевыми циклами в i-м оперативно-стратегическом районе в момент времени t

$\mathbb{k}^{А(Б)}_{уО_{i,j}}(t)$ – показатель эффективности управления боевыми циклами в j-м оперативном районе i-го оперативно-стратегического района в момент времени t

L – функция меток, сопоставляющая каждому состоянию (сообщению) локального процесса множество информационных элементов, используемых в этом состоянии (сообщении)

$\mathscr{L}_{e,h}$ – количество задач h-го этапа в e-м процессе технологии применения элемента боевого порядка

$L_{\text{ИТВ\_оп}}$ – показатель снижения вероятности выполнения процессов в подсистеме огневого поражения Красных за счет кибератак, радиоэлектронного подавления или поражения электромагнитным излучением

$L_{\text{ИТВ\_р}}$ – показатель снижения вероятности выполнения процессов в подсистеме разведки Красных за счет кибератак, радиоэлектронного подавления или поражения электромагнитным излучением

M – множество типов сообщений, которыми обмениваются информационно-технические средства заданного образца автоматизированной системы

$\mathcal{M}$ – множество параметров ущерба элемента боевого порядка воинского формирования для вывода его из строя

$\mathfrak{A}$ – набор задач, обеспечиваемых информационно-техническими средствами, при котором стоимость элемента боевого порядка не больше максимальной и удовлетворяются ограничения на время выполнения задач, структуру процессов в элементе боевого порядка и используемую модель системы массового обслуживания

M^* – количество траекторных матриц сценариев боя, каждая из которых соответствует базовой группе траекторий

M_0 – методологический базис киберзащиты автоматизированных систем воинских формирований

M_1 – метод генерации кибератак на телекоммуникационное оборудование

M_2 – метод оценки эффективности кибератак в боевых действиях

M_i – количество альтернативных траекторий движения i-го элемента боевого порядка

$m_{i,j,\mu,r}$ – r-й тип сообщения, используемый в μ-м процессе j-го информационно-технического средства заданного i-го образца автоматизированной системы

$m_{v,i,j}$ – длительность интервала передачи специального программного средства v-го типа между связанными i-м и j-м узлами

N – количество уязвимых и доступных для специальных программных средств узлов сети

$\boldsymbol{n}$ – используемый порядок обобщенного закона Эрланга

$\mathbb{N}$ – количество боеприпасов для уничтожения цели

$n_{\text{п}}$ – количество попыток прохождения фазы боевого цикла в условиях влияния техники радиоэлектронной борьбы

N_0 – остаточная доля численности воинского формирования, оснащенного защищаемой автоматизированной системой, без применения мероприятий по защите от кибератак

$N_{n(m)}$ – количество образцов информационно-технических средств и устройств в $n(m)$-м элементе боевого порядка

$N_{\text{АТ}}$ – количество абонентских терминалов сети цифровой радиосвязи

$N_{\text{им\_кр}}$ – количество имитируемых средств огневого поражения Красных

$N_{\text{им\_син}}$ – количество имитируемых средств огневого поражения Синих

$N_{\text{КА}}$ – остаточная доля численности воинского формирования, оснащенного защищаемой автоматизированной системой, с применением мероприятий по защите от кибератак

$N_{\text{кр}}$ – количество средств огневого поражения Красных в начале боя

$N_{\text{крит\_кр}}$ – критическое значение численности Красных, при котором они прекращают сопротивление

$N_{\text{син}}$ – количество средств огневого поражения Синих в начале боя

$N_{\text{Л}_{n(m)}}$ – количество людей в $n(m)$-м элементе боевого порядка

$N^{\text{А}}_{\text{ОП}}$ – множество элементов боевого порядка с функцией огневого поражения

$N^{\text{А}}_{\text{Р}}$ – множество элементов боевого порядка с функцией разведки

$N^{\text{Б(А)}}_{\text{РЭП}}$ – множество элементов боевого порядка с функцией радиоэлектронного подавления в воинском формировании Б(А)

$N^{\text{Б(А)}}_{\text{ЭМИ}}$ – множество элементов боевого порядка с функцией поражения электромагнитным излучением в воинском формировании Б(А)

$N^{\text{Б(А)}}_{\text{КА}}$ – множество элементов боевого порядка с функцией реализации кибератак в воинском формировании Б(А)

$N^{\text{А(Б)}}_{*\text{беспр}_{\#}}$ – множество информационно-технических средств для беспроводной связи в #-м элементе боевого порядка с функцией *

$N^{\text{А(Б)}}_{\text{Р}\,\text{развИТС}_{\#}}$ – множество разведывательных информационно-технических средств #-го элемента боевого порядка с функцией разведки

$N^{\text{Б(А)}}_{*\,\text{достИТС}_{\#}}$ – множество информационно-технических средств, доступных для #-го элемента боевого порядка с функцией радиоэлектронного подавления или реализации кибератак

$N^{\text{А(Б)}}_{*\text{нав}_{\#}}$ – множество информационно-технических средств #-го элемента боевого порядка с функцией * для получения внешней навигационной информации, без которой он неработоспособен

$N_{\text{упр}_{n(m)}}$ – количество информационно-технических средств в $n(m)$-м элементе боевого порядка, обеспечивающих решение задач управления

$n_{\text{Р}_j}$ – количество элементов боевого порядка с функцией разведки, информация от которых поступает в j-й элемент боевого порядка с функцией управления

$O_{\$}$ – множество внутренних параметров стоимости работ по устранению уязвимостей информационно-технических средств

$O_{\text{С}}$ – множество внутренних параметров состава, структуры, местоположения, процессов функционирования, воздействия, обеспеченности ресурсами с детализацией элементов боевых порядков воинских формирований до устройств, информационно-технических средств автоматизированных систем, людей и критически важных объектов гражданской инфраструктуры

O_i – множество попарно смежных через грани или ребра элемобов, которые занимает i-й элемент боевого порядка

O_{R} – множество внутренних параметров связей устройств, информационно-технических средств и людей

$O^*_{\text{С}}$ – множество процессов функционирования образцов информационно-технических средств автоматизированной системы, в которых осуществляется поиск уязвимостей

O^*_{R} – множество процессов информационного взаимодействия образцов информационно-технических средств автоматизированной системы

Opt – множество вариантов набора исходных данных, обеспечивающих требуемый уровень показателя эффективности воинского формирования

$\mathbb{P}$ – доля сбереженного времени на применение элемента боевого порядка за счет информатизации

$P(\ldots)_{\text{совм}}$ – вероятность суммы совместных событий

$P(t)$ – вероятностно-временная характеристика нахождения информационно-технического средства в работоспособном состоянии в конфликте средства реализации кибератак и подсистемы защиты информации информационно-технического средства

PM – множество параметров местоположения элемента боевого порядка воинского формирования

$P_{\text{1бп\_кр}}$ – вероятность поражения цели одним боеприпасом средства огневого поражения Красных

$P_{\text{1бп\_син}}$ – вероятность поражения цели одним боеприпасом средства огневого поражения Синих

PE – множество параметров работы людей

P_{f} – вероятность постановки радиопомехи во временном слоте

P_g – вероятность реализации g-го сценария боя

$P_{g,i}(t)$ – вероятностно-временная характеристика заражения i-го узла g-м экземпляром специального программного средства v-го типа в момент времени t

$pr(\ldots)$ – приоритет соответствующего процесса технологии применения элемента боевого порядка

$P_{\text{гар}}$ – требуемая вероятность гарантированного огневого поражения цели

$P_{\text{гпи}}$ – вероятность гарантированной передачи информации

$P_{\text{дост}}$ – вероятность нахождения забрасываемого передатчика помех в работоспособном состоянии после приземления

$P_{\text{зо}}(t)$ – вероятностно-временная характеристика нахождения в работоспособном состоянии специального программного обеспечения задач обеспечения в информационно-техническом средстве

$P_{\text{зу}}(t)$ – вероятностно-временная характеристика нахождения в работоспособном состоянии специального программного обеспечения задач управления в информационно-техническом средстве

$P_{\text{ирз}}(t)$ – вероятностно-временная характеристика нахождения в работоспособном состоянии специального программного обеспечения информационно-расчетных задач в информационно-техническом средстве

$P_{\text{ИТВ}}$ – вероятность реализации информационно-технического воздействия

$P_{\text{оп\_кр}}$ – вероятность работоспособного состояния подсистемы огневого поражения Красных в момент времени вскрытия ими местонахождения подсистемы информационно-технического воздействия Синих

$P_{\text{опо}}(t)$ – вероятностно-временная характеристика нахождения в работоспособном состоянии общего программного обеспечения в информационно-техническом средстве

$P_{\text{р\_кр}}$ – вероятность вскрытия и распознавания цели подсистемой разведки Красных

$P_{\text{р\_син}}$ – вероятность вскрытия и распознавания цели подсистемой разведки Синих

$P_{\text{РЭП}}(t)$ – вероятность выполнения задач обеспечения в информационно-техническом средстве в условиях радиоэлектронного подавления в момент времени t

$P_{\text{св\_кр}}$ – вероятность гарантированной передачи информации по каналу связи Красных

$P_{\text{св\_син}}$ – вероятность гарантированной передачи информации по каналу связи Синих

$P_{\text{тк}}(t)$ – вероятностно-временная характеристика нахождения в работоспособном состоянии технического компонента в информационно-техническом средстве

$P^{\text{А(Б)}}_{\text{нф}_{n(m)}}$ – вероятность выполнения личным составом $n(m)$-го элемента боевого порядка воинского формирования А(Б) неавтоматизированных функций

$P_{\text{РХБВ}_{n(m)}}(d)$ – вероятность вывода из строя личного состава в $n(m)$-м элементе боевого порядка на расстоянии d средством/боеприпасом радиационного, химического или биологического воздействия

$P_{\text{НелВ}_{n(m)}}(d)$ – вероятность вывода из строя личного состава в $n(m)$-м элементе боевого порядка на расстоянии d средством/боеприпасом нелетального воздействия

$P_{\text{ПсВ}_{n(m)}}(d)$ – вероятность вывода из строя личного состава в $n(m)$-м элементе боевого порядка на расстоянии d средством/боеприпасом психологического воздействия

$P_{\text{РХБЗкол}_{n(m)}}$ – максимальная вероятность защиты средством радиационной, химической и биологической защиты коллективного пользования в $n(m)$-м элементе боевого порядка

$P_{\text{РХБЗ}_{n(m),i}}$ – вероятность защиты индивидуального средства радиационной, химической и биологической защиты i-го человека в $n(m)$-м элементе боевого порядка

p_0 – вероятность первичной передачи сообщения абонентским терминалом во временной слот

p_r – вероятность повторной передачи сообщения абонентским терминалом во временной слот

$Q_{\text{втор}}$ – количество вторичных сообщений, одновременно переданных абонентскими терминалами

$\mathbb{Q}$ – доля сбереженного личного состава элемента боевого порядка за счет информатизации

$\mathbb{Q}_{i,j,\text{ц},r}$ – множество пар «сообщение-время»

$Q_{\text{зо}}$ – показатель функциональной пригодности специального программного обеспечения задач обеспечения в информационно-техническом средстве

$Q_{\text{зу}}$ – показатель функциональной пригодности специального программного обеспечения задач управления в информационно-техническом средстве

$Q_{\text{ирз}}$ – показатель функциональной пригодности специального программного обеспечения информационно-расчетных задач в информационно-техническом средстве

$Q_{i,m}$ – количество элемобов, через которые перемещается i-й элемент боевого порядка на m-й траектории движения

Q_{y_i} – уровень качественного состояния органа управления (расчета, экипажа) i-го элемента боевого порядка

q_v – количество экземпляров специальных программных средств v-го типа

$\mathbb{R}$ – множество параметров среды функционирования автоматизированной системы

R – распределенный процесс, объединяющий несколько информационно-технических средств посредством обмена сообщениями

$\Re$ – множество параметров защиты элемента боевого порядка воинского формирования от воздействий противника

R_0 – численность Красных в начале боя

$R(t)$ – численность Красных в момент времени t

RA – множество параметров функционирования информационно-технического средства

$R_{i,m}$ – кортеж последовательно расположенных и попарно смежных через грани или ребра элемобов, через которые проходит m-я траектория движения i-го элемента боевого порядка

S – множество информационно-технических средств, входящих в рассматриваемую автоматизированную систему

$S_{\text{пер}}$ – количество первичных сообщений, одновременно переданных абонентскими терминалами

S' – множество информационно-технических средств, с которыми может взаимодействовать рассматриваемая автоматизированная система

$\mathbb{S}(x)$ – функция стоимости элемента боевого порядка для набора задач x, обеспечиваемых информационно-техническими средствами

$S(t)$ – количество альтернативных боевых эпизодов в k-м тактическом районе j-го оперативного района i-го оптативно-стратегического района в момент времени t

$S^{\sim}$ – множество корректных процессов

$S_{i,j}$ – множество процессов функционирования программного обеспечения в j-м информационно-техническом средстве i-го образца автоматизированной системы, шаги которых могут включать прием/передачу сообщений

s_{m_g} – наибольшая из всех заданных длин траекторий пути элементов боевых порядков противоборствующих воинских формирований в g-й траекторной матрице

$\mathbb{S}_{\max}$ – максимально допустимая стоимость информатизации элемента боевого порядка

$S_{\text{тр}}$ – множество траекторий движения элементов боевых порядков

sp – способ реализации кибератаки

$T_{i,m,j}$ – время нахождения i-го элемента боевого порядка в j-й точке действия m-й траектории движения

TS – множество параметров функционирования устройств

TY_{η} – множество типов связей в η-й паре информационно-технических средств

$T_{\text{безРЭБ}}$ – время прохождения фазы боевого цикла через элемент боевого порядка без учета влияния техники радиоэлектронной борьбы

$T_{\text{бц\_кр}}$ – время боевого цикла Красных

$T_{\text{бц\_син}}$ – время боевого цикла Синих

$T_{\text{вскр\_ИТВ}}$ – время вскрытия Красными местонахождения подсистемы информационно-технического воздействия Синих

