МИР
электроники

А.И. Белоус,
В.А. Солодуха,
С.В. Шведов

Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия

Под общей редакцией
А.И. Белоуса

В 2-х книгах
Книга 1

ТЕХНОСФЕРА
Москва
2018

УДК 004.492
ББК 32.85
Б43

Б43 Белоус А.И., Солодуха В.А., Шведов С.В.
Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия
Под общей редакцией Белоуса А.И.
В 2-х книгах
Книга 1
Москва: ТЕХНОСФЕРА, 2018. – 688 с. ISBN 978-5-94836-524-4

Впервые в мировой научно-технической литературе в объеме одного комплексного издания последовательно и детально исследован феномен программных и аппаратных троянов, которые фактически являются технологической платформой современного и перспективного информационно-технического оружия (кибероружия). Материал энциклопедии представлен в виде 12 глав.

В первой вводной главе, обобщающей результаты анализа технических возможностей и ограничений современного оружия (атомного, космического, сейсмического, климатического, различных видов СВЧ-оружия), показано, что развитие всех «обычных» и «новейших» видов вооружений дошло до такой стадии, что их реальное использование на практике будет равносильно самоубийству начавшей войну стороны. Осознание этого факта привело к развитию информационно-технического оружия (кибероружия и нейрооружия). В главе 2 детально исследованы концепции, методы, технические средства и примеры реализации этого вида оружия. В главе 3 рассмотрены основные виды программных троянов, вирусов и шпионских программ, которые в «кибероперациях» обычно действуют солидарно, защищая и помогая друг другу. В главе 4 наглядно показан эволюционный путь развития аппаратных троянов от «ящиков» и «коробочек» до микросхем, приведены примеры их применения в компьютерах, серверах, мобильных телефонах, автомобилях и даже в одежде и обуви человека. В главах с 5-й по 9-ю детально рассмотрены основные типы троянов в микросхемах, принципы их проектирования и работы, способы внедрения, методы их маскировки, выявления в микросхемах, а также защиты и противодействия. В главах с 10-й по 12-ю представлен детальный сравнительный ретроспективный анализ основ государственной политики в США и России в области обеспечения безопасности каналов поставки микросхем.

Книга ориентирована на широкий круг читателей: от инженеров, специалистов по информационной безопасности, чиновников министерств и ведомств до школьников и пенсионеров, активно использующих социальные сети.

УДК 004.492
ББК 32.85

ISBN 978-5-94836-524-4

Кто роет яму, сам упадет в нее, и кто ставит сеть, сам будет уловлен ею.

(Книга Премудрости Иисуса, сына Сирахова. XXVII, 29)

Ибо нет ничего тайного, что не сделалось бы явным, ни сокровенного, что не сделалось бы известным и не обнаружилось бы.

(Евангелие от Луки, глава 8, ст. 17)

Содержание

Предисловие

Предлагаемая вниманию читателя книга ориентирована на очень широкий круг читателей – от разработчиков микросхем и радиоэлектронной аппаратуры, для которых она предназначена в первую очередь, до студентов технических вузов, школьников старших классов, а также простых граждан, которые в своей служебной и неслужебной деятельности используют Интернет и другие социальные сети.

По структуре построения и содержанию материалов эта книга пока не имеет аналогов в отечественной и мировой научно-технической печати.

Столь широкий круг потенциальных читателей книги обусловлен уникальностью предмета исследований – программными и аппаратными троянами, представляющими собой технологическую платформу современного информационно-технического оружия, которое в иностранной печати называют «кибероружием». Изначально авторы планировали включить в книгу только технические материалы, имеющие отношение исключительно к аппаратным троянам в микросхемах в связи с недавно возникшей угрозой информационной безопасности современных информационных и электронных систем. Внедренные в микросхемы, эти трояны, попадая затем на платы электронных блоков различных радиоэлектронных и информационно-коммуникационных систем, по команде извне могут не только организовывать скрытые каналы передачи злоумышленнику – «хозяину» трояна конфиденциальную информацию, но и сами вмешиваться в работу этих устройств и систем, искажая информацию, ухудшая технические характеристики, надежность вплоть до вывода всей системы из строя.

В зависимости от цели злоумышленника такой троян может очень долгое время (месяцы, годы) «спать», «просыпаясь» или по внешнему сигналу, или в зависимости от редких сочетаний внутренних сигналов и внешних воздействий (определенной температуры, механических воздействий и т.д.).

Самый «низший в иерархии» троян – «временная бомба» – находится в спящем состоянии сколь угодно долго, чтобы «проснуться» (активизироваться) в установленный заранее злоумышленником точный момент времени.

Поэтому основная часть материала книги посвящена аппаратным троянам – их принципам работы, разновидностям, способам внедрения в микросхемы, способам их выявления, методам противодействия на аппаратном и программном уровне и т.д. Однако, чтобы понять причины появления этого технического феномена, авторам пришлось не только изучить историю их возникновения и развития, но и самим разобраться в основополагающих причинах этого явления, для чего в состав книги пришлось включить дополнительные, ранее не планировавшиеся главы.

Основная причина заключается в том, что (как показано в первой такой главе) все известные сегодня виды современных вооружений – атомное оружие, космические средства поражения, СВЧ-оружие, метеорологическое и сейсмическое оружие, наряду с огромными разрушительными возможностями обладают столь же существенными ограничениями: фактически их применение на практике будет равносильно самоубийству «начавшей» войну стороны. Поэтому и появились совершенно новые виды вооружений, которые, по мнению их создателей и идеологов, дают им реальный шанс «победить и остаться в живых». Это нейронное

оружие (нейрооружие) и кибероружие, которые, в свою очередь, являются только разновидностями очередного новейшего вида оружия – информационно-технического.

Интересно, что в исторической ретроспективе программные и аппаратные трояны первыми начали использовать в своей «работе» национальные криминальные группы (мафиози, гангстеры, якудза) для достижения своих чисто криминальных целей без классического применения оружия (незаконные банковские операции, сбор конфиденциальной информации, уничтожение улик в базах данных и т.п).

Спецслужбы США и Великобритании, военные этих стран раньше других оценили как уровень этой новой угрозы, так и поистине неограниченные возможности данного направления, которое уже потом журналисты назвали кибероружием. Кстати, в книге мы приводим типовые примеры ставших известными операций спецслужб США, Израиля и других стран с использованием внедренных в системы атакуемого государства таких троянов, а также весьма обширный перечень уже «засвеченных» перебежчиком Сноуденом «шпионских» программ АНБ и других спецслужб.

Наиболее известные примеры применения троянов – это начальная фаза войны в Персидском заливе и атака на сирийский ядерный исследовательский центр, когда за несколько минут до нападения израильских самолетов с крылатыми ракетами «ослепли и оглохли» все иракские и сирийские системы ПВО (в книге мы приводим фотографии микросхемы с платы радиоэлектронного блока сирийского радара с таким трояном – «до атаки» и «после атаки»).

Поэтому вторая глава нашей книги посвящена исследованию концепций, методов и конкретных технических средств реализации различных возможностей применения этого информационно-технического оружия – от стратегического уровня систем государственного управления и систем управления оружием до нейрооружия и даже до «бытового» уровня офиса обычной современной компании, которой очень интересуются конкуренты.

А поскольку аппаратные трояны, как правило, в подобных «кибероперациях» действуют солидарно с программными троянами, вирусами и «шпионскими» программами, взаимно дополняя и защищая друг друга, авторы посвятили также и им отдельную (третью) главу энциклопедии.

Появление аппаратных троянов в современных микросхемах – это всего лишь логическое следствие глобальной тенденции развития инновационных технологий от «шкафов», «ящиков» и «коробочек» до микрочипов. Такой естественный эволюционный процесс позволил аппаратным троянам захватывать все новые и новые «сферы применения». Поэтому авторы сочли необходимым привести в четвертой главе именно такие наглядные примеры применения предыдущих поколений аппаратных троянов, которые можно «пощупать руками», обнаружив их по нашим рекомендациям в своем рабочем кабинете, в мобильном телефоне, в клавиатуре любимого компьютера и даже в приборах так называемой бытовой электроники (утюгах, СВЧ-печах, автомобильных видеорегистраторах и т.п.). Впервые в отечественной технической литературе мы приводим примеры появления такого нового вида угроз нашей с вами бытовой безопасности, как автомобильные программные и аппаратные трояны.

Наука, техника и экономика развиваются по своим объективным законам, обычно никак не связанным с официальной идеологией государств. Совершенно неожиданно для лидеров и идеологов западных стран, и в первую очередь для США, которые провозгласили своей главной целью обеспечение абсолютного и безусловного мирового лидерства и превосходства в области высоких технологий, и прежде всего в военной сфере, аппаратные трояны в микросхемах превратились в одну из самых опасных угроз. Чтобы исследовать причины этого парадоксального только на первый взгляд факта, авторы были вынуждены более глубоко изучить процессы глобализации, происходящие в мировой полупроводниковой индустрии в последние 10–15 лет, результаты анализа которых мы в сжатом виде приводим в этой книге.

Как увидит читатель, в силу ряда объективных экономических факторов производство самых современных микросхем было перенесено с территории США и его стратегических союзников в страны Юго-Восточной Азии – Китай, Тайвань, Южную Корею. Этот процесс носит необратимый характер. Первый «звонок» для США прозвучал еще в 2005 г., когда Министерство юстиции США обнародовало результаты судебных расследований фактов контрафактной поставки (подделок) микросхем, предназначенных для комплектации систем управления подводными лодками, боевыми и гражданскими самолетами, системами вооружений, системами обеспечения безопасности стратегических объектов и органов государственного управления.

Если популярно объяснять этот феномен, как говорят, «на пальцах», то любому инвестору (даже американскому), чтобы построить полупроводниковую фабрику в США, в то время надо было заплатить правительству страны на 2–3 млрд долларов больше, чем если построить эту же фабрику в Китае. При этом для сбора всех разрешительных документов для строительства фабрики в США требуется полтора-два года, а в Китае на все – всего 2-3 месяца. А еще – дешевая и дисциплинированная китайская рабочая сила.

Ради исторической справедливости здесь следует заметить, что и здравомыслящие политики США, и руководители абсолютно всех спецслужб (ФБР, ЦРУ, АНБ), и руководители Министерства обороны США многократно обращались в правительство и Сенат, чтобы снять эти «чисто экономические» преграды, но непоколебимый культ владельцев капиталистического «золотого тельца» устоял: с их точки зрения возможность «потерять просто так» десятки потенциальных миллиардов долларов была несоизмерима с возможностью нейтрализации потенциальных угроз каких-то «троянов», якобы угрожающих национальной безопасности Америки.

Но, надо сказать, что и Министерство обороны США, и спецслужбы достаточно быстро отреагировали на эту новую угрозу путем создания целого ряда правительственных программ и мероприятий, научных и прикладных исследований, специальных исследовательских центров по анализу безопасности микросхем, разработали и ввели в действие комплекс директивных (подлежащих обязательному исполнению) законодательных и нормативно-технических документов, при безусловной реализации которых вероятность поставки в электронные системы ответственного назначения США микросхем с внедренными «кем-то» троянами снизилась сразу на несколько порядков. Поэтому в завершающих техническую часть книги двух «организационно-методических » главах авторы детально рассмотрели

уже разработанные и опробованные в практической деятельности комплексы «американских» документов наряду с анализом ситуации по разработке аналогичных документов Российской Федерации.

Поскольку в результате такого детального анализа было выявлено достаточно много различий в американских и отечественных подходах к решению этой проблемы, авторы решили их сформулировать в нестандартном для технической энциклопедии разделе «Вместо заключения».

Как и принято при издании подобного рода технических энциклопедий, весь основной материал книги построен на результатах системного анализа в основном иностранной литературы, из отечественных публикаций по этой проблеме редкое исключение составляют работы научной школы академика Саурова.

В приложении 1 к этой энциклопедии приведены все авторы работ, чьи графические и текстовые материалы были использованы авторами при подготовке рукописи, фактически все они являются соавторами книги.

При оформлении материалов рукописи книги огромную техническую помощь и моральную поддержку авторам оказали наши сотрудники: Антипенко Ольга, Гордиенко Светлана, Гуминский Владимир, Мотевич Ричард. С нюансами перевода с английского языка авторам помогали разобраться Сизов Юрий, Сахарук Геннадий, Мазурина Надежда, Кутас Анастасия, Чикилев Виктор.

Авторы также благодарят инженера Гайворонского Кирилла за предоставленные материалы главы 4 «Аппаратные трояны в электронной аппаратуре», существенно обогатившие информационное содержание энциклопедии.

Авторы также благодарят академика Национальной академии наук Беларуси, иностранного избранного академика АН Российской Федерации Лабунова Владимира Архиповича и д.т.н., профессора кафедры защиты информации БГУИР Лынькова Леонида Михайловича за конструктивную критику и полезные предложения по уточнению содержания и структуры изложения материала, сделанные ими в процессе рецензирования данной работы.

Также авторы выражают искреннюю благодарность академику РАН Красникову Геннадию Яковлевичу, директору МНИИРИП Минпромторга РФ Куцько Павлу Павловичу, начальнику Военного представительства 4778 МО РБ Хартановичу Валерию Арсентьевичу, начальнику отдела оборонной промышленности и военно-технического сотрудничества Постоянного Комитета Союзного государства Осипову Михаилу Сергеевичу за профессиональную конструктивную критику и конкретные предложения по совершенствованию структуры и стиля изложения представленных материалов энциклопедии, которые несомненно способствовали улучшению качества предлагаемой вниманию читателей технической энциклопедии.

Введение

Первая глава посвящена проблемам современного оружия: его основным техническим возможностям и имеющимся ограничениям его применения в реальных условиях. Здесь прежде всего рассмотрены основные научно-технические и военно-стратегические аспекты построения и использования средств поражения космического и наземного эшелонов противоракетной обороны, в том числе СВЧ-оружие наземного применения, оружие несмертельного (нелетального) действия наземного применения, СВЧ-оружие атмосферного и космического применения. Особое внимание уделено американской программе высокочастотных активных исследований HAARP, а также еще одному стремительно развивающемуся виду оружия – нейронному оружию. В итоговом заключении по этой главе сделан вывод о том, что имеющиеся ограничения всех видов современного оружия делают его для нападающей стороны ни чем иным, как изощренным орудием самоубийства.

Вторая глава посвящена анализу концепции, средств, методов и примеров применения нового самого опасного и эффективного оружия – информационно-технического (кибероружия). Для более глубокого понимания всех аспектов, связанных с его разработкой и особенностями применения, здесь последовательно рассмотрены такие вопросы, как принципы обеспечения информационной безопасности суверенного государства, основы ведения информационной войны, определение и классификация информационно-технических воздействий, наиболее распространенные средства информационно-технического воздействия, технические каналы утечки информации.

Третья глава посвящена компьютерным вирусам, программным закладкам и шпионским программам. Рассмотрены основные известные модели воздействия на компьютеры программных закладок, способы внедрения и их взаимодействие с нарушителем: это программные клавиатурные шпионы, основные принципы работы RootKit-технологий, шпионские программы типа cookies, шпионская программа Regin. Также приведены примеры способов внедрения программного трояна в стандартный PE-файл операционной системы MICROSOFT WINDOWS, примеры недокументированных функций в микросхемах 80-х годов. Здесь же проанализированы известные методы снятия секретной информации на основании анализа акустических и электромагнитных излучений, а также особенности организации защиты информации при работе с криптовалютами.

Четвертая глава посвящена анализу особенностей внедрения троянов в различную электронную аппаратуру. Рассмотрены программно-аппаратные трояны в телекоммуникационных системах, аппаратные трояны в компьютерах, трояны в системах мобильной связи, в автомобилях, в бытовой электронике, электронные приборы для беспроводного перехвата данных, а также различные экзотические «шпионские штучки» типа микрошпионов в одежде и в обуви.

Пятая глава посвящена анализу аппаратных троянов в современных микросхемах. В начале главы рассмотрены теоретические основы проектирования безопасной электронной аппаратуры для ответственных применений, приведено описание первых задокументированных фактов обнаружения аппаратных троянов

в микросхемах ответственного назначения. Детально рассмотрена классификация аппаратных троянов в микросхемах, способы их внедрения в микросхемы, все основные механизмы активации внедренных аппаратных троянов. Подробно исследованы наиболее известные методы выявления аппаратных троянов в микросхемах ответственного назначения. Приведены конкретные примеры разработки и реализации аппаратных троянов, рассмотрены особенности внедрения аппаратных троянов в пассивные радиочастотные метки, в беспроводные криптографические ИС. В заключительной части главы детально рассмотрены основные методы проектирования аппаратных закладок и приведен обобщенный анализ наиболее эффективных методов выявления аппаратных троянов в микросхемах.

Шестая глава посвящена изучению особенностей внедрения аппаратных троянов в микросхемы памяти типа SRAM: приведены основные виды моделей отказов в микросхемах SRAM, представлен анализ типовых механизмов запуска троянов в SRAM – аппаратных троянов типа «короткое замыкание», типа «резистивный обрыв» и других типов.

Здесь же представлены экспериментальные результаты исследований аппаратных троянов типа «короткое замыкание» и типа «обрыв».

Седьмая глава целиком посвящена описанию методов выявления аппаратных троянов в микросхемах. В начале главы приведен краткий обзор основных известных методов выявления аппаратных троянов в микросхемах ответственного назначения, в том числе методов обнаружения аппаратных троянов на основе анализа спектра электромагнитного излучения, рассмотрены особенности выявления последовательных аппаратных троянов с использованием метода TeSR. В конце главы кратко рассмотрены все другие известные из литературы методы исследований и обнаружения аппаратных троянов в микросхемах, а также приведены конкретные примеры из опыта работы белорусских «охотников за троянами».

Восьмая глава целиком посвящена проблемам обратного проектирования микросхем. В начале главы рассмотрены юридические особенности обеспечения защиты прав интеллектуальной собственности на полупроводниковые микросхемы в США и в России, приведены типовые методики восстановления топологий кристаллов микросхем, основные методы восстановления электрической схемы из топологии кристалла, методики подготовки образцов субмикронных микросхем для исследований электрофизическими РЭМ-методами. В отдельном параграфе детально рассмотрены методы защиты и противодействия процессам реинжиниринга микросхем космического и военного назначения, приведены практические примеры схемотехнических методов защиты микросхем от реинжиниринга.

