

## Решение задачи обнаружения и идентификации $n$ -мерных информационно-технических объектов путем использования кибернетического пространства

*к.т.н. В.В. Мухортов, д.т.н. И.Д. Королев*

*Краснодарское высшее военное училище им. генерала армии С.М. Штеменко*

**Аннотация:** В статье рассматривается применение кибернетического пространства для обнаружения  $n$ -мерных информационно-технических объектов и их последующей идентификации. Представлена концептуальная модель многомерной разведывательно-поисковой системы, описан разведывательный цикл поиска информационно-технических объектов, а также взаимосвязь радиотехнической разведки с кибернетической разведкой.

**Ключевые слова:** идентификация, информационно-технический объект, инфосфера, киберпространство, обнаружение, разведка, разведывательный цикл, распознавание.

Вопросы поиска являются одними из самых важнейших во всех сферах человеческой деятельности, из которых самыми актуальными являются задачи поиска реальных объектов.

Однако в настоящее время приобретает необходимость обнаружения нового класса объектов – информационно-технических (далее – ИТО), обладающих рядом специальных свойств, обусловленных особенностями их функционирования кроме общепринятого физического пространства в инфосфере (информационном пространстве; киберпространстве, как глобальном домене внутри инфосферы) [1], то есть объектов, обладающих виртуальностью, возможностью функционирования за границами физической реальности.

Сегодня наблюдается рост применения ИТО в условиях сложной радиоэлектронной обстановки, а также их миниатюризация (робототехнические комплексы, беспилотный автотранспорт, беспилотная авиация и т.д.) и автоматизация, что создает ряд опасностей как с точки зрения безопасности движения, так и с точки зрения общественной безопасности (террористические угрозы, экстремизм, нарушения границ

---

охраняемых объектов и др.), а также авиационной (авиакосмической) безопасности и требует разработки эффективных систем обнаружения, способных работать в любых условиях обстановки, что позволяет применять к ним, с использованием теории обнаружения сигналов, определенные научно-методические подходы к обнаружению, а также решить проблему идентификации, путем использования аппарата теории распознавания образов [2].

Все ИТО обладают рядом свойств, способных решить эти проблемы.

Решение этих вопросов расширяет теорию пространственного поиска на киберпространство, эволюционирующее сейчас в «метавселенные» [3].

Системы, реализующие функционал обнаружения, распознавания и идентификации, относятся к разведывательным (разведывательно-поисковым) системам (далее – РПС) и в процессе функционирования осуществляют разведывательные (разведывательно-поисковые) действия (мероприятия) (далее – РПД).

Они должны удовлетворять следующим требованиям: своевременность, достоверность, информативность (полнота) и точность данных, а для специализированных систем военного назначения: скрытностью, низкой уязвимостью, возможностью функционирования на территории занятой противником [4,5].

При рассмотрении основной задачи поиска подразумевается, что наблюдатель побуждается своей волей и намерением решить ее возможно лучше, наилучшим при данных условиях образом. Для того, чтобы решить эту задачу наилучшим образом, информация должна оцениваться с определенными критериями в требуемые сроки. Эти критерии должны определять решающую функцию, значения которой зависят от решений наблюдателя. Решающая функция в свою очередь определяет решающее правило, которое максимизирует (или минимизирует) эту функцию.

---

Решающее правило дает возможность делать соответствующий выбор при каждом наблюдении [6].

При принятии решения имеет значение достаточности информации, необходимой для анализа соответствующей решающей функции.

Согласно учению Вернадского о ноосфере [3], развитие человечества прошло следующие этапы: биосфера (около 100 млн. лет), техносфера (около 50 тыс. лет), инфосфера (около 5 тыс. лет), а также киберпространство (около 80 лет).

Однако, около 10 лет назад в киберпространстве начал формироваться феномен «метавселенных» (гибридных пространств), под которым первоначально стали понимать – обширную сеть постоянных реализуемых трехмерных миров и симуляций, которые поддерживают непрерывность идентичности, объектов, истории и прав и могут быть испытаны синхронно неограниченным числом пользователей, каждый из которых обладает индивидуальным ощущением присутствия (рис.1), что существенно меняет текущую картину мира и требует развития теорий, изучающих взаимодействие многомерных объектов, функционирующих в различных пространствах, к которым можно отнести ИТО.