$T_{\text{доп}}$ – максимальное время, отводимое на расчеты

$T_{\text{кон}}$ – время завершения боевого эпизода

$T_{\text{кр}}$ – момент времени, когда Красные прекратили сопротивление

$T_{\text{кр(РЭП)}}$ – время уничтожения Красных в режиме «радиоэлектронное подавление $\succ$ огневое поражение»

$T_{\text{м}}$ – параметр масштабирования боя

$T_{\text{нач}}$ – время начала боевого эпизода

$T_{\text{ост}}$ – время уничтожения Красными оставшейся доли подсистемы огневого поражения Синих после уничтожения подсистемы информационно-технического воздействия

$T_{\text{ПЗИ}}$ – оперативность подсистемы защиты информации информационно-технического средства

$T_{\text{св\_кр}}$ – время передачи информации по каналу связи Красных

$T_{\text{св\_син}}$ – время передачи информации по каналу связи Синих

$T_{\text{син}}$ – момент времени, когда Синие были бы уничтожены, если бы Красные продолжили сопротивление

$T_{\text{сРЭБ}}$ – время прохождения фазы боевого цикла через элемент боевого порядка с учетом влияния техники радиоэлектронной борьбы

$T_{\text{ун\_ИТВ}}$ – время уничтожения подсистемы информационно-технического воздействия Синих

$T_{\text{упр\_кр}}$ – время работы подсистемы управления Красных

$T_{\text{упр\_син}}$ – время работы подсистемы управления Синих

$T_{\text{эп}}$ – время расчета одного боевого эпизода

$T^{\text{А}}_{\text{~пер}}$ – время передвижения элемента боевого порядка воинского формирования А на требуемую позицию («~» – любой элемент);

$T^{\text{А}}_{\text{~под}}$ – время подготовки элемента боевого порядка воинского формирования А к работе

$T^{\text{А}}_{\text{Ррез}}$ – время получения результатов разведки элементом боевого порядка с функцией разведки воинского формирования А

$T^{\text{А}}_{\text{ОПупр}}$ – время получения, подготовки, ретрансляции, обработки, анализа информации и принятия решения на применение элемента боевого порядка воинского формирования А

$T^{\text{Б(А)}}_{\text{КА физ}_{\#}}$ – время получения физического доступа #-го элемента боевого порядка воинского формирования Б(А) с функцией реализации кибератак к информационно-техническому средству целевого для него элемента

$T^{\text{Б(А)}}_{\text{КА техн}_{\#}}$ – время получения технического доступа #-го элемента боевого порядка воинского формирования Б(А) с функцией реализации кибератак к информационно-техническому средству целевого для него элемента

$T^{\text{Б(А)}}_{\text{КА сет}_{\#}}$ – время до начала скрытого нарушения #-м элементом боевого порядка воинского формирования Б(А) с функцией реализации кибератак доступности информации информационно-технического средства целевого для него элемента боевого порядка на сетевом уровне и выше

$T^{\text{Б(А)}}_{\text{КА кан}_{\#}}$ – время до начала скрытого нарушения #-м элементом боевого порядка воинского формирования Б(А) с функцией реализации кибератак доступности информации информационно-технического средства целевого для него элемента боевого порядка на канальном уровне

$T_{\text{кр(ОП)}}$ – время уничтожения Красных в режиме «огневое поражение $\succ$ радиоэлектронное подавление»

$T_{\text{кр(РЭП)}}$ – время уничтожения Красных в режиме «радиоэлектронное подавление $\succ$ огневое поражение»

$T_{\text{син(ОП)}}$ – время уничтожения Синих в режиме «огневое поражение $\succ$ радиоэлектронное подавление» при условии, что их подсистема ИТВ не является целью

$T_{\text{син(РЭП)}}$ – время уничтожения Синих в режиме «радиоэлектронное подавление $\succ$ огневое поражение»

$T^{\bullet}_{\text{син(ОП)}}$ – время уничтожения Синих в режиме «огневое поражение $\succ$ радиоэлектронное подавление» при условии, что их подсистема ИТВ не уничтожена, но является целью

$T^{\text{А(Б)}}_{i,j,k,s}$ – время уничтожения воинского формирования А(Б) в s-м боевом эпизоде графа позиционной динамики элементов боевых порядков воинских формирований в k-м тактическом районе j-го оперативного района i-го оптативно-стратегического района

$T_{\text{1бп\_кр}}$ – время воздействия одним боеприпасом в подсистеме огневого поражения Красных

$T_{\text{1бп\_син}}$ – время воздействия одним боеприпасом в подсистеме огневого поражения Синих

$T_{\text{оп\_кр}}$ – время подготовки подсистемы огневого поражения Красных

$T_{\text{оп\_син}}$ – время подготовки подсистемы огневого поражения Синих

$T_{\text{р\_кр}}$ – время работы подсистемы разведки Красных

$T_{\text{р\_син}}$ – время работы подсистемы разведки Синих

$t_{\text{пр}}$ – среднее время выполнения процессов в элементе боевого порядка без применения информационно-технических средств

$t^{*}_{\text{пр}}$ – среднее время выполнения процессов в элементе боевого порядка с применением информационно-технических средств

$t(m_{\xi})$ – момент фиксации передачи ξ-го сообщения

$t_{i,j,k}$ – время выполнения k-й задачи в j-м этапе i-го процесса технологии применения элемента боевого порядка

U – коэффициент снижения ущерба обороняемым позициям

$U_{\text{зл}}$ – количество переданных злоумышленником сообщений от имени абонентских терминалов и (или) наличие радиопомехи в канале

$U^{\text{А}}_{\sim\text{дал}}(d)$ – дальностная характеристика применения элемента боевого порядка воинского формирования А на расстоянии d

$U^{\text{Б(А)}}_{\text{РЭПдал}_{\#}}(d,q)$ – дальностная характеристика применения #-го элемента боевого порядка воинского формирования Б(А) с функцией радиоэлектронного подавления, характеризующая его способность нарушить работу q-го информационно-технического средства, обеспечивающего беспроводной связью целевой элемент боевого порядка воинского формирования А(Б), на расстоянии d

$U^{\text{Б(А)}}_{\text{ЭМИдал}_{\#}}(d)$ – дальностная характеристика применения #-го элемента боевого порядка воинского формирования Б(А) с функцией поражения электромагнитным излучением, характеризующая плотность потока энергии электромагнитного поля, формируемого этим элементом на расстоянии d

$U^{\text{Б(А)}}_{\text{КАдал}_{\sim}}(d,q)$ – дальностная характеристика применения ~-го элемента боевого порядка воинского формирования Б(А) с функцией реализации кибератак, характеризующая его способность установить информационное взаимодействие с q-м информационно-техническим средством, обеспечивающим беспроводной связью и/или навигационной информацией целевой элемент боевого порядка воинского формирования А(Б), на уровне чувствительности приемника этого средства на расстоянии d

$u^{\text{Б}}_{\text{баз}}$ – уровень базовой защищенности элемента боевого порядка воинского формирования Б от огневого поражения

$u^{\text{Б}}_{\text{доп}}$ – уровень дополнительной защищенности элемента боевого порядка воинского формирования Б от огневого поражения

$u^{\text{Б}}_{\text{замет}}(h)$ – уровень заметности элемента боевого порядка воинского формирования Б для h-го вида заметности

$u^{\text{Б}}_{\text{маск}}(h)$ – уровень маскировки (с учетом аэрозольного противодействия) элемента боевого порядка воинского формирования Б для h-го вида заметности

$u^{\text{А(Б)}}_{*\text{п/с}_{\#}}(q)$ – пороговый уровень помеха/сигнал для нарушения работы q-го информационно-технического средства, обеспечивающего беспроводной связью #-й элемент боевого порядка воинского формирования А(Б) с функцией *

$u^{\text{А(Б)}}_{*\text{с/ш}_{\#}}(q)$ – минимальный уровень приема сигнала q-м информационно-техническим средством, обеспечивающим беспроводной связью #-й элемент боевого порядка воинского формирования А(Б) с функцией *

$u^{\text{А(Б)}}_{*\text{завис}_{\#}}$ – пороговая плотность потока энергии электромагнитного поля, достаточная для подавления информационно-технических средств #-го элемента боевого порядка воинского формирования А(Б) с функцией *

$V(t)$ – подверженность информационно-технического средства разведке с применением специальных программных средств в момент времени t

VP – множество параметров времени подготовки элемента боевого порядка воинского формирования к работе

$W_{i,m}$ – ранг важности m-й траектории движения i-го элемента боевого порядка на единой для всех элементов θ-бальной шкале

$W^{+}_{i,j,\mu,r,k}$ – k-й элемент множества предусмотренных протоколом вариантов содержания сообщения r-го типа μ-го процесса j-го информационно-технического средства i-го образца автоматизированной системы

$W^{-}_{i,j,\mu,r,k}$ – k-й элемент множества непредусмотренных протоколом вариантов содержания сообщения r-го типа μ-го процесса j-го информационно-технического средства i-го образца автоматизированной системы

$W^{\sim}_{i,j,\mu,r,k}$ – k-й элемент множества допустимых протоколом вариантов содержания сообщения r-го типа в μ-м процессе j-го информационно-технического средства i-го образца автоматизированной системы

$W^{\text{А(Б)}}_{n(m)}$ – коэффициент боевой соизмеримости $n(m)$-го элемента боевого порядка воинского формирования А(Б)

$W_{\text{у\_у}_{c,s}}$ – коэффициент боевой соизмеримости s-го непосредственно подчиненного образующему элементу c-го сегмента управляющей сети элементов с функцией управления

$W_{\text{р\_у}_{c,s}}$ – коэффициент боевой соизмеримости s-го непосредственно подчиненного образующему элементу c-го сегмента управляющей сети элементов с функцией разведки

$W_{\text{и\_у}_{c,s}}$ – коэффициент боевой соизмеримости s-го непосредственно подчиненного образующему элементу c-го сегмента управляющей сети элементов с исполнительной функцией

$W_{\text{и(у,р)\_и}_{c}}$ – коэффициент боевой соизмеримости элемента, образующего c-й сегмент исполнительной сети

$W_{\text{у\_и}_{s}}$ – коэффициент боевой соизмеримости s-го элемента с функцией управления, образующего сегмент исполнительной сети

$W_{\text{и\_и}_{s}}$ – коэффициент боевой соизмеримости s-го элемента с исполнительной функцией, образующего сегмент исполнительной сети

$W_{\text{р\_и}_{s}}$ – коэффициент боевой соизмеримости s-го элемента с функцией разведки, образующего сегмент исполнительной сети

W_{OC_i} – показатель важности i-го оперативно-стратегического района

$W_{O_{i,j}}$ – показатель важности j-го оперативного района i-го оперативно-стратегического района

$W_{T_{i,j,k}}$ – показатель важности, k-го тактического района j-го оперативного района i-го оперативно-стратегического района

w – одинаковый для всех элементов боевого порядка воинского формирования усредненный коэффициент боевой соизмеримости

w' – одинаковый для всех элементов боевого порядка воинского формирования усредненный коэффициент боевой соизмеримости при одном исключенном элементе

X – множество исходных параметров способов реализации кибератак, эксплуатирующих уязвимости автоматизированной системы

x – набор задач, обеспечиваемых информационно-техническим средством

x^* – набор задач, обеспечиваемых информационно-техническими средствами, стоимость которого не превосходит заданную и при котором уровень информатизации максимален

$X_{кр}$ – подмножество способов реализации кибератак, которое необходимо парировать в процессе создания (модернизации) автоматизированной системы

Y – множество выходных параметров эффективности автоматизированной системы

$Y(t)$ – количество абонентских терминалов, одновременно находящихся в режиме вторичной передачи сообщений в момент времени t

Y_+ – подмножество выходных параметров, при которых достигается заданное пороговое значение боевой эффективности воинского формирования с минимальной затратой доступных ресурсов

Y_{max} – подмножество выходных параметров, при которых достигается максимальное значение боевой эффективности воинского формирования при недостижимости порогового значения ε

$Y_{БОЕВ}$ – выходные боевые параметры эффективности автоматизированной системы

$Y_{ИНФ}$ – выходные информационные параметры эффективности автоматизированной системы

$Y_{ИНФБ}$ – выходные информационно-боевые параметры эффективности автоматизированной системы

Z – конечное непустое множество состояний локального процесса

$Z(t)$ – заразность информационно-технического средства для специальных программных средств в момент времени t

$Z_{до}$ – доля средств огневого поражения Синих, уничтоженных Красными до уничтожения подсистемы информационно-технического воздействия Синих

$Z_{после}$ – доля средств огневого поражения Синих, уничтоженных Красными после уничтожения подсистемы информационно-технического воздействия Синих

α_1 – нештатное состояние потери работоспособности информационно-технического средства

α_2 – нештатное состояние сниженной эффективности функционирования информационно-технического средства

α_3 – нештатное состояние управляемости информационно-технического средства

α_4 – нештатное состояние доступности информационно-технического средства для углубленного анализа противником

$\alpha_{n(m)}$ – вероятность использования $n(m)$-го элемента боевого порядка разведывательно-диверсионными подразделениями противника

$\alpha_{v,i,j}$ – длительность интервала с момента готовности специального программного средства v-го типа к размножению в i-м узле до момента его внедрения в j-й узел

β – скорострельность одной боевой единицы Красных

$\beta_{n(m),h}$ – доля решаемых h-м информационно-техническим средством задач управления оружием $n(m)$-го элемента боевого порядка

$\beta_{v,i}$ – длительность интервала с момента внедрения специального программного средства v-го типа в i-й узел до момента, когда оно будет готово к размножению

$\beta(x)$ – функция стоимости варианта набора исходных данных x

Γ – множество типов элемобов

γ – скорострельность одной боевой единицы Синих

$\gamma_i(t)$ – целостность информации i-го элемента боевого порядка в момент времени t