В девятой главе детально рассмотрены известные методы противодействия аппаратным троянам в микросхемах, в том числе программно-аппаратные методы противодействия аппаратным троянам. Два крупных раздела посвящены рассмотрению особенностей проектирования защищенных от троянов систем на кристалле SoC, приведена так называемая безопасная архитектура системы на кристалле, которая может безопасно функционировать даже с внедренным трояном. Здесь же показано использование классической «песочницы» как новый метод защиты от аппаратных троянов в SoC, приводятся примеры использования математических инструментов теории игр для противодействия аппаратным троянам в ИС. В заклю-

чительных разделах главы детально рассмотрены конкретные программно-аппаратные методы защиты FPGA от несанкционированного копирования информации и основные эффективные методы отслеживания безопасности микросхем после их изготовления в производстве.

Десятая глава посвящена детальному исследованию основ государственной политики США в области обеспечения безопасности каналов поставки микросхем. В ней рассматриваются структура и функции Министерства обороны США, стратегия обеспечения кибербезопасности в США, организационная структура DARPA, структура формирования и управления программами научно-исследовательских работ Министерства обороны США, стратегия Министерства обороны США по обеспечению безопасности микросхем, дан краткий анализ специальных проектов DARPA в области киберугроз. Завершает главу раздел, посвященный анализу основных положений государственной политики США и ЕС в области контроля экспорта микросхем ответственного назначения.

Последняя глава 11 целиком посвящена анализу особенностей организации российской системы управления развитием военной электроники. Здесь рассмотрены основные проблемы обеспечения информационной безопасности современного российского оборонно-промышленного комплекса, дан ретроспективный анализ эволюции системы управления российской военной электроники, проанализированы на предмет безопасности все существующие каналы поставки микросхем для ОПК РФ.

Рассмотрены основные достоинства и недостатки применения индустриальной ЭКБ иностранного производства, дан анализ текущего состояния и перспектив развития российской ЭКБ специального и двойного назначения.

ГЛАВА 1

СОВРЕМЕННОЕ ОРУЖИЕ: ТЕХНИЧЕСКИЕ ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

1.1. Некоторые научно-технические и военно-стратегические аспекты построения и использования средств поражения космического эшелона противоракетной обороны

1.1.1. Технические возможности и ограничения потенциальных средств поражения баллистических ракет

Основной проблемой создания современной противоракетной системы является создание подсистемы поражения межконтинентальных и баллистических ракет (МБР) и баллистических ракет, запускаемых с подводных лодок (БРПЛ), на всех участках их территории (в «старых» системах ПРО речь шла лишь об обороне от атакующих ракет на конечном участке их траектории).

Как известно [1], основные элементы траектории атакующей баллистической ракеты, начиная со старта, можно разделить на четыре участка (рис. 1.1):

1) *активный* участок, где за счет работы двигателей первых ступеней ракеты производится ее разгон до скорости 6–7 км/с;
2) участок *разделения*, где происходит отделение боеголовок индивидуального наведения и ложных целей;
3) *баллистический* участок, где все выведенные ракетой объекты движутся по траекториям свободного полета;

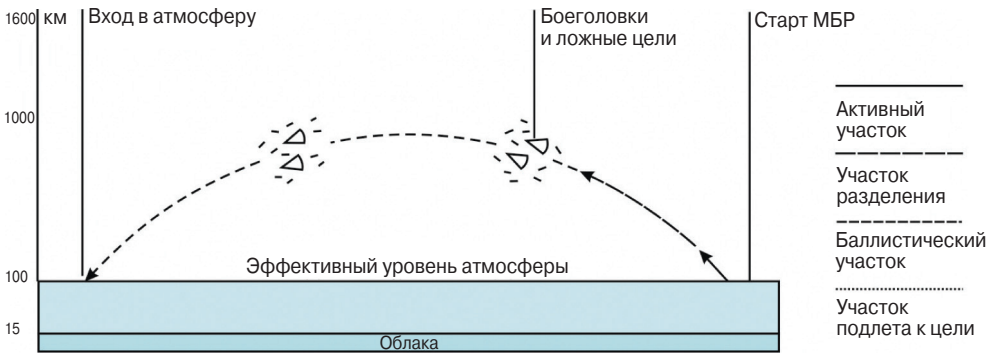

Рис. 1.1. Элементы траектории межконтинентальной баллистической ракеты

4) участок *подлета* (конечный участок), на котором боеголовки входят в плотные слои атмосферы и направляются к объектам поражения (ложные цели сгорают в атмосфере).

Эффективная противоракетная система должна включать свои средства поражения именно на активном участке по следующим очевидным причинам:

1) количество подлежащих уничтожению объектов минимально: еще не произошло отделение боеголовок и не выпущены ложные цели;
2) из-за мощного факела от сгоревшего топлива атакующая ракета наиболее легко обнаруживается средствами слежения;
3) сама ракета-носитель – значительно более «крупный» объект, чем боеголовки, и легче обнаруживается;
4) ракета наиболее уязвима, так как ее корпус фактически образуют стенки топливных баков, которые намного хуже защищены от тепловых и механических (ударных) нагрузок, чем боеголовки.

В свою очередь, активный участок траектории характеризуется двумя основными параметрами – *временем* набора конечной скорости и *высотой*, на которой эта скорость достигается.

Первый параметр определяет требуемые темпы подготовки соответствующего эшелона системы ПРО к действию, а также, условно говоря, «скорострельность», которой должны обладать средства поражения при массированной ракетной атаке.

Второй параметр определяет состав и характеристики технических средств, которые могут быть использованы для поражения целей.

Здесь важно, находится ли эта высота в пределах атмосферы или за ее пределами.

Обычно в подобных расчетах военными принимается эффективная высота, равная 100 км.

Для баллистических ракет прошлого века типичное время полета на активном участке составляло не более трех минут, а соответствующая высота – в пределах 250–350 км.

Для современных ракет значения этих параметров, по мнению экспертов, значительно снижены: время – не более 50 секунд, высота – 80–100 км. Это говорит о том, что эффективно фиксировать ракету на данном участке можно только из космоса.

1.1.2. Космический эшелон противоракетной обороны

Одной из важнейших характеристик так называемых *боевых космических станций* (БКС), предназначенных для поражения ракет противника на активном участке, является радиус действия средств поражений, размещенных на таких БКС.

Кроме того, имеется и ряд других не менее важных параметров, которые в терминах артиллеристов обозначаются как боезапас и скорострельность БКС.

Сочетание этих характеристик с вышеуказанными параметрами и с требованием, чтобы любая точка территории потенциального противника (или акватории, где могут находиться его подводные ракетоносцы) в любой момент времени находилась в поле зрения хотя бы одной БКС, определяет общую необходимую численность боевых станций и структуру их размещения в околоземном пространстве.

Необходимо отметить и некоторые особенности одного из «подэтапов» активного участка, на котором происходит разделение: отделение индивидуальных боеголовок от тела ракеты – носителя (будем называть ее далее платформой) сопровождается кратковременной работой двигателей малой тяги, что, соответственно, и позволяет системам наблюдения обнаружить платформу и по возможности максимально точно определить ее положение в пространстве, а также вектор скорости движения, чтобы точно проанализировать (рассчитать) ее дальнейшую траекторию в последующие моменты времени.

Поскольку обычно боеголовки отделяются не все сразу, операторы БКС какое-то время обладают теоретической возможностью «одним ударом» обезвредить боезапас платформы, хотя в данном случае объектом поражения являются не относительно уязвимые топливные баки ракеты, а более надежно защищенные объекты.

Важнейшими особенностями баллистического участка являются максимальная его продолжительность и наибольшее число целей (истинных и ложных); каждая стартующая ракета может нести десять боеголовок и такое же число ложных целей (которые полностью имитируют боеголовку при входе в атмосферу), а также более сотни «упрощенных» ложных целей для насыщения системы ПРО на этом участке траектории.

В этом случае встает дилемма: уничтожать все цели или предварительно провести их селекцию, что является достаточно сложной технической задачей как для первого, так и для второго вариантов.

Во многих ставших известными в конце 90-х годов военно-стратегических исследованиях американских специалистов предполагалось, что в случае широкомасштабного ракетно-ядерного конфликта между СССР и США основной обмен ударами произойдет через Северный полюс. Хотя этими исследованиями допускалась и возможность построения противоракетных систем наземного базирования (для борьбы с боеголовками на баллистическом участке траектории), более эффективными оказались средства космического базирования. Это должны быть БКС, располагаемые на полярных (или приполярных) орбитах высотой порядка 1000 км.

В зависимости от направления движения БКС на орбите она может либо лететь *навстречу* атакующим боеголовкам противника (с относительной скоростью порядка 10–20 км/с), либо медленно их *догонять* (в этом случае с относительной скоростью 1–3 км/с).

Станции первого типа («встречающие») лучше решают задачи поражения целей, станции второго типа («догоняющие») лучше решают задачи селекции целей.

Если боеголовка (или ложная цель) двигается вне атмосферы, траекторию ее движения легко рассчитать с использованием высокопроизводительных вычислительных комплексов.

На конечном участке траектории число атакующих целей на порядки сокращается (ложные цели сгорают в плотных слоях атмосферы), но зато оставшиеся реальные цели (боеголовки) проходят конечный участок очень быстро – не более одной минуты. Причем современные боеголовки обладают возможностью маневрирования на этом участке, что затрудняет слежение и использование некоторых средств поражения.

В подобном случае как отечественные, так и зарубежные эксперты сходятся в том, что наиболее эффективными являются системы «заатмосферного» поражения наземного или воздушного (космического) базирования. Однако надо понимать, что их действия будут носить только локальный (на этом участке траектории) характер, тогда как средства ПРО на активном и баллистическом участках траектории ракеты должны обеспечивать глобальную защиту всей территории обороняющейся стороны.

В табл. 1.1 представлены в систематизированном виде вышеотмеченные особенности отдельных участков траектории полета атакующих баллистических ракет, важные для понимания особенности построения современной ПРО.

Таблица 1.1. Сравнительный анализ участков траектории полета баллистических ракет с точки зрения выбора средств базирования ПРО

Участок траектории	Продолжительность полета, с	Длительность движения в атмосфере, с	Число целей ПРО (без учета действия предыдущего эшелона)	Основные объекты поражения	Оптимальное место базирования
Активный	50—200	50—150	Минимальное	Топливные баки ракетоносителей	Космическое базирование
Баллистический	от 150 (при настильных траекториях до 1000)	нет	Максимальное (увеличение более чем в 100 раз)	Боеголовки (если решена задача селекции целей) или все объекты	Космическое базирование
Конечный	40—100	полностью	В 2—3 раза больше минимального (но цели уже рассредоточились в пространстве)	Боеголовки	Наземное (или космическое базирование)

1.1.3. Анализ основных типов потенциальных космических средств поражения противовоздушной обороны

Американские военные эксперты в процессе технической проработки провозглашенной в свое время президентом США Рейганом известной «стратегической оборонной инициативы» (СОИ) рассматривали следующие основные типы потенциальных средств поражения ПРО:

- *лазерное* оружие (энергия выделяется в сравнительно тонком поверхностном слое мишени);
- *пучковое* оружие (более «глубокое» проникновение энергии в материал мишени);
- *кинетическое* оружие (баллистические или самонаводящиеся снаряды, разгоняемые до сверхбольших скоростей и наносящие механические повреждения целям);
- *электромагнитное* оружие (ЭМИ, волны миллиметрового диапазона, потоки частиц).

Экспертами назывались следующие достоинства лазерного оружия как элемента ПРО:

а) почти мгновенное (энергия переносится со скоростью света) поражение цели;

б) гравитационное поле Земли практически не влияет на траекторию «пучков» энергии;

в) большая дальность поражения.

Все эти факторы теоретически могут быть наилучшим образом использованы в задачах ПРО.

Однако вся известная из открытых литературных источников информация о разновидностях лазерного оружия имеет и весьма существенные недостатки. Лазерные «пучки» воздействуют только на поверхностный слой материала мишени, что в принципе позволяет эффективно разрушать в результате теплового или ударного (для импульсных лазеров) воздействия тонкостенные преграды – стенки топливных баков ракет, обшивку воздушных судов (самолетов и вертолетов), стенки стратегических хранилищ топлива (нефте- и газохранилищ и т.п.).

Следовательно, это оружие в принципе можно использовать как при ударе «из космоса» по наземным и воздушным целям, так и против ракет на активном участке их траектории.

Как известно, атмосфера прозрачна для лазерного излучения в диапазонах длин волны примерно от 0,3 до 1,0 мкм. Однако лазерный луч, теоретически свободно проникающий через атмосферу, весьма интенсивно рассеивается («гаснет») в облаках, пыли, тумане, на различных природных аэрозолях и пр.

Однако разработчики ракет тоже не стоят на месте: например, для повышения порога теплового поражения от лазерного луча поверхность ракеты (оболочки боевой платформы боеголовок) покрывается слоями веществ с низкой теплопроводностью (абляционное покрытие). Тогда падающая на корпус ракеты энергия всецело поглощается в этом специальном тонком слое покрытия, разогревая и далее испаряя его полностью, но оставляя основную «несущую» конструкцию корпуса (оболочки) неповрежденной.

Боеголовки имеют также прочную оболочку и лучше теплоизолированы, поскольку они рассчитаны на торможение при высокоскоростном движении в плотных слоях атмосферы (от 10 кДж/см^3 до 200 МДж/см^3).

Есть еще целый ряд негативных моментов, ограничивающих возможности использования лазерного оружия на БКС.

Так, количество энергии «в одном выстреле» такой лазерной пушки должно составлять не менее 200 МДж (что эквивалентно взрыву 50 кг заряда тринитротолуола).

А поскольку КПД лазеров, работающих на атомных или молекулярных переходах, очень низок (пока реально не более 10%), то выделяемая в самом лазерном излучении энергия настолько велика, что активная среда, в которой идет активный лазерный процесс, мгновенно разрушается после первого «выстрела» и проблематично говорить о лазерных источниках «многократного» действия.

Еще один гипотетический пример: некоторое количество МБР стартовало одновременно с одной локальной территории противника, т.е. нескольким БКС, находящимся в этом расчете боевого дежурства, будут противостоять несколько сот целей (ракеты + «ложняки»). Поэтому стандартная БКС должна как минимум обеспечить выполнение следующих требований:

– боезапас не менее тысячи «выстрелов»;

– скорострельность не менее десятка «выстрелов» в секунду.

В открытой американской научно-технической печати применительно к задачам ПРО рассматривались также четыре основных типа лазеров:

а) *химические* лазеры на фтористом водороде;

б) *эксимерные* лазеры;

в) *рентгеновские* лазеры с накачкой от ядерного взрыва;

г) лазеры *на свободных электронах*.

Однако все эти типы лазеров имеют свои специфические особенности, усложняющие решение задачи их реализации на борту БКС [1].

Так, например, химические лазеры в силу технических особенностей работы имеют большое газовыделение, причем в космосе всякая анизотропия газовых струй эквивалентна реактивной тяге, вызывающей соответствующие перемещения и развороты БКС, для компенсации которых потребуются запасы топлива, сравнимые с массой рабочей газовой смеси такого лазера.

В эксимерных лазерах, которые относятся к группе импульсных многократных лазеров, активной струей являются нестабильные возбужденные состояния химических соединений различных инертных газов.

Здесь одна из проблем – необходимость «охлаждать» рабочую смесь практически после каждого «выстрела», а при энерговыделениях, соответствующих задачам БКС, не удастся обеспечить требуемую «скорострельность».

Кроме того, эксимерные лазеры излучают в ультрафиолетовом диапазоне, для которого атмосфера «малопрозрачна».

Если химическим лазерам не нужна специальная энергосистема для накачки, то для эксимерных лазеров с их низким КПД проблема энергетики накачки заключается в основной необходимости обеспечивать мощность более сотни гигаватт с частотой повторения 10–100 Гц. Подобные требования не могут быть удовлетворены энергетическими установками космического базирования с их жесткими ограничениями габаритов и массы.

На рис. 1.2 показан один из вариантов использования в системах ПРО эксимерных лазеров наземного базирования, использующих схемы нацеливания на основе специальной системы зеркал космического базирования.

Пучковое оружие пригодно для использования только за пределами атмосферы (на высотах свыше 200 км) и на сравнительно небольших (не более 1000 км) расстояниях.

Если в качестве основной цели применения пучкового оружия рассматривать разрушение ядерной боеголовки, можно привести некоторые простейшие соображения по оценке эффективности [1]. Критическая масса урановой сферы с отражателем составляет 15–20 кг, радиус сферы ~ 6 см, плотность урана и плутония ~ 20 г/см^3. Достаточно расплавка только части ядерного заряда, поэтому эффективная длина свободного пробега протонов должна составлять около 100 г/см^2, что соответствует энергии протонов 300 МэВ.

Если получить размер пятна пучка на мишени $d = 1$ м, то радиус поражения составляет 250 км; радиусу поражения 500 км соответствует поперечный размер пучка 1,6 м, радиусу поражения 1000 км – почти 3 метра. При этом необходимая минимальная плотность тока должна составлять 10^{-4} А/см^2, что соответствует требуемому уровню полного тока 1 А, во втором – около 3 А, в третьем – 9 А.