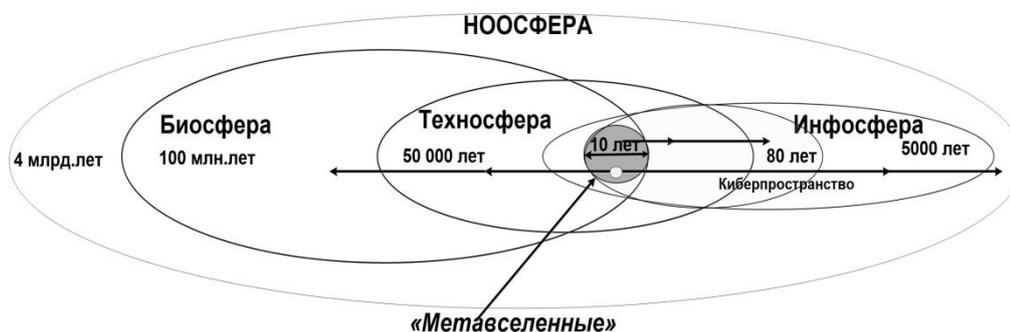


Рис. 1. – Ретроспективный анализ формирования «метавселенных» (гибридных пространств) и их связь с другими сферами

Для дальнейшего исследования в рамках синтеза в первую очередь теорий пространственного поиска и обнаружения сигналов [6,7] введем ряд определений [8-10].

Все имеющиеся РПС функционируют в рамках инфосферы.

Объект разведки (цель разведки, объект поиска, Ц) – то, что требуется обнаружить; цель. С точки зрения теории поиска могут быть подвижными (динамическими), либо неподвижными (статическими), иметь различную природу и располагаться в различных средах.

Цель разведки (поиска) – обнаружение разнообразных сторонних объектов в обследуемом пространстве с определением их характера и местоположения.

Обнаружение – выявление наблюдателем того или иного объекта, определение его положения на местности, в требуемом пространстве, а также характера его действий.

Распознавание:

1. Узнавание чего-либо по известным признакам;
2. Установление принадлежности данного элемента к определенному множеству по известному алгоритму;
3. Формирование образа при восприятии сигнала в деятельности человека-оператора.

Идентификация – установление соответствия ИТО конкретному типу, классу или же конкретному объекту (совокупности объектов), а также управляющих систем (контура управления и взаимодействия). Является высшей степенью процедуры распознавания.

Разведывательные процессы протекают в инфосфере, с учетом технологического развития формирующейся в единое разведывательно-информационное пространство (далее – РИП) [11,12].

Разведывательно-информационное пространство (*RP*) – глобальная информационная среда, реализующая основные цели разведки, а также обеспечивающая комплексную обработку сведений в реальном масштабе времени в интересах принятия решений по противодействию и эффективному применению имеющихся средств в различных условиях обстановки.

Инфосфера (*IS*) – это совокупность информации, информационных объектов, информационных процессов, информационной инфраструктуры (электро- и радиосвязь, средства передачи, тиражирования, хранения, воспроизведения, визуализации и обработки информации); сущностей (субъектов), осуществляющих сбор (добывание), транспортировку, обработку, хранение, распределение (распространение), производство и потребление информации, а также системы регулирования, возникающих при этом отношений производства, использования, владения и распоряжения информацией.

Основными видами разведки, направленными на ИТО, являются радиотехническая и кибернетическая разведка [9,12,13].

Радиотехническая разведка (*RTR*) – вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций, радионавигационных и радиотелекодowych систем, использует методы радиоприема, пеленгования и анализа радио сигнала.

Кибернетическая разведка (*KR*) – техническая разведка, осуществляемая путем извлечения и анализа информации, циркулирующей в киберпространстве. Осуществляется путем сбора информации, обрабатываемой в ЭВМ (компьютерах), информационно-телекоммуникационных сетях, ИТО, информации о характеристиках программных, аппаратных и программно-аппаратных средств ЭВМ

---

(компьютеров) и сетей, а также информации об их пользователях, их аватаров и систем искусственного интеллекта.

Киберпространство (*KIP*) – глобальный домен внутри информационной сферы, состоящий из взаимосвязанной сети информационно-технологических инфраструктур, включая «Интернет», телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

Все ИТО обладают рядом информативных параметров.

Информативные параметры (характеристики) объекта разведки (разведывательные, демаскирующие признаки) ( $S_m$ ) – признаки по которым можно обнаружить цель, отличить ее от других целей и дать ей характеристику.

Таким образом, объект разведки –  $\Pi$  можно представить в виде кортежа:

$$\Pi = \langle S_1, S_2, \dots, S_{m-1}, S_m \rangle. \quad (1)$$

Разведка должна обладать такими свойствами, как активность, разнообразие и упреждение.

Активность – деятельное, энергичное стремление к достижению целей РПД.

Разнообразиие – применение различных форм, способов и приемов РПД.

Упреждение – опережение действий искомого ИТО на свои системы.

Все объекты разведки обладают определенной информативностью.

Информативность – степень насыщенности источника информации.