$\gamma_{v,i}$ – длительность интервала с момента внедрения специального программного средства v-го типа в i-й узел до момента, когда данный узел от этого средства будет излечен

$\gamma_{\text{у}}^{\text{А(Б)}}(t)$ – показатель целостности информации совокупности управляющих потоков воинского формирования А(Б) в момент времени t

$\gamma_{\text{и}}^{\text{А(Б)}}(t)$ – показатель целостности информации совокупности исполнительных потоков воинского формирования А(Б) в момент времени t

$\gamma_{\text{р}}^{\text{А(Б)}}(t)$ – показатель целостности информации совокупности разведывательных потоков воинского формирования А(Б) в момент времени t

Δ – уровень информатизации воинского формирования Красных

$\Delta(x)$ – уровень информатизации элемента боевого порядка для набора задач x, обеспечиваемых информационно-техническими средствами

$\Delta_{n(m)}$ – уровень информатизации $n(m)$-го элемента боевого порядка

$\Delta N(x)$ – функция эффективности воинского формирования для варианта набора исходных данных x

Δp_0 – вероятность первичной передачи сообщения, задаваемая в легитимном потоке управления

Δp_0^* – вероятность первичной передачи сообщения, задаваемая в ложном потоке управления

$\Delta p_{\text{г}}$ – вероятность вторичной передачи сообщения, задаваемая в легитимном потоке управления

$\Delta p_{\text{г}}^*$ – вероятность вторичной передачи сообщения, задаваемая в ложном потоке управления

$\Delta t_<$ – интервал запаздывающей передачи сообщения

$\Delta t_>$ – интервал преждевременной передачи сообщения

$\Delta t_\circ$ – интервал своевременной передачи сообщения

$\Delta t_{\min}$ – продолжительность интервала отправки сообщения

Δt_{wait} – продолжительность интервала, в течение которого сообщение в информационно-техническом средстве ожидается

$\delta\beta_{\text{р}}$ – ослабление скорострельности Красных за счет тотального радиоэлектронного подавления их подсистем разведки, связи и огневого поражения

δB – боевые потери победивших Синих

$\delta_i(t)$ – доступности информации i-го элемента боевого порядка в момент времени t

$\delta N_{\text{син}}$ – потери Синих в бою

$\delta N^{+}_{\text{син}}$ – остаточная численность победивших Синих

$\delta N^{*}_{\text{син}}$ – остаточная доля численности победивших Синих

$\delta^{\text{А(Б)}}_{\text{у}}(t)$ – показатель доступности информации совокупности управляющих потоков воинского формирования А(Б) в момент времени t

$\delta^{\text{А(Б)}}_{\text{и}}(t)$ – показатель доступности информации совокупности исполнительных потоков воинского формирования А(Б) в момент времени t

$\delta^{\text{А(Б)}}_{\text{р}}(t)$ – показатель доступности информации совокупности разведывательных потоков воинского формирования А(Б) в момент времени t

ε – пороговое значение эффективности функционирования автоматизированной системы в боевых условиях

ζ – размер стороны элементарного объема пространства боя (элемоба)

$\boldsymbol{\eta}$ – коэффициент, характеризующий вклад целевой для информационно-технических воздействий подсистемы противника в его боевой потенциал

η_i – вероятность уничтожения i-го элемента боевого порядка разведывательно-диверсионными подразделениями противника

Θ – вспомогательная переменная

$\Theta_{\$}$ – множество ограничений параметров максимально допустимой стоимости работ по устранению уязвимостей

$\Theta_{\mathbb{R}}$ – множество ограничений параметров среды

Θ_{R} – множество ограничений связей устройств, информационно-технических средств и людей

Θ_{C} – множество ограничений физической реализуемости компонентов автоматизированной системы и элементов боевых порядков воинских формирований в целом и критически важных объектов

θ – вариант передачи сообщения в тестовом способе реализации кибератаки

$\kappa_i(t)$ – конфиденциальность информации i-го элемента боевого порядка в момент времени t

$\kappa_{c,h}(t)$ – конфиденциальность информации образующего элемента в c-м сегменте сети в момент времени t

$\kappa^{\text{Б(А)}}_{\text{у}}(t)$ – показатель конфиденциальности информации совокупности управляющих потоков воинского формирования А(Б) в момент времени t

$\kappa^{\text{Б(А)}}_{\text{и}}(t)$ – показатель конфиденциальности информации совокупности исполнительных потоков воинского формирования А(Б) в момент времени t

$\kappa^{\text{Б(А)}}_{\text{р}}(t)$ – показатель конфиденциальности информации совокупности разведывательных потоков воинского формирования А(Б) в момент времени t

$\kappa_{\text{св\_р}_{c,g,q}}(t)$ – конфиденциальность информации q-го промежуточного элемента с функцией связи, обеспечивающего передачу разведданных g-му элементу в c-м сегменте разведывательной сети в момент времени t

$\kappa_{\text{св\_и}_{c,q}}(t)$ – показатель конфиденциальности информации q-го промежуточного элемента связи c-го сегмента исполнительной сети, обеспечивающего передачу информации от образующего сегмент элемента в момент времени t

$\kappa_{\text{св\_у\_у}_{c,s,q}}(t)$ – конфиденциальность информации q-го промежуточного элемента с функцией связи c-го сегмента управляющей сети, обеспечивающего передачу информации от образующего элемента данного сегмента s-му непосредственно подчиненному элементу с функцией управления в момент времени t

$\kappa_{\text{св\_р\_у}_{c,s,q}}(t)$ – конфиденциальность информации q-го промежуточного элемента с функцией связи c-го сегмента управляющей сети, обеспечивающего передачу информации от образующего элемента данного сегмента s-му непосредственно подчиненному элементу с функцией разведки

$\kappa_{\text{св\_и\_у}_{c,s,q}}(t)$ – конфиденциальность информации q-го промежуточного элемента с функцией связи c-го сегмента управляющей сети, обеспечивающего передачу информации от образующего элемента данного сегмента s-му непосредственно подчиненному элементу с исполнительной функцией

Λ – пространство боя, которое образуется множеством кубических элемобов

$\Lambda_{\text{доп}}$ – допустимая стоимость реализации варианта набора исходных данных

λ_i – интенсивность поступления заявок на обработку в i-м процессе технологии применения элемента боевого порядка

$\lambda_{x,y,z}$ – кубический элемоб в прямоугольной системе координат в пространстве боя

$\lambda_{\text{зо}}$ – интенсивность выполнения задач обеспечения в информационно-техническом средстве

$\lambda_{\text{зу}}$ – интенсивность поступления задач управления в информационно-техническом средстве

$\lambda_{\text{ирз}}$ – интенсивность выполнения информационно-расчетных задач в информационно-техническом средстве

μ – максимальная производительность информационно-технического средства

μ_g – вероятность изначального заражения информационно-управляющей сети g-м экземпляром специального программного средства

$\mu_{\text{зо}}$ – ресурсоемкость задач обеспечения в информационно-техническом средстве

$\mu_{\text{зу}}$ – ресурсоемкость задач управления в информационно-техническом средстве

$\mu_{\text{ирз}}$ – ресурсоемкость информационно-расчетных задач в информационно-техническом средстве

$v_i(\gamma)$ – скорость i-го элемента боевого порядка при движении по элемобу γ-го типа

Ξ – конечное непустое множество сообщений с уникальной семантикой

Ξ_k – событие воздействия специального программного средства k-го типа на информационно-техническое средство

ξ_i – вероятность подмены информации в i-м элементе боевого порядка разведывательно-диверсионными подразделениями противника

$\xi_{\text{боп}}$ – весовой коэффициент боевого опыта

$\xi_{\text{бп}}$ – весовой коэффициент боевой подготовки

π – множество цепочек состояний, содержащих информационные элементы, используемые в рассматриваемом состоянии

$\wp_{\text{и}}$ – вес совокупности исполнительных потоков информации

$\wp_{\text{р}}$ – вес совокупности разведывательных потоков информации

$\wp_{\text{у}}$ – вес совокупности управляющих потоков информации

$\rho_{i,j}$ – стоимость j-го информационно-технического средства или устройства в i-м элементе боевого порядка

Σ – счетчик несовпадений

$\sum$ – множество всех нештатных состояний информационно-технического средства

ς – шаг дискретизации параметра масштабирования боя

σ – цепочка из состояний локального процесса, описывающая путь информационного элемента от состояния, в котором он возник, до состояния, в котором использован

τ – шаг дискретизации времени боя

$\tau_{i,j}$ – среднестатистический временной интервал между штатными сеансами связи i-го узла с j-м узлом

$\tau_{\text{мин}}$ – продолжительность временного слота в сети цифровой радиосвязи

τ_v – длительность интервала внедрения нескрытного специального программного средства v-го типа

$\varphi_{n(m),s}$ – коэффициент боевой соизмеримости s-го образца информационно-технического средства/устройства в $n(m)$-м элементе боевого порядка

$\phi^{\text{A}}(f, n)$ – коэффициент противодействия выполнению боевого цикла n-м элементом с функцией разведки и f-м элементом с функцией огневого поражения воинского формирования А

$\chi_{n(m)}^{\text{А(Б)}}(t)$ – устойчивость к диверсии $n(m)$-го элемента боевого порядка воинского формирования А(Б) в момент времени t

Ψ – множество состояний локального процесса функционирования информационно-технического средства, непосредственно использующих информационные элементы из локальных процессов других информационно-технических средств

$\boldsymbol{\Psi}_g$ – множество траекторно-временных матриц позиционной динамики боя

$\Psi_{\text{кр}}$ – множество искомых нештатных состояний информационно-технического средства

$\psi_{n(m)}^{\text{А(Б)}}(t)$ – работоспособность $n(m)$-го элемента боевого порядка воинского формирования А(Б) в момент времени t

Ω – вспомогательная переменная

$\boldsymbol{\Omega}_g$ – траекторная матрица g-го альтернативного варианта позиционной динамики боя

$\Omega_{i,j,\mu,r,k}^{+}$ – k-й элемент множества предусмотренных моментов времени передачи сообщения r-го типа в μ-м процессе j-го информационно-технического средства i-го образца автоматизированной системы

$\Omega_{i,j,\mu,r,k}^{-}$ – k-й элемент множества непредусмотренных моментов времени передачи сообщения r-го типа в μ-м процессе j-го информационно-технического средства i-го образца автоматизированной системы

$\Omega_{i,j,\mu,r,k}^{\sim}$ – k-й элемент множества моментов времени передачи сообщения r-го типа в μ-м процессе j-го информационно-технического средства i-го образца

автоматизированной системы, длительность интервалов между которыми синхронизирована с каналом связи, обеспечивающим этот процесс

$\omega_{i,j,k,s}$ – вес *s*-го боевого эпизода в *k*-м тактическом районе *j*-го оперативного района *i*-го оптативно-стратегического района

ϑ_i – вероятность разведки информации *i*-го элемента разведывательно-диверсионными подразделениями противника

$Э^A$ – множество координат, доступных для элемента боевого порядка воинского формирования А

$\aleph$ – множество параметров управления элемента боевого порядка воинского формирования

$\lfloor ... \rfloor$ – знак округления до ближайшего целого в меньшую сторону

$\lceil ... \rceil$ – знак округления до ближайшего целого в большую сторону

$\#$ – знак конкатенации элементов в цепочке

$\varnothing$ – знак пустого множества

$\forall$ – квантор общности «для всех … истинно …»

$\exists$ – квантор существования «существует … такое, что …»

$\in$ – знак принадлежности

$\Rightarrow$ – символ следствия

$\Leftrightarrow$ – символ эквивалентности

$\subseteq$ – подмножество с возможностью равенства

$\vee$ – логическое «ИЛИ»

$\wedge$ – логическое «И»

$\cup$ – объединение множеств

$\cap$ – пересечение множеств

$\succ$ – знак отношения предпочтения

$\vdash_i$ – отношение на множестве $Z \times Z$

$\vdash_r$ – отношение на множестве $Z \times \Xi \times Z$, описывающее получения сообщения

$\vdash_s$ – отношение на множестве $Z \times \Xi \times Z$, описывающее передачу сообщения

: – разделитель, означающий «такой, что»

{<…>} – множество кортежей

{…} – множество элементов

| – ограничение

|…| – количество элементов в множестве

<…> – упорядоченное множество (кортеж)

~,*,# в нижнем индексе – обозначение любой функции, любого номера элемента боевого порядка или любой подсистемы воинского формирования

Глоссарий терминов и определений

В настоящей монографии используются следующие специальные термины и соответствующие им определения.

автоматизированная система: Система, состоящая из персонала и комплекса средств автоматизации его профессиональной деятельности, реализующая информационную технологию выполнения установленных функций [84].

автоматизированная система воинского формирования: Автоматизированная система, обеспечивающая с применением средств вычислительной техники выполнение одного, нескольких или всех этапов одного или нескольких боевых циклов воинского формирования.

безопасность информации (данных): Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, целостность и доступность [86].

боевая ситуация: Совокупность условий и обстоятельств в бою.

боевая техника: Часть военной техники, предназначенная для боевых действий.

боевой потенциал воинского формирования: Интегральный показатель, характеризующий максимальный объем боевых задач, который может выполнить воинское формирование по своему функциональному предназначению в расчетных условиях применения [46, 56]. В монографии: доля воинского формирования, выполняющего заданную боевую задачу в расчетных условиях применения, которая остается после выполнения этой задачи. Понятие «боевой потенциал» применимо к воинскому формированию только для заданных условий боевой обстановки.

боевой порядок: Построение (расположение) соединений, частей и подразделений с их средствами усиления для ведения боя.

боевой цикл: Повторяющаяся последовательность действий по сбору информации, ее анализу и осознанию, планированию, принятию решения и его исполнению, которую реализует воинское формирование или его элемент (элементы) в боевых условиях [175, 272]. Синоним терминов «цикл «разведка-поражение», «цикл управления», «цикл боевого управления», «управленческий цикл», «цикл выполнения боевого задания».