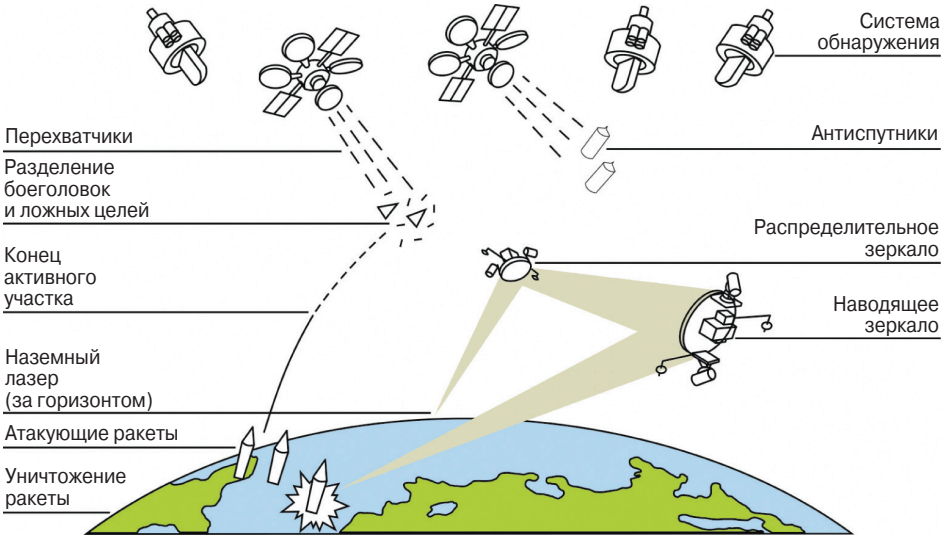

Рис. 1.2. Один из вариантов поражения МБР на активном участке траектории

Соответствующая мощность, вкладываемая в пучок, составит 300, 900 и 2700 мегаватт. Отдельные данные указывают, что метровый размер пучок приобретает уже на расстоянии всего 50 км, при радиусе поражения 1000 км требуется ток пучка почти 30 А, а поперечный размер пятна будет превышать 5 м.

Пучковое оружие обладает определенным потенциалом противодействия кинетическому оружию.

Кинетическое оружие (КО) – снаряды, направляемые обычно на объекты космического базирования противника в целях их уничтожения путем механического разрушения. Можно уничтожить цель и взрывом снаряда при наличии на его борту взрывного устройства автономного и программно управляемого типа.

Обычно используют следующие классификации типов КО:

1) инерционно-баллистические снаряды (движутся по инерции за пределами атмосферы);
2) снаряды-перехватчики с системами наведения (самонаведения).

Последние, в свою очередь, разделяются на два основных вида: не рассчитанные на прямое попадание в цель и снабженные фугасной или боевой частью; самонаводящиеся снаряды-перехватчики, рассчитанные на столкновение с целью.

Основной технической задачей здесь является обеспечение снаряду-перехватчику скорости не менее 10 км/с, при этом энергозатраты на один выстрел составляют порядка 100 МДж (что в принципе сравнимо с аналогичными характеристиками для лазерного и пучкового оружия).

Эту задачу решают по трем различным направлениям:

– артиллерийское (набор скорости под давлением пороховых газов);
– электромагнитное (использование электромагнитной ускоряющей системы типа хорошо известного физикам-экспериментаторам «рельсотрона») [1, 20];
– реактивное (использование ракетного двигателя для набора скорости за счет системы тяги при сжигании ракетного топлива).

Для «артиллерийских» технических решений предельная скорость в каждом случае определяется скоростью молекул пороховых газов, а это всего лишь около 3 км/с; кроме того, возникает проблема компенсации эффекта «отдачи» при выстреле, кроме дополнительного расхода топлива на систему ориентации и БКС, и в силу этого практически непригодна для использования в космическом эшелоне ПРО.

Для «реактивного» направления время разгона до конечной скорости зависит от выбранной тяги двигателя и массы перехватчика и для рубежа 15–18 км/с может лежать в пределах от 10 до 100 секунд.

И, наконец, *электромагнитные системы* имеют два основных недостатка, ограничивающие возможность их боевого применения в ближайшей перспективе:

1) значительные линейные размеры (пока – десятки метров), что затрудняет перенацеливание, ухудшает скорострельность и повышает уязвимость БКС;
2) непомерно большая масса энергосистемы.

1.1.4. Проблемы обеспечения надежности функционирования средств космического эшелона системы ПРО

Как показано в работах [1, 2], задача уничтожения баллистических ракет (на всем протяжении их траектории полета), космических аппаратов противника, наземных целей предполагает выведение на околоземные орбиты целого ряда базовых элементов космического эшелона ПРО. Это как сами средства поражения и их компоненты (например отражающие зеркала лазерных установок наземного базирования), так и различные средства обнаружения, целеуказания, управления, энергетического обеспечения, ракет защиты и др.

Основным элементом космического эшелона базирования являются так называемые боевые платформы или боевые космические станции (БКС).

Поэтому как к ним, так и к другим вышеперечисленным компонентам космического эшелона ПРО, вне зависимости от их назначения, предъявляются следующие основные требования:

– возможность находиться на орбитах в рабочем состоянии в течение длительного времени, обладать исключительно высокой надежностью и высоким быстродействием;
– быть обеспеченными необходимыми бортовыми ресурсами на все время функционирования (для автоматических компонентов) или иметь активную систему возобновления ресурсов (для БКС);
– иметь надежную аппаратурную и программную защиту от любых (как случайных, так и преднамеренных) воздействий различного характера, нарушающих их работоспособность;
– обеспечивать надежную, постоянную высокозащитную связь со всеми другими компонентами космоса и наземных элементов системы ПРО.

Надо сказать, что эти требования и сопутствующие им технические проблемы были известны и ранее для научных и коммерческих спутников, но с выводом в космос, размещением на платформах и при эксплуатации там различных боевых средств поражения эти требования и проблемы по своим масштабам возрастают многократно.

Также многократно возрастает в этих компонентах роль электроники вообще, и в особенности СВЧ-электроники.

Действительно, одним из важнейших факторов этих компонентов наземного и космических эшелонов ПРО является надежность их функционирования.

Однако для систем космического оружия необходимо отдельно рассматривать две ее составляющие: *техническую* надежность и *оперативную* (боевую) надежность.

Техническая надежность определяет ресурс работы БКС в основном (стационарном) режиме боевого дежурства. Очевидно, что быстрая замена на орбите вышедших из строя или исчерпавших свой ресурс электронных блоков и узлов не может быть проведена быстро, дешево и без ущерба для эффективности не только данного компонента, но и всего космического эшелона.

Поэтому требование обеспечения высокой *технической* надежности БКС прежде всего определяет необходимость обеспечения гарантированного максимального уровня надежности всех электронных блоков (и их элементной базы) при одновременном обеспечении максимально возможного ресурса их работы в условиях космического пространства (не менее десяти лет). И все это должно обеспечиваться не только без привычных для Земли «ремонтных» работ, но и без «регламентного технического обслуживания».

Здесь имеет место одно из многочисленных противоречий. С одной стороны, мировая техническая практика, в том числе в области авиа- и ракетостроения, показывает, что усложнение конструкции любых, в том числе и ранее отработанных, технических средств, позволяя расширять функциональные возможности и технические характеристики, влечет за собой сокращение сроков их безопасного функционирования. На Земле эта проблема решается более «частыми» процедурами технического обслуживания.

С другой стороны, все компоненты космического эшелона ПРО, учитывая предъявляемые к ней высокие требования, должны разрабатываться на основе самых передовых и, естественно, все более сложных технических и технологических решений.

Конечно же, как показано в работе [2], технически эта проблема частично решается известными путями (многократное резервирование, дублирование, троирование, мажоритирование, специальное программное обеспечение и т.п.).

Однако надо сказать, что проблема обеспечения чисто «технической» надежности (не только БКС, но и всех без исключения компонентов и подсистем, размещенных в околоземном пространстве космического эшелона) порождает исключительно сложные *проблемы военно-политического уровня*.

Любому «неспециалисту» по космическому оборудованию понятно, что даже временный (не катастрофический) отказ какого-либо важного электронного блока БКС, тем более в сочетании с выходом из строя какого-либо одного элемента подсистемы боевого управления, может повлечь за собой лавинообразную цепь непредсказуемых реакций всего предельно автоматизированного механизма принятия решений, который начнет управлять действием системы ПРО.

Нельзя при этом сбрасывать со счетов существующую определенную вероятность возникновения таких комбинаций технических сбоев и отказов различных компонентов ПРО, которые могут вызвать самопроизвольную (без участия чело-

века) активизацию и дальнейшее срабатывание как отдельных компонентов, так и всей системы ПРО.

Очевидно, что последствия развития подобного сценария настолько неприемлемы и непредсказуемы, что, как ни мала его вероятность (а ее никто из экспертов не отрицает), ею никак нельзя пренебрегать.

Даже «гражданские» специалисты по проблемам надежности могут сказать, что применяемые сегодня методы резервирования, дублирования, троирования и т.д. компонентов (и даже БКС в целом) не только эту проблему не решают, но могут даже ее усугубить, поскольку работает классическое правило: рост числа элементов в любой технической системе только увеличивает вероятность отказа этой системы, а также вероятность возникновения «неблагоприятных» комбинаций технических неисправностей (отказов).

Вот об этих проблемах надо думать в первую очередь ученым и военным, занимающимся проблемами создания различных вариантов рассматриваемого ниже в этой главе «наземного» и «космического» оружия и систем его боевого применения.

К сожалению, кроме одной из первых (и последних) фундаментальных работ группы советских ученых «Космическое оружие – дилемма безопасности» под редакцией вице-президента АН СССР Е.П. Велихова, академика АН СССР Р.З. Сагдеева и доктора исторических наук А.А. Кокошина (Москва, «Мир», 1986 г.) [1], выпущенной в свет только по инициативе существовавшей в то время общественной организации «Комитет советских ученых в защиту мира, против ядерной угрозы», ни в российской, ни в зарубежной «открытой» научно-технической печати эти проблемы, их последствия и возможные пути решения серьезно не обсуждались.

Да и появление этой вышеупомянутой работы имело определенную политическую цель – используя авторитетных ученых с мировым именем, показать нереальность технической реализации провозглашенной в то время президентом США Р. Рейганом так называемой стратегической оборонной инициативы (СОИ), впоследствии тихо ушедшей из «открытой» научно-периодической печати в десятки и сотни «закрытых» программ и проектов (как в США, так и в СССР).

Как мы видим, эта работа [1], написанная более тридцати лет назад, до сих пор актуальна, поэтому авторы настоящей технической энциклопедии постарались максимально близко к исходному тексту изложить проблемные вопросы, актуальность которых не только сохранилась, но даже выросла в связи с развитием научно-технического прогресса в области техники и ее электронной компонентной базы за этот прошедший период времени.

Наука и техника непрерывно развиваются, ученые и «технари» решают свои частные проблемы, а абсолютное большинство генералов, сенаторов, правительственных чиновников не читает подобные «умные» книги, решая свои военно-политические, стратегические и прочие «глобальные» проблемы, формируя и финансируя все новые амбициозные программы и проекты, не особо задумываясь о возможных негативных их последствиях.

Это в полной мере относится и к стремительно развивающейся СВЧ-электронике, ведь СВЧ-электроника не только является одной из основных компонент обеспечения требуемых технических характеристик современной РЭА гражданского и

военного применения, но в последнее время стала основой для создания различных видов вооружений и военной техники, а также весьма специализированного, ранее неизвестного оружия.

То, что, как будет сказано ниже, отдельные разновидности этого оружия называют «нелетальными» (несмертельными для человека), не должно читателя вводить в заблуждение: это действительно современное (и перспективное) оружие, направленное прежде всего против человека, по какую сторону от символической «линии фронта» он бы ни находился.

Причем давно известно: если новый вид оружия появился с одной стороны этой символической «линии», то рано или поздно он появится и на другой стороне («гонка вооружений»).

К сожалению для человечеств, а в последнее время и упомянутая СВЧ-электроника оказалась втянутой в эту эволюционную «гонку», причем далеко не в роли «аутсайдера», а тихо и незаметно для большинства непосвященных масс «зрителей», постепенно выходя на лидирующие позиции среди всех остальных «гонщиков».

Одним из побудительных мотивов авторов к написанию этой главы послужила несколько идеалистическая надежда, что, может быть, кто-то из генералов, политиков, дипломатов или правительственных чиновников все-таки ее прочитает и задумается об аспектах развития этой ветви научно-технического прогресса, возможных негативных моментах и в своей последующей профессиональной деятельности будет правильно учитывать все эти аспекты (как безусловно полезные для международного сообщества и каждого индивидуума, так и весьма проблематичные и даже крайне опасные).

Еще одной, не менее (а может и более) важной общей проблемой обеспечения надежности БКС и компонентов эшелона в целом является так называемая *оперативная надежность*, характеризующая способность выполнять запрограммированные боевые функции в любых ситуациях и во всех заложенных военными заказчиками технических условиях и рабочих режимах. Прежде всего это относится к основной функции – уничтожению цели – как ракет противника на любом участке траектории их наблюдения, так и заданных воздушных, наземных (стационарных и/или мобильных) целей, в том числе малоразмерных, быстроперемещающихся целей (вертолетов, самолетов), шахт и мест базирования ядерных ракет, надводных кораблей, мест предполагаемого нахождения подводных ракетоносцев с готовыми к старту баллистическими ракетами и т.д.

К сожалению, тема оперативной надежности компонентов космического эшелона с начала 90-х годов прошлого века является полностью закрытой для публикаций. Если говорить «простым» языком, технических проблем здесь много, а путей их решения катастрофически мало, и наиболее «простые» технические решения требуют огромных финансовых затрат, ставящих под сомнение саму возможность эффективной работы ПРО в целом.

Поэтому ниже мы приведем информацию без ссылок на литературные источники, поскольку она была получена авторами из «неофициальных» источников, а также результатов личных контактов авторов с техническими специалистами, так или иначе задействованными в решении этой проблемы, во время междуна-

родных конференций, семинаров, чтения авторами лекций в профильных учебных заведениях, научно-исследовательских институтах и лабораториях Китая, Индии, Германии, Франции, Англии и других стран.

Так, например, один из очевидных путей повышения оперативной надежности – это качественное совершенствования конкретных средств поражения, развернутых на БКС, с учетом оптимального баланса комбинаций параметров «боезапас – скорострельность».

Причем если «лобовое» решение – просто увеличение боезапаса (количества средств поражения) на борту БКС является хотя и сложной, но технически вполне реализуемой задачей, то повысить ее скорострельность сверх заложенных в систему возможностей будет значительно труднее.

Оптимальный баланс «боезапас – скорострельность» зависит от многочисленных технических параметров как самих боезапасов (средств поражения), так и от различных так называемых вспомогательных компонентов, без которых невозможно обеспечить эффективную работу БКС в активной боевой фазе. Например, проблема эффективности и быстрого отвода избыточной тепловой энергии в боевом режиме: ведь, как показано выше, ни один из известных из открытой печати видов оружия направленной передачи энергии (в том числе лазерное и ЭМИ-оружие) не обладает достаточно высоким КПД и при боевой работе («стрельбе») выделение огромной тепловой энергии просто приводит к выходу из строя БКС. Специальные лаборатории закрытых институтов США и СССР (России) занимаются уже более 30 лет проблемами создания таких эффективных «систем теплосъема» различных боевых космических платформ, несущих вышеописанные виды средств поражения, но, по имеющейся разрозненной информации, все испытанные технические решения при весьма значительных массогабаритных характеристиках до настоящего времени обладают недостаточной для этого класса задач эффективностью. Ситуация усугубляется еще и тем очевидным фактором, что развернутое в космосе широко рекламируемое ПРО космического эшелона по понятным причинам *не может быть испытано в реальных условиях* и, как уклончиво говорят американские специалисты, «существует значительная неопределенность» в количественных оценках технической и оперативной надежности БКС и боевых платформ, а также развертываемых на их базе вспомогательных средств.

Еще одна очевидная проблема – *обеспечение эффективной защиты* БКС и других орбитальных средств ПРО от мер активного противодействия и прямой атаки (нападения) противника. Поскольку все боевые станции и другие необходимые компоненты космического эшелона системы ПРО имеют значительные габариты и массу (в перспективе – сотни тонн), все они двигаются в околоземном пространстве по постоянным (заранее известным противнику) орбитам, все они сами по себе являются достаточно уязвимыми целями для атаки самыми различными (и зачастую исключительно простыми и дешевыми) противоспутниковыми средствами (один из возможных вариантов продекларированного в свое время президентами России Медведевым и Путиным «несимметричного» ответа России на развертываемую НАТО европейскую ПРО).

Анализ проблемы уязвимости не только БКС, но и всех эшелонов космического базирования системы ПРО позволяет утверждать, что вне зависимости от

конкретных технических вариантов обеспечения любые средства такой защиты с точки зрения финансовых затрат явно не будут «дешевыми» и потребуют выведения в космос значительных масс грузов.

Конечно, специалисты разрабатывают и различные относительно «малобюджетные» средства, в том числе маневрирование БКС и боевых платформ на орбите «для ухода из-под удара», специальные технические мероприятия по «маскировке» (за счет развертывания разветвленной сети «ложных» целей, мгновенно активизирующихся в момент атаки БКС) и др.

Другие известные направления «пассивной» защиты – оснащение компонентов космического эшелона ПРО различного рода защитными экранами, использование специальных материалов покрытий и пр.

Еще одна группа защитных мер – разработка и использование различных «интеллектуальных» активных поражающих систем, создающих в этом радиусе защиты своего рода «зоны суверенитета», при этом размещаемые на БКС средства такой самозащиты могут уничтожить *любой объект*, приближающийся к станции ближе заранее установленного расстояния или с неразрешенной скоростью.

Но здесь возникает еще одна проблема – проблема «ограниченности» безграничного космического пространства. Действительно, размеры таких защитных зон с развитием средств поражения неизбежно будут увеличиваться и при определенных параметрах могут создавать серьезные препятствия для *коммерческой* деятельности в космосе: эти зоны будут постоянно расширяться, их число (как и число защищаемых объектов) будет постоянно увеличиваться, в итоге в околоземном пространстве может возникнуть целая система таких «запретных» зон (американская, китайская, российская, европейская, индийская и т. п.), заход в которые «невоенных» объектов, даже случайных (в результате ошибки навигационного оборудования), будет представлять реальную опасность для космических объектов не только «других» стран, но и самого обладателя такого «противоракетного щита».

А если учесть довольно высокую вероятность попадания в эти зоны метеоритов и других «вольных» космических тел (а также остатков переставших функционировать искусственных спутников Земли, обломков взорвавшихся и взорванных [2] ракет и спутников, просто космического мусора, которые сегодня на орбите исчисляются уже сотнями тысяч штук), то эта «вероятность» уже может очень скоро превратиться в реальность. Ведь в соответствии с правилами и законами «машинной» логики каждое такое вторжение – это нарушение суверенитета защищаемой зоны объекта, и ее защита *немедленно* будет приведена в действие.

