УДК 623.624

Описательная модель комплексов разведки, используемых для вскрытия системы воздушно-космической обороны и целеуказания при нанесении удара средствами воздушно-космического нападения

Афонин И. Е., Макаренко С. И., Петров С. В.

Актуальность. *США завершили разработку оперативно-стратегической концепции «быстрый глобальный удар». В целях обеспечения целеуказания средствам воздушно-космического нападения (СВКН) при нанесении «быстрого глобального удара» комплексы высокоточного оружия сопрягаются с средствами разведки. Для обоснования эффективных военно-технических решений по отражению «быстрого глобального удара» необходимо исследовать обобщенный информационный конфликт, возникающий между системой СВКН и системой воздушно-космической обороны (ВКО). Одним из частных информационных конфликтов в составе этого обобщенного конфликта «система СВКН – система ВКО» является конфликт между комплексами и средствами разведки и целеуказания в составе системы СВКН и разведываемыми объектами системы ВКО.* ***Целью работы*** *является формирование описательной модели комплексов и средств разведки, используемых для вскрытия элементов системы ВКО и целеуказания при нанесении «быстрого глобального удара». Данная описательная модель в дальнейшем планируется к использованию при формировании исходных данных, используемых при формализации следующих частных конфликтов: между средствами разведки в составе СВКН и источниками информации в системе ВКО; между средствами разведки в составе СВКН и средствами связи системы ВКО. Описательная модель комплексов разведки, используемых для вскрытия системы ВКО, основана на обобщении и анализе исключительно открытых источников и публикаций.* ***Результаты и их новизна.*** *Элементом новизны работы являются сформированные обобщённые тактико-технических характеристики типовых комплексов и средств разведки космического и воздушного базирования в составе системы СВКН, решающих задачи радио- и радиотехнической, оптико-электронной и радиолокационной разведки, а также описательная модель средств и способов компьютерной разведки.* ***Практическая значимость.*** *Представленная в работе описательная модель будет полезна техническим специалистам для обоснования новых технологических решений при разработке и обосновании особенностей эксплуатации источников информации и средств связи в системе воздушно-космической обороны. Кроме того, данная модель будет полезна научным работникам и соискателям, ведущим научные исследования в области исследования информационных конфликтов и в области устойчивости системы воздушно-космической обороны.*

Ключевые слова: *модель, описательная модель, быстрый глобальный удар, система воздушно-космической обороны, средства разведки, радио- и радиотехническая разведка, оптико-электронная разведка, компьютерная разведка.*

Введение

В течение 2009-2012 гг. вооруженные силы (ВС) США завершили разработку оперативно-стратегической концепции «Prompt Global Strike» – «Быст-

Библиографическая ссылка на статью:
Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель комплексов разведки, используемых для вскрытия системы воздушно-космической обороны и целеуказания при нанесении удара средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2021. № 1. С. 190-214. DOI: 10.24411/2410-9916-2021-10108.

Reference for citation:
Afonin I. E., Makarenko S. I., Petrov S. V. Descriptive model of intelligence systems used to detection the elements of an aerospace defense system and target designation when aerospace attack means are doing prompt global strike. *Systems of Control, Communication and Security*, 2021, no. 1, pp. 190-214 (in Russian). DOI: 10.24411/2410-9916-2021-10108.

рый глобальный удар» (БГУ) и активизировали деятельность, направленную на практическую реализацию ключевых положений этой концепции. Основные и частные положения этой концепции изложены в работах [1-8]. Основной целью концепции БГУ является придание ВС США способности высокоточного воздействия на объекты противника в кратчайшие сроки на большие дальности с использованием набора ударных средств в обычном или ядерном оснащении. Концепция БГУ предусматривает одновременный удар большого количества средств поражения высокоточного оружия (ВТО), прежде всего крылатыми ракетами (КР), по выбранным целям, административным и военным центрам, в том числе и по пусковым установкам межконтинентальных баллистических ракет (МБР) противника, с высокой интенсивностью пуска КР и МБР. В перспективе ВС США за счет развития ВТО и сопряжения его с глобальной системой разведки и целеуказания для нанесения БГУ планируют задействовать только КР и МБР в обычном оснащении для достижения текущих стратегических задач, а ядерные силы использовать только как оружие устрашения [1]. Задачи планирования, подготовки и проведения боевых операций в соответствии с концепцией БГУ возложены на Командование глобальных ударов и интеграции, созданное в структуре Объединенного стратегического командования ВС США.

При практической реализации концепции БГУ эксперты Пентагона рассматривают несколько возможных сценариев, при этом в отношении потенциального конфликта с Российской Федерацией (РФ) интерес представляет следующий основной сценарий – «Применение БГУ по упреждению ракетно-ядерного удара со стороны государства, обладающего арсеналом ядерного оружия». Данный сценарий был подробно разобран в работе [5]. Отметим что БГУ в своем составе будет содержать два основных эшелона. Первый эшелон – средства воздушно-космического нападения (СВКН), ориентированные на поражение элементов системы воздушно-космической обороны (ВКО) с целью снижения ее эффективности при отражении удара СВКН второго эшелона БГУ. Второй эшелон (основной) – СВКН, предназначенные для поражения объектов системы государственного и военного управления, объектов критической инфраструктуры государства, в том числе и пусковых установок МБР, в условиях уже подавленной системы ВКО.

Для обеспечения целеуказания СВКН при нанесении БГУ комплексы ВТО сопрягаются с средствами разведки. При этом средства разведки обеспечивают как первичное добывание сведений о местоположении объектов поражения в первом и втором эшелонах БГУ, так и уточнение данных и выявление новых объектов поражения уже в процессе нанесения БГУ.

Направлением исследований авторов является формирование моделей конфликта «СВКН – система ВКО» при отражении удара первого эшелона БГУ. Данный конфликт может быть декомпозирован на ряд частных конфликтов:

– «средства разведки в составе СВКН – источники информации в системе ВКО», формализующий процессы оценки разведзащищенности радиолокационных станций (РЛС) контроля воздушного пространства в составе радиотехнических войск (РТВ), РЛС системы контроля космиче-

ского пространства (СККП), РЛС системы предупреждения о ракетном нападении (СПРН), а также РЛС зенитно-ракетных комплексов (ЗРК);

- «средства разведки в составе СВКН – средства связи системы ВКО», формализующий процессы оценки разведзащищенности линий связи и центров передачи и обработки информации на пункты управления (ПУ) системы ВКО, а также других ее элементов (в т.ч. резервных РЛС и ЗРК), передающих информацию в радиодиапазоне;
- «средства радиоэлектронного подавления (РЭП) в составе СВКН – источники информации в системе ВКО», формализующий процессы оценки помехозащищенности РЛС контроля воздушного пространства в составе РТВ, РЛС СПРН, РЛС СККП, а также РЛС ЗРК и пассивные средства радиоэлектронной разведки (РЭР);
- «средства РЭП в составе СВКН – средства связи системы ВКО», формализующий процессы оценки помехозащищенности формализующий процессы оценки помехозащищенности линий связи и центров приема и обработки информации на ПУ системы ВКО, а также других ее элементов (в т.ч. резервных РЛС и ЗРК), принимающих информацию в радиодиапазоне;
- «средства поражения в составе СВКН – элементы системы ВКО», формализующий процессы оценки живучести всех элементов системы ВКО: ПУ, РЛС, средства РЭР, ЗРК и пр.

Целью настоящей статьи является формирование описательной модели комплексов и средств разведки, используемых для вскрытия элементов системы ВКО и целеуказания при нанесении БГУ. Данная описательная модель в дальнейшем планируется к использованию при формировании исходных данных, используемых при формализации первого и второго из вышеуказанных частных конфликтов.

1. Особенности использования комплексов и средств разведки при планировании и нанесении «быстрого глобального удара» средствами воздушно-космического нападения

Как показал анализ работ [2, 4, 5, 9, 10], особенностью разведки и целеуказания при БГУ СВКН является следующее (рис. 1).