боевой эпизод: Промежуток времени, в течение которого ни один элемент боевых порядков противоборствующих воинских формирований не находится в неподвижном состоянии дважды. Не путать с боевой ситуацией. В каждом боевом эпизоде местоположение всех элементов боевых порядков приводится к статичному с использованием методики в параграфе 5.2.

военная техника: Техника, предназначенная для ведения и обеспечения боевых действий, управления войсками, их обучения, испытаний и обеспечения заданного уровня готовности этой техники к использованию по назначению.

воинское формирование: Обобщенное наименование подразделений, воинских частей, соединений, объединений и иных структурных единиц вооруженных сил и других войск [74].

вооружение: Часть боевой техники, представляющая собой совокупность оружия, технических средств, обеспечивающих его применение, и средств воздействия.

декларативная программная помеха: Специальное программное средство, переносимое электромагнитной волной (или электрическим током), воспринимаемое целевым объектом как легитимное сообщение и предназначенное для нарушения работоспособности приемо-передающей аппаратуры.

доступность информации: Состояние информации, при котором к ней обеспечивается беспрепятственный доступ субъектов, имеющих на это полномочия.

заразность информационно-технического средства: Способность информационно-технического средства заражать специальными программными средствами, находящимися в его программном обеспечении, информационно-технические средства, с которыми оно взаимодействует по телекоммуникационному протоколу.

защищенность: Состояние надежной безопасности, защиты от кого-либо или от чего-либо [123].

информатизация: Процесс внедрения цифровых информационных технологий.

информационная сфера: Совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [108].

информационная технология (в автоматизированных системах): Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных [84].

информационно-техническое воздействие: Совокупность мероприятий и действий по реализации кибератак на информационно-технические средства автоматизированных систем, а также по их электромагнитному (в том числе радиоэлектронному) и акустическому (в различных средах) подавлению и поражению.

информационно-техническое средство: Изделие и/или его составные части, в основу функционирования которых положены принципы радиотехники

и/или электроники, предназначенные для формирования, обработки, хранения и передачи информации [16].

информационное оружие: Оружие, поражающее действие которого основано на использовании средств и технологий разрушения, подавления, поражения и (или) защиты целей информационной сферы. Включает информационно-техническое и информационно-психологическое оружие.

информационно-психологическое оружие: Психотропное оружие, психотронное оружие, психогенное (в том числе лингвистическое) оружие, психосоматическое оружие, психофизическое оружие, средства информационно-психологической защиты, обеспечивающие средства (средства объективного контроля и поддержки принятия решений).

информационно-техническое оружие: Средства технической разведки, кибероружие и средства защиты от него, электромагнитное оружие (средства электромагнитного (в том числе радиоэлектронного, оптоэлектронного) подавления и поражения в различных диапазонах длин электромагнитных волн), средства акустического подавления и поражения в различных средах, самонаводящееся на излучение оружие, средства имитации обстановки, средства искажения среды распространения волн в различных средах, средства противодействия разведке, обеспечивающие средства (средства объективного контроля и поддержки принятия решений).

информация: Сведения (сообщения, данные) независимо от формы их представления [260].

кибератака (в компьютерной сфере): Синоним термина «компьютерная атака».

киберзащита (в компьютерной сфере): Процесс обеспечения защищенности программного обеспечения автоматизированных систем от кибератак.

кибернетика: Наука об общих закономерностях получения, хранения, преобразования и передачи информации в сложных управляющих системах, будь то машины, живые организмы или общество [273].

кибероперация (в компьютерной сфере): Операция, проводимая в киберпространстве воинскими формированиями, оснащенными средствами реализации кибератак.

кибероружие (в компьютерной сфере): Оружие, поражающее действие которого основано на использовании средств и технологий разрушения, подавления, поражения и (или) защиты информационно-технических средств.

киберпространство: Синоним термина «информационная сфера».

когнитивный субфактор: Субфактор фактора соотношения сил, влияющего на успех в бою, представляющий собой совокупность используемых в боевых циклах противоборствующих воинских формирований данных и алгоритмов их обработки, конфиденциальность, целостность и

доступность которых каждая из сторон стремится нарушить у противника и сохранить у себя для нанесения боевому потенциалу противника максимально возможного ущерба.

компьютерная атака: Целенаправленное воздействие программными и/или программно-аппаратными средствами на автоматизированную систему в целях нарушения и/или прекращения ее функционирования и/или создания угрозы безопасности обрабатываемой такой системой информации [103, 318].

конфиденциальность информации: Состояние информации, когда она принадлежит только тем субъектам, которые имеют на ее использование соответствующие полномочия.

кортеж: Упорядоченное множество.

коэффициент боевой соизмеримости: Интегральный показатель, характеризующий способность объекта выполнять совокупность заданий по целевому назначению при реализации предельных тактико-технических характеристик за заданное время в заданных условиях в составе своего воинского формирования против заданного противника при нормативных уровнях возможностей тылового обеспечения и подготовки личного состава (является относительным).

локальный процесс: Процесс функционирования информационно-технического средства, описываемый множеством взаимосвязанных состояний, переходы между которыми могут быть связаны с внутренними событиями, с передачей и с приемом сообщений.

оружие: Изделие, предназначенное для поражения цели или доставки к ней средств воздействия. Средствами воздействия могут быть: боеприпасы, боевая часть управляемой ракеты, лазерный луч, инфракрасное излучение и др. Средства воздействия расходуются и пополняются.

подавление: Воздействие на объект, нарушающее его работоспособное состояние, которое восстанавливается без проведения ремонта после завершения воздействия или в процессе воздействия в результате применения мер помехозащиты.

подверженность информационно-технического средства дезинформации: Способность информационно-технического средства противодействовать находящимся в его программном обеспечении специальным программным средствам, искажающим содержащиеся в нем данные и/или внедряющим заведомо ложные данные.

подверженность информационно-технического средства перехвату управления: Способность информационно-технического средства противодействовать находящимся в его программном обеспечении специальным программным средствам, осуществляющим перехват управления этим средством и/или управляемыми им устройствами.

подверженность информационно-технического средства разведке: Способность информационно-технического средства противодействовать находящимся в его программном обеспечении специальным программным средствам, получающим доступ к его данным и алгоритмам их обработки.

поражение: Воздействие на объект, нарушающее его работоспособное состояние, которое может быть восстановлено только после проведения ремонта.

протокол: Правила (соглашения, стандарт) передачи информации в сети.

процедурная программная помеха: Специальное программное средство, переносимое электромагнитной волной (или электрическим током), воспринимаемое целевым объектом как легитимное, способное проникать в атакуемую автоматизированную систему и приводить ее в нужное для атакующей стороны состояние.

распределенный процесс: Процесс информационного взаимодействия нескольких информационно-технических средств, каждому из которых соответствует собственный локальный процесс.

скрипт-кидди: Злоумышленник, использующий чужие наработки и не понимающий принципа работы используемых средств реализации кибератак.

специальное программное средство: Данные, предназначенные для управления компонентами систем обработки информации информационно-технических объектов/средств в целях реализации определенного алгоритма, не предусмотренного штатным режимом их работы.

способ реализации кибератаки: Последовательность действий, необходимых для формирования совокупности факторов, нацеленных на нарушение конфиденциальности, целостности и/или доступности обрабатываемой информационно-техническим средством информации и/или алгоритмов ее обработки в этом средстве, и достаточных для реализации с использованием электромагнитных полей и/или электрических токов условий функционирования этого средства, при выполнении которых оно переходит в состояние потери работоспособности, сниженной эффективности функционирования, управляемости или доступности для углубленного анализа источником воздействия.

телекоммуникационное оборудование: Совокупность информационно-технических средств, необходимая для информационного взаимодействия пространственно распределенных элементов автоматизированной системы.

угроза безопасности информации: Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [94].

устойчивость элемента боевого порядка к диверсии: Способность элемента боевого порядка противодействовать его выводу из строя или

нелегитимному применению штатным личным составом, диверсионно-разведывательными группами противника или специальными программными средствами.

устройство: Техническое средство, не относящееся к классам радиоэлектронных средств, средств вычислительной техники и средств электронной автоматики.

уязвимость: Недостаток (слабость) программного (информационно-технического) средства или автоматизированной системы в целом, который (которая) может быть использован(а) для реализации угроз безопасности информации [94].

целостность информации: Состояние информации, при котором обеспечивается неизменность ее формы представления и содержания в условиях или в результате преднамеренного или непреднамеренного деструктивного воздействия.

электронная компонентная база: Совокупность изделий электронной техники, квантовой электроники и/или электротехнических изделий, представляющих собой сборочную единицу или их совокупность, обладающих конструктивной целостностью, принцип действия которых основан на электрофизических, электрохимических, электромеханических, фотоэлектронных и/или электронно-оптических процессах и явлениях, не подвергаемых изменениям в процессе применения при создании образцов радиоэлектронной аппаратуры, в которых они применяются, изготавливаемых по самостоятельным комплектам конструкторской и технологической документации, выполняющих функции генерирования, преобразования, переключения, задержки, распределения, запоминания, передачи и фильтрации радиочастотных и электрических сигналов, и не подлежащих восстановлению или ремонту (далее – электрорадиоизделия), а также электронных модулей нулевого уровня, представляющих собой совокупность электрически соединенных электрорадиоизделий, образующих функционально и конструктивно законченные сборочные единицы, предназначенные для реализации функций приема, обработки, преобразования, хранения и/или передачи информации или формирования (преобразования) энергии, выполненные на основе несущих конструкций или размещенных на общей подложке, обладающие свойствами конструктивной и функциональной взаимозаменяемости и рассматриваемые как единое целое с точки зрения требований к разработке, производству, приемке, поставке и эксплуатации [96].

элемент боевого порядка: Обособленная в пространстве боя часть построения (расположения) воинского формирования для ведения боя.

элемоб: Акроним словосочетания «элементарный объем». Элементарный объем имеет кубическую форму. Из элементарных объемов состоит трехмерное пространство, в котором ведется бой.

Литература

1 Абчук В. А. Справочник по исследованию операций. – М.: Воениздат, 1979. – 368 с.

2 Агафонов А. А., Артюх С. Н., Афанасьев В. И., Афанасьева Е. М., Бостынец И. П., Быков В. В., Донцов А. А., Ермаков А. И., Калинков А. К., Каунов А. Е., Кирсанов Э. А., Лаптев И. В., Ложкин К. Ю., Марек Я. Л., Миронов В. А., Нечаев С. С., Новиков И. И., Овчаренко Л. А., Огреб С. М., Поддубный В. Н., Понькин В. А., Радзиевский В. Г., Разиньков С. Н., Романов А. Д., Рыжов А. В., Сирота А. А., Соловьев В. В., Сорокин Ю. А., Сухоруков Ю. С., Телков А. Ю., Уфаев В. А., Харченко Т. В., Юхно П. М., Яньшин С. Н. Современная радиоэлектронная борьба. Вопросы методологии. – М.: Радиотехника, 2006. – 424 с.

3 Агеев С. А., Саенко И. Б., Егоров Ю. П., Гладких А. А., Богданов А. В. Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2014. № 3. С. 78-88.

4 Адамадзиев К. Р., Рабаданова Р. М. Оценка уровня информатизации регионов России: динамика, межрегиональные различия // Фундаментальные исследования. 2013. № 4. С. 462-466.

5 Алексеев О. Г., Анисимов В. Г., Анисимов Е. Г. Марковские модели боя. – М.: МО СССР, 1985. – 85 с.

6 Алексеев О. Г., Анисимов В. Г., Анисимов Е. Г. Модели распределения средств поражения в динамике боя. – М.: МО СССР, 1989. – 110 с.

7 Алиев Т. И. Основы моделирования дискретных систем. – СПб: СПбГУ ИТМО, 2009. – 363 с.

8 Американская АСУВ FBCB2. Часть 1. – URL: http://pentagonus.ru/publ/amerikanskaja_asuv_fbcb2_2012/11-1-0-22-01 (дата обращения 01.07.2021).

9 Андреев С. М., Демков В. В., Кривошеев Р. А. Методика оценки эффективности системы тылового обеспечения бригады материально-технического обеспечения // Вестник Военной академии материально-технического обеспечения. 2016. № 3. С. 31-38.

10 Антонов С. Г., Климов С. М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Т. 17. № 1. С. 32-39.

11 Антонович П. И. О сущности и содержании кибервойны // Военная Мысль. 2011. № 7. С. 39-46.

12 Арбузов И. В., Болховитинов О. В., Волочаев О. В., Вольнов И. И., Гостев А. В., Мышкин Л. В., Хабиров Р. Н., Шеховцов В. Л. Боевые авиационные комплексы и их эффективность. – М.: ВВИА им. проф. Н. Е. Жуковского, 2008. – 224 с.

13 Армия Ирана перехватила управление американскими БПЛА над Сирией и Ираком. – URL: http://rusvesna-su.turbopages.org/rusvesna.su/s/news/1550785364 (дата обращения 01.07.2021).

14 Архангельский Б. В., Черняховский В. В. Поиск устойчивых ошибок в программах. – М.: Радио и связь, 1989. – 240 с.

15 Астапенко Ю. А., Вайпан С. Н., Вакуленко А. А., Вакуленко Н. Н., Верба Б. С., Грибков Р. А., Гузенко О. Б., Дод В. Н., Зайцев А. Г., Иванов А. Н., Ионкин А. А., Король О. В., Кузьмин Г. В., Лясковский В. Л., Марухленко А. С., Неплюев О. Н., Приступюк И. А., Проскурин В. И., Рюмшин А. Р., Самушкин А. Н., Сенчаков Г. В., Турко Н. И., Шевчук В. И., Шевчук Д. В., Ягольников С. В. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза. – М.: Радиотехника, 2015. – 312 с.

16 Балыбин В. А., Донсков Ю. Е. Бойко А. А. О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства // Военная Мысль. 2013. № 9. С. 28-32.