Понятно, что в ответ на каждый такой акт «нарушения суверенитета» системы защиты БКС будут непременно автоматически активизироваться (реакция человека здесь неприемлема – слишком малое время отводится как на фиксацию факта «агрессии», так и на ответные защитные действия), а результат можно будет охарактеризовать, как в известном армейском анекдоте – «сначала выстрелим, а потом спросим пароль».

Срабатывание автоматики активной системы защиты станции неизбежно должно сопровождаться «боевой активизацией» этой самой станции, зафиксировавшей факт «нападения» и запустившей автоматически систему боевого управления (для этого ее и создавали конструкторы).

Другая сторона (а реально – все «другие» стороны, вышедшие в открытый космос) неизбежно должна обнаружить техническими средствами факт активизации ПРО потенциального противника и просто обязана считать, что он готовит первый ядерно-ракетный, лазерный или «обезоруживший» удар, и будет вынуждена экстренно принимать меры по *соответствующему реагированию* своих наступательных стратегических вооружений.

Понятно даже «гражданским» экспертам, что вышеописанная «цепная реакция» эскалации инцидента будет протекать настолько быстро, что не оставит никаких временных шансов для дипломатического (политического) урегулирования возникшего на «ровном месте» кризиса.

1.1.5. Европейская безопасность и европейская СПРО

Вышеизложенные *общие* научно-технические и военно-стратегические аспекты ПРО в целом в полной мере можно отнести и к *частному* вопросу – европейскому театру возможных боевых действий по отражению ракетной атаки на космические или наземные элементы ПРО.

Очевидно, что каждый эшелон ПРО в отдельности заведомо «недостаточно самодостаточен», чтобы даже теоретически обеспечить надежную защиту территории. Поэтому и создаются обычно несколько эшелонов, каждый последующий из которых должен устранять «ошибки» функционирования предыдущих путем уничтожения «прорвавшихся» единиц боевого оружия (ядерных боеголовок и мобильного СВЧ-оружия).

Создавая *свой* противоракетный «щит», США заявляют, что якобы смогут «прикрыть» им *не только себя, но и всех своих союзников*. Мол, надо только разместить некоторые его элементы и на территории этих союзников (в частности на европейской территории).

К сожалению для наших европейских партнеров, это далеко не так, и об этом надо бы открыто говорить в СМИ всех европейских стран, но, к сожалению, за последние годы мы видим обратную картину. Хотя, как многократно заявляло руководство России, никто у нас не собирается нападать на европейские страны, в европейских СМИ активно обсуждается тезис об «угрозе с Востока», почему-то при этом делается акцент на угрозы «исламского терроризма» и конкретной страны – исламского государства Иран.

Прежде всего надо понимать, что включение европейских союзников США в зону действия космического эшелона американской глобальной системы ПРО означает необходимость обеспечения их защиты от носителей ядерного оружия *совершенно другого типа* по сравнению с МБР. На европейском теоретическом театре военных действий смогут применяться только ракеты средней дальности, с «пологими» траекториями полета, значительно более короткими временами прохождения активных участков траектории, намного укороченным пролетным временем и т.п.

Эти и ряд других факторов заведомо указывают *любым беспристрастным экспертам* на невозможность подключения всех систем и средств эшелонов космической ПРО для эффективного выполнения заявленных по отношению к Европе защитных функций даже теми элементами ПРО, которые теоретически могут быть задействованы.

Действительно, в отличие от МБР баллистические ракеты среднего радиуса действия (или тем более *современные оперативно-тактические ракеты* – ОТР) имеют время продолжительности полета на активном участке траектории намного меньше, чем даже известные для нижнего предела скоростей, необходимого для эффективного срабатывания средств первого эшелона системы ПРО.

Ясно, что последующие эшелоны СПРО будут в этой ситуации работать в условиях огромного дефицита времени (ведь время подлета до цели ОТР в 2–4 раза меньше, чем у МБР), тем более что эта атака не может быть значительно ослаблена (как планируется) предыдущими эшелонами СПРО.

Далее, поскольку полет ОТР на баллистическом участке проходит на значительно меньшей высоте, чем у МБР, это фактически исключит (или существенно ограничит) использование на европейском ТВД целого ряда видов вышерассмотренного в этой главе оружия. Так, из-за сильного поглощения в атмосфере лазерного излучения невозможно будет эффективно использовать любые лазеры космического базирования, поскольку большую часть времени года облачность покрывает большую часть европейской территории.

Кроме того, малая высота полета ОТР требует привлечения большого числа космических элементов противодействия (средств обнаружения, наведения, поражения) для постоянного боевого дежурства при ограниченной дальности их действия.

То же *кинетическое оружие* для «европейского» варианта СПРО уже будет совершенно другим, поскольку высота базирования боевой платформы с пусковыми установками всегда выбирается исходя из общего количества носителей и времени активного существования на орбите соответствующих боевых платформ; снижение траекторий целей и сокращение времени их нахождения на «заатмосферном» участке боевых траекторий потребуют либо *увеличения радиуса действия противоракетного космического оружия* (при очевидной необходимости усложнения его конструкции), либо *снижения высоты рабочих орбит БКС* со всеми вытекающими последствиями.

Короче говоря, миф о возможности распространения на европейских союзников США созданного ими противоракетного щита, очевидно, несостоятелен уже в силу специфических особенностей БРСД ядерных средств доставки меньшей дальности потенциального противника (называя Иран, имеют в виду Россию), поскольку эффективность «европейского» сегмента глобальной американской СПРО для союзников США будет значительно ниже ее эффективности (тоже невысокой) для «старшего брата» именно *на стратегическом уровне*, и это надо ясно понимать европейским (включая страны Балтии) политикам, активно поднимающим мифические проблемы опасности «Востока», но не замечающим этих совершенно очевидных реальных *стратегических опасностей*.

Европейские политики должны бы ясно понимать, что из-за высокой концентрации населения и промышленных объектов на европейской территории будет невозможно избежать катастрофически высокой степени материального урона, человеческих жертв при первых же попытках такой «защиты» как всей территории, так и отдельных стратегических и промышленных объектов.

Следует также отметить и такой очевидный для специалистов факт: возможность поражения средствами космического эшелона СПРО основных средств доставки

именно *ядерного* оружия, в случае его использования военными на специфическом европейском «театре боевых действий», в общем случае представляется *крайне сомнительной*; это относится к крылатым ракетам (наземного, морского и воздушного базирования), современным стратегическим ядерным бомбардировщиком, так называемой ядерной артиллерии и нижеперечисленным системам доставки современного СВЧ-оружия. А ведь надо понимать, что здесь речь идет не о сотнях, а о тысячах (а может, и десятках тысяч – в зависимости от военных бюджетов противников) носителей ядерного оружия, причем в основном относящегося в данном случае к категории тактического ядерного оружия.

И еще один существенный для понимания всей сложности рассматриваемой проблемы технический аспект, который никогда публично не поднимают зарубежные специалисты, в том числе аналитики стран Балтии, Польши и других бывших стран Варшавского договора времен СССР.

«Выбивая» из бюджетов европейских стран финансы для развития систем «противодействия восточной угрозе», политики говорят о необходимости и эффективности создания на территориях их стран в рамках американской легенды «ядерного зонтика» так называемых *ограниченных (объектовых или зональных) систем ПРО*, ориентированных на защиту конкретных локально ограниченных участков территорий их стран, на которых расположены стратегические объекты.

Причем даже многие руководители крупнейших европейских производственных зон предлагают свои территории в качестве таких объектов защиты. Но, во-первых, следует четко представлять критерии, по которым определяется ценность для государства того или иного объекта.

А ведь на европейском театре в силу вышеизложенных факторов (высокая концентрация промышленности и населения, это не Сибирь) реально не представляется возможным выделить только десяток-два *особо важных* регионов и объектов, поскольку просто нет там наземных целей для МБР.

Таким образом, *объективное* рассмотрение все технических аспектов эффективности защиты европейских партнеров НАТО американским ракетно-ядерным «зонтиком» со всеми его компонентами наземного и космического эшелона показывает очевидно более низкую эффективность такой системы даже в сравнении с аналогичными возможностями, может, и более ограниченных, но *национальных* систем ПРО европейских стран и даже «независимых» стран Балтии.

Есть и еще многие другие чисто стратегические и военно-политические аспекты, без знания которых сложно ориентироваться в вопросах создания современного ядерного и СВЧ-оружия.

Учитывая, во-первых, ограниченный объем этой книги, а во-вторых, ее чисто техническую ориентацию, тем не менее следует отметить *некоторые стратегические и политические аспекты*, используемые европейскими лидерами при принятии решений в этом направлении, которые рассмотрим на примере только двух европейских стран – Германии и Франции, при этом покажем, что они объясняются либо неверными представлениями о реальной ситуации в вопросах СПРО, либо ложными амбициями лидеров этих государств.

Так, например, очевидное стремление *Германии* как можно шире участвовать во всех работах по созданию СПРО отчасти объясняется тем фактом, что, *являясь вме-*

сте с США вроде бы постоянным членом военно-политического союза НАТО (созданного США) и обладая весьма существенным промышленным и научным потенциалом, это государство не обладает ядерным оружием и в силу этого не может реально играть достаточно влиятельную роль в международной политике с позиции потенциальной силы. Принимая участие во всех инициативах НАТО, США и Англии в сфере развития европейской СПРО, политическое и военное руководство Германии хотело бы, хотя и в косвенной форме, но все-таки получить реальный доступ к техническим аспектам создания (или использования) собственного ядерного оружия. Это позволило бы Германии оказывать такое же, как ядерные державы, влияние на все аспекты современной международной политики, где до сих пор фактор обладания ядерным оружием, к сожалению, является одним из основных понимаемых партнерами «очевидных» аргументов «правоты».

Другая же крупная европейская страна – *Франция*, обладающая ядерным оружием, попыталась пойти по другому пути, исходя из этих же стратегических аспектов, сформулированных выше для Германии. Еще в 80-х годах прошлого века политическое руководство Франции выступило с инициативой создания собственного (европейского) проекта создания СПРО, который известен под названием «Эврика» и который в противовес американской концепции был призван служить «святому делу» интеграции научных и производственных возможностей Западной Европы в деле стимулирования западноевропейской науки и техники, его результаты могли бы успешно быть применены и в военных целях – для защиты Европы от космических атак и возможности агрессии со стороны тогдашнего мощного ракетно-ядерного коммунистического СССР.

Некоторые наиболее активные политики этих стран с трибуны своих парламентских собраний даже на момент издания этой энциклопедии активно проводят тезисы о том, что только присоединение к военно-политическим инициативам США в области создания европейской СПРО может увеличить влияние этих стран в международном сообществе и будет способствовать активизации используемых программ развития научно-технического прогресса.

Но очевидно, что следовать таким призывам *и опасно, и бессмысленно*: сейчас международный авторитет любой страны далеко не определяется только мощностью имеющегося в ее распоряжении ядерного или любого другого оружия.

Если и будут в итоге «подключения» к американским инициативам получены ими какие-то элементы оборонительного оружия, то это будет далеко не ожидаемое этими политиками «сверхоружие»: Западной Европе будут переданы в лучшем случае второстепенные и не связанные друг с другом технические компоненты подобных систем.

Нельзя «сбрасывать со счетов» и *ядерные амбиции Великобритании*: многие вышерассмотренные (и более детально рассмотренные ниже в этой главе) средства противодействия системам противоракетного оружия, включая модернизацию лазерных и СВЧ-вооружений, активно разрабатываются и *испытываются* в этой стране, в том числе в последних военных конфликтах на Ближнем Востоке (в Ираке, Сирии и других странах).

Из всего вышеизложенного нужно сделать один важный для понимания ситуации вывод: *широко пропагандируя в западной печати идею о создании «маленького*

американского зонтика», прикрывающего «европейского младшего брата» от возможных «актов агрессии экстремистов – террористов и русских», авторы этой идеи просто выполняют «отвлекающий маневр».

Действительный военно-стратегический замысел американских идеологов состоит в том, чтобы в условиях ими же весьма искусно создаваемой истеричной обстановки вокруг проблем Украины и Крыма прикрыть этим щитом *только США* от возможного превентивного или ответного удара, а Европу использовать только *как экспериментальный полигон* для ведения там различных политических (или даже военных) игрищ и действий.

1.1.6. Космический эшелон системы предупреждения о ракетном нападении

1.1.6.1. Российская космическая система обнаружения стартов ракет

В соответствии с концепцией создания системы раннего предупреждения, разработанной в СССР в начале 70-х годов, система, наряду с надгоризонтными и загоризонтными РЛС «наземного эшелона», должна была включать в себя космический эшелон, который был призван существенно расширить ее возможности за счет своей способности обнаруживать баллистические ракеты практически сразу после старта [3].

Работа над стратегией построения космического эшелона системы предупреждения была поручена ЦНИИ «Комета», а разработка космических аппаратов – КБ им. С.А. Лавочкина.

В соответствии с проектом, разработанным в ЦНИИ «Комета», космическая система предупреждения, известная сегодня как УС-КС или «Око», должна была включать в себя группировку спутников, размещенных на высокоэллиптических орбитах, и пункт управления вблизи Москвы. На спутниках размещались детекторы излучения инфракрасного и видимого диапазонов, которые были способны регистрировать сигнал, излучаемый работающим двигателем стартующих баллистических ракет. Сигнал должен был устойчиво фиксироваться на фоне космического пространства (но не на фоне земной поверхности). Система начала работу в сокращенном составе в 1978 г., а поставлена на боевое дежурство в 1982 г.

Одновременно с развертыванием системы УС-КС шла работа над выработкой технических требований для новой системы, получившей наименование УС-КМО (на Западе эту систему называли «Прогноз»). Эта система была призвана обеспечивать наблюдение за пусками ракет морского базирования из акватории мирового океана, а также пуски ракет с территории США и Китая. Для решения этой задачи средства новой системы должны были осуществлять обнаружение стартующих ракет уже на фоне земной поверхности. Однако вплоть до 1984 г. продолжались проблемы, которые вынуждали взрывать космические аппараты на орбите [3].

Космическая система обнаружения стартов ракет с континентальной части США «Око» включала в себя спутники УС-КС на высокоэллиптических орбитах со станцией управления и приема информации (СУПИ) и стартовый комплекс. Создание космической системы обнаружения стартов ракет было поручено КБ Челомея в начале 1960-х гг. В 1962 г. был подготовлен аванпроект системы, вклю-

чавшей 20 спутников массой в 1400 кг, расположенных на одной полярной орбите высотой 3600 км.

Спутники выводились на орбиту РН УР-200 и должны были обнаруживать ракеты по тепловому излучению факела двигателей первой ступени.

19 сентября 1972 г. с космодрома Плесецк РН «Молния» вывела на орбиту первый КА «Око» («Космос-520»).

Следует сказать, что в начале программы имелись серьезные проблемы с технической надежностью спутников. Из первых 13 спутников, запущенных в 1972–1979 гг., только семь проработали всего лишь более 100 дней. Впоследствии срок активного существования КА удалось довести до 3 лет (в это время американские аппараты IMEWS-2 функционировали на орбите 5–7 лет). Развертывание системы «Око» началось запуском четырех аппаратов в 1979 г., 5 апреля 1979 г. система была принята на вооружение, а уже в июле 1979 г. она зафиксировала старт ракеты-носителя с атолла Кваджалейн.

В 1980 г. на эллиптические орбиты были выведены шесть спутников, а сама система была сопряжена с глобальной системой предупреждения о ракетном нападении (СПРН). 30 декабря 1982 г. космическая система с шестью спутниками заступила на боевое дежурство.

До 1983 г. все спутники были оснащены *электронной системой самоуничтожения*, активировавшейся в случае потери связи с пунктом наземного контроля. По этой причине до 1983 г. было утрачено 11 из 31 КА (табл. 1.2), т.е. *каждый третий спутник* [3]. После 1983 г. было принято решение все-таки не активизировать системы самоликвидации в этой ситуации, что не намного улучшило статистику отказов на орбите.

Таблица 1.2. Хронология эксплуатации российских спутников космического эшелона СПРН за период с 1972 по 1992 гг.

Спутник	Номер NORAD	Международное обозначение	Тип	Дата запуска (дд. мм.гг)	Время старта (UTC)	Орбитальная плоскость или точка стояния	Окончание работы (оценка) дд.мм.гг	Комментарий
Космос-520	6192	1972-072A	HEO	19.09.72	19:19:03	4	??	
Космос-606	6916	1973-084A	HEO	02.11.73	13:01:56	4	30.04.74	
Космос-665	7352	1974-050A	HEO	29.06.74	15:59:58	2	07.09.75	
Космос-706	7625	1975-007A	HEO	30.01.75	15:02:00	7	20.11.75	
Космос-775	8357	1975-097A	GEO	08.10.75	00:30:00	??	??	Орбита не была стабилизирована
Космос-862	9495	1976-105A	HEO	22.10.76	09:12:00	5	15.03.77	Взорван
Космос-903	9911	1977-027A	HEO	11.04.77	01:38:00	7	08.06.78	Взорван
Космос-917	10059	1977-047A	HEO	16.06.77	04:58:00	9	30.03.79	Взорван
Космос-931	10150	1977-068A	HEO	20.07.77	04:44:00	2	24.10.77	Не достиг штатной орбиты. Взорван
Космос-1024	10970	1978-066A	HEO	28.06.78	02:58:00	2	24.05.80	Переведен на нештатную орбиту в октябре 1979 г.