РПД осуществляются в рамках функционирования разведывательного контура [14].

Разведывательный контур – интегрированная совокупность сил и средств, объединенных единым автоматизированным комплексом

управления, обеспечивающим выполнение поставленной задачи по обнаружению (распознаванию и идентификации) цели.

Согласно классической теории поиска, основной задачей является поиск объекта, эффективность которой выражается через два критерия оценки эффективности [2]:

- 1.) вероятность обнаружения цели (результативность разведки);
- 2.) средняя продолжительность процесса поиска (оперативность).

Результативность разведки ( $Y_{\text{Э}}$ ) – определение возможности получения разведанных рассматриваемым средством разведки в заданных условиях. Выражается через вероятность обнаружения объекта, дальности действия технических средств разведки и точности определения местоположения объекта и ошибки измерения его параметров, а также вероятности ошибки воспроизведения перехваченных сообщений.

Система позиционирования – это механизм определения положения объекта в требуемом пространстве.

Целенаправленность – четкая определенность задач и их реализация в строгом соответствии с целями.

Оперативность ( $Y_R$ ) – своевременное реагирование на изменение информационной обстановки, обеспечивающее максимальную результативность. Оперативность выражается через временные характеристики, зависящие от дальности обнаружения, распознавания и/или идентификации.

Дальность обнаружения ( $D_{\text{ОБН}}$ ) – максимальное расстояние между станцией разведки и объектом, при котором обнаружение и измерение координат объекта осуществляется с заданными вероятностями правильного обнаружения и ложной тревоги или измерение его параметров с заданной среднеквадратичной погрешностью.

Дальность распознавания ( $D_{РАСП}$ ) – максимальное расстояние между РПС и объектом, при котором осуществляется распознавание с заданными вероятностями правильного распознавания ( $P_{РАСП}$ ) и ложной тревоги ( $P_{Л.ТР}$ ).

Дальность идентификации ( $D_{ИДЕНТ}$ ) – максимальное расстояние на котором РПС может гарантированно идентифицировать цель РПД с установленными критериями.

Эффективная (требуемая) дальность разведывательной системы ( $D_{ТРЕБ}$ ) – способность РПС обнаруживать (распознавать и/или идентифицировать) цель РПД в заданных границах установленных критериев.

Таким образом,  $D_{ОБН} + D_{РАСП} + D_{ИДЕНТ} \leq D_{ТРЕБ}$ .

Время затрачиваемое на выполнение РПД должно стремиться к *min*:  $t_{обн} + t_{расп} + t_{иден} \rightarrow \min$ , при чем для реализации  $Y_R \rightarrow \max$  эта сумма должна быть не более времени требуемого –  $t_{треб}$  для достижения эффективной дальности разведывательной системы:  $t_{обн} + t_{расп} + t_{иден} \leq t_{треб}$ .

Непрерывность – непрекращающееся ведение РПД во всех видах функционирования РПС.

Исходя из [4,7] задача обнаружения включает в себя по три основных элемента:

событие → наблюдение → решение, или же

объект поиска → разведка → решение на противодействие.

Разведка, являющаяся производной от наблюдения, включает ряд процедур:

процедура сбора информации → процедура анализа информации → процедура обнаружения → процедура распознавания → процедура привязки к системам позиционирования.

В зависимости от требуемого качества, распознавание может делиться на процедуру первичного распознавания и идентификацию обнаруженного объекта.

Комплекс разведывательных процедур представляет собой разведывательный цикл (рис. 2).



Рис. 2. – Разведывательный цикл поиска ИТО

При ряде допущений [7] вероятность обнаружения ИТО можно выразить формулой:

$$P_{обн}(\Phi) = 1 - e^{-\Phi}, \quad (1)$$

где  $\Phi$  – поисковый потенциал РПС.

Смысл данной формулы можно выразить через функцию  $p(x)$ , характеризующую вероятность обнаружения цели, расстояние до которой в физическом пространстве равняется  $x$ .

Согласно [7] наиболее подходящей мерой, выражающей эффективность осуществления РПД в имеющихся РПС является ширина полосы обзора –  $W$

$$W = \int_{-\infty}^{+\infty} p(x) d(x). \quad (2)$$

Всю обследуемую площадь обследуемой области (района, зоны)  $\Omega$  можно обозначить через  $V_{\Omega}$ . Исходя из [4] поисковое покрытие  $E$ , находится

в зависимости от маршрута перемещения цели внутри области  $\Omega$  –  $L$  и ширины полосы обзора –  $W$

$$E = WL, \quad (3)$$

а единичный поисковый потенциал РПС прямо пропорционален размеру поискового покрытия  $E$  и обратно пропорционален размеру обследуемой области  $V_{\Omega}$ , то есть:

чем больше обследуемая область, при имеющейся возможности поискового покрытия, тем меньше поисковый потенциал РПС  $\Phi$ ;

или же чем больше возможность поискового покрытия при имеющейся обследуемой области, тем он выше:

$$\Phi = E / V_{\Omega}. \quad (4)$$

В ходе разбиения маршрута движения цели на  $N$  участков мы получим, что вероятность обнаружения на  $n$ -ом участке будет иметь следующее значение:

$$p_n = \Phi / N. \quad (5)$$

А общая вероятность обнаружения цели на всем маршруте передвижения будет равна:

$$P_N = 1 - (1 - p_n)^N. \quad (6)$$

Подставляя сюда (5) при  $N \rightarrow \infty$  согласно второго замечательного предела получаем формулу (1).

Однако с учетом технологического развития и совершенствования способов противодействия объектам  $\mathbf{Ц}$ , классическое обнаружение становится не достаточным и, в зависимости от целей и возможности систем искусственного интеллекта, может принимать следующий вид:

при наличии требований по обнаружению и распознаванию ( $P_{\mathbf{Ц\_OP}}$ )

$$P_{\mathbf{Ц\_OP}} = P_{\text{обн}} P_{\text{расп}}, \quad (7)$$

а при наличии требований по обнаружению и идентификации, которой в обязательном порядке предшествует первичное распознавание ( $P_{Ц_{ОИ}}$ )

$$P_{Ц_{ОИ}} = P_{обн} P_{пер.расп} P_{идент} . \quad (8)$$

Эти вероятности являются условными, и каждая следующая вероятность принимает свое некоторое значение, при условии, что вероятности предыдущих этапов уже равны единице.

Поисковый потенциал обладает свойством аддитивности, т.е. чем больше средств и способов разведки, которые обладают потенциалом  $\Phi_i$ , тем он выше:

$$\Phi = \Phi_1 + \Phi_2 + \dots + \Phi_{i-1} + \Phi_i . \quad (9)$$

Таким образом, конечные формулы, характеризующие цели РПД и возможности РПС примут вид:

$$P_{Ц_{ОР}}(\Phi) = 1 - e^{-\Phi} , \quad (10)$$

или же:

$$P_{Ц_{ОИ}}(\Phi) = 1 - e^{-\Phi} . \quad (11).$$

Поисковый потенциал зависит от возможности РПС анализировать в РИП определенных параметров (характеристик) –  $S_m$  объекта разведки  $\mathbf{Ц}$  и значение  $P_{Ц_{ОР}}$  и  $P_{Ц_{ОИ}}$  при наличии одного потенциала  $\Phi$  будут отличаться.

Таким образом: увеличивая размер поискового покрытия –  $E$  РПС мы увеличиваем поисковый потенциал  $\Phi$ , а с его увеличением мы увеличиваем  $P_{Ц_{ОР}}$  и  $P_{Ц_{ОИ}}$  соответственно.

Наиболее полное раскрытие структуры ИТО в киберпространстве в настоящее время возможно через концепцию цифровых двойников, введенную в 2003 году [14-16]. В общем виде под цифровым двойником понимают – виртуальное представление физического продукта, содержащего информацию об указанном продукте, с его характеристиками в области управления жизненным циклом.

Цифровой двойник включает в себя следующие взаимосвязанные элементы: физический объект, виртуальное представление этого объекта и двунаправленный канал связи для передачи данных от физического к виртуальному объекту, и обратно — от виртуального к физическому.

В основе этой концепции лежит идея о том, что виртуальное пространство состоит из неограниченного количества подпространств, которые позволяют выполнять определенные виртуальные операции.

Эта концепция до настоящего времени находила применение только в промышленности и при моделировании объектов для научных исследований, но в обязательном порядке в ней является интегрированная система физической и виртуальной сред взаимодействия объектов реального и виртуальных миров, как элементов киберпространства.

Физическая среда относится к пространству «реального мира», в котором находится физический объект исследования.

В отличие от физической среды, описания виртуальной среды иногда называют базовой технологией, такой как «база данных», «хранилище данных», «облачная платформа», «сервер», «API» (*Application Programming Interface*, программный интерфейс приложений), и т.п., что подтверждает невозможность создания и реализации единой технологии работы с цифровыми двойниками.