17 Банк данных угроз безопасности информации // ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: http://bdu.fstec.ru (дата обращения 01.07.2021).

18 Бегаев А. Н., Гречишников Е. В., Добрышин М. М., Закалкин П. В. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий // Вопросы кибербезопасности. 2018. № 3. С. 2-8.

19 Бегаев А. Н., Стародубцев Ю. И., Федоров В. Г. Методика оценки управляемости фрагмента сети связи общего пользования с учетом влияния множественности центров управления и деструктивных программных воздействий // Вопросы кибербезопасности. 2017. № 4. С. 32-39.

20 Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программных средств и систем. – СПб.: Питер, 2004. – 318 с.

21 Белов А. С., Скубьев А. В. Теоретический подход по оценке и обеспечению живучести распределенных сетей связи в условиях информационного противоборства // Наукоемкие технологии в космических исследованиях Земли. 2018. № 2. С. 22-33.

22 Белоглазов Д. А., Гайдук А. Р., Косенко Е. Ю., Медведев М. Ю., Пшихопов В. Х., Соловьев В. В., Титов А. Е., Финаев В. И., Шаповалов И. О. Групповое управление подвижными объектами в неопределенных средах. – М.: Физматлит, 2015. – 305 с.

23 Белотелов Н. В., Бродский Ю. И., Павловский Ю. Н. Сложность. Математическое моделирование. Гуманитарный анализ: Исследование исторических, военных, социально-экономических и политических процессов. – М.: ЛИБРОКОМ, 2013. – 320 с.

24 Белый А. Ф. Управление функциональной устойчивостью комплексов средств автоматизации в условиях программно-аппаратных воздействий // Стратегическая стабильность. 2011. № 4. С. 34-36.

25 Бирюков Д. Н., Ломако А. Г., Петренко С. А. Интеллектуальные системы предотвращения кибератак // The 2019 Symposium on Cybersecurity

of the Digital Economy. Труды третьей Международной научно-технической конференции. 2019. С. 184-195.

26 Бирюков Д. Н., Ломако А. Г., Петренко С. А. Порождение сценариев предупреждения кибератак // Защита информации. INSIDE. 2017. № 4. С. 70-78.

27 Бойко А. А, Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.

28 Бойко А. А. Боевая эффективность кибератак: аналитическое моделирование современного боя // Системы управления, связи и безопасности. 2020. № 4. С. 101-133.

29 Бойко А. А. Боевая эффективность кибератак: практические аспекты // Системы управления, связи и безопасности. 2020. № 4. С. 134-162.

30 Бойко А. А. Метод разработки иерархических многоуровневых моделей для аналитической оценки соотношения сил воинских формирований // Военная Мысль. 2019. № 7. С. 104-113.

31 Бойко А. А. О защищенности информации воинских формирований в современном вооруженном противоборстве // Военная Мысль. 2016. № 4. С. 38-51.

32 Бойко А. А. Способ аналитического моделирования боевых действий // Системы управления, связи и безопасности. 2019. № 2. С. 1-27.

33 Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. № 5. С. 196-211.

34 Бойко А. А. Способ оценки уровня информатизации образцов вооружения // Системы управления, связи и безопасности. 2019. № 1. С. 264-275.

35 Бойко А. А. Способ стратифицированного аналитического описания процесса функционирования информационно-технических средств // Информационные технологии. 2015. № 1. С. 35-42.

36 Бойко А. А., Будников С. А. Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно-технического средства // Радиотехника. 2015. № 4. С. 136-141.

37 Бойко А. А., Будников С. А. Обеспечение конфликтной устойчивости программной реализации алгоритмов управления радиоэлектронной аппаратурой пространственно распределенных организационно-технических систем // Системы управления, связи и безопасности. 2019. № 4. С. 100-139.

38 Бойко А. А., Дегтярев И. С. Метод оценки весовых коэффициентов элементов организационно-технических систем // Системы управления, связи и безопасности. 2018. № 2. С. 245-266.

39 Бойко А. А., Иванников К. С., Ищук В. А., Стрельников С. И. Расчетно-моделирующий комплекс для оценки эффективности боевых действий // Военная Мысль. 2020. № 12. С. 56-64.

40 Бойко А. А., Иванников К. С., Кузнецов Д. А. Методика построения графоаналитической модели позиционной динамики боя на основе вероятностно-временной синхронизации действий элементов боевых порядков

воинских формирований // Системы управления, связи и безопасности. 2020. № 2. С. 24-48.

41 Бойко А. А., Обущенко Е. Ю., Щеглов А. В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2017. № 2. С. 33-45.

42 Бойко А. А., Храмов В. Ю. Методика оценки правильности и устойчивости к ошибкам специального программных средств автоматизированных систем военного назначения // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2007. № 1. С. 106-115.

43 Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

44 Большаков К. Р. О проблемах протоколов взаимодействия распределенных вычислительных систем // Информационно-управляющие системы. 2004. № 6. С. 18-20.

45 Большой энциклопедический словарь. – М.: Советская энциклопедия, 1993. – 1632 с.

46 Бонин А. С., Горчица Г. И. О боевых потенциалах образцов ВВТ, формирований и соотношениях сил группировок сторон // Военная Мысль. 2010. № 4. С. 61-67.

47 Борисов В. В., Сысков В. В. Мультиагентное моделирование сложных организационно-технических систем в условиях противоборства // Информационные технологии. 2012. № 4. С. 7-14.

48 Бородакий Ю. В. Информатизация вооруженных сил // Военная Мысль. 2009. № 6. С. 33-41.

49 Будко П. А. Управление ресурсами информационно-телекоммуникационных систем. Методы оптимизации. – СПб.: ВАС, 2012. – 512 с.

50 Будников С. А. Модель обобщенного конфликта радиоэлектронных средств // Радиотехника. 2008. № 11. С. 8-10.

51 Будников С. А., Гревцев А. И., Иванцов А. В., Кильдюшевский В. М., Козирацкий А. Ю., Козирацкий Ю. Л., Кущев С. С., Лысиков В. Ф., Паринов М. Л., Прохоров Д. В. Модели информационного конфликта средств поиска и обнаружения. – М.: Радиотехника, 2013. – 232 с.

52 Будников С. А., Козирацкий Ю. Л., Паринов М. Л. Обобщенная модель конфликта основных систем вооружения // Вооружение и экономика. 2011. № 1. С. 13-23.

53 Буравлев А. И., Горшков П. С. К вопросу о построении агрегированной модели противоборства группировок войск // Вооружение и экономика. 2017. № 5. С. 35-48.

54 Буравлев А. И., Русанов И. П. Динамика боевых потенциалов // Военная Мысль. 2011. № 1. С. 26-30.

55 Буравлев А. И., Тимофеев М. В. Анализ динамики противоборства однородных группировок при различных стратегиях огневых воздействий // Вооружение и экономика. 2011. № 3. С. 17-22.

56 Буравлев А. И., Цырендоржиев С. Р., Брезгин В. С. Основы методологического подхода к оценке боевых потенциалов образцов ВВТ и воинских формирований // Вооружение и экономика. 2009. № 3. С. 4-12.

57 Бурдонов И. Косачев А., Сортов А. Распределенные алгоритмы на корневых неориентированных графах // Труды ИСП РАН. 2017. Т. 29. № 5. С. 283-310.

58 Бурдонов И. Б., Евтушенко Н. В., Косачев А. С. Синтез тестов для синхронной композиции детерминированных и полностью определенных автоматов // Научный сервис в сети Интернет: труды XX Всероссийской научной конференции. – М.: ИПМ им. М. В. Келдыша, 2018. С. 100-110.

59 Бурдонов И. Б., Косачев А. С. Тестирование системы автоматов // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2017. № 38. С. 63-71.

60 Буренин А. Н., Воробьев С. П., Давыдов А. Е., Курносов В. И. Инфокоммуникационные сети: энциклопедия. Том 2: Основы управления и обеспечения безопасности связи и информации в инфокоммуникационных сетях. – СПб.: Наукоемкие технологии, 2019. – 611 с.

61 Буренок В. М., Горчица Г. И., Ищук В. А., Пишков В. Н. Развитие систем компьютерного моделирования боевых действий с использованием полномасштабных технологий формирования виртуальной реальности // Известия РАРАН. 2017. № 1. С. 3-8.

62 Буренок В. М., Горчица Г. И., Ищук В. А., Цырендоржиев С. Р. Проблемные вопросы моделирования военных действий в целях создания перспективных систем вооружения // Военная Мысль. 2015. № 11. С. 34-45.

63 Буренок В. М., Цырендоржиев С. Р. Создание системы моделирования необходимое условие развития ВС РФ // Вооружение и экономика. 2013. № 4. С. 4-11.

64 Быстрых Р. А., Асташов Р. А., Уткин Д. М. Направление совершенствования программно-технических комплексов в целях повышения командной управляемости перспективных образцов бронетанковой военной техники для ЕСУ ТЗ // Теория и техника радиосвязи. 2018. № 2. С. 34-38.

65 Вавренюк А. Б., Васильев Н. П., Вельмякина Е. В., Гуров Д. В., Иванов М. А., Матвейчиков И. В., Мацук Н. А., Михайлов Д. М., Шустова Л. И. Разрушающие программные воздействия: учебно-методическое пособие. – М.: НИЯУ МИФИ, 2011. – 328 с.

66 Вайнер А. Я. Тактические расчеты. – М.: Воениздат, 1982. – 176 с.

67 Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. – М.: Советское радио, 1968. – 448 с.

68 Веденеев А. В., Махинов Ю. Н., Толстых Н. Н. Модельное представление корпоративной сети в условиях информационного конфликта // Теория и техника радиосвязи. 2019. № 4. С. 116-123.

69 Вишневский В. М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с.

70 Вишневский В. М., Ляхов А. И., Сафонов А. А. Исследование эффективности механизмов синхронизации в беспроводных персональных сетях со сложной структурой // Информационные технологии и вычислительные системы. 2008. № 3. С. 63-77.

71 Владимиров В. И., Владимиров И. В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: Военный авиационный инженерный университет, 2008. – 231 с.

72 Владимиров В. И., Лихачев В. П., Шляхин В. М. Антагонистический конфликт радиоэлектронных систем. Методы и математические модели. – М.: Радиотехника, 2004. – 384 с.

73 Владимиров В. И., Стучинский В. И. Выбор системы показателей информационного превосходства в операциях в условиях двухсторонней радиоэлектронной борьбы // Военная Мысль. 2016. № 10. С. 33-39.

74 Военный энциклопедический словарь. – М.: Военное издательство, 2007. – 831 с.

75 Воробьев И. Н., Киселев В. А. Киберпространство как сфера непрямого вооруженного противоборства // Военная Мысль. 2014. № 12. С. 21-28.

76 Высторобский Г. Д., Бакумов В. В. Актуальное вопросы управления в единой многофункциональной системе радиоэлектронной борьбы // Военная Мысль. 2010. № 8. С. 49-54.

77 Вялых А. С., Вялых С. А., Сирота А. А. Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта // Информационные технологии. 2012. № 9. С. 15-21.

78 Галатенко В. А. Основы информационной безопасности: учебное пособие. – М.: ИНТУИТ, 2008. – 205 с.

79 Гирин А. В. Усовершенствованная методика определения боевых возможностей общевойсковой группировки войск // Военная Мысль. 2012. № 10. С. 26-30.

80 Глазунов О. А., Мокроусов А. Н., Осицкая Т. В. Носимые программно-технические комплексы // Теория и техника радиосвязи. 2018. № 2. С. 39-42.

81 Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. – М.: Наука, 1987. – 336 с.

82 Горчица Г. И., Ищук В. А. Проблемы применения и направления развития систем моделирования в интересах сопровождения создания перспективных комплексов вооружения // Известия РАРАН. 2018. № 4. С. 15-22.

83 ГОСТ 19.701-90 Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Введ. 1992–01–01. –

М.: Государственный комитет СССР по управлению качеством продукции и стандартам, 1990. – 27 с.

84 ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введ. 1991–01–01. – М.: Государственный комитет СССР по стандартам, 1990. – 16 с.

85 ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Введ. 1996–01–01. – М.: Стандартинформ, 2006. – 8 с.

86 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введ. 2007–01–01. – М.: Стандартинформ, 2006. – 12 с.

87 ГОСТ Р 51189-98 Средства программные систем вооружения. Порядок разработки. Введ. 1999–01–01. – М.: ГОССТАНДАРТ России, 1998. – 16 с.

88 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введ. 2007–01–01. – М.: ГОССТАНДАРТ России, 2007. – 10 с.

89 ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения. Введ. 2001–01–01. – М.: Стандартинформ, 2000. – 11 с.

90 ГОСТ Р 51904-2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию. Введ. 2003–01–01. – М.: Стандартинформ, 2002. – 67 с.

91 ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введ. 2009–01–01. – М.: Стандартинформ, 2009. – 12 с.

92 ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. Введ. 2010–01–01. – М.: Стандартинформ, 2010. – 12 с.

93 ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016–01–01. – М.: Стандартинформ, 2015. – 22 с.

94 ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей. Введ. 2016–04–01. – М.: Стандартинформ, 2015. – 17 с.

95 ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программных средств. Общие требования. Введ. 2017–01–01. – М.: Стандартинформ, 2016. – 24 с.

96 ГОСТ Р 58857-2020 Ракетно-космическая техника. Электронная компонентная база. Общие положения. Введ. 2020–08–01. – М.: Стандартинформ, 2020. – 24 с.

97 ГОСТ Р ИСО 5725-1-2002 Точность (правильность и прецизионность) методов и результатов измерений. Часть 1. Основные положения и определения. Введ. 2003–01–01. – М.: ГОССТАНДАРТ России, 2002. – 23 с.

98 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введ. 2014–01–01. – М.: Стандартинформ, 2014. – 161 с.

99 ГОСТ Р ИСО/МЭК 27001-2013 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 2014–01–01. – М.: Стандартинформ, 2008. – 31 с.