Таблица 1.2 *(продолжение)*

Спутник	Номер NORAD	Международное обозначение	Тип	Дата запуска (дд.мм.гг)	Время старта (UTC)	Орбитальная плоскость или точка стояния	Окончание работы (оценка) дд.мм.гг	Комментарий
Космос-1030	11015	1978-083A	НЕО	06.09.78	03:04:00	4	10.10.78	Взорван. Орбита не была стабилизирована
Космос-1109	11417	1979-058A	НЕО	27.06.79	18:11:00	9	15.02.80	Взорван. Орбита не была стабилизирована
Космос-1124	11509	1979-077A	НЕО	28.08.79	00:17:00	4	09.09.79	Взорван. Орбита не была стабилизирована
Космос-1164	11700	1980-01 ЗА	НЕО	12.02.80	00:53:00	9		Аварийный запуск
Космос-1172	11758	1980-028A	НЕО	12.04.80	20:18:00	9	09.04.82	
Космос-1188	11844	1980-050A	НЕО	14.06.80	20:52:00	2	28.10.80	
Космос-1191	11871	1980-057A	НЕО	02.07.80	00:54:00	4	16.05.81	
Космос-1217	12032	1980-085A	НЕО	24.10.80	10:53:00	2	20.03.83	
Космос-1223	12078	1980-095A	НЕО	27.11.80	21:37:00	7	11.08.82	
Космос-1247	12303	1981-016A	НЕО	19.02.81	10:00:00	5	20.10.81	Взорван
Космос-1261	12376	1981-031A	НЕО	31.03.81	09:40:00	6	01.05.81	Взорван
Космос-1278	12547	1981-058A	НЕО	19.06.81	19:37:04	4	05.07.84	Взорван в декабре 1986 г.
Космос-1285	12627	1981-071A	НЕО	04.08.81	00:13:00	6	21.11.81	Не достиг штатной орбиты. Взорван
Космос-1317	12933	1981-108A	НЕО	31.10.81	22:54:00	9	26.01.84	Взорван
Космос-1341	13080	1982-016A	НЕО	03.03.82	05:44:38	5	01.02.84	
Космос-1348	13124	1982-029A	НЕО	07.04.82	13:42:00	9	22.07.84	
Космос-1367	13205	1982-045A	НЕО	20.05.82	13:09:00	1	30.09.84	
Космос-1382	13295	1982-064A	НЕО	25.06.82	02:28:00	7	29.09.84	
Космос-1409	13585	1982-095A	НЕО	22.09.82	06:23:00	2	05.01.87	
Космос-1456	14034	1983-038A	НЕО	25.04.83	19:34:00	4	13.08.83	Взорван
Космос-1481	14182	1983-070A	НЕО	08.07.83	19:21:00	6	09.07.83	Не достиг штатной орбиты. Взорван
Космос-1518	14587	1983-126A	НЕО	28.12.83	03:48:00	5	01.06.84	
Космос-1541	14790	1984-024A	НЕО	06.03.84	17:10:00	3	31.10.85	
Космос-1546	14867	1984-031A	GEO	29.03.84	05:53:00	1,4	16.11.86	
Космос-1547	14884	1984-ОЗ-ЗА	НЕО	04.04.84	01:40:04	7	23.08.85	
Космос-1569	15027	1984-055A	НЕО	06.06.84	15:34:00	5	26.01.86	
Космос-1581	15095	1984-071A	НЕО	03.07.84	21:31:00	8	19.08.85	
Космос-1586	15147	1984-079A	НЕО	02.08.84	08:38:00	4	01.04.85	
Космос-1596	15267	1984-096A	НЕО	07.09.84	19:13:00	9	26.11.86	
Космос-1604	15350	1984-107A	НЕО	04.10.84	19:49:13	1	27.09.85	
Космос-1629	15574	1985-016A	GEO	21.02.85	07:57:00	4, 3, 1	16.01.87	
Космос-1658	15808	1985-045A	НЕО	11.06.85	14:27:00	6	03.09.87	

Таблица 1.2 *(продолжение)*

Спутник	Номер NORAD	Международное обозначение	Тип	Дата запуска (дд.мм.гг)	Время старта (UTC)	Орбитальная плоскость или точка стояния	Окончание работы (оценка) дд.мм.гг	Комментарий
Космос-1661	15827	1985-049A	НЕО	18.06.85	00:40:26	??	21.10.89	Переведен на нештатную орбиту в начале работы
Космос-1675	15952	1985-071A	НЕО	12.08.85	15:09:00	8	18.01.86	
Космос-1684	16064	1985-084A	НЕО	24.09.85	01:18:10	4	09.03.89	
Космос-1687	16103	1985-088A	НЕО	30.09.85	19:23:00	2	30.09.85	Орбита не была стабилизирована
Космос-1698	16183	1985-098A	НЕО	22.10.85	20:24:00	3	24.08.86	
Космос-1701	16235	1985-105A	НЕО	09.11.85	08:25:00	8	23.11.87	Переведен на нештатную орбиту в декабре 1986 г.
Космос-1729	16527	1986-011A	НЕО	01.02.86	18:11:56	5	14.05.88	
Космос-1761	16849	1986-050A	НЕО	05.07.86	01:16:47	3	23.10.88	
Космос-1774	16922	1986-065A	НЕО	28.08.86	08:02:43	7	17.07.88	
Космос-1783	16993	1986-075A	НЕО	03.10.86	13:05:40	1	03.10.86	Не достиг штатной орбиты
Космос-1785	17031	1986-078A	НЕО	15.10.86	09:29:18	9	16.01.91	Переведен на нештатную орбиту в декабре 1989 г.
Космос-1793	17134	1986-091A	НЕО	20.11.86	12:09:20	2	13.08.91	Переведен на нештатную орбиту в июне 1990 г.
Космос-1806	17213	1986-098A	НЕО	12.12.86	18:35:36	5	20.11.88	
Космос-1849	18083	1987-048A	НЕО	04.06.87	18:50:23	1	20.05.90	
Космос-1851	18103	1987-050A	НЕО	12.06.87	07:40:28	6	23.11.89	
Космос-1894	18443	1987-091A	GEO	28.10.87	15:15:00	1	22.12.91	
Космос-1903	18701	1987-105A	НЕО	21.12.87	22:35:42	8	11.11.92	
Космос-1922	18881	1988-01 ЗА	НЕО	26.02.88	09:31:12	5	30.07.90	
Космос-1966	19445	1988-076A	НЕО	30.08.88	14:14:54	3	14.12.90	
Космос-1974	19554	1988-092A	НЕО	03.10.88	22:23:39	7	20.05.93	
Космос-1977	19608	1988-096A	НЕО	25.10.88	18:02:31	6	12.07.90	
Космос-2001	19796	1989-011A	НЕО	14.02.89	04:21:11	4	15.03.93	
Космос-2050	20330	1989-091A	НЕО	23.11.89	20:35:44	9	08.10.93	
Космос-2063	20536	1990-026A	НЕО	27.03.90	16:40:08	2	21.06.95	
Космос-2076	20596	1990-040A	НЕО	28.04.90	11:37:02	1	30.10.92	
Космос-2084	20663	1990-055A	НЕО	21.06.90	20:45:52	6	21.06.90	Не достиг штатной орбиты
Космос-2087	20707	1990-064A	НЕО	25.07.90	18:13:56	6	21.01.92	
Космос-2097	20767	1990-076A	НЕО	28.08.90	07:49:13	3	30.04.95	
Космос-2105	20941	1990-099A	НЕО	20.11.90	02:33:14	3	04.04.93	Переведен на нештатную орбиту в феврале 1992 г.

Таблица 1.2 *(окончание)*

Спутник	Номер NORAD	Международное обозначение	Тип	Дата запуска (дд.мм.гг)	Время старта (UTC)	Орбитальная плоскость или точка стояния	Окончание работы (оценка) дд.мм.гг	Комментарий
Космос-2133	21111	1991-010A	GEO	14.02.91	08:31:56	4, 3, 2, 1,4	09.11.95	
Космос-2155	21702	1991-064A	GEO	13.09.91	17:51:02	1	16.06.92	
Космос-2176	21847	1992-003A	HEO	24.01.92	01:18:01	6	13.04.96	
Космос-2196	22017	1992-040A	HEO	08.07.92	09:53:14	5	23.06.94	
Космос-2209	22112	1992-059A	GEO	10.09.92	18:01:18	1	16.11.96	
Космос-2217	22189	1992-069A	HEO	21.10.92	10:21:22	8	07.11.96	
Космос-2222	22238	1992-081A	HEO	25.11.92	12:18:54	1	03.12.96	
Космос-2224	22269	1992-088A	GEO	17.12.92	12:45:00	2, 1,2	17.06.99	
Космос-2232	22321	1993-006A	HEO	26.01.93	15:55:26	4	04.06.98	

В 1984 г. на геостационарной орбите начал работу КА УС-КС системы «Око-С». Спутник помещался в точку стояния на 240° западной долготы, обеспечивая наблюдение за центральной частью территории США. Этот спутник видел пуски ракет с территории США под точно таким же углом, что и спутник на высокоэллиптической орбите (ВЭО) во время рабочей части своей орбиты, не изменяя свою позицию относительно Земли.

Введение геостационарных спутников сделало систему несколько более надежной. Так, спутник на ГСО способен обнаружить запуски, даже если высокоэллиптические спутники не развернуты вовсе. Однако при этом может пострадать качество покрытия и надежность обнаружения, хотя система не является полностью «слепой». Аппаратура КА регистрирует инфракрасное излучение стартующих ракет только на краю видимого диска Земли (на фоне атмосферы) и передает инфракрасное изображение на Землю в реальном времени. Только за период с 1972 по 2002 гг. было запущено 86 аппаратов УС-КС (четыре на ГСО). Наибольшее число пусков (по восемь) произведено в 1984–1985 гг.

Трассы спутников системы «Око» значительно смещены к западу, что позволяет наблюдать за территорией США из апогея, находясь одновременно в зоне радиовидимости России. Для наблюдения используются телекамеры-видиконы, приспособленные для ближнего ИК- и УФ-диапазонов.

Выбор геометрии наблюдения и, соответственно, высокоэллиптических орбит для размещения спутников объясняется *отсутствием в Советском Союзе в то время микроэлектронной технологии создания полупроводниковых приемников инфракрасного диапазона и микроэлектронных средств обработки данных*, которые позволили бы реализовать регистрацию ракет на фоне земной поверхности. Не имея подходящих ИК-приемников, Советский Союз был вынужден создавать систему, которая полагалась бы на геометрию наблюдения под скользящим углом и которая позволяла наблюдать сигнал стартующей ракеты на фоне космического пространства. Такие условия наблюдения предъявляли к приемникам гораздо менее жесткие требования, но требовали от государства привлечения больших объемов финансовых средств, поскольку в состав группировки на высокоэллиптических орбитах должно

входить *большее количество спутников, чем требуется для создания геостационарной группировки*.

Вышеприведенные примеры из нашей недавней истории лишь подтверждают исключительно важную роль обеспечения безопасности ЭКБ в вопросах создания эффективных космических эшелонов систем ПРО.

1.1.6.2. Военно-разведывательные спутники

Создание космического эшелона СПРО было невозможно без военно-разведывательных (разведывательных) спутников, предназначенных для наблюдения Земли (телевизионная съемка, фотосъемка) в целях обеспечения разведывательной деятельности. Журналисты называют их «спутники-шпионы» [4].

Основные функции разведывательных ИСЗ:

- фотографирование с высоким разрешением (видовая разведка);
- прослушивание систем связи и определение местоположения радиосредств (радиотехническая разведка);
- слежение за выполнением запрета на ядерные испытания;
- обнаружение пусков ракет (система предупреждения о ракетном нападении).

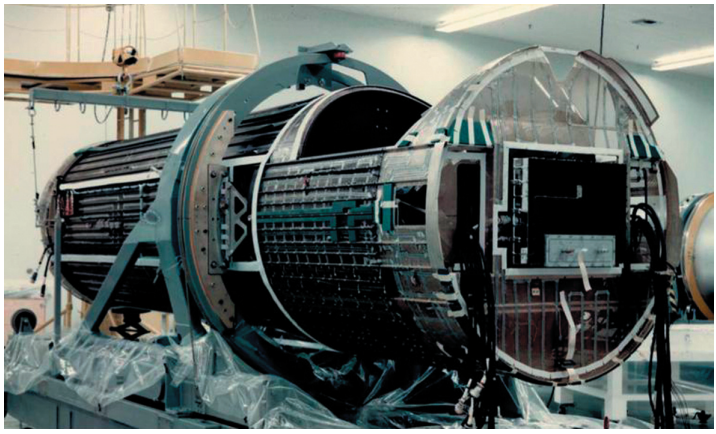

Рис. 1.3. Трехтонный спутник-шпион КН-8

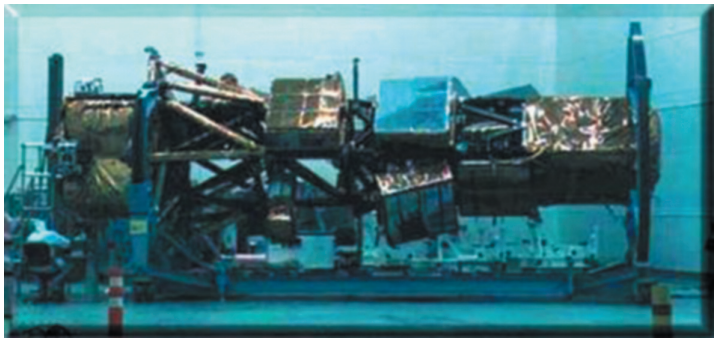

Рис. 1.4. Американский радиолокационный разведывательный спутник Lacrosse во время сборки

Рис. 1.5. Модель немецкого разведывательного спутника SAR-Lupe внутри ракеты «Космос-3М»

Информация об американских программах доступна в основном до 1972 года, о более поздних программах просочилась лишь небольшая информация. Несколько изображений, полученных с современных ИСЗ, было рассекречено по случайности или из-за утечки, например как в случае с КН-11, фотографии с которого были посланы в Jane's Defence Weekly в 1985 году.

В российском документальном фильме «Секретный космос» в 2012 году сообщалось, что на высокой орбите находится около 2 тысяч отработанных разведывательных ИСЗ только советского производства.

Все разведывательные ИСЗ космического эшелона можно разделить на три группы: спутники видовой фотографической разведки, оптико-электронные и радиолокационные.

Разведывательные спутники заняли одно из главных мест в космических программах СССР и США. Если после запуска первого спутника С.П. Королев основное внимание сконцентрировал на лунной программе, то усилия американцев были направлены на осуществление военно-разведывательной программы «Дискавери».

План запуска спутников, разработанный в 1956 г., предусматривал как выполнение разведывательных функций (наблюдение из космоса за объектами возможного противника), так и обнаружение запусков баллистических ракет. В период холодной войны военно-космическая программа США была нацелена на сбор разведывательной информации о Советском Союзе.

В 1954 г. США разработали программу «Перспективные разведывательные системы» [3–4], в рамках которой реализовывались два проекта разведывательных искусственных спутников Земли (ИСЗ): «Самос», находившийся в ведении ВВС США, и «Корона», решавший задачи ЦРУ.

Спутники «Дискаверер» предназначались для отработки методов военной космической фоторазведки (спутники-шпионы). На них также проводились предварительные исследования возможности полета животных и человека в космическом пространстве. Запуск первого ИСЗ «Дискаверер-1» был произведен 28 февраля 1959 г., положив начало серии запусков (38 спутников), которая была осуществлена в довольно короткие сроки – 3 года. Последний «Дискаверер-38» был запущен 27 февраля 1961 г. Эти ИСЗ, снабженные специальной системой ориентации и устройствами для возвращения на Землю, запускались на полярные орбиты. Команда на спуск, по которой происходило отделение спускаемой капсулы и включение тормозной двигательной установки, давалась с пункта наблюдения на Гавайских островах. Возвращение капсул на Землю долгое время американцам не удавалось. Улавливанием и поиском капсулы занимались авиационные и военно-морские силы США. Программа возвращения экспонированной пленки со спутников на Землю реализовывалась в условиях наивысшей секретности. Первое успешное возвращение отснятой пленки было выполнено со спутника «Дискаверер-14», выведенного на орбиту 18 августа 1960 г. После того как возвращаемая капсула была выпущена со спутника на 17-м витке его полета, транспортный самолет С-130 при помощи специального трала с третьего захода поймал ее в воздухе. Поскольку возвращался не весь спутник, а только небольшая капсула (около 50 кг), она приземлялась не сама, а с помощью вертолета, подхватывавшего ее во время спуска на парашюте.

Из 38 запусков (1959–1961 гг.) около 13 были неудачными. Часть капсул подхватить вертолетами не удалось. После ИСЗ «Дискаверер-38» вся информация о спутниках, запускаемых на орбиту командованием ВВС США, была засекречена. Вновь она стала открытой лишь в 1990-х гг. ИСЗ получил название «Корона».

Два других проекта США «Самос» и «Мидас» были проектами военными.

По проекту «Мидас» (первый запуск 24 мая 1960 г.) отрабатывалась возможность использования спутников для раннего обнаружения запуска межконтинентальных ракет. Работоспособность системы была подтверждена в октябре 1961 г., когда был зарегистрирован запуск баллистической ракеты «Титан» с мыса Канаверал. В связи с отработкой системы сообщение о запуске пришло только через 90 сек. Удачным в проекте «Мидас» был запуск в 1963 г. спутника-разведчика «Меркурий» весом до 1100 кг, предназначенного для фотографирования земной поверхности с высоты 160–200 км и исследования жизнедеятельности человека в условиях космического полета.

Национальное разведывательное управление, Агентство национальной безопасности и Научно-исследовательская лаборатория ВМС США недавно рассекретили информацию о запуске в период 1962–1971 гг. ряда спутников типа POPPY для радарного наблюдения за кораблями советского военно-морского флота. POPPY были преемниками спутников GRAB (первый запуск 22.06.1960), запускавшихся в 1960–1962 гг.

В октябре 2002 г. США рассекретили документы, касающиеся полетов в 1960–1980-х гг. разведывательных спутников типа КН-7 и КН-9 (CORONA) [48]. Программа КН («Ки-Хоул» – от англ. «замочная скважина») имела ряд модификаций

спутников КН-7, -8, -9, -12 и т.д. Они использовались для целей ЦРУ до середины 1990-х гг. ИСЗ КН-11А приписывается способность различать объекты поперечным размером менее 10 см.

Существенный недостаток этих космических систем был связан со способом передачи информации на Землю. Во-первых, большой промежуток времени от съемки до доставки фотоинформации на Землю. Кроме того, после отделения капсулы с пленкой от спутника оставшееся на ИСЗ дорогостоящее оборудование становилось бесполезным. Эти проблемы были частично решены оснащением спутников (начиная с КН-4В) несколькими капсулами с пленкой.

Кардинальным решением первой проблемы стала разработка системы электронной передачи данных в режиме реального времени. С 1976 г. до завершения программы в начале 1990-х гг. США запустили восемь спутников серии КН-11 с электронной системой передачи данных.