На этапе планирования БГУ в основном используются космические средства разведки, прежде всего средства радио- и радиотехнической разведки (РРТР) и оптико-электронной разведки (ОЭР). Воздушная разведка ведется на большой высоте пилотируемыми и беспилотными летательными аппаратами (БПЛА) вдоль границ без захода в воздушное пространство атакуемой страны. На данном этапе средствами РРТР вскрывается структура и местоположение основных объектов системы ВКО, являющихся целями для поражения в первом эшелоне БГУ: РЛС РТВ; РЛС СПРН; РЛС СККП; РЛС и ПУ ЗРК; ПУ различного уровня. Средствами ОЭР космического базирования определяется назначение объектов системы ВКО, уточняются и корректируются данные о местоположении стационарных объектов системы ВКО, которые в дальнейшем исполь-

№1. 2021
ISSN 2410-9916

зуются для формирования целеуказаний средствам ВТО. На этом же этапе формируются и уточняются данные о местоположении основных ПУ государственного и военного управления, объектов критической инфраструктуры государства, являющихся целями для поражения во втором (основном) эшелоне БГУ.

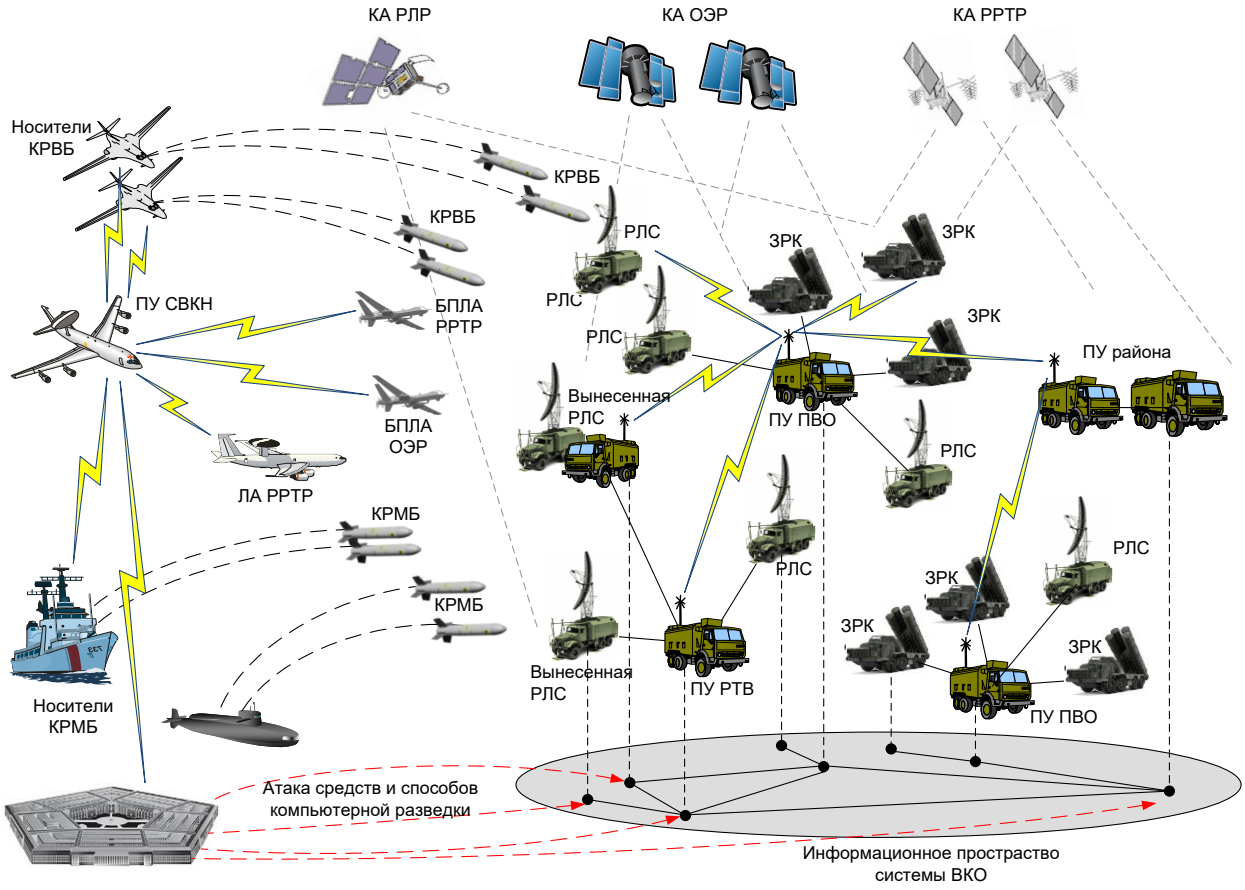

Рис. 1. Применение средств разведки для вскрытия объектов системы ВКО и целеуказания для средств ВТО в процессе нанесения БГУ

На этапе, предшествующем непосредственному нанесению БГУ, космическими и воздушными средствами РРТР и ОЭР уточняется местоположение мобильных объектов системы ВКО: мобильных РЛС РТВ, РЛС, пусковых установок, ПУ ЗРК, мобильных ПУ различного уровня. Формируются окончательные данные по целеуказанию средствам ВТО в первом эшелоне БГУ. Формируются варианты по перенацеливанию средств ВТО на различные точки размещения мобильных объектов ВКО в процессе нанесения БГУ.

В процессе нанесения БГУ в составе первого эшелона для вскрытия новых объектов системы ВКО, а также для контроля результативности поражения ранее вскрытых объектов, используются как пилотируемые летательные аппараты (ЛА) – специальные самолеты РРТР, действующие за пределами зон поражения ЗРК системы ВКО, так и БПЛА, оборудованные средствами РРТР и ОЭР, действующие непосредственно в зоне ведения боевых действий. Информация с ЛА и БПЛА, действующих в первом эшелоне БГУ используется для целеуказания по вновь выявленном объектам системы ВКО: резервным РЛС, ПУ и ЗРК.

DOI: 10.24411/2410-9916-2021-10108
URL: http://sccs.intelgr.com/archive/2021-01/08-Afonin.pdf

К космическим аппаратам (КА), которые могут решать задачи разведки объектов системы ВКО, можно отнести следующие: КА РТР Ferret-D, SSU и SSU-2; КА РР Vortex, Mercury, Magnum, Orion, Mentor; КА ОЭР KeyHole, TacSat-3 и ORS [2, 10, 11].

К пилотируемым ЛА, которые могут решать задачи РРТР, можно отнести RC-135W Rivet Joint, RC-12, RC-7B и EC-130H CompassCall. К БПЛА, которые могут решать задачи РРТР и ОЭР, можно отнести RQ-4 Global Hawk, RQ-6 Outrider и MQ-1C Grey Eagle [2, 10].

Отметим, что кроме комплексов и средств РРТР и ОЭР космического и воздушного базирования, определенную роль для вскрытия объектов системы ВКО играют средства компьютерной разведки и радиолокационной разведки (РЛР).

Средства сетевой, потоковой и аппаратной компьютерной разведки, действуя в сетях связи общего пользования (СС ОП), сопряженных с линиями связи системы ВКО (в том числе проводными и оптическими), могут обеспечивать добывание оперативно-ценной информации, позволяющей вскрыть принадлежность и структуру виртуальных каналов обмена данными в системе государственного и военного управления [12], в том числе – в системе ВКО, проходящих через сегменты СС ОП, идентифицировать тип и роль объекта в системе ВКО, используемое им программное обеспечение (ПО), интенсивность обмена данными с другими объектами. Результаты применения средств компьютерной разведки в дальнейшем могут использоваться в интересах формирования целеуказаний для атакующих информационно-технических воздействий (ИТВ), осуществляющих как информационное блокирование объектов системы ВКО, так и нарушение целостности информации, предаваемой в ней.

Средства семантической, форматной, пользовательской компьютерной разведки действуя в открытых сетях связи, в социальных сетях и на электронно-вычислительных машинах (ЭВМ) лиц командного состава и обслуживающего персонала объектов системы ВКО, могут вскрывать местоположение и уточнять предназначение значимых объектов, дислокацию сил и средств системы ВКО, схем организации управления, которые в дальнейшем используются для определения приоритетности поражения объектов при проведении БГУ [12].

В отношении средств РЛР стоит отметить, что в ряде случаев космические средства РЛР могут использоваться как аналоги средств ОЭР. Однако, по мнению авторов, средства РЛР воздушного базирования, по все видимости не будут использоваться, т.к. являются активно излучающими источниками радиоизлучения (ИРИ), которые будут заблаговременно обнаруживаться и поражаться ЗРК системы ВКО сразу же после входа в их зону поражения.