100 ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Введ. 2000–01–01. – М.: ГОССТАНДАРТ России, 1999. – 62 с.

101 Гречишников Е. В., Добрышин М. М. Оценка эффективности деструктивных программных воздействий на сети связи // Системы управления, связи и безопасности. 2015. № 2. С. 135-146.

102 Громов М. Л., Евтушенко Н. В. Синтез различающих экспериментов для временных автоматов // Программирование. 2010. № 4. С. 40-50.

103 Громов М. Л., Евтушенко Н. В., Коломеец А. В. К синтезу условных тестов для недетерминированных автоматов // Программирование. 2008. № 6. С. 24-34.

104 Грошев С. Г. Применение технологии UniTesK для тестирования систем с различной конфигурацией активных потоков управления. – URL: http://software-testing.ru/ (дата обращения 01.07.2021).

105 Далингер Я. М., Бабанин Д. В., Бурков С. М. Математические модели распространения вирусов в компьютерных сетях различной структуры // Информатика и системы управления. 2012. № 3. С. 25-33.

106 Деменченок О. Г. Информационная безопасность: учебное пособие. – Иркутск: Восточносибирский институт МВД РФ, 2010. – 112 с.

107 Динер И. Я. Исследование операций. – Л.: ВМОЛУА, 1969. – 606 с.

108 Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 05.12.2016 № 646).

109 Долуханов М. П. Распространение радиоволн. Учебник для вузов. – М.: Связь, 1972. – 336 с.

110 Донсков Ю. Е., Зимарин В. И., Илларионов Б. В. Формализованное описание мобильных радиосетей передачи данных в интересах РЭБ // Военная Мысль. 2016. № 4. С. 32-37.

111 Донсков Ю. Е., Спасибухов С. Н., Демин В. Е. О системном подходе к моделированию конфликтного взаимодействия в радиоэлектронной борьбе // Военная Мысль. 2009. № 3. С. 31-39.

112 Донсков Ю. Е., Фомин В. В., Матвеев Д. С. Формирование группировок войск при подготовке и выполнении ими боевых задач в условиях сетецентризма // Военная Мысль. 2012. № 8. С. 14-21.

113 Дорохов В. Н., Ищук В. А. Боевые потенциалы подразделений как интегральный критерий оценки боевых возможностей воинских формирований и боевой эффективности ВВСТ // Известия РАРАН. 2017. № 4. С. 27-36.

114 Дроботун Е. Б. Риск-ориентированный подход к формированию функциональных требований к системам защиты от кибератак для автоматизированных систем управления. – Тверь: Издатель А. Н. Кондратьев, 2017. – 195 с.

115 Дроботун Е. Б. Теоретические основы построения систем защиты от кибератак для автоматизированных систем управления. – СПб.: Наукоемкие технологии, 2017. – 120 с.

116 Дроботун Е. Б., Бердышев В. П. Защита автоматизированных систем управления военного назначения от разрушающих программных воздействий // Военная Мысль. 2016. № 10. С.15-19.

117 Дружинин В. В., Конторов Д. С., Конторов М. Д. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

118 Дубограй И. В., Рябцев Р. А., Чуев В. Ю. Вероятностные модели двусторонних боевых действий многочисленных группировок при упреждающем ударе одной из них // Известия РАРАН. 2017. № 4. С. 37-46.

119 Дубровин А. С., Душкин А. В., Кочедыков С. С., Новосельцев В. И. К вопросу моделирования высоконадежного процесса обработки информации в автоматизированной системе специального назначения в условиях воздействия внутренних угроз информационной безопасности // Вестник Воронежского института ФСИН России. 2017. № 2. С. 48-54.

120 Дульнев П. А., Колесниченко А. П., Котов А. В. Системный анализ общевойскового боя. – М.: Граница, 2018. – 271 с.

121 Еременко В. Т., Парамохина Т. М. Метод формирования тестовых комплектов для протоколов безопасности в системах обработки данных // Информационные системы и технологии. 2015. № 2. С. 131-137.

122 Еременко В. Т., Парамохина Т. М., Кириченко О. Е. Математическое моделирование протоколов информационного обмена на основе расширенных конечных автоматов // Известия Орловского государственного технического университета. Серия: Информационные системы и технологии. 2007. № 4. С. 4-10.

123 Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. Том 1. – М.: Русский язык, 2000. – 1210 с.

124 Жидко Е. А., Разиньков С. Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности. 2018. № 1. С. 122-135.

125 Захаров Л. В., Богданов С. А. О выработке единых подходов к оценке боевых потенциалов // Военная Мысль. 1992. № 8-9. С. 42-49.

126 Захарченко Р. И., Королев И. Д., Саенко И. Б. Синергетический подход к обеспечению устойчивости функционирования автоматизированных

систем специального назначения // Системы управления, связи и безопасности. 2018. № 4. С. 207-225.

127 Иванкин М. П., Толстых Н. Н., Савинков А. Ю., Свердел В. Ф. К вопросу оценки эффективности функционирования систем программно-определяемого радио в условиях информационного конфликта // Теория и техника радиосвязи. 2018. № 4. С. 14-18.

128 Иванов С. С., Педенко Н. П., Таненя О. С. Методологические основы описания процессов общевойскового боя при имитационном моделировании // Военная Мысль. 2020. № 3. С. 74-83.

129 Калинин В. Н., Резников Б. А., Варакин Е. И. Теория систем и оптимального управления. Часть 1. Основные понятия, математические модели и методы анализа систем. – Л.: ВИКИ им. А.Ф. Можайского, 1979. – 320 с.

130 Калинин В. Н., Резников Б. А., Варакин И. С. Теория систем и оптимального управления. Часть 2. Понятия, модели, методы и алгоритмы оптимального выбора. – М.: МО СССР, 1987. – 589 с.

131 Канер С., Фолк Дж., Нгуен Е. Тестирование программных средств. – Киев: Издательство DiaSoft, 2001. – 554 с.

132 Карпов Ю. Г. Model Checking. Верификация параллельных и распределенных программных систем. – СПб.: БХВ-Петербург, 2010. – 560 с.

133 Карповский Е. Я., Чижов С. А. Надежность программной продукции. – Киев: Техника, 1990. – 160 с.

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

135 Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы: Каталист, 2008. – 316 с.

136 Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы. – М.: МГТУ имени Н. Э. Баумана, 2013. – 110 с.

137 Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Технологические основы. – М.: МГТУ имени Н. Э. Баумана, 2013. – 71 с.

138 Ковалев В. В., Компаниец Р. И., Новиков В. А. Верификация программ на основе соотношений подобия // Труды СПИИРАН. 2015. № 1 (38). С. 233-245.

139 Козирацкий А. Ю., Паринов М. Л. Методический подход к построению вероятностной модели конфликта сложных систем, обеспечивающей анализ динамики изменения их численностей // Вестник Воронежского военного института. 2006. № 1. С. 9-19.

140 Козирацкий Ю. Л., Ерофеев А. Н., Соколовский С. П. Модель конфликтного взаимодействия «нарушитель подсистема защиты информации автоматизированной системы управления» // Вестник Военного авиационного инженерного университета. 2012. № 1. С. 210-217.

141 Козирацкий Ю. Л., Иванцов А. В. Оценка оперативности выполнения противником циклических задач поражения в условиях противодействия его

техническим средствам разведки // Вооружение и экономика. 2014. № 1. С. 34-38.

142 Козирацкий Ю. Л., Паринов М. Л., Албузов А. Т., Иванцов А. В. Полумарковская модель конфликта противоборствующих группировок малых численностей // Радиотехника. 2017. № 9. С. 6-11.

143 Козирацкий Ю. Л., Паринов М. Л., Петренков С. В., Балаин С. Е., Будников С. А. Методические основы формирования модели конфликта // Телекоммуникации. 2011. № 4. С. 2-7.

144 Кокс Д., Смит В. Теория восстановления. – М.: Сов. радио, 1967. – 300 с.

145 Колесниченко В. И., Корниенко В. В., Семенов С. А. Оценка эффективности автоматизированной системы с ограниченными ресурсами // Вопросы радиоэлектроники. Системы отображения информации и управления спецтехникой. 2008. № 1. С. 16-23.

146 Кондратьев М. А. Методы прогнозирования и модели распространения заболеваний // Компьютерные исследования и моделирование. 2013. Т. 5. № 5. С. 863-882.

147 Коробейников А. С., Холуенко Д. С., Пасичник С. И. Эффективность группировки войск радиоэлектронной борьбы в ходе комплексного поражения информационно-управляющей системы противника // Военная Мысль. 2015. № 8. С. 30-34.

148 Костин Н. А. Методический подход к определению боевых потенциалов войсковых формирований // Военная Мысль. 2017. № 10. С. 44-48.

149 Костогрызов А. И., Зубарев И. В. Моделирование процессов для эффективного управления рисками в обеспечение качества и безопасности функционирования современных и перспективных систем реального времени // Радиопромышленность. 2017. № 2(27). С. 91-100.

150 Костогрызов А. И., Степанов П. В. Инновационное управление качеством и рисками в жизненном цикле систем. – М.: Изд-во «Вооружение. Политика. Конверсия», 2008. – 404 с.

151 Котенко В. И., Котенко И. Б., Коцыняк М. А., Лаута О. С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. № 6. С. 160-184.

152 Котенко И. В., Десницкий В. А. Противодействие целевым киберфизическим атакам в распределенных крупномасштабных критически важных системах // Защита информации. INSIDE. 2017. № 4. С. 66-69.

153 Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. 2007. № 4. С. 208-224.

154 Котенко И. В., Воронцов В. В., Уланов А. В. Модели и системы имитационного моделирования распространения сетевых червей // Труды СПИИРАН. 2007. № 4. С. 225-238.

155 Котенко И. В., Резник С. А., Шоров А. В. Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств // Труды СПИИРАН. 2009. № 8. С. 292-310.

156 Котенко И. В., Шоров А. В. Механизмы защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода «нервная система сети» // Вопросы защиты информации. 2013. № 2. С. 57-66.

157 Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: технические средства противодействия терроризму. 2019. № 1-2. С. 58-62.

158 Коцыняк М. А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. – СПб.: ЛО ЦНИИС, 2015. – 126 с.

159 Кочедыков С. С., Душкин А. В., Новосельцев В. И., Соколовский С. П. Моделирование системы конфликтных взаимодействий в информационной системе критического применения // Вестник Воронежского института ФСИН России. 2017. № 4. С. 74-84.

160 Кропачева М. С., Легалов А. И. Формальная верификация программ, написанных на функционально-потоковом языке параллельного программирования // Моделирование и анализ информационных систем. 2012. № 5. С. 81-99.

161 Крутских П. П., Губарев В. А. Концептуальная модель конфликта в информационной борьбе // Радиотехника. 1998. № 6. С. 29-31.

162 Кузнецов В. И. Радиосвязь в условиях радиоэлектронной борьбы. – Воронеж: ВНИИС. 2002. – 403 с.

163 Кузнецов В. И. Системное проектирование радиосвязи: Методы и обеспечение. Часть 1. Системотехника. – Воронеж: ВНИИС, 1994. – 387 с.

164 Кулямин В. В., Петренко А. К., Косачев А. С., Бурдонов И. Б. Подход UniTesK к разработке тестов // Программирование. 2003. № 29. С. 25-43.

165 Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.

166 Ласточкин Ю. И., Ярыгин Ю. Н., Бывших Д. М. Методическое обеспечение обоснования способов боевого применения сил и средств радиоэлектронной борьбы при противодействии радиоэлектронной разведке в операциях объединений Сухопутных войск // Военная Мысль. 2018. № 6. С. 58-66.

167 Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления. – Воронеж: Научная книга, 2014. – 590 с.

168 Липаев В. В. Тестирование программ. – М.: Радио и связь, 1986. – 296 с.

169 Ломако А. Г., Еремеев М. А., Новиков В. А. Метод выявления дефектов и недокументированных возможностей программ // Информационное противодействие угрозам терроризма. 2010. № 14. С. 46-49.

170 Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. – СПб.: Наукоемкие технологии, 2018. – 122 с.

171 Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: МГГУ им. М. А. Шолохова, 2009. – 372 с.

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

173 Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. – СПб.: Наукоемкие технологии, 2020. – 337 с.

174 Макаренко С. И. Справочник научных терминов и обозначений. – СПб.: Наукоемкие технологии, 2019. – 254 с.

175 Макаренко С. И., Иванов М. С. Сетецентрическая война - принципы, технологии, примеры и перспективы. – СПб.: Наукоемкие технологии, 2018. – 898 с.

176 Макаренко С. И., Михайлов Р. Л. Информационные конфликты анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178.

177 Масленников О. В. Основные направления информатизации Вооруженных Сил Российской Федерации в современных условиях // Информационные технологии, связь и защита информации МВД России. 2016. С. 26-27.

178 Меркулов С. Н., Сухоруков Ю. С., Донсков Ю. Е. Проблемы автоматизации интеллектуальной поддержки принятия решений общевойсковыми командирами в тактическом звене // Военная Мысль. 2009. № 9. С. 43-53.

179 Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 343 с.

180 Микони С. В., Соколов Б. В., Юсупов Р. М. Квалиметрия моделей и полимодельных комплексов. – М.: РАН, 2018. – 314 с.

181 Мильграм Ю. Г., Попов И. С. Боевая эффективность авиационной техники и исследование операций. – М.: ВВИА им. Н. Е. Жуковского, 1970. – 506 с.

182 Мистров Л. Е. Информационные войны: основы методологии синтеза систем информационной безопасности // Информационные войны. 2014. № 1. С. 64-74.

183 Мистров Л. Е., Павлов В. А., Шерстяных Е. С. Устойчивость информационных систем в конфликтном взаимодействии организационно-технических систем // Стратегическая стабильность. 2017. № 2. С. 43-49.

184 Мистров Л. Е., С. Н. Плотников Метод теоретико-игрового распределения ресурса для обоснования подвижных точек конфликтной устойчивости взаимодействия социально-экономических систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 2. С. 38-46.