11 февраля 1965 г. в США был запущен спутник LES-1 из серии военных спутников связи, которые предназначались для оценки мер по снижению уязвимости спутников военного применения к средствам военно-космической обороны (в СССР в те годы проходили испытания системы уничтожения спутников). К числу мер предохранения спутников относились: замена солнечных элементов радиоизотопными энергетическими установками, применение системы ориентации на базе двухстепенного гироскопа, использование линии связи «спутник – спутник» для того, чтобы при осуществлении дальней связи обходиться без промежуточных наземных станций-ретрансляторов.

Активная эксплуатация спутниковых средств разведки позволила использовать в программе CORONA [4] ИСЗ второго поколения – «Феррет», «Джампсит», ИСЗ-ретрансляторы SDS, «Спук Берд» («Каньон»).

Спутники «Каньон», которые начали эксплуатироваться в 1968 г. на орбитах, близких к геостационарной, были нацелены на прослушивание советских систем связи. В конце 1970-х гг. они были заменены ИСЗ «Чейлет» и «Вортекс».

Спутники «Райолит» и «Аквакейд» (на геостационарной орбите, 1970-е гг.) предназначались для отслеживания данных телеметрии советских баллистических ракет. В 1980-е гг. они были заменены ИСЗ «Магнум» и «Орион», запускавшимися с многоразового транспортного космического корабля.

Читатель должен понимать, что здесь представлена далеко не полная картина событий, поскольку сведения о разведывательной космической технике как СССР (России), так и США имеют гриф «совершенно секретно», а все данные, приводимые в открытой печати, носят ориентировочно-рекламный (а порой и явно дезинформационный) характер.

Американцев интересовало наличие баллистических ракет в СССР и их количество, расположение космодромов на севере и в Казахстане, расположение объектов ядерной энергетики, подводных лодок с межбаллистическими ракетами и мест их базирования и многое другое, относящееся к стратегически важным объектам.

Почти все объекты, выводимые в космос, имели двойное назначение: научно-исследовательское, прикладное и военное. Примером тому могут служить серия американских спутников DMS, советские ИСЗ «Космос», запускавшиеся как простые спутники и как орбитальные станции.

Спутники серии DMS в первую очередь предназначались для нужд военных ведомств, т.к. обеспечивали информацией специальные стратегические программы, командные системы, системы управления в различных регионах земного шара. Они позволяли получать снимки с высоким разрешением (в видимом и инфракрасном диапазоне) в реальном масштабе времени, являясь на тот момент единственным источником подобных данных для береговых и корабельных метеостанций ВМС США. От метеорологической аппаратуры поступали данные о температуре, влажности и плотности атмосферы в подспутниковом вертикальном профиле. Метеоинформация могла приниматься с борта как в реальном режиме времени, так и в записи. Спутники этой серии запускались с начала 1970-х гг. 2 февраля 1988 г. на орбиту был выведен ИСЗ усовершенствованной модели DMS-5D-2.

Спутниковые разведсистемы в СССР начали разрабатываться позже, чем в США.

Решение о разработке первого корабля-спутника для разведки и полета человека в космос в СССР было принято 22 мая 1959 г. (Постановление ЦК КПСС и СМ СССР № 569-264сс). Были созданы пилотируемый космический корабль (КК) «Восток» и фоторазведывательный КА «Зенит-2». 26 апреля 1962 г. со спутника «Космос-4» была проведена первая телевизионная съемка облачного покрова Земли. Это событие было революционным в деле прогнозирования погоды.

Космический аппарат «Зенит-2» стал первым отечественным разведывательным спутником. 10 марта 1964 г. «Зенит-2» был принят на вооружение ВС СССР. В отличие от американских спутников, на которых предусматривалось возвращение только пленки, на спутниках серии «Восток-Д» для возвращения на Землю использовалась более крупная капсула, содержавшая и камеры, и пленку. С 1962 г. до 1968 г. для фоторазведки использовались спутники семейства «Зенит-2, -4».

Следующей модификацией стал КА «Зенит-6» (1976 по 1980 гг.).

12 июля 1963 г. США запустили новый космический аппарат оптической разведки КН-7 Gambit с улучшенными характеристиками. В СССР был разработан аппарат новой серии «Янтарь», после принятия на вооружение получивший название «Феникс» (разработан Самарским ЦСКБ). Он стал прототипом серии спутников оптической разведки: спутника 1Ф622 «Янтарь-1» для обзорной фоторазведки и 1Ф623 «Янтарь-2» для детальной фоторазведки. Для ведения комплексной разведки из космоса одновременно велась разработка пилотируемого КА «Союз-Р». На смену ему пришел транспортный корабль 11Ф727К-ТК для снабжения станции «Алмаз». Параллельно активно прорабатывался военно-исследовательский корабль 11Ф73 «Звезда». Но ни один из этих проектов не был доведен до стадии ЛКИ.

Комплекс «Янтарь-2К» («Феникс») был принят на вооружение в мае 1978 г. По техническим характеристикам он не уступал американскому многокапсульному спутнику «Большая птица». С 1974 по 1983 гг. было произведено 30 пусков РН 11А511У «Союз-У» с КА «Янтарь-2К». Два раза отказывала РН. Дважды аппараты были подорваны на орбите из-за серьезных технических неисправностей.

В 1980 г. ПО «Арсенал» стало серийно производить космические аппараты типа «Кобальт» (модификация КА «Янтарь-2К») для наблюдения и детальной фотосъемки земной поверхности (разработка ЦСКБ «Прогресс», Самара). На смену ему пришли космические аппараты «Кобальт-М» с возвращаемой на Землю капсулой

с пленкой. Штатный срок активного существования этих аппаратов на орбите составлял 60–120 суток. 16 апреля 2010 г. с космодрома Плесецк произведен успешный запуск ракеты-носителя «Союз-У» с космическим аппаратом «Космос-2462» – спутником оптической разведки типа «Кобальт-М».

Пятое поколение советских спутников оптической разведки с электронной передачей данных в режиме реального времени отсчитывается от «Космоса-1426», стартовавшего 28 декабря 1982 г. В отличие от спутников четвертого поколения они сохраняют почти круговую орбиту и поддерживают высоту в узком диапазоне. Длительность полетов этих спутников – 6–8 месяцев. Штатный режим эксплуатации системы фоторазведки пятого поколения предусматривает функционирование одновременно двух спутников, находящихся на орбитах, отстоящих друг от друга на 910. Ввод в эксплуатацию долгоживущих спутников пятого поколения позволил сократить число обзорных полетов спутников третьего поколения, а в 1990 г. – полностью их прекратить. Последней новинкой в советской программе оптической разведки стал КА «Космос-2031», запущенный в июле 1989 г.

Еще *одно из направлений космической разведки – радиоэлектронное наблюдение.*

Начало работ по созданию космических средств радиоэлектронного наблюдения относится к августу 1960 г., когда была поставлена задача создания в интересах Минобороны СССР экспериментального космического аппарата ДС-К8 для отработки методов и средств определения параметров радиолокационных сигналов РЛС оборонного назначения. На первом этапе предусматривались разработка унифицированных КА ДС-У и запуск двух экспериментальных космических аппаратов ДС-К40, которые состоялись в 1965–1966 гг., но оказались неудачными из-за аварий ракеты-носителя. Вторым этапом стало создание КА радиотехнического наблюдения системы «Целина» с аппаратурой на микроэлементной базе (КБ «Южное», 1964 г.).

Своеобразный ответ американскому «Лакроссу» – спутник радиолокационной разведки «Алмаз-Т» (разработчик НПО ПМ) с разрешением 10–15 м, был запущен в СССР в 1981 г.

Отдельного внимания заслуживает *система морской космической разведки и целеуказания (МКРЦ)* «Легенда».

Разработка первой в мире космической системы обзора акватории Мирового океана комплексом разведывательных КА различных типов в интересах применения ударного противокорабельного оружия кораблями и подводными лодками ВМФ СССР стартовала в начале 1960-х гг. Система МКРЦ использовала аппараты двух типов: радиолокационной УС-А (управляемый спутник активный) и радиотехнической разведки УС-П (управляемый спутник пассивный) (рис.1.6). Головным разработчиком системы МКРЦ было КБ-1 (ЦНИИ «Комета», Москва). КА УС-А и УС-П разработаны ОКБ-52 («НПО машиностроения», г. Реутов). В те же годы проводились работы по созданию системы контроля радиотехнической обстановки «Целина», осуществлявшей регистрацию излучений в широком диапазоне частот. Но отсутствие решения о едином заказчике космических средств в Минобороны не позволило это сделать в 1960 г.

Для питания комплекса потребовалось использование ядерной энергетической установки (ЯЭУ) «Бук» с электрической мощностью 3 кВт. В период отработки бортового спецкомплекса несколько КА было запущено с химическими источниками.

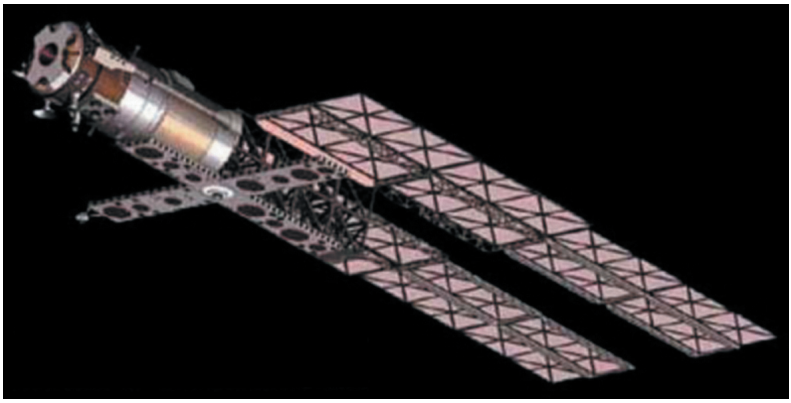

Рис. 1.6. Спутник радиотехнической разведки УС-П

Первый пуск состоялся в 1965 г. После успешных летных испытаний система активной радиолокационной морской разведки и целеуказания с КА УС-А была принята в эксплуатацию в 1975 г., КА радиотехнической разведки УС-П – в 1978 г.

Из-за запрета использования КА с ЯЭУ на низких орбитах (высота орбит 250–290 км) производство УС-А было прекращено. Всего было осуществлено 37 запусков КА УС, два из которых закончились аварией РН. В 1975–1976 гг. и 1981–1982 гг. производилось по 3–4 пуска. Первые аппараты выводились на орбиту при помощи РН серии «Союз», а после принятия на вооружение – РН «Циклон-2». 25.04.1973 г. из-за аварии РН «Циклон-2» спутник УС-А упал на территорию Канады. Корпус реактора выдержал удар, радиоактивного заражения не произошло, но, тем не менее, Советскому Союзу пришлось выплатить Канаде около 3 млн долл.

КА УС-П осуществлял поиск и идентификацию надводных целей без радиолокационного облучения, только регистрируя спектры их электронных излучений, характерные для каждого типа корабля. На КА УС-П применялись солнечные энергетические установки и буферные аккумуляторные батареи. За период с 1974 по 1991 гг. было запущено 37 КА этого типа. Пуски КА УС-П (и УС-А) проводились только с космодрома Байконур. Штатная группировка КА УС-П должна была включать три аппарата. Их орбиты фазировались так, чтобы все спутники двигались вдоль одной и той же трассы со сдвигом в 1 сутки друг от друга.

По завершении активного существования КА выполняли маневр увода с рабочей орбиты. На аппаратах 1975–1987 гг. увод осуществлялся небольшим разгонным импульсом. Спутники оставались на орбите до нескольких лет и разрушались из-за взрывов остатков топлива в двигательной системе или гермоконтейнеров с буферными химическими батареями (рис. 1.6).

1.1.6.3. Роль военно-технической разведки в современных локальных конфликтах

В завершение этого раздела для конкретного примера использования военно-разведывательных спутников в качестве средств поддержки космического эшелона СПРО следует отметить *роль военно-космической разведки США в современных локальных конфликтах.*

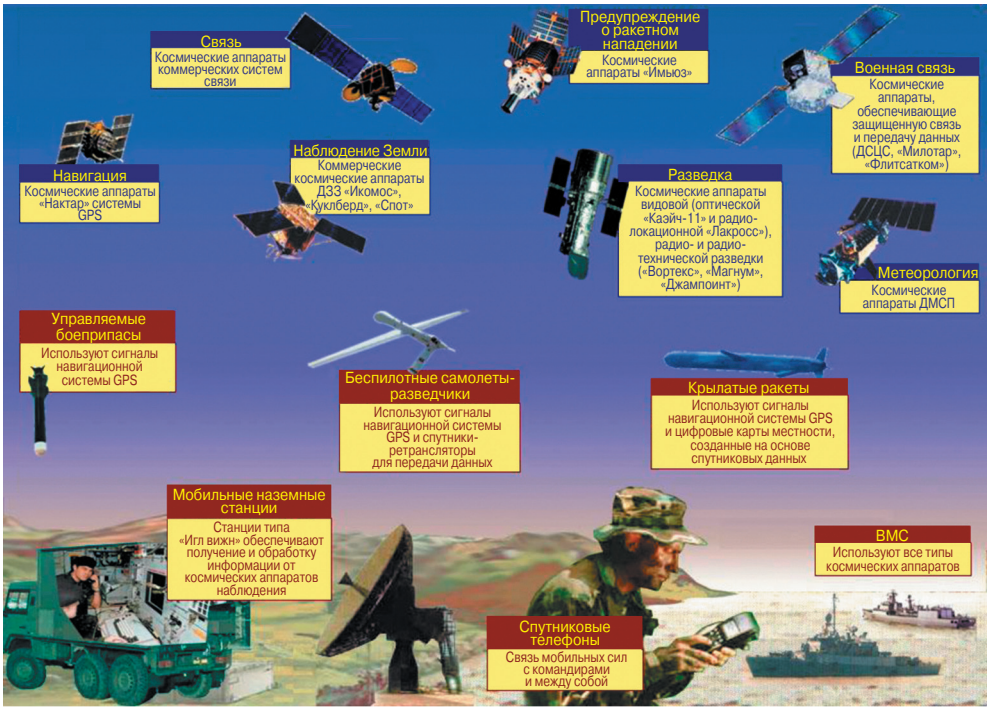

Рис. 1.7. Основные направления использования данных от космических средств [2]

Актуальность данной темы заключается в том, что с принятием Пентагоном концепции сетецентрических войн (Network Warfare) значительно возросла роль космической разведки при организации и ведении современного «наземного» боя. Современные космические разведывательные аппараты космического эшелона способны выявить активность противника на этапе глубокой подготовки к боевым действиям, а быстродействие современных систем обработки и передачи данных позволяет в кратчайшие сроки выявить цель, опознать и создать условия для ее уничтожения.

Наиболее впечатляющей по масштабам использования данных от космических средств стала война в Ираке 2003 года. На рис. 1.7 представлены основные направления использования космических аппаратов в войне с Ираком.

Для американской армии эта война стала своеобразным полигоном для испытаний новых образцов вооружения. В полной мере это утверждение относится и к средствам космического эшелона. Использовались не только военные, но и коммерческие спутники наблюдения, связи, навигационные и метеорологические аппараты, а также спутники предупреждения о ракетном нападении. Задействованная в ходе войны орбитальная группировка содержала, по данным открытых источников, 50–59 военных космических аппаратов различного целевого назначения, 28 аппаратов системы GPS и большое число коммерческих КА связи и дистанционного зондирования Земли [2].

В подготовительный период операции космическая группировка США не наращивалась, скрытое обеспечение боевых действий проводилось существующим со-

ставом находящихся на орбитах космических аппаратов, что говорит о достижении Соединенными Штатами такого положения в космосе, когда заблаговременно развернутая и функционирующая в мирное время орбитальная группировка способна гарантированно обеспечить проведение боевых операций подобного масштаба в любое время и в любом месте земного шара.

Очевидно, что информационная поддержка из космоса действий вооруженных сил в XXII в. будет оставаться одной из ключевых задач, решение которой должны обеспечивать военно-космические средства, включая доведение «космической» информации до самых низших звеньев боевого управления, а в перспективе – до отдельного солдата. По своим последствиям такую «информационную войну» можно сравнить только с созданием в середине XX в. ядерного оружия. В одном из следующих разделов мы более подробно рассмотрим проблемы такого нового вида оружия, как информационно-техническое оружие.

Практика жизни и деятельности современных вооруженных сил в различных условиях оперативно-стратегической обстановки убедительно показывает, что в настоящее время без средств космического эшелона нормальное функционирование вооруженных сил любой страны даже в мирное время *крайне затруднительно*, а при ведении боевых действий *практически невозможно*.

Другим путем использования в войсках информации от космических разведывательных средств является создание специальных подразделений космической поддержки. В российской армии имеется положительный опыт использования «групп космической поддержки» в оперативно-тактическом и тактическом звеньях, что подтвердили известные события в Сирии. Основными задачами указанных групп являются оценка состояния и работоспособности КА и подготовка предложений по их использованию для получения оперативных данных, а также предоставление полученной информации (разведывательной, метеорологической, навигационной и связной) различным звеньям боевого управления. Группы космической поддержки – одно из наиболее перспективных направлений ликвидации «разрыва» между потенциальными возможностями средств космического эшелона и их практическим использованием в войсках РФ.

Однако все эти перспективы должны учитывать опасности и угрозы, обусловленные стремительным развитием нового типа оружия XXII века – информационно-технического, основой которого являются аппаратные трояны – предмет исследований этой книги.