Таким образом, комплексы и средства РРТР и ОЭР космического и воздушного базирования, а также средства компьютерной разведки играют важную роль в формировании целеуказаний средствам поражения ВТО для вывода из строя элементов системы ВКО. В связи с этим целесообразным является их подробный анализ и формирование обобщённых тактико-технических характеристик (ТТХ) типовых средств разведки.

2. Описательная модель комплексов и средств радио- и радиотехнической разведки

Радиоэлектронная разведка (РЭР) – процесс получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами (РЭС) [13].

Составными частями радиоэлектронной разведки являются радиоразведка и радиотехническая разведка.

Радиоразведка (РР) – вид радиоэлектронной разведки, ориентированный на различные виды радиосвязи, основным содержанием которого является: обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения ИРИ; снижение нагрузки или подрыв криптографических систем [13].

Применительно к системе ВКО основными объектами РР являются: передающие средства радиосвязи, размещённые на мобильных объектах системы ВКО; центры радиосвязи на стационарных и мобильных ПУ; средства радиосвязи вынесенных и удаленных РЛС РТВ, ЗРК ПВО и других объектах [10, 14].

Радиотехническая разведка (РТР) – вид радиоэлектронной разведки, целью которого являются сбор и обработка информации, получаемой с помощью РЭС о радиоэлектронных системах противника по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах.

В общем случае объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также электромагнитные излучения (ЭМИ), создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т.п.) [13].

Применительно к системе ВКО основными объектами РТР являются: стационарные и мобильные РЛС РТВ; РЛС воздушного базирования, размещенные на ЛА истребительной авиации и БПЛА контроля воздушного пространства; РЛС СПРН; РЛС СККП; РЛС ЗРК [10, 14].

Средства РРТР позволяют:

- установить несущую частоту передающих ИРИ;
- определить координаты ИРИ;
- определить тип ИРИ, в некоторых случаях – идентифицировать ИРИ, как какое-то определённое РЭС;
- измерить параметры сигнала (частоту повторения, длительность, вид модуляции и другие параметры);
- определить структуру боковых лепестков излучения радиоволн;
- определение поляризации радиоволн;
- установить скорость сканирования антенн и метод обзора пространства у РЛС;
- проанализировать и записать информацию.

Необходимо отметить, что средства РР ориентированы главным образом на перехват и выделение семантического содержания передаваемых сообщений, а средства РТР – на определение параметров сигналов, их накопление с целью формирования радиоэлектронного портрета ИРИ, и его последующее отождествление с конкретным образцом вооружения или военной техники (ВВТ). Однако особенностью современного этапа развития средств РР и РТР является, во-первых, невозможность дешифровки сообщений, которые в подавляющем большинстве передаются в зашифрованном виде, во-вторых, средствам РРТР на современном этапе их развития свойственна определенная универсальность относительно объектов разведки [15]. При этом отнесение тех или иных РЭС к объектам РР или РТР может быть произведено уже после обработки результатов разведки и классификации вскрытых объектов. Такая тенденция не позволяет утверждать об ориентированности на вскрытие объектов системы ВКО исключительно средств РТР, а требует учитывать возможности интегрированных средств РРТР при оценке разведзащищенности системы ВКО.

Основными способами обнаружения сигналов, используемыми системами РРТР, являются [16]:

- непрерывное сканирование диапазона частот;
- дискретное сканирование полосы частот;
- комбинированное сканирование.

Вероятность обнаружения РЭС систем радиосвязи зависит от отношения скорости сканирования к длительности принимаемых сигналов. Например, при продолжительности связи в УКВ-диапазоне, равной нескольким секундам, скорость сканирования в этом диапазоне, равная 20-50 МГц/с, будет являться приемлемой [16].

Чувствительность приемников разведывательных устройств в КВ- и УКВ-диапазонах с широкополосными антеннами лежит в пределах 0,5-5 мкВ/м, а разрешающая способность по частоте находится в пределах 20-30 кГц [16].

Сложнее обстоит дело с перехватом сигналов средств радиосвязи, которые используют режимы псевдослучайной перестройки рабочей частоты (ППРЧ). В этом случае средствам РРТР необходимо дополнительно вскрыть программу, по которой изменяется ППРЧ [17].

Современные цифровые приемные устройства, работающие в режиме радиомониторинга в диапазоне частот 1,5-30 МГц, имеют чувствительность 184 дБВт/Гц, динамический диапазон не менее 80 дБ, скорость поиска по частоте 3-50 ГГц/с, разрешение по частоте от 100 Гц до 5 кГц. Они способны вести разведку сигналов с ППРЧ, сигналов со сжатием, со всеми видами модуляции и кодирования [16]. Однако вскрытие содержания передаваемых сообщений, за предполагаемое время оперативной ценности передаваемой информации, является практически нерешаемой задачей из-за повсеместного использования средств криптографической защиты.

Дальность электромагнитной доступности ИРИ из состава систем связи для средств РРТР определяется типом ИРИ и используемым ими диапазоном [16]:

- для средств КВ радиосвязи – 3000 км;

– для средств УКВ радиосвязи – 200 км (при наличии прямой видимости);
– для средств радиотехнического обеспечения – 100 км для наземных целей, до 300 км для воздушных целей.

2.1. Средства космического базирования

Рассматривая КА РТР Ferret-D, SSU и SSU-2 как прототипы космических средств РТР, можно сформировать обобщенные ТТХ такого типового средства [2, 10, 11]:

– диапазон ведения РТР: от 30 МГц до 80 ГГц;
– вскрываемые параметры РЭС: местоположение, тип, режимы работы;
– точность определения местоположения РЭС: 1-10 км;
– ширина полосы сканирования: 5500-8000 км;
– высота развертывания орбитальной группировки КА: 800-1200 км;
– периодичность безпропускного обзора поверхности Земли: 1,5-5,5 ч.

Рассматривая КА РР Vortex, Mercury, Magnum, Orion, Mentor как прототипы космических средств РР, можно сформировать обобщенные ТТХ такого типового средства [2, 10, 11]:

– диапазон ведения РР: от 45 МГц до 40 ГГц;
– функциональность: вскрытие местоположения, типа, режимов работы связных РЭС; перехват информации наземных радиосредств, а также переговоров по УКВ-линиям радиосвязи; перехват сообщений в УВЧ каналах правительственной и военной радиосвязи;
– периодичность безпропускного обзора поверхности Земли: непрерывно.

2.2. Средства воздушного базирования

Как показано в работе [2], средства РРТР воздушного базирования являются основными средствами добывания информации об объектах ВКО (прежде всего – РЛС) в военных конфликтах. При этом могут использоваться как специализированные самолеты РРТР (RC-135W Rivet Joint, EC-130H CompassCall), так и относительно универсальные БПЛА (типа RQ-4 Global Hawk), оборудованные аппаратурой РРТР.

Как правило, для решения задач РРТР в ходе военных операций средства воздушного базирования декомпозируются на два компонента.

1. Основной компонент, образованный специализированными комплексами РРТР (например, RC-135W Rivet Joint), действующими в пределах воздушного пространства противника, но вне зоны поражения ЗРК либо за его пределами, и решающими базовые задачи по ведению РРТР.
2. Вспомогательный компонент, включающий в себя средства РРТР на БПЛА, действующие в пределах воздушного пространства противника, недоступного для средств РРТР основного компонента (например, в пределах зон гарантированного поражения ЗРК), которые решают задачи РРТР непосредственно над территорией противника.

Рассматривая комплексы RC-135W Rivet Joint, RC-12, RC-7B и EC-130H CompassCall как прототипы первого компонента средств РРТР воздушного базирования, а также с учетом ТТХ таких средства РРТР как ES-5000, AN/ALQ-61, WJ-1740, FASTHAT, LR-5200, можно сформировать обобщенные ТТХ такого типового средства.