Необходимым условием функционирования киберфизических систем является наличие физико-виртуальных связей между физическим объектом и его виртуальным аналогом. Физико-виртуальные связи — это средства, с помощью которых состояние физического объекта передается в виртуальную среду и реализуется в ней, т.е. происходит обновление виртуальных параметров таким образом, чтобы они отражали текущее состояние физических параметров. К ним можно отнести датчики интернета вещей, сервисы, 5G, и т.п. Описание цифрового двойника невозможно без

---

физического и виртуального взаимодействия между объектами. Соединение состоит из фазы метрологии, в которой фиксируется состояние физического объекта, и фазы реализации, в которой рассчитывается погрешность между физической и виртуальной моделями.

Виртуально-физическая связь представлена потоком информации и процессов от виртуального к физическому объекту, т.е. цифровой двойник содержит функциональные возможности для физического влияния на состояние реального объекта.

По своим особенностям ИТО являются одной из ступеней развития киберфизических систем. Таким образом, видна реальная взаимосвязь между элементами ИТО в киберпространстве и физической реальности.

Отсюда возникает следующая проблема: создание соответствующей системы координат в киберпространстве с последующей привязкой к физическому пространству для отслеживания перемещения ИТО в кибернетическом и физическом пространствах.

Формируемое координатное пространство должно учитывать все характеристики ИТО в киберпространстве с учетом модели OSI, что позволит осуществить проецирование  $n$ -мерного ИТО в физическое пространство (рис. 3).

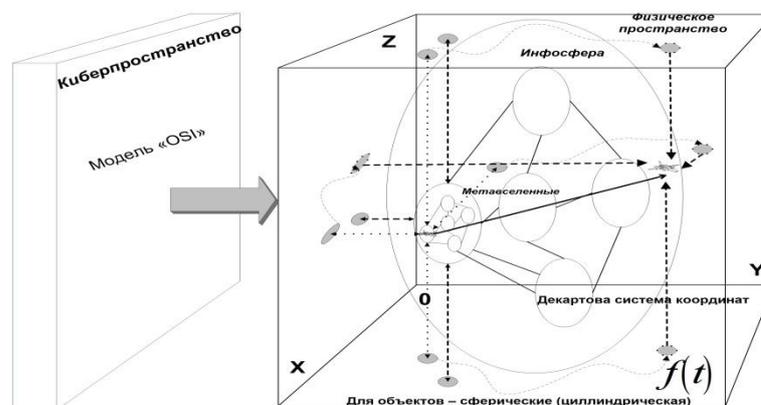


Рис. 3. – Проецирование  $n$ -мерного ИТО в физическое пространство

Как видно из рисунка,  $n$ -мерный ИТО может функционировать в одной (в нескольких) из множества метавселенных, являющихся следующей ступенью эволюции киберпространства [17].

С учетом особенностей взаимосвязи метавселенных с физической реальностью можно произвести соответствующую привязку координат в метавселенных с физическим пространством путем преобразования их в Декартову систему координат (сферическую или цилиндрическую), тем самым получив соответствующую проекцию обнаруженного ИТО в киберпространстве в привычное физическое пространство.

С учетом многомерности, а также неопределенного количества возможных измерений и пространственной неоднородности любой статический ИТО, находящийся в трехмерном, или динамический ИТО, находящийся в четырехмерном физическом пространстве, обладает определенным множеством признаков  $S$  (рис. 4).

Этот объект проецирует свою первичную структуру в иные пространства, которые могут быть ближайшими пространствами, непосредственно проистекающими из нашего, которое мы будем считать эталонным пространством в количестве от 1 до  $m$ , а также производными от них в количестве от 1 до  $n$ .

В ближайших измерениях, которые будут производными от  $S$  первого порядка, структура будет принимать вид от 0 до  $S'm$ .

Производные второго порядка, в котором отображается вторичная структура нашего объекта  $S$  от  $S'0$ , будет принимать вид от  $S'1$  до  $S'n$  и так далее. Все эти структуры взаимосвязаны между собой и сходятся в точке, характеризующей структуру  $S$ . Таким образом, при выполнении определенных операций, можно из любой системы измерений и пространств выйти в наше эталонное  $S$ .

---

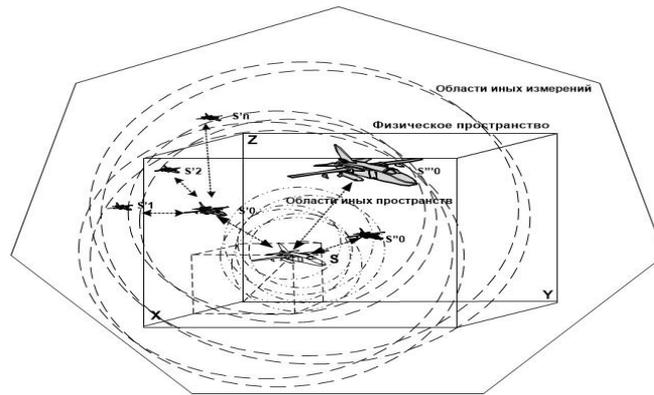


Рис. 4. – Соответствие сред и сфер функционирования  $n$ -мерного ИТО

Это, в целом, соответствует основным концепциям  $M$ -теории вселенной, восприятие которой ограничивается нашими возможностями относительно структуры  $S$  [18].