1.2. СВЧ-оружие наземного применения

1.2.1. Основные поражающие факторы и методы воздействия СВЧ-излучений на системы управления радиоэлектронных устройств

Известно, что импульсы СВЧ-излучения большой мощности способны выводить из строя элементы любой радиоэлектронной аппаратуры (РЭА), в первую очередь полупроводниковые элементы [2, 6]. Деградационные эффекты элементов РЭА могут быть обратимыми и необратимыми. В дальнейшем под термином «пора-

жение» элемента будем понимать его необратимый отказ. К сожалению, богатый инженерный опыт защиты РЭА от электромагнитного импульса (ЭМИ) ядерного взрыва практически не пригоден для защиты от СВЧ-излучения, поскольку характер воздействия импульсов СВЧ-излучения существенно отличается от характера воздействия электромагнитного импульса ядерного взрыва. ЭМИ не имеет высокочастотного заполнения (т.е. это видеоимпульс), и его спектр в основном сосредоточен в области относительно низких частот 1–100 МГц, СВЧ-импульсы генерируются на определенной несущей частоте, а их спектр лежит в пределах от единиц до сотен гигагерц. Низкочастотный характер ЭМИ создает серьезные проблемы для его направленной канализации в пространстве на объект поражения, а для СВЧ-излучения такая канализация легко реализуется с помощью специальных антенных систем (рупорных, зеркальных, фазированных антенных решеток), что существенно повышает уровень СВЧ-мощности, действующей на РЭА. ЭМИ проникает непосредственно через стенки корпуса радиоэлектронной аппаратуры, в то время как СВЧ-излучение может проникать в РЭА через отверстия, стыки и неоднородности корпусов, а также через открытые разъемы отрывных кабельных линий. Поэтому оценка деградационного воздействия СВЧ-излучения на объекты, содержащие элементы и устройства вычислительной техники и системы управления, а также поиск средств и методов защиты являются важной и актуальной задачей.

Уровни энергии, достаточные для поражения (необратимой деградации) СВЧ-излучением полупроводниковых элементов (диодов, транзисторов, микросхем) РЭА достаточно хорошо известны. В табл. 1.3 представлены известные экспериментальные данные о величине энергии, достаточной для поражения некоторых полупроводниковых элементов в зависимости от длительности СВЧ-импульса [7–9].

Например, энергия поражения p-i-n-диодов, используемых в ограничителях и антенных коммутаторах радиоэлектронных средств (РЭС), лежит в пределах $5 \cdot 10^{-5}$–10^{-4} Дж при длительности импульса десятки наносекунд [9]. В ряде случаев выход из строя приемного модуля РЭС определяется отказом малошумящего усилителя, который в современной аппаратуре СВЧ-диапазона проектируется на основе полевого транзистора с затвором Шотки (ПТШ GaAs) [9]. Его энергия поражения приведена в табл. 1.3.

Таблица 1.3. Энергия поражения полупроводниковых приборов [Дж] при различных длительностях СВЧ-импульса [нс]

Полупроводниковые приборы	Длительность СВЧ-импульса, нс		
	0,1 нс	10 нс	100 нс
Диоды: смесители кремниевые	2×10^{-6}–2×10^{-4} 1×10^{-3}–0,01	2×10^{-5}–2×10^{-3} 0,01–0,1	6×10^{-5}–6×10^{-3} $3{,}2 \times 10^{-2}$–3,2
Транзисторы средней мощности	5×10^{-5}–0,01	5×10^{-4}–0,1	2×10^{-4}–3×10^{-1}
ЦИМС: ТТЛ МОП	3×10^{-5}–6×10^{-4} 2×10^{-4}–5×10^{-3}	3×10^{-4}–6×10^{-3} 2×10^{-3}–5×10^{-2}	1×10^{-3}–2×10^{-2} 6×10^{-3}–0,14
АИМС	3×10^{-4}–6×10^{-3}	3×10^{-3}–6×10^{-2}	1×10^{-2}–0,19

Наиболее чувствительными, а значит, и наиболее уязвимыми элементами РЭС являются детекторные головки средств доставки ядерных боеприпасов, в которых чаще всего используются смесительные диоды Д603 (в коаксиальных устройствах) и Д608 (в волноводных устройствах). Экспериментально полученные пороги перегорания смесительных диодов детекторных головок РЭС лежат в интервале 10^{-5}–10^{-3} Дж при длительности СВЧ-импульса десятки наносекунд [7, 9]. Известно, что уровень энергии поражения в рабочем режиме ниже в 5–10 раз, а при воздействии импульсной последовательности уменьшается в 10–100 раз [7–13]. В табл. 1.4 представлены значения напряженности СВЧ-поля, при которых обычно наступает деградация микросхем различных типов [8, 9].

Таблица 1.4. Уровни деградации интегральных микросхем

Степень деградации	Характер деградации	Тип ИМС	*ЕП*, кВ/см	
			Пассив.	Актив.
I	Сбои функционирования	ТТЛ	8	0,3
		МОП		0,6
		Бип АИС		0,3–1,4
II	Устойчивые изменения параметров	ТТЛ	0,8–1,5	1,8
		МОП	0,5	0,1
		Бип АИС	1,2–15	4,0
III	Катастрофические необратимые отказы	ТТЛ	4	1,4–1,8
		МОП	2,5–15	0,1–4
		Бип АИС	1,4–5,5	1,0–6

Как известно, источником мощного СВЧ-излучения могут являться мощные радиолокационные станции, а также СВЧ-установки специального и военного назначения, некоторые из них будут более детально рассмотрены ниже.

1.2.2. СВЧ-оружие боевого применения

В настоящее время широко обсуждается и используется термин «СВЧ-оружие» (в зарубежной печати также используется термин «микроволновое оружие») [6, 11–14]. Основным поражающим фактором СВЧ-оружия является импульсное электромагнитное излучение с длиной волны от 0,1 до 10 см. Как было указано выше, испытания такого оружия и его элементов проводились США при проведении военных операций в Ираке [13, 14], однако *официально* такого оружия нет (пока) на вооружении ни у одного государства.

СВЧ-оружие эксперты разделяют на два вида: первый – СВЧ-установки, второй – СВЧ-боеприпасы. В свою очередь, СВЧ-боеприпасы могут подразделяться на *обычные* и *ядерные*. В *обычных* СВЧ-боеприпасах источником энергии является взрывомагнитный генератор на основе обычного взрывчатого вещества, а в *ядерном* – на основе ядерного заряда. Нагрузкой взрывомагнитного генератора является специальная генерирующая система, которая преобразует электрический импульс со взрывомагнитного генератора в импульс электромагнитного излучения СВЧ-диапазона [6]. В таких СВЧ-установках в качестве источника энергии могут использоваться *емкостные накопители и взрывомагнитные генераторы* с обычным

взрывчатым веществом, а в качестве источника СВЧ-излучения – *генераторы на основе сверхмощных СВЧ-приборов* [9]. В табл. 1.5 приведены основные ожидаемые параметры СВЧ-оружия, взятые на основе анализа источников [6–13].

Таблица 1.5. Ожидаемые параметры СВЧ-оружия

Параметры СВЧ-оружия	СВЧ-установки	СВЧ-боеприпасы
Мощность в импульсе, ГВт	10–100	1–10
Длина волны излучения, см	0,1–10	
Длительность импульса, нс	5–100	
Длительность фронта импульса, нс	0,1–1	
КНД антенны	10^3–10^7	10^2–10^3
Частота следования импульсов, Гц	0–400	–

Как уже было отмечено выше, в зависимости от назначения СВЧ-оружие может быть космического (воздушного) и наземного (морского) базирования, что обусловливает достаточно широкий спектр его применения. На рис. 1.8 изображены несколько *типовых боевых ситуаций*, которые можно разбить на два класса. Первый класс – характерный для СВЧ-установок, второй – для СВЧ-боеприпасов. Отличительной особенностью ситуаций первого класса является то, что главный максимум диаграммы направленности антенны СВЧ-установки может быть точно направлен на цель, например, с помощью РЛС обнаружения и наведения. Для ситуаций второго класса, т.е. для СВЧ-боеприпасов, особенность заключается в том, что в момент его задействования возможно значительное отклонение главного максимума диаграммы направленности антенны СВЧ-боеприпаса от точки цели, но при этом цель попадает в угол раствора диаграммы направленности СВЧ-боеприпаса.

Пути проникновения СВЧ-излучения в радиоэлектронную аппаратуру достаточно хорошо известны [7–13], однако *механизмы* проникновения недостаточно исследованы. Однозначно установлено, что СВЧ-излучение может проникать в РЭА через антенно-фидерные устройства (АФУ), щели, отверстия и стыки в корпусах аппаратуры, через открытые разъемы, а также может непосредственно воздействовать через радиопрозрачные (пластиковые) элементы конструкции, например на заряды твердого топлива.

Воздействие СВЧ-излучения на РЭС цели *через антенно-фидерное устройство* можно оценить по его параметрам [6]. Проникновение СВЧ-излучения в отверстия, щели и стыки корпуса – явление значительно более сложное для анализа. Известны отдельные результаты экспериментальных исследований эффектов проникновения СВЧ-излучения через отверстия, которые показали, что максимум проникающей способности СВЧ-излучения наблюдается при соблюдении резонансных условий, т.е. в том случае, когда размеры отверстий кратны длине волны излучения. Проникающая способность резко уменьшается на волнах длиннее резонансной волны отверстия, но наблюдаются небольшие случайные пики на резонансных длинах волн отдельных проводников, находящихся внутри корпуса. На волнах короче резонансной длины волны отверстия наблюдается более медленный спад проникающей способности, но возникают острые резонансы благодаря множеству типов колебаний в объеме корпуса аппаратуры [6, 8].

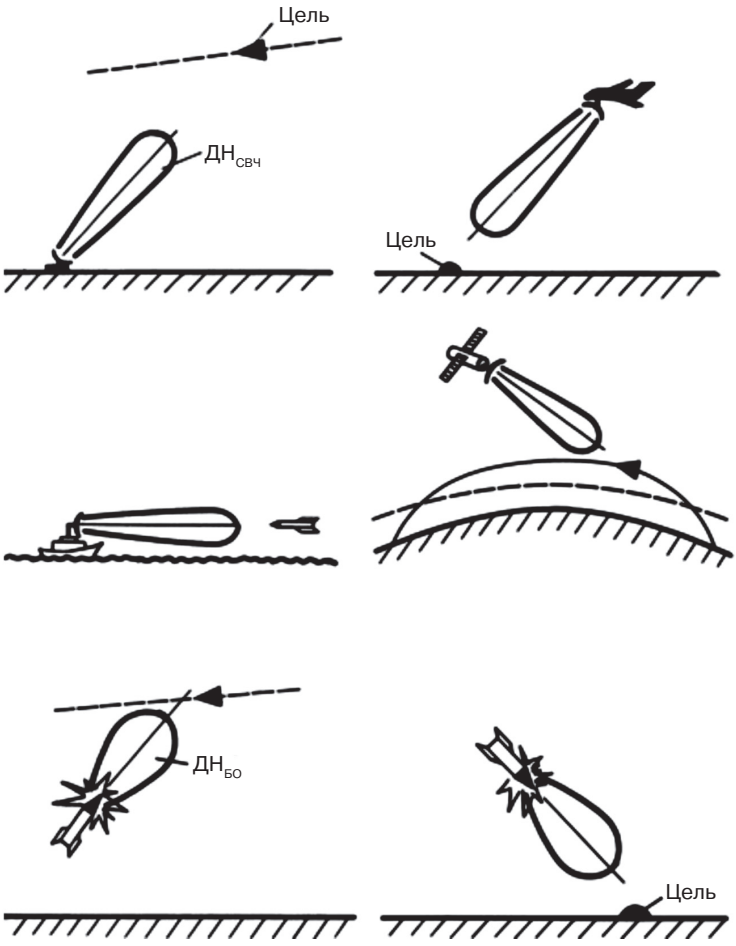

Рис. 1.8. Типовые варианты боевого применения СВЧ-оружия

Проникновение СВЧ-излучения *через разъемы и кабельные соединения* существенно зависит от их конструктивных особенностей. Открытые штепсельные разъемы имеют существенные отличия от отверстий (наличие штырей, кабеля и т.д.). Литературных сведений об анализе прохождения СВЧ-излучения через разъемы крайне мало. Воздействие СВЧ-излучения через открытые штепсельные разъемы отрывных кабельных соединений объектов авиационно-космической техники может привести к выходу из строя бортовой РЭА и других внутренних элементов, например элементов пироавтоматики. Однако в большинстве образцов авиационно-космической техники элементы бортовой РЭА не подвергаются непосредственному воздействию СВЧ-излучения, так как находятся в составе экранированных узлов. В этом случае поражение элементов происходит под действием вторичных напряжений и токов, индуцированных в штырях открытых штепсельных разъемов и неэкранированных кабелях, которые электрически соединены с элементами РЭА. Теоретические оценки ослабления СВЧ-излучения при проникновении через открытые штепсельные разъемы весьма затруднены вследствие большого числа влияющих факторов. В то же

время необходимость и актуальность подобных теоретических и экспериментальных исследований не вызывают сомнений. Это обусловлено наличием открытых штепсельных разъемов в современных образцах авиационно-космической техники. Известны результаты экспериментальных исследований и некоторого теоретического описания проникновения СВЧ-излучения с длиной волны 3,2 см через некоторые штепсельные разъемы, используемые в авиационно-космической технике [10].

Таким образом, на основе анализа типовых образцов авиационно-космической техники можно заключить, что для таких объектов основными путями проникновения СВЧ-излучения являются:

1) антенно-фидерные устройства бортовых радиоэлектронных средств;
2) открытые штепсельные разъемы бортовой РЭА и отрывных кабельных соединений;
3) радиопрозрачные элементы конструкции корпусов как самих объектов, так и аппаратуры.

За основу методического аппарата для оценки уровня гарантоспособности вычислительных систем и систем управления авиационно-космической техники в условиях воздействия СВЧ-излучения (СВЧ-оружия) можно взять разработанную интегральную вероятностную модель, которая состоит из четырех взаимосвязанных вероятностных моделей. *Первая* – вероятностная модель ослабления излучения СВЧ-оружия при распространении в атмосфере, которая учитывает случайный характер погодных условий и параметров атмосферы. Эта модель позволяет получить закон распределения коэффициента ослабления и использовать его в вероятностных моделях для определения величин нагрузок. Под нагрузкой понимается параметр, характеризующий поражающее действие СВЧ-оружия на критический(ие) элемент(ы) РЭА и другие функциональные узлы вооружения и военной техники.

Вторая модель – вероятностная модель воздействия СВЧ-излучения через АФУ РЭС цели, которая учитывает частотную избирательность элементов АФУ при внеполосовом воздействии СВЧ-оружия. При разработке модели авторами [6] был принят антенный механизм взаимодействия и использована теория радиоприема. В этом случае СВЧ-источник рассматривается как передатчик, а цель – как приемник СВЧ-излучения. Авторами [6] было получено выражение для расчета величины нагрузки, действующей на критический элемент. Методом статистического моделирования определялся закон распределения нагрузки, который использовался для расчета показателя эффективности поражающего действия СВЧ-излучения.

Третья модель – это вероятностная модель воздействия СВЧ-излучения через открытые штепсельные разъемы объектов вооружения и военной техники, она позволяет определить законы распределения нагрузок при воздействии через разъем. При этом используются полученные эмпирические зависимости для расчета коэффициента ослабления разъема и экспериментально полученная поправка для расчета диаграмм направленности штырей разъема [14]. Для определения закона распределения нагрузок используется метод статистического моделирования.

В результате корреляционного анализа были выделены значимые параметры, которые использовались в вышеуказанных моделях как случайные величины.

В качестве *четвертой* модели обычно используется адаптированная вероятностная модель «нагрузка – стойкость» [15]. Она позволяет рассчитать величину

показателя эффективности поражающего действия СВЧ-излучения. В качестве показателя эффективности поражающего действия принята вероятность функционального поражения цели, которая характеризует уровень гарантоспособности цели, в частности ее радиоэлектронной аппаратуры.

На основе *общей вероятностной модели* ведущими экспертами была разработана методика построения зоны функционального поражения цели, которая учитывает направленные свойства СВЧ-источника и другие его особенности. Под зоной поражения понимается область пространства, в которой цель поражается с вероятностью не ниже заданной. Основными параметрами СВЧ-оружия, определяющими размеры зоны поражения при его постоянных энергетических характеристиках, являются: для СВЧ-установок – ширина главного лепестка диаграммы направленности антенны и точность наведения ее на цель; для СВЧ-боеприпаса дополнительно к ним – отклонение точки подрыва от точки прицеливания. Также в качестве примера в работе [6] был рассчитан радиус поражения радиолокационной головки самонаведения противокорабельной крылатой ракеты «Томагавк» BGM-109 с помощью СВЧ-установки, размещенной на корабле. Радиус поражения с вероятностью 0,95 составляет от 4 до 4,5 км, следовательно, уровень гарантоспособности на данном расстоянии составляет 0,05.

Следует отметить, что разработанная в [6] вероятностная модель явилась теоретической основой создания методического аппарата:

- для обоснования рекомендаций по выбору основных параметров СВЧ-оружия и его применению для достижения заданной эффективности поражения цели;
- для оценки эффективности поражающего действия СВЧ-оружия на любые образцы авиационно-космической техники, содержащие РЭА;
- для оценки стойкости авиационно-космической техники и различных систем к действию СВЧ-излучения;
- для обоснования величины показателя стойкости к действию СВЧ-оружия и СВЧ-излучения;
- для обоснования требований к испытательной базе экспериментального исследования стойкости элементов и устройств образцов авиационно-космической техники и систем к действию СВЧ-излучения.

1.3. Оружие несмертельного (нелетального) действия наземного применения

Оружие несмертельного (нелетального) действия (ОНД) предназначено для временного выведения людей из строя. Как известно, ряд таких средств существует уже достаточно давно, к ним можно отнести резиновые пули или слезоточивый газ.

Однако борьба с преступностью, массовыми беспорядками и терроризмом, особенности проведения оперативных мероприятий спецподразделениями настоятельно требовали создания нового оружия, новых методов и средств, в том числе для применения несмертельных образцов такого оружия в различных миротворческих операциях, проводимых под эгидой ООН, а иногда и в серьезных боевых задачах. В настоящее время интенсивные работы по созданию ОНД ведутся в США, Германии, Франции, Китае и ряде других стран.

Практически все созданное сегодня несмертельное оружие основано на следующих основных принципах воздействия: механическом, акустическом, химическом, электрическом, электромагнитном или оптическом.

Работы по созданию такого оружия ведутся и в России. В частности специалисты одного из научно-исследовательских институтов Министерства обороны разработали электромагнитное оружие нелетального воздействия, в качестве главного поражающего фактора в котором применяется крайне высокочастотное (КВЧ) электромагнитное излучение.