185 Митюков Н. В. Имитационное моделирование в военной истории. – М.: ЛЕНАНД, 2018. – 280 с.

186 Михайлов Р. Л. Двухуровневая модель координации подсистем радиомониторинга и радиоэлектронной борьбы // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 43-50.

187 Михайлов Р. Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238-251.

188 Михайлов Р. Л. Модель информационных контактов устройств телекоммуникаций информационно-телекоммуникационной системы специального назначения со средствами наблюдения и воздействия противостоящей стороны // Труды учебных заведений связи. 2020. Т. 6. № 3. С. 17-27.

189 Многодоменная оперативная группа: армия США формирует в Германии подразделение нового типа – URL: https://vpk.name/news/503420_mnogodomennaya_operativnaya_gruppa_armiya_ssha_formiruet_v_germanii_podrazdelenie_novogo_tipa.html (дата обращения 01.07.2021).

190 Мукминов В. А., Войнов Ю. В. Методика оценки реального уровня защищенности автоматизированных систем в условиях кибератак // Известия Института инженерной физики. 2013. Т. 1. № 27. С. 80-85.

191 Мукминов В. А., Войнов Ю. В., Баландин А. В. О новых методах и алгоритмах тестирования программного обеспечения // Двойные технологии. 2011. № 2. С. 22-25.

192 Мукминов В. А., Грубов Ю. Е. Методы и средства сбора данных параметров выявленных уязвимых мест автоматизированных систем // Информационное противодействие угрозам терроризма. 2008. № 10. С. 94-101.

193 Муслимов Т. З. Алгоритмы управления строем автономных беспилотных летательных аппаратов самолетного типа с помощью метода векторного поля // Системы управления, связи и безопасности. 2019. № 4. С. 187-214.

194 Нестеров С. А. Информационная безопасность и защита информации: учебное пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

195 Никешин А. В., Пакулин Н. В., Шнитман В. З. Мутационное тестирование сетевых протоколов с использованием формальных моделей // Сборник трудов XVII Всероссийской научной конференции «Научный сервис в сети Интернет». М.: ИПМ им. М.В. Келдыша, 2015. С. 259-266.

196 Николаев В. И., Толстых Н. Н. Адаптивное, ситуационное и рефлексивное управление подсистемой защиты информации автоматизированных телекоммуникационных комплексов // Теория и техника радиосвязи. 2006. № 2. С. 79-87.

197 Николаев В. И., Толстых Н. Н., Власов Ю. Б., Челядинов Ю. В. Оценка информационной защищенности инфокоммуникационных систем // Радиотехника. 2013. № 12. С. 99-103.

198 Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-61.

199 Новиков С. В. Модель распространения вирусных атак в сетях передачи данных общего пользования на основе расчета длины гамильтонова пути: дис. … канд. техн. наук: 05.13.19 / Новиков Сергей Валерьевич. – СПб, 2007. – 98 с.

200 Новосельцев В. И., Душкин А. В., Сумин В. И., Кочедыков С. С., Орлова Д. Е. Моделирование систем безопасности. – Воронеж: ФКОУ ВО Воронежский институт ФСИН России, 2019. – 197 с.

201 Онуфриев В. А. Управление группой автономных роботов с использованием полярных координат // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика, телекоммуникации и управление. 2017. Т. 10. № 4. С. 97-106.

202 Орлов С. А. Технологии разработки программных средств. – СПб.: Питер, 2004. – 528 с.

203 Осипов М. П. Влияние численности сражающихся сторон на их потери // Военный сборник. 1915. № 10. С. 93-96.

204 Остапенко А. Г., Ермилов Е. В., Калашников А. О. Риски ущербности, шансы полезности и жизнестойкость компонент автоматизированных систем в условиях воздействия на них информационных угроз // Информация и безопасность. 2013. № 2. С. 215-218.

205 Остапенко А. Г., Ермилов Е. В., Шершень А. Н., Соколова Е. С., Шевченко И. В. Предупреждение и минимизация последствий кибератак на элементы критической информационной инфраструктуры и автоматизированные системы критически важных объектов: риск-анализ и оценка эффективности защиты // Информация и безопасность. 2013. № 2. С. 167-178.

206 Остапенко Г. А., Плотников Д. Г., Батищев Р. В., Гончаров И. В. Распределенные системы: методология оценки эффективности в условиях атак // Информация и безопасность. 2010. № 3. С. 359-366.

207 Перегудов М. А., Бойко А. А. Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7-15.

208 Перегудов М. А., Бойко А. А. Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75-81.

209 Перегудов М. А., Бойко А. А. Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13-18.

210 Перегудов М. А., Бойко А. А. Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA // Информационные технологии. 2015. Т. 21. № 7. С. 527-534.

211 Перегудов М. А., Семченко И. А. Оценка эффективности случайного множественного доступа к среде типа ALOHA при голосовых соединениях, передаче служебных команд, текстовых сообщений и мультимедийных файлов в условиях деструктивных воздействий // Труды СПИИРАН. 2019. № 4. С. 887-911.

212 Перегудов М. А., Стешковой А. С., Бойко А. А. Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. № 4. С. 92-114.

213 Петренко С. А., Бирюков Д. Н., Ломако А. Г. Метод упреждения кибератак на основе свойства антиципации // Информационные технологии и системы. Труды шестой Международной научной конференции. 2017. С. 225-230.

214 Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, цели. – М.: МО СССР, 1989. – 660 с.

215 Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. – М: АСТ, 2006. – 504 с.

216 Поддубный В. Н., Батурин Ю. О., Зайцев И. В., Пустовойтов Ю. И., Чикин М. Г. Состояние и направления развития методологии обоснования требований к технике радиоподавления систем радиосвязи // Радиотехника. 2010. № 6. С. 80-86.

217 Поленин В. И., Сущенков Д. А. Разработка модели вооруженного противоборства боевых систем тактического уровня с нанесением ударов непосредственно по боевой системе противника и отражением ударов противника по своей боевой системе // Национальная ассоциация ученых. 2015. № 8. С. 167-171.

218 Половко А. М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург, 2006. – 704 с.

219 Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». – URL: https://fstec.ru/normotvor-cheskaya/akty/53-prikazy/1598-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения 01.07.2021).

220 Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 01.07.2021).

221 Программно-технический комплекс автоматизированного планирования действий войск (сил) и обеспечения оперативной и боевой подготовки «Спектр-7Э» – URL: https://rusbitech.ru/products/tks/ptk-spektr-7e/ (дата обращения 01.07.2021).

222 Проданец В. В., Ошеров А. Я. Определение функциональной способности системы управления противовоздушной обороны армии посредством оценки ее качественного состояния // Военная Мысль. 2007. № 1. С. 15-20.

223 Прохоров Д. В. Влияние эффективности и живучести подразделения радиоэлектронной борьбы на успех боя соединения Сухопутных войск // Военная Мысль. 2020. № 3. С. 96-102.

224 Радзиевский В. Г., Трифонов П. А. Обработка сверхширокополосных сигналов и помех. – М.: Радиотехника, 2009. – 286 с.

225 Радиостанция AN/PRC-117G – URL: https://military.trcvr.ru/2015/11/07/radiostancija-anprc-117g/ (дата обращения 01.07.2021).

226 Радиостанция AN/PRC-150(C) – URL: https://military.trcvr.ru/2015/09/05/radiostancija-anprc-150c/ (дата обращения 01.07.2021).

227 Радиостанция портативная Р-168-МРА. Руководство по эксплуатации. ИТНЯ.464425.033 РЭ. – 128 с.

228 Радиостанция портативная Р-187-П1. Руководство по эксплуатации. ПАКД.464113.005 РЭ. – 242 с.

229 Резников Б. А. Системный анализ и методы системотехники. Часть 1. Методология системных исследований. Моделирование сложных систем. – М.: Издательство Министерство обороны СССР, 1990. – 522 с.

230 Ромашкина Н. П., Махукова А. В. Компьютерная вредоносная атака на ядерную программу Ирана // Информационные войны. 2013. № 4. С. 88-98.

231 Российская Федерация. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: офиц. текст. – М.: Кремль, 2017. – 36 с.

232 Саенко И. Б., Захарченко Р. И., Ясинский С. А., Грязев А. Н. Модели функционирования критической информационной инфраструктуры в условиях кибернетического противоборства // Информация и Космос. 2018. № 2. С. 46-51.

233 Саенко И. Б., Старков А. М. Модель оценки устойчивости функционирования локальных вычислительных сетей при использовании технологии VLAN // Труды ЦНИИС. Санкт-Петербургский филиал. 2019. № 7. С. 46-52.

234 Саяпин О. В., Тиханычев О. В., Чернов Н. А. Создание межвидовой разведывательно-поражающей системы как основы повышения эффективности огневого поражения // Военная Мысль. 2017. № 6. С. 32-37.

235 Свидетельство об официальной регистрации программы для ЭВМ в Роспатенте, Российская Федерация. Модель оценки эффективности деструктивных воздействий на радиоэлектронные средства способом «радиоэлектронное блокирование» / Р. С. Никишин, А. П. Богомолов, С. В. Курбатов, С. Н. Подрезов № 2019666404; заявл. 02.12.2019; опубл. 10.12.2019.

236 Свидетельство об официальной регистрации программы для ЭВМ в Роспатенте, Российская Федерация. Модель исследования влияния деструктивных воздействий на элементы сетевой системы обмена информацией сложной топологии / Р. С. Никишин, А. П. Богомолов, С. В. Курбатов, С. Н. Подрезов. № 2019667058; заявл. 02.12.2019; опубл. 18.12.2019.

237 Свидетельство об официальной регистрации программы для ЭВМ в Роспатенте, Российская Федерация. Программный комплекс разработки полного множества способов тестовых удаленных информационно-технических

воздействий на пространственно распределенные системы информационно-технических средств / А. А. Бойко, А. В. Щеглов, Е. Ю. Обущенко. № 2017660508; заявл. 27.06.2017; опубл. 22.09.2017.

238 Семенов А. В. Методика оценки уровня информатизации хозяйствующего субъекта // Региональная экономика: теория и практика. 2012. № 7. С. 60-64.

239 Сирота А. А. Компьютерное моделирование и оценка эффективности сложных систем. – М.: Техносфера, 2006. – 280 с.

240 Сирота А. А., Гончаров Н. И. Исследование конфликта коалиций систем с использованием формализма гибридных автоматов // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2017. № 4. С.56-70.

241 Сирота А. А., Гончаров Н. И. Модели информационных процессов несимметричного конфликтного взаимодействия систем и их применение в задачах исследования безопасности использования облачных технологий // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2018. № 3. С. 103-118.

242 Система боевого управления XXI века FBCB2 – URL: https://topwar.ru/65260-sistema-boevogo-upravleniya-xxi-veka-fbcb2.html (дата обращения 01.07.2021).

243 Смолян Г. Л., Черешкин Д. С. Двадцать лет спустя (От Концепции информатизации советского общества к Стратегии развития информационного общества в РФ) // Информационные ресурсы России. 2009. № 2. С. 11-18.

244 Советов Б. Я., Яковлев С. А. Моделирование систем. – М.: Высшая школа, 2009. – 343 с.

245 Сосюра О. В. Расчет обобщенных показателей боевых возможностей войск в операциях (боевых действиях) с учетом эффективности управления ими (потенциально-долевой метод). – М.: Военная Мысль, 1997. – 142 с.

246 Справочник по терминологии в оборонной сфере. Министерство обороны Российской Федерации – URL: dictionary.mil.ru/folder/123101/item/127800/ (дата обращения 01.07.2021).

247 Стародубцев Ю. И., Бречко А. А. Моделирование сетей связи, функционирующих в условиях деструктивных программных воздействий // Вопросы оборонной техники. Серия 16. 2017. № 11. С. 21-28.

248 Стародубцев Ю. И., Ерышов В. Г., Корсунский А. С. Модель процесса мониторинга безопасности информации в информационно-телекоммуникационных системах // Автоматизация процессов управления. 2011. № 1. С. 58-61.

249 Стародубцев Ю. И., Чукариков А. Г., Корсунский А. С., Федоров В. Г. Способ защиты инфотелекоммуникационных сетей критически важных объектов от сетевых кибератак // Автоматизация процессов управления. 2018. № 1. С. 14-19.

250 Стучинский В. И. Методический подход к оценке влияния дезорганизации управления оперативными резервами на темп наступления противника // Военная Мысль. 2016. № 11. С. 43-49.

251 Сухоруков Ю. С., Шляхин В. М. Принципы моделирования динамики взаимодействия сторон в условиях радиолокационного конфликта // Радиотехника. 1992. № 1-2. С. 4-11.

252 Сысоев В. В., Крутских П. П., Дикарев В. А., Свинцов А. А. Математическая модель информационного конфликта // Радиосистемы. Серия: Обработка сигналов и полей. 1999. № 2. С. 39-42.

253 Тараканов К. В. Математика и вооруженная борьба. – М.: Воениздат, 1974. – 240 с.

254 Твардовский А. С., Эль-Факи К., Громов М. Л., Евтушенко Н. В. Синтез тестов с гарантированной полнотой для недетерминированных временных автоматов // Моделирование и анализ информационных систем. 2017. Т. 24. № 4. С. 496-507.

255 Текунов В. В., Язов Ю. К. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова // Информация и безопасность. 2018. № 1. С. 38-47.

256 Ткаченко П. Н., Куцев Л. Н., Мещеряков Г. А., Чавкин А. М., Чебыкин А. Д. Математические модели боевых действий. – М.: Советское радио, 1969. – 240 с.

257 Толстых Н. Н., Пятунин А. Н., Марейченко И. В., Слепов Ю. И., Павлов В. А. Принципы раннего обнаружения признаков конфликтного режима взаимодействия автоматизированных телекоммуникационных комплексов // Теория и техника радиосвязи. 2004. № 2. С. 95-99.