Так как размеры  $V_{\Omega}$  зависят от зоны  $\Omega$ , находящейся в определенной зависимости от законов пространства, в котором она находится, увеличение  $\Phi$  возможно за счет увеличения  $E$ , которая также зависит от того же пространства, в котором функционирует объект структуры  $S$ . Увеличение  $E$  возможно за счет обхода законов эталонного пространства, путем работы с иными пространствами и применяемыми в них системами измерений путем рассмотрения структур от  $S^0$  до  $S^n$ , и их производных.

Однако, чем больше  $S^n$ , тем больше итераций требуется для восстановления исходной структуры  $S$ , что также ограничивает наши возможности по расширению поискового потенциала  $E$  РПС.

Это позволяет нам с учетом разведывательного цикла, представленного на рис. 2, сформировать соответствующую концептуальную модель любой РПС (рис. 5).

Для обнаружения объекта разведки (цели)  $\Pi$ , применяется поиск определенных характеристик (параметров объекта разведки, демаскирующих

признаков)  $S-m$ , свидетельствующих о его существовании в некотором пространстве  $S$  и/или иных пространствах  $S'n$ .



Рис. 5. – Концептуальная модель РПС

Обработка найденных параметров осуществляется в разведывательном контуре, включающем в себя различные подсистемы ( $PC-n$ ), работающие с определенными характеристиками объектов (пространствами и системами измерений), осуществляющие анализ поступающих параметров  $S-m$  и генерирующие определенные результаты после их анализа ( $R-n$ ) в зависимости от цели РПД и возможностей РПС.

Далее информация должна поступать на подсистему обнаружения (и первичного распознавания), после чего может производиться идентификация ИТО с последующей привязкой объекта разведки (цели) Ц в требуемой системе позиционирования.

Далее, в зависимости от результата, включается в работу система поддержки принятия решения на противодействие обнаруженному объекту.

Весь комплекс решений можно разделить на 3 основных класса:

- активное (проактивное) противодействие. Активное противодействие осуществляется в форме какого-либо действия по отношению к объекту

разведки (цели) Ц, причем противодействие может иметь проактивный характер, то есть осуществлять противодействие только при наступлении определенных факторов;

- пассивное противодействие. Пассивное противодействие осуществляется в виде бездействия по отношению к объекту разведки, путем изменения своих характеристик, позволяющих избежать взаимодействие с объектом разведки (цели) Ц;

- ликвидация последствий взаимодействия с объектом разведки. Этот класс действий реализуется, если активное (проактивное) и пассивное противодействие не привели к успеху, или же система обнаружения и идентификации не выполнила свой функционал в требуемые сроки, и произошло нежелательное взаимодействие с объектов разведки (цели) Ц (столкновение).

Также при наличии систем идентификации наша система получит гораздо более высокий выигрыш (будет более эффективна), чем без них, путем принятия более «правильных» решений, т.е.  $Y_3 \rightarrow \max$ , путем сокращения времени на принятие решения по противодействию цели Ц.

Частный случай, рассматривающий синтез двух направлений РПД, а именно радиотехнической разведки *RTR* и киберразведки *KR*, представлен на рис. 6.



Рис. 6. – Комплексная система обнаружения и идентификации ИТО

Подсистема *RTR* взаимодействует с инфосферой *IS* на уровнях радио сигналов.

Подсистема *KR* взаимодействует с инфосферой, через киберпространство *KIP*, путем извлечения и анализа информации, циркулирующей в киберпространстве. Данная информация имеет привязку к излучению ИТО и взаимодействующих с ним системами.

Сама по себе подсистема *RTR* не может реализовать функцию идентификации цели [19,20], в отличие от подсистемы *KR* [1], однако она является базисной (несущей) для киберпространства.

Таким образом, эффективное обнаружение и идентификация ИТО (в первую очередь воздушных и малозаметных, в том числе функционирующих в условиях сложной радиоэлектронной обстановки – городских условиях) реализуема с использованием гибридных РСП, интегрированных с системами киберразведки.

Выводы: таким образом, решение проблемы идентификации ИТО для противодействия им при организации транспортной (авиационной) безопасности, кибербезопасности и охраны объектов (снижении разведдоступности, повышении разведзащищенности и обеспечении живучести) становится возможной с включением в разведывательный контур средств кибернетической разведки.