ТТХ типового средства основного компонента средств РРТР [2, 16, 18, 19]:

- назначение: ведение РРТР ИРИ наземного, морского и воздушного базирования в СМВ, ДМВ и МВ диапазонах длин волн, а также пеленгование ИРИ в автоматическом и ручном режимах;
- функциональность РР: перехват и пеленгование, запись, дешифрирование и анализ радиопереговоров противника, в том числе переговоров экипажей боевых самолетов между собой и с наземными ПУ на дальности до 900 км;
- функциональность РТР: одновременное обнаружение, распознавание и предварительное определение местоположения ИРИ на дальности до 500 км;
- диапазон ведения РР: от 3 МГц до 18 ГГц;
- диапазон ведения РТР: 0,5-40 ГГц;
- точность пеленгования ИРИ: 0,01°-2°;
- точность определения координат ИРИ: 100-150 м;
- ширина мгновенной полосы обзора: 0,5 ГГц;
- скорость перестройки: 100 МГц/мкс;
- чувствительность: 190 дБВт/Гц;
- высота ведения разведки: 3-7 км;
- удаление от линии соприкосновения войск: 50-100 км;
- дальность полета: до 11000 км;
- скорость полета: до 970 км/ч;
- высота полета: до 16,5 км;
- масса: 54-146 т;
- экипаж: до 5 человек, оперативная группа – до 25 человек.

Рассматривая БПЛА RQ-4 Global Hawk, RQ-6 Outrider и MQ-1C Grey Eagle [20] как прототипы второго компонента средств РРТР воздушного базирования, можно сформировать обобщенные ТТХ такого типового средства:

- диапазон частот: 1,8-18 ГГц;
- динамический диапазон: 60 дБ;
- точность определения частоты ИРИ: 2 МГц;
- точность пеленга ИРИ: 0,8°;
- скорость полета: до 500 км/ч;
- высота полета: до 18 км;
- дальность полета: до 6000 км.

Задачами БПЛА, оснащенных комплексами РРТР, являются следующие [20]:

- проведение первоначальной разведки в оперативной глубине;

– определение местоположения ИРИ и их параметров в интересах формирования целеуказаний для комплексов РЭП и средств ВТО по результатам РРТР;
– вскрытия местоположения базовых станций сетей Wi-Fi, базовых станций мобильной сотовой и транкинговой связи.

На стратегическом уровне управления основной функцией БПЛА является ведение РРТР, в ходе которой они должны осуществлять перехват сигналов, их анализ и формирование карты радиоэлектронной обстановки. Одновременно происходит пополнение баз данных/библиотек РЭС, расположенных в районе патрулирования. На оперативном уровне решаются задачи по ведению разведки, в том числе видовой, формированию целеуказаний системам ВТО. На тактическом уровне БПЛА с помощью систем и средств РРТР могут собирать и передавать пользователям критически важные данные о радиоэлектронной обстановке и формировать целеуказание на подавление или уничтожение вновь обнаруженных РЭС [20].

В перспективе до 2030 г. ожидается, что воздушные средства РТР будут использовать диапазон частот 0,7-160 ГГц для тактических самолетов и 0,25-160 ГГц для стратегических самолетов. Чувствительность приемной части систем РТР может составить до 190 дБВт/Гц, динамический диапазон – до 90 дБ, точность пеленга – до 0,02-0,05°, число каналов – более 100, число РЭС, параметры которых хранятся в запоминающем устройстве, может составить несколько тысяч. К этому же сроку ожидается, что системы РР будут использовать диапазон частот от 0,03 МГц до 100 ГГц, иметь чувствительность 150-180 дБВт/Гц, избирательность 90-95 дБ, точность пеленга 0,1-0,5 °, точность определения координат на дальности до 300 км – 10-20 м [16].

3. Описательная модель комплексов и средств оптико-электронная разведки

Оптико-электронная разведка (ОЭР) – процесс добывания информации с помощью средств, включающих в свой состав входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и инфракрасного (ИК)-диапазонов, излученных или отраженных объектами и местностью [13].

Оптико-электронная разведка ориентирована на доразведку объектов, вскрытых по результатам РРТР, уточнение местоположения и классификацию ИРИ как объекта системы ВКО, вскрытие стационарных и мобильных ПУ, мест дислокации РЛС и ЗРК, районов их рассосредоточения, запасных позиций и т.д.

3.1. Средства космического базирования

Принимая средства КА KeyHole, TacSat-3 и ORS как прототипы космических средств ОЭР, можно сформировать их обобщенные ТТХ [2, 10, 11]:

– диапазон ведения разведки: днем – видимый диапазон волн (с получением стереоизображений), ночью – ИК-диапазон;
– разрешающая способность: до 0,15 м в панхроматическом режиме и до 1,5 м в многоспектральном режиме;
– ширина полосы обзора: 1200-3600 км;
– высота развертывания орбитальной группировки КА: 200-500 км;
– периодичность безпропускного обзора поверхности Земли: 1,5-2,5 ч.

3.2. Средства воздушного базирования

Необходимо отметить, что подавляющая часть средств ОЭР размещается на БПЛА. Такие БПЛА ведут разведку в режиме «дежурство в воздухе». Рассматривая MQ-9 Reaper и RQ-4 Global Hawk как варианты типового БПЛА, можно сформировать ТТХ обобщенного БПЛА – носителя средств ОЭР [2]:

– вариант боевого применения в интересах обнаружения объектов системы ВКО: следование в боевых порядках СВКН; дежурство в воздухе до 45 ч на высоте до 18 км;
– скорость полета: до 500 км/ч;
– дальность полета: до 6000 км;
– аппаратура разведки: единый интегрированный радиотехнический, оптико-электронный и радиолокационный комплекс;
– параметры разведки: обеспечивает получение радиолокационного и оптического изображения местности с разрешением до 0,3 м. За сутки может быть получено изображение с площади 138 км^2 на расстоянии 200 км.

Более полные сведения о средствах ОЭР представлены в работе [2].

4. Описательная модель комплексов и средств радиолокационной разведки

Как показано ранее, для обеспечения разведки и целеуказания при нанесении БГУ могут использоваться КА РЛР, особенностью применения которых, с одной стороны, является дублирование средств ОЭР, с другой стороны, космические средства РЛР являются всепогодными, не зависят от метеорологических условий, обладают разрешающей способностью, сопоставимой с ОЭР.

Рассматривая КА Lacrosse, TerraSAR-X2, SAR-Lupe, TanDEM-X, Cosmo-Skymed как варианты типовых КА РЛР, можно сформировать ТТХ обобщенного средства комической РЛР [11, 21-23]:

– диапазон ведения разведки: X и L диапазоны;
– разрешающая способность:
  а) в фоторежиме детальной съемки: 0,25-0,9 м;
  б) в фоторежиме обзорной съемки: 2-3 м;
  в) в режиме ведения съемки в полосе: 10-15 м;
– ширина полосы обзора: 3-200 км;

– высота развертывания орбитальной группировки КА: 600-700 км;
– периодичность обновления данных обзора поверхности Земли: в масштабе времени, близком к реальному, при передаче данных через КА-ретрансляторы.

Более полные сведения о космических средствах РЛР представлены в работах [21-24].

5. Описательная модель средств и способов компьютерной разведки

5.1. Средства и способы компьютерной разведки

Компьютерная разведка – добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [20].

Выделяют три типа источников информации для компьютерной разведки [13]:

– данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
– характеристики программных, аппаратных и программно-аппаратных комплексов;
– данные о пользователях компьютерных систем и сетей, а также об их деятельности и интересах.

Несмотря на то, что в большинстве работ, посвященных вопросам разведзащищённости системы ВКО, компьютерная разведка не рассматривается, с учетом текущих тенденций развития систем военной связи, образующих информационное пространство системы ВКО, данный тип разведки начинает играть всё большую роль. Как показал проведенный в работе [12] анализ современных систем военной связи, а также перспектив их развития, в этих системах преобладают следующие основные тенденции:

– переход от иерархического принципа построения систем военной связи, когда их структура жестко увязывается со структурой организационной подчиненности абонентов, к децентрализовано-сетевой структуре, которая не зависит от системы подчиненности абонентов и, в большей степени, соответствует современным требованиям к сетецентрическим системам государственного и военного управления;
– отказ от построения систем военной связи на основе выделенной сетевой инфраструктуры и переход к их построению на основе гибридного подхода, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальной сети (типа Интернет) используются в качестве элементов транспортной инфраструктуры систем военной связи;
– максимальное широкое использование для построения систем военной связи подходов, протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Данные тенденции подтверждаются общими принципами построения систем военной связи как для ВС РФ, так и для ВС США.