258 Тюгашев А. А. Синтез и верификация управляющих алгоритмов реального времени для бортовых вычислительных систем космических аппаратов: дис. … д-ра техн. наук: 05.12.13 / Тюгашев Андрей Александрович. Самара, 2007. – 312 с.

259 Утакаева И. Х., Кунижева Л. А. Математическая модель распространения вирусов в сети на предфрактальных графах // Информационное противодействие угрозам терроризма. 2012. № 18. С. 64-70.

260 Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации».

261 Фендриков Н. М., Яковлев В. И. Методы расчетов боевой эффективности вооружения. – М.: Военное издательство, 1971. – 224 с.

262 Цыгичко В. Н., Стокли Ф. Метод боевых потенциалов: история и настоящее // Военная Мысль. 1997. № 4. С. 23-28.

263 Чаднов А. П., Гель В. Э., Гудков М. А. «Цифровые» ВС РФ. Часть 1. Роль военных сетевых цифровых технологий в строительстве и развитии ВС РФ нового облика // Информация и космос. 2018. № 1. С. 25-32.

264 Черноскутов А. И., Ситкевич А. В. Оценка результатов боевых действий при поочередном уничтожении группировок противника // Стратегическая стабильность. 2012. № 3. С. 51-55.

265 Черноскутов А. И., Ситкевич А. В., Тришкин В. С. Рациональный способ уничтожения разнородных группировок // Военная Мысль. 2018. № 1. С. 63-67.

266 Чикин М. Г. Метод аналитического описания процессов с дискретным множеством состояний и не показательными распределениями времен переходов // Информационно-измерительные и управляющие системы. 2004. № 5. Том 2. С. 8-11.

267 Чикин М. Г. Особенности использования аппарата полумарковских процессов для моделирования направлений радиосвязи в интересах оценки эффективности радиоподавления // Радиотехника. 2005. № 9. С. 35-39.

268 Чуев Ю. В. Исследование операций в военном деле. – М.: Воениздат, 1970. – 256 с.

269 Чуркин И. П., Костров С. А., Бегларян С. Г. Имитационное моделирование вооруженного противоборства в воздушно-космической сфере // Военная Мысль. 2018. № 9. С. 41-47.

270 Шербаков В. Б., Толстых Н. Н., Остапенко Г. А. Обнаружение вторжений на основе анализа фрагментов унитарного кода. – Воронеж: ВГТУ, 2007. – 150 с.

271 Шляхин В. М., Шляхин А. В. Особенности моделирования конфликта в условиях несанкционированного доступа // Проблемы информационной безопасности. Компьютерные системы. 2007. № 2. С. 95-99.

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

273 Энциклопедия кибернетики. Том 1. / Ред. коллегия: В. М. Глушков (отв. ред.) [и др.]; АН УССР. – Киев: Украинская советская энциклопедия, 1974. – 606 с.

274 Юдинцев Б. С. Синтез нейросетевой системы планирования траекторий для группы мобильных роботов // Системы управления, связи и безопасности. 2019. № 4. С. 163-186.

275 Язов Ю. К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов-на-Дону: СКНЦ ВШ, 2006. – 270 с.

276 Язов Ю. К., Авсентьев О. С., Авсентьев А. О., Рубцова И. О. Метод оценки эффективности защиты электронного документооборота с применением аппарата сетей Петри-Маркова // Труды СПИИРАН. 2019. № 6. С. 1269-1299.

277 Abramson N. The ALOHA System-Another Alternative for Computer Communications // Fall Joint Comput. Conf.: AFIPS Conf. Proc. 1970. Vol. 37. pp. 281-285.

278 Adamy D. L. EW 104: Electronic Warfare Against a New Generation of Threats. – Boston-London: Artech House, 2015. – 491 p.

279 Brigade Combat Teams. Force Structure Reference Data. Supplemental Manual 3-90. – Fort Benning. Maneuver Center of Excellence, January 2015. – 193 p.

280 Canvas – URL: https://www.immunityinc.com/products/canvas/ (дата обращения 01.07.2021).

281 Carleial A. B., Hellman M. E. Bistable Behavior of ALOHA-type Systems // IEEE Trans. Commun. 1975. Vol. COM-23. pp. 401-410.

282 Clarke E. M., Grumberg O., Peled D. Model Checking. – N. Y.: MIT Press, 1999. – 314 p.

283 Clarke R. A., Knake R. K. Cyber War: the Next Threat to National Security and What to Do About it. – New York: Harper Collins, 2010. – 290 p.

284 Codebases. Millions of lines of code // Beautiful News Daily. – URL: https://www.informationisbeautiful.net/visualizations/million-lines-of-code/. (дата обращения 01.07.2021).

285 Commercial Off-The-Shelf – URL: https://en.wikipedia.org/wiki/Commercial_off-the-shelf (дата обращения 01.07.2021).

286 Common Vulnerabilities and Exposures – URL: https://cveform.mitre.org/ (дата обращения 01.07.2021).

287 Core Impact – URL: https://www.coresecurity.com/products/core-impact (дата обращения 01.07.2021).

288 Drozer – URL: https://labs.f-secure.com/tools/drozer/ (дата обращения 01.07.2021).

289 Ettus Research – URL: https://www.ettus.com (дата обращения 01.07.2021).

290 ETSI ETR 300-1 Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' Guide; Part 1: Overview, technical description and radio aspects. – Sophia Antipolis: ETSI, 1997. – 84 p.

291 ETSI TS 102 361-2 V2.3.1 Electromagnetic compatibility and Radio Spectrum Matters. Digital Mobile Radio Systems. Part 2: DMR voice and generic services and facilities. – Sophia Antipolis: ETSI, 2016. – 107 p.

292 ETSI TS 102 361-4 V1.5.1 Electromagnetic compatibility and Radio Spectrum Matters. Digital Mobile Radio (DMR) Systems. Part 4: DMR trunking protocol. Technical Specification. – Sophia Antipolis: ETSI, 2016. – 287 p.

293 Gan C., Yang X., Liu W., Zhu Q. A propagation model of computer virus with nonlinear vaccination probability // Communications in Nonlinear Science and Numerical Simulation. 2014. vol. 19. no. 1. pp. 92-100.

294 Hayhurst K. J., Veerhusen D. S., Chilenski J. J., Rierson L. K. A Practical Tutorial on Modified Condition / Decision Coverage. Technical Report. – NASA, 2001. – 85 p.

295 Hui-min C., An-Xiang H., JinSong L., Lei X. Research on Construction and Evaluation Methods of the Operation Simulation Environment // 16th Asia Simulation Conference and SCS Autumn Simulation Multi-Conference. 2016. pp. 315-324.

296 IEEE 1516-2010. Standard for Modeling and Simulation (M&S) High Level Architecture. – URL: https://standards.ieee.org/standard/1516-2010.html. (дата обращения 01.07.2021).

297 IEEE Std 802.11-2012. Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications. – URL:

https://standards.ieee.org/getieee802/download/802.11-2012.pdf. (дата обращения 01.07.2021).

298 Iranian Navy captured two U.S. UAVs in past: admiral. – URL: http://tehrantimes.com/politics/104598-iranian-navy-captured-two-us-uavs-in-past-admiral. (дата обращения 01.07.2021).

299 Ivancevic V., Pourbeik P., Reid D. Tensor-Centric Warfare I: Tensor Lanchester Equations // Intelligent Control and Automation. 2018. no. 9. pp. 11-29.

300 Jaiswal N. K. Military operations research: quantitative decision making. – N. Y.: Kluwer Academic Publishers, 1997. – 388 p.

301 Jamal T., Amaral P., Khan A. Denial of Service Attack in Wireless LAN // ICDS. Rome. Italy. 2018.

302 Knuth D. E. Backus Normal Form vs. Backus Naur Form. 1967. pp. 735-736.

303 Kobayashi H., Onozato Y., Huynh D. An Approximate Method for Design and Analysis of an ALOHA System // IEEE Trans. Commun. 1977. Vol. COM-25. pp. 148-158.

304 Kress M., Lin K., MacKay N. The Attrition Dynamics of Multilateral War // Operation Research. 2018. no. 4. pp. 950-956.

305 Kuznetsov A. V. A Simplified Combat Model Based on a Cellular Automation // International Journal of Computer and Systems Sciences. 2017. vol. 56. no. 3. pp. 379-409.

306 Lanchester F. Aircraft in Warfare: The Dawn of the Fourth Arm. – London, Constable and Co, 1916. – 243 p.

307 Liu H., Lin Z., Cao M., Wang X., Lu J. Coordinate-free formation control of multi-agent systems using rooted graphs // Systems & Control Letters. 2018. vol. 119. no. 9. pp. 8-15.

308 Metasploit – URL: https://www.metasploit.com/ (дата обращения 01.07.2021).

309 Mishra B. K., Jha N. SEIQRS model for the transmission of malicious objects in computer network // Applied Mathematical Modelling. 2010. Vol. 34. No. 3. pp. 710-715.

310 Myers G. J. The Art of Software Testing. – New Jersey: John Wiley & Sons, 2004. – 255 p.

311 National Vulnerabilities Database – URL: https://nvd.nist.gov/ (дата обращения 01.07.2021).

312 Ning L., Wei-Hua L., Xiao-Yuan P., Zhou W. Research on Construction and Interoperability of Complex Distributed Simulation System // Third Asian Simulation Conference. 2004. pp. 131-140.

313 Offensive security exploit archive online – URL: https://www.offensive-security.com/backtrack/offensive-security-exploit-archive-online/ (дата обращения 01.07.2021).

314 Onozato Y., Nogochi S. On the Thrashing Cusp in Slotted ALOHA Systems // IEEE Trans. Commun. 1985. Vol. COM-33. pp. 1171-1182.

315 Pelletier E. Battlefield Simulations for Canadian Army Indirect Fire Modernization Options Analysis // Proceedings of the 2015 Winter Simulation Conference. 2015. pp. 2448-2455.

316 Qin J., Qichao M., Yu X., Wang L. On Synchronization of Dynamical Systems over Directed Switching Topologies: An Algebraic and Geometric Perspective // IEEE Transactions on Automatic Control. 2020. 17 p.

317 R&S®M3TR Software Defined Radios – URL: https://www.rohde-schwarz.com/ru/product/m3tr-productstartpage_63493-10287.html (дата обращения 01.07.2021).

318 RouterSploit – Router Exploitation Framework – URL: https://github.com/nawfling/routersploit. (дата обращения 01.07.2021).

319 Ruan C., Yang H., Yu L., Kou Y. Combat Network Synchronization of UCAV Formation Based on RTBA Model // Mathematical Problems in Engineering. vol. 2016. Article ID 2630790. 11 p.

320 Taylor J. G. Lanchester-Type Models of Warfare. Volume II. – Monterey: Naval Postgraduate School Publ., 1980. – 814 p.

321 Tel G. Introduction to Distributed Algorithms. – N.Y.: Cambridge University Press, 2001. – 612 p.

322 Test Advisor – URL: https://techdocs.broadcom.com/us/en/ca-enterprise-software/devops/continuous-delivery-director-saas/1-0/testing/test-advisor.html (дата обращения 01.07.2021).

323 The ICT Development Index: conceptual framework and methodology. – URL: https:// www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx. (дата обращения 01.07.2021).

324 The Nessus Family – URL: https://www.tenable.com/products/nessus (дата обращения 01.07.2021).

325 Tolk A. Engineering principles of combat modeling and distributed simulation. – New Jersey: John Wiley & Sons Publ., 2012. – 909 p.

326 VulnDB – URL: https://vulndb.cyberriskanalytics.com/ (дата обращения 01.07.2021).

327 Vulnerability Nodes Database – URL: https://kb.cert.org/vuls/ (дата обращения 01.07.2021).

328 Washburn A. Combat Modeling. M. Kress. – London: Springer, 2009. – 281 p.

329 XSpider – URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (дата обращения 01.07.2021).

Научное издание

Бойко Алексей Александрович

Киберзащита автоматизированных систем воинских формирований

Монография

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197372, Санкт-Петербург, пр. Богатырский, дом 32, к. 1 лит. А, пом. 6Н.
https://publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

Гарнитура «TimesNewRoman». 18,75 п.л.
Тираж 500 экз. Подписано в печать 30.10.2021

Материалы изданы в авторской редакции

Киберзащита автоматизированных систем воинских формирований

Современная война характеризуется значительным использованием компьютерных технологий в образцах вооружения. С одной стороны, это привело к существенному сокращению длительности боевых циклов и потерь личного состава. С другой стороны, эти технологии снизили надежность образцов вооружения за счет их многократного усложнения, затруднили процессы освоения, ремонта и привели к появлению кибероружия. В известных работах нет ответа на вопрос: как создать необходимое и достаточное множество способов реализации кибератак на защищаемую автоматизированную систему, оценить их на уровне боевой эффективности противоборствующих сторон в заданной обстановке, чтобы выбрать подлежащие устранению уязвимости, когда ресурсов для устранения всех уязвимостей не хватает? В монографии впервые с системной позиции дается ответ на этот вопрос в контексте создания ранее неизвестных способов реализации кибератак и оценки эффективности новых и известных способов на уровне информационных, информационно-боевых и боевых показателей.

Материалы работы могут быть полезны специалистам в области моделирования боевых действий и оценки эффективности перспективных образцов вооружения, а также курсантам, студентам, адъюнктам, аспирантам и научным сотрудникам соответствующих специальностей.

Алексей Александрович Бойко – доктор технических наук, доцент, лауреат премии Президента Российской Федерации в области науки и инноваций для молодых ученых.

В 2004 году окончил Военный институт радиоэлектроники (г. Воронеж). Проходил службу на научных и административных должностях в Вооруженных Силах Российской Федерации. Принимал участие в разработке перспективных образцов вооружения, а также в обосновании и апробации способов их применения.

Автор более 150 научных трудов и изобретений. Область научных интересов – методы и системы защиты информации, методы оценки эффективности сложных организационно-технических систем.

ISBN 978-5-6046688-3-2