1.3.1. СВЧ-оружие «система активного отбрасывания»

Направленный луч данной установки [16] вызывает у человека непереносимые болевые ощущения: сгенерированный установкой мощнейший луч начинает взаимодействовать с влагой, которая содержится в верхних слоях человеческой кожи, и проникает внутрь всего лишь на десятые доли миллиметра, воздействие на внутренние органы человека полностью исключено. При этом облученный данным лучом человек начинает испытывать серьезное жжение кожных покровов, что способно вызвать у него даже тепловой шок. Подверженный воздействию установки человек инстинктивно пытается укрыться от невидимого поражающего луча.

Стоит отметить, что еще раньше данная разработка была представлена в США и получила название *«система активного отбрасывания»* (ADS – Active Denial System), известна эта система и под другим названием – «луч боли». Впервые о существовании программы ADS широкая общественность узнала в 2011 году. Американская разработка нелетального оружия также направлена на разгон митингов. За счет использования высокочастотных электромагнитных лучей она может поражать цели на расстоянии до 1 километра.

Рис. 1.9. Система активного отбрасывания – Active Denial System

Данная установка размещается на базе специального грузовика или автомобиля «Хаммер» (рис 1.9). Используемые в системе активного отбрасывания высокочастотные электромагнитные колебания не наносят вреда человеку, при этом создавая у последнего ощущение нестерпимого жара, именно поэтому разработка и получила название «луч боли» или «тепловой луч». Данную разработку можно отнести к наиболее безопасным типам вооружения, использующимся на сегодняшний день. Она не вызывает у человека рака, не изменяет его гены, что могло бы плохо отразиться на его детях. Для обеспечения большей безопасности время работы системы активного отбрасывания может быть принудительно ограничено 3 секундами.

В отличие от резиновых пуль или тех же дубинок и слезоточивого газа, такой вид оружия безопасен даже для беременных женщин. Правда, по мнению некоторых скептиков, использование таких лучей на практике может грозить возникновением паники в толпе людей. В результате оружие может оставить после применения даже больше жертв, чем применение традиционной бомбы.

Система активного отбрасывания – Active Denial System является лишь одним из видов оружия, которые разрабатываются в рамках специальной американской программы «Оружие управляемых эффектов» [16]. Оружие представляет собой установку, которая излучает электромагнитные колебания в диапазоне миллиметровых волн с большой частотой – 94 ГГц, что оказывает на людей кратковременное шоковое воздействие. Принцип действия данного типа нелетального оружия заключается в том, что при попадании луча от устройства на человека не менее 80% его энергии поглощается верхним слоем кожи облученного, разогревая его до невыносимой температуры [16].

Эффект, производимый этим лучом, называют «незамедлительное и высокомотивированное поведение спасения». Журналисты назвали его «Goodbye effect» – англ. «эффект «до свидания». Пентагон провел сертификационные испытания установки ADS на добровольцах (военнослужащих и резервистах), которые при облучении испытывали болевой шок и рефлекторное стремление немедленно скрыться из зоны поражения. Около 10 тыс. проведенных испытаний показали, что болевой порог достигался в течение 3 секунд облучения, а после 5 секунд боль становилась невыносимой. Однако только в шести случаях испытуемые получали слабые ожоги в виде покраснений и вздутий кожи, а в одном случае – даже ожог второй степени.

Прошедший испытания экспериментальный комплекс ADS, получивший наименование System 1, оснащен антенной системой, способной формировать луч диаметром 2 метра, эффективная дальность действия которого составляет 500 метров (рис. 1.10). Возможна установка малогабаритного СВЧ-комплекса на шасси БТР Stryker, а также на воздушные и морские платформы. Более мощный комплекс ADS планируется установить на борту спецсамолета АС-130.

В ходе испытаний были опробованы различные тактические приемы использования СВЧ-установки ADS в боевых операциях для поддержки наступления, подавления огневых точек и срыва контратак. Однако основное ее предназначение – дистанционный разгон враждебно настроенной толпы и удаление гражданских лиц от контролируемых объектов. Остается открытым вопрос о средствах защиты от ADS.

Рис. 1.10. Комплекс ADS System 1

Рис. 1.11. Пример использования СВЧ-установки ADS

Излучение этой длины волны быстро поглощается водосодержащими материалами, и даже в полевых условиях можно изготовить относительно эффективные средства защиты.

Впервые существование программы ADS было открыто для прессы в 2001 году, но подробности оставались засекреченными. Первая боевая СВЧ-установка для дистанционного несмертельного воздействия на людей прошла сертификацию ВВС США для применения в Ираке. На разработку установки под наименованием Active Denial System (ADS) было затрачено 40 млн долл. США в течение последних 10 лет. По оценкам представителей ВВС, испытания показали, что установка ADS является эффективным оружием. Идея создания оружия возникла в середине 1990-х годов,

после того как американцы были вынуждены уйти из Сомали под напором восстания местного населения. Главная проблема сомалийской кампании заключалась в том, что помимо боевиков на американских солдат постоянно нападали толпы разгневанных, но вооруженных только палками и камнями туземцев. Стрелять по ним опасались: тогда Америка еще прислушивалась к мнению мирового сообщества и не желала испортить свой имидж «миротворца». Решили создать что-то несмертельное, но весьма болезненное. За основу взяли принцип СВЧ-печки, разогревающей завтраки электромагнитным полем высокой частоты. Вот только поле военной «печки», очень мощное и направленное, – в виде широкого луча, с эффективной дальностью действия около 1 километра. В военных целях свойства электромагнитного поля используются давно – для вывода из строя электронных приборов противника. Еще во время первых испытаний ядерного оружия был открыт эффект электромагнитного импульса (ЭМИ), доставивший столько проблем создателям военной техники и военных объектов. Кстати, интересно, что «топорная» советская электроника гораздо лучше выдерживала ЭМИ, чем «продвинутая» западная.

Затем военные научились создавать ЭМИ и без ядерного взрыва. Во время операции «Буря в пустыне» и натовских бомбардировок Югославии использовались электромагнитные боеголовки и бомбы. Их конструкция не так уж сложна: катушка индуктивности и взрывчатка. При взрыве частота и сила тока катушки резко возрастают и в радиусе действия боезаряда на доли секунды возникает мощное электромагнитное поле, уничтожающее приборы и оборудование противника. В 1980-х годах начали создавать также передвижные СВЧ-генераторы. Это установки с антенными излучателями направленного действия, предназначенные для точного поражения одиночных и групповых целей. Со временем удалось максимально уменьшить их размеры, первоначально достигавшие габаритов вагона: излучатель мощностью в один гигаватт теперь весит всего 20 кг, а аппарат мощностью в 20 гигаватт имеет вес около 180 кг. Планировалось применять их для уничтожения вражеских ракет, самолетов, наземной техники.

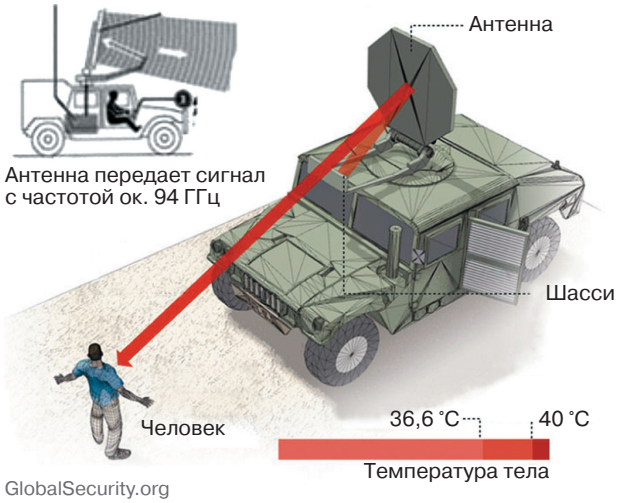

Рис. 1.12. Принцип воздействия ADS

В апреле 2001 года на авиабазе Киртленд (Нью-Мексико) провели испытания этого оружия. С расстояния в несколько сот метров пучок электромагнитных волн направили на грузовик, система зажигания которого тут же вышла из строя. Но вместе с электроникой страдали и люди, получая массу неприятных ощущений или теряя сознание. Как известно, электронный прибор, положенный в микроволновку, мягко говоря, выходит из строя. Уже в октябре 2001 года на все той же авиабазе Киртленд на нескольких добровольцах прошли испытания Active Denial System, предназначенной для «гуманной» борьбы с живыми людьми. Им пришлось довольно сильно пожалеть о своей храбрости: в клетках кожи под воздействием высокочастотного поля (96 ГГц) начинала вскипать вода, ткани нагревались до 45–50 градусов и возникала нестерпимая боль. Впрочем, как только человек выбегал из зоны действия установки, боль проходила и даже якобы не оставалось никаких повреждений.

Обрадованные создатели быстро отрапортовали об успехе, а Пентагон начал строить грандиозные планы. По ним ADS должен выполнять такую же задачу, как и акустическая пушка LRAD, – разгонять агрессивные акции протеста, защищать объекты от террористов и хулиганов, но более эффективно. Если LRAD только оглушил и отогнал пиратов, то на его месте ADS мог бы еще и вывести из строя их катера. Также, в принципе, он может на расстоянии остановить автомобиль с преступниками или обезвредить бомбу шахида. А главное – если акустическая установка бесполезна в столкновении с серьезным противником, то ADS может одинаково использоваться не только в «мирных», но и в боевых целях – для борьбы с техникой вражеской армии. Однако на пути внедрения ADS как «гуманного» оружия возникла серьезная проблема, ставящая эту самую «гуманность» под сомнение. Дело в том, что добровольцев тщательно готовили к испытаниям: с них сняли все металлические предметы, контактные линзы, защитили глаза специальными очками, их контролировали. А теперь представьте толпу ничего не подозревающих людей, которые просто растеряются и вряд ли сообразят, что нужно срочно покинуть опасную зону.

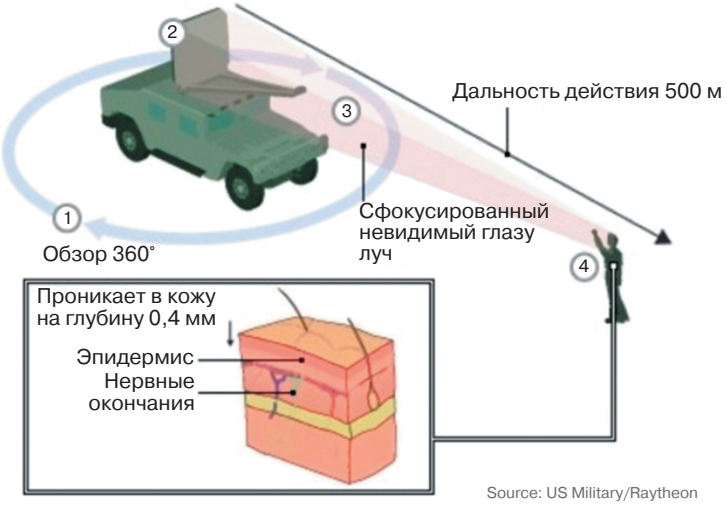

Рис. 1.13. Схематически показано воздействие на тело человека (глубина проникновения в кожный покров 0,4 мм) с расстояния 500 м

У многих – цепочки, браслеты, золотые коронки, у кого-то, возможно, кардиостимулятор. Кто-то может беспомощно метаться или упасть, и уже через пару минут его кожа получит серьезные ожоги, а глазам грозит потеря зрения.

Ряд американских и британских ученых высказались за более серьезные испытания ADS с целью выявить все негативные физические и психические последствия применения этого оружия, в том числе и те, которые могут проявиться спустя какое-то время. Но к их мнению не прислушались. Ведь в проект были вложены огромные деньги, которые в нашем мире перевешивают все принципы гуманизма.

Так, эксперименты с использованием этого оружия на добровольцах показали, что СВЧ-оружие нарушает работу головного мозга и центральной нервной системы: человек слышит несуществующие шум и свист.

1.3.2. Лазерное устройство PHASR для временного ослепления и дезориентации противника

Это устройство [16] также представляет собой лазерное оружие несмертельного действия, созданное Минобороны США. Оно используется для временного ослепления и дезориентации противника. Прототипом для винтовки PHASR стало близкое по принципу действия британское лазерное оружие Dazzler, которое использовалось для ослепления аргентинских летчиков во время короткой войны за Фолклендские острова. Разработанный американцами PHASR является лазером низкой интенсивности, поэтому его ослепляющий эффект носит лишь временный характер. При этом в случае необходимости длина волны может быть изменена.

В 1995 году лазерное оружие, которое причиняло бы вред зрению, было запрещено конвенцией ОНН, которая называлась «Протокол об ослепляющих лазерных вооружениях». После принятия данного протокола Пентагон официально свернул часть своих разработок, но винтовку PHASR ему удалось поставить на вооружение спецслужб.

Рис. 1.14. Система PHASR

Это решение было аргументировано коротким временем ее воздействия, а также тем, что Протокол не запрещает применения лазеров, не вызывающих необратимых ухудшений зрения. По мнению Минобороны США, данное оружие может быть незаменимым в тех ситуациях, когда противника необходимо временно ослепить.

«Вы не увидите его, вы не услышите его, вы не уловите его запах: вы почувствуете его», – рассказал, представляя ADS, полковник морской пехоты США Трейси Таффола, который курирует программу разработки оружия несмертельного действия. Он также пояснил, что установка, способная «бить» на расстояние до тысячи метров, является «самым безопасным несмертельным» оружием ВС США, которое разрабатывалось в течение 15 лет, но никогда не применялось в реальных условиях. Презентация нового оружия прошла на базе ВМС Quantico в штате Виргиния, передает РИА «Новости».

1.3.3. «Бесшумный страж» (Silent Guardian)

Компанией Raytheon еще в конце 2005 года создан образец микроволнового оружия Silent Guardian («Бесшумный страж») (рис. 1.15) для вооруженных сил США, вызывающий сильнейшие болевые ощущения у тех, кто окажется в зоне действия этого прибора. Raytheon предполагает продавать это устройство вооруженным силам США и их союзникам. Это оружие может быть использовано войсками США в крупных городах для разгона агрессивно настроенных толп. Его развернут также возле важных военных объектов, чтобы предотвратить проникновение на них боевых групп противника.

Принцип работы этого оружия массового воздействия довольно прост: Silent Guardian испускает пучки миллиметровых волн, которые, достигнув нарушителей спокойствия, проникают под кожу на глубину порядка 0,5 мм, вызывая тем самым невыносимое жжение, мгновенно распространяющееся по всему телу.

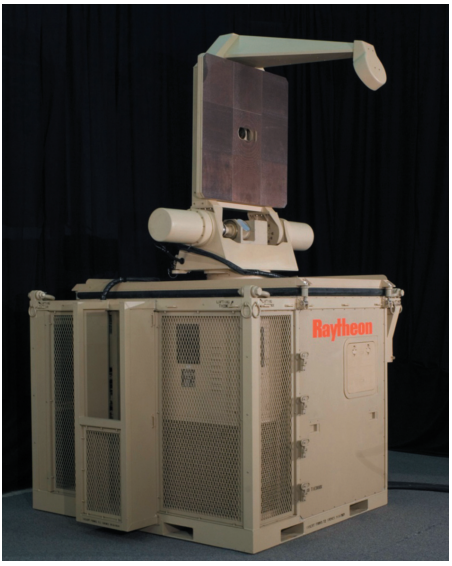

Рис. 1.15. «Бесшумный страж» компании Raytheon

Как отмечают журналисты Daily Mail, Silent Guardian оставляет ощущение соприкосновения с раскаленным проводом под напряжением. И хотя разработчики утверждают, что боль прекращается, едва человек покидает зону действия прибора, журналисты утверждают, что саднить продолжает еще несколько часов.

Мозг в этом случае повинуется инстинкту самосохранения и вынуждает хозяина бежать прочь либо падать навзничь. Что интересно, разработчик Silent Guardian, компания Raytheon, клянется, что никакого негативного воздействия на организм сие оружие не оказывает и чувство жжения есть не что иное, как естественная реакция нервных окончаний на миллиметровые волны. Так или иначе, а полномасштабный прототип в ходе испытаний обращал в бегство даже самых закаленных десантников.

По официальному заявлению создателей, «Silent Guardian уже доступен и готов к действию», так что остается лишь порекомендовать всем любителям массовых беспорядков начать вкладывать свою неуемную энергию во что-нибудь более полезное. Пока Raytheon предполагает, что в страны, где «плохо с правами человека», это устройство поставляться не будет.

Кстати, микроволновое оружие имеет и другую интересную особенность – может парализовать радиосвязь, забив эфир помехами, и повредить электронные приборы.

1.3.4. Наиболее известные системы нелетального оружия из арсенала Министерства обороны США

1.3.4.1. «Глушитель речи»

Данное весьма своеобразное устройство было создано учеными из Японии *под названием The SpeechJammer*, в переводе на русский язык его можно назвать «глушителем речи». Если направить данный прибор в сторону постоянно говорящего человека и запустить его, то уже через несколько минут оратор начнет путать слова в своем выступлении и вскоре замолкнет. Данное устройство не совсем оружие, но, возможно, при должном развитии сможет использоваться во время стихийных или несанкционированных митингов в целях прекращения речи кого-либо из наиболее активных ораторов.

Рис. 1.16. The SpeechJammer

Стоит отметить, что данная установка уже смогла получить Шнобелевскую премию 2012 года. Данная премия ежегодно вручается в США за наиболее сомнительные достижения в науке [16].

1.3.4.2. The Incapacitating Flashlight

Прибор с данным названием был создан калифорнийской компанией Intelligent Optical Systems. Больше всего он напоминает обычный фонарик, с помощью мощных светодиодов которого генерируется серия световых импульсов различных цветов и продолжительности, очень болезненных для человеческого глаза. В результате воздействия такого «фонаря» живая мишень, оставаясь в полном здравии, временно теряет ориентацию в пространстве [16].

Рис. 1.17. The Incapacitating Flashlight

1.3.4.3. Суперзловонный артиллерийский снаряд

Данный артиллерийский снаряд *XM1063* является химическим оружием, действие которого основано на поражении вероятного противника *очень сильным зловонием*.

Рис. 1.18. Гаубица для XM1063