Стационарные и мобильные узлы связи, на основе которых формируется информационное пространство системы ВКО, привязываются к единой системе связи (ЕСЭ) РФ, которая одновременно с услугами организации связи для военных потребителей предоставляет услуги связи для СС ОП операторов связи и доступа пользователей РФ в сеть Интернет. Широко распространена практика аренды необходимых канальных ресурсов для привязки объектов системы ВКО у региональных и национальных операторов связи. Ряд экспертов считает, что в настоящее время развертывание отдельной телекоммуникационной инфраструктуры для систем военной связи является экономически нецелесообразным, и что современные и перспективные системы связи для военных потребителей должны активно использовать ресурсы гражданских операторов СС ОП национального и регионального масштаба. Однако, использование в системах военной связи «гражданских технологий», одновременно с их фактической интеграцией через общие сегменты СС ОП в мировое информационное пространство, существенно расширяет спектр уязвимостей военных систем связи (в частности – подсистемы проводной связи системы ВКО), которые могут быть использованы противником при реализации ведения компьютерной разведки и ИТВ с целью как информационного блокирования объектов системы ВКО, так и нарушения целостности и конфиденциальности информации, передаваемой в ее подсистеме связи.

По виду реализации средства и способы компьютерной разведки можно классифицировать следующем образом:

- *физические* – реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* – реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков, циркулирующих в них.

Рассматривая отдельные объекты системы ВКО как человеко-машинные компьютерные системы, объединенные через средства радио- и проводной связи в компьютерные сети, можно выделить следующие типы компьютерной разведки значимые для оценки разведзащищенности системы ВКО [13]:

- *семантическая* – обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных информационных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов;

- *алгоритмическая* – обеспечивающая добывание информации путем использования заранее внедренных изготовителем программных или аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;
- *вирусная* – обеспечивающая добывание данных путем внедрения вирусных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;
- *разграничительная* – обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, которые могут не входить в состав сети, осуществляемая на основе преодоления средств разграничения доступа путем несанкционированного доступа к информации, физического доступа к компьютерной системе или к носителям информации;
- *сетевая* – обеспечивающая добывание информации из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов и объектов пользователей, а также последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;
- *потоковая* – обеспечивающая добывание информации путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров;
- *аппаратная* – обеспечивающая добывание информации путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
- *форматная* – обеспечивающая добывание информации путем агрегированной обработки, фильтрации, декодирования, а также проведения других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию, для последующего ее наилучшего представления пользователям;
- *пользовательская* – обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения доступа пользователей к информации, циркулирующей в специально созданной информационной инфраструктуре.

На современном этапе развития компьютерных систем и сетей перечисленные типы компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно

выделение нескольких подтипов разведки, например, по виду добываемой информации на: *фактографическую* («*видовую*») и *параметрическую*.

Общая классификация средств и способов компьютерной разведки представлена на рис. 2.

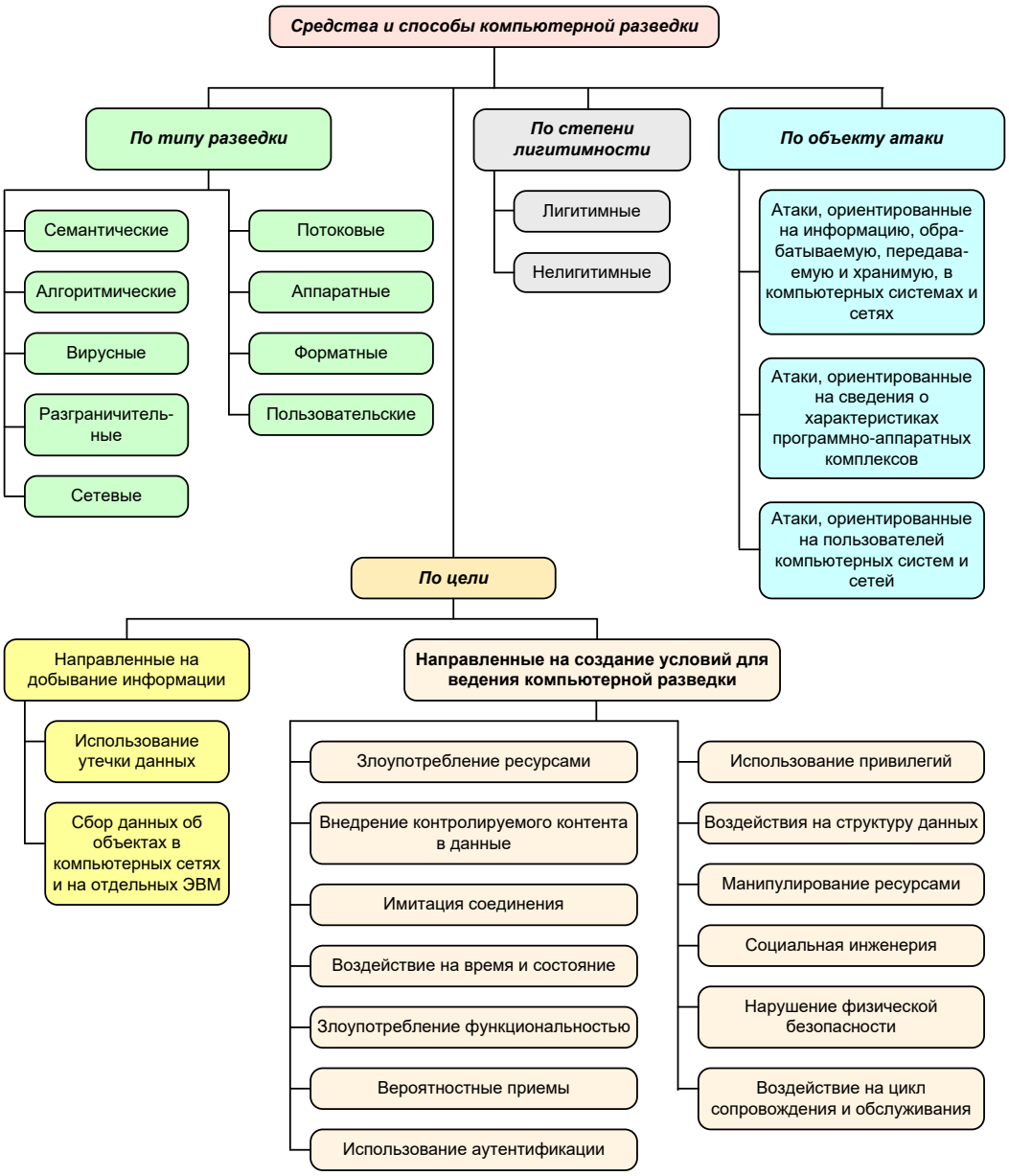

Рис. 2. Классификация средств и способов компьютерной разведки [20]

Основным способом реализации компьютерной разведки является атака средств компьютерной разведки [25, 26].

Атака средств компьютерной разведки – это как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия, направленные на создание условий, благоприятствующих добыванию информации.

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества призна-

ков. Один из наиболее полных учетов признаков реализован в классификации CAPEC [27], разработанной корпорацией MITRE. Однако классификация CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [26] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 3.

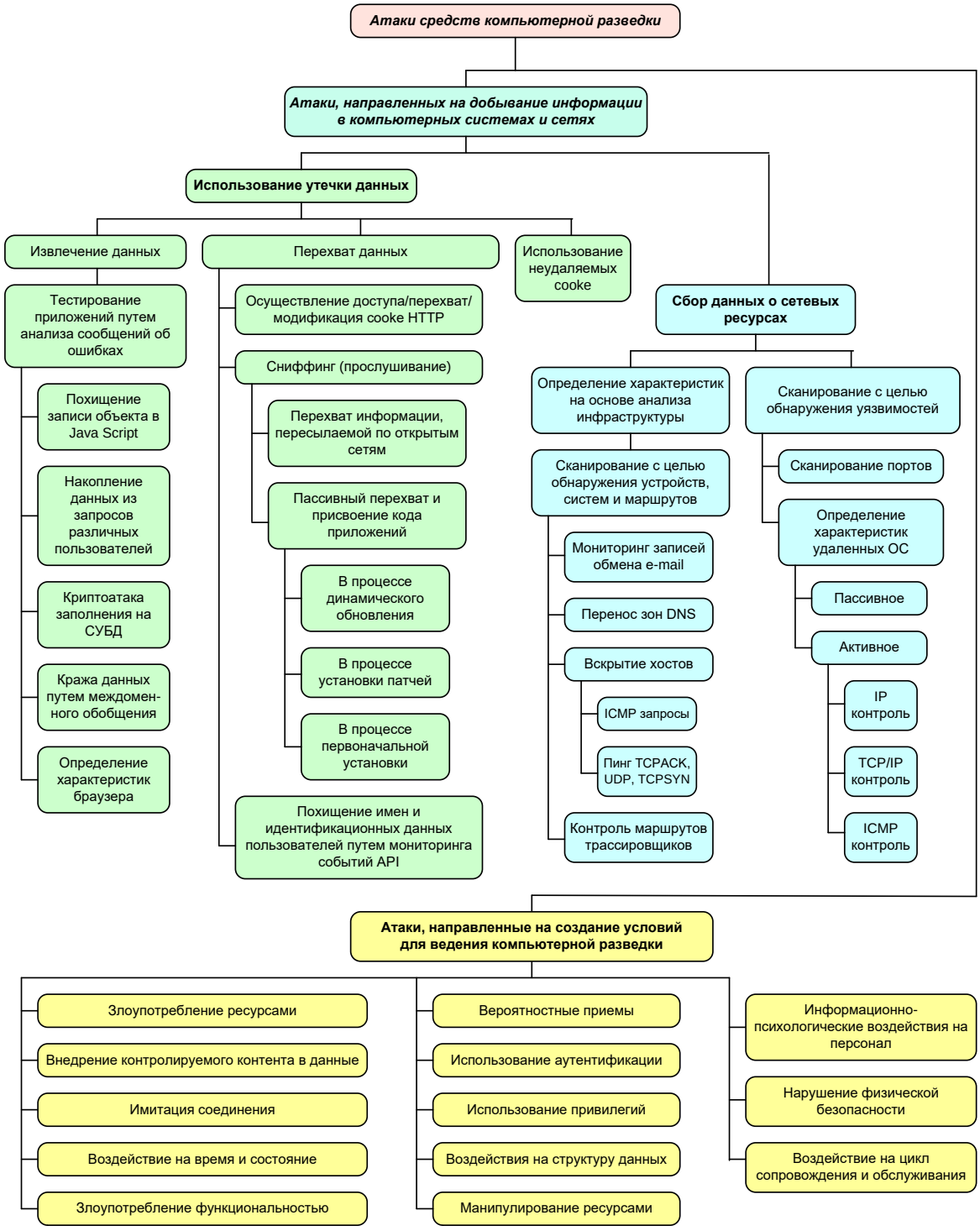

Рис. 3. Классификация атак средств компьютерной разведки [26]

5.2. Разведка по открытым источникам

При вскрытии параметров и мест размещения объектов системы ВКО, их состава и предназначения всё большую роль играет сбор организационной и технической информации, а также информации об эксплуатирующем ее персонале и лицах, принимающих решения, в социальных сетях, на общедоступных геоинформационных сервисах (типа Google Map) и на тематических сайтах сети Интернет. Большое количество комментариев лиц, проходящих службу на объектах системы ВКО, фото- и видеоматериалы, геотеги на электронных картах позволяют при соответствующей обработке получить информацию как о том или ином объекте системы ВКО, так и вскрыть общую структуру системы, роль и предназначение отдельных объектов, а также в реальном времени отслеживать тенденции ее развития (перевооружения) или смены дислокации (перебазировании).

При сборе такой информации широко используются средства разведки по открытым источникам – в рамках проведения семантической и пользовательской компьютерной разведки. Классификация средств разведки по открытым источникам представлена на рис. 4. Более подробные данные об этих средствах представлены в работе [20].

Во многом повышение значимости разведки по открытым источникам обусловлено тем фактом, что порядка 10-15% необходимой информации имеется в глобальной сети Интернет уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и представленных в различных источниках фактов. Естественно, что информация, полученная таким образом, нуждается в верификации.

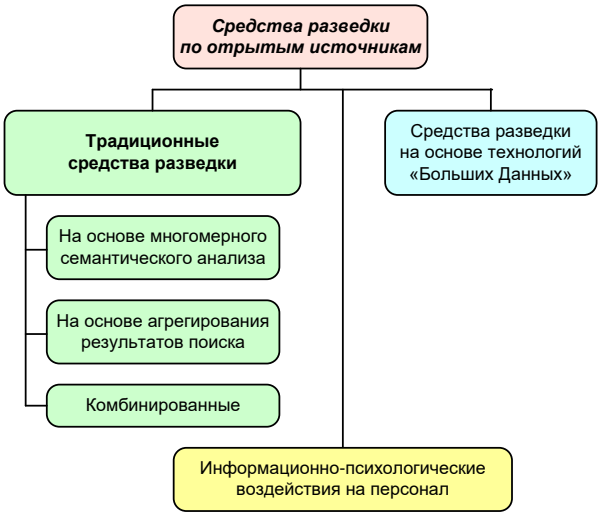

Рис. 4. Классификация средств разведки по отрытым источникам [20]

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Специальные программы опрашивают сайты и извлека-

ют из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в сети Интернет.

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде находится в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с совпадающим целевым контентом, начинают «собирать» информационное наполнение запроса пользователей. Более интересным направлением развития таких средств разведки является анализ разнородных, изначально семантически не связанных между собой данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы «Больших данных» (Big Date).

Формирование глобального электронного постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и коммерческих компаний до небольших групп и отдельных индивидуумов, в сети Интернет послужило основой появления Больших данных.

Технологии Больших данных основаны, прежде всего, на методах статистического и интеллектуального анализа данных, применяемых на огромных постоянно пополняемых массивах данных.

Технологии Больших данных позволяют [28]:

– проводить различные и подробные классификации той или иной совокупности людей, их информации, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают понимание взаимосвязи тех или иных характеристик объекта с теми или иными его действиями;
– осуществлять многомерный статистический корреляционный анализ, выявляющий закономерности и связи различных факторов;
– прогнозировать и управлять, путем использования выявленной корреляционной связи факторов, для определения наиболее целесообразного способа воздействия в информационном пространстве.

Более подробная информация об использовании технологий Больших данных при решении задач разведки представлена в работах [20, 28].

Выводы

Средства технической разведки – это основной фактор, влияющий на разведзащищенность структуры, режимов работы, местоположения объектов системы ВКО. При этом для системы ВКО из всего многообразия средств технической разведки основную угрозу представляют следующие типы разведки:

1) РРТР, ориентированная на вскрытие параметров и местоположения ИРИ, отождествление их с конкретными объектами или элементам системы ВКО; места и времени контроля воздушно-космического про-

странства; содержания ведущегося радиообмена; с последующим формированием целеуказаний для средств поражения ВТО и средств РЭБ;
2) ОЭР, ориентированная на уточнение местоположения и классификации ИРИ как конкретного объекта системы ВКО; вскрытие резервных позиций и дополнительных мест дислокации мобильных РЛС, ЗРК и других объектов;
3) РЛР, ориентированная на дублирование задач ОЭР в сложных метеоусловиях;
4) компьютерная разведка, ориентированная на добывание оперативно-ценной информации, позволяющей вскрыть принадлежность и структуру виртуальных каналов обмена данными в системе ВКО, проходящими через сегменты СС ОП, уточнять схемы организации управления, идентифицировать тип и роль объекта в системе ВКО, используемое им программное обеспечение, интенсивность обмена данными с другими объектами.

В статье представлена описательная модель комплексов и средств разведки, используемых противником для вскрытия системы ВКО и целеуказания при нанесении БГУ СВКН, с учетом их перспективного развития в период до 2030 г., которая может быть использована при формировании исходных данных для оценки разведзащищенности и скрытности системы ВКО в соответствующих моделях, а также при разработке методов, методик и способов повышения соответствующих показателей РЛС, ЗРК и ПУ.

Литература

1. Тулин С. Вооружённые силы США: сценарии глобальных ударов неядерными средствами // Зарубежное военное обозрение. 2010. № 4. С. 19–23.

2. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

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

4. Михайлов Д. В. Война будущего: возможный порядок нанесения удара средствами воздушного нападения США в многосферной операции на рубеже 2025-2030 годов // Воздушно-космические силы. Теория и практика. 2019. № 12. С. 44-52.

5. Афонин И. Е., Макаренко С. И., Митрофанов Д. В. Анализ концепции «Быстрого глобального удара» средств воздушно-космического нападения и обоснование перспективных направлений развития системы воздушно-космической обороны в Арктике в интересах защиты от него // Воздушно-космические силы. Теория и практика. 2020. № 15. С. 75-87.

6. Макаренко С. И., Ковальский А. А., Афонин И. Е. Обоснование перспективных направлений развития системы противокосмической обороны российской федерации в интересах своевременного вскрытия и отражения «Быстрого глобального удара» средств воздушно-космического нападения // Воздушно-космические силы. Теория и практика. 2020. № 16. С. 99-115.

7. Краснослободцев В. П., Раскин А. В., Савельев С. С., Купач О. С. Анализ возможности по реализации США концепции быстрого глобального удара // Стратегическая стабильность. 2014. № 2 (67). С. 67-69.

8. Фененко А. В. Концепция «Быстрого глобального удара» в контексте развития военной стратегии США // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. 2016. Т. 8. № 4. С. 18-50.

9. Стучинский В. И., Корольков М. В. Обоснование боевого применения авиации для срыва интегрированного массированного воздушного удара в многосферной операции противника // Воздушно-космические силы. Теория и практика. 2020. № 16. С. 29-36.

10. Средства воздушно-космического нападения и воздушно-космической обороны. Состояние и развитие / Под общей ред. И.Р. Ашурбейли. – М.: ПЛАНЕТА, 2017. – 336 с.

11. Макаренко С. И. Использование космического пространства в военных целях: современное состояние и перспективы развития систем информационно-космического обеспечения и средств вооружения // Системы управления, связи и безопасности. 2016. № 4. С. 161-213. DOI: 10.24411/2410-9916-2016-10409.

12. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

13. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

14. Диалектика технологий воздушно-космической обороны / Под ред. В.Н. Минаева. – М.: Издательский дом «Столичная энциклопедия», 2011. – 367 с.

15. Перунов Ю. М., Куприянов А. И. Радиоэлектронная борьба: радиотехническая разведка. – М.: Вузовская книга, 2017. – 190 с.

16. Перунов Ю. М., Мацукевич В. В., Васильев А. А. Зарубежные радиоэлектронные средства / Под ред. Ю.М. Перунова. В 4-х книгах. Кн. 2: Системы радиоэлектронной борьбы. – М.: Радиотехника, 2010. – 352 с.

17. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб.: Свое издательство, 2013. – 166 с.

18. Пиунов О., Щербинин Р. Американский стратегический разведывательный самолёт RC-135 и его модификации // Зарубежное военное обозрение. 2012. № 3. С. 70-76.

19. Максименко А. Американские системы радиоэлектронной разведки // Зарубежное военное обозрение. 2004. № 9. С.45-49.

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

21. Шпенст В. Радиолокационные станции дистанционного зондирования Земли космического базирования // Компоненты и технологии. 2013. № 3.

С. 154-158. – URL: https://kit-e.ru/assets/files/pdf/2013_3_154.pdf (дата обращения 10.02.2021).

22. Лисицын А. Космические системы дистанционного зондирования земли зарубежных стран // Зарубежное военное обозрение. 2019. № 7. С. 63-67. – URL: http://factmil.com/publ/strana/germanija/kosmicheskie_sistemy_distancionnogo_zondirovanija_zemli_zarubezhnykh_stran_2019/41-1-0-1666 (дата обращения 10.02.2021).

23. Бабурин А., Пахомова А. Состояние и перспективы развития средств космической видовой радиолокационной разведки западноевропейских стран // Зарубежное военное обозрение. 2017. № 9. С. 64-68. – URL: http://factmil.com/publ/strana/germanija/sostojanie_i_perspektivy_razvitija_sredstv_kosmicheskoj_vidovoj_radiolokacionnoj_razvedki_zapadnoevropejskikh_stran_2017/41-1-0-1217 (дата обращения 10.02.2021).

24. Груздов В. В., Колковский Ю. В., Криштопов А.В., Кудря А. И. Новые технологии дистанционного зондирования Земли из космоса. – М.: Техносфера, 2018. – 482 с.

25. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.

26. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

27. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description. Version 1.3. Cigital Inc. 2008. – URL: https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf (дата обращения 09.01.2020).

28. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

References

1. Tulin *S.* Vooruzhyonnye sily SSHA: scenarii globalnyh udarov neyadernymi sredstvami [US Armed Forces: scenarios of global non-nuclear strikes]. *Zarubezhnoe voennoe obozrenie*, 2010, no. 4, pp. 19-23 (in Russian).

2. Makarenko S. I., Ivanov M. S. *Setecentricheskaya vojna – principy, tekhnologii, primery i perspektivy. Monografiya* [*Network-centric warfare – principles, technologies, examples and perspectives. Monography*]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2018. 898 p. (in Russian).

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

4. Mihajlov D. V. The War of the future: the possible order of the US air attack strike in the multi-sphere operation at the turn of 2025-2030. *Aerospace forces. Theory and practice*, 2019, no. 12, pp. 44-52 (in Russian).

5. Afonin I. E., Makarenko S. I., Mitrofanov D. V. Analysis of the concept of "Prompt global strike" of air-space attack means and substantiation of prospective directions of air-space defense system development in the arctic in the interest of defense. *Aerospace forces. Theory and practice*, 2020, no. 15. pp. 75–87 (in Russian).

6. Makarenko S. I., Kovalskiy A. A., Afonin I. E. Justification of Perspective Directions of Development of the Russian Federation's Anti-Space Defense System in the Interests of Timely Opening and Repulse the Aerospace Attack Means «Prompt Global Strike». *Aerospace forces. Theory and practice*, 2020, vol. 16, pp. 99-115 (in Russian). Aviliable at: https://cyberleninka.ru/article/n/obosnovanie-perspektivnyh-napravleniy-razvitiya-sistemy-protivokosmicheskoy-oborony-rossiyskoy-federatsii-v-interesah (accessed: 20.12.2020).

7. Krasnoslobodcev V. P., Raskin A. V., Savel'ev S.S., Kupach O.S. Analysis of the possibilities for the implementation of the concept of USA Prompt global strike. *Strategicheskaya stabilnost'* [Strategic stability], 2014, vol. 67, no. 2, pp. 67-69 (in Russian).

8. Fenenko A. V. Prompt global strike in the context of the U.S. military strategy development. *Vestnik Moskovskogo universiteta. Seriya 25: Mezhdunarodnye otnosheniya i mirovaya politika*, 2016, vol. 8, no. 4, pp. 18-50 (in Russian).

9. Stuchinskiy V. I., Korolkov M. V. The aviation battle application justification aviation to disrupt an integrated massive air strike in the enemy multi-sphere operation. *Aerospace forces. Theory and practice*, 2020, no. 16. pp. 29-36 (in Russian).

10. *Sredstva vozdushno-kosmicheskogo napadeniya i vozdushno-kosmicheskoj oborony. Sostoyanie i razvitie* [*Means of air-space attack and air-space defense. Status and development*]. Moscow, "Planeta" Publ., 2017, 336 p. (in Russian).

11. Makarenko S. I. Information-Space Systems and Space Weapons – Current State and Prospects of Improvement. *Systems of Control, Communication and Security*, 2016, no. 4, pp. 161-213 (in Russian). DOI: 10.24411/2410-9916-2016-10409.

12. Makarenko S. I. *Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. Monografija* [*Models of communication systems in conditions of deliberate destabilizing impacts and intelligence. Monograph*]. Saint Petersburg, Naukoemkie Tehnologii Publ., 2020. 337 p. (in Russian).

13. Menshakov Iu. K. *Teoreticheskie osnovy tekhnicheskikh razvedok* [The theoretical basis of technical intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2008. 536 p. (in Russian).

14. *Dialektika tekhnologij vozdushno-kosmicheskoj oborony* [*Dialectics of aerospace defense technologies*]. Moscow, "Stolichnaya enciklopediya" Publishing House, 2011. 367 p. (in Russian).

15. Perunov Ju. M., Kupriianov A. I., *Radioelektronnaya bor'ba: radiotekhnicheskaya razvedka* [Electronic warfare: electronic intelligence]. Moscow, Vuzovskaya kniga Publ., 2017. 190 p. (in Russian).

16. Perunov Ju. M., Matsukevich V. V., Vasil'ev A. A. *Zarubezhnye radioelektronnye sredstva. Tom 2: Sistemy radioelektronnoi bor'by* [Overseas Radio-Electronic Equipment. Tom 2: Electronic Warfare Systems]. Moscow, Radiotekhnika Publ., 2010. 352 p. (in Russian).

17. Makarenko S. I., Ivanov M. S., Popov S. A. *Pomekhozashchishchennost' sistem sviazi s psevdosluchainoi perestroikoi rabochei chastity. Monografija*

[Interference Resistance Communication Systems with Frequency-Hopping Spread Spectrum. Treatise]. Saint Petersburg, Svoe Izdatelstvo Pabl., 2013, 166 p. (in Russian).

18. Piunov O., Shcherbinin R. Amerikanskij strategicheskij razvedyvatelnyj samolyot RC-135 i ego modifikacii [American strategic reconnaissance aircraft RC-135 and its modifications]. *Zarubezhnoe voennoe obozrenie*, 2012, no. 3, pp. 70-76 (in Russian).

19. Maksimenko A. Amerikanskie sistemy radioelektronnoj razvedki [American electronic intelligence systems]. *Zarubezhnoe voennoe obozrenie*, 2004, no. 9, pp. 45-49 (in Russian).

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

21. Shpenst V. Radiolokacionnye stancii distancionnogo zondirovaniya Zemli kosmicheskogo bazirovaniya [Space-based Earth remote sensing radars]. *Components & Technologies*, 2013, no. 3, pp. 154-158. Available at: https://kit-e.ru/assets/files/pdf/2013_3_154.pdf (accessed 10 February 2021) (in Russian).

22. Lisicyn A. Kosmicheskie sistemy distancionnogo zondirovaniya zemli zarubezhnyh stran [Space systems of remote sensing of the earth of foreign countries]. *Zarubezhnoe voennoe obozrenie*, 2019, no. 7, pp. 63-67. Available at: http://factmil.com/publ/strana/germanija/kosmicheskie_sistemy_distancionnogo_zondirovanija_zemli_zarubezhnykh_stran_2019/41-1-0-1666 (accessed 10 February 2021) (in Russian).

23. Baburin A., Pahomova A. Sostoyanie i perspektivy razvitiya sredstv kosmicheskoj vidovoj radiolokacionnoj razvedki zapadnoevropejskih stran [State and prospects of development of space specific radar reconnaissance facilities in Western European countries]. *Zarubezhnoe voennoe obozrenie*, 2017, no. 9, pp. 64-68. Available at: http://factmil.com/publ/strana/germanija/sostojanie_i_perspektivy_razvitija_sredstv_kosmicheskoj_vidovoj_radiolokacionnoj_razvedki_zapadnoevropejskikh_stran_2017/41-1-0-1217 (accessed 10 February 2021) (in Russian).

24. Gruzdov V. V., Kolkovskij Yu. V., Krishtopov A. V., Kudrya A. I. *Novye tekhnologii distancionnogo zondirovaniya Zemli iz kosmosa* [New technologies for remote sensing of the Earth from space]. Moscow, Technosphera Publ., 2018. 482 p. (in Russian).

25. Varlamov O. O. O sistemnom podkhode k sozdaniiu modeli komp'iuternykh ugroz i ee roli v obespechenii bezopasnosti informatsii v kliuchevykh sistemakh informatsionnoi infrastruktury [A systematic approach to creating models of computer threats and its role in information security in the key systems of information infrastructure]. *Izvestiya SFedU. Engineering sciences*, 2006, vol. 62, no. 7, pp. 216-223 (in Russian).

26. Pakhomova A. S., Pakhomov A. P., Yurasov V. G. To the implementation of the known computer attacks classification to develop a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16, no. 1, pp. 81-86 (in Russian).

27. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description. Version 1.3. Cigital Inc. 2008. Available at:

https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf (accessed 9 January2020) (in English).

28. Larina E. S., Ovchinskii V. S. *Kibervoiny XXI veka. O chem umolchal Edvard Snouden* [Cyberwar XXI century. What silent Edward Snowden]. Moscow, Knizhnyi Mir Publ., 2014. 352 p. (in Russian).

Статья поступила 12 марта 2021 г.

Информация об авторах

Афонин Илья Евгеньевич – кандидат технических наук, доцент. Доцент кафедры авиационного и радиоэлектронного оборудования. Краснодарское высшее военное авиационное училище летчиков. Область научных интересов: информационный конфликт средств воздушно-космического нападения и системы воздушно-космической обороны; радиолокационные системы обнаружения, распознавания и целеуказания; обработка радиолокационных сигналов. E-mail: ilyaafonin@yandex.ru

Адрес: Россия, 350090, г. Краснодар, ул. Дзержинского, д. 135.

Макаренко Сергей Иванович – доктор технических наук, доцент. Ведущий научный сотрудник. Санкт-Петербургский Федеральный исследовательский центр РАН. Профессор кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: 199178, Россия, Санкт-Петербург, 14 линия, д. 39.

Петров Сергей Валерьевич – соискатель ученой степени кандидата наук. Преподаватель кафедры авиационного и радиоэлектронного оборудования. Краснодарское высшее военное авиационное училище летчиков. Область научных интересов: устойчивость системы воздушно-космической обороны; радиоэлектронная борьба. E-mail: perskub@yandex.ru

Адрес: Россия, 350090, г. Краснодар, ул. Дзержинского, д. 135.

Descriptive model of intelligence systems used to detection the elements of an aerospace defense system and target designation when aerospace attack means are doing prompt global strike

I. E. Afonin, S. I. Makarenko, S. V. Petrov

Relevance**. The US has developed the prompt global strike concept. In order to means of aerospace attack accurately strike targets, these means joint to intelligence systems. Parameters of these systems determine the accuracy of the aerospace attack means. **The aim of the paper** is to form a descriptive model of intelligence systems used to detection the elements of an aerospace defence system and target designation when aerospace attack means are doing prompt global strike. The descriptive model is based on synthesis and analysis of exclusively open sources and publications. **Results and their novelty.** An element of the novelty of the model is generalized tactical and technical characteristics of standard space and air-based intelligence systems such as communications, electronic and computer intelligence systems. **Practical signifi-

cance. *The descriptive model presented in this paper will be useful for technical specialists to justify new technological solutions for the aerospace defence system. In addition, this model will be useful for researchers and carrying out study in the field of information conflict and in the field of the stability of the aerospace defence system.*

Keywords: *model, descriptive model, prompt global strike, aerospace defence system, aerospace attack means, communications intelligence, electronic intelligence, computer intelligence.*

Information about Authors

Ilya Evgenievich Afonin – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of aviation and radio-electronic equipment. Krasnodar Higher Military Aviation School of Pilots. Field of research: information conflict of air and space attacking means and air and space defense systems; radar detection; recognition and target designation systems; radar signal processing. E-mail: ilyaafonin@yandex.ru

Address: Russia, 350090, Krasnodar, Dzerzhinsky Street, 135.

Sergey Ivanovich Makarenko – Dr. habil. of Engineering Sciences, Docent. Leading Researcher. St. Petersburg Federal research center of the Russian Academy of Sciences. Professor of Information Security Department. Saint Petersburg Electrotechnical University 'LETI'. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197376, Saint Petersburg, 14th Linia, 39.

Sergey Valerievich Petrov – Lecturer at the Department of aviation and radio-electronic equipment. Krasnodar Higher Military Aviation School of Pilots. Field of research: stability of the aerospace defense system; electronic warfare. E-mail: perskub@yandex.ru

Address: Russia, 350090, Krasnodar, Dzerzhinsky Street, 135.