Развитие комплексных систем обнаружения и идентификации ИТО с использованием средств радиотехнической и кибернетической разведки позволит в дальнейшем расширить:

- теорию пространственного поиска на *n*-мерные (в том числе виртуальные) пространства;
- теорию обнаружения сигналов на теорию пространственного поиска, путем синтеза их научно-методического аппарат;

- теорию распознавания образов с использованием концепции «цифровых двойников» на теорию пространственного поиска и теорию принятия решений, путем максимизации решающей функцией.

### Литература

1. Мухортов В.В., Нефедьев Ю.В. Метод оценки живучести информационно-технических объектов по отношению к программно-аппаратным воздействиям // Инженерный вестник Дона, 2020, №4. URL: ivdon.ru/ru/magazine/archive/n4y2020/6414 (дата обращения: 18.04.2022).

2. Обнаружение, распознавание и определение параметров образов объектов. Методы и алгоритмы / Под ред. А.В. Коренного. – М.: Радиотехника, 2012. – 112 с.

3. Соловьёв И.В. О происхождении и содержании понятия «инфосфера». инфосфера как объект исследования наук об информации // Фундаментальные исследования. – 2013. – № 6-1. – С. 66-71; URL: fundamental-research.ru/ru/article/view?id=31415 (дата обращения: 18.04.2022).

4. Терентьев А.В., Коротков В.Ф. Радиотехническая разведка: Теория и практика обработки радиолокационных сигналов. – Санкт-Петербург: Медиапапир, 2021. – 346 с.

5. 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.

6. Акимов П.С., Бакут П.А., Богданович В.А., Бриккер А.М., Валеев В.Г., Власов И.Б., Корато В.В., Розанов В.А, Трифонов А.П. Теория обнаружения сигналов / Под ред. П.А. Бакута. – М.: Радио и связь, 1984 – 440 с.

7. Ким Д.П. Методы поиска и преследования подвижных объектов. – М.: Наука, 1989. – 336 с.

8. Бойко А.А., Балыбин В.А., Донсков Ю.Е. О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства // Военная Мысль. 2013. № 9. С. 28-32.

9. 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.

10. Фиговский О.Л. В интервале пяти лет появятся инновации, которые сегодня кажутся фантастикой// Инженерный вестник Дона, 2011, №4. URL: [ivdon.ru/ru/magazine/archive/n4y2011/643](http://ivdon.ru/ru/magazine/archive/n4y2011/643) (дата обращения: 18.04.2022).

11. Морз Ф. Теория поиска. Исследование операций. – Т. 1. – М.: Мир. 1981. – С. 549-629.

12. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. – СПб.: Научно-технические технологии, 2017. – 546 с.

13. Кошелев В.И. Основы теории радиосистем и комплексов радиоэлектронной борьбы: Учебное пособие. – М. : Общество с ограниченной ответственностью Издательство «КУРС», 2021. – 200 с.

14. Грошева Е.С. Конкурентная разведка в структуре современной организации // Модели, системы, сети в экономике, технике, природе и обществе. – 2020. – № 4(36). – С. 5-13.

15. Merah Y., Kenaza T. Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence // ACM International Conference Proceeding Series : 16, Virtual, Online, 17–20 августа 2021 года. – Virtual, Online, 2021. – P. 3470024. – DOI 10.1145/3465481.3470024

16. Сливицкий А.Б. Обзор и анализ современных инструментов поддержки создания перспективной техники // Большая Евразия: развитие, безопасность, сотрудничество: ежегодник, Москва, 06–07 октября 2021 года.

---

– Москва: Институт научной информации по общественным наукам РАН, 2022. – С. 955-961.

17. Мельник Н.А. Основные направления развития средств воздушно-космического нападения США и НАТО. Часть 1 // Зарубежное военное обозрение. – 2015. – № 8. – С. 65–71.

18. Галушкин А.И. Синтез многослойных систем распознавания образов. – М.: Энергия, 1974. 220 с.

19. Королев И.Д., Мухортов В.В. Современные научно-методические подходы к обнаружению и идентификации информационно-технических объектов, перспективы их обнаружения и идентификации в инфосфере // Информационные системы и технологии. – 2022. – № 2(130). – С. 100-106. – EDN UAVEBG.

20. Gylling A., Eliasson P., Ekstedt M., Afzal Z. Mapping cyber threat intelligence to probabilistic attack graphs // Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021, Virtual, Rhodes, 26–28 июля 2021 года. – Virtual, Rhodes, 2021. – P. 304-311.

### References

1. Mухортov V.V., Nefed'ev YU.V. Inzhenernyj vestnik Dona, 2020, №4, URL: [ivdon.ru/ru/magazine/archive/n4y2020/6414](http://ivdon.ru/ru/magazine/archive/n4y2020/6414).

2. Obnaruzhenie, raspoznavanie i opredelenie parametrov obrazov ob"ektov. Metody i algoritmy [Detection, recognition and determination of the parameters of object images. Methods and algorithms]. Pod red. A.V. Korennogo. M.: Radiotekhnika, 2012. 112 p.

3. Solov'yov I.V. Fundamental'nye issledovaniya. 2013. № 6-1. pp. 66-71; URL: [fundamental-research.ru/ru/article/view?id=31415](http://fundamental-research.ru/ru/article/view?id=31415).

4. Terent'ev A.V., Korotkov V.F. Radiotekhnicheskaya razvedka: Teoriya i praktika obrabotki radiolokacionnyh signalov [Electronic Intelligence: Theory and practice of processing of radiolocation signals].

Theory and Practice of Radar Signal Processing]. Sankt-Peterburg: Mediapapir, 2021. 346 p.

5. Makarenko S.I., Koval'skij A.A., Afonin I.E. Vozdushno-kosmicheskie sily. Teoriya i praktika. 2020. № 16. pp. 99-115.

6. Akimov P.S., Bakut P.A., Bogdanovich V.A., Brikker A.M., Valeev V.G., Vlasov I.B., Korado V.V., Rozanov V.A, Trifonov A.P. Teoriya obnaruzheniya signalov [Signal Detection Theory]. Pod red. P.A. Bakuta. M.: Radio i svyaz', 1984. 440 p.

7. Kim D.P. Metody poiska i presledovaniya podvizhnyh ob"ektov [Methods of searching and chasing moving objects]. M.: Nauka, 1989. 336 p.

8. Bojko A.A., Balybin V.A., Donskov YU.E. O terminologii v oblasti radioelektronnoj bor'by v usloviyah sovremennogo informacionnogo protivoborstva. Voennaya Mysl'. 2013. № 9. pp. 28-32.

9. Men'shakov YU.K. Teoreticheskie osnovy tekhnicheskikh razvedok: ucheb.posobie [Theoretical foundations of technical intelligence: a textbook]. Pod red. YU.N. Lavruhina. M.: Izd-vo MGTU im. N.E. Baumana, 2008. 536 p.

10. Figovskij O.L. Inzhenernyj vestnik Dona, 2011, №4. URL: [ivdon.ru/ru/magazine/archive/n4y2011/643](http://ivdon.ru/ru/magazine/archive/n4y2011/643).

11. Morz F. Teoriya poiska. Issledovanie operacij [Search theory. Operations Research]. T. 1. M.: Mir. 1981. pp. 549-629.

12. Makarenko S.I. Informacionnoe protivoborstvo i radioelektronnaya bor'ba v setecentricheskikh vojnah nachala XXI veka. Monografiya. [Information warfare and electronic warfare in the network-centric wars of the beginning of the XXI century. Monograph.]. SPb.: Naukoemkie tekhnologii, 2017. 546 p.

13. Koshelev .I. Osnovy teorii radiosistem i kompleksov radioelektronnoj bor'by: Uchebnoe posobie. [Fundamentals of the theory of radio systems and electronic warfare complexes: Textbook]. M.: Obshchestvo s ogranichennoj otvetstvennost'yu Izdatel'stvo «KURS», 2021. 200 p.

---

14. Grosheva E.S. Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve. 2020. № 4(36). pp. 5-13.
15. Merah Y., Kenaza T. Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. ACM International Conference Proceeding Series : 16, Virtual, Online, 17–20 avgusta 2021 goda. Virtual, Online, 2021. pp. 3470024.
16. Slivickij A.B. Bol'shaya Evraziya: razvitie, bezopasnost', sotrudnichestvo: ezhegodnik, Moskva, 06–07 oktyabrya 2021 goda. Moskva: Institut nauchnoj informacii po obshchestvennym naukam RAN, 2022. pp. 955-961.
17. Mel'nik N.A. Zarubezhnoe voennoe obozrenie. 2015. № 8. pp. 65–71.
18. Galushkin A.I. Sintez mnogoslojnyh sistem raspoznavaniya obrazov. [Synthesis of multilayer image recognition systems]. M.: Energiya, 1974. 220 p.
19. Korolev I.D., Muhortov V.V. Informacionnye sistemy i tekhnologii. 2022. № 2(130). pp. 100-106.
20. Gylling A., Eliasson P., Ekstedt M., Afzal Z. Mapping cyber threat intelligence to probabilistic attack graphs. Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021, Virtual, Rhodes, 26–28 iyulya 2021 goda. Virtual, Rhodes, 2021. pp. 304